МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ИНСТИТУТ ТЕКСТИЛЬНОЙ И ЛЕГКОЙ ПРОМЫШЛЕННОСТИ

Кафедра «Автоматизация и управление технологических процессов и производств»

ст. пр. Жукова Ю. А

Лекции по курсу

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И КОММУНИКАЦИОННЫЕ СЕТИ

Для студентов бакалавриата по направлению
5311000- Автоматизация и управление производственными и технологическими процессами

Ташкент – 2014

Материал предназначен для изучения и приобретения знаний и практических навыков в построении, настройке и обслуживании локальных компьютерных сетей. Концепции и понятия, которые подробно изложены в лекциях, позволят получить неоценимые сведения по установке кабельных систем, маршрутизации, IP-адресации, протоколах маршрутизации и обслуживании сетей. В лекциях рассмотрены особенности операционных систем, сетового оборудования, протоколов TCP/IP, списков управления доступом, коммутации и маршрутизации.

Предложенные темы расширят знания и практические навыки студентов в области проектирования, конфигурирования и поддержки коммутаторов, локальных сетей и виртуальных локальных сетей. Изложенные в лекциях понятия и концепции позволят студентам приобрести практический опыт в конфигурировании сетей локальных сетей LAN, распределенных сетей, расширенного протокола маршрутизации внутреннего шлюза. В дополнение к этому тематика лекций позволяет расширить знания и практические навыки в сфере использования распределенных сетей WAN.

Лекционный материал предназначен для бакалавров специальностей 5311000 – Автоматизация и управление производственными и технологическими процессами (для текстильной, лёгкой и хлопковой промышленности), а так же для других направлений и специальностей в сфере изучения современных коммуникационных и сетевых технологий.

Материал подготовлен в соответствии и типовой программой.

Составитель: ст. пр. Ю. А. Жукова

Рецензенты: д.т.н., проф. Марахимов А.Р. (ТГТУ)
к.т.н., доц. Атамирзаев М. (ТИТЛП)

Рассмотрено и утверждено на заседании учебно-методического совета ТИТЛП

Протокол № от 201 года

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современная эпоха характеризуется стремительным процессом информатизации общества. Это сильней всего проявляется в росте пропускной способности и гибкости информационных сетей. Полоса пропускания в расчете на одного пользователя стремительно увеличивается благодаря нескольким факторам. Во-первых, растет популярность приложений World Wide Web и количество электронных банков информации, которые становятся достоянием каждого человека. Падение цен на компьютеры приводит к росту числа домашних ПК, каждый из которых потенциально превращается в устройство, способное подключиться к сети Internet. Во-вторых, новые сетевые приложения становятся более требовательными в отношении полосы пропускания – входят в практику приложения Internet, ориентированные на мультимедиа и видеоконференцсвязь, когда одновременно открывается очень большое количество сессий передачи данных. Как результат, наблюдается резкий рост в потреблении ресурсов Internet – по оценкам средний объем потока информации в расчете на одного пользователя в мире увеличивается в 8 раз каждый год.

Противодействовать растущим объемам передаваемой информации на уровне сетевых магистралей можно только привлекая оптическое волокно. И поставщики средств связи при построении современных информационных сетей используют волоконно-оптические кабельные системы наиболее часто. Это касается как построения протяженных телекоммуникационных магистралей, так и локальных вычислительных сетей. Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния. Волоконная оптика, став главной рабочей лошадкой процесса информатизации общества, обеспечила себе гарантированное развитие в настоящем и будущем. Сегодня волоконная оптика находит применение практически во всех задачах, связанных с передачей информации. Стало допустимым подключение рабочих станций к информационной сети с использованием волоконно-оптического миникабеля. Однако, если на уровне настольного ПК волоконно-оптический интерфейс только начинает единоборство с проводным, то при построении магистральных сетей давно стало фактом безусловное господство оптического волокна. Коммерческие аспекты оптического волокна также говорят в его пользу – оптическое волокно изготавливается из кварца, то есть на основе песка, запасы которого очень велики. Стремительно входят в нашу жизнь волоконно-оптические интерфейсы в локальных и региональных сетях Ethernet, Fast Ethernet, FDDI, Gigabit Ethernet, ATM. Настоящий дипломный проект ставит своей целью показать возможности современного оборудования для построения сетей в области волоконно-оптических технологий, раскрыть технологические особенности планирования, построения и эксплуатации волоконно-оптических сетей.

Лекция 1
Архитектура компьютера

1. **Структура информационной системы: аппаратная и информационная составляющие, их взаимодействие.**
2. **Основные типы современных компьютеров.**
3. **Основные блоки компьютера и их функциональное назначения и характеристики.**

Ключивые слова: информационная система, информационная база, мэйнфреймы, миниэвм, суперкомпьютеры, рабочая станция, персональный компьютер, блоки компьютера, системная шина, периферийные устройства

1. Структура информационной системы: аппаратная и информационная составляющие, их взаимодействие

Информационная система (ИС) – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Современное понимание ИС предполагает использование в качестве основного технического средства переработки информации персонального компьютера.

Необходимо понимать разницу между компьютерами и ИС. Компьютеры, оснащены специализированными программными средствами, являются технической базой и инструментом для ИС. Без персонала, взаимодействующего с компьютерами и телекоммуникациями, ИС немыслима.

Структуру ИС составляет совокупность отдельных ее частей, называемых подсистемами (часть системы, выделенная по какому-либо признаку).

Общую структуру ИС можно рассматривать как совокупность подсистем независимо от сферы применения. Таким образом, структура любой ИС может быть представлена совокупностью обеспечивающих подсистем.

Информационное обеспечение состоит в своевременном формировании и выдаче достоверной информации для принятия решений.

Техническое обеспечение – комплекс технических средств, обеспечивающих работу ИС, а также соответствующая документация на эти средства и технологические процессы. Комплекс технических средств составляют: компьютеры любых моделей; устройства сбора, накопления, обработки, передачи и вывода информации; устройства передачи данных и линии связи; оргтехника и устройства автоматического считывания информации; эксплуатационные материалы и др.

Математическое и программное обеспечение – совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств.

Информационное обеспечение ИС является средством для решения следующих задач: однозначного и экономического представления информации в системе (на основе кодирования

объектов); организации процедур анализа и обработки информации с учетом характера связей объектами (на основе классификации объектов); организации взаимодействия пользователей с системой (на основе экранных форм ввода-вывода данных); обеспечения эффективного использования информации в контуре управления деятельностью объекта автоматизации (на основе унифицированной системы документации).

Информационное обеспечение ИС включает два комплекса: внемашинное и информационное обеспечение (классификаторы технико-экономической информации, документы, методические инструктивные материалы) и внутримашинное информационное обеспечение (макеты/экранные формы для ввода первичных данных в ЭВМ или вывода результатной информации, структуры информационной базы: входных, выходных файлов, базы данных).

Внемашинное информационное обеспечение обеспечивает эффективный поиск, обработку на ЭВМ и передачу по каналам связи технико-экономической информации, ее необходимо представить в цифровом виде. С этой целью ее нужно сначала упорядочить (классифицировать), а затем формализовать (закодировать) с использованием классификатора.

Основной компонент внемашинного информационного обеспечения ИС является система документации, применяемая в процессе управления экономическим объектом. Под документом понимается определенная совокупность сведений, используемая при решении технико-экономических задач, расположенная на материальном носителе в соответствии с установленной формой.

Внутримашинное информационное обеспечение включает макеты (экранные формы) для ввода первичных данных в ЭВМ или вывода результатной информации, и структуры информационной базы: входных, выходных файлов, базы данных.

Основной частью внутримашинного информационного обеспечения является информационная база (ИБ) – совокупность данных, организованная определенным способом и хранимая в памяти вычислительной системы в виде файлов, с помощью которых удовлетворяются информационные потребности управленческих процессов и решаемых задач.

С точки зрения программно-аппаратной реализации можно выделить ряд типовых архитектур ИС.

Традиционные архитектурные решения основаны на использовании выделенных файл-серверов или серверов баз данных. Существует также варианты архитектур информационных систем, базирующихся на технологии Internet (Internet-приложения). Следующая разновидность архитектуры информационной системы основывается на концепции «хранилища данных» (Data Warehouse) – интегрированной информационной среды, включающей разнородные информационные ресурсы. И, наконец, для построения глобальных распределенных информационных приложений используется архитектура интеграции информационно-вычислительных компонентов на основе объектно-ориентированного подхода.

2. Основные типы современных компьютеров.

Все компьютеры обрабатывают информацию одними и теми же методами, но при этом по-разному классифицируются. Мы используем такие показатели как физические размеры и

скорость обработки данных, для того чтобы подразделить современные компьютеры на большие универсальные ЭВМ, миникомпьютеры, микрокомпьютеры, и суперкомпьютеры.

Признак, по которому разделяются компьютеры, - платформа.

Платформа IBM-современных компьютеров включает громадный спектр самых различных компьютеров, от простеньких домашних персоналок до сложных серверов.

Платформа Apple представлена довольно популярными на Западе компьютерами серии Macintosh. Они используют свое, особое программное обеспечение, да «начинка» их существенно отличается от IBM-ской.

Большие универсальные ЭВМ (mainframes) или ***мэйнфреймы*** – машины размером с комнату, памятью очень большой емкости, обеспечивающие сверхбыструю скорость обработки данных. Они используются для очень крупных коммерческих, научных и военных приложений, где компьютер должен оперировать огромными массивами данных или управлять сложнейшими процессами. С одним мэйнфреймом могут одновременно работать несколько пользователей. Пользователи, работающие с мэйнфреймами, пользуются терминалами для ввода данных и просмотра результатов обработки данных. Терминал (*terminal*) состоит из клавиатуры, монитора и устройства, с помощью которого он подключается к мэйнфрейму.

Миникомпьютеры (minicomputers), или миниЭВМ – это компьютеры средних размеров, обычно используемые в университетах, на заводах или в исследовательских лабораториях. Доступ пользователей к миникомпьютерам осуществляется также, как и к большим ЭВМ, то есть посредством терминалов.

Пожалуй, наиболее трудно классифицируются по своим физическим размерам микрокомпьютеры (*microcomputers*) или микроЭВМ. Когда-то (а точнее, в 80-х годах) любой микрокомпьютер не превышал размеров коробки из-под телевизора, но к 90-м ситуация изменилась: наметилось четкое разделение семейства микроЭВМ на три вида – персональных компьютеров, рабочих станций и серверов. ***Персональный компьютер***, ПК (*personal computer, PC*) можно поставить на рабочий стол или переносить из комнаты в комнату. ПК используются в качестве персональных ЭВМ. ***Рабочая станция*** (*workstation*) также может быть установлена на рабочий стол, но, по сравнению с ПК, является более мощной в скорости обработки информации, а также по своим графическим характеристикам. Рабочие станции применяются для решения инженерных и научных задач, где требуется мощные средства компьютерной графики и математических вычислений. ***Серверы (servers)*** – мощные микрокомпьютеры, размерами от обычного персонального компьютера до небольшого шкафа для одежды. В серверы устанавливают устройства первичной и вторичной памяти большой емкости, высокопроизводительные устройства телекоммуникаций, а в последнее время – не один, а несколько микропроцессоров. Основное назначение серверов – предоставлять свои вычислительные и дисковые ресурсы в совместное использование пользователям других компьютеров, поэтому в них применяют компоненты повышенной надежности.

Суперкомпьютеры или суперЭВМ (supercomputers) – очень сложные и мощные машины, которые применяются для решения задач, требующих сверхбыстрых и сложных вычислений с тысячами и тысячами переменных. Традиционно суперкомпьютеры использовались в научной и военной сферах, но сейчас начинают применяться и в бизнесе.

Настольный компьютер (Desktop) – самый популярный и распространенный сегодня тип. Включает центральный элемент – системный блок, в котором сосредоточены все самые важные устройства компьютера (процессор, оперативная память, жесткий диск и т.д.). К системному блоку подключаются также дополнительные, внешние устройства – монитор, сканер, принтер, модем и т.д.

Настольные мини-компьютеры (Book PC, slim-desk) – переходной вариант от обычного компьютера к портативному. Дополняет картину тонкий жидкокристаллический монитор.

Портативный компьютер (notebook) –Как правило, notebook содержит только необходимый минимум устройств, а большая их часть (дополнительный жесткий диск, модем, дисководы) подключаются к компьютеру при необходимости, через специальные разъемы. Понятно, что устройства эти в десятки раз меньше, чем их «коллеги», предназначенные для настольных ПК.

Электронные секретари (palmtop) – пик миниатюрности, переходной этап от компьютера к обычной электронной «записной книжке». Эти крохи, спокойно помещающиеся на ладони, способны выполнять довольно ограниченный круг задач: на них можно набрать текст, составить простенькую электронную таблицу, подготовить и отправить электронную почту. Однако они довольно нетребовательны по части дополнительных устройств и модернизации им в большинстве случаев не нужна.

3. Основные блоки компьютера их функциональное назначение и характеристики

Блок-схема современной архитектуры компьютера приведена на следующем рис. 1.

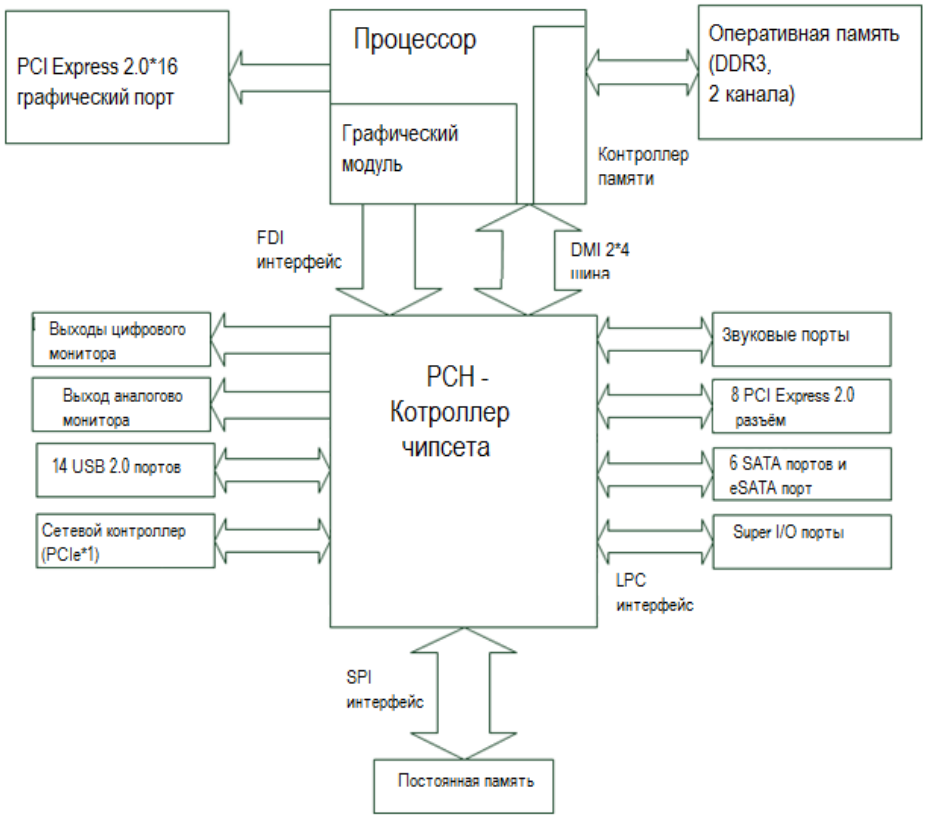


Рис. 1. Архитектура компьютера

На рисунке приведена архитектура современного компьютера в виде блок-схемы, на которой представлены основные компоненты компьютерной системы во главе с процессором, с которым интегрированы контроллер памяти и графический контроллер. Процессор соединяется с другими компонентами системы через быстрый интерфейс прямого доступа к памяти (*Direct Memory Interface (DMI)*). Последний используется вместо системной шины (*FSB - Front Side Bus*) и сходен с шиной PCI Express.

Графический ускоритель, содержащийся в процессоре, соединятся с выходным портом посредством интерфейса FDI (*Flexible Display Interface*). Компонент чипсета (*PCH -Platform Controller Hub*) даёт возможность вычислительной системе общаться с внешним миром, используя различные шины. К ним относятся графические порты, PCIe ja PCI шины, SATA интерфейсы и порты, USB интерфейсы и порты, звуковые карты и порты, сетевые карты и RJ-45 порты. На рисунке приведены также интерфейс SPI (*Serial Peripheral Interface Bus*) для связи с BIOS'i и интерфейс LPC (*Low Pin Count*), через который соединяются с чипсетом последовательные и параллельные порты для доступа к другим функциональным модулям (DMA контроллер, контроллеры прерываний, синхронизатор системы, управления режимами потребления энергии и т. д.).

Производительность CPU характеризуется следующими основными параметрами:

- степень интеграции;
- внутренняя и внешняя разрядность обрабатываемых данных;
- тактовая частота;
- память, к которой может адресоваться CPU.

Степень интеграции микросхемы показывает, сколько транзисторов (самый простой элемент любой микросхемы) может поместиться на единице площади. Для процессора Pentium Intel эта величина составляет приблизительно 3 млн на 3,5 кв. см, у Pentium Pro - 5,5 млн.

Внутренняя разрядность процессора определяет, какое количество бит он может обрабатывать одновременно при выполнении арифметических операций (в зависимости от поколения процессоров - от 8 до 32 бит).

Внешняя разрядность процессора определяет, сколько бит одновременно он может принимать или передавать во внешние устройства (от 16 до 64 бит в современных процессорах).

Тактовая частота определяет быстродействие процессора. Для процессора различают внутреннюю (собственную) тактовую частоту (с таким быстродействием выполняются внутренние простейшие операции) и внешнюю (определяет скорость передачи данных по внешней шине).

Количество адресов оперативного запоминающего устройства (ОЗУ), доступное процессору, определяется разрядностью адресной шины.

Системная шина

Одной из важнейших характеристик компьютера, которая на ряду с типом основного микропроцессора определяет возможности и диапазон применимости компьютера – это тип системной магистрали передачи данных внутри компьютера, в просторечии – шины.

Шина входит в состав материнской платы компьютера и осуществляет обмен данными между процессором или оперативной памятью и контроллерами внешних устройств компьютера: клавиатуры, монитора, дисков и т.д. Все контроллеры внешних устройств, кроме размещенных непосредственно на материнской плате, подключаются к компьютеру путем вставки этих контроллеров в свободные разъемы (слоты) шины.

Большинство компьютеров невысокой производительности оснащено шиной ISA, которая была разработана фирмой при создании компьютера IBM PC AT. Эта шина является весьма дешевой, но малоинтеллектуальной и малопроизводительной.

Основные разновидности этих шин таковы:

шина MCA - разработанная фирмой IBM в80-х годах, стала первым стандартом высокопроизводительной системной шины. Эта шина не совместима с шинами ISA, то есть все разработанные для шин ISA не годятся для шин MCA.

шина EISA - разработанная в 1989 году, также обеспечивает обмен данными между процессором или оперативной памятью и контроллерами внешних устройств по 32-битовой магистрали с высокой скоростью. В разъемы этой шины могут вставляться как контроллеры для шины EISA, так и контроллеры для шины ISA. Кроме того, шина EISA во многих случаях не обеспечивает нужное быстродействие, особенно в задачах изображений, анимации и т. д.;

шина VESA (обычно называемая локальной шиной), разработанная ассоциацией VESA. Эта шина обеспечивает более дешевое и более эффективное подключение высокоскоростных внешних устройств, поддерживая непосредственный доступ центрального процессора к соответствующим контроллерам (видеоконтроллерам, контроллерам жестких дисков, адаптерам локальной сети). Для использования остальных устройств на такие компьютеры устанавливается другая шина (ISA или, для высокопроизводительных компьютеров EISA). Благодаря разработанным ассоциациями VESA правилам “шинного арбитража” эти шины могут сосуществовать в одном компьютере, не мешая друг другу. Компьютеры с шинами VESA и EISA часто называют «VESA /EISA». Наиболее часто шина VESA используется в компьютерах на основе микропроцессора Intel – 80486;

шина PCI - разработанная фирмой Intel с участием ряда других фирм, является конкурентом шины VESA и во многих случаях обеспечивает еще более быстрый обмен с внешними устройствами, чем шина VESA. Наиболее часто шина PCI используется для микропроцессоров типа Pentium, так как она обеспечивает наиболее эффективное использование их возможностей. Как и шина VESA, шина PCI обычно используется совместно с шиной ISA или EISA.

Запоминающие устройства

Запоминающие устройства (ЗУ) предназначены для хранения информации, выраженной двоичными числами. Такая информация заносится (записывается) в ЗУ и в нужные моменты из него выбирается (считывается).

Запоминающее устройство – один из основных функциональных блоков электронных вычислительных машин; в нем хранятся числа, над которыми должны быть произведены определенные действия, и числа – коды команд, определяющие характер этих действий.

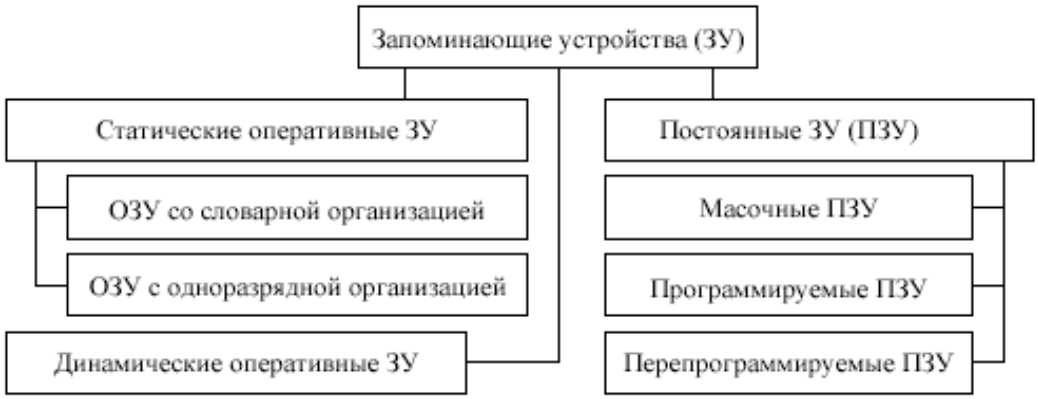


Рис. 2. Класиификация ЗУ

По характеру и использованию записанной информации ЗУ делятся на оперативные (ОЗУ) и постоянные (ПЗУ) (рис.2). К оперативным ЗУ относятся запоминающие устройства с относительно кратковременным хранением часто сменяющейся информации. В процессе работы информация в них периодически заносится и считывается. Постоянные запоминающие устройства используют для хранения программ, по которым многократно будет работать ЭВМ, стандартных программ (например, для вычисления тригонометрических функций), ряда встречающихся в расчетах констант и т. д. В процессе работы предварительно занесенная в них информация только считывается.

Постоянно запоминающее устройство – быстрая энергонезависимая память и предназначена только для чтения (драйвера)

Кеш – память – очень быстрое запоминающее устройство, небольшого объема, которое используется при обмене данными между микропроцессором и оперативной памятью для компенсации разности в скорости обработки информации процессором и несколько менее быстродействующей оперативной памятью.

Перепрограммируемая постоянная память – энергозависимая память, допускающая многократную перезапись своего содержимого с дискеты, важнейшей микросхемой такой памяти является модуль БИОС

Современные ПК имеют следующие типы запоминающих устройств: DRAM, SRAM

ОЗУ – это то устройство, без которого не обходится не один ПК, она помогает работать ПК и служит передатчиком информации с носителей памяти процессору и наоборот. ОЗУ состоит из микросхем системной логики, которые в отличии от всех других микросхем состоят не из транзисторов, а из микро конденсаторов, емкость такого конденсатора 1 Бит.

Жесткий диск. Наиболее надежным и вместительным элементом хранения информации является жесткий диск. Винчестер представляет собой металлическую коробочку, внутри которой расположены магнитные диски, способные сохранять информацию. Любой винчестер состоит из нескольких частей: блок HDA, внутри которого находится непосредственно сами жесткие диски; плата управления (контройлер винчестера) – на которой расположены элементы управления винчестером. Плата управления винчестером содержит разъемы для подключения к ПК и микросхемы со всеми необходимыми параметрами, а мак же собственным БИОСом. К материнской плате жесткий диск может быть подключен следующим образом: через порт IDE, через порт SATA, через порт связи SC SI, через USB (рис. 3).

Среди других параметров, которые влияют на быстродействие жесткого диска следует отметить следующее:

· скорость обращения дисков

· емкость Кеш-памяти

· среднее время доступа

· время задержки

· скорость обмена

CD-ROM включен в базовую конфигурацию ПК 1995 г. Поверхность диска разбивается на 3 области: НАЧАЛЬНАЯ – расположена в центре диска и считывается первой, она содержит таблицу адресов всех записей, метку диска и другую служебную информацию; СРЕДНЯЯ – со-

держит основную информацию и занимает большую часть диска; КОНЕЧНАЯ – содержит метку конца диска.

Рис. 3. Устройсво жесткого диска

Флеш-накопитель памяти: Первые флеш-брелки появились в 2001 году. Достоинством флеш-брелков является малый вес, высокая надежность и стандартность.

Compact Flash – эти карты обладают большой емкостью – более 2 ГБ и появились в 2005 году. Используются в основном в цифровых фотоаппаратах

Micro Drive – самый емкий носитель (более 4 ГБ, используется как жесткий диск в мобильных телефонах)

Secure Digital – компактная, емкость более 4 ГБ, применяется в цифровых фотоаппаратах, в цифровых плеерах и других ПК устройствах.

Memory Stick – очень маленького размера и большой емкости данных.

Периферийные или внешне устройства

Периферийными или внешними устройствами называют устройства, размещенные вне системного блока и задействованные на определенном этапе обработки информации. Прежде всего - это устройства фиксации выходных результатов: принтеры, плоттеры, модемы, сканеры и т.д.

Принтеры предназначены для вывода информации на твердые носители, большей частью на бумагу. Существует большое количество разнообразных моделей принтеров, которые различаются по принципу действия, интерфейсу, производительности и функциональным возможностями. По принципу действия различают: матричные, струйные и лазерные принтеры.

Сканер - это устройство, позволяющее вводить в компьютер черно-белое или цветное изображения, считывать графическую и текстовую информацию. Сканер используют в случае, когда возникает потребность ввести в компьютер из имеющегося оригинала текст и/или графическое изображение для его дальнейшей обработки (редактирование и т.д.).

Модем - это устройство, предназначенное для подсоединения компьютера к обычной телефонной линии. Название происходит от сокращения двух слов - Модуляция и Демодуляция.

Компьютер вырабатывает дискретные электрические сигналы (последовательности двоичных нулей и единиц), а по телефонным линиям информация передается в аналоговой форме (то есть в виде сигнала, уровень которого изменяется непрерывно, а не дискретно). Модемы выполняют цифро-аналоговое и аналого-цифровое преобразования. При передаче данных, модемы накладывают цифровые сигналы компьютера на непрерывную частоту телефонной линии (модулируют ее), а при их приеме демодулируют информацию и передают ее в цифровой форме в компьютер. Модемы передают данные по обычным, то есть комутированным, телефонным каналам со скоростью от 300 до 56 000 бит в секунду, а по арендованным (выделенным) каналам скорость может быть и выше. Кроме того, современные модемы осуществляют сжатие данных перед отправлением, и соответственно, реальная скорость может превышать максимальную скорость модема.

По конструктивному выполнению модемы бывают встроенными (вставляются в системный блок компьютера в один из слотов расширения) и внешними (подключаются через один из коммуникационных портов, имеют отдельный корпус и собственный блок питания). Однако, без соответствующего коммуникационного программного обеспечения, важнейшей составляющей которого является протокол, модемы не могут работать. Наиболее распространенными протоколами модемов являются v.32 bis, v.34, v.42 bis и прочие.

Контрольные вопросы

1. Что такое информационная система и для чего они предназначены?
2. Каковы основные компаненты и в чем их функции?
3. Перечислите основные типы современных компьютеров.
4. Опишите основные блоки компьютера.
5. Какие функции выполняют блоки компьютера?

Лекция 2
Архитектура вычислительных систем

1. **Информационная технология**
2. **Информационная система**
3. **Классификация информационных систем**
4. **Многомашинные и многопроцессорные вычислительные комплексы**

Ключивые слова: информационная технология, информационная система, вычислительные комплексы, многомашинные системы, многопроцессорные системы.

Информационная технология

Информационная технология - это системно-организованная последовательность операций, выполняемых над информацией с использованием средств и методов автоматизации. Операциями являются элементарные действия над информацией.

Процедура передачи информации включает кроме самой передачи операции ввода данных в систему, в сеть, преобразования из цифровой формы в аналоговую и наоборот, операции вывода сообщений, контроль ввода и вывода, защиту данных.

Процедуры обработки информации являются главными в информационных технологиях. Остальные процедуры носят вспомогательный характер.

Автоматизированная информационная технология (АИТ) – системно организованная для решения задач управления совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, поиска, обработки и защиты информации на базе применения развитого программного обеспечения, используемых средств вычислительной техники и связи, а также способов, с помощью которого информация предлагается клиентам.

Основная цель автоматизированной информационной технологии – получать посредством переработки первичных данных информацию нового качества, на основе которой вырабатываются оптимальные управленческие решения.

Этапы развития информационных технологий

Существует несколько точек зрения на развитие информационных технологий с использованием компьютеров, которые определяются различными признаками деления.

Общим для всех изложенных ниже подходов является то, что с появлением персонального компьютера начался новый этап развития информационной технологии.

Признак деления – виды инструментария технологии

1-й этап (до второй половины XIX в.) – *«ручная»* информационная технология, инструментарий которой составляли: перо, чернильница, книга. Коммуникации осуществлялись ручным способом путем переправки через почту писем, пакетов, депеш. Основная цель технологии – представление информации в нужной форме.

2-й этап (с конца XIX в.) – *«механическая»* технология, инструментарий которой составляли: пишущая машинка, телефон, диктофон, оснащенная более совершенными средствами доставки почта. Основная цель технологии – представление информации в нужной форме более удобными средствами.

3-й этап (40 – 60-е гг. XX в.) – *«электрическая»* технология, инструментарий которой составляли: большие ЭВМ и соответствующее программное обеспечение, электрические пишущие машинки, ксероксы, портативные диктофоны.

Изменяется цель технологии. Акцент в информационной технологии начинает перемещаться с формы представления информации на формирование ее содержания.

4-й этап (с начала 70-х гг.) – *«электронная»* технология, основным инструментарием которой становятся большие ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ) и информационно-поисковые системы (ИПС), оснащенные широким спектром базовых и специализированных программных комплексов. Центр тяжести технологии еще более смещается на формирование содержательной стороны информации для управленческой среды различных сфер общественной жизни, особенно на организацию аналитической работы. Множество объективных и субъективных факторов не позволили решить стоящие перед новой концепцией информационной технологии поставленные задачи.

5-й этап (с середины 80-х гг.) – *«компьютерная»* («новая») технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов разного назначения. На этом этапе происходит процесс персонализации АСУ, который проявляется в создании систем поддержки принятия решений определенными специалистами. Подобные системы имеют встроенные элементы анализа и интеллекта для разных уровней управления, реализуются на персональном компьютере и используют телекоммуникации. В связи с переходом на микропроцессорную базу существенным изменениям подвергаются и технические средства бытового, культурного и прочего назначений. Начинают широко использоваться в различных областях глобальные и локальные компьютерные сети.

Признак деления – вид задач и процессов обработки информации

1-й этап (60 - 70-е гг.) – обработка данных в вычислительных центрах в режиме коллективного пользования. Основным направлением развития информационной технологии являлась автоматизация операционных рутинных действий человека.

2-й этап (с 80-х гг.) – создание информационных технологий, направленных на решение стратегических задач.

Признак деления – проблемы, стоящие на пути информатизации общества

1-й этап (до конца 60-х гг.) характеризуется проблемой обработки больших объемов данных в условиях ограниченных возможностей аппаратных средств.

2-й этап (до конца 70-х гг.) связывается с распространением ЭВМ серии 1BM/360. Проблема этого этапа – отставание программного обеспечения от уровня развития аппаратных средств.

3-й этап (с начала 80-х гг.) – компьютер становится инструментом непрофессионального пользователя, а информационные системы – средством поддержки принятия его решений. Проблемы - максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.

4-й этап (с начала 90-х гг.) – создание современной технологии межорганизационных связей и информационных систем. Проблемы этого этапа весьма многочисленны. Наиболее существенными из них являются:

- выработка соглашений и установление стандартов, протоколов для компьютерной связи;

- организация доступа к стратегической информации;
- организация защиты и безопасности информации.

Признак деления – преимущество, которое приносит компьютерная технология

1-й этап (с начала 60-х гг.) характеризуется довольно эффективной обработкой информации при выполнении рутинных операций с ориентацией на централизованное коллективное использование ресурсов вычислительных центров. Основным критерием оценки эффективности создаваемых информационных систем была разница между затраченными на разработку и сэкономленными в результате внедрения средствами.

2-й этап (с середины 70-х гг.) связан с появлением персональных компьютеров. Изменился подход к созданию информационных систем – ориентация смещается в сторону индивидуального пользователя для поддержки принимаемых им решений. На этом этапе используется как централизованная обработка данных, характерная для первого этапа, так и децентрализованная, базирующаяся на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.

3-й этап (с начала 90-х гг.) связан с понятием анализа стратегических преимуществ в бизнесе и основан на достижениях телекоммуникационной технологии распределенной обработки информации. Информационные системы имеют своей целью не просто увеличение эффективности обработки данных и помощь управленцу. Соответствующие информационные технологии должны помочь организации выстоять в конкурентной борьбе и получить преимущество.

Классификация информационных технологий

АИТ в настоящее время можно классифицировать по ряду признаков, в частности:

- способу реализации в автоматизированных информационных системах (*АИС)*;
- степени охвата АИТ задач управления;
- классам реализуемых технологических операций;
- типу пользовательского интерфейса;
- вариантам использования сети ЭВМ;
- обслуживаемой предметной области.

Информационная система

Информационная система – это любая система, реализующая или поддерживающая информационный процесс.

К информационным можно относить любые системы, включающие в себя работу с информацией. В настоящее время основным помощником человека при работе с информацией является компьютер, поэтому именно его мы и будем рассматривать в качестве источника, способа изменения и хранения информационных систем. А в качестве информационных систем будем рассматривать программное обеспечение компьютера.

В зависимости от предметной области информационные системы могут весьма значительно различаться по своим функциям, архитектуре, реализации. Однако можно выделить ряд свойств, которые являются общими.

Информационные системы предназначены организации и поддержке информационного процесса, поэтому в основе любой из них лежит среда хранения и доступа к информации.

Информационные системы ориентированы на конечного пользователя, не обладающего высокой квалификацией в области вычислительной техники. Поэтому клиентские приложения

информационной системы должны обладать простым, удобным, легко осваиваемым интерфейсом.

Таким образом, при разработке информационной системы приходится решать две основные задачи:

- разработка базы данных, предназначенной для хранения информации;
- разработка графического интерфейса пользователя клиентских приложений.

Подавляющее большинство информационных систем работает в режиме диалога с пользователем.

В наиболее общем случае типовые программные компоненты, входящие в состав информационной системы, реализуют:

- диалоговый ввод-вывод;
- логику диалога;
- прикладную логику обработки данных;
- логику управления данными;
- операции манипулирования файлами и (или) базами данных.

Классификация информационных систем

Информационные системы классифицируются по разным признакам.

Классификация по масштабу

По масштабу информационные системы подразделяются на следующие группы (рис. 1):

Рис. 1. Деление информационных систем по масштабу.

Одиночные информационные системы

Одиночные информационные системы реализуются, как правило, на автономном персональном компьютере (сеть не используется). Такая система может содержать несколько простых приложений, связанных общим информационным фондом, и рассчитана на работу одного пользователя или группы пользователей, разделяющих по времени одно рабочее место.

Подобные приложения создаются с помощью так называемых настольных, или локальных, систем управления базами данных (*СУБД*). Среди локальных СУБД наиболее известными являются Clarion, Clipper, FoxPro, Paradox, dBase и Microsoft Access.

Групповые информационные системы

Групповые информационные системы ориентированы на коллективное использование информации членами рабочей группы и чаще всего строятся на базе локальной вычислительной сети. При разработке таких приложений используются серверы баз данных (называемые также SQL (*Structured Query Language* – структурированный язык запросов)-серверами) для рабочих групп. Существует довольно большое количество различных SQL-серверов как коммерческих, так и свободно распространяемых. Среди них наиболее известны такие серверы баз данных, как Oracle, DB2, Microsoft SQL Server, InterBase, Sybase, Informix.

Корпоративные информационные системы

Корпоративные информационные системы являются развитием систем для рабочих групп, они ориентированы на крупные компании и могут поддерживать территориально разнесенные узлы или сети. В основном они имеют иерархическую структуру из нескольких уровней. Для таких систем характерна архитектура клиент-сервер со специализацией серверов или же многоуровневая архитектура. При разработке таких систем могут использоваться те же серверы баз данных, что и при разработке групповых информационных систем. Однако в крупных информационных системах наибольшее распространение получили серверы Oracle, DB2 и Microsoft SQL Server.

Классификация по сфере применения

По сфере применения информационные системы делятся на четыре группы (рис. 2):

- системы обработки транзакций (протоколов);
- системы поддержки принятия решений;
- информационно-справочные системы;
- офисные информационные системы.

Системы обработки транзакций, в свою очередь, по оперативности обработки данных разделяются на пакетные информационные системы и оперативные информационные системы. В информационных системах организационного управления преобладает режим оперативной обработки транзакций (OnLine Transaction Processing, OLTP) для отражения актуального состояния предметной области в любой момент времени, а пакетная обработка занимает весьма ограниченную часть. Для систем OLTP характерен регулярный (возможно, интенсивный) поток довольно простых транзакций, играющих роль заказов, платежей, запросов и т.п. Важными требованиями для них являются:

- высокая производительность обработки транзакций;
- гарантированная доставка информации при удаленном доступе к БД по телекоммуникациям.

Рис. 2. Деление информационных систем по сфере применения.

Системы поддержки принятия решений (Decision Support System, DSS) представляют собой другой тип информационных систем, в которых с помощью довольно сложных запросов производится отбор и анализ данных в различных разрезах: временных, географических, по другим показателям.

Обширный класс ***информационно-справочных систем*** основан на гипертекстовых документах и мультимедиа. Наибольшее развитие такие информационные системы получили в Интернете.

Класс ***офисных информационных систем*** нацелен на перевод бумажных документов в электронный вид, автоматизацию делопроизводства и управление документооборотом.

Классификация по способу организации

По способу организации групповые и корпоративные информационные системы подразделяются на следующие классы (рис. 3):

- системы на основе архитектуры файл-сервер;
- системы на основе архитектуры клиент-сервер;
- системы на основе многоуровневой архитектуры;
- системы на основе Интернет/интранет-технологий.

Рис. 3. Деление информационных систем по способу организации.

В любой информационной системе можно выделить необходимые функциональные компоненты (табл. 1), которые помогают понять ограничения различных архитектур информационных систем. Рассмотрим более подробно особенности вариантов построения информационных приложений.

Таблица 1. Типовые функциональные компоненты информационной системы

Обозначение	Наименование	Характеристика
PS	Presentation Services (средства представления)	Обслуживает пользовательский ввод и отображает то, что сообщает ему компонент логики представления (PL), с использованием соответствующей программной поддержки
PL	Presentation Logic (логика представления)	Управляет взаимодействием между пользователем и ЭВМ. Обрабатывает действия пользователя при выборе команды в меню, щелчке на кнопке или выборе пункта в списке
BL	Business Logic (прикладная логика)	Набор правил для принятия решений, вычислений и операций, которые должно выполнить приложение
DL	Data Logic (логика управления данными)	Операции с базой данных (реализуемые SQL-операторами), которые нужно выполнить для реализации прикладной логики управления данными

DS	Data Services (операции с базой данных)	Действия СУБД, реализующие логику управления данными, такие как манипулирование данными, определение данных, фиксация или откат транзакций и т. п. СУБД обычно компилирует SQL-предложения
FS	File Services (файловые операции)	Дисковые операции чтения и записи данных для СУБД и других компонентов. Обычно являются функциями операционной системы (ОС)

Информационная система (ИС) является системой информационного обслуживания работников управленческих служб и выполняет технологические функции по накоплению, хранению, передаче и обработке информации. Она складывается, формируется и функционирует в регламенте, определенном методами и структурой управленческой деятельности, принятой на конкретном экономическом объекте, реализует цели и задачи, стоящие перед ним.

Информационная система управления (ИСУ) – это совокупность информации, экономико-математических методов и моделей, технических, программных, других технологических средств и специалистов, а также предназначенная для обработки информации и принятия управленческих решений.

Экономическая информационная система (ЭИС) – это совокупность внутренних и внешних потоков прямой и обратной информационной связи экономического объекта, методов, средств, специалистов, участвующих в процессе обработки информации и выработке управленческих решений.

Автоматизированная информационная система (АИС) представляет собой совокупности информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенную для обработки информации и принятия управленческих решений.

3. Классификация атоматизированных информационных систем

Автоматизированные информационные системы разнообразны и могут быть классифицированы по ряду признаков. Классификация информационных систем управления зависит от видов процессов управления, уровня управления, сферы функционирования экономического объекта и его организации, степени автоматизации управления и т.д. Можно привести, например, и такую классификацию, как на рис. 4.

Так как классификация систем по сфере функционирования объекта управления очевидна, рассмотрим другие признаки.

По ***видам процессов управления*** автоматизированные информационные системы подразделяются на:

АИС управления технологическими процессами – это человеко-машинные системы, обеспечивающие управление технологическими устройствами, станками, автоматическими линиями. Предназначены для автоматизации различных технологических процессов (гибкие технологические процессы, энергетика и т.д.).

АИС управления организационно-технологическими процессами представляют собой многоуровневые иерархические системы, сочетающие АИС управления технологическими процессами и АИС управления предприятиями.

Рис. 4. Классификация автоматизированных информационных систем

Для *АИС организационного управления* объектом служат производственно-хозяйственные, социально-экономические функциональные процессы, реализуемые на всех уровнях управления экономикой, в частности:

- налоговые АИС;
- АИС таможенной службы;
- статистические АИС;
- АИС промышленных предприятий и организаций и др.

Предназначены для автоматизации функций управленческого персонала.

К этому классу АИС относятся информационные системы управления как промышленными фирмами, так и непромышленными экономическими объектами – предприятиями сферы обслуживания. Основными функциями таких систем являются оперативный контроль и регулирование, оперативный учет и анализ, перспективное и оперативное планирование, бухгалтерский учет, управление сбытом и снабжением и решение других экономических и организационных задач.

АИС научных исследований обеспечивают высокое качество и эффективность межотраслевых расчетов и научных опытов. Обеспечивают решение научно-исследовательских задач на базе экономико-математических методов и моделей. Методической базой таких систем служат экономико-математические методы, технической базой – самая разнообразная вычислительная техника и технические средства для проведения экспериментальных работ моделирования. Как организационно-технологические системы, так и системы научных исследований могут включать в свой контур системы автоматизированного проектирования работ (САПР).

Обучающие АИС получают широкое распространение при подготовке специалистов в системе образования, при переподготовке и повышении квалификации работников разных отраслей.

К этой классификации можно добавить:

Интегрированные АИС предназначены для автоматизации всех функций управления фирмой и охватывают весь цикл функционирования экономического объекта: начиная от научно-исследовательских работ, проектирования, изготовления, выпуска и сбыта продукции до анализа эксплуатации изделия.

Корпоративные АИС используются для автоматизации всех функций управления фирмой или корпорацией, имеющей территориальную разобщенность между подразделениями, филиалами, отделениями, офисами и т.д.

В соответствии с третьим признаком классификации выделяют отраслевые, территориальные и межотраслевые АИС, которые одновременно являются системами организационного управления, но уже следующего – более высокого уровня иерархии.

Отраслевые АИС функционируют в сферах промышленного и агропромышленного комплексов, в строительстве, на транспорте. Эти системы решают задами информационного обслуживания аппарата управления соответствующих ведомств.

Территориальные АИС предназначены для управления административно-территориальными районами. Предназначены для решения информационных задач управления административно-территориальными объектами, расположенными на конкретной территории. Деятельность территориальных систем направлена на качественное выполнение управленческих функций в регионе, формирование отчетности, выдачу оперативных сведений местным государственным и хозяйственным органам.

Межотраслевые АИС являются специализированными системами функциональных органов управления национальной экономикой (банковских, финансовых, снабженческих, статистических и др.). Имея в своем составе мощные вычислительные комплексы, межотраслевые многоуровневые АИС обеспечивают разработку экономических и хозяйственных прогнозов, государственного бюджета, осуществляют контроль результатов регулирование деятельности всех звеньев хозяйства, а также контроль наличия и распределения ресурсов.

К этой классификации можно добавить:

АИС федерального значения решают задачи информационного обслуживания аппарата административного управления и функционируют во всех регионах страны.

Муниципальные АИС функционируют в органах местного самоуправления для информационного обслуживания специалистов и обеспечения обработки экономических, социальных и хозяйственных прогнозов, местных бюджетов, контроля и регулирования деятельности всех звеньев социально-экономических областей города, административного района и т. д.

4. Многомашинные и многопроцессорные вычислительные комплексы

В настоящее время исключительно важное значение приобрела проблема обеспечения высокой надежности и готовности вычислительных систем, работающих в составе различных АСУ и АСУ ТП, особенно при работе, в режиме реального времени. Эта проблема решается на основе использования принципа избыточности, который ориентирует также на построение многомашинных или многопроцессорных систем (комплексов). Появление дешевых и небольших по размерам микропроцессоров и микро-ЭВМ облегчило построение и расширило область применения многопроцессорных и многомашинных ВС разного назначения

Различие понятий многомашинной и многопроцессорной ВС поясняет рис.5. Многомашинная ВС (ММС) содержит несколько ЭВМ, каждая из которых имеет свою ОП и работает под управлением своей операционной системы, а также средства обмена информацией между машинами. Реализация обмена информацией происходит, в конечном счете, путем взаимодействия операционных систем машин между собой. Это ухудшает динамические характеристики процессов межмашинного обмена данными. Применение многомашинных систем позволяет повысить надежность вычислительных комплексов. При отказе в одной машине обработку данных может продолжать другая машина комплекса. Однако можно заметить, что при этом оборудование комплекса недостаточно эффективно используется для этой цели. Достаточно в системе, изображенной на рис.5а, а в каждой ЭВМ выйти из строя по одному устройству (даже разных типов), как вся система становится неработоспособной.

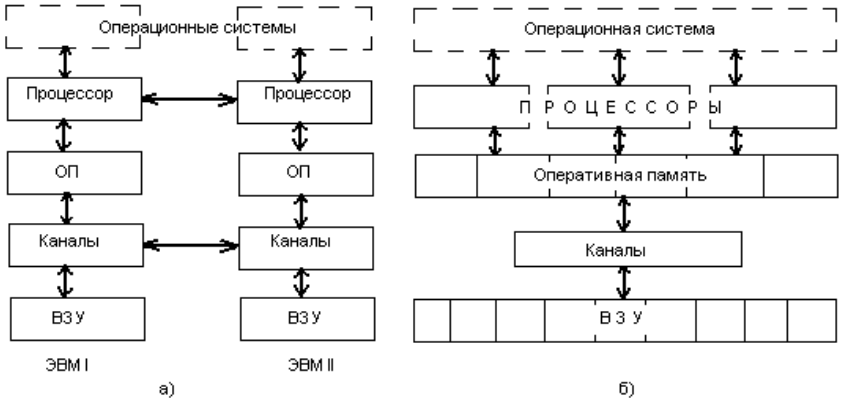


Рис. 5. Многомашинные (а) и многопроцессорные (б) системы

Этих недостатков лишены многопроцессорные системы (МПС). В таких системах (рис. 5б) процессоры обретают статус рядовых агрегатов вычислительной системы, которые подобно другим агрегатам, таким, как модули памяти, каналы, периферийные устройства, включаются в состав системы в нужном количестве.

Вычислительная система называется многопроцессорной, если она содержит несколько процессоров, работающих с общей ОП (общее поле оперативной памяти) и управляется одной общей операционной системой. Часто в МПС организуется общее поле внешней памяти.

В МПС по сравнению с ММС достигается более быстрый обмен информацией между процессорами и поэтому может быть получена более высокая производительность, более быстрая реакция на ситуации, возникающие внутри системы и в ее внешней среде, и более высокие надежность и живучесть, так как система сохраняет работоспособность, пока работоспособны хотя бы по одному модулю каждого типа устройств.

Многопроцессорные системы представляют собой основной путь построения ВС сверхвысокой производительности. При создании таких ВС возникает много сложных проблем, к которым в первую очередь следует отнести распараллеливание вычислительного процесса (программ) для эффективной загрузки процессоров системы, преодоление конфликтов при попытках нескольких процессоров использовать один и тот же ресурс системы (например, некоторый модуль памяти) и уменьшение влияния конфликтов на производительность системы, осуществление быстродействующих экономичных по аппаратурным затратам межмодульных связей. Указанные вопросы необходимо учитывать при выборе структуры МПС.

На основе многопроцессорности и модульного принципа построения других устройств системы возможно создание отказоустойчивых систем, или, другими словами, систем повышенной живучести.

Однако построение многомашинных систем из серийно выпускаемых ЭВМ с их стандартными операционными системами значительно проще, чем построение МПС, требующих преодоления определенных трудностей, возникающих при реализации общего поля памяти, и, главное, трудоемкой разработки специальной операционной системы.

Многомашинные и многопроцессорные системы могут быть однородными и неоднородными. Однородные системы содержат однотипные ЭВМ или процессоры. Неоднородные ММС состоят из ЭВМ различного типа, а в неоднородных МПС используются различные специализи-

рованные процессоры, например процессоры для операций с плавающей запятой, для обработки десятичных чисел, процессор, реализующий функции операционной системы, процессор для матричных задач и др.

Многопроцессорные системы и ММС могут иметь одноуровневую или иерархическую (многоуровневую) структуру. Обычно менее мощная машина (машина-сателлит) берет на себя ввод информации с различных терминалов и ее предварительную обработку, разгружая от этих сравнительно простых процедур основную, более мощную ЭВМ, чем достигается увеличение общей производительности (пропускной способности) комплекса. В качестве машин-сателлитов используют малые или микро-ЭВМ.

Контрольные вопросы

1. Что такое информационные технологии, и каковы их главные процедуры?
2. Каково назначение атоматизированных информационных технологий и признаки их деления?
3. В чем заключаются особенности АИС и их классификация?
4. По каким признакам классифицируются информационные системы?
5. В чем достоинства и недостатки многомашинных и много процессорных комплексов?

Лекция 3. Параллельные архитектуры

1. **Параллельная обработка**
2. **Конвейерная обработка**
3. **Классификация Флинна**
4. **Закон Амдаля**
5. **Оценка производительности вычислительных систем**

Ключивые слова: архитектура компьютера, параллельная обработка, конвейерная обработка, классификация флинна, закон Амдаля, производительность вычислительных систем, единицы измерения, ливерморские циклы, linpack.

Один из первых в мире компьютеров EDSAC (1949 г.) выполнял около 100 арифметических операций в секунду. Производительность самых мощных современных компьютеров составляет несколько десятков триллионов (10^{-12}) операций в секунду. Чем же объясняется такой колоссальный рост производительности?

Несомненно, одной из причин является совершенствование элементной базы. Смена электронных ламп транзисторами, появление интегральных схем, разработка кремниевых чипов – каждое из этих событий производило революцию в компьютерной технике. Современные технологии создания чипов позволяют работать с элементами размеров порядка десятых долей микрона (10^{-6} м). Регулярное уменьшение размеров чипов обеспечивает эволюционный рост тактовой частоты работы процессоров. Так, EDSAC имел время такта 2 микросекунды (10^{-6} сек), а современный компьютер Hewlett-Packard V2600 выполняет один такт за 1.8 наносекунды (10^{-9} сек). В то же время его производительность составляет 77 миллиардов операций в секунду, и это в семьсот миллионов раз больше, чем у EDSAC. Такой рост производительности не может объясняться только лишь изменением элементной базы.

Вторая по счету, но первая по значению причина заключается в использовании новых решений в архитектуре компьютера.

Архитектура компьютера - это описание компонент компьютера и их взаимодействия. Организация компьютера - это описание конкретной реализации архитектуры, ее воплощения «в железе». Третий термин - это схема компьютера, детальное описание его электронных компонент, их соединений, устройств питания, охлаждения и других.

Революцию в компьютерных архитектурах произвел принцип параллельной обработки данных, воплощающий идею одновременного (параллельного) выполнения нескольких действий. Параллельная обработка данных имеет две разновидности: конвейерность и собственно параллельность.

1. Параллельная обработка

Если некое устройство выполняет одну операцию за единицу времени, то тысячу операций оно выполнит за тысячу единиц. Если предположить, что есть пять таких же независимых устройств, способных работать одновременно, то ту же тысячу операций система из пяти устройств может выполнить уже не за тысячу, а за двести единиц времени. Аналогично система

из N устройств ту же работу выполнит за 1000/N единиц времени. Однако это идеальное ускорение удается получить лишь в очень специальных ситуациях, когда подзадачи полностью независимы (например, задачи перебора, взламывание паролей).

2. Конвейерная обработка

Что необходимо для сложения двух вещественных чисел, представленных в форме с плавающей запятой? Целое множество мелких операций таких, как сравнение порядков, выравнивание порядков, сложение мантисс, нормализация и т.п. Процессоры первых компьютеров выполняли все эти «микрооперации» для каждой пары аргументов последовательно одна за другой до тех пор, пока не доходили до окончательного результата, и лишь после этого переходили к обработке следующей пары слагаемых.

Идея конвейерной обработки заключается в выделении отдельных этапов выполнения общей операции, причем каждый этап, выполнив свою работу, передавал бы результат следующему, одновременно принимая новую порцию входных данных. Предположим, что в операции можно выделить пять микроопераций, каждая из которых выполняется за одну единицу времени. Если есть одно неделимое последовательное устройство, то 100 пар аргументов оно обработает за 500 единиц. Если каждую микрооперацию выделить в отдельный этап (или иначе говорят - ступень) конвейерного устройства, то на пятой единице времени на разной стадии обработки такого устройства будут находиться первые пять пар аргументов, а весь набор из ста пар будет обработан за 5+99=104 единицы времени - ускорение по сравнению с последовательным устройством почти в пять раз (по числу ступеней конвейера).

Впервые конвейерный принцип выполнения команд был использован в машине ATLAS, разработанной в Манчестерском университете в 1963г. Выполнение команд разбито на 4 стадии: выборка команды, вычисление адреса операнда, выборка операнда и выполнение операции. Конвейеризация позволила уменьшить время выполнения команд с 6 мкс до 1,6 мкс.

3. Классификация Флинна

Самой ранней и наиболее известной является классификация архитектур вычислительных систем, предложенная в 1966 году М. Флинном. Классификация базируется на понятии потока, под которым понимается последовательность элементов, команд или данных, обрабатываемая процессором. На основе числа потоков команд и потоков данных Флинн выделяет четыре класса архитектур: SISD, MISD, SIMD, MIMD.

SISD (single instruction stream / single data stream) - одиночный поток команд и одиночный поток данных (рис. 1, а). К этому классу относятся, прежде всего, классические последовательные машины, или иначе, машины фон-неймановского типа.

В таких машинах есть только один поток команд, все команды обрабатываются последовательно друг за другом, и каждая команда инициирует одну операцию с одним потоком данных. Не имеет значения тот факт, что для увеличения скорости обработки команд и скорости выполнения арифметических операций может применяться конвейерная обработка - как машина CDC 6600 со скалярными функциональными устройствами, так и CDC 7600 с конвейерными попадают в этот класс.

SIMD (single instruction stream / multiple data stream) - одиночный поток команд и множественный поток данных (рис. 1, б). В архитектурах подобного рода сохраняется один поток команд, включающий, в отличие от предыдущего класса, векторные команды. Это позволяет выполнять одну арифметическую операцию сразу над многими данными - элементами вектора.

MISD (multiple instruction stream / single data stream) - множественный поток команд и одиночный поток данных (рис. 1, в). Определение подразумевает наличие в архитектуре многих процессоров, обрабатывающих один и тот же поток данных.

MIMD (multiple instruction stream / multiple data stream) - множественный поток команд и множественный поток данных (рис. 1, г).

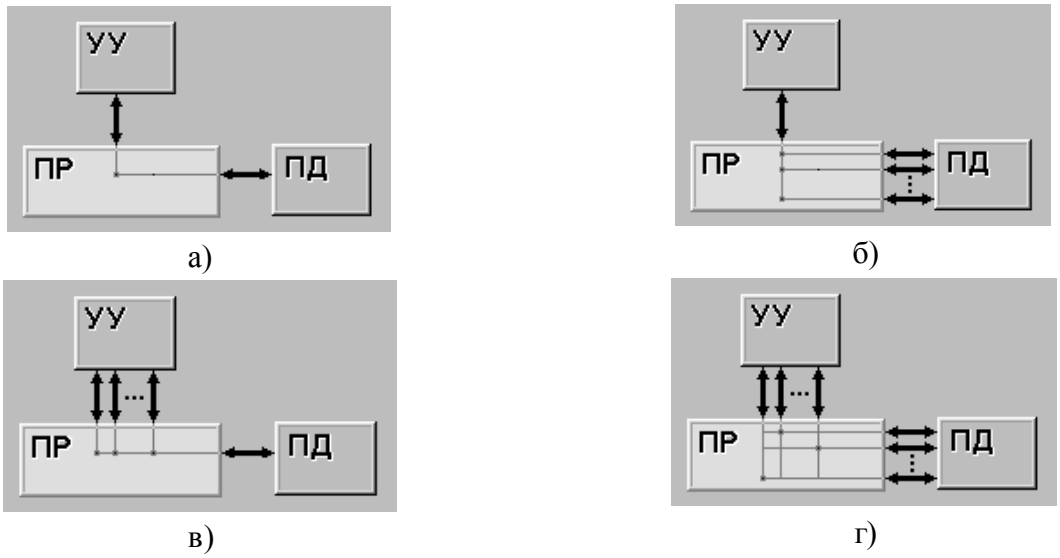


Рис. 1. УУ – управляющее устройство (организует поток команд), ПР – процессор, ПД – поток данных

Этот класс предполагает, что в вычислительной системе есть несколько устройств обработки команд, объединенных в единый комплекс и работающих каждое со своим потоком команд и данных.

4. Закон Амдаля

Одной из целей при конструировании параллельных алгоритмов является достижение по возможности большего ускорения; в идеальном случае $S_p = p$. Однако мы уже видели на примере сложения n чисел, что эта ситуация не всегда достижима. В самом деле, максимальное ускорение можно получить только для задач, по существу тривиальных.

Главные факторы, обусловливающие отклонение от максимального ускорения, таковы:

1. Отсутствие максимального параллелизма в алгоритме и/или несбалансированность нагрузки процессоров.
2. Обмены, конфликты памяти и время синхронизации.

Хотя задержки, связанные с синхронизацией, обменами и конфликтами памяти, по своей природе весьма различны, их воздействие на общий процесс вычисления одинаково: они замедляют его на время, необходимое для подготовки данных, нужных для дальнейшего счета. Поэтому иногда следует объединять все три фактора задержки, как это сделано в следующем определении.

Обратимся теперь к фактору отсутствия максимального параллелизма. Он может проявляться по-разному. При сложении n чисел мы видели, что на первом этапе алгоритма параллелизм максимален, однако на каждом последующем этапе степень параллелизма уменьшается вдвое. Таким образом, в большинстве случаев средняя степень параллелизма алгоритма меньше.

5. Оценка производительности вычислительных систем

Основу для сравнения различных типов компьютеров между собой дают стандартные методики измерения производительности. В процессе развития вычислительной техники появилось несколько таких стандартных методик. Они позволяют разработчикам и пользователям осуществлять выбор между альтернативами на основе количественных показателей, что дает возможность постоянного прогресса в данной области.

Единицей измерения производительности компьютера является время: компьютер, выполняющий тот же объем работы за меньшее время, является более быстрым. Время выполнения любой программы измеряется в секундах. Часто производительность измеряется как скорость появления некоторого числа событий в секунду, так что меньшее время подразумевает большую производительность.

Однако в зависимости от того, что мы считаем, время может быть определено различными способами. Наиболее простой способ определения времени называется астрономическим временем, временем ответа (response time), временем выполнения (execution time) или прошедшим временем (elapsed time). Это задержка выполнения задания, включающая буквально все: работу процессора, обращения к диску, обращения к памяти, ввод/вывод и накладные расходы операционной системы. Однако при работе в мультипрограммном режиме во время ожидания ввода/вывода для одной программы процессор может выполнять другую программу, и система не обязательно будет минимизировать время выполнения данной конкретной программы.

В большинстве современных процессоров скорость протекания процессов взаимодействия внутренних функциональных устройств определяется не естественными задержками в этих устройствах, а задается единой системой синхросигналов, вырабатываемых некоторым генератором тактовых импульсов, как правило, работающим с постоянной скоростью. Дискретные временные события называются тактами синхронизации (*clock ticks*), просто тактами (*ticks*), периодами синхронизации (*clock periods*), циклами (*cycles*) или циклами синхронизации (*clock cycles*). Разработчики компьютеров обычно говорят о периоде синхронизации, который определяется либо своей длительностью (например, 10 наносекунд), либо частотой (например, 100 МГц). Длительность периода синхронизации есть величина, обратная к частоте синхронизации.

Таким образом, время ЦП для некоторой программы может быть выражено двумя способами: количеством тактов синхронизации для данной программы, умноженным на длительность такта синхронизации, либо количеством тактов синхронизации для данной программы, деленным на частоту синхронизации.

Важной характеристикой, часто публикуемой в отчетах по процессорам, является среднее количество тактов синхронизации на одну команду - CPI (*clock cycles per instruction*). При известном количестве выполняемых команд в программе этот параметр позволяет быстро оценить время ЦП для данной программы.

Таким образом, производительность ЦП зависит от трех параметров: такта (или частоты) синхронизации, среднего количества тактов на команду и количества выполняемых команд. Невозможно изменить ни один из указанных параметров изолированно от другого, поскольку базовые технологии, используемые для изменения каждого из этих параметров, взаимосвязаны: частота синхронизации определяется технологией аппаратных средств и функциональной организацией процессора; среднее количество тактов на команду зависит от функциональной организации и архитектуры системы команд; а количество выполняемых в программе команд определяется архитектурой системы команд и технологией компиляторов. Когда сравниваются две машины, необходимо рассматривать все три компоненты, чтобы понять относительную производительность.

Пиковая и реальная производительность

Различают пиковую и реальную производительность. Под пиковой понимают величину, равную произведению пиковой производительности одного процессора на число таких процессоров в данной машине. При этом предполагается, что все устройства компьютера работают в максимально производительном режиме. Пиковая производительность компьютера вычисляется однозначно, и эта характеристика является базовой, по которой производят сравнение высокопроизводительных вычислительных систем . Чем больше пиковая производительность, тем (теоретически) быстрее пользователь сможет решить свою задачу. Пиковая производительность есть величина теоретическая и, вообще говоря, недостижимая при запуске конкретного приложения. Реальная же производительность, достигаемая на данном приложении, зависит от взаимодействия программной модели, в которой реализовано приложение, с архитектурными особенностями машины, на которой приложение запускается.

Существует два способа оценки пиковой производительности компьютера. Один из них опирается на число команд, выполняемых компьютером за единицу времени. Единицей измерения, как правило, является MIPS (*Million Instructions Per Second*). Производительность, выраженная в MIPS, говорит о скорости выполнения компьютером своих же инструкций. Но, во-первых, заранее не ясно, в какое количество инструкций отобразится конкретная программа, а во-вторых, каждая программа обладает своей спецификой, и число команд от программы к программе может меняться очень сильно. В связи с этим данная характеристика дает лишь самое общее представление о производительности компьютера.

Другой способ измерения производительности заключается в определении числа вещественных операций, выполняемых компьютером за единицу времени. Единицей измерения является Flops (*Floating point operations per second*) – число операций с плавающей точкой, производимых компьютером за одну секунду. Такой способ является более приемлемым для пользователя, поскольку ему известна вычислительная сложность программы, и, пользуясь этой характеристикой, пользователь может получить нижнюю оценку времени ее выполнения.

Однако пиковая производительность получается только в идеальных условиях, т.е. при отсутствии конфликтов при обращении к памяти при равномерной загрузке всех устройств. В реальных условиях на выполнение конкретной программы влияют такие аппаратно-программные особенности данного компьютера как: особенности структуры процессора, системы команд, состав функциональных устройств, реализация ввода/вывода, эффективность работы компиляторов.

Единицы измерения

MIPS

Одной из альтернативных единиц измерения производительности процессора (по отношению к времени выполнения) является MIPS - (миллион команд в секунду). Имеется несколько различных вариантов интерпретации определения MIPS.

В общем случае MIPS есть скорость операций в единицу времени, т.е. для любой данной программы MIPS есть просто отношение количества команд в программе к времени ее выполнения. Таким образом, производительность может быть определена как обратная к времени выполнения величина, причем более быстрые машины при этом будут иметь более высокий рейтинг MIPS.

MFLOPS

Измерение производительности компьютеров при решении научно-технических задач, в которых существенно используется арифметика с плавающей точкой, всегда вызывало особый интерес. Именно для таких вычислений впервые встал вопрос об измерении производительности, а по достигнутым показателям часто делались выводы об общем уровне разработок компьютеров. Обычно для научно-технических задач производительность процессора оценивается в MFLOPS (миллионах чисел-результатов вычислений с плавающей точкой в секунду, или миллионах элементарных арифметических операций над числами с плавающей точкой, выполненных в секунду).

Как единица измерения MFLOPS предназначена для оценки производительности только операций с плавающей точкой и поэтому не применима вне этой ограниченной области.

Ясно, что рейтинг MFLOPS зависит от машины и от программы. Этот термин менее безобидный, чем MIPS. Он базируется на количестве выполняемых операций, а не на количестве выполняемых команд. Именно поэтому рейтинг MFLOPS предназначался для справедливого сравнения различных машин между собой.

Наиболее часто MFLOPS, как единица измерения производительности, используется при проведении контрольных испытаний на тестовых пакетах «Ливерморские циклы» и LINPACK

Ливерморские циклы

Ливерморские циклы - это набор фрагментов фортран-программ, каждый из которых взят из реальных программных систем, эксплуатируемых в Ливерморской национальной лаборатории им. Лоуренса (США). Обычно при проведении испытаний используется либо малый набор из 14 циклов, либо большой набор из 24 циклов.

На векторной машине производительность зависит не только от элементной базы, но и от характера самого алгоритма, т.е. коэффициента векторизуемости. Среди Ливерморских циклов коэффициент векторизуемости колеблется от 0 до 100%,. Кроме характера алгоритма, на коэффициент векторизуемости влияет и качество векторизатора, встроенного в компилятор.

На параллельной машине производительность существенно зависит от соответствия между структурой аппаратных связей вычислительных элементов и структурой вычислений в алгоритме. В Ливерморских циклах встречаются последовательные, сеточные, конвейерные, волновые вычислительные алгоритмы, что подтверждает их пригодность и для параллельных машин. Однако обобщение результатов измерения производительности, полученных для одной параллельной машины, на другие параллельные машины или хотя бы на некоторый подкласс парал-

лельных машин может дать неверный результат, ибо структуры аппаратных связей в таких машинах гораздо более разнообразны, чем, скажем, в векторных машинах.

LINPACK - это пакет фортран-программ для решения систем линейных алгебраических уравнений.

В основе алгоритмов действующего варианта LINPACK лежит метод декомпозиции. Исходная матрица размером 100x100 элементов (в последнем варианте размером 1000x1000) сначала представляется в виде произведения двух матриц стандартной структуры, над которыми затем выполняется собственно алгоритм нахождения решения. Подпрограммы, входящие в LINPACK, структурированы. В стандартном варианте LINPACK выделен внутренний уровень базовых подпрограмм, каждая из которых выполняет элементарную операцию над векторами. Набор базовых подпрограмм называется BLAS (Basic Linear Algebra Subprograms). Результат измеряется в MFLOPS.

Контрольные вопросы

1. В чем заключается сть параллельной обработки информации?
2. В чем заключается метод конвеерной обработки информации?
3. На каком понятии базируется классификация Флина?
4. Какие факторы обуславливают отклонение от максимального ускорения?
5. По каким принципам рассичтывается производительность вычислительных систем?

Лекция 4
Классификация сетей

1. **Введение в компьютерные сети. Эволюция сетей.**
2. **Операционная система**
3. **Классификация компьютерных сетей**

Ключивые слова: передача данных, компьютерная сеть, коммуникационное оборудование, операционная система, сетевые приложения, ядро, командный интерпретатор, драйвер, интерфейс, разрядность, классификация сетей.

1. Сети для передачи цифровых данных

Сети передачи данных появились и начали развиваться из-за того, что на коммерческих предприятиях и в правительственных организациях возникла потребность в обмене электронной информацией на больших расстояниях. В то время микрокомпьютеры не были соединены между собой, как терминалы мейнфрейма с центральным блоком, и вследствие этого отсутствовал эффективный способ совместного использования данных несколькими микрокомпьютерами.

С течением времени становилось очевидным, что совместное использование данных путем переноса их на гибких дисках является неэффективным и дорогостоящим способом работы.

Компании осознали, что применение сетевых технологий повысит производительность труда и позволит сэкономить средства. По мере появления новых сетевых технологий, аппаратных и программных продуктов, столь же стремительно появлялись новые сети и расширялись прежние.

Компьютерная сеть - это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов.

Эволюция сетей.

Вообще всю сетевую эволюцию можно разделить на 6 этапов:

1. системы пакетной обработки (50-е годы);
2. многотерминальные системы (60-е годы);
3. первые глобальные сети;
4. первые локальные сети (70-е годы):
5. создание стандартных технологий локальных сетей (середина 80-ых);
6. современные тенденции развития.

Первоначально сети представляли собой абсолютно не стандартизованные средства взаимодействия автономных компьютеров в настолько же не стандартизованных вычислительных системах. Компании, перед которыми в предшествовавшие появлению персональных компьютеров времена стояли задачи автоматизации обработки данных и бухгалтерского учета, вынуждены были доверять решение «под ключ» единственному производителю.

Года	Название периода	Основные характеристики
50-ые	системы пакетной обработки	- пакетная обработка (не интерактивная); - строились на базе мейнфреймов (MainFrame); - главное – эффективность работы вычислительной машины (процессора) в ущерб эффективности работы использующего его специалистов.
60-ые – н.70-ых	многотерминальные системы разделения времени (прообраз сети)	- удешевление процессоров; - каждому пользователю по терминалу; - вычислительная мощность всё ещё централизованная, хотя некоторые функции (в/в) – распределённые; - действует «закон Гроша».
	первые глобальные сети	- возможность обмениваться данными в автоматическом режиме; - впервые: многоуровневое построение коммуникационных протоколов, технологии коммутации пакетов, маршрутизация пакетов в составных сетях.
конец 70-ых	первые локальные сети	- появились БИС – создание микрокомпьютеров; - концепция распределения компьютерных ресурсов по всему предприятию; - использование нестандартного оборудования для соединения мини-ЭВМ.
середина 80-ых	стандартные технологии ЛВС	- появление персональных компьютеров; - утверждение стандартных технологий объединения компьютеров в сеть (Ethernet, Token Ring, Arcnet); - новые способы организации работы пользователей.
наше время	современные тенденции	- сокращается разрыв м/д локальными и глобальными сетями; - возобновляется интерес к крупным корпоративным компьютерам; - широкое развитие Интернет; - обработка несвойственной ЛВС информации – голоса, видео, рисунков; - дальнейшая интеграция любых информационных сетей (вычислительных, телефонных, телевизионных и т.п.).

Коммуникационное оборудование.

–кабельные системы,

–повторители,

–мосты,

–коммутаторы,

–маршрутизаторы

–модульные концентраторы

В настоящий момент занимают центральное положение наряду с компьютерами и системным программным обеспечением:

–основное влияние на характеристики сети (скорость, время доступа, и т.п.),

–существенное влияние на стоимость сети.

Сегодня коммуникационное устройство – сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Изучение принципов работы коммуникационного оборудования требует знакомства с большим количеством протоколов, используемых как в локальных, так и глобальных сетях.

Операционные системы (ОС).

Эффективность работы всей сети зависит от того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС.

При проектировании сети важно учитывать следующие моменты:

- насколько просто данная операционная система может взаимодействовать с другими ОС сети;
- насколько она обеспечивает безопасность и защищенность данных;
- до какой степени она позволяет наращивать число пользователей;
- можно ли перенести ее на компьютер другого типа;
- и т.д.

Сетевые приложения.

- сетевые базы данных,
- почтовые системы,
- средства архивирования данных,
- системы автоматизации коллективной работы
- и др.

Очень важно представлять диапазон возможностей, предоставляемых приложениями для различных областей применения, а также знать, насколько они совместимы с другими сетевыми приложениями и операционными системами.

2. Операционная система

Операционная система — вот так называется первая и самая главная программа, благодаря которой становится возможным общение между компьютером и человеком.

Операционная система (ОС) — это своего рода буфер-передатчик между компьютерным железом и остальными программами. ОС принимает на себя сигналы-команды, которые посылают другие программы, и «переводит» их на понятный машине язык. ОС управляет всеми подключенными к компьютеру устройствами, обеспечивая доступ к ним другим программам. Наконец, третья задача ОС — обеспечить удобство работы с компьютером для человека-пользователя.

Получается, что каждая ОС состоит как минимум из трех обязательных частей.

Первая — ***ядро, командный интерпретатор,*** «переводчик» с программного языка на «железный», язык машинных кодов.

Вторая - специализированные программки для управления различными устройствами, входящими в состав компьютера. Такие программки называются ***драйверами*** — т. е. «водите-

лями», управляющими. Сюда же относятся так называемые «системные библиотеки», используемые как самой операционной системой, так и входящими в ее состав программами.

И, наконец, третья часть — удобная оболочка, с которой общается пользователь — ***интерфейс.***

Сегодня графический интерфейс неизменный атрибут любой операционной системы, будь то Windows 98/ME, Windows NT/2000 или MacOS, операционная система для компьютеров Apple Macintosh. Но операционные системы первых поколений имели не графический, а текстовый интерфейс, т. е. команды компьютеру отдавались не щелчком мышки по рисунку-пиктограмме, а с помощью введения команд с клавиатуры.

Операционные системы делятся на **однозадачные и многозадачные.** Здесь тоже все ясно: однозадачные операционные системы (DOS) могут выполнять в одно и то же время не более одной задачи, а многозадачные ОС (Windows 98/ME) способны, одновременно управляться с несколькими процессами, деля между ними мощность компьютера.

Еще один критерий — число пользователей ОС.

Операционная система бывает **однопользовательской** (предназначенной для обслуживания одного клиента) и **многопользовательской** (рассчитанной на работу с группой пользователей одновременно). Примером первой может служить все та же Windows 98/ME, а второй - Windows NT/2000. Для домашнего использования вам понадобится, конечно же, однопользовательская ОС.

И последнее — **разрядность.** Мы с вами уже говорили о разрядности процессора — точно также разрядность характеризует и ОС. 16-разрядные операционные системы (DOS, Windows 3.1, Windows 3.11) ушли в прошлое с появлением Windows 98/ME. 64-разрядных ОС для домашнего использования пока нет — неудивительно, ведь первый 64-разрядный процессор для рынка массовых компьютеров под названием Itanium появился на рынке только в 2001 году.

Сетевые операционные системы

Структура сетевой операционной системы

Сетевая операционная система составляет основу любой вычислительной сети. Каждый компьютер в сети в значительной степени автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам - протоколам. В узком смысле сетевая ОС - это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

В сетевой операционной системе отдельной машины можно выделить несколько частей (рис.1):

Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами в мультипроцессорных машинах, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.

Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов;

обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.

Рис. 1. Структура сетевой ОС

Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи.В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

На рис. 2 показано взаимодействие сетевых компонентов. Здесь компьютер 1 выполняет роль «чистого» клиента, а компьютер 2 - роль «чистого» сервера, соответственно на первой машине отсутствует серверная часть, а на второй - клиентская. На рисунке отдельно показан компонент клиентской части - редиректор. Именно редиректор перехватывает все запросы, поступающие от приложений, и анализирует их. Если выдан запрос к ресурсу данного компьютера, то он переадресовывается соответствующей подсистеме локальной ОС, если же это запрос к удаленному ресурсу, то он переправляется в сеть. При этом клиентская часть преобразует запрос из локальной формы в сетевой формат и передает его транспортной подсистеме, которая отвечает за доставку сообщений указанному серверу. Серверная часть операционной системы компьютера 2 принимает запрос, преобразует его и передает для выполнения своей локальной ОС. После того, как результат получен, сервер обращается к транспортной подсистеме и направляет ответ клиенту, выдавшему запрос. Клиентская часть преобразует результат в соответствующий формат и адресует его тому приложению, которое выдало запрос.

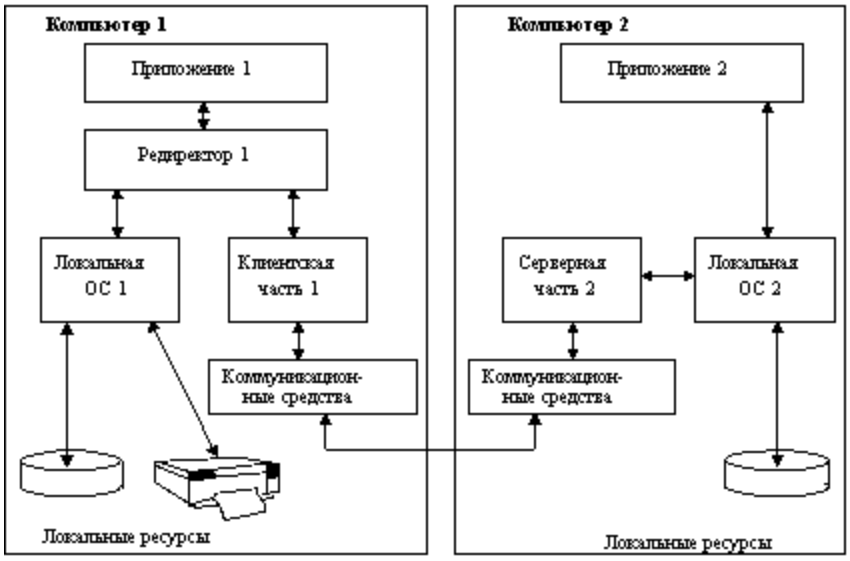


Рис. 2. Взаимодействие компонентов операционной системы при взаимодействии компьютеров

На практике сложилось несколько подходов к построению сетевых операционных систем (рис. 3).

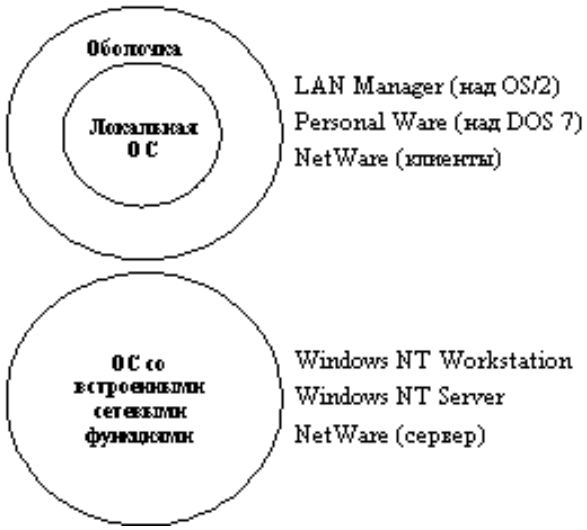


Рис. 3. Варианты построения сетевых ОС

Первые сетевые ОС представляли собой совокупность существующей локальной ОС и надстроенной над ней сетевой оболочки. При этом в локальную ОС встраивался минимум сетевых функций, необходимых для работы сетевой оболочки, которая выполняла основные сетевые функции. Примером такого подхода является использование на каждой машине сети операционной системы MS DOS (у которой начиная с ее третьей версии появились такие встроенные функции, как блокировка файлов и записей, необходимые для совместного доступа к файлам).

Принцип построения сетевых ОС в виде сетевой оболочки над локальной ОС используется и в современных ОС, таких, например, как LANtastic или Personal Ware.

Обзор сетевых операционных систем

Большое разнообразие типов компьютеров, используемых в вычислительных сетях, влечет за собой разнообразие операционных систем: для рабочих станций, для серверов сетей уровня отдела и серверов уровня предприятия в целом. К ним могут предъявляться различные требования по производительности и функциональным возможностям, желательно, чтобы они обладали свойством совместимости, которое позволило бы обеспечить совместную работу различных ОС.

Сетевые ОС могут быть разделены на две группы: масштаба отдела и масштаба предприятия. ОС для отделов или рабочих групп обеспечивают набор сетевых сервисов, включая разделение файлов, приложений и принтеров. Они также должны обеспечивать свойства отказо-

устойчивости, например, работать с RAID-массивами, поддерживать кластерные архитектуры. Сетевые ОС отделов обычно более просты в установке и управлении по сравнению с сетевыми ОС предприятия, у них меньше функциональных свойств, они меньше защищают данные и имеют более слабые возможности по взаимодействию с другими типами сетей, а также худшую производительность.

Сетевая операционная система масштаба предприятия прежде всего должна обладать основными свойствами любых корпоративных продуктов, в том числе:

- масштабируемостью, то есть способностью одинаково хорошо работать в широком диапазоне различных количественных характеристик сети,
- совместимостью с другими продуктами, то есть способностью работать в сложной гетерогенной среде интерсети в режиме plug-and-play.

Корпоративная сетевая ОС должна поддерживать более сложные сервисы. Подобно сетевой ОС рабочих групп, сетевая ОС масштаба предприятия должна позволять пользователям разделять файлы, приложения и принтеры, причем делать это для большего количества пользователей и объема данных и с более высокой производительностью. Кроме того, сетевая ОС масштаба предприятия обеспечивает возможность соединения разнородных систем - как рабочих станций, так и серверов.

Важным элементом сетевой ОС масштаба предприятия является централизованная справочная служба, в которой хранятся данные о пользователях и разделяемых ресурсах сети. Такая служба, называемая также службой каталогов, обеспечивает единый логический вход пользователя в сеть и предоставляет ему удобные средства просмотра всех доступных ему ресурсов. Администратор, при наличии в сети централизованной справочной службы, избавлен от необходимости заводить на каждом сервере повторяющийся список пользователей, а значит избавлен от большого количества рутинной работы и от потенциальных ошибок при определении состава пользователей и их прав на каждом сервере.

Важным свойством справочной службы является ее масштабируемость, обеспечиваемая распределенностью базы данных о пользователях и ресурсах.

Такие сетевые ОС, как Banyan Vines, Novell NetWare 4.x, IBM LAN Server, Sun NFS, Microsoft LAN Manager и Windows NT Server, могут служить в качестве операционной системы предприятия, в то время как ОС NetWare 3.x, Personal Ware, Artisoft LANtastic больше подходят для небольших рабочих групп.

Критериями для выбора ОС масштаба предприятия являются следующие характеристики:

- Органичная поддержка многосерверной сети;
- Высокая эффективность файловых операций;
- Возможность эффективной интеграции с другими ОС;
- Наличие централизованной масштабируемой справочной службы;
- Хорошие перспективы развития;
- Эффективная работа удаленных пользователей;
- Разнообразные сервисы: файл-сервис, принт-сервис, безопасность данных и отказоустойчивость, архивирование данных, служба обмена сообщениями, разнообразные базы данных и другие;
- Разнообразные программно-аппаратные хост-платформы: IBM SNA, DEC NSA, UNIX;

- Разнообразные транспортные протоколы: TCP/IP, IPX/SPX, NetBIOS, AppleTalk;
- Поддержка многообразных операционных систем конечных пользователей: DOS, UNIX, OS/2, Mac;
- Поддержка сетевого оборудования стандартов Ethernet, Token Ring, FDDI, ARCnet;
- Наличие популярных прикладных интерфейсов и механизмов вызова удаленных процедур RPC;
- Возможность взаимодействия с системой контроля и управления сетью, поддержка стандартов управления сетью SNMP.

Конечно, ни одна из существующих сетевых ОС не отвечает в полном объеме перечисленным требованиям, поэтому выбор сетевой ОС, как правило, осуществляется с учетом производственной ситуации и опыта. В таблице приведены основные характеристики популярных и доступных в настоящее время сетевых ОС.

3. Классификация компьютерных сетей

Для классификации компьютерных сетей используются различные признаки, но чаще всего сети делят на типы ***по территориальному признаку***, то есть по величине территории, которую покрывает сеть. И для этого есть веские причины, так как отличия технологий локальных и глобальных сетей очень значительны, несмотря на их постоянное сближение.

- локальных сетей (Local Area Networks - LAN);
- распределенных сетей (Wide Area Networks - WAN);
- городских или региональных сетей (Metropolitan Area Networks - MAN);
- сетей хранилищ данных (Storage Area Networks - SAN);
- центров обработки данных (Data center);
- внутренних сетей (Intranet сети);
- внешних сетей (Extranet сети);
- виртуальных частных сетей (Virtual Private Networks - VPN).

Локальные сети – Local Area Networks (LAN).

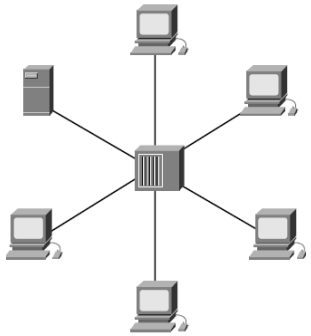


Рис. 4. Локальная сеть (LAN)

Локальная сеть (Local Area Network - LAN) состоит из компьютеров, сетевых адаптеров (network interface cards), периферийных устройств, среды передачи данных по сети и других сетевых устройств. На рис. 4 проиллюстрирована локальная сеть LAN.

- Сосредоточенны на небольшой территории (обычно в радиусе не более 1-2 км).
- В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации.
- Использование относительно дорогих высококачественных линий связи (короткие расстояния в локальных сетях), которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными порядка 100 Мбит/с.

Глобальные сети - Wide Area Networks (WAN).

Распределенные сети (Wide Area Networks - WAN) соединяют между собой локальные сети LAN, что позволяет компьютерам LAN-сетей получать доступ к компьютерам и файловым серверам, находящимся в других локальных сетях. Поскольку WAN-сети соединяют пользователей, расположенных в обширной географической области, они делают возможным для предприятий осуществление связи на больших расстояниях (рис. 5).

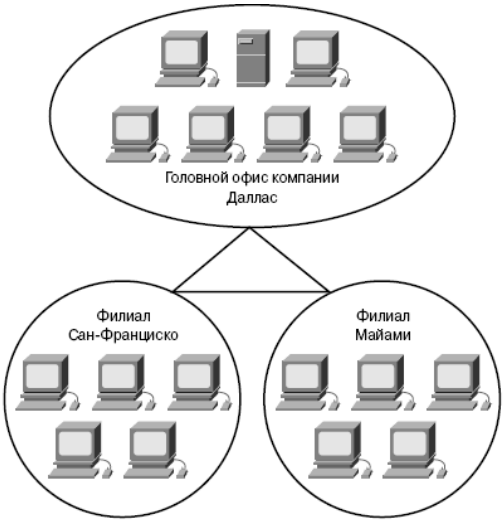


Рис. 5. Распределенная сеть (WAN)

Использование технологий распределенной сети позволяет компьютерам, принтерам и другим устройствам локальной сети LAN обмениваться данными с удаленными локальными сетями.

Распределенные сети WAN предназначены для выполнения следующих функций:

- осуществления связи в больших, географически разделенных областях;
- предоставления пользователям возможности коммуникации в реальном времени с другими пользователями;
- непрерывного обеспечения доступа к удаленным ресурсам через соединения с локальными службами;
- обеспечения службы электронной почты, World Wide Web, передачи файлов и средств электронной коммерции в сети Internet.

Городские сети (или сети мегаполисов) - Metropolitan Area Networks (MAN)

Под региональной или городской сетью (Metropolitan Area Network -MAN) понимается сеть, охватывающая территорию крупного города, включая пригородные зоны. Сети MAN соединяют между собой локальные сети LAN, находящиеся на определенном расстоянии друг от друга, но в одной общей географической области, как показано на рис. 6. Например, MAN-сеть может использоваться банком, имеющим в городе несколько отделений. Обычно провайдер службы соединяет между собой две или более LAN-сетей, используя свои частные линии коммуникаций или оптические службы. MAN-сеть также может быть создана с использование беспроводной мостовой технологии путем передачи сигналов через открытые телекоммуникационные инфраструктуры. Широкая полоса пропускания, предоставляемая доступными в настоящее время оптическими каналами, делает MAN-сети более функциональным и экономически доступным средством, чем раньше. MAN-сети отличаются от LAN- и WAN-сетей следующими функциями:

- MAN-сети соединяют друг с другом пользователей, находящихся в географической зоне или области большей, чем область LAN-сети, но меньшей, чем WAN-сети;

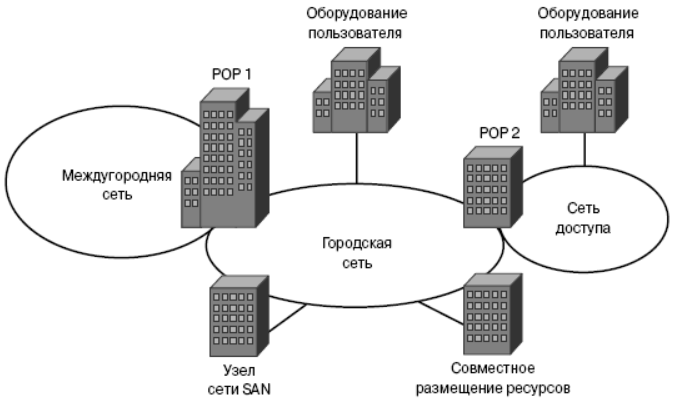


Рис. 6. Сеть масштаба города

- MAN-сети соединяют сети города в одну сеть большего размера (которая может также обеспечивать эффективное соединение с WAN-сетью);
- MAN-сети также используются для соединения между собой нескольких локальных сетей LAN путем создания мостовых соединений через магистральные линии.

Первоначально были разработаны для передачи данных, но сейчас они поддерживают и такие услуги, как видеоконференции и интегральную передачу голоса и текста.

Сети хранилищ данных

Рис. 7. Сеть хранилищ данных

Сетями хранилищ данных (Storage Area Network - SAN) называются специализированные выделенные высокоскоростные сети, которые перемещают данные между серверами и хранилищами ресурсов. Поскольку они являются отдельными выделенными сетями, конфликтов между потоками данных от серверов и их клиентов не возникает (рис. 7). SAN-технология позволяет осуществлять высокоскоростные соединения типа «сервер-хранилище», «хранилище-хранилище» и «сервер-сервер».

При таком подходе используется отдельная сетевая инфраструктура, что устраняет все проблемы, связанные с наличием уже установленных в сети соединений. SAN-технология обеспечивает выполнение перечисленных ниже функций.

- **Высокая производительность при передаче данных.** SAN-сети позволяют осуществлять на конкурентной основе доступ к накопителям двум и более серверам с высокой скоростью, что повышает эффективность работы сети.
- **Доступность.** SAN-сети обладают большей внутренней устойчивостью к стихийным бедствиям, поскольку при использовании технологии SAN данные могут быть продублированы на расстояниях вплоть до 10 км.
- **Масштабируемость**. Как и сети LAN/WAN, сети хранилищ SAN могут использовать различные технологии. Это позволяет легко переносить операции резервирования данных, перемещения файлов и дублирования данных из одной системы в другую.

Виртуальные частные сети

Виртуальной частной сетью (Virtual Private Network - VPN) называется частная сеть, которая создается в инфраструктуре открытой сети, такой, например, как глобальная сеть Internet. Используя VPN-сеть, работник может получить доступ к сети головного офиса компании через

сеть Internet путем создания безопасного туннеля между компьютером телеработника и VPN-маршрутизатором в головном офисе.

Существуют три типа VPN-сетей, они показаны на рис. 8.

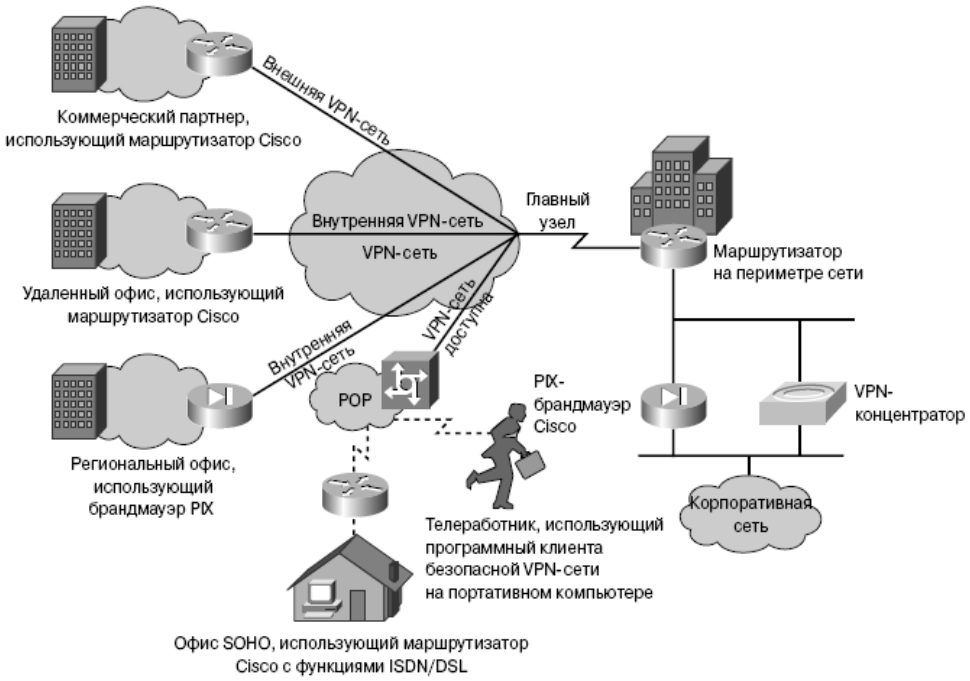


Рис. 8. Технологии VPN-сетей

- *VPN-сети доступа (Access VPN)* обеспечивают удаленный доступ мобильным сотрудникам и малым/домашним офисам (*Small Office/Home Office- SOHO*) к внутренней или внешней сети (*Intranet* или *Extranet*) головного офиса по совместно используемой инфраструктуре. VPN-сети доступа используют аналоговый удаленный доступ, технологии ISDN, DSL, протокол мобильных IP-соединений и кабельные технологии для создания безопасных соединений между сотрудниками головного офиса, телеработниками и филиалами компании.
- *VPN-сети Intranet (внутренние виртуальные частные сети)* связывают между собой региональные и удаленные офисы с головным офисом компании в совместно используемую инфраструктуру с помощью выделенных линий. Внутренние VPN-сети (Intranet) отличаются от внешних VPN-сетей (Extranet) тем, что они разрешают доступ только сотрудникам компании.
- *VPN-сети Extranet (внешние виртуальные частные сети)* соединяют коммерческих партнеров компании с сетью головного офиса через совместно используемую инфраструктуру с помощью выделенных линий. Внешние VPN-сети (Extranet) отличаются от внутренних VPN-сетей (Intranet) тем, что они разрешают доступ некоторым пользователям, не являющимся сотрудниками компании.

VPN-сети обладают следующими преимуществами:

- единая VPN-технология обеспечивает конфиденциальность нескольким приложениям протокола TCP/IP. Это особенно важно в ситуациях, когда требуется обеспечить безопасный доступ партнерам или телеработникам;

- службы шифрования могут быть обеспечены всем соединениям TCP/IP между авторизованным пользователем и VPN-сервером. Преимуществом такого подхода является его прозрачность для конечного пользователя. Поскольку включен режим шифрования, сервер может повысить уровень шифрования;
- VPN-сети обеспечивают мобильность сотрудникам компании и позволяют им получать безопасный доступ к корпоративной сети.

Внутренние и внешние сети предприятия

Одной из типичных конфигураций LAN-сетей является *сеть Intranet* (*внутренняя сеть*). Web-серверы внутренней сети (Intranet) отличаются от открытых Web-серверов тем, что посторонние лица не имеют доступа к Intranet-сети организации без соответствующего разрешения и пароля. Внутренние сети (Intranet) спроектированы таким образом, что доступ к ним может быть получен только пользователем, имеющим право привилегированного доступа к внутренней локальной сети организации. Во внутренних сетях Web-серверы находятся внутри сети, а использование браузера является основным средством получения доступа к финансовым данным, а также к графическим и текстовым данным, хранящимся на этих серверах.

Сетью *Extranet (внешняя сеть*) называют внутреннюю сеть (Intranet), частичный доступ, к которой имеют и авторизованные внешние пользователи. В то время как внутренняя сеть (Intranet) находится за брандмауэром и доступна только сотрудникам компании или организации, сеть Extranet обеспечивает различные уровни доступа для посторонних внешних пользователей. Пользователь может получить доступ к внешней сети (Extranet) только в том случае, если у него есть зарегистрированные в этой сети имя и пароль; идентификационные данные пользователя определяют уровень разрешенного ему доступа и доступные для просмотра области внешней сети (Extranet). Внешние сети (Extranet) помогают расширить сферу действия приложений и служб, которые базируются на Intranet-сети предприятия, но используют расширенный безопасный доступ ко внешним пользователям и предприятиям. Такой доступ обычно осуществляется с помощью паролей, идентификаторов (ID) пользователей и других средств обеспечения безопасности на уровне приложений. Соответственно, внешнюю сеть (Extranet) можно рассматривать как расширение стратегий двух или более внутренних сетей (Intranet) с безопасным взаимодействием участвующих предприятий и их соответствующих внутренних сетей (Intranet). Внешние сети (Extranet) поддерживают управление доступом ко внутренним сетям (Intranet) отдельных предприятий. Как правило, они используются для поддержки соединений потребителей, поставщиков, коммерческих партнеров и сообществ по интересам с корпоративной внутренней сетью (Intranet) по совместно используемой инфраструктуре с использованием выделенных линий. На рис. 6 показаны внешняя и внутренняя сети (Intranet и Extranet).

Промышленные сети - Fieldbus

Современные технологии автоматизации, используемые в промышленных структурах, предполагают наличие сложных разнородных сетей передачи данных, сетей сбора технологической информации, а также телефонных систем. Крупные коммерческие и/или банковские структуры, как правило, также применяют сети сбора данных с различного «технологического» обо-

рудования (источники бесперебойного питания для компьютерных систем, системы охраны, контроля доступа и видео наблюдения, системы энерго и тепло обеспечения зданий и пр.).

Общими особенностями структурной реализации таких сетей является:

- территориальная распределенность,
- разнородность применяемого оборудования,
- необходимость интеграции в компьютерные сети более высокого уровня.

Промышленная сеть Fieldbus (полевая шина, или промышленная сеть) - коммуникационная технология построения единой информационной сети, объединяющей интеллектуальные контроллеры, датчики и исполнительные механизмы, определяется одним термином.

Fieldbus - это, во-первых, некая физическая коммуникационная технология объединения устройств и, во-вторых, программно-логический протокол взаимодействия этих устройств.

Fieldbus - это сеть для промышленного применения, логически очень похожая на LAN-сети, применяемые в офисных приложениях. Однако промышленные сети призваны выполнять специфический набор функций:

- жесткая детерминированность (предсказуемость) поведения;
- обеспечение функций реального времени;
- работа на длинных линиях с использованием недорогих физических сред (например, витая пара);
- повышенная надёжность физического и канального уровней передачи данных для работы в промышленной среде (высокий уровень электромагнитных помех);
- наличие специальных высоконадёжных механических соединительных компонентов;

Примеры промышленных технологий это – протокол BITBUS, технологии CAN, INTERBUS, LON, PROFIBUS и т.д.

Контрольные вопросы

1. На какие этапы можно разделить развитие компьютерных сетей?
2. Что такое операционная система и каковы ее функции?
3. Как классифицируются сетевые ОС?
4. По какому признаку классифицируются компьютерные сети?
5. Сколько типов компьютерных сетей существует и каковы их характеристики?

Лекция 5
Топология сетей

1. **Топологии и типы физических связей**
2. **Типы сетей**

Ключивые слова: топология, одноранговые сети, клиент-сервер, соединительная точка, сегмент, lan ethernet, фрейм, магистральный узел, рабочие группы.

1. Топологии и типы физических связей

При объединении в сеть большего числа компьютеров возникает целый комплекс новых проблем. В первую очередь необходимо выбрать способ организации физических связей, то есть *топологию*.

Под топологией вычислительной сети понимается конфигурация графа, вершинам которого соответствуют компьютеры сети (иногда и другое оборудование, например концентраторы), а ребрам - физические связи между ними.

Компьютеры, подключенные к сети, часто называют станциями или узлами сети.

Сети имеют как физическую, так и логическую топологии. Термин *физическая топология* относится к физическому расположению устройств и соединениям передающей среды.

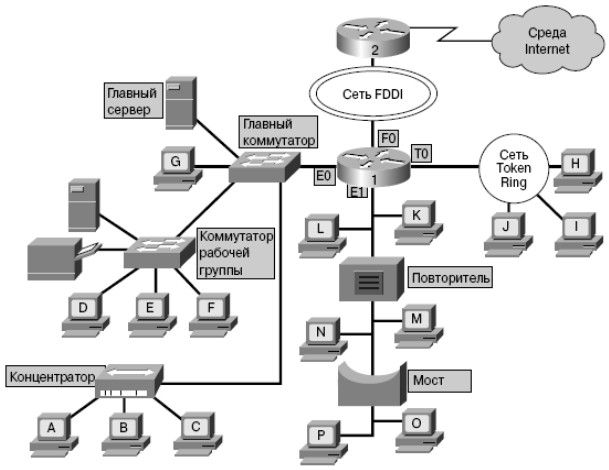


Рис. 1. Сетевые топологии

Логическая топология определяет, каким образом рабочие станции получают доступ к передающей среде для отправки данных. В следующих разделах описываются различные типы физических и логических топологий. На рис. 1 показаны несколько сетей с различными топологиями, которые соединены с разными традиционными сетевыми устройствами. На этом рисунке изображена сеть средней сложности, типичная для школы или малого предприятия.

Шинная топология

Обычно называемая линейной шиной (linear bus) *шинная топология* (*bus topology*) подразумевает соединение всех устройств одним кабелем (рис. 2). Этот кабель проходит от одного компьютера к другому.

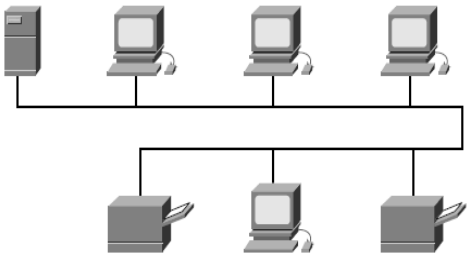


Рис. 2. Шинная топология

Основные характеристики:

- передаваемая информация распространяется в обе стороны;
- применение общей шины снижает стоимость проводки;
- унифицирует подключение различных модулей;

- обеспечивает возможность почти мгновенного широковещательного обращения ко всем станциям сети.

Основными преимуществами (достоинствами) такой схемы является дешевизна и простота разводки кабеля по помещениям.

Недостатки общей шины:

- самый серьезный, ее низкая надежность: любой дефект кабеля или какого-нибудь из многочисленных разъемов полностью парализует всю сеть. К сожалению, дефект коаксиального разъема редкостью не является.
- невысокая производительность, так как при таком способе подключения в каждый момент времени только один компьютер может передавать данные в сеть. Поэтому пропускная способность канала связи всегда делится здесь между всеми узлами сети.

Звездообразная и расширенная звездообразная топологии

Звездообразная топология (star topology), показанная на рис. 3, представляет собой наиболее часто используемый тип сетевой топологии как в локальных структурах, так и в распределенных. Звездообразная топология состоит из центральной соединительной точки, и расходящихся от нее сегментов кабелей.

В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети.

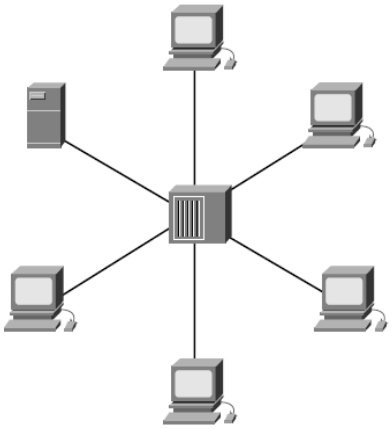


Рис. 3. Звездообразная топология

Достоинства:

- главное, высокая надежность. Любые неприятности с кабелем касаются лишь того компьютера, к которому этот кабель присоединен, и только неисправность концентратора может вывести из строя всю сеть;
- интеллектуальность сети. Концентратор может играть роль интеллектуального фильтра информации, поступающей от узлов в сеть, и при необходимости блокировать запрещенные администратором передачи.

Недостатки топологии типа звезда:

- более высокая стоимость сетевого оборудования из-за необходимости приобретения концентратора;
- возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора.

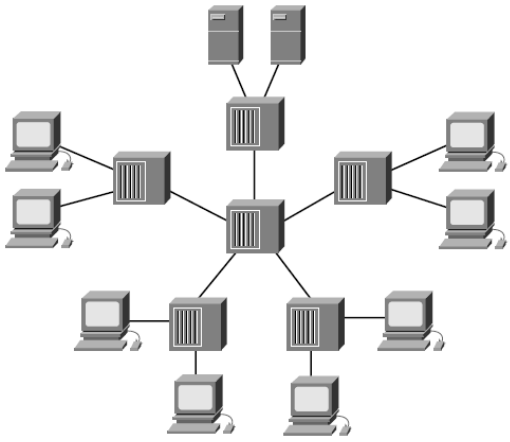


Рис. 4. Расширенная звездообразная топология

Если сеть со звездообразной топологией расширяется для включения дополнительных сетевых устройств, подсоединенных к главному сетевому устройству (центральной точке), то полученную топологию называют *расширенной звездообразной топологией (extended star topology)*. Такая сеть показана на рис. 4.

Поскольку каждая рабочая станция подсоединена к центральному устройству отдельным кабелем, то при возникновении проблем с одним из таких кабелей сеть останется работоспособной. Такое свойство звездообразной топологии особенно важно, и этим объясняется тот факт, что практически все новые локальные сети LAN Ethernet имеют физическую звездообразную топологию.

Кольцевая топология

Другой важной разновидностью топологии локальных сетей является *кольцевая топология (ring topology*). Как видно из названия, в этой топологии рабочие станции соединены между собой так, что образуют непрерывное кольцо. В отличие от физической шинной топологии, сеть с кольцевой топологией не имеет начала и конца и не требует наличия терминатора. Способ передачи данных по сети с кольцевой топологией значительно отличается от того, который применяется в сети с шинной топологией. В такой сети специальный фрейм перемещается по кольцу, останавливаясь на каждом узле. Если какому-либо узлу требуется передать данные, то он может вставить в этот фрейм свои данные и адрес получателя. После этого фрейм перемещается по кольцу до тех пор, пока не дойдет до узла с адресом получателя, который извлекает данные из этого фрейма. Преимуществом такого способа передачи данных является невозможность коллизий.

Существуют два типа кольцевых топологий:

- одиночное кольцо;
- двойное кольцо.

В топологии одиночного кольца, показанной на рис. 5, все устройства сети вместе используют один кабель, а данные перемещаются только в одном направлении. Каждое устройство ожидает своей очереди для передачи данных по сети. Большинство сетей с топологией одиночного кольца в действительности имеют физические соединения, соответствующие звездообразной топологии.

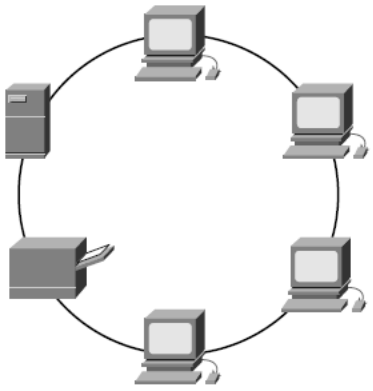


Рис. 5. Кольцевая топология

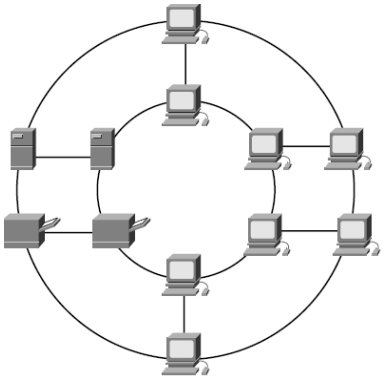


Рис. 6. Топология двойного кольца

В сетях с топологией двойного кольца наличие двух колец позволяет посылать данные в обоих направлениях, как показано на рис. 6. Такая топология обеспечивает в сети избыточность, т.е. возможность в случае выхода из строя одного из кабелей передавать данные по другому кольцу.

Еще одним преимуществом двойного кольца является возможность «сворачивания» (wrap) кольца, т.е. восстановления его работоспособности в случае обрыва.

Достоинства:

Кольцо представляет собой очень удобную конфигурацию для организации обратной связи - данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому этот узел может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для

тестирования связности сети и поиска узла, работающего некорректно. Для этого в сеть посылаются специальные тестовые сообщения.

Недостатки:

В сети с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прервался канал связи между остальными станциями.

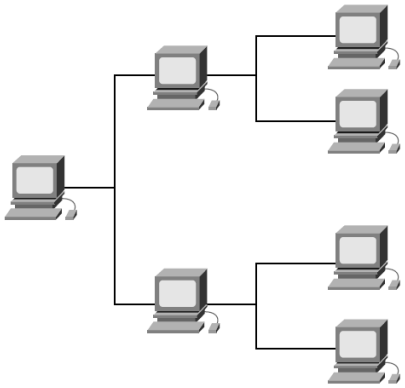


Рис. 7. Иерархическая топология

Иерархическая топология

Иерархическая топология (*hierarchical topology*) создается аналогично расширенной звездообразной топологии. Основным отличием является отсутствие в такой сети центрального узла. Вместо этого используется магистральный узел (*trunk node*), от которого отходят ветви (*branches*) к другим узлам, как показано на рис. 7. Существуют два типа иерархической (древовидной) топологии: бинарное дерево - от каждого узла отходят два соединения; и магистральное дерево - магистральный узел имеет узлы-ветви, от которых отходят каналы к рабочим станциям.

Полно- и неполносвязная топологии

В сети с *полносвязной топологией (full mesh topology*) все устройства (узлы) соединены друг с другом, что обеспечивает избыточность (а в итоге - резервирование) и устойчивость к сбоям, как показано на рис. 8. Такое расположение кабелей сети имеет очевидные достоинства и недостатки.

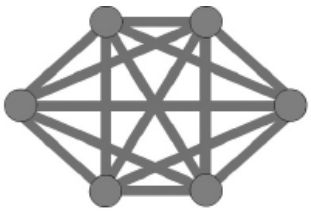


Рис. 8. Полносвязная топология

Достоинством такой структуры является то, что каждый узел физически соединен со всеми остальными, что обеспечивает высокую степень избыточности.

Если какой-либо канал выходит из строя, то существует много других маршрутов, позволяющих передать данные в требуемый пункт назначения. Очевидным недостатком такой сети является то, что, за исключением случая очень небольшого количества узлов в сети, количество соединений становится чрезвычайно большим.

Полносвязная топология обычно используется лишь в соединениях между собой маршрутизаторов распределенных сетей WAN.

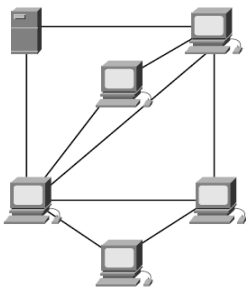


Рис.9. Неполносвязная топология

В сети с *неполносвязной топологией (partial mesh topology*) по крайней мере одно устройство поддерживает несколько соединений с другими устройствами; при этом полносвязная топология не создается.

Пример такой сети приведен на рис. 9. Неполносвязная топология все же создает определенную степень избыточности за счет наличия нескольких альтернативных маршрутов. Если какой-либо из них не может быть использован, данные отправляются по другому маршруту, хотя он может оказаться и более протяженным.

Неполносвязная топология используется во многих телекоммуникационных магистралях, а также в глобальной сети Internet.

2. Типы сетей

Тип сети описывает способ доступа к подключенным ресурсам.

В качестве ресурсов выступают клиенты, серверы или любые устройства, файлы и т.д., принадлежащие клиенту или серверу.

К этим ресурсам можно обращаться одним из двух способов: через одноранговую сеть или через архитектуру клиент/сервер.

Одноранговые сети (peer-to-peer network).

Одноранговые сети предоставляет реструктуризированный доступ к сетевым ресурсам.

Каждое устройство в одноранговой сети может быть и клиентом и сервером одновременно.

В локальных сетях LAN и распределенных сетях WAN объединено большое количество соединенных друг с другом компьютеров, которые предоставляют службы своим пользователям. Для обеспечения связи сетевые компьютеры принимают на себя различные роли или функции по отношению друг к другу. Некоторые типы приложений требуют, чтобы компьютеры выступали в качестве равноправных партнеров. Другие приложения распределяют свою работу таким образом, чтобы один компьютер обслуживал несколько других, т.е. они становятся неравноправными.

В обоих случаях два компьютера взаимодействуют друг с другом, используя протоколы запросов и ответов. Один компьютер посылает запрос на службу, другой компьютер его получает и отвечает на него. Компьютер, посылающий запрос, становится клиентом, а отвечающий принимает на себя роль сервера.

В *одноранговых сетях* (*peer-to-peer network*) сетевые компьютеры выступают равноправными партнерами по отношению друг к другу. Такие сети часто называются *рабочими группами (workgroups)*. Являясь равноправными партнерами, оба компьютера могут принять на себя как функции клиента, так и функции сервера. Например, в одном случае компьютер А может запросить файл у компьютера Б, который отвечает, предоставляя компьютеру А этот файл. При этом компьютер А выступает в качестве клиента, а компьютер Б - в качестве сервера. В другой ситуации компьютеры А и Б могут поменяться ролями. Например, компьютер Б делает запрос на печать компьютеру А, к которому подсоединен совместно используемый принтер, и последний, распечатывая файл, отвечает компьютеру Б, выступая в качестве сервера (рис. 10.).

Рис. 10. Одноранговая сеть

Компьютеры А и Б при этом выступают в качестве равноправных или действуют как одноранговая система. В одноранговых сетях отдельные пользователи сами управляют своими ресурсами. Они могут принять решение о совместном с другими пользователями использовании определенных файлов.

Пользователи могут также потребовать введения пароля перед тем, как разрешить другим компьютерам доступ к своим ресурсам. Поскольку такие решения могут приниматься отдельными пользователями, в рассматриваемых одноранговых сетях отсутствует центральная точка

управления или централизованное администрирование. Кроме того, отдельные пользователи должны самостоятельно делать резервные копии в своих системах, для того чтобы при сбое иметь возможность восстановить свои данные. В случае, когда какой-либо компьютер выступает в качестве сервера, пользователь этой станции может заметить замедление работы своей системы в моменты, когда она обрабатывает запросы других систем.

Одноранговые сети относительно легко устанавливаются и отлаживаются. При этом не требуется никакое дополнительное оборудование, кроме соответствующей операционной системы, устанавливаемой на каждом компьютере. Большинство современных операционных систем для настольных компьютеров обеспечивает поддержку одноранговых сетей. Поскольку пользователи самостоятельно управляют своими ресурсами, специальный сетевой администратор не требуется. Одноранговые сети функционируют достаточно эффективно при небольшом количестве компьютеров - как правило, не более десяти. По мере роста сети становится все труднее координировать одноранговые связи и управлять ими. Ввиду недостаточной масштабируемости одноранговых сетей их эффективность резко падает при увеличении числа компьютеров в сети. Кроме того, тот факт, что управление доступом осуществляется индивидуально каждым пользователем, приводит к тому, что управление безопасностью сети становится затруднительным. Для преодоления ограничений, налагаемых одноранговыми сетями, может быть использована модель «клиент/сервер».

Сети архитектуры клиент-сервер

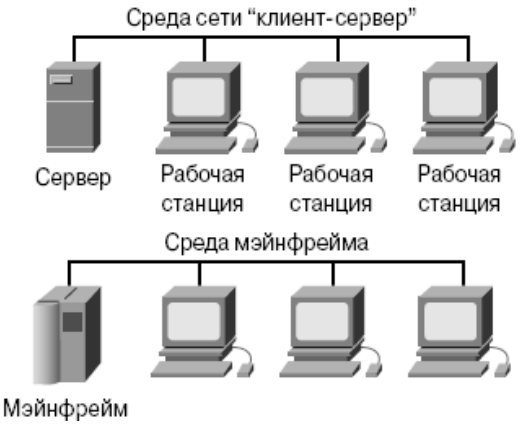


Рис. 11. Модель сети клиент-сервер

В сети со структурой «клиент-сервер» сетевые службы сосредоточены на одном специально предназначенном (выделенном) компьютере, называемом сервером, который отвечает на запросы клиентов, как показано на рис. 11. Этот сервер является центральным компьютером, который постоянно доступен для того, чтобы отвечать на запросы клиентов относительно файловых служб, печати, предоставления приложений и других служб. Большинство сетевых операционных систем (*Network Operating System -NOS*) поддерживают работу сети по модели клиент-сервер.

Обычно настольные компьютеры функционируют как клиенты, а один или более компьютеров, обладающие большей мощностью процессоров, бо́льшим объемом памяти и специализированным программным обеспечением, выступают в качестве серверов.

Серверы предназначены для одновременного обслуживания нескольких клиентов, как показано на рис. 12. До того, как клиент получит доступ к ресурсам сервера, он должен пройти идентификацию и получить авторизацию на право использования ресурсов.

Такая авторизация осуществляется путем назначения каждому пользователю учетной записи (account name) и пароля, который проверяется службой аутентификации, выступающей в качестве охранной службы для предотвращения несанкционированного доступа к сети.

Централизация учетных записей, обеспечения безопасности и управления доступом в сети модели «клиент-сервер» значительно упрощает работу сетевого администратора.

Рис. 12. Ресурсы сервера

Контрольные вопросы

1.По какому признаку деляться топологие компьютерных сетей?
2. Какие виды топологий существуют?
3. В чем приемущества и недостатки различных видов топологий?
4. Какие типы сетей существуют?
5. В чем приемущества и недостатки тазличных типов сетей?

Лекция 6
Методы коммутации

1. **Коммутация каналов**
2. **Коммутация пакетов**
3. **Коммутация сообщений**
4. **Механизмы доступа к среде**

Ключивые слова: коммутация, канал, пакет, сообещник, выделенный канал, арендуемый канал, коммутатор, мультиплексор, демультиплексор, эталонная модель, полудуплекс, дуплекс, синхронизация.

Любые сети поддерживают некоторый способ коммутации своих абонентов между собой. Этими абонентами могут быть удаленные компьютеры, локальны сети, факс-аппараты или просто собеседники, общающиеся между собой с помощью телефонного аппарата. В любой сети всегда применяется какой-либо способ коммутации абонентов, который обеспечивает доступность имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети.

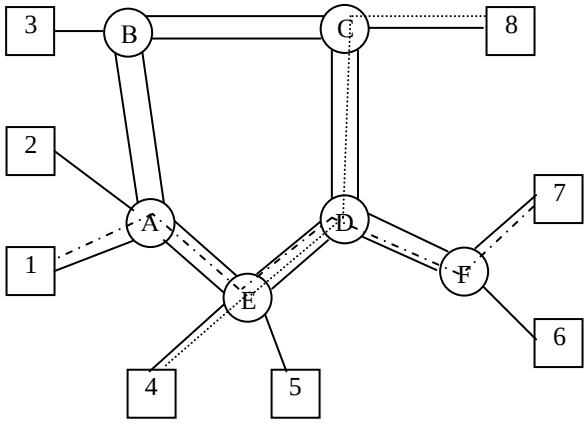


Рис.1 Общая структура сети с коммутацией абонентов

Абоненты соединяются с коммутаторами индивидуальными линиями связи, каждая из которых используется в любой момент времени только одним, закрепленным за этой линией абонентом. Между коммутаторами линии связи разделяются насколькими абонентами, то есть используются совместно.

Существают три принципиально различные схемы коммутации абонентов в сетях:

- коммутация каналов (circuit switching);
- коммутация пакетов (packet switching);
- коммутация сообещний (message switching).

Сети с коммутацией каналов и коммутацией пакетов можно разделить на два класса по другому признаку:

- сети с динамической коммутацией;

- сети с постоянной коммутацией.

В первом случае сеть разрешает устанавливать соединение по инициативе пользователя сети. Коммутация выполняется на время сеанса связи, а затем (опять по инициативе одного из взаимодействующих пользователей) связь разрывается.

Во втором случае сеть не предоставляет пользователю возможность выполнить динамическую коммутацию с другим произвольным пользователем сети. Вместо этого сеть разрешает паре пользователей заказать соединение на длительный период времени. Соединение устанавливается не пользователем, а персоналом, обслуживающим сеть. Режим постоянной коммутации в сетях с коммутацией каналов часто называют сервисом *выделенных (dedicated)* или *арендуемых (leased) каналов*.

Примерами сетей с динамической коммутацией являются телефонные сети общего пользования, локальные сети, сети TCP/IP.

Примером сетей с постоянной коммутацией является сети технологии SDH, на основе которой строятся выделенные каналы с пропускной способностью в несколько гигабит.

Некоторые типы сетей поддерживают оба режима работы (ATM, X25).

1. Коммутация каналов

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой – коммутаторами. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны обладать следующими свойствами:

- быть высокоскоростными;
- поддерживать технику мультиплексирования.

В настоящее время для мультиплексирования абонентских каналов используется две техники:

- техника частотного мультиплексирования (*Frequency Division Multiplexing, FDM*);
- техника мультиплексирования с разделением времени (*Time Division Multiplexing, TDM*).

Коммутация каналов на основе частотного мультиплексирования

Разработана была для телефонных сетей, но применяется и для других видом, например сетей кабельного телевидения.

Рассмотрим особенности этого вида мультиплексирования на примере телефонной сети.

Речевые сигналы имеют спектр шириной примерно в 10 000 Гц, однако основные гармоники укладываются в диапазон от 300 до 3400 Гц. Поэтому для качественной передачи речевых сообщений достаточно иметь канал с полосой пропускания 3100Гц. В тоже время полоса пропускания кабельных систем с промежуточным усилением, соединяющих телефонные коммутаторы между собой, обычно составляет сотни килогерц, а иногда и сотни мегагерц. Однако непосредственно передавать сигналы нескольких абонентских каналов по широкополосному каналу

невозможно, так как все они работают в одном и том же диапазоне частот и сигналы разных абонентов смешиваются между собой так, что разделить их будет не возможно.

Для разделения абонентских каналов характерна техника модуляции высокочастотного несущего синусоидального сигнала низкочастотным речевым сигналом. В результате спектр модулированного сигнала переносится в другой диапазон, который симметрично располагается относительно несущей частоты и имеет ширину, приблизительно совпадающую с шириной модулируемого сигнала.

Если сигналы каждого абонентского канала перенести в свой собственный диапазон частот, то в одном широкополосном канале можно одновременно передавать сигналы нескольких абонентских каналов.

На входы FDM-коммутатора поступают исходные сигналы от абонентов телефонной сети. Коммутатор выполняет переносы частот каждого канала в свой диапазон частот. Обычно высокочастотный диапазон делиться на полосы, которые отводятся для передачи данных абонентских каналов. Чтобы низкочастотные составляющие сигналов разных каналов не смешивались между собой, полосы делают шириной в 4кГц, а не в 3.1кГц, оставляя между собой, промежуток в 900Гц. В канале между двумя FDM-коммутаторами одновременно передаются сигналы всех абонентских каналов, но каждый из них занимает свою полосу частот. Такой канал называют *утопленным*.

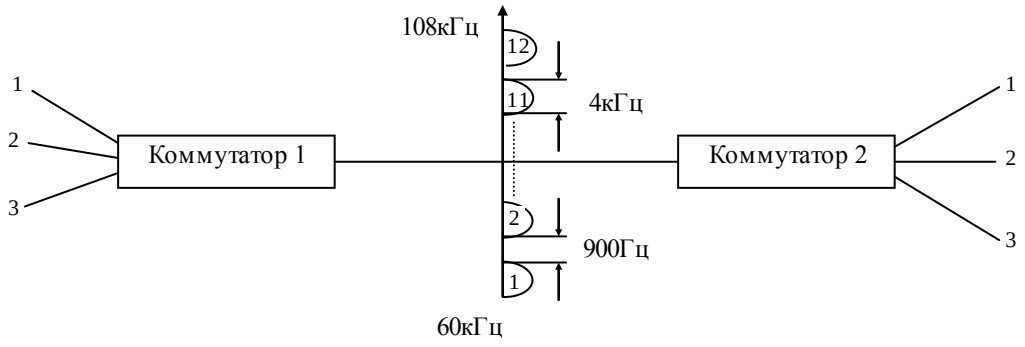


Рис. 2 Коммутация на основе частотного уплотнения

Выходной FDM-коммутатор выделяет модулированные сигналы каждой несущей частоты и передает их на соответствующий выходной канал, к которому непосредственно подключен абонентский телефон.

Коммутаторы FDM могут выполнять как динамическую, так и постоянную коммутацию. При динамической коммутации один абонент инициирует соединение с другим абонентом, посылая номер вызываемого абонента. Коммутатор динамически выделяет данному абоненту одну из свободных полос своего уплотненного канала. При постоянной коммутации за абонентом полоса в 4кГц закрепляется на длительный срок путем настройки коммутатора по отдельному входу, недоступному пользователям.

Принципы коммутации на основе разделения частот остается неизменным и в сетях другого вида, меняются только границы полос, выделяемых отдельному абонентскому каналу, а так же количество низкоскоростных каналов в уплотнении высокоскоростном.

Коммутация каналов на основе разделения времени

Разрабатывалась, ориентируясь на дискретный характер передаваемых данных.

Аппаратура TDM-сетей – мультиплексоры, коммутаторы, демультиплексоры – работает в режиме разделения времени, поочередно обслуживая в течение цикла своей работы все абонентские каналы. Цикл работы оборудования TDM равен 125мкс, что соответствует периоду следования замеров голоса в цифровом абонентском канале. Это значит, что мультиплексор и коммутатор успевает вовремя обслужить любой абонентский канал и передать его очередной замер далее по сети.

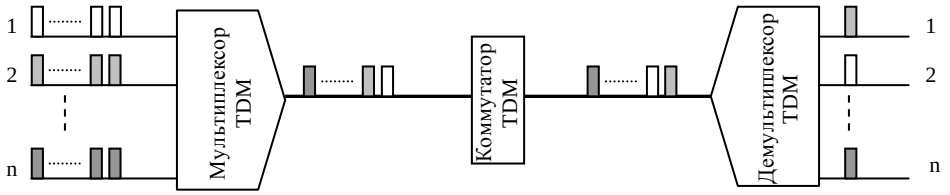


Рис. 3. Коммутация на основе разделения во времени

Каждому соединению выделяется один квант времени цикла работы аппаратуры, называемый также тайм-слотом. Длительность тайм-слота зависит от числа абонентских каналов, обслуживаемых мультиплексором TDM или коммутатором.

Мультиплексор принимает информацию по N входным каналам от конечных абонентов, каждый из которых передает данные по абонентскому каналу со скоростью 64Кбит/с – 1 байт за 125мкс.

В каждом цикле мультиплексор выполняет следующие действия:

- прием от каждого канала очередного байта данных;
- составление из принятых байтов уплотненного кадра, называемого также обоймой;
- передача уплотненного кадра на выходной канал с битовой скоростью, равной N*64 Кбит/с.

Порядок байт в обойме соответствует номеру входного канала, от которого этот байт получен. Количество обслуживаемых мультиплексором абонентских каналов зависит от его быстродействия.

Демультиплексор выполняет обратную задачу – он разбивает байты уплотненного кадра и распределяет их по своим выходным каналам, при этом он считает, что порядковый номер байта в обойме соответствует номеру выходного канала.

Коммутатор принимает уплотненный кадр по скоростному каналу от мультиплексора и записывает каждый байт из него в отдельную ячейку своей буферной памяти, причем в том порядке, котором эти байты упакованы в уплотненный кадр. Для выполнения операции коммутации байты извлекаются из буферной памяти не в порядке поступления, а в таком порядке, который соответствует поддерживаемым в сети соединениям абонентов. «Перемешивая» нужным образом байты в обойме, коммутатор обеспечивает соединение конечных абонентов в сети.

Работа оборудования TDM напоминает работу сетей с коммутацией пакетов, так как каждый байт данных можно считать некоторым элементарным пакетом. Однако в отличие от пакета компьютерной сети, «пакет» сети TDM не имеет индивидуального адреса. Его адресом является порядковый номер в обойме или номер выделенного тайм-слота в мультиплексоре или коммутаторе.

Сети, использующие технику TDM, требуют синхронной работы оборудования. Нарушение синхронности разрушает требуемую коммутацию абонентов, так как при этом теряется адресная информация. Поэтому перераспределение тайм-слотов между различными каналами в оборудовании TDM невозможно, даже если в каком-то цикле работы мультиплексора тайм-слот одного из каналов оказывается избыточным, так как на входе этого канала в этот момент нет данных для передачи.

Существует модификация техники TDM, называется статическим разделением канала во времени (*Statistical TDM, STDM*). Эта техника разработана специально для того, что бы с помощью временно свободных тайм-слотов одного канала можно было увеличить пропускную способность остальных. Для решения этой задачи каждый байт данных дополняется полем адреса небольшой длины, например 4 или 5 бит, что позволяет мультиплексировать 16 или 32 канала. Однако техника STDM не нашла широкого применения и используется в основном в нестандартном оборудовании подключения терминалов к мэйнфреймам. Развитие идей статического мультиплексирования стала технология асинхронного режима передачи – ATM, которая вобрала в себя лучшие черты техники коммутации каналов и пакетов.

2. Коммутация пакетов

Коммутация пакетов – это техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика. Проблема заключается в пульсирующем характере трафика (сначала вы только просматриваете заголовки файлов – небольшой трафик, потом начинаете смотреть сам файл – большой трафик и т.д.). Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может составлять 1:50 или 1:100.

При коммутации пакетов все передаваемые пользователям сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Сообщения могут иметь произвольную длину от нескольких байт, до многих мегобайт. Пакеты обычно тоже имеют переменную длину, но в узких пределах от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а так же номер пакета, который будет использоваться узлом назначения для сборки сообщения. Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге – узлу назначения.

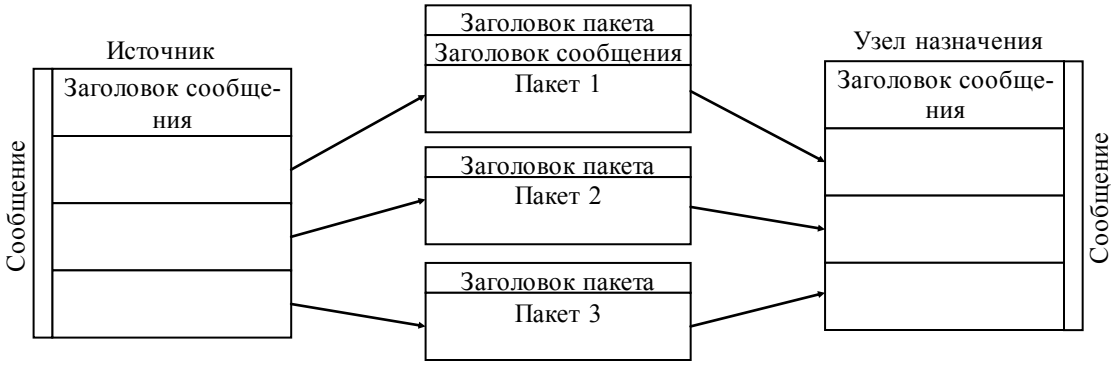


Рис.4 Разбиение сообщения на пакеты

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, то он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их наиболее эффективным образом для повышения пропускной способности сети в целом.

3. Коммутация сообщений

Под коммутацией сообщений понимается передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера.

Сообщение в отличие от пакета имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием информации, составляющей сообщение. Например, сообщение может быть текстовый документ, файл с кодом программы, электронное письмо.

Транзитные компьютеры могут соединяться между собой как сетью с коммутацией пакетов, так и сетью с коммутацией каналов. Сообщение храниться в транзитном компьютере на диске, причем время хранения может быть достаточно большим, если компьютер загружен другими работами или сеть временно перегружена.

По такой схеме обычно передаются сообщения, не требующие немедленного ответа, чаще всего сообщения электронной почты. Режим коммутации сообщений разгружает сеть для передачи трафика, требующего быстрого ответа, например трафика WWW или файловой службы.

Количество компьютеров стараются по возможности уменьшить. Если компьютеры подключены к сети с коммутацией пакетов, то число промежуточных компьютеров обычно уменьшается до двух. Например, пользователь предает сообщение своему серверу исходящей почты, а тот сразу старается передать сообщение серверу входящей почты адресата. Но, если компьютеры связаны между собой телефонной сетью, то часто используется несколько промежуточных серверов, так как прямой доступ к конечному серверу может быть не возможен в данный момент из-за перегрузки телефонной сети.

Сегодня техника коммутации сообщений работает только для некоторых не оперативных служб, причем чаще всего поверх сети с коммутацией пакетов, как служба прикладного уровня.

4. Механизмы доступа к среде

Каждая сеть должна поддерживать определенный механизм управления доступом к среде передачи данных. Реализуется доступ к среде на втором (канальном) уровне эталонной модели OSI. Хотя теоретически механизм доступа к среде должен быть универсальным, на практике различают несколько способов его реализации. В частности, в локальных сетях для управления доступом к среде передачи данных используется четыре различных подхода:

- конкуренция за право доступа;
- передача маркера;
- доступ по приоритету;
- коммутируемый доступ.

Доступ к среде на основе конкуренции

В локальной сети, устройства которой соревнуются за право на передачу данных, применяется метод доступа к среде на основе конкуренции (contention-based media access method). Совокупность устройств, соперничающих друг с другом за полосу пропускания, называются конфликтным доменом (collision domain). Данный метод применяется во многих разновидностях Ethernet.

Технология доступа к среде на основе конкуренции довольна примитивна и не предполагает использования централизованного механизма управления. Вместо этого каждое сетевое устройство берет на себя все функции по организации процесса передачи своих данных. Каждый раз, когда устройство собирается передать данные, оно должно определить, доступен ли кабель для передачи или уже используется другим устройством. Если кабель используется, необходимо подождать и через некоторое время предпринять следующую попытку.

Из приведенного описания механизма доступа к среде на основе конкуренции можно сделать вывод, что все подключенные к сети устройства передают и принимают данные в одном и том же диапазоне частот. Среда передачи способна передавать только один сигнал в отдельный момент времени, и этот сигнал занимает весь диапазон. Другими словами среда передачи данных поддерживает режим моно полосной передачи.

Технология монополосной передачи использует только один канал для транспортировки всех данных. Поэтому:

- только одно устройство может передавать данные в отдельный момент времени;
- устройство может либо передавать, либо получать данные. Такой режим называется полудуплексным (half-duplex).

Полудуплексный и дуплексный режим

Полудуплексная сеть позволяет осуществлять передачу данных только одному устройству в данный момент времени – все остальные должны оставаться пассивными и прослушивать трафик на наличие адресованных им кадров.

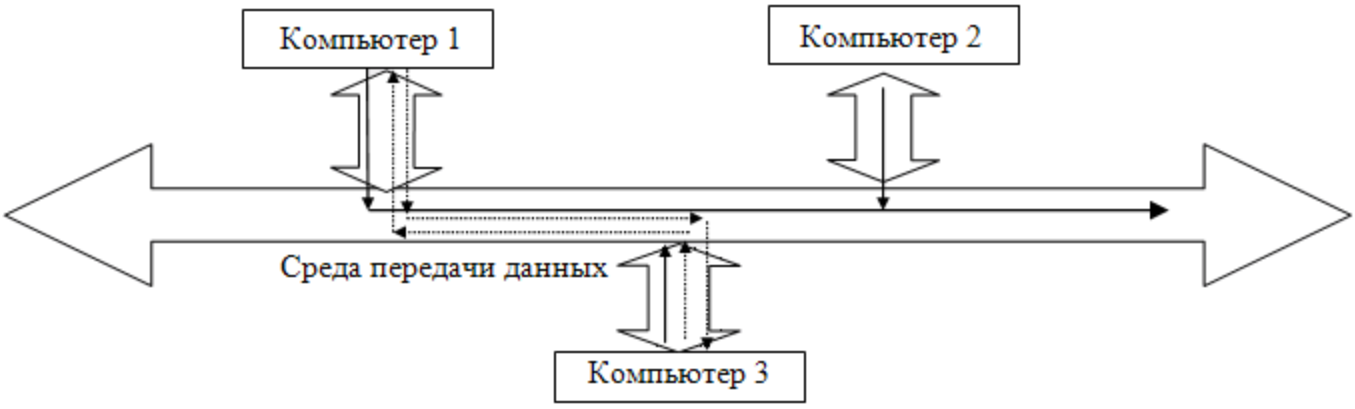


Рис. 5 Полудуплексная монопольная передача и дуплексная коммутируемая передача

В дуплексной (full-duplex) сети доступная полоса пропускания делиться на дискретные каналы. В альтернативном варианте физически разделенные проводники могут использоваться для создания избыточного канала, использующего тот же диапазон частот. В типичной дуплексной сети используется технология коммутации. В любом случае каждому устройству предоставляется в единицу времени как принимать, так и передавать данные.

Следует заметить, что полностью в дуплексной сети, предоставляющей доступ на основе конкуренции, только одно устройство в отдельном конфликтном домене имеет право передавать данные в определенный момент времени. Однако при развертывании дуплексной сети каждое устройство оказывается подключенным к коммутируемому порту. Таким образом, количество устройств в каждом конфликтном домене сокращается до двух: само устройство и коммутируемый порт, к которому оно подключено.

Синхронизация

Для синхронизации всех подключенных устройств кадры канального уровня должны быть определенным образом согласованы. Однако на практике длина этих кадров является переменной величиной.

Стандарт 802.3 CSMA/CD избегает конфликтов в сети Ethernet путем определения максимального и минимального размера кадра. Длина кадра должна составлять не менее 64 и не более 1524 октетов, включая полезные данные и заголовок. На любой известной скорости эти данные используются для непосредственного вычисления времени распространения стандартных кадров.

Вероятность возникновения конфликтов в сети повышается двумя факторами:

- количеством устройств, подключенных к сети;
- физическим размером сети.

Чем больше устройств подключено к сети, тем жестче конкуренция за доступную полосу пропускания. Количество подключаемых устройств можно увеличить, используя устройства сегментации, такие как мосты, маршрутизаторы и коммутаторы. Эти устройства уменьшают размер конкурирующего домена локальной сети.

Метод доступа с передачей маркера

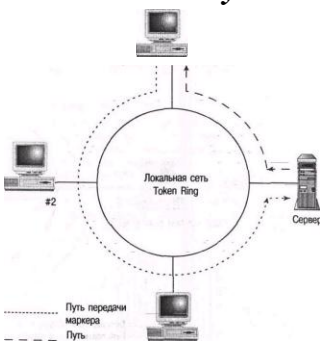


Рис. 6 Передача маркера

Передача маркера – это характерный признак локальных сетей кольцевой топологии. Примеры: Token Ring, FDDI.

Маркер – это специальный кадр, который последовательно передается от устройства к устройству в кольце. Этот кадр состоит всего из нескольких октетов и содержит специальную битовую маску, которую можно преобразовать в ограничительную последовательность начала кадра (SOF), уведомляющие расположенные «ниже по течению» сетевые устройства о прибытие кадра данных. Непосредственно за полем SOF следует пара адресов отправителя и получателя, указанных передающим устройством.

Маркер распознается всеми устройствами как разрешение на доступ к среде передачи данных. Если маркер передается устройству, которое не нуждается в передаче, оно имеет право задержать его в течении 10 миллисекунд или дольше, если значение по умолчанию не известно.

Это позволяет устройству завершить формирование кадра из данных, полученных от протоколов верхних уровней. Чтобы поместить кадр в сеть устройство должно обладать маркером. Если устройство не обладает маркером, оно должно ждать его получение от соседней станции.

Если за это время у устройства не появилось необходимость в передаче данных, оно освобождает маркер и передает следующему устройству в кольце. Обойдя все кольцо, маркер возвращается к своему отправителю. Обычно это происходит, после того как предполагаемый по-

лучатель скопировал себе данные кадра и изменил соответствующим образом битовую маску, сообщив эти об успешном приеме. Отправитель убеждается в успешной доставке содержания кадра, после чего-либо удерживает его в течение дозволенного времени и передает полномочия доступа к среде другому устройству, либо использует для транспортировки следующих данных.

Можно рассчитать максимальное время, по истечении которого устройство сможет возобновить передачу кадров. Для этого следует умножить максимальный интервал времени, в течение которого любой узел может удерживать маркер, на количество подключенных к кольцу устройств. К этому значению следует прибавить время, необходимое маркеру для обхода кольца. Хотя полученное значение не включает время операций ввода/вывода, время обработки, время перемещения головок дисковых накопителей и других задержек, оно представляет собой приемлемую оценку времени максимальной задержки сети.

Это суммарное время изменяется при добавлении или удалении узлов из кольца. Следовательно, сети с передачей маркера идеально подходят для приложений, требующих предсказуемой задержки.

Метод доступа с передачей маркера в сетях FDDI

В сетях FDDI используется несколько иная схема передачи маркера по сравнению с описанной в предыдущем разделе. Это различие едва уловимое, но важное. Вместо того, чтобы заставлять все станции ожидать, пока отправитель получит подтверждение доставки, технология FDDI использует механизм быстро освобождения, позволяющий другим устройствам начать передачу еще во время передачи предыдущего кадра. Механизм быстрого освобождения в действительности достаточно простой. Непосредственно после передачи кадра (который содержит маркер, модифицированный в SOF) передающее устройство передает следующий маркер. Таким образом, следующая в кольце станция для своей передачи не должна ждать, пока отправленный предыдущей станцией кадр данных обойдет все кольцо. В сети FDDI возможность доступа среде передачи данных предоставляется устройствам намного быстрее.

Преимущества быстрого освобождения контроля над передачей очевидны. Следующее в кольце устройство намного быстрее получает возможность передать свои данные. Это устройство может получить из кольца новый маркер и преобразовать его в ограничитель SOF еще до того, как первый кадр данных будет принят предполагаемым получателем.

Второе преимущество этой схемы заключается в значительном повышении эффективности сети. Следовательно, реальная пропускная способность сети с механизмом быстрого освобождения может, достигнут теоретической максимальной пропускной способности.

Доступ к среде по приоритету

Доступ к среде по приоритету (*Demand-Priority Access Method — DPAM*) используется в спецификаций VG-AnyLAN IEEE 802.12, обладающей пропускной способностью 100 Мбит/с. DPAM предполагает карусельный метод разрешения конфликтов, в соответствии с которым центральный повторитель (концентратор) регулярно опрашивает подключенные к нему порты. Этот опрос выполняется в определенном порядке с целью обнаружения портов, содержащих запросы на передачу. После обнаружения такого запроса повторитель определяет его приоритет (высокий или нормальный). Эти приоритеты позволяют обслуживать критичные ко времени запросы перед обычными запросами к полосе пропускания. Порты, которые не передают данные,

автоматически генерируют сигнал ожидания. Порты, которые либо находятся в режиме ожидания, либо по каким-то причинам отложили запросы на передачу.

Сигнал ожидания станции подавляется повторителем в том случае, если эта станция выбрана следующей в последовательности приоритетов передачи. Другими словами, повторитель определяет следующую станцию в своей последовательности приоритетов и дает ей указание прекратить генерацию сигнала ожидания. После исчезновения сигнала ожидания устройство начинает передачу собственно данных

Когда это происходит, повторитель предупреждает другие станции о том, что они могут получить входящее сообщение. Затем повторитель считывает адрес получателя входящего кадра, обращается к своей таблице конфигурации связей и коммутирует кадр на адрес необходимого получателя, а также на все порты, функционирующие в режиме приема всех сетевых пакетов (promiscuous port) Центральный или *корневой* (root) повторитель управляет работой области приоритетов которая может включать в себя до трех уровней последовательных концентраторов. Это позволяет соединенным между собой повторителям функционировать как один большой повторитель. Центральный повторитель передает весь трафик каждому повторителю нижнего уровня. Каждый повторитель нижнего уровня в свою очередь опрашивает свои активные порты на предмет запросов после передачи пакета.

Ни одна станция не может осуществить передачу данных два раза подряд в том случае, если есть отложенные запросы на передачу с таким же приоритетом от других станций. На центральном повторителе запрос с высоким приоритетом не может прервать запрос с нормальным приоритетом, который уже обрабатывается. На повторителе нижнего уровня запрос с нормальным приоритетом вытесняется для выполнения запроса с высоким приоритетом. Чтобы прерванный запрос не был полностью проигнорирован запросы с нормальным приоритетом, которые прождали обработки более 250 мс, автоматически переходя в статус высокого приоритета.

Этот метод доступа используется только в спецификации IEEE 802.12 для сетей с пропускной способностью 100 Мбит/с, использующих формат кадров Ethernet или Token Ring (но не оба одновременно) звездообразную топологию. Данная спецификация, известная под названием VG-AnyLAN (voice grade wiring, any *LAN architecture* - речевая проводка, любая архитектура локальной сети), может использовать четыре не экранированные витые пары категорий 3 и 5, экранированные витые пары и волоконно-оптический кабель.

При этом на расстоянии до 100 метров между повторителями и станциями может быть установлено до трех уровней повторителей. Диаметр сети может составлять до 1200 метров.

Контрольные вопросы

1. Какие существуют методы коммутации?
2. На какие классы делятся сети с коммутацией каналов и пакетов?
3. В чес заключается сущность методов коммутации?
4. Какие походы используются для управления доступом к среде?
5. В чес сущеность дуплексного и полудуплексного методов?

Лекция 7
Сетевые модели

1. **Эталонная модель OSI**
2. **Уровни эталонной модели OSI и их функции**
3. **Сетевая модель TCP/IP**
4. **Структура стека протоколов TCP/IP**
5. **Сравнение уровней моделей OSI и TCP/IP**

Ключивые слова: эталонная модель OSI, стек протоколов, семь уровней, internet-протокол, одноранговая связь, пакет, фрейм, сегмент, сетевая модель TCP/IP.

Изучить вопросы, связанные с функционированием сетей, легче, если начать с изучения первичных понятий и теоретических положений, а затем перейти к конкретным аспектам реализации сети. Изучение принципов работы сети на разных уровнях поможет понять, что происходит при передаче информации с одного компьютера на другой.

Использование уровней для анализа проблем передачи данных

Концепция использования уровней для анализа работы сети помогает лучше понять, что происходит при передаче информации от одного компьютера другому.

Процесс сетевой коммуникации достаточно сложен. Данные, передаваемые в форме электронных сигналов, должны пройти по передающей среде к требуемому компьютеру-получателю и вновь быть преобразованы в первоначальную форму для прочтения их получателем. Этот процесс включает в себя несколько этапов, поэтому наиболее эффективным способом реализовать сетевую коммуникацию является разделение процесса на различные уровни. В таком случае каждый уровень выполняет свои конкретные задачи независимо от других.

Использование уровней для описания процесса обмена данными в сети

Трудность реализации сетевого проекта состоит в том, что это достаточно сложный процесс. Он становится особенно трудным, если смотреть на него как на единое целое. Решение этой проблемы состоит в разделении всей системы сетевой коммуникации на ряд уровней. При этом каждый уровень отвечает за определенную часть процесса коммуникации и взаимодействует только с уровнем, находящимся непосредственно под ним, и с уровнем над ним. Такое взаимодействие строго определяет назначение каждого уровня. Двумя основными сетевыми моделями, использующими уровни, являются эталонная модель взаимодействия открытых систем (Open System Interconnection - OSI) и сетевая модель протоколов TCP/IP.

1. Эталонная модель OSI

Модель взаимодействия открытых систем была разработана Международной Организацией по Стандартизации (ISO) в 1984 году. В отличие от модели TCP/IP, она не описывает взаимодействий между отдельными протоколами. Она была создана в качестве базовой архитектуры, которую разработчики использовали для создания протоколов сетевого взаимодействия. Хотя в очень немногих стеках протоколов в точности реализованы все семь уровней модели взаимо-

действия открытых систем, на сегодня она считается эталонной моделью межкомпьютерных взаимодействий.

В модели OSI представлены все функции или задачи, ассоциированные с межсетевыми взаимодействиями, а не только с определенными протоколами TCP/IP. В отличие от модели TCP/IP, в которой представлено только четыре уровня, модель OSI организует задачи на семь более специфических групп.

Суть стека протоколов заключается в разделении и организации наиболее значимых функций. Разделение функций обеспечивает независимое функционирование каждого уровня в стеке. Например, доступ на веб-сайт возможен как с портативного компьютера, подключенного к домашнему модему, так и с портативного компьютера с помощью беспроводного или мобильного телефона с поддержкой функций беспроводного доступа. Нижние уровни не влияют на эффективность работы уровня приложения.

Точно так же нижние уровни не зависят от других уровней. Например, на скорость соединения с Интернет не влияет одновременный запуск нескольких приложений, например, электронная почта, просмотр веб-страниц, обмен мгновенными сообщениями и загрузка музыкальных файлов.

Использование упомянутой выше модели в качестве общего эталона облегчает решение вопросов, связанных с внесением изменений в сеть, а ее иерархическая структура позволяет подразделить проектирование сети на проектирование отдельных ее уровней. Эталонная модель OSI является основой проектирования и установки сетей, а ее уровни выполняют свои частные задачи при осуществлении обмена данными. Уровни 1-4 являются важнейшими для обеспечения работы сети. Эти четыре уровня выполняют следующие функции:

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

Эталонная модель OSI определяет сетевые функции, выполняемые каждым ее уровнем. Что еще более важно, она является базой для понимания того, как информация передается по сети. Кроме того, модель OSI описывает, каким образом информация или пакеты данных перемещается от программ-приложений (таких, как электронные таблицы или текстовые процессоры) по сетевой передающей среде (такой, как провода) к другим программам-приложениям, работающим на другом компьютере этой сети, даже если отправитель и получатель используют разные виды передающих сред.

Эталонная модель OSI содержит семь пронумерованных уровней, каждый из которых выполняет свои особые функции в сети (рис. 1).

Такое разделение выполняемых сетью функций называется *делением на уровни*.

Подразделение сети на семь уровней обеспечивает следующие преимущества:

- процесс сетевой коммуникации подразделяется на меньшие и более простые этапы;
- стандартизируются сетевые компоненты, что позволяет использовать и поддерживать в сети оборудование разных производителей;

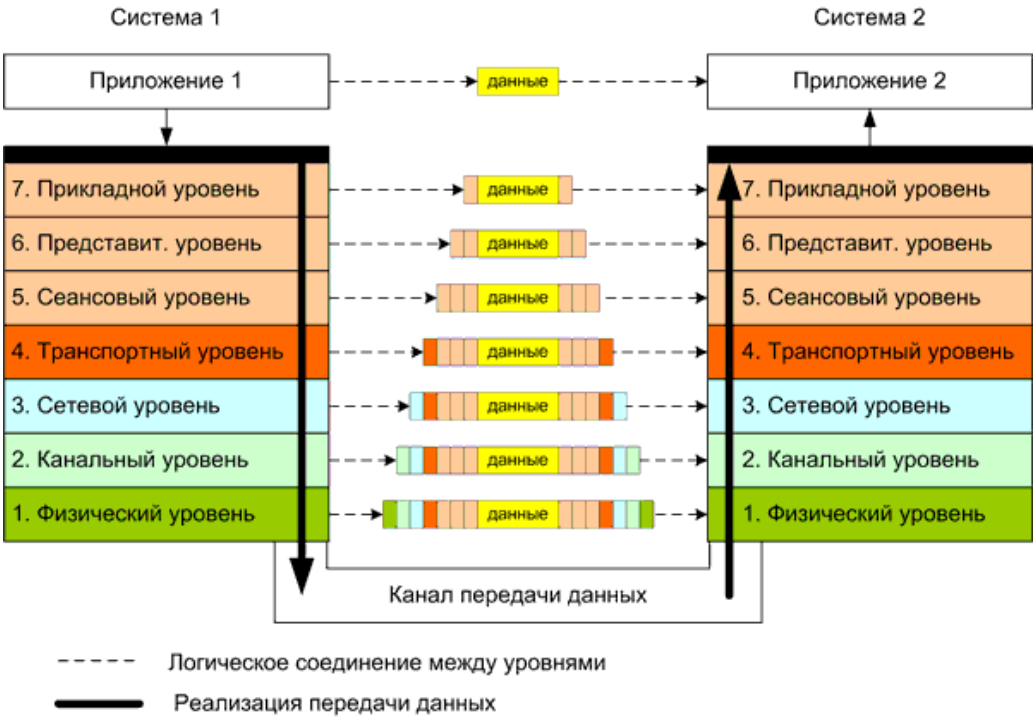


Рис. 1 Модель OSI

- подразделение процесса обмена данными на уровни позволяет осуществлять связь между различными типами аппаратного и программного обеспечения;
- изменения на одном уровне не влияют на функционирование других уровней, что позволяет быстрее разрабатывать новые программные и аппаратные продукты;
- коммуникация в сети подразделяется на компоненты меньшего размера, что облегчает их изучение.

Рассматривая перемещение информации по различным уровням эталонной модели OSI, читатель сможет понять, каким образом пакеты данных перемещаются по сети и какие устройства работают на каждом уровне. В конечном итоге знание функций и особенностей уровней поможет устранять проблемы, если таковые возникнут при передаче данных по сети.

2. Уровни эталонной модели OSI и их функции

Для передачи пакетов данных по сети от отправителя получателю каждый уровень модели OSI должен выполнить свой набор функций.

Уровень 7: уровень приложений

Уровень приложений (application layer) является ближайшим к пользователю и предоставляет службы его приложениям. От других уровней он отличается тем, что не предоставляет служб другим уровням; вместо этого он предоставляет службы только приложениям, которые находятся вне рамок эталонной модели OSI. Примерами таких приложений могут служить электронные таблицы (например, программа Excel) или текстовые процессоры (например, программа Word). Уровень приложений определяет доступность партнеров по сеансу связи друг для друга, а также синхронизирует связь и устанавливает соглашение о процедурах восстановления данных в случае ошибок и процедурах контроля целостности данных. Примерами приложений седьмого уровня могут служить протоколы Telnet и HTTP.

Уровень 6: уровень представления данных

Задача *уровня представления данных (presentation layer*) состоит в том, чтобы информация уровня приложений, которую посылает одна система (отправитель), могла быть прочитана уровнем приложений другой системы (получателя). При необходимости уровень представления преобразует данные в один из многочисленных существующих форматов, который поддерживается обеими системами. Другой важной задачей этого уровня является шифрование и расшифровка данных. Типовыми графическими стандартами шестого уровня являются стандарты PICT, TIFF и JPEG. Примерами стандартов шестого уровня эталонной модели, описывающих формат представления звука и видео, являются стандарты MIDI и MPEG.

Уровень 5: сеансовый уровень

Как показывает само название этого уровня, *сеансовый уровень (session layer*) устанавливает сеанс связи между двумя рабочими станциями, управляет им и разрывает его. Сеансовый уровень предоставляет свои службы уровню представления данных. Он также синхронизирует диалог между уровнями представления двух систем и управляет обменом данными. Кроме своей основной постоянной функции - управления, уровень сеанса связи обеспечивает эффективную передачу данных, требуемый класс обслуживания и рассылку экстренных сообщений о наличии проблем на сеансовом уровне, уровне представления данных или уровне приложений. Примерами протоколов пятого уровня могут служить сетевая файловая система (*Network File System - NFS*), система X-Window и протокол сеанса AppleTalk (*AppleTalk Session Protocol - ASP*).

Уровень 4: транспортный уровень

Транспортный уровень (transport layer) сегментирует данные передающей станции и вновь собирает их в одно целое на принимающей стороне. Границу между транспортным уровнем и уровнем сеанса связи можно рассматривать как границу между протоколами приложений и протоколами передачи данных. В то время как уровни приложений, представления данных и сеанса связи занимаются аспектами коммуникаций, которые связаны с работой приложений, нижние четыре уровня решают вопросы транспортировки данных по сети. Транспортный уровень пытается обеспечить службу передачи данных таким образом, чтобы скрыть от верхних уровней детали процесса передачи данных. В частности, задачей транспортного уровня является обеспечение надежности передачи данных между двумя рабочими станциями.

При обеспечении службы связи транспортный уровень устанавливает, поддерживает и соответствующим образом ликвидирует виртуальные каналы. Для обеспечения надежности транспортной службы используются выявление ошибок при передаче и управление информационными потоками. Примерами протоколов четвертого уровня могут служить протокол управления передачей (*Transmission Control Protocol - TCP*), протокол пользовательских дейтаграмм (*User Datagram Protocol - UDP*) и протокол последовательного обмена пакетами (*Sequenced Packet Exchange - SPX*).

Уровень 3: сетевой уровень

Сетевой уровень (network layer) является комплексным уровнем, обеспечивающим выбор маршрута и соединение между собой двух рабочих станций, которые могут быть расположены в географически удаленных друг от друга сетях. Кроме того, сетевой уровень решает вопросы логической адресации. Примерами протоколов третьего уровня могут служить Internet-протокол

(*IP*), протокол межсетевого пакетного обмена (*Internetwork Packet Exchange -IPX*) и протокол AppleTalk.

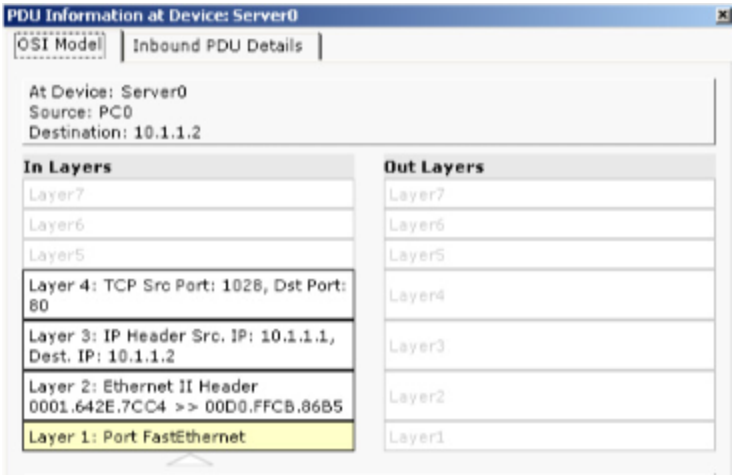
Уровень 2: канальный уровень

Канальный уровень (data link layer) обеспечивает надежную передачу данных по физическому каналу. При этом канальный уровень решает задачи физической (в противоположность логической) адресации, анализа сетевой топологии, доступа к сети, уведомления об ошибках, упорядоченной доставки фреймов и управления потоками.

Уровень 1: физический уровень

Физический уровень (*physical layer*) определяет электрические, процедурные и функциональные спецификации для активизации, поддержки и отключения физических каналов между конечными системами. Спецификациями физического уровня определяются уровни напряжений, синхронизация изменений напряжения, физическая скорость передачи данных, максимальная дальность передачи, физические соединения и другие аналогичные параметры.

В графическом интерфейсе программы трассировки пакетов (PT) можно просматривать эмулируемые данные, передаваемые между двумя узлами. В нем используются протокольные блоки данных (PDUs) для представления кадров трафика сети и отображения информации о стеках протоколов на соответствующих уровнях модели OSI.



Как видно из графика, запрос от веб-клиента принимается платой Ethernet NIC на веб-сервере. В модели взаимодействия открытых систем представлены следующие 4 уровня с 1 по 4.

Уровень 1 (Физический): порт Fast Ethernet

Уровень 2 (Канал передачи данных): адреса Ethernet Mac

Уровень 3 (Сеть): IP-адреса

Уровень 4 (Транспортный): номера портов TCP

Одноранговая связь

Для того чтобы передать пакеты данных от отправителя получателю, необходимо, чтобы каждый уровень модели OSI станции-отправителя вступил в связь с аналогичным уровнем получателя. Такая форма коммуникации называется *одноранговой связью (peer-to-peer communication)* (рис 3). Во время этого процесса протоколы одного и того же уровня обеих систем обмениваются информацией, называемой протокольными единицами обмена (Protocol Data Unit - PDU). Каждый уровень коммуникации компьютера-отправителя создает соответствующий ему модуль PDU и вступает в связь с одноименным уровнем компьютера-получателя.

Рис. 3. Одноранговая связь

Пакеты данных создаются станцией-отправителем, а затем передаются в пункт назначения. Функционирование каждого уровня зависит от службы, предоставляемой уровнем модели OSI, лежащим непосредственно под ним. Для предоставления такой службы нижний уровень использует инкапсуляцию, которая заключается в размещении модуля PDU находящегося над ним уровня в поле данных своего модуля PDU. После этого каждый уровень может добавить заголовки, которые требуются ему для выполнения своих функций. По мере того, как данные перемещаются по уровням модели OSI, к ним добавляются дополнительные заголовки. Модуль данных протокола (PDU) на четвертом уровне называется *сегментом (segment*).

Сетевой уровень предоставляет службы транспортному уровню. Он обеспечивает передачу данных по объединенной сети путем инкапсуляции данных транспортного уровня и добавления заголовка, в результате чего создается *пакет (packet*), являющийся модулем PDU третьего уровня. Заголовок пакета содержит информацию, требуемую для передачи пакета по сети, такую, в частности, как логические адреса отправителя и получателя. Канальный уровень предоставляет службу сетевому уровню. Он инкапсулирует информацию сетевого уровня во *фрейм (frame*), являющийся модулем PDU второго уровня. Заголовок фрейма содержит физический адрес, требуемый для выполнения канальным уровнем своих функций, а концевик (trailer) содержит контрольную последовательность фрейма (Frame Check Sequence - FCS), которая используется для проверки того, не был ли поврежден фрейм в процессе передачи. Получившийся модуль данных передается вниз, на физический уровень.

Физический уровень предоставляет службу канальному уровню. Физический уровень кодирует фрейм канального уровня, превращая его в последовательность нулей и единиц (в биты) для передачи по сетевой среде (обычно по медному проводу) на первом уровне.

Сетевые устройства, такие, как концентраторы, коммутаторы и маршрутизаторы, функционируют на трех нижних уровнях эталонной модели OSI. Концентраторы функционируют на первом уровне, коммутаторы - на втором, а маршрутизаторы - на третьем уровне модели OSI. Первым уровнем, который связан с процессом сквозной (end-to-end) передачи данных между конечными устройствами, является транспортный (четвертый).

3. Сетевая модель TCP/IP

Сеть Internet разрабатывалась как общая телекоммуникационная сеть, основная задача которой выстоять в случае войны. Несмотря на то, что эта сеть развивалась и продолжает развиваться совсем не так, как представляли себе ее создатели, сегодня она работает, как и многие годы назад, на основе стека протоколов TCP/IP. Структура и принцип построения протокола набора TCP/IP обеспечивает децентрализацию и уровень устойчивости, которые требуются от современных распределенных сетей, таких, например, как сеть Internet. Многие из использующихся сегодня протоколов были разработаны в рамках четырехуровневой модели TCP/IP.

История и развитие стека TCP/IP

Модель стека протоколов TCP/IP, которая схематически проиллюстрирована на рис.1, была разработана в процессе создания сети, способной сохранять работоспособность в любых условиях. Чтобы немного прояснить это, представим себе реальный мир с бесчисленным множеством возможных сетевых соединений - медных проводов, оптических кабелей, коротковолновых и спутниковых каналов. Предположим также, что данные непременно должны быть доставлены по назначению вне зависимости от состояния узлов, образующих сеть.

Решение этой непростой проблемы привело к созданию набора протоколов TCP/IP, впоследствии ставшего стандартом де-факто при построении сети Internet.

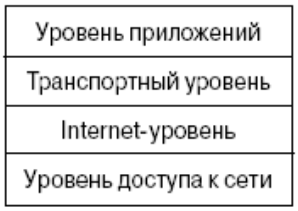


Рис. 1. Уровни стека протоколов TCP/IP

Модель TCP/IP состоит из четырех уровней: уровня приложений (access layer), транспортного уровня (transport layer), уровня Internet и уровня сетевого доступа (network access layer). Стоит отметить, что некоторые из них имеют те же названия, что и уровни в модели OSI.

Однако не следует путать назначения уровней в обеих моделях. Номера уровней в них различны, поэтому функции, выполняемые на втором уровне модели OSI, могут отличаться от функций того же уровня модели TCP/IP. Например, в модели OSI третий уровень соответствует протоколу IP, в то время как для модели TCP/IP протокол IP располагается на втором уровне. Еще один пример: протоколы TCP и UDP принадлежат четвертому уровню (транспортному) модели OSI и в то же время соответствуют третьему уровню (транспортному) в модели TCP/IP.

Структура стека протоколов TCP/IP

Базируясь на классификации OSI (Open System Integration) всю архитектуру протоколов семейства TCP/IP попробуем сопоставить с эталонной моделью (рис 2).

Прежде чем обсуждать эту схему, введем необходимую для этого терминологию.

- ***Драйвер*** - программа, непосредственно взаимодействующая с сетевым адаптером.
- ***Модуль*** - это программа, взаимодействующая с драйвером, с сетевыми прикладными программами или с другими модулями.
- ***Сетевой интерфейс*** - физическое устройство, подключающее компьютер к сети. В нашем случае - карта Ethernet.
- ***Кадр*** - это блок данных, который принимает/отправляет сетевой интерфейс.
- ***IP-пакет*** - это блок данных, которым обменивается модуль IP с сетевым интерфейсом.
- ***UDP-датаграмма*** - блок данных, которым обменивается модуль IP с модулем UDP.

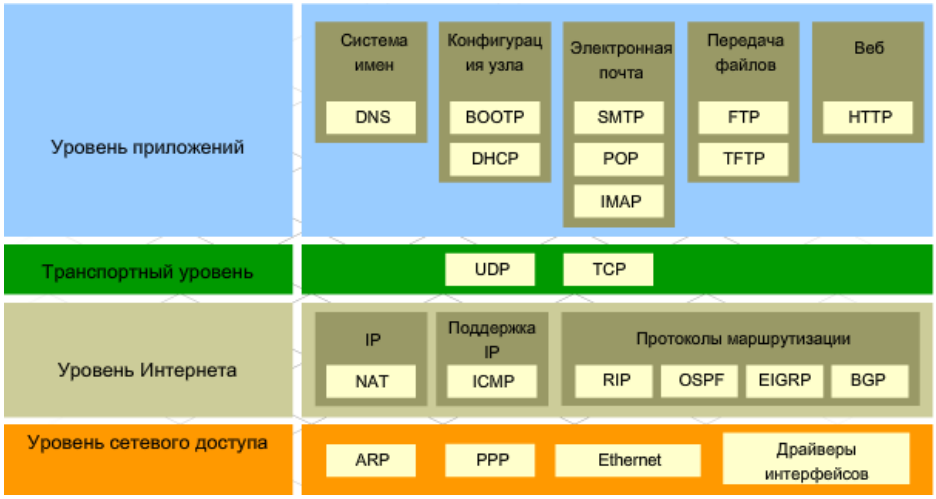


Рис 2. Структура стека протоколов TCP/IP

- ***TCP-сегмент*** - блок данных, которым обменивается модуль IP с модулем TCP.
- ***Прикладное сообщение*** - блок данных, которым обмениваются программы сетевых приложений с протоколами транспортного уровня.
- ***Инкапсуляция*** - способ упаковки данных в формате одного протокола в формат другого протокола. Например, упаковка IP-пакета в кадр Ethernet или TCP-сегмента в IP-пакет.

Вся схема называется стеком протоколов TCP/IP или просто стеком TCP/IP.

- ***TCP*** - **Transmission Control Protocol** - базовый транспортный протокол, давший название всему семейству протоколов TCP/IP.
- ***UDP*** - **User Datagram Protocol** - второй транспортный протокол семейства TCP/IP. Различия между TCP и UDP будут обсуждены позже.
- ***ARP*** - **Address Resolution Protocol** - протокол используется для определения соответствия IP-адресов и Ethernet-адресов.
- ***SLIP*** - **Serial Line Internet Protocol** (Протокол передачи данных по телефонным линиям).
- ***PPP*** - **Point to Point Protocol** (Протокол обмена данными «точка-точка»).
- ***FTP*** - **File Transfer Protocol** (Протокол обмена файлами).
- ***TELNET*** - протокол эмуляции виртуального терминала.
- ***RPC*** - **Remote Process Control** (Протокол управления удаленными процессами).
- ***TFTP*** - **Trivial File Transfer Protocol** (Тривиальный протокол передачи файлов).
- ***DNS*** - **Domain Name System** (Система доменных имен).
- ***RIP*** - **Routing Information Protocol** (Протокол маршрутизации).
- ***NFS*** - **Network File System** (Распределенная файловая система и система сетевой печати).

Все указанные выше значения прописываются в заголовке сообщения модулями на отправляющем компьютере. Так как схема протоколов - это дерево, то к его корню ведет только один путь, при прохождении которого каждый модуль добавляет свои данные в заголовок блока. Машина, принявшая пакет, осуществляет демультиплексирование в соответствии с этими отметками.

Уровень приложений

Модель TCP/IP включает протокол верхнего уровня, использующий сеансовый уровень (*session*), уровень представления (*presentation*) и уровень приложений (*application*) модели OSI. *Уровень приложений*, показанный на рис. 3, обслуживает протоколы верхних уровней и решает задачи представления, кодирования данных и контроля взаимодействия между конечными системами.

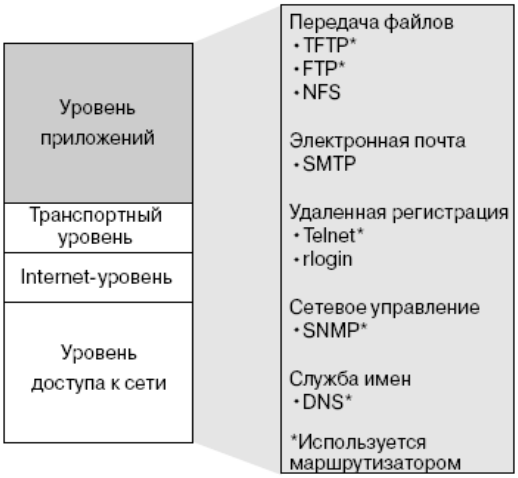


Рис. 3. Протоколы уровня приложений модели TCP/IP

Набор протоколов TCP/IP решает задачи, связанные с приложениями, и гарантирует, что данные будут надлежащим образом подготовлены для использования на следующем уровне. Стандарт TCP/IP описывает спецификации не только для средств Internet-уровня и транспортного уровня (например, таких, как протоколы IP и TCP), но также и правила разработки общих пользовательских приложений. В набор TCP/IP входят протоколы для передачи файлов, электронной почты и удаленной регистрации, а также приложения, перечисленные ниже.

1. Веб.

Протокол передачи гипертекстовых файлов (Hypertext Transfer Protocol - HTTP) это базовый протокол для работы Web-служб. Задает правила обмена в Интернете текстом, графическими изображениями, звуковыми, видео и другими файлами мультимедиа.

2. Передача файлов.

Простейший протокол передачи файлов (Trivial File Transfer Protocol - TFTP) - это простой протокол передачи данных без установления соединения. Это оптимальный протокол доставки файтов без подтверждения. Этот протокол бывает полезен в локальных сетях, поскольку в стабильных условиях работает быстрее, чем протокол FTP.

Протокол передачи файлов (File Transfer Protocol - FTP) - надежная служба, которая работает с установлением соединения. Он задает правила, которые позволяют пользователю на одном узле получить доступ к узлу в другой сети. Этот протокол обеспечивает двунаправленный обмен как бинарными файлами, так и файлами в тестовом формате.

Сетевая файловая система (Network File System - NFS) - набор протоколов распределенной файловой системы, позволяющий предоставлять удаленный доступ к файлам по сети.

3. Электронная почта

Простой протокол передачи электронной почты (Simple Mail Transfer Protocol - SMTP) - это служба, которая управляет передачей сообщений по электронной почте в компьютерных сетях и поддерживает передачу только текстовых данных.

Протокол почтового офиса версии 3 (POP3) – Позволяет клиентам получать электронную почту от почтового сервера. Поддерживает загрузку электронной почты с постового сервера на персональный компьютер.

Протокол доступа к Интернет-сообщениям (IMAP) – Позволяет клиентам получить доступ к электронной почте на почтовом сервере. Поддерживает электронную почту на сервере.

4. Конфигурация узла

Протокол загрузки (BOOTP) – Позволяет бездисковым рабочим станциям обнаруживать свой собственный IP-адрес, IP-адреса BOOTP-сервера в сети и загружать файл в память для запуска компьютера.

Протокол динамической конфигурации узлов (DHCP) – при запуске динамически назначает IP-адреса клиентским станциям. Позволяет повторно использовать адреса, которые больше не нужны.

5. Удаленная регистрация

Стандартный протокол виртуального терминала (telnet) - это служба, которая предоставляет удаленный доступ к компьютеру. Позволяет пользователям регистрироваться на Internet-узлах и выполнять команды операционной системы. Telnet-клиент называется локальным узлом, а Telnet-сервер - удаленным.

6. Сетевое управление

Простой протокол управления сетью (Simple Network Management Protocol - SNMP) - это протокол, предоставляющий средства мониторинга и контроля над сетевыми устройствами, механизмы управления конфигурацией, статистическими данными, производительностью и безопасностью.

7. Система имен

Служба доменных имен (Domain Name System - DNS) - это служба, используемая в сети Internet для преобразования доменных имен открытых сетевых узлов в IP-адреса.

Транспортный уровень

Рис. 4. Протоколы транспортного уровня модели TCP/IP

Транспортный уровень, как следует из его названия, предоставляет транспортные услуги от узла отправителя к узлу получателя. Он поддерживает логическое соединение между конечными точками сетевого маршрута. Транспортный протокол, который показан на рис. 4, сегментирует (т.е. разбивает на блоки) данные, отправленные приложениями верхнего уровня, формируя таким образом трафик между конечными узлами.

Поток данных транспортного уровня предоставляет сквозные транспортные услуги (т.е. из одного конца сети в другой) вдоль всего маршрута.

Поток данных транспортного уровня использует логическое соединение между передающим и принимающим узлами сети. При использовании протокола UDP основной задачей транспортного уровня является негарантированная доставка данных от отправителя получателю. Протокол транспортного уровня TCP гарантирует контроль над сквозной передачей благодаря применению метода скользящего окна с использованием последовательной нумерации и подтверждений. Транспортный уровень организует сквозную связь между приложениями, выполняемыми на удаленных системах. Транспортные механизмы, которые используют протокол

TCP, включают все из перечисленных ниже служб, в то время как приложения, использующие протокол UDP, предоставляют только первые две службы.

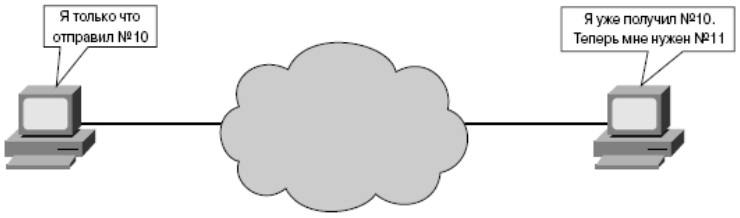


Рис. 5. Сетевая среда Internet

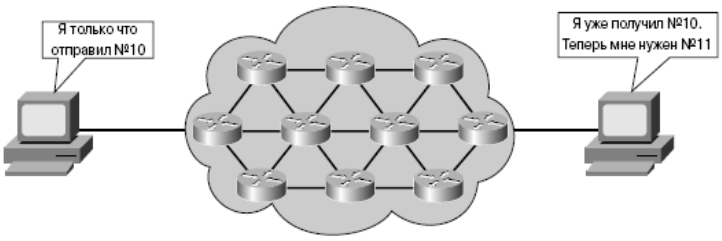


Рис. 6. Маршруты в сети Internet

Службы протокола TCP:

1. сегментация данных от приложений верхнего уровня;
2. передача сегментов от одного конечного устройства другому;
3. установление двунаправленного взаимодействия;
4. контроль потока с использованием метода скользящего окна;
5. гарантированная доставка, которая обеспечивается использованием последовательной нумерации и подтверждений.

Транспортный уровень предполагает, что он может использовать всю сеть как единую среду передачи, пересылая пакеты данных от отправителя конечному получателю, как это показано на рис. 5. Вопросы о том, какому из нескольких возможных маршрутов отдать предпочтение, для заданного получателя решаются на уровне сетевой среды (рис. 6).

Internet-уровень

В модели OSI сетевой уровень управляет сетевыми соединениями и освобождает протоколы более высоких уровней от необходимости непосредственного взаимодействия с физической инфраструктурой сети. Протокол IP обычно называют сетевым уровнем модели TCP/IP. Поскольку сетевой уровень стека TCP/IP в первую очередь отвечает за межсетевое взаимодействие, его часто называют *Internet-уровнем* модели TCP/IP (рис. 7). Протокол IP задействован во всех процессах взаимодействия верхних и нижних уровней, поскольку обычно они задействуют весь стек протоколов TCP/IP. Internet-уровень обеспечивает отправку пакетов сетевыми устройствами посредством соответствующего протокола. На этом уровне происходит выбор наилучшего маршрута и пересылка пакета.

Перечисленные ниже протоколы работают на Internet-уровне набора TCP/IP.

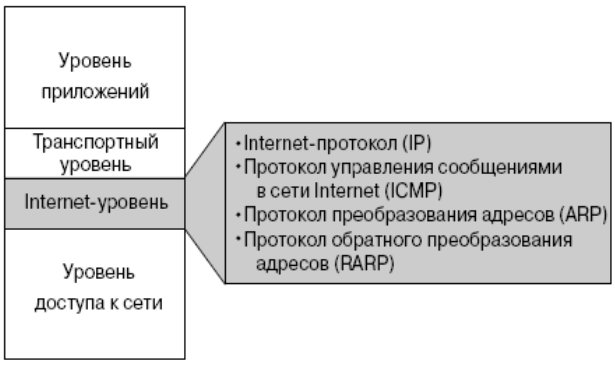


Рис. 7. Протоколы Internet-уровня

- **Протокол IP** — это протокол без установления соединения, обеспечивающий выбор наилучшего маршрута для доставки пакетов. Он не заботится о содержимом пакетов, а лишь находит наилучший способ направить пакеты в пункт назначения.
- **Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol - ICMP)** предоставляет функции контроля и управления сообщениями.

- **Протокол преобразования адресов (Address Resolution Protocol - ARP**) определяет адреса канального уровня (MAC-адреса) по известным IP-адресам.
- **Протокол обратного преобразования адресов (Reverse Address Resolution Protocol - RARP**) определяет IP-адреса для известных адресов канального уровня (т.е. MAC-адресов).

Протокол IP выполняет следующие функции:

1. определяет формат пакета и схему адресации;
2. осуществляет передачу данных от уровня Internet уровню доступа к сети;
3. осуществляет маршрутизацию к удаленным узлам.

И, наконец, следует пояснить, почему некоторые разработчики считают, что IP не является надежным протоколом. Это не означает, что протокол не гарантирует доставку данных; имеется ввиду, что протокол IP не осуществляет проверку данных и коррекцию ошибок. Обе функции выполняются на более высоких уровнях: транспортном и уровне приложений.

Уровень доступа к сети

Уровень доступа к сети (рис. 8) еще называют уровнем соединения узла и сети. Он «занимается вопросами», связанными с организацией физической связи между IP-пакетами и сетевой средой передачи данных. Этот уровень описывает методы построения локальных (Local Area Network - LAN) и распределенных (Wide Area Network - WAN) вычислительных сетей и соответствует физическому и канальному уровням модели OSI.

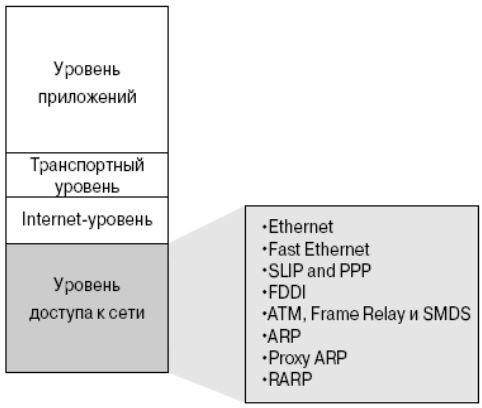


Рис. 8. Протоколы уровня сетевого доступа TCP/IP

Программное обеспечение и драйверы специфических устройств, таких, как, сетевые адаптеры (Network Interface Card - NIC) технологий Ethernet, Tocken Ring, ISDN и модемы, обычно работают именно на уровне сетевого доступа. Многие протоколы описываются другими стандартами и при этом фактически располагаются на рассматриваемом уровне, что часто приводит к путанице и недопониманию. Протоколы транспортного уровня и уровня Internet (протоколы IP, TCP и UDP) обычно сразу же ассоциируются с набором протоколов TCP/IP, а вот с привязкой протоколов уровня приложений (SMTP, HTTP и FTP) часто бывают проблемы.

К функциям уровня сетевого доступа относятся преобразование IP-адресов в аппаратные адреса и инкапсуляция IP-пакетов во фреймы (frames).

Уровень сетевого доступа отвечает за физическую связь со средой передачи данных для данного аппаратного типа сетевого интерфейса.

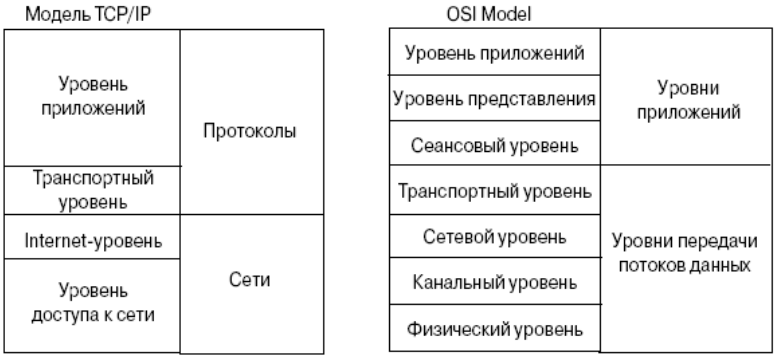
Хорошим примером настройки уровня сетевого доступа является установка драйверов сетевого адаптера для операционной системы Windows. Сетевой адаптер будет автоматически распознан операционной системой и, в зависимости от версии операционной системы Windows, будет установлен соответствующий драйвер. Если используется одна из старых версий операционной системы, то необходимо будет указать вручную местоположение драйвера сетевого адаптера.

5. Сравнение уровней моделей OSI и TCP/IP

На рис. 9 приведены модели OSI и TCP/IP для сравнения.

Следует обратить внимание, что модели имеют как сходства, так и отличия.

Сходства обеих моделей:



1. обе модели содержат уровни;
2. обе модели имеют уровень приложений, хотя в них входят разные службы;
3. обе модели имеют практически одинаковые транспортный и сетевой уровни;

Рис. 9. Сравнение модели OSI с моделью TCP/IP.

4. в обоих случаях подразумевается использование технологии коммутации пакетов (а не коммутации каналов);
5. профессионалы в области сетевых технологий обязаны знать обе модели.

Различия моделей OSI и TCP/IP:

1. в модели TCP/IP уровень представлений и сеансовый уровни объединены в один - уровень приложений TCP/IP;
2. в модели TCP/IP уровень канального доступа и физический уровень модели OSI объединены в один уровень сетевого доступа;
3. модель TCP/IP выглядит проще, поскольку содержит меньше уровней;
4. транспортный уровень модели TCP/IP, использующий протокол UDP, в отличие от транспортного уровня модели OSI, не гарантирует доставку пакетов.

Благодаря тому, что протоколы TCP/IP являются стандартами, по которым была создана сеть Internet, модель TCP/IP приобрела известную степень доверия. В большинстве случаев существующие сети построены не в строгом соответствии с эталонной моделью OSI; она служит лишь руководством для понимания коммуникационных процессов.

Контрольные вопросы

1. Для чего предназначены сетевые модели OSI и TCP/IP?
2. Какие уровни входят в модель OSI и каковы их функции?
3. Какие уровни входят в модель TCP/IP и каковы их функции?
4. Какие сходства и различия имеются в моделях OSI и TCP/IP?
5. Какои образом при помощи сетевых моделей происходит пересылка пакетов?

Лекция 8
Кабели компьютерных сетей

1. **Кабельный аспект LAN-сетей**
2. **Коаксиальный кабель**
3. **Витая пара**
4. **Оптоволоконные кабели**
5. **Беспроводные сети**

Ключивые слова: передающая среда, коаксиальный кабель, оптоволоконный кабель, экранированная витая пара, неэкранированная витая пара, разъем RJ-45, карта сетевого интерфейса, прямой кабель, перекрещенный кабель, многомодовое, одномодовое, светодиоды, лазеры, беспроводные сети, Wi-Fi.

1. Кабельный аспект LAN-сетей

Кабельный аспект LAN-сетей рассматривается на первом уровне эталонной модели взаимодействия открытых систем (Open System Interconnection - OSI). LAN-сети поддерживаются многими топологиями и физическими передающими средами.

На рис. 1 показано подмножество реализаций физического уровня, которые могут быть использованы для сети Ethernet.

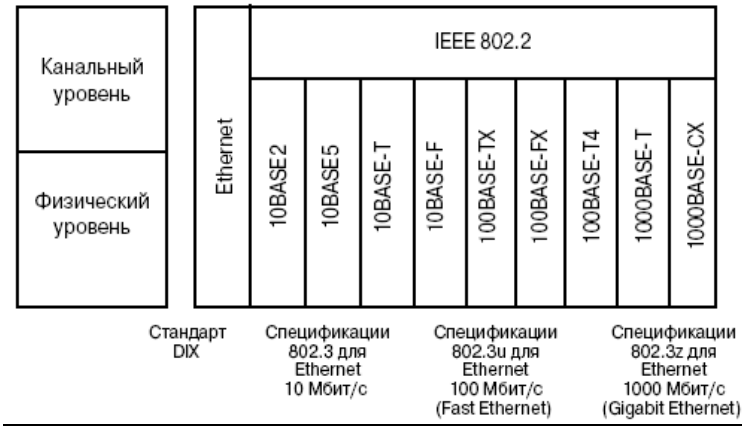


Рис. 1. Стандарты LAN-сетей на физическом уровне

Базовой функцией передающей среды является передача информации в форме битов или байтов по локальной сети LAN. За исключением беспроводных сетей LAN (в которых в качестве среды выступает атмосфера или пространство), в остальных видах сетевых сред сетевые сигналы заключены в проводе, кабеле или оптоволоконном кабеле. Сетевая передающая среда рассматривается как компонент первого уровня локальной сети.

Компьютерные сети могут быть построены с использованием различных передающих сред. Каждая сетевая среда имеет свои достоинства и недостатки. Показатель, который является достоинством для одной среды (например, невысокая стоимость у кабеля CAT5), может оказаться недостатком для другой (например, для дорогостоящего оптоволоконного кабеля). Первичными параметрами при оценке преимуществ и недостатков передающих сред являются следующие:

- максимально допустимая длина кабеля;
- стоимость;
- простота установки;
- подверженность интерференции.

Передавать сетевые сигналы могут коаксиальный кабель, оптоволоконный кабель и даже вакуум. Однако основной средой, является неэкранированный кабель витой пары 5-й категории

Существуют два типа медного кабеля: экранированный и неэкранированный.

У экранированных кабелей имеется защитная оболочка, которая защищает передаваемые сигналы данных от источников помех (также называемых наводками). Некоторые типы экранов защищают сигнал от внешних источников шума, другие защищают одну пару проводов в кабеле от шумов, порождаемых электрическими сигналами других пар проводов того же кабеля.

2. Коаксиальный кабель

Коаксиальный кабель является одной из разновидностей экранированного кабеля (рис. 2).

4 - оболочки (служит для изоляции и защиты от внешних воздействий) из светостабилизированного (то есть устойчивого к ультрафиолетовому излучению солнца) полиэтилена, поливинилхлорида, повива фторопластовой ленты или иного изоляционного материала;

3 - внешнего проводника (экрана) в виде оплетки, фольги, покрытой слоем алюминия пленки и их комбинаций, а также гофрированной трубки, повива металлических лент и др.;

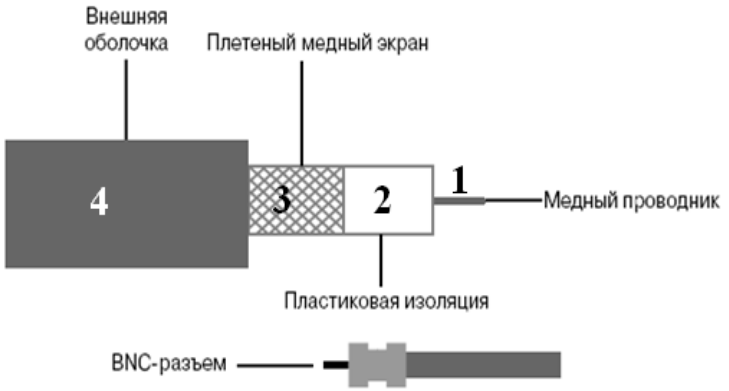


Рис. 2. Коаксиальный кабель

2 - изоляции, выполненной в виде сплошного (полиэтилен, вспененный полиэтилен, сплошной фторопласт, фторопластовая лента и т. п.) или полувоздушного (кордельно-трубчатый повив, шайбы и др.) диэлектрического заполнения, обеспечивающей постоянство взаимного расположения (соосность) внутреннего и внешнего проводников;

1 - внутреннего проводника в виде одиночного прямолинейного (как на рисунке) или свитого в спираль провода, многожильного провода, трубки, выполняемых из меди и т. п.

Категории

Кабели делятся по шкале Radio Guide. Наиболее распространённые категории кабеля:

RG-8 и RG-11 - «Толстый Ethernet» (Thicknet), 50 Ом. Стандарт 10BASE5;

RG-58 - «Тонкий Ethernet» (Thinnet), 50 Ом. Стандарт 10BASE2:

RG-58/U - сплошной центральный проводник,

RG-58A/U - многожильный центральный проводник,

RG-58C/U - военный кабель;

RG-59 - телевизионный кабель (Broadband/Cable Television), 75 Ом.;

RG-6 - телевизионный кабель (Broadband/Cable Television), 75 Ом. Кабель категории RG-6 имеет несколько разновидностей, которые характеризируют его тип и материал исполнения.;

RG-11- магистральный кабель. Этот вид кабеля можно использовать на расстояниях около 600 м.;

RG-62 - ARCNet, 93 Ом

«Толстый» Ethernet

Толстый - около 12 мм в диаметре. Плохо гнулся и имел значительную стоимость. Кроме того, при присоединении к компьютеру были некоторые сложности - использовались трансиверы AUI (Attachment Unit Interface), присоединённые к сетевой карте с помощью ответвления, пронизывающего кабель. За счёт более толстого проводника передачу данных можно было осуществлять на расстояние до 500 м со скоростью 10 Мбит/с.

«Тонкий» Ethernet

Был наиболее распространённым кабелем для построения локальных сетей. Диаметр примерно 6 мм и значительная гибкость позволяли ему быть проложенным практически в любых местах. Кабели соединялись друг с другом и с сетевой платой в компьютере при помощи Т-коннектора BNC (Bayonet Neill-Concelman). Между собой кабели могли соединяться с помощью I-коннектора BNC (прямое соединение). На обоих концах сегмента должны быть установлены терминаторы. Поддерживает передачу данных до 10 Мбит/с на расстояние до 185 м.

3. Витая пара

Кроме коаксиального кабеля, широко используются два типа кабелей на основе витой пары:

- экранированная витая пара (Shielded Twisted Pair -STP) (рис. 3);
- неэкранированная витая пара (Unshielded Twisted Pair - UTP) (рис. 4).

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

- неэкранированная витая пара (англ. UTP — Unshielded twisted pair) — без защитного экрана;
- фольгированная витая пара (англ. FTP - Foiled twisted pair), также известна как F/UTP) - присутствует один общий внешний экран в виде фольги;
- экранированная витая пара (англ. STP - Shielded twisted pair) — присутствует защита в виде экрана для каждой пары и общий внешний экран в виде сетки;
- фольгированная экранированная витая пара (англ. S/FTP - Screened Foiled twisted pair) - внешний экран из медной оплетки и каждая пара в фольгированной оплетке;
- незащищенная экранированая витая пара (SF/UTP - или с англ. Screened Foiled Unshielded twisted pair).Отличие от других типов витых пар заключается в наличии двойного внешнего экрана, сделанного из медной оплётки, а так же фольги.

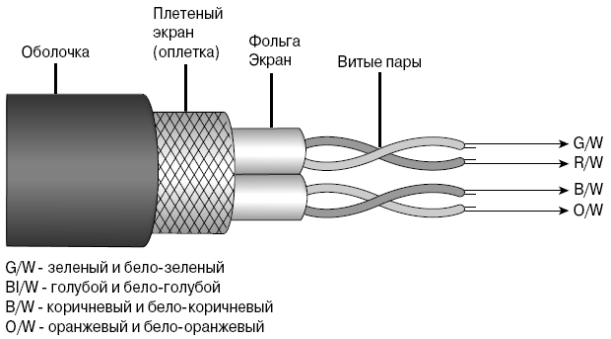


Рис. 3. Экранированный кабель на основе витой пары

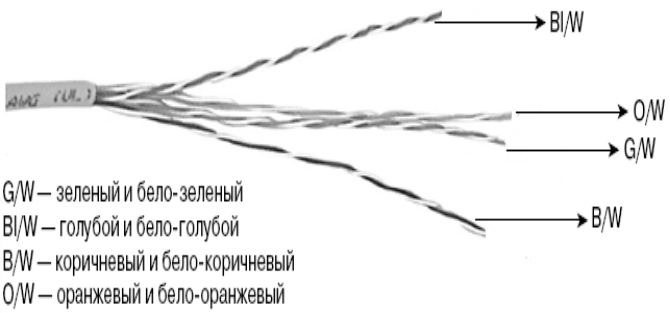


Рис. 4. Неэкранированный кабель на основе витой пары

Экранирование обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних и т. д. Экран по всей длине соединен с неизолированным дренажным проводом, который объединяет экран в случае разделения на секции при излишнем изгибе или растяжении кабеля.

Категории кабеля витая пара

Существует несколько категорий кабеля витая пара, которые нумеруются от CAT1 до CAT7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины.

CAT1 (полоса частот 0,1 МГц) — телефонный кабель, всего одна пара. Используется только для передачи голоса или данных при помощи модема.

CAT2 (полоса частот 1 МГц) — старый тип кабеля, 2 пары проводников, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях Token ring и Arcnet. Сейчас иногда встречается в телефонных сетях.

CAT3 (полоса частот 16 МГц) — 4-парный кабель, используется при построении телефонных и локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с по технологии 100BASE-T4 на расстоянии не дальше 100 метров. Отвечает требованиям стандарта Eternet.

CAT4 (полоса частот 20 МГц) — кабель состоит из 4 скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре, сейчас не используется.

CAT5 (полоса частот 100 МГц) — 4-парный кабель, использовался при построении локальных сетей 100BASE-TX и для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар.

CAT5e (полоса частот 125 МГц) — 4-парный кабель, усовершенствованная категория 5. Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель обеспечивает скорость передач данных до 100 Мбит/с.

CAT6 (полоса частот 250 МГц) — применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с и до 10 гигабит на расстояние до 50 м. Добавлен в стандарт в июне 2002 года.

CAT6a (полоса частот 500 МГц) — применяется в сетях Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 10 Гбит/с и планируется использовать его для приложений, работающих на скорости до 40 Гбит/с. Добавлен в стандарт в феврале 2008 года.

CAT7 — спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных до 10 Гбит/с, частота пропускаемого сигнала до 600—700 МГц. Кабель этой категории имеет общий экран и экраны вокруг каждой пары. Седьмая категория, строго говоря, не UTP, а S/FTP (Screened Fully Shielded Twisted Pair).

CAT7a (полоса частот выше сорока тысяч МГц)

Причиной проблем с передачей данных может быть не только некачественный кабель, но также наличие «скруток» в кабеле и использование розеток более низкой категории, чем кабель.

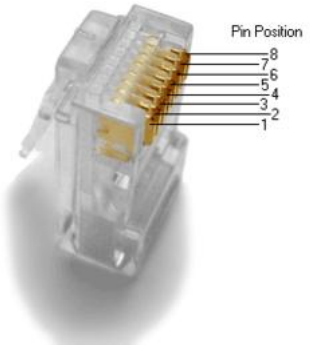


Рис 5. Нумерация в штекере 8P8C

Кабель подключается к сетевым устройствам при помощи разъёма 8P8C, который часто неверно называют RJ45 (рис. 5).

Схемы обжима

Стандарт Ethernet определяет, что каждый из контактов разъема RJ-45 имеет свое назначение, как показано на рис. 6. Карта сетевого интерфейса (Network Interface Card - NIC) передает сигналы по контактам 1 и 2, а получает сигналы на контактах 3 и 6. Провода кабеля UTP должны быть соединены с соответствующими контактами на каждом конце кабеля. Проверка соответствия проводов и контактов разъемов обеспечивает отсутствие в кабеле незамкнутых цепей или цепей короткого замыкания.

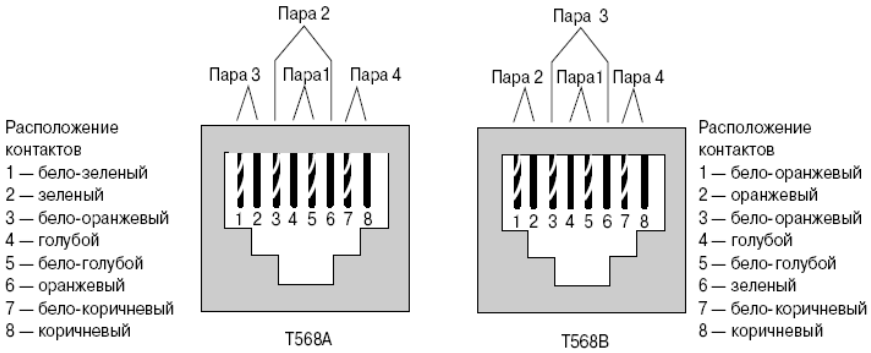


Рис. 6. Стандарты Ethernet для разъемов RJ-45

Требования к среде Ethernet и разъемам

Категории кабелей для сетей Ethernet определяются стандартами EIA/TIA-568 (SP-2840) на провода для кабелей промышленных коммерческих телекоммуникаций. Ассоциации EIA/TIA определяют для кабелей UTP использование разъема *RJ-45*. Аббревиатура *RJ* означает *registered jack (зарегистрированный разъем)*, а число 45 относится к модели физического разъема, имеющего восемь проводников.

На рис.7 показаны различные типы соединений, используемых при реализации физического уровня.

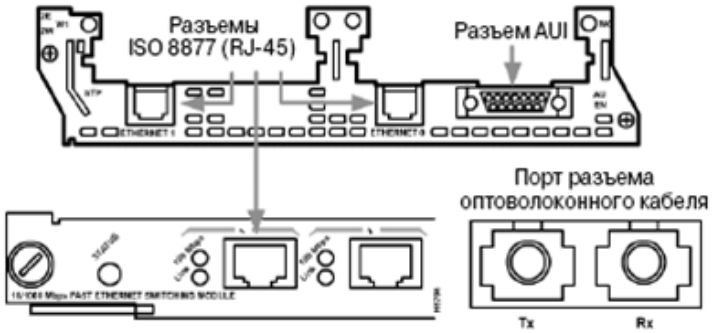


Рис. 7. Различные типы разъемов

Кабель UTP и его установка

Если посмотреть на прозрачный штекер RJ-45 на конце кабеля UTP, то можно увидеть восемь цветных проводов. Эти провода скручены в четыре пары. На четыре провода (две пары)

подается положительное (или настоящее) напряжение; это сигнальные провода («tip», от T1 до T4); остальные четыре (от R1 до R4) заземлены и передают инверсное (или фиктивное) напряжение и называются нулевым уровнем («ring»). Эти два провода в первой проводной паре кабеля или гнезда обозначаются как T1 и R1, во второй паре - как T2 и R2, и т.д.

Разъем RJ-45 запрессован на конце кабеля и является внешней частью разъема. Если посмотреть на него с лицевой части (т.е. когда зажим направлен вниз), то контакты нумеруются от 8 до 1 слева направо, как показано на рис. 8. Гнездо, показанное на рис.9, представляет собой внутренний (female) компонент разъема и встраивается в сетевое устройство, стену, в напольную розетку или в распределительную панель.

Для того чтобы токи в разъеме проходили в правильном направлении, порядок проводов в штекере и гнезде должен соответствовать стандартам EIA/TIA-568-A и EIA/TIA-568-B.

Рис. 8. Расположение контактов в разъеме RJ-45

Кроме правильного выбора кабеля соответствующей категории EIA/TIA для соединения устройств (что определяется стандартом распайки, используемым в разъеме), необходимо также определить, какой из приведенных ниже двух типов кабелей будет использоваться:

- *прямой кабель (straightthrough*), в котором порядок контактов остается неизменным по всей длине кабеля, и таким образом контакт 1 остается одним и тем же на обоих концах кабеля;
- *перекрещенный кабель (crossover*), в котором контакты в каждой паре на конце кабеля инвертируются (меняются местами) для передачи и приема сигналов в требуемом порядке

Если расположить рядом два конца кабеля с разъемами RJ-45, то в каждом из них видны цветные провода (или контакты). Если порядок цветных проводов на каждом конце один и тот же, то такой кабель называется прямым (straight through). На рис. 9 показано, что порядок проводов обоих разъемов одинаков.

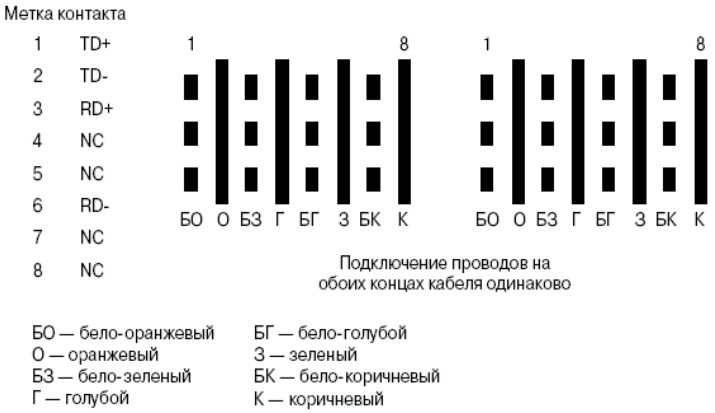


Рис. 9. Прямой кабель UTP

Согласно спецификации Ethernet, в кабеле UTP категории 5 для передачи сигналов (TD) и приема (RD) используются только провода 1, 2, 3 и 6. Остальные четыре провода не используются. Как показано на рис. 9, в прямом кабеле RJ-45 контакты 1, 2, 3 и 6 на одном конце соединения соединены с контактами 1, 2, 3 и 6 на другом конце. Однако в технологии Gigabit Ethernet используются все восемь проводов.

Прямой кабель может быть использован для соединения между собой таких устройств, как PC или маршрутизаторы, с другими устройствами, такими, как концентраторы или коммутаторы.

При использовании перекрещенного кабеля по разъемам RJ-45 на двух концах кабеля можно обнаружить, что некоторые контакты одного конца кабеля на другом конце кабеля подсоединены к иным контактам. В частности, для сетей Ethernet контакт 1 на одном конце кабеля RJ-45 на другом конце подсоединен к контакту 3, а контакт 2 -к контакту 6, как показано на рис. 10.

Перекрещенный кабель может быть использован для соединения между собой «одинаковых» устройств, например, коммутатора с другим коммутатором или коммутатора с концентратором.

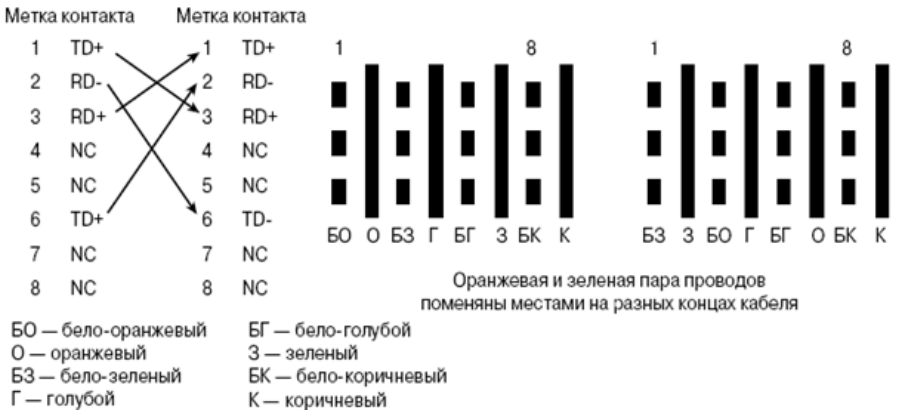


Рис. 10. Перекрещенный кабель UTP

Ниже приводятся рекомендации по выбору типа кабеля для соединения между собой сетевых устройств.

Прямой кабель следует использовать для соединения:

- коммутаторов с маршрутизаторами;
- коммутаторов с ПК или серверами;
- концентраторов с ПК или серверами.

Инвертированный кабель следует использовать для соединения:

- коммутаторов с коммутаторами;
- коммутаторов с концентраторами;
- концентраторов с концентраторами;
- маршрутизаторов с маршрутизаторами;
- ПК с ПК;
- маршрутизаторов с ПК.

4. Оптоволоконные кабели

Оптоволоконные кабели — это сетевая среда передачи, в которой используются световые импульсы для передачи данных. Сигналы, которые представляют собой биты данных, преобразовываются в световые импульсы.

Конструкция

Оптическое волокно, как правило, имеет круглое сечение и состоит из двух частей - сердцевины и оболочки.

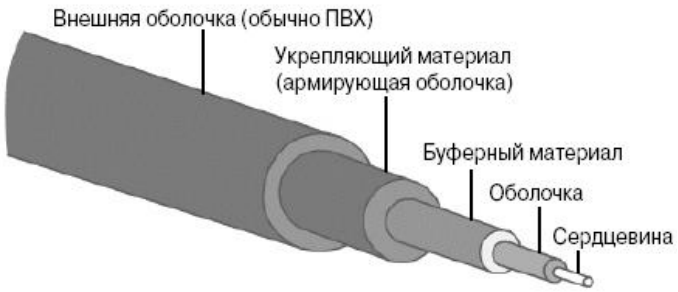


Рис. 11. Пять типичных компонентов оптоволоконного кабеля

Как показано на рис. 11, существуют пять типичных компонентов, из которых состоит:

- оптоволоконный кабель:
- сердцевина;
- оболочка;
- буферный материал;
- армирующий материал;
- внешняя оболочка.

Средой передачи сигналов в оптическом волокне служит сердцевина, которая расположена в центре волокна и переносит все световые импульсы. Сердцевину обычно изготавливают из кварца (диоксида кремния) или других подобных по характеристикам материалов. Сердцевина покрыта оболочкой, которая также состоит из кварца, но имеет меньшее значение коэффициента преломления, чем сердцевина. Лучи света, распространяющиеся в сердцевине волокна, отражаются от границы сердцевина-оболочка обратно в сердцевину и продолжают свой путь внутри нее.

Оболочку окружает буферный материал, который предохраняет сердцевину и оболочку от физических повреждений. Армирующий материал, окружающий буфер, предохраняет кабель от растяжений и разломов во время его прокладки. Материал, из которого изготавливают этот слой, называется кевларом.

Последний элемент - внешняя оболочка - защищает оптическое волокно от стирания, растворения и загрязнения. Состав вещества, из которого изготовлена внешняя оболочка, может изменяться в зависимости от предназначения оптоволоконного кабеля.

Часть оптического волокна, по которой распространяются световые лучи, называют *сердцевиной* оптического волокна. Световые лучи не могут входить в сердцевину под любыми углами, а только под углами, которые лежат в пределах числовой апертуры оптического волокна. Более того, для входящего светового луча в оптическом волокне существует ограниченное количество путей распространения. Такие оптические пути называются модами. Если диаметр сердцевины достаточно большой, в нем может существовать большое количество путей для распространения световых лучей; такое оптическое волокно называют *многомодовым*. В *одномодовом* оптическом волокне диаметр сердцевины настолько мал, что позволяет использовать только один путь (одну моду) для распространения светового луча (рис 12).

Для передачи сигналов по многомодовому кабелю применяются светодиоды, а для передачи информации по одномодовому кабелю – лазеры. С помощью светодиодного излучателя невозможно получить однородный сигнал и точно направить его внутрь светопроводящей жилы, поэтому при распространении сигнала по многомодовому кабелю приходится учитывать не только затухание, но и дисперсию сигнала. Лазерные же источники света по своей природе когерентны, т.е. излучают одну длину волны, поэтому на дальность распространения сигнала по одномодовому кабелю влияет только величина затухания.

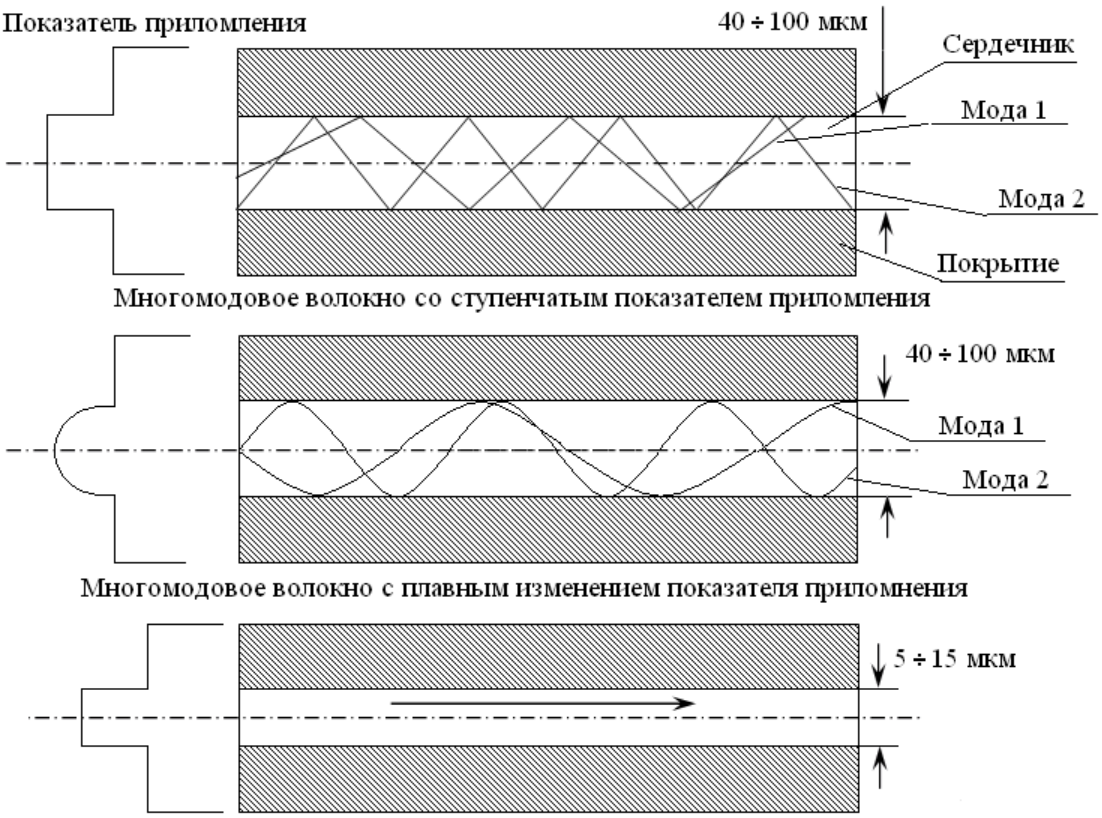


Рис.12. Типы оптического кабеля

Любой оптоволоконный кабель, использующийся для сетевых соединений, содержит два оптических волокна, каждое из которых имеет свою оболочку. Одно волокно переносит сигнал от устройства А к устройству Б, а второе волокно - в обратном направлении, от устройства Б к устройству А. Такой механизм передачи данных позволяет создать дуплексное коммуникационное соединение. Аналогично витой паре, которая использует разные пары проводников для передачи данных (Tx - передача) и для приема (Rx - прием), в оптоволоконном кабеле одно волокно используется для передачи, а второе - для приема данных, как показано на рис. 13. Обычно такие два волокна находятся в единой внешней оболочке, кроме тех точек, где к ним крепятся соединительные разъемы.

Рис. 13. Дуплексное оптическое волокно

На рис. 14 проиллюстрированы относительные размеры сердцевины и оболочки всех рассмотренных выше разновидностей оптического волокна в разрезе. Самая малая и тонкая сердцевина устанавливается в одномодовом оптическом волокне, что приводит к высокой стоимости его изготовления, но это оправдывается высокой пропускной способностью и бо́льшим максимальным расстоянием, на которое можно передавать данные, чем у многомодового волокна.

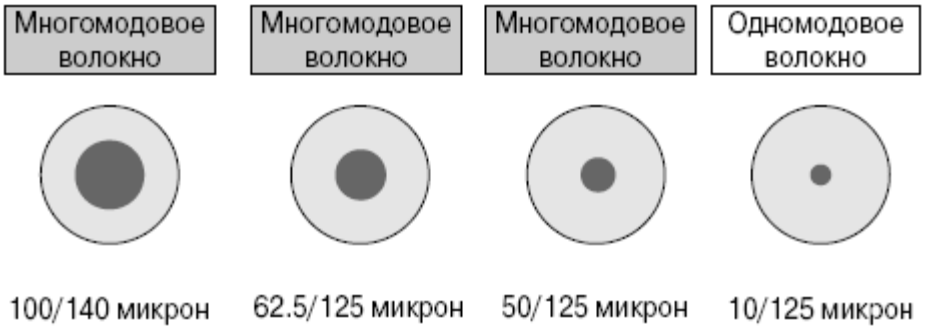


Рис. 14. Одномодовое и многомодовое оптические волокна

Основные характеристики оптических кабелей:

- **пропускная способность** составляет более 1 Гбит/с;
- **средняя стоимость узла** высока;
- **размеры кабеля и разъема для соединения** малы;
- **максимальная длина кабеля** - более 10 км для одномодового, до 2-х км – для многомодового.

Другие оптические сетевые компоненты

Большинство данных, передаваемых по локальным сетям, представляет собой электрические сигналы. Оптические же соединения используют световые импульсы для передачи данных, поэтому необходимы устройства, которые будут преобразовывать электрические сигналы в световые на одном конце кабеля и световые в электрические - на другом его конце. В такой схеме как минимум должны присутствовать два устройства: передатчик и приемник.

Передатчики

Передатчики получают данные, которые необходимо передать далее, от маршрутизаторов и коммутаторов в виде электрических сигналов. Передатчик преобразовывает электрические сигналы в эквивалентные им импульсы света. Существуют два типа источников света, которые преобразовывают и передают данные по оптическим кабелям:

- **светодиоды (Light_Emitting Diode - LED)** способны создавать инфракрасное излучение с длиной волны 850 либо 1310 нм. Излучение на таких длинах волн используется для передачи данных по многомодовым оптическим волокнам в локальных сетях. Для фокусировки и передачи светового потока в сердцевину используются линзы;
- **лазеры (Laser - Light Amplification by Stimulated Emission of Radiation)** способны создавать тонкий интенсивный луч инфракрасного излучения с длиной волны 1310 либо 1550 нм. Лазеры используются совместно с одномодовым оптическим волокном для создания соединений на больших расстояниях, обычно встречающихся в распределенных сетях (WAN), либо для построения опорной территориальной сети. С лазерами необходимо обращаться осторожно, чтобы не повредить глаза.

Каждый из источников света может очень быстро включаться и выключаться и обеспечивает формирование единиц и нулей с высокой частотой.

Приемники

На противоположном от передатчика конце оптического волокна должен находиться приемник. Его функция очень похожа на ту, которую выполняют фотоэлементы в калькуляторе с

солнечными батареями. Когда свет попадает на его поверхность, он должен вырабатывать электрический ток. Первоочередная функция приемника заключается в регистрации импульсов света, которые приходят по оптическому волокну. Приемник преобразовывает световые импульсы обратно в электрический сигнал, который был получен передатчиком на другом конце волокна для передачи. Теперь сигнал снова присутствует в форме электрических импульсов и готов к передаче через медные проводники к любым электронным устройствам приема, таким, как компьютер, коммутатор и маршрутизатор. Полупроводниковые устройства, которые обычно используются в приемниках с оптоволоконными каналами, называются p-i-n диодами (PIN-фотодиодами).

PIN-фотодиоды чувствительны к определенной длине световой волны (850, 1310 либо 1550 нм), которую передатчик генерирует на другом конце кабеля. Если на такой светодиод попадает световой луч с соответствующей длиной волны, он начинает вырабатывать электрический ток для сети. Электрический ток исчезает сразу же после того, как пропадает световой луч, падающий на полупроводниковый фотодиод.

Такой процесс вызывает появление электрического тока в цепи, которое представляет собой единицы и нули данных в медных проводниках.

Разъемы

Для подсоединения оптоволоконных кабелей к передатчикам и приемникам используются специальные разъемы, которые закрепляются на концах оптических волокон. Наиболее распространенным разъемом для многомодового оптического волокна является пользовательский разъем (Subscriber Connector - SC); его внешний вид показан на рис. 15. Для одномодовых оптоволоконных линий чаще используется разъем с прямым наконечником (Straight Tip - ST), который показан на рис. 16. По одному SC- или ST-разъему нужно устанавливать на каждое волокно. Самые новые модификации разъемов совмещают в себе передающее и принимающее оптические волокна для экономии места и по своей величине сравнимы с разъемом RJ-45.

Рис. 15. Разъем SC

Рис. 16. Разъем ST

5. Беспроводные сети

Беспроводные системы используют электромагнитные волны, которые могут распространяться в космическом вакууме или через некоторые среды передачи данных, такие, как воздух. Для беспроводных систем не нужна физическая медная либо оптическая среда передачи данных, вследствие чего беспроводное взаимодействие является универсальным методом построения сетей. Беспроводная передача может быть осуществлена на большие расстояния при использовании высоких несущих частот.

Структура и стандарты беспроводных сетей

В качестве основной технологии, которая описана в стандарте 802.11, выступает технология DSSS. Беспроводные устройства, работающие на скоростях от 1 до 2 Мбит/с, используют технологию DSSS, которая теоретически может обеспечить максимальную скорость передачи

данных вплоть до 11 Мбит/с, но, тем не менее, обычно ее не используют для получения скоростей выше 2 Мбит/с. Следующий (т.е. более новый) стандарт 802.11b позволяет увеличить скорость передачи данных до 11 Мбит/с. Несмотря на то, что теоретически технологии DSSS и FHSS могут использоваться в одной беспроводной сети, на практике возникают проблемы совместимости между устройствами различных производителей, поэтому Институт IEEE создал ряд стандартов, отвечающих запросам производителей.

Стандарт IEEE 802.11b носит название Wi-Fi (высокоскоростные беспроводные сети) и описывает взаимодействие устройств с использованием технологии DSSS на скоростях 1, 2, 5,5 и 11 Мбит/с. Все устройства, соответствующие стандарту 802.11b, совместимы с устройствами, отвечающими стандарту 802.11 и использующими систему DSSS. Такая совместимость очень важна, поскольку позволяет модернизировать беспроводную сеть без замены всех сетевых плат и точек доступа.

Устройства, соответствующие стандарту 802.11b, позволяют достигать более высоких скоростей передачи данных Большинство устройств, соответствующих стандарту 802.11b, не достигают пропускной способности в 10 Мбит/с, реальная скорость передачи данных обычно находится в пределах 2-4 Мбит/с.

Устройства и структуры беспроводных сетей

Наименьшее количество устройств, из которых может состоять беспроводная сеть, - это два устройства с беспроводными сетевыми адаптерами. Беспроводные устройства могут быть установлены как в настольные, так и в портативные или карманные компьютеры.

Оборудованные адаптерами беспроводной связи, они создают *сеть сопряженных устройств*, которая очень схожа с одноранговой кабельной сетью. Оба устройства в такой среде работают и как сервер, и как клиент. Несомненно, такая конфигурация позволяет объединить несколько устройств и установить между ними связь.

Наиболее часто для доступа отдельных устройств к беспроводной сети в сеть помещают точку доступа (*Access Point - AP*), которая выступает в роли концентратора для беспроводных устройств. Точка доступа подключена к кабельной сети и предоставляет беспроводным устройствам доступ к остальной сети, обеспечивает подключение к сети Internet. Точка доступа комплектуется антенной, которая предоставляет возможность доступа беспроводным устройствам к сети в некой области (называемой областью покрытия); такая область называется *ячейкой*.

В зависимости от типа помещения, в котором установлена точка доступа, размеры одной ячейки могут колебаться от нескольких десятков метров до десятков километров. В большинстве случаев размер ячейки составляет от 90 до 150 метров. Для создания беспроводной сети в более широких пределах необходимо установить несколько точек доступа с перекрывающимися ячейками, а также разрешить *роуминг (roaming*) между ячейками, как показано на рис. 17.

Перекрытие отдельных ячеек очень важно, т.к. позволяет беспроводному устройству свободно перемещаться без потери соединения в пределах беспроводной локальной компьютерной сети. Рекомендуемый процент перекрытия ячеек должен составлять около 20-30. Такое перекрытие позволяет осуществлять процедуру роуминга, позволяя при этом устройству отсоединяться от одной точки доступа и соединяться со второй без потери соединения с беспроводной сетью.

Если устройство-клиент было включено в пределах беспроводной локальной сети, оно прослушивает эфир для нахождения совместимых устройств, с которыми можно было бы соединиться. Такой процесс называют *сканированием*. Процесс сканирования может быть как пассивным, так и активным.

В активном режиме сканирования устройство посылает зондирующие запросы, с помощью которых пытается найти совместимое устройство и использовать его для подключения к сети.

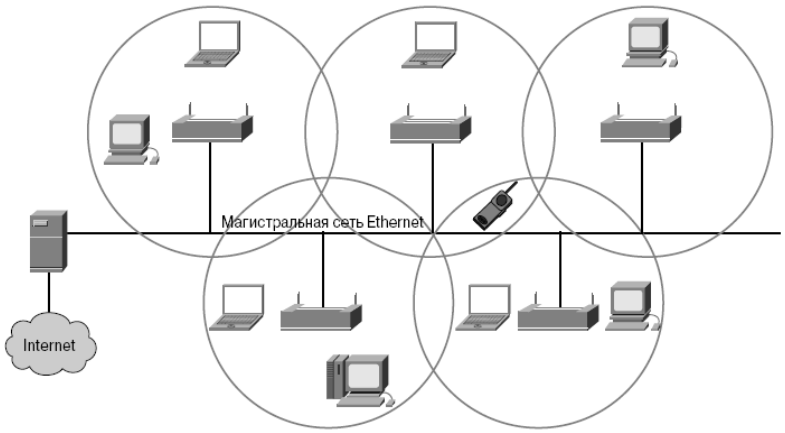


Рис. 17. Роуминг

В зондирующем запросе содержится идентификационный номер набора служб (*Service Set Identifier - SSID*) для той сети, к которой тификационным номером, она отвечает устройству зондирующим ответом и, соответственно, выполняет этапы аутентификации и подключения устройства к сети.

Устройства, которые находятся в пассивном режиме сканирования, прослушивают эфир и принимают сигнальные фреймы. Источником таких фреймов являются точки доступа и беспроводные станции. Когда устройство получает сигнальный фрейм с необходимым ему идентификатором SSID, оно пытается подсоединиться к беспроводной сети. Процесс пассивного сканирования является непрерывным, устройство может соединяться или разъединяться с точками доступа, в зависимости от изменения уровня их сигналов.

Взаимодействие в беспроводной сети

После установления соединения устройства с беспроводной сетью дальнейшее взаимодействие осуществляется посредством фреймов. В беспроводных локальных сетях существуют три типа фреймов: контрольные, управляющие и фреймы данных.

Управляющие фреймы:

- фрейм запроса на соединение;
- фрейм-ответ на запрос об установлении соединения;
- фрейм зондирующего запроса;
- фрейм зондирующего ответа;
- сигнальный фрейм;
- фрейм аутентификации.

Контрольные фреймы:

- готовность к передаче (*Request To Send - RTS*);
- готовность к приему (*Clear To Send - CTS*);
- подтверждение (*Acknowledgement*).

Фреймы данных.

Только фреймы данных схожи с фреймами стандарта 802.3. Размер поля данных спецификации 802.3 ограничен 1500 байтами, поэтому общий размер фрейма не может превышать 1518

байтов. В то же время размеры фрейма в беспроводных сетях могут достигать 2346 байтов, но обычно модули передачи данных беспроводных локальных сетей не превышают 1518 байтов по той причине, что точки доступа соединяются с проводной сетью стандарта Ethernet.

Исходя из того, что связь на основе радиоволн осуществляется с использованием общей среды передачи данных, в беспроводных локальных сетях могут возникать коллизии, так же, как и в кабельной сети с общим доступом к среде передачи данных. Из-за такой ситуации в беспроводных сетях используется множественный доступ с контролем несущей и предотвращением коллизий (*Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA*). Этот тип доступа к среде передачи данных немного похож на множественный доступ с контролем несущей и обнаружением конфликтов (*Carrier Sense Multiple Access with Collision Detection — CSMA/CD*), который используется в технологии Ethernet.

Контрольные вопросы

1. Какими стандартами реализуется фзической уровень в сетях Ethernet?
2. Для каких сетей применятеся коакиальный кабель, каковы его структура и категории?
3. Для каких сетей применятеся витая пара, каковы ее структура и категории?
4. Для каких сетей применятеся оптоволоконный кабель, каковы его структура и категории?
5. Каковы характеристики беспроводных сетей?

Лекция 9
Оборудование локальных сетей

1. **Распределение ресурсов в сетях**
2. **Сетевое оборудование**
3. **Беспроводные коммуникации**

Ключивые слова: интерсеть, сетевые станции, мост, маршрутизатор, шлюз, повторитель, концентратор, коммутатор, сетевые карты, коллизия, домен коллизий, фильтрация, последовательное соединение, терминальное оборудование.

Сети LAN объединяют между собой много устройств различных типов. Они называются аппаратными компонентами локальных сетей. Устройства сетей LAN могут включать в себя повторители, концентраторы, мосты, а также коммутаторы и маршрутизаторы, которые преобладают в современных локальных сетях.

1. Распределение ресурсов в сетях

Интерсеть – объединение многих ЛВС с помощью специальных сетевых станций (мостов – B, маршрутизаторов – R, шлюзов – G) (рис. 1).

- Мост (bridge) – сетевая станция для подключения сетей с одинаковой архитектурой.

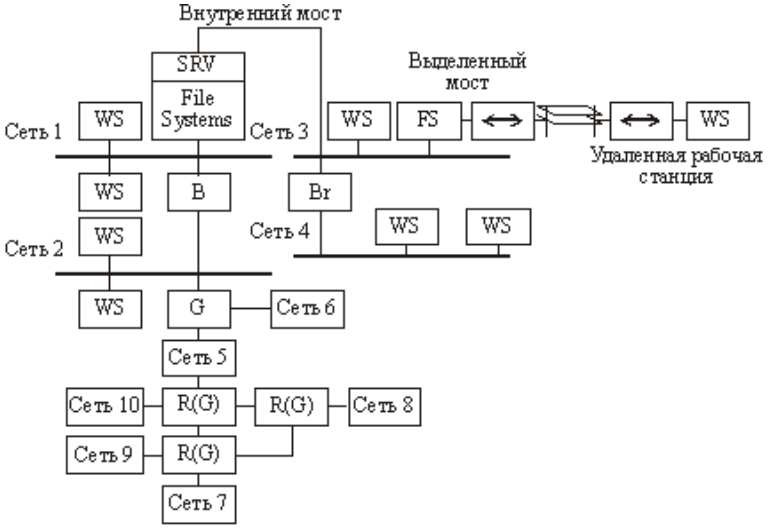


Рис 1. Пример структуры LAN

- Внутренний мост – файл-сервер может выполнять функции моста.
- Внешний мост – рабочая станция выполняет функции моста.
- Совмещенный мост – работа совмещается с рабочей станцией.
- Выделенный мост-ПК – выполняет только функции связи между ЛВС.
- Удаленный мост – удаленная рабочая станция (связь через модем).
- Шлюз (Gateway) – сетевая станция для объединения сетей с разной архитектурой.

Сетевые станции, объединяющие компьютеры в сетевые ассоциации, можно в порядке возрастания функциональных возможностей разбить на следующие классы:

– повторитель (repeater), концентратор (hub);

– мост (bridge), коммутатор (switch);

– маршрутизатор (router);

– шлюз (gateway).

Существует множество различных передающих сред, каждая из которых имеет свои достоинства и недостатки. Одним из недостатков кабеля категории 5 UTP является ограничение на длину кабеля. Максимальная длина кабеля UTP для одного участка сети составляет 100 м. Если

требуется большее расстояние, то нужно использовать повторители. В большинстве современных сетей Ethernet вместо повторителей используются концентраторы, которые являются многопортовыми повторителями или коммутирующими устройствами, созданными на основе новых технологий.

2. Сетевое оборудование

Сетевые карты

Платы (или карты) сетевых интерфейсов (Network Interface Card - NIC), коротко называемые *сетевыми картами*, рассматриваются как устройства второго уровня, поскольку все выпускаемые в мире адаптеры имеют уникальный код, называемый адресом *управления доступом к среде передачи* (*Media Access Control - MAC*), или MAC-адресом. Этот адрес управляет обменом данными между рабочей станцией и локальной сетью LAN. Адаптер NIC управляет доступом рабочей станции к среде передачи.

Повторитель (repeater)

Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Самый простой тип устройства для соединения фрагментов ЛВС. Он ретранслирует все принимаемые пакеты из единой секции ЛВС в другую или между отдельными ЛВС.

Назначение повторителей, показанных на рис. 2 и 3, состоит в регенерации и ресинхронизации сетевых сигналов на битовом уровне для того, чтобы они могли пройти большее расстояние по передающей среде. Повторители обычно используются в тех случаях, когда в сети имеется слишком много узлов или длины имеющегося кабеля недостаточно для достижения удаленных точек. Правило четырех повторителей для шинной топологии Ethernet 10 Мбит/с, также известное как правило 5-4-3, используется в качестве стандарта при расширении сегментов локальных сетей LAN. Это правило утверждает, что не более пяти сегментов сети могут быть соединены друг с другом с помощью четырех повторителей, но только три сегмента могут при этом иметь подключенные к ним рабочие станции (компьютеры). Хотя правило 5-4-3 справедливо для сетей с шинной топологией, для более сложных сетей с коммутаторами и звездообразной топологией оно не всегда применимо.

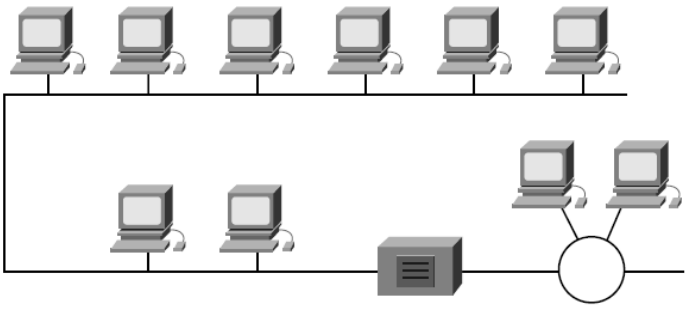


Рис. 2. Повторители

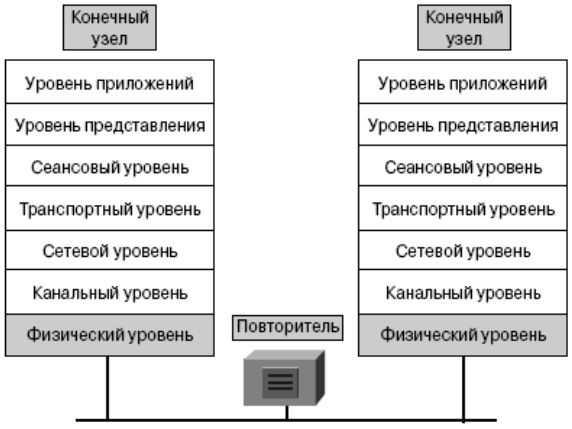


Рис. 3. Повторитель соединяет между собой два конечных узла

Концентраторы (hub)

Использование *концентраторов (hub)* обусловлено необходимостью в регенерации и ресинхронизации сетевых сигналов. Характеристики концентратора аналогичны характеристикам повторителя. Как показано на рис. 4, концентратор является общей точкой для нескольких сетевых соединений. Концентраторы обычно соединяют между собой несколько сегментов локальной сети LAN. Концентратор имеет несколько портов. Когда на порт концентратора поступают пакеты, они копируются на все остальные порты и в результате могут быть просмотрены всеми сегментами LAN-сети.

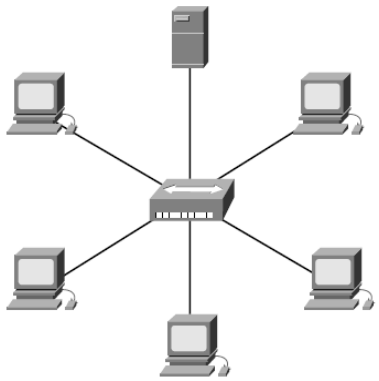


Рис. 4. Концентратор

Ниже приведены наиболее важные свойства устройств данного типа:

- концентраторы усиливают сигналы;
- концентраторы распространяют сигналы по сети;
- концентраторам не требуется фильтрация;
- концентраторам не требуется определение маршрутов и коммутации пакетов;
- концентраторы используются как точки объединения трафика в сети.

Концентраторы считаются устройствами первого уровня, поскольку они всего лишь регенерируют сигнал и повторяют его на всех своих портах (на выходных сетевых соединениях). В сетях Ethernet все рабочие станции подсоединены к одной и той же физической передающей среде.

Сигналы, передаваемые по этой общей среде, принимаются другими устройствами сети. *Коллизия (collision)* представляет собой ситуацию, в которой два или более битов распространяются по одной и той же сети одновременно. Область сети, в которой создаваемые пакеты могут испытать коллизию, называется *доменом коллизий (collision domain*). Сеть с совместно используемой средой передачи данных является доменом коллизий, называемым также доменом разделяемой полосы пропускания (*bandwidth domain*).

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют концентратором (concentrator) или хабом (hub). Главная задача концентратора – повторение сигнала, пришедшего с одного из портов, на других портах. Во многих случаях разница между этими двумя устройствами состоит только в количестве предоставляемых ими портов.

Кроме того, концентраторы чаще всего используются в сетях 10BASE-T и 100BASE-T, хотя могут использоваться и в других типах сетей. Использование концентратора преобразует сетевую топологию из шинной, в которой каждое устройство непосредственно подсоединено к общей шине, в звездообразную. При использовании концентраторов данные, поступающие на один из портов концентратора, повторяются посредством микросхем на всех остальных портах, подсоединенных к этому же сетевому сегменту, за исключением порта, с которого эти данные были отправлены.

Концентраторы принадлежат к одному из трех указанных типов:

- **активный концентратор** должен быть подключен к источнику внешнего питания, поскольку ему нужна энергия для усиления входящего сигнала перед передачей его на внешние порты;
- **интеллектуальный концентратор** иногда называют «умным» (*smart hubs)*. В целом такие устройства функционируют как обычные концентраторы, однако имеют встроенный микропроцессор и обладают возможностями диагностики. Они дороже обычных концентраторов, однако полезны в аварийных ситуациях;
- **пассивный концентратор** выступает исключительно в качестве точки физического соединения устройств. Такой концентратор не проверяет проходящий через него трафик и не выполняет никаких действий с потоками данных; он не усиливает и не очищает сигнал. Пассивный концентратор только предоставляет доступ к общей шине и поэтому не требует наличия источника питания.

Все устройства, подсоединенные к концентратору, получают все направленные ему данные. Вследствие этого они образуют единый домен коллизий. Под коллизией понимается ситуация, в которой два устройства пытаются одновременно передавать данные.

При объединении нескольких сегментов с помощью концентратора (повторителя) загрузка каждого из них становится равной сумме всех загрузок до их объединения. Некоторые концентраторы могут выполнять следующие операции:

- контроль наличия связи между портом и узлом (link status);
- регистрация коллизий и затянувшихся передач (jabber);
- согласование типов соединения (autonegotiation). В этом случае они снабжены SNMP-поддержкой.

Мосты (bridge)

Мост (bridge) представляет собой устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным коллизионным доменом. Иными словами, мосты предназначены для более рационального использования полосы пропускания. Целью моста является фильтрация потоков данных в LAN-сети с тем, чтобы локализовать внутрисегментную передачу данных и вместе с тем сохранить возможность связи с другими частями (сегментами) LAN-сети для перенаправления туда потоков данных. Каждое сетевое устройство имеет связанный с NIC-картой уникальный MAC-адрес. Мост собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов. По этой причине они могут быстро пересылать данные любых протоколов сетевого уровня. На решение о пересылке не влияет тип используемого протокола сетевого уровня, вследствие этого мосты принимают решение только о том, пересылать или не пересылать фрейм, и это решение основывается лишь на MAC-адресе получателя. Ниже приведены наиболее важные свойства мостов.

Отличительными функциями моста являются фильтрация фреймов на втором уровне и используемый при этом способ обработки трафика. Для фильтрации или выборочной доставки данных мост создает таблицу всех MAC-адресов, расположенных в данном сетевом сегменте и в

других известных ему сетях, и преобразует их в соответствующие номера портов. Этот процесс подробно описан ниже.

Этап 1. Если устройство пересылает фрейм данных впервые, мост ищет в нем MAC-адрес устройства-отправителя и записывает его в свою таблицу адресов.

Этап 2. Когда данные проходят по сетевой среде и поступают на порт моста, он сравнивает содержащийся в них MAC-адрес пункта назначения с MAC-адресами, находящимися в его адресных таблицах.

Этап 3. Если мост обнаруживает, что MAC»адрес получателя принадлежит тому же сетевому сегменту, в котором находится отправитель, то он не пересылает эти данные в другие сегменты сети. Этот процесс называется *фильтрацией (filtering)*. За счет такой фильтрации мосты могут значительно уменьшить объем передаваемых между сегментами данных, поскольку при этом исключается ненужная пересылка трафика.

Этап 4. Если мост определяет, что MAC-адрес получателя находится в сегменте, отличном от сегмента отправителя, он направляет данные только в соответствующий сегмент.

Этап 5. Если MAC-адрес получателя мосту неизвестен, он рассылает данные во все порты, за исключением того, из которого эти данные были получены. Такой процесс называется *лавинной рассылкой (flooding)*. Лавинная рассылка фреймов также используется в коммутаторах.

Этап 6. Мост строит свою таблицу адресов (зачастую ее называют мостовой таблицей или таблицей коммутации), изучая MAC-адреса отправителей во фреймах. Если MAC-адрес отправителя блока данных, фрейма, отсутствует в таблице моста, то он вместе с номером интерфейса заносится в адресную таблицу.

Иногда требуется разделить большую локальную сеть LAN на меньшие, легче управляемые сегменты. Такая стратегия позволяет ограничить поток данных через отдельную часть LAN и расширить поддерживаемую сетью географическую область, как показано на рис. 4. В качестве устройств, которые могут быть использованы для соединения между собой сетевых сегментов, могут быть использованы мосты. Они функционируют на канальном уровне модели OSI. Функция моста состоит в определении (принятии осмысленного решения) того, требуется ли отправлять поступившие на него сигналы в другой сегмент сети.

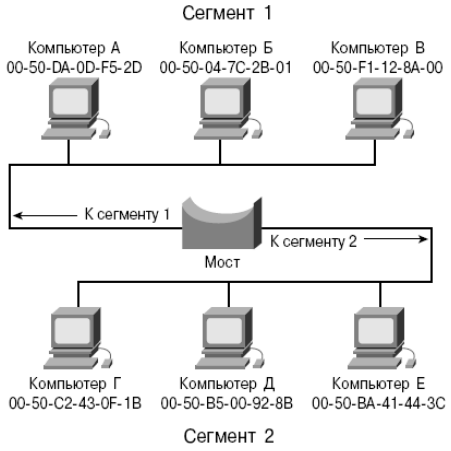


Рис. 4. Мосты делят сеть на сегменты

Мосты могут также быть использованы для соединения сетей, использующих различные протоколы или различные передающие среды, как, например, в случае беспроводных мостов, соединяющих сети LAN Ethernet в сеть городского масштаба.

Когда мост получает фрейм, он сравнивает MAC-адрес отправителя с имеющейся у него адресной таблицей для определения того, следует ли отфильтровать этот фрейм (отбросить), разослать его лавинным способом или скопировать фрейм в другой сегмент. Принятие такого решения происходит следующим образом:

- если устройство-получатель находится в том же сегменте, из которого этот фрейм был получен, то мост предотвращает его передачу в другие сегменты, как показано на рис. 5. Этот процесс называется *фильтрацией (filtering*);
- если устройство-получатель находится в другом сегменте и его адрес присутствует в адресной таблице, то мост пересылает фрейм в соответствующий сегмент, как показано на рис. 6;
- если устройство-получатель отсутствует в таблице адресов (т.е. «неизвестно» мосту), то мост рассылает фрейм во все сегменты за исключением того, откуда был получен фрейм. Такое поведение называют *лавинной рассылкой* сообщений.

Стратегически правильно установленный мост может значительно увеличить производительность сети.

Коммутаторы (switch)

Коммутатор иногда называют многопортовым мостом.Коммутаторы извлекают определенную информацию из пакетов данных, которые они получают от различных компьютеров сети. В дальнейшем эта информация используется для построения таблиц коммутации данных, которые затем используются для определения направления потоков данных, отправляемых одним из компьютеров сети другому, как показано на рис. 5.

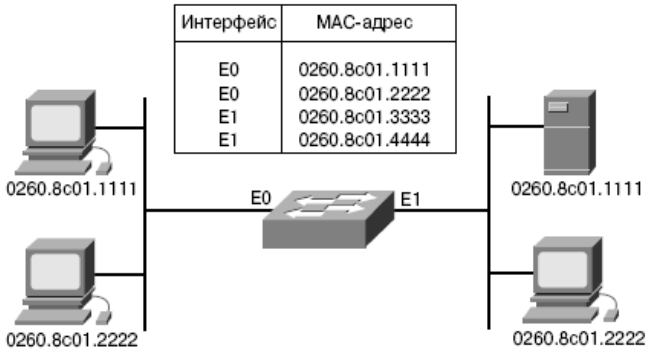


Рис.5. Таблица коммутации

Коммутатор имеет несколько портов, к которым подсоединены сегменты сети. Коммутатор выбирает порт, к которому подсоединено устройство-получатель или рабочая станция.

Коммутация представляет собой технологию, снижающую вероятность возникновения в сетях Ethernet LAN заторов за счет уменьшения объемов передаваемых по сети данных и увеличения полосы пропускания. Коммутаторы часто используются для замены концентраторов, поскольку не требуют изменения существующей кабельной инфраструктуры, что позволяет повысить производительность сети с минимальным количеством изменений в уже существующей сети. В настоящее время в сфере передачи данных все коммутирующее оборудование выполняет две основные операции:

- **коммутацию фреймов данных.** Под этим термином понимается процесс передачи фрейма, полученного из одной сетевой среды, в другую (выходную) среду;
- **поддержку коммутации.** Для выполнения этой функции коммутаторы строят и поддерживают таблицы коммутации и следят за возможным образованием маршрутных петель.

Коммутаторы работают с бо́льшими скоростями, чем мосты, а также могут поддерживать дополнительные и достаточно важные функции, такие, как виртуальные локальные сети VLAN (*Virtual LAN*).

Коммутатор Ethernet имеет много преимуществ, в частности, позволяет многим пользователям осуществлять связь параллельно за счет использования виртуальных каналов и создавать выделенные сетевые сегменты, свободные от коллизий. Другим преимуществом является возможность повторно использовать уже существующее аппаратное обеспечение и кабельную инфра структуру, что делает переход к использованию коммутаторов финансово эффективным.

Маршрутизаторы (route)

Маршрутизаторы (router) представляют собой устройства объединенных сетей, которые пересылают пакеты между сетями на основе адресов третьего уровня. Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных. Функционируя на третьем уровне, маршрутизатор может принимать решения на основе сетевых адресов вместо использования индивидуальных MAC-адресов второго уровня. Маршрутизаторы также способны соединять между собой сети с различными технологиями второго уровня, такими, как Ethernet, Token Ring и Fiber Distributed Data Interface (*FDDI - распределенный интерфейс передачи данных по волоконно-оптическим каналам*). Обычно маршрутизаторы также соединяют между собой сети, использующие технологию асинхронной передачи данных ATM (*Asynchronous Transfer Mode - ATM*) и последовательные соединения. Вследствие своей способности пересылать пакеты на основе информации третьего уровня, маршрутизаторы стали основной магистралью глобальной сети Internet и используют протокол IP.

Маршрутизатор – устройство связи, которое имеет аналогичные мосту функции и осуществляет передачу кадров в соответствии с определенным протоколом. Маршрутизаторы, анализируя только адресованные им кадры, направляют их в нужные межсетевые каналы по оптимальному маршруту, основываясь на информации относительной эффективности и надежности различных путей между узлами источника и получателя. Они обеспечивают соединение на сетевом уровне эталонной модели (рис. 6).

Рис. 6. Уровни работы маршрутизатора

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше, чем мосты.

Маршрутизатор представляет собой сложное многофункциональное устройство, в задачи которого входит: построение таблиц маршрутизации, определение на ее основе маршрута, буферизация, фрагментация и фильтрация поступающих пакетов, поддержка сетевых интерфейсов.

В отличие от мостов маршрутизаторы не содержат таблиц, где описывается каждый узел и соответствующая ЛВС. Маршрутизаторы используют не плоские аппаратные, как мосты, MAC-адреса, а составные числовые IP-адреса. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одной подсети (subnet). Они знают о существовании только других маршрутизаторов, которые идентифицируются адресом подсети. Для них безразлично, в каком формате поступает пакет или кадр. Они только чи-

тают адрес подсети, выбирают маршрут и, возможно, вкладывают пакет или кадр в соответствующий «конверт», формируя тем самым, пакет другого протокола.

Тем не менее, пакеты или кадры данных, посылаемые маршрутизатору, должны соответствовать требованиям конкретных протоколов сетевого уровня. Маршрутизаторов, преобразующих любые протоколы во всевозможные другие, пока нет в природе. Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня.

Функции маршрутизаторов могут выполнять как специализированные устройства, так и универсальные компьютеры с соответствующим программным обеспечением и числом сетевых карт, соответствующим количеству объединяемых подсетей.

Маршрутизаторы и последовательные соединения

Последовательной передачей называется метод передачи данных, при котором биты данных передаются последовательно по одному каналу.

На рис. 7 показаны несколько типов разъемов последовательных каналов. Последовательные порты и разъемы используются для подсоединения устройств конечного пользователя к устройствам провайдера службы.

Кроме выбора типа кабеля, необходимо определить, какого типа разъемы требуются для сети пользователя: разъемы терминального оборудования (*Data Terminal Equipment - DTE*) или телекоммуникационного (*Data Communications Equipment - DCE*). Модуль DTE представляет собой устройство пользователя в конечной точке канала WAN. Под DCE-модулем подразумевается устройство, на котором пользовательские данные DTE-устройства преобразовываются в приемлемую форму для устройств, обеспечивающих службы WAN. Как показано на рис. 8, если осуществляется непосредственное подсоединение к провайдеру службы или к устройству, осуществляющему синхронизацию сигнала (такому, например, как модуль CSU/DSU), то маршрутизатор является устройством DTE, и необходимо использовать последовательный кабель DTE. Такая ситуация типична при использовании маршрутизаторов.

Если соединение установлено непосредственно с провайдером службы или с устройством, которое обеспечивает синхронизацию (*clocking*), например, с модулем CSU/DSU (*Channel Service Unit/Data Service Unit* - модуль обслуживания канала и данных), маршрутизатор будет выступать в качестве конечного (терминального) оборудования (*Data Terminal Equipment - DTE*), и для подключения к каналу или службе понадобится DTE-кабель. Обычно именно такая схема подключения используется в сетях. Тем не менее, иногда возникает необходимость получать синхроимпульсы от местного маршрутизатора; в таком случае необходимо использовать DCE-кабель, и устройство будет выступать в качестве аппаратуры передачи данных (*Data Communications Equipment - DCE*) или телекоммуникационного оборудования, т.е. оборудования обслуживания канала. В лабораторных работах (и в тестовых условиях), когда один маршрутизатор подключен непосредственно к другому, одно устройство будет DTE-модулем, а другое - DCE, и для подключения их друг к другу понадобится кабель DTE-DCE.

Однако в некоторых случаях функции DCE выполняет маршрутизатор, как показано на рис. 9. Например, при непосредственном лабораторном соединении маршрутизаторов (*back-to-back*), т.е. когда на обоих концах соединения находятся маршрутизаторы, один из них выполняет функции DTE-устройства, а другой – DCE-устройства, осуществляя синхронизацию.

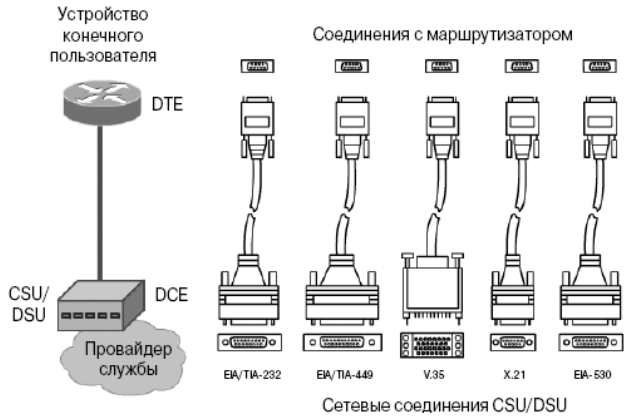


Рис. 7. Различные варианты последовательных соединений WAN

Рис. 8. Последовательное соединение: DTE и DCE

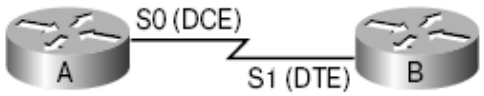


Рис. 9. Непосредственное лабораторное последовательное соединение маршрутизаторов

Для создания последовательного соединения в маршрутизаторах есть фиксирванные, или модульные, порты.

3. Беспроводные коммуникации

Беспроводная среда представляет собой альтернативный способ подключения к сети LAN. При беспроводном подключении можно без использования постоянного кабельного соединения передавать сигналы от одного компьютера другому с помощью радиосвязи (radio frequency - RF), лазера, инфракрасных лучей (infrared - IR), а также спутниковых сигналов.

В основе беспроводной коммуникации лежат устройства, называемые передатчиками и приемниками. Источник сигнала взаимодействует с передатчиком, который преобразует данные в электромагнитные волны (electromagnetic - EM), которые затем детектируются приемником. Приемник преобразует волны в цифровые данные для получателя. Для двусторонней связи каждому устройству требуются как передатчик, так и приемник. Многие производители сетевого оборудования включают передатчик и приемник в один блок, называемый трансивером (приемопередатчиком), или беспроводным сетевым адаптером. Все устройства беспроводной сети LAN должны иметь соответствующий беспроводной сетевой адаптер.

RF-технология позволяет осуществлять связь между устройствами, находящимися в разных помещениях или даже разных зданиях. Технология RF может использовать одну или несколько частот.

Контрольные вопросы

1. Какое оборудование применяется для создания компьютерных сетей?
2. Какие функции в сети выполняют коммутаторы?
3. Какие функции в сети выполняют повторители и концентраторы?
4. Какие функции в сети выполняют маршрутизаторы и мосты?
5. Какими способами осуществляется коммутация в беспроводных сетях?

Лекция 10
Адресация в локальных сетях

1. **IP-адреса**
2. **Адресация IPv4**
3. **Классы IP-адресов**
4. **Открытые и частные адреса**
5. **MAC-адреса**
6. **Новое поколение протоколов IP**

Ключивые слова: IP-адреса, IPv4, адрес сети, адрес узла, класс адреса, диапазон IP-адресов, широковещательный адрес, открытые адреса, частные адреса, общие IP-адреса, MAC-адрес, IPv6.

Сетевой уровень отвечает за навигацию данных по сети, и его задача заключается в нахождении наилучшего маршрута. Устройства используют схему адресации сетевого уровня для определения адреса пункта назначения информации при ее передаче по сети.

1. IP-адреса

Чтобы любые две системы могли взаимодействовать между собой, они должны иметь возможность однозначно идентифицировать друг друга.

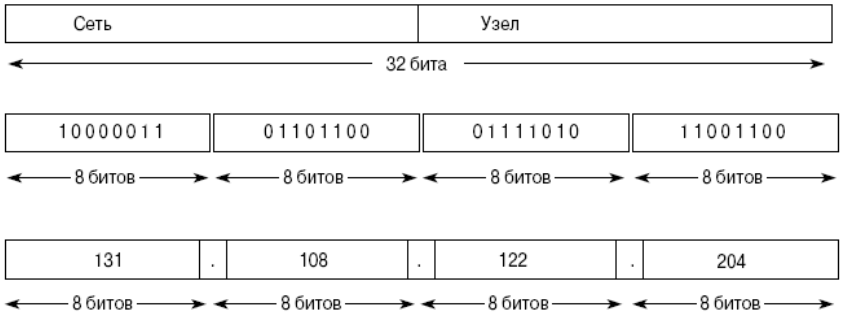


Рис. 3. Формат IP-адреса

Компьютеры хранят IP-адрес в виде 32-битовой последовательности единиц и нулей (рис. 3). Для простоты использования IP-адрес обычно записывается в виде четырех десятичных номеров, разделенных точками.

2. Адресация IPv4

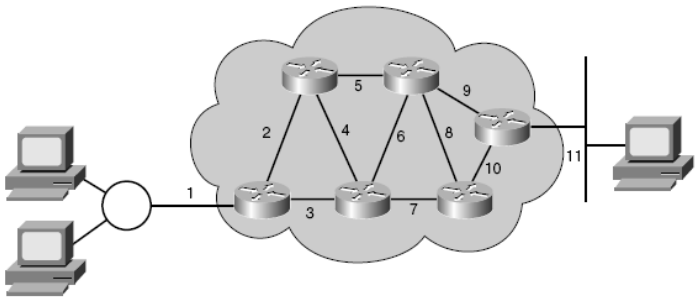
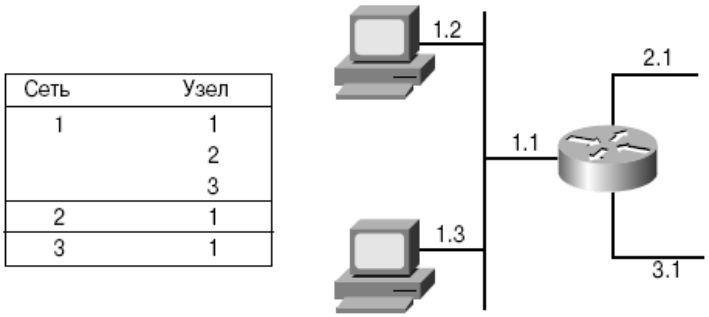


Рис. 4. Коммуникационный маршрут

Протокол IP пересылает пакеты, порожденные в одной из сетей, в другую, т.е. в сеть назначения, используя некоторые уникальные параметры (рис. 4). Следовательно, в этой схеме должны быть заданы идентификаторы сети-отправителя и сети-получателя. Используя идентификатор сети назначе-



ния, протокол IP доставляет пакеты в сеть, которой они адресованы. Когда пакет достигает интерфейса маршрутизатора, подключенного к сети получателя, протокол IP должен идентифицировать определенный компьютер, подключенный к этой же сети, которому адресован пакет.

Рис. 5. Две части IP-адреса

Аналогично IP-адреса состоят из двух частей, как это показано на рис. 5. Одна часть идентифицирует сеть, к которой подключена система, вторая же служит идентификатором самой системы. Такая адресация называется иерархической, поскольку включает несколько уровней, как показано на рис. 5.

Адрес группы, находящийся в иерархической схеме (рис. 6) непосредственно над группой, является идентификатором для всей порождаемой ветви адресов и сетей и может рассматриваться как единое целое. IP-адрес объединяет оба идентификатора в один адрес. Такой номер должен быть уникальным, поскольку дублирование адресов не допускается; его первая часть идентифицирует адрес сети, а вторая – адрес узла - однозначно задает машину в этой сети.

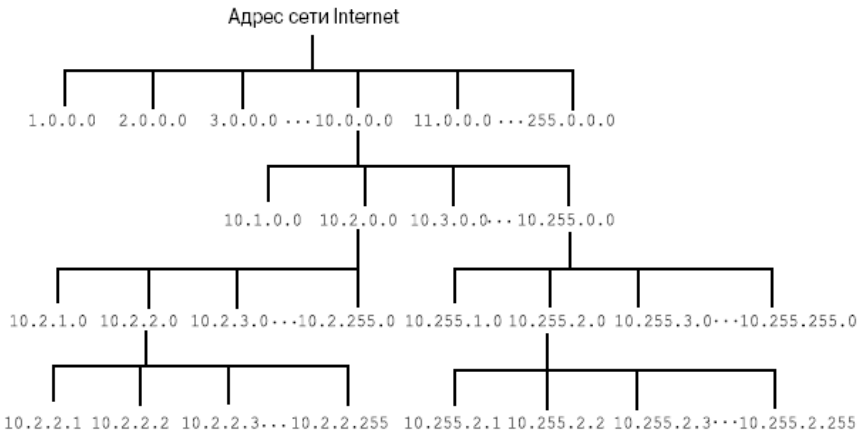


Рис. 6. Иерархические IP-адреса

Каким же образом пользователь может отличить, какая часть адреса задает адрес сети, а какая - адрес узла? Впервые этот вопрос задали себе создатели сети Internet, полагавшие, что будут создаваться сети разного размера, исходя из необходимого числа компьютеров, входящих в ее состав, что проиллюстрировано в табл. 1.

Таблица 1. Классы IPадресов

Класс адреса	**Количество сетей**	**Количество узлов**
A	126	16777216
B	16384	65535
C	2097152	254
D (многоадресатный)	-	-

Разработчики разделили доступные IP-адреса на классы и задали таким образом размер сетей: большие (класс A), средние (класс B) и мелкие (класс C) (табл. 2). Информация о классе адреса - это первая подсказка, которая используется, чтобы определить, какая часть адреса описывает сеть, а какая - адрес узла.

Таблица 2. Определение классов адресов

Класс адреса	**Начальные биты адреса**	**Диапазон значений первого октета адреса**	**Количество битов в сетевой части адреса**
A	0	от 0 до 127	8
B	10	от 128 до 191	16
C	110	от 192 до 223	24
D (многоадресатный)	1110	от 224 до 239	28

3. Классы IP-адресов

Чтобы иметь возможность описать сети разного размера и облегчить их классификацию, IP-адреса были разделены на группы, называемые классами (рис. 7).

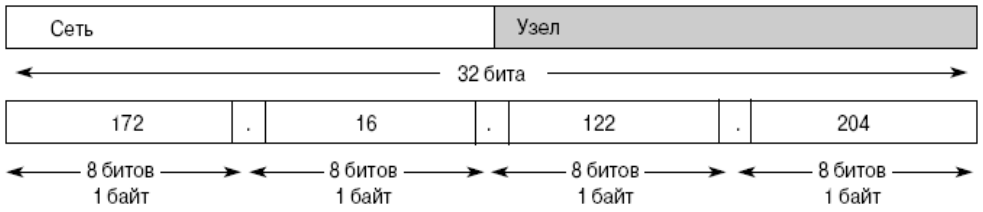


Рис. 7. Разделение адреса на сетевую и узловую части

Такая схема адресации называется классовой. Каждый полный 32-битовый IP-адрес делится на две части, описывающие сеть и узел. Бит или последовательность битов в начале каждого адреса задают его класс. Существуют пять классов IP-адресов.

Адреса класса A

Адреса класса A (рис. 8.) предназначены для очень больших сетей. В адресе класса A используется только первый октет в качестве идентификатора сети. Оставшиеся три октета выделены для перечисления адресов узлов.

Первый бит в адресе класса A всегда равен 0. Следует заметить, что оба номера, 0 и 127, являются зарезервированными и не могут быть использованы в качестве сетевых адресов.

Сеть с номером 127.0.0.0 зарезервирована для обратного петлевого (loopback) тестирования (маршрутизаторы или локальные узлы могут использовать его для передачи пакетов самим себе). Следовательно, такой адрес не может быть присвоен сети.

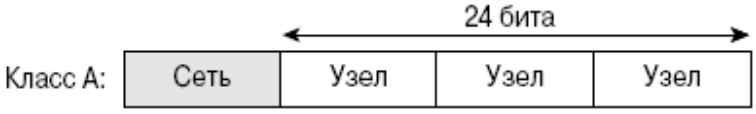


Рис. 8. Адреса класса A

Адреса класса B

Адреса класса B используются для сетей среднего и крупного размера (рис. 9). В IP-адресе класса B используются два первых октета для сетевого адреса. Оставшиеся два октета представляют адрес узла.

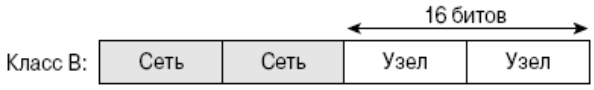


Рис. 9. Адреса класса B

Первые два бита первого октета всегда равны 10. Таким образом, наименьшее число, которое может быть использовано для адресов этого класса, равно 10000000 (десятичное 128), и наибольшее - 10111111 (десятичное значение равно 191). Любые адреса, содержащие в первом октете числа от 128 до 191, являются адресами класса B.

Адреса класса C

Адреса класса C (рис. 10) - это наиболее часто используемые из исходных классов адресов. Данный класс адреса предназначен для использования в малых сетях.

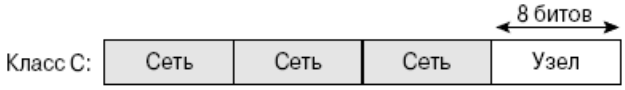


Рис. 10. Адреса класса C

Адрес этого класса начинается с двоичной комбинации 110. Таким образом, наименьшее доступное число - 11000000 (десятичное 192), а наибольшее – 11011111 (десятичное значение 223). Если адрес в первом октете содержит числа от 192 до 223, значит, он относится к классу C.

Адреса класса D

Адреса класса D (рис. 11) были созданы для реализации в IP-адресах механизма многоадресатной рассылки. *Многоадресатным, или групповым, адресом (multicast address*) называется уникальный сетевой адрес, используемый для отправки пакетов, содержащих адрес рассматриваемого класса в поле получателя, предопределенным группам сетевых устройств. Таким образом, одна сетевая станция может передавать один поток данных нескольким получателям.

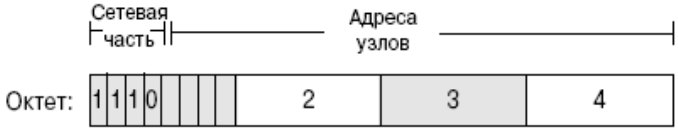


Рис. 11. Адреса класса D

Диапазон адресов класса D так же, как и других классов, определенным образом ограничен. Первые четыре бита адреса класса D должны быть равны 1110. Следовательно, первый октет адресов этого класса может принимать значения от 11100000 до 11101111 или, в десятичной записи, от 224 до 239. Многоадресатный IP-адрес, первый октет которого начинается с чисел в диапазоне от 224 до 239, является адресом класса D.

Адреса класса E

Адреса класса E (рис. 12) также были описаны в стандартах и выделены в отдельный блок. Однако они были зарезервированы проблемной группой проектирования Internet (Internet Engineering Task Force - IETF) для собственных исследовательских нужд. В результате адреса класса

E никогда не использовались в сети Internet. Первые четыре бита адресов класса E всегда содержат 1. Следовательно, значение первого октета находится в диапазоне от 11110000 до 11111111 или от 240 до 255 - в десятичном виде.

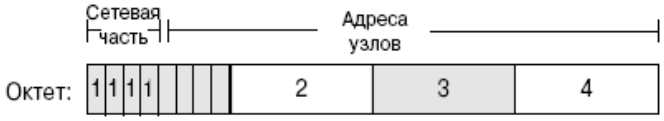


Рис. 12. Адреса класса E

Диапазоны значений первого октета в IP-адресах для каждого из классов приведены в табл. 3.

Таблица 3. Классы IP_адресов: диапазон значений первого октета

Класс IP-адреса	**Диапазон IP-адресов (десятичное число первого октета)**
Класс A	от 0 до 126 (от 00000001 до 01111111)
Класс B	от 128 до 191 (от 10000000 до 10111111)
Класс C	от 192 до 223 (от 11000000 до 11011111)
Класс D	от 224 до 239 (от 11100000 до 11101111)
Класс E	от 240 до 255 (от 11110000 до 11111111)

Зарезервированные IP-адреса

Некоторые адреса являются зарезервированными и не могут быть присвоены сетевым устройствам. К ним относятся следующие:

- сетевые адреса, идентифицирующие саму сеть (рис. 13). Верхний прямоугольник на рисунке обозначает сеть с адресом 198.150.11.0. Данные, адресованные любому из узлов, находящихся в этой сети (198.150.11.1 или 198.150.11.254), вне этой сети выглядят как данные, которые отправлены на адрес 198.150.11.0. Адрес узла принимается во внимание только тогда, когда пакет с данными нужно адресовать получателю внутри локальной сети. Нижний прямоугольник на рисунке обозначает другую такую же локальную сеть, но с адресом 198.150.12.0;

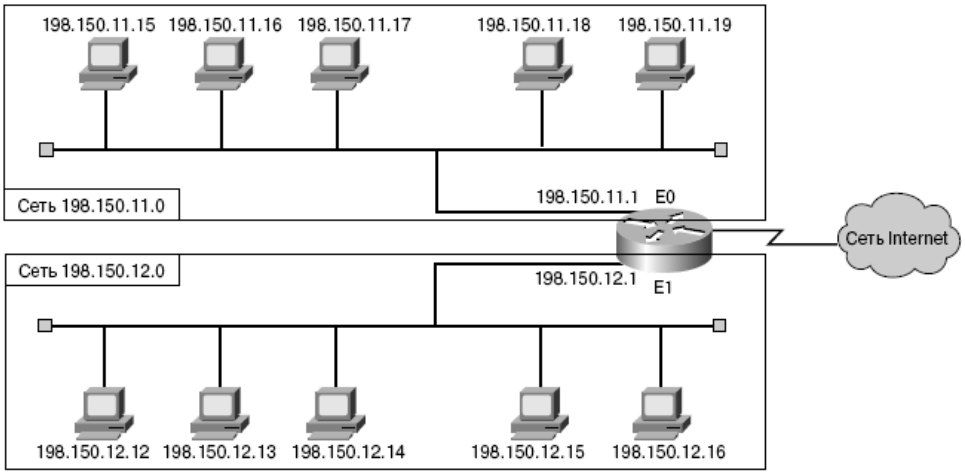


Рис. 13. Адрес сети

- как следует из названия, *широковещательный адрес* используется для широковещательной рассылки всем сетевым устройствам (рис. 14). Верхний прямоугольник схематически поясняет широковещательный адрес 198.150.11.255. Данные, отправленные по этому адресу, будут получены каждым из узлов в сети (от 198.150.11.1 до 198.150.11.254). Нижний прямоугольник иллюстрирует подобную ситуацию для широковещательного адреса 198.150.12.255.

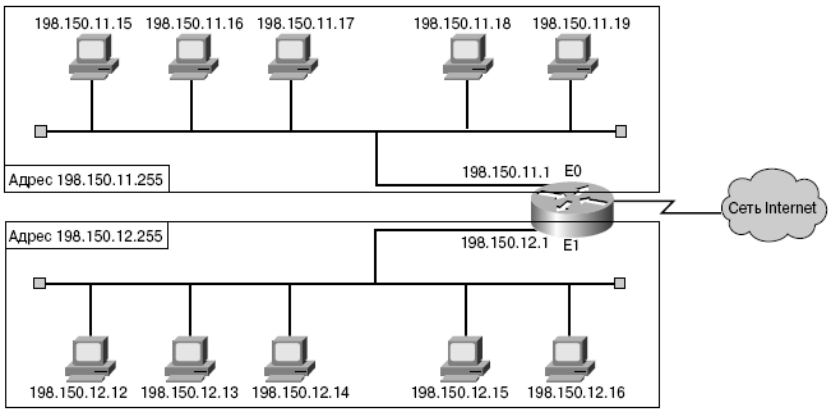


Рис. 14. Широковещательный адрес

IP-адрес, у которого все биты, отведенные под адрес узла, заполнены нулями, зарезервирован под *адрес сети* (рис. 14). Показанный адрес класса B имеет нули во всех битах, отведенных под адрес узла. Таким образом, в примере для сети класса A число 113.0.0.0 является адресом сети, содержащей узел 113.1.2.3. Маршрутизатор использует IP-адрес сети при пересылке данных через сеть Internet.

Для адреса сети класса B, записанного в виде чисел в точечно-десятичном формате, первые два октета стандартно идентифицируют сеть. Последние два октета содержат нули, поскольку именно эти 16 битов являются той частью адреса, которая отведена для идентификации подключенных к сети устройств. Такой адрес называется одноадресатным (unicast). Одноадресатный адрес указывает только на один узел во всей сети. IP-адрес из рассмотренного выше примера (176.10.0.0) зарезервирован в качестве адреса сети и ни при каких условиях не может быть использован в качестве адреса подключенного к сети устройства.

Для передачи данных всем узлам в сети требуется широковещательный адрес. Широковещательная рассылка используется, когда отправитель пересылает данные всем устройствам в сети.

Открытые и частные адреса

Стабильное функционирование сети Internet зависит от уникальности используемых в сети публичных адресов. Как показано на рис. 15, при использовании сетевой схемы адресации могут возникнуть некоторые проблемы. В проиллюстрированной на рисунке структуре обе сети имеют адрес 198.150.11.0. Когда данные приходят на маршрутизатор, в какую из сетей они должны быть перенаправлены? Схемы, подобные этой, могут значительно увеличить объем сетевого трафика и сделать невозможным выполнение основной функции маршрутизатора; следовательно, нужно предусмотреть какие-либо механизмы для проверки уникальности используемых адресов.

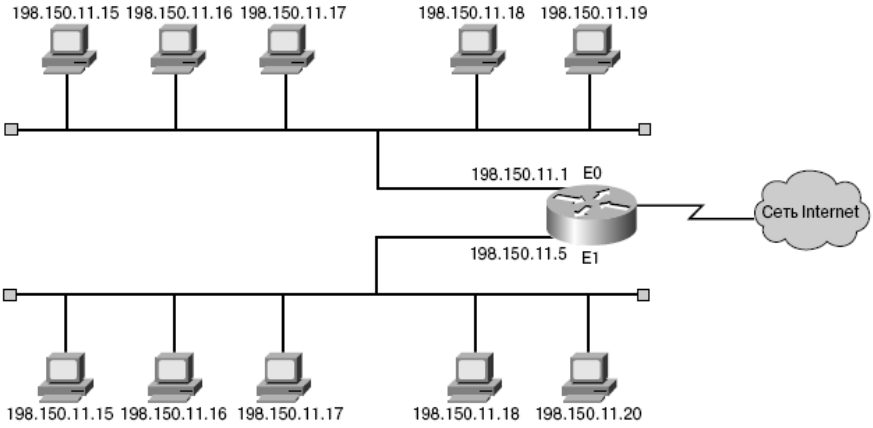


Рис. 15. Уникальность адресов

Открытые IP-адреса уникальны. Не существует двух устройств с одинаковыми IP-адресами, которые были бы подключены к открытой сети, поскольку такие адреса используются в глобальном масштабе и подчиняются стандарту. Все компьютеры, подключенные к сети Internet, следуют такому требованию. Открытые IP-адреса должны выделяться поставщиками услуг Internet (*Internet Service Provider - ISP*).

Как уже говорилось, узлы в сети Internet должны иметь глобально-уникальные адреса. Однако частные сети, не подключенные к открытой сети, могут использовать любые действительные адреса, которые должны быть уникальны только внутри локальной сети. Поскольку количество 32-битных адресов конечно, существует риск, что их не хватит. Чтобы частично решить проблему нехватки адресного пространства, был разработан альтернативный вариант - использование частных IP-адресов (табл. 4).

Таблица 4. Частные IP-адреса

Класс IP-адреса	**Число зарезервированных сетевых адресов**	**Диапазон IP-адресов (для внутреннего использования)**
Класс A	1	от 10.0.0.0 до 10.255.255.255
Класс B	16	от 172.16.0.0 до 176.31.255.255
Класс C	256	от 192.168.0.0 до 192.168.255.255

Таким образом, внутренние узлы смогут обмениваться данными друг с другом без уникальных общих IP-адресов.

В соответствии со стандартом RFC 1918 несколько диапазонов адресов класса A, B и C были зарезервированы. Как видно из таблицы 4, в диапазон частных адресов входит одна сеть класса A, 16 сетей класса B и 256 сетей класса C. Адреса из этих диапазонов не передаются магистральными маршрутизаторами сети Internet, и пакеты с адресами из частных сетей немедленно будут отброшены такими устройствами. Таким образом, сетевые администраторы получили определенную степень свободы в плане предоставления внутренних адресов.

В очень большой сети можно использовать частную сеть класса A, где можно создать более 16 миллионов частных адресов.

В средних сетях можно использовать частную сеть класса B с более чем 65 000 адресов.

В домашних и небольших коммерческих сетях обычно используется один частный адрес класса C, рассчитанный на 254 узла.

Одну сеть класса A, 16 сетей класса B или 256 сетей класса C могут использовать организации любого размера. Многие организации пользуются частной сетью класса A.

Узлы из внутренней сети организации могут использовать частные адреса до тех пор, пока им не понадобится прямой выход в Интернет. Соответственно, один и тот же набор адресов подходит для нескольких организаций. Частные адреса не маршрутизируются в Интернете и быстро блокируются маршрутизатором Интернет-провайдера.

Частные адреса можно использовать как меру безопасности, поскольку они видны только в локальной сети, а посторонние получить прямой доступ к этим адресам не могут (рис. 16).

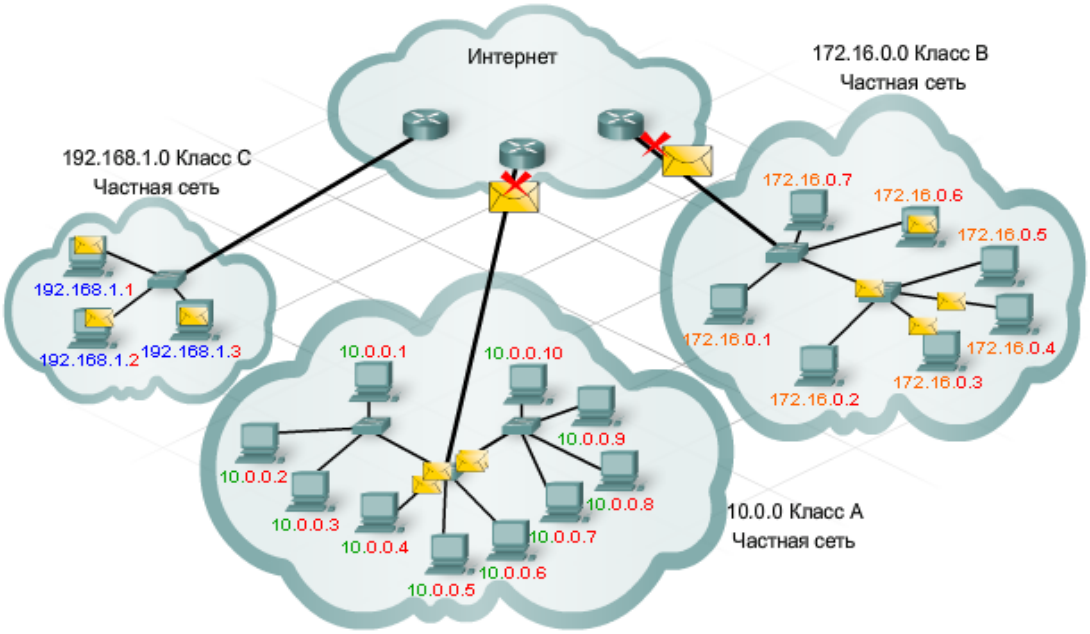


Рис. 16. Частные адреса

Кроме того, существуют частные адреса для диагностики устройств. Они называются адресами обратной связи. Для таких адресов зарезервирована сеть 127.0.0.0 класса A.

В том случае, когда нужно выбрать схему адресации для внутренней сети тестовой лаборатории или домашней сети, можно использовать диапазоны адресов, перечисленные в табл. 3.4, вместо глобально уникальных. Частные IP-адреса могут использоваться совместно с публичными для внутренних соединений, что позволяет экономить открытые уникальные адреса.

Многие частные сети используются совместно с открытыми сетями, поэтому использование выбранных произвольно адресов настоятельно не рекомендуется, поскольку однажды частная сеть может оказаться подключенной к глобальной сети Internet.

При подключении сети предприятия, в которой используются частные адреса, к сети Internet необходимо обеспечить преобразование частных адресов в открытые. Такой процесс называется трансляцией сетевых адресов (*Network Address Translation - NAT*) и обычно выполняется маршрутизатором.

5. MAC-адреса

MAC-адреса (Media Access Control addresses - адреса второго уровня модели OSI) Стандартизированный адрес канального уровня, который назначается каждому устройству или порту, подключенному к локальной сети. Другие сетевые устройства используют такой адрес для нахождения определенных портов в сети, для создания и обновления таблиц маршрутизаций. Длина MAC-адреса равна 6 байтам, уникальность которых контролируется институтом IEEE.

Этот адрес управляет обменом данными между рабочей станцией и локальной сетью LAN.

MAC-адресация

Для того чтобы в сети Ethernet стала возможной локальная доставка фреймов, необходима определенная система адресации, т.е. присвоения имен компьютерам и интерфейсам. Каждый компьютер имеет уникальный способ самоидентификации.

Никакие два физических адреса в сети не должны быть одинаковыми. Физические адреса, называемые адресами *управления доступом к передающей среде (Media Access Control – MAC-адрес)*, записаны в сетевом адаптере NIC. Для MAC-адреса используются и другие названия: аппаратный адрес, NIC-адрес, адрес второго уровня и Ethernet-адрес.

MAC-адреса в сети Ethernet используются для уникальной идентификации отдельных устройств. Каждое устройство (ПК, маршрутизатор, коммутатор и т.д.), имеющее Ethernet-интерфейс к сети LAN, должно иметь MAC-адрес, в противном случае другие устройства не смогут обмениваться с ним данными. MAC-адрес имеет длину 48 битов и записывается в виде 12-ти шестнадцатеричных цифр. Первые шесть шестнадцатеричных цифр, задаваемых IEEE, идентифицируют производителя или продавца устройства и, таким образом, включают в себя *уникальный идентификатор организации (Organizationally Unique Identifier - OUI*). Остальные шесть шестнадцатеричных цифр включают в себя серийный номер интерфейса или другое значение, задаваемое конкретным производителем. MAC-адреса иногда называют прошитыми (Burned In Address - BIA), поскольку они записаны в постоянной памяти (Read Only Memory - ROM) интерфейса или устройства и копируются в оперативную память (Random Access Memory - RAM) при инициализации сетевого адаптера NIC. На рис. 17 показан формат MAC-адреса.

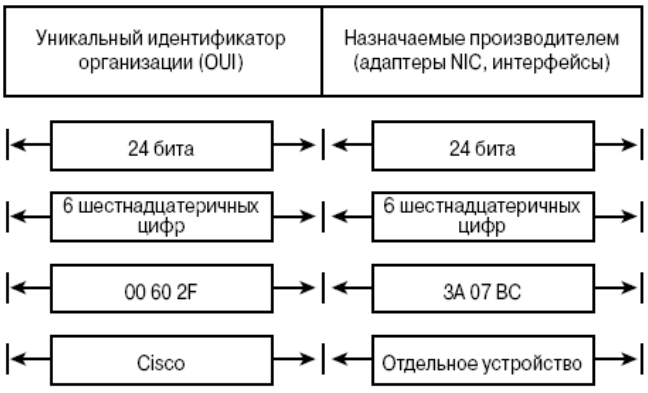


Рис. 17. Формат MAC-адреса

Без MAC-адресов сеть LAN представляла бы собой лишь группу изолированных компьютеров, и доставка Ethernet-фреймов была бы невозможной. Вследствие этого на канальном уровне к данным верхних уровней добавляются *заголовок (header*), содержащий MAC-адрес устройства, и *концевик (trailer*). Заголовок и концевик содержат управляющую информацию, предназначенную для канального уровня устройства, которому направляется фрейм.

Данные верхних уровней инкапсулируются в заголовок и концевик канального уровня.

LAN-сети спецификаций Ethernet и 802.3 являются широковещательными. Это означает, что все станции сети видят все проходящие по сети фреймы, и каждая станция должна исследо-

вать каждый фрейм, для того чтобы выяснить, не является ли она требуемым пунктом назначения этого фрейма.

В сети Ethernet в случае, когда устройству требуется отправить данные другому устройству, оно может открыть маршрут коммуникации к другому устройству, используя свой MAC-адрес. Когда устройство-отправитель посылает данные в сеть, эти данные включают в себя MAC-адрес требуемого пункта назначения. По мере того, как эти данные перемещаются по сетевой среде, адаптер NIC каждого устройства, к которому они поступают, проверяет, не совпадает ли его MAC-адрес с адресом пункта назначения, содержащимся во фрейме данных. Если такого соответствия нет, то адаптер отбрасывает этот фрейм. Если же такое соответствие имеется, то адаптер NIC проверяет адрес получателя в заголовке фрейма, для того чтобы удостовериться в правильности адресации пакета. При поступлении данных на требуемую станцию ее адаптер делает их копию, удаляет заголовок и концевик и передает их компьютеру для обработки протоколами более высокого уровня, такими, как IP и TCP.

Новое поколение протоколов IP

До сих пор, при обсуждении IP-технологии, основное внимание уделялось проблемам межсетевого обмена и путям их решения в рамках существующей технологии. Однако, все эти задачи, вызванные необходимостью приспособления IP к новым физическим средам передачи данных меркнут перед действительно серьезной проблемой - ростом числа пользователей Сети. Число пользователей увеличивается, следовательно, растет популярность сети. Такое положение дел должно только радовать. Но проблема заключается в том, что Internet стал слишком большой, он перерос заложенные в него возможности.

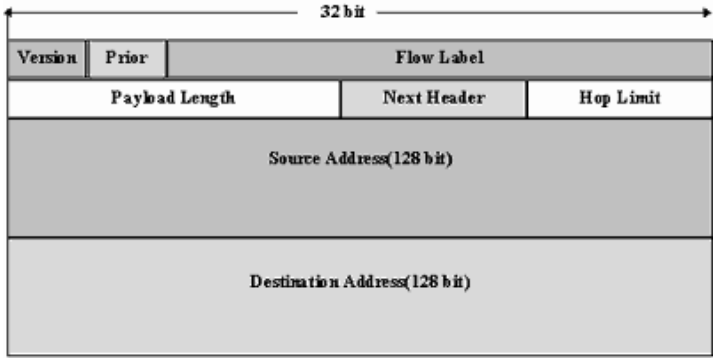


Рис.18. Заголовок IPv6

В начале 1995 года IETF, выпустило предложения по новому стандарту протокола IP - IPv6, который еще называют IPing (рис. 18). Сейчас Internet-сообщество живет по стандарту IPv4. IPv6 призван не только решить адресную проблему, но и попутно помочь решению других задач, стоящих в настоящее время перед Internet.

В этом заголовке поле ***«версия»*** - номер версии IP, равное 6. Поле ***«приоритет»*** может принимать значения от 0 до 15.

Первые 8 значений закреплены за пакетами, требующими контроля переполнения, например:

- 0 - несимвольная информация;
- 1 - информация заполнения (news),
- 2 - не критичная ко времени передача данных (e-mail);
- 4 - передача данных режима on-line (FTP, HTTP, NFS и т.п.);
- 6 - интерактивный обмен данными (telnet, X);
- 7 - системные данные или данные управления сетью (SNMP, RIP и т.п.).

Поле **«метка потока»** предполагается использовать для оптимизации маршрутизации пакетов. В IPv6 вводится понятие потока, который состоит из пакетов. Пакеты потока имеют одинаковый адрес отправителя и одинаковый адрес получателя, и ряд других одинаковых опций. Подразумевается, что маршрутизаторы будут способны обрабатывать это поле и оптимизировать процедуру пересылки пакетов, принадлежащих одному потоку. В настоящее время алгоритмы и способы использования поля «метка потока» находятся на стадии обсуждения.

Поле **«длины пакета»** определяет длину следующей за заголовком части пакета в байтах.

Поле **«следующий заголовок»** определяет тип следующего за заголовком IP-заголовка. Заголовок IPv6 имеет меньшее количество полей, чем заголовок IPv4. Многие необязательные поля могут быть указаны в дополнительных заголовках, если это необходимо.

Поле **«ограничение переходов»** определяет число промежуточных шлюзов, которые ретранслируют пакет в сети. При прохождении шлюза это число уменьшается на единицу. При достижении значения «0» пакет уничтожается.

После первых 8 байтов в заголовке указываются адрес отправителя пакета и адрес получателя пакета. Каждый из этих адресов имеет длину 16 байт.

Таким образом, длина заголовка IPv6 составляет 48 байтов (рис. 19).

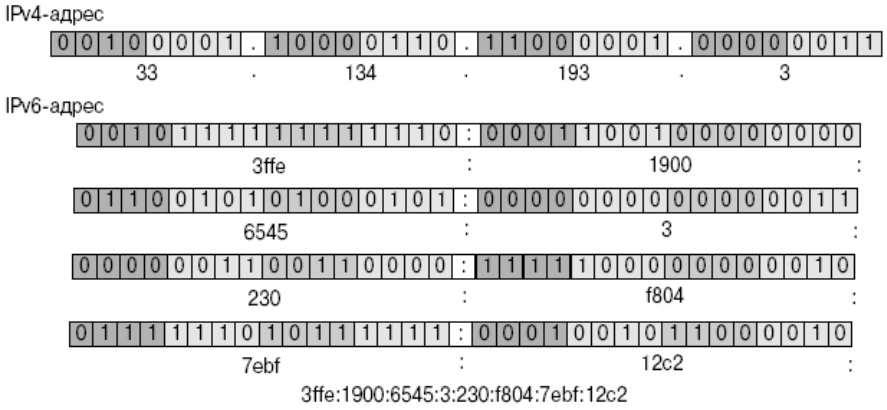


Рис. 19. Форматы адресов IPv4 и IPv6

После 4 байтов IP-адреса стандарта IPv4, шестнадцать байт IP-адреса для IPv6 выглядят достаточными для удовлетворения любых потребностей Internet. Не все 2128 адресов можно использовать в качестве адреса сетевого интерфейса в сети. Предполагается выделение отдельных групп адресов, согласно специальным префиксам внутри IP-адреса, подобно тому, как это делалось при определении типов сетей в IPv4. Так, двоичный префикс «0000 010» предполагается закрепить за отображением IPX-адресов в IP-адреса.

В новом стандарте выделяются несколько типов адресов:

- *unicast addresses* - адреса сетевых интерфейсов,
- *anycast addresses* - адреса не связанные с конкретным сетевым интерфейсом, но и не связанные с группой интерфейсов,
- *multicast addresses* - групповые адреса.

Разница между последними двумя группами адресов в том, что anycast address это адрес конкретного получателя, но определяется адрес сетевого интерфейса только в локальной сети,

где этот интерфейс подключен, а multicast-сообщение предназначено группе интерфейсов, которые имеют один multicast-адрес.

Разработка и планирование технологии заняли годы, прежде чем протокол IPv6 постепенно начал использоваться в отдельных сетях. В перспективе стандарт IPv6 может заменить IPv4 в качестве доминирующего протокола в сети Internet.

Контрольные вопросы

1. При помощи каких средств компьютерные сети идентифицируют друг друга?
2. На какие классы делтся IP-адреса?
3. В чем особенности открытых и частных IP-адресов?
4. Каковы структура и назначение MAC-адреса?
5. С какими целями был создан протокол IPv6 и каково его отличие от IPv4?

Лекция 11

Сетевая адресация

1. **Задачи IP-адресов**
2. **Подсети**
3. **Назначение IP-адресов**

Ключивые слова: IP-адрес, сетевая интерфейсная плата, маска подсети, подсеть, адресное пространство, статические IP-адреса, протокол RARP, динамические IP-адреса, протокол DHCP.

1. Задачи IP-адресов

Для обмена данными в Интернете узлу необходим IP-адрес. Это логический сетевой адрес конкретного узла. Для обмена данными с другими устройствами, подключенными к Интернету, необходим правильно настроенный, уникальный IP-адрес.

IP-адрес присваивается сетевому интерфейсу узла. Обычно это сетевая интерфейсная плата (NIC), установленная в устройстве. Примерами пользовательских устройств с сетевыми интерфейсами могут служить рабочие станции, серверы, сетевые принтеры и IP-телефоны. Иногда в серверах устанавливают несколько NIC, у каждой из которых есть свой IP-адрес (рис. 1).

У интерфейсов маршрутизатора обеспечивающего связь с сетью IP, также есть IP-адрес.

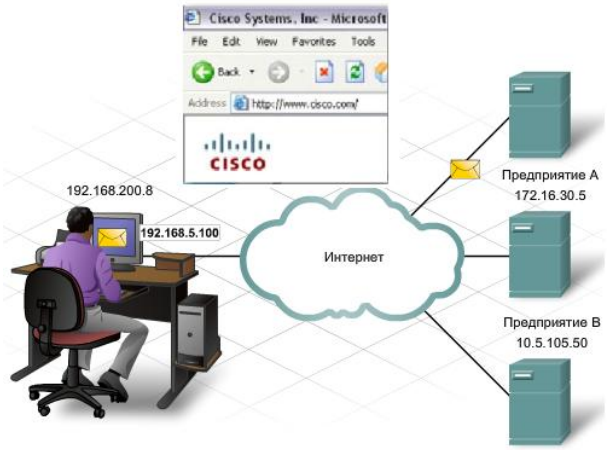


Рис. 1. IP-адреса

В каждом отправленном по сети пакете есть IP-адрес источника и адресата. Эта информация необходима сетевым устройствам для передачи информации адресату и передачи источнику ответа.

Структура IP-адресов

Получая IP-адрес, узел просматривает все 32 бита по мере поступления на сетевой адаптер. Напротив, людям приходится преобразовывать эти 32 биты в десятичные эквиваленты, то есть в четыре октета. Каждый октет состоит из 8 бит, каждый бит имеет значение. У четырех групп из 8 бит есть один и тот же набор значений. Значение крайнего правого бита в октете - 1, значения остальных, слева направо - 2, 4, 8, 16, 32, 64 и 128 (рис. 2.).

Чтобы определить значение октета, нужно сложить значения позиций, где присутствует двоичная единица.

Взаимодействие IP-адресов и масок подсети

Каждый IP-адрес состоит из двух частей. Как узлы определяют, где сетевая часть, а где адрес узла? Для этого используется маска подсети.

При настройке IP узлу присваивается не только IP-адрес, но и маска подсети. Как и IP-адрес, маска состоит из 32 бит. Она определяет, какая часть IP-адреса относится к сети, а какая - к узлу.

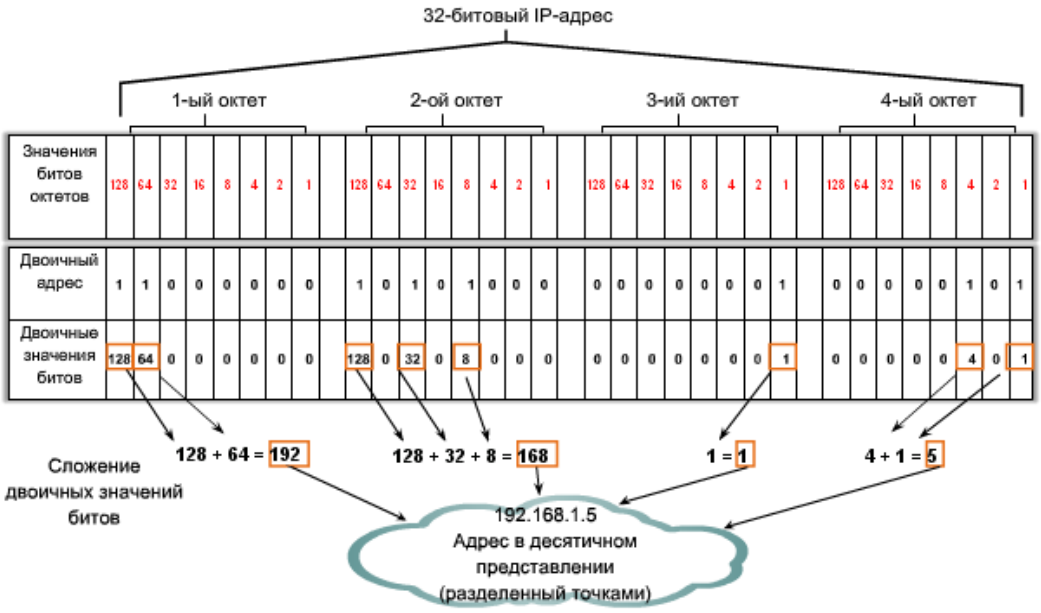


Рис. 2. Структура IP-адресов

Маска сравнивается с IP-адресом побитно, слева направо. В маске подсети единицы соответствуют сетевой части, а нули - адресу узла. В приведенном примере первые три октета представляют собой адрес сети, а последний - адрес узла.

Отправляя пакет, узел сравнивает маску подсети со своим IP-адресом и адресом получателя. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если нет, отправляющий узел передает пакет на интерфейс локального маршрутизатора для отправки в другую сеть (рис. 3.).

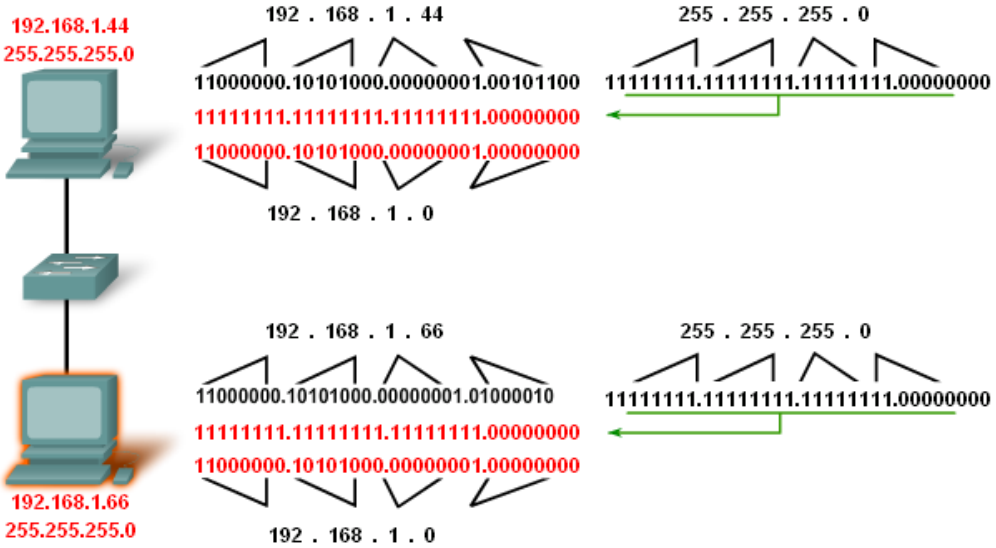


Рис. 3. Взаимодействие IP-адресов и масок подсети

В небольших компаниях чаще всего встречаются следующие маски подсети: 255.0.0.0 (8 бит), 255.255.0.0 (16 бит) и 255.255.255.0 (24 бита). В маске подсети 255.255.255.0 (десятичный вариант), 24 бита идентифицируют сеть, а 8 - узлы в сети.

Чтобы вычислить количество возможных сетевых узлов в данном случае нужно взять количество отведенных для них бит в степени 2 ($2^8 = 256$). Из полученного результата необходимо вычесть 2 (256-2). Дело в том, что состоящая из одних единиц отведенная узлам часть IP-адреса предназначена для широковещательных адресов и не может принадлежать одному узлу. Часть, состоящая только из нулей, является идентификатором сети и тоже не может быть присвоена конкретному узлу.

IP-адрес и маска подсети совместно определяют то, какая часть IP-адреса является сетевой, а какая соответствует адресу узла (рис. 4).

В адресах класса С сетевая часть состоит из трех октетов, а адрес узла - из одного. Выбранная по умолчанию маска подсети состоит из 24 битов (255.255.255.0). Адреса класса С обычно присваиваются небольшим сетям.

В адресах класса В сетевая часть и адрес узла состоят из двух октетов. Выбранная по умолчанию маска подсети состоит из 16 бит (255.255.0.0). Обычно эти адреса используются в средних сетях.

Классы IP-адресов

Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зеленые биты не меняются)	Сетевая (С) и узловая (У) части адреса	Маска подсети по умолчанию (в двоичном и десятичном формате)	Число возможных сетей и узлов для каждой сети
A	1 - 127	00000000 - 01111111	С.У.У.У	255.0.0.0 11111111.00000000.00000000.00000000	126 сетей (2^7-2) 16 777 214 узлов для каждой сети (2^24-2)
B	128 - 191	10000000 - 10111111	С.С.У.У	255.255.0.0 11111111.11111111.00000000.00000000	16 382 сетей (2^14-2) 65 534 узла для каждой сети (2^16-2)
C	192 - 223	11000000 - 11011111	С.С.С.У	255.255.255.0 11111111.11111111.11111111.00000000	2 097 150 сетей (2^21-2) 254 узла для каждой сети (2^8-2)
D	224 - 239	11100000 - 11101111	В качестве узла не для коммерческого использования		
E	240 - 255	11110000 - 11111111	В качестве узла не для коммерческого использования		

^^ Все адреса, состоящие только из нулей (0) или единиц (1), - недействительные адреса узлов.

Рис. 4. Классы IP-адресов и соответсвующие им маски подсетей

2. Подсети

Еще одним способом экономии IP-адресов, который используется наряду с уже упомянутыми выше технологиями CIDR, адресацией IPv6 и частными адресами, является механизм использования подсетей (subnetting). Этот метод позволяет разбивать полные классовые блоки сетевых адресов на меньшие и помогает избежать полного исчерпания IP-адресов.

Подсеть - это подмножество сети, не пересекающееся с другими подсетями.

Чтобы создать подсеть, сетевой администратор заимствует биты из поля адресов узлов исходного адреса всей сети и назначает их в качестве адреса подсети (табл. 3).

Минимальное число битов, которое может быть заимствовано, - два. Если использовать всего один бит, то после разбиения будет получен только один сетевой адрес (.0 - адрес сети) и один широковещательный (.255). Максимальное число битов, которые разрешено заимствовать, может быть любым (в рамках максимальной длины узловой части адреса), при условии, что останутся незадействованными не менее двух битов для адресов узлов. В табл. 3 показано, что для сети класса С может быть заимствовано не более 6 битов из поля адреса узла для создания подсети.

Таблица 3. Адреса подсетей

Первый октет адреса узла в десятичной нотации	**Количество подсетей**	**Количество узлов класса А в каждой подсети**	**Количество узлов класса В в каждой подсети**	**Количество узлов класса С в каждой подсети**
.192	2	4194302	16382	62
.224	6	2097150	8190	30
.240	14	1048574	4094	14
.248	30	524286	2046	6
.252	62	262142	1022	2
.254	126	131070	510	-
.255	254	65534	254	-

Вообще говоря, подсети придуманы для того, чтобы обойти ограничения физических сетей на число узлов в них и максимальную длину кабеля в сегменте сети. Например, сегмент тонкого Ethernet имеет максимальную длину 185 м и может включать до 32 узлов. Самая маленькая сеть - класса С - может состоять из 254 узлов. Для того чтобы достичь этой цифры, надо объединить несколько физических сегментов сети. Сделать это можно либо с помощью физических устройств (например, репитеров), либо при помощи машин-шлюзов. В первом случае разбиения на подсети не требуется, т.к. логически сеть выглядит как одно целое. При использовании шлюза сеть разбивается на подсети.

На рис. 5 изображен фрагмент сети класса В - 144.206.0.0, состоящий из двух подсетей - 144.206.130.0 и 144.206.160.0. В центре схемы изображена машина шлюз, которая связывает подсети. Эта машина имеет два сетевых интерфейса и, соответственно, два IP-адреса.

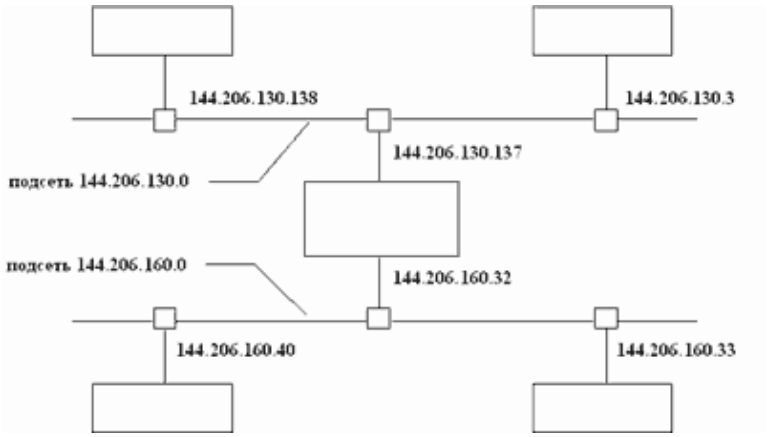


Рис. 5. Схема разбиения адресного пространства сети на подсети

В принципе, разбивать сеть на подсети необязательно. Можно использовать адреса сетей другого класса (с меньшим максимальным количеством узлов). Но при этом возникает, как минимум, два неудобства:

- В сети, состоящей из одного сегмента Ethernet, весь адресный пул сети не будет использован, т.к., например, для сети класса С (самой маленькой с точки зрения количества узлов в ней), из 254 возможных адресов можно использовать только 32;
- Все машины за пределами организации, которым разрешен доступ к компьютерам сети данной организации, должны знать шлюзы для каждой из сетей. Структура сети становится открытой во внешний мир. Любые изменения структуры могут вызвать ошибки маршрутизации. При использовании подсетей внешним машинам надо знать только шлюз всей сети организации.

Разбиение сети на подсети использует ту часть IP-адреса, которая закреплена за номерами хостов. Администратор сети может замаскировать часть IP-адреса и использовать ее для назначения номеров подсетей. Фактически, способ разбиения адреса на две части, теперь будет применяться к адресу хоста из IP-адреса сети, в которой организуется разбиение на подсети.

Маска подсети - это четыре байта, которые накладываются на IP-адрес для получения номера подсети. Например, маска 255.255.255.0 позволяет разбить сеть класса В на 254 подсети по 254 узла в каждой.

На приведенной схеме сеть класса В (номер начинается с 10) разбивается на подсети маской 255.255.224.0. При этом первые два байта задают адрес сети и не участвуют в разбиении на подсети. Номер подсети задается тремя старшими битами третьего байта маски. Такая маска позволяет получить 6 подсетей. Для нумерации подсети нельзя использовать номер 000 и номер 111. Номер 160 задает 5-ю подсеть в сети 144.206.0.0.

Для нумерования машин в подсети можно использовать оставшиеся после маскирования 13 битов, что позволяет создать подсеть из 8190 узлов. Перестроить сеть, состоящую из более чем 400 машин, не такая простая задача, так как ей управляет не один администратор, которые должны изменить маски на всех машинах сети. Ряд компьютеров работает в круглосуточном режиме и все изменения надо произвести в тот момент, когда это минимально скажется на работе пользователей сети. Данный пример показывает, насколько внимательно следует подходить к вопросам планирования архитектуры сети и ее разбиения на подсети. Многие проблемы можно решить за счет аппаратных средств построения сети.

К сожалению, подсети не только решают, но также и создают ряд проблем. Например, происходит потеря адресов, но уже не по причине физических ограничений, а по причине принципа построения адресов подсети. Как было видно из примера, выделение трех битов на адрес подсети не приводит к образованию 8-ми подсетей. Подсетей образуется только 6, так как номера сетей 0 и 7 использовать в силу специального значения IP-адресов, состоящих из 0 и единиц, нельзя. Таким образом, все комбинации адресов хоста внутри подсети, которые можно было бы связать с этими номерами, придется забыть. Чем шире маска подсети (чем больше места отводится на адрес хоста), тем больше потерь. В ряде случаев приходится выбирать между приобретением еще одной сети или изменением маски. При этом физические ограничения могут быть превышены за счет репитеров, хабов и т. п.

3. Назначение IP-адресов

Статическое назначение IP-адресов

Когда IP-адреса распределяются статически, каждое устройство обязано иметь свой адрес. Операционные системы по-разному конфигурируют стек протоколов TCP/IP. При использовании этого метода необходимо хранить записи о назначенных IP-адресах, поскольку использование дублирующихся адресов может вызвать проблемы в работе сети. Некоторые операционные системы, такие, как Windows XP и Windows NT корпорации Microsoft, рассылают ARP-запросы, проверяя уникальность назначенных адресов при попытке инициализации средств набора TCP/IP.

Если обнаружено дублирование, протокол инициализирован не будет, что вызовет соответствующее сообщение об ошибке. Не все операционные системы идентифицируют дублирующиеся адреса.

Основной причиной, по которой устройству может быть выделен постоянный адрес, является необходимость предоставить другим устройствам возможность ссылаться на него. Хорошим примером может служить Web-сервер. Если бы Web-сервер каждый раз при запуске получал новый IP-адрес, его было бы сложно найти.

У статических адресов есть несколько преимуществ. Например, их полезно присваивать принтерам, серверам и другим сетевым устройствам, которые всегда должны быть доступны сетевым клиентам. Если обычно узлы подключаются к серверу с определенным IP-адресом, ничего хорошего не будет в том, что он изменится (рис. 6)

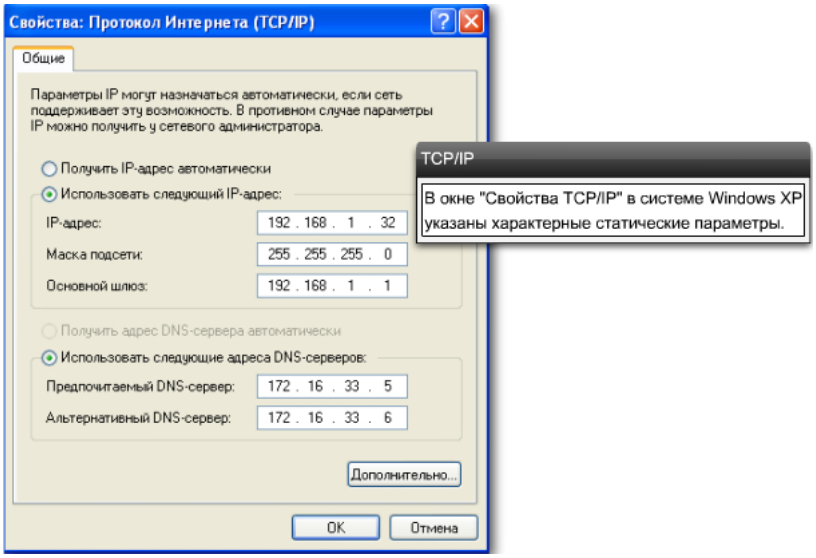


Рис. 6. Статическое назначение IP-адресов

Статическое присвоение адресов усиливает контроль над сетевыми ресурсами, но ввод информации для каждого узла отнимает много времени. При статическом вводе узел выполняет только базовый поиск ошибок в IP-адресе. Соответственно, риск возникновения ошибки больше.

При использовании статической IP-адресации важно вести точный перечень адресов и устройств, которым они присвоены.

Кроме того, обычно эти постоянные адреса повторно не используются.

Назначение IP-адресов по протоколу RARP

Протокол определения сетевого адреса по местоположению узла (Reverse Address Resolution Protocol - RARP) устанавливает соответствие между MAC-адресами и IP-адресами. Такая привязка позволяет некоторым сетевым устройствам инкапсулировать данные до их отправки через сеть. Возможна ситуация, когда сетевому устройству или рабочей станции известен MAC-адрес, но не известен собственный IP-адрес.

Для устройств, использующих протокол RARP, требуется присутствие RARP-сервера, как показано на рис. 7.

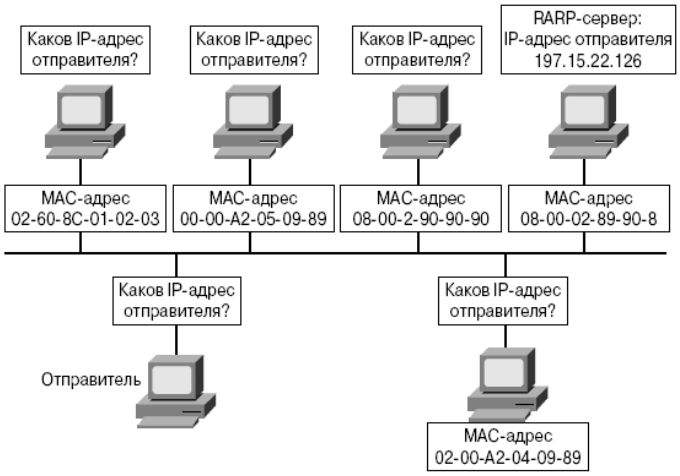


Рис. 7. Назначение IP-адресов с помощью протокола RARP

Рассмотрим пример, в котором устройство-отправитель передает данные некоторому устройству. Отправитель знает MAC-адрес получателя, но не может найти собственный IP-адрес в ARP-таблице. С другой стороны, устройству получателю, чтобы принять данные, передать их протоколам верхнего уровня модели OSI и ответить отправителю, должны быть известны как MAC, так и IP-адрес отправителя. Поэтому отправитель инициирует процесс, называемый RARP-запросом, который поможет определить ему свой IP-адрес. Устройство создает пакет RARP-запроса (рис. 8) и отправляет его через сеть. Для того чтобы все устройства в сети могли получить пакеты RARP-запроса, используется широковещательный MAC-адрес.

0-15 битов		16-31 битов
Аппаратный тип		Тип протокола
HLen (1 байт)	Plen (1 байт)	Операция
HA отправителя (Байтов 1-4)		
HA отправителя (5-6 байта)		PA отправителя (1-2 байта)
PA отправителя (3-4 байта)		HA получателя (1-2 байта)
HA получателя (3-6 байт)		
PA получателя (1-4 байта)		
Структура заголовка RARP		

Рис. 8. Структура сообщений ARP/RARP

Составные части заголовка RARP:

- **аппаратный тип (Hardware type**) задает тип аппаратного интерфейса, для которого отправитель ожидает ответ;
- **тип протокола (Protocol type**) задает тип адреса для протокола верхнего уровня;
- **поле Hlen (сокращение от Hardware length)** - длина аппаратного адреса;
- **поле Plen (сокращение от Protocol length)** - длина адреса соответствующего протокола;
- **поле Operation** операция; может принимать следующие значения:
    1. ARPзапрос,
    2. ARPответ,
    3. RARPзапрос,
    4. RARPответ,
    5. динамический RARPзапрос,

6. динамический RARPответ,
7. сообщение об ошибке динамического протокола RARP,
8. InARPзапрос,
9. InARPответ;

- **Sender HA** (**Sender Hardware Address**) аппаратный адрес отправителя, который имеет длину, равную HLen байтам;
- **Sender PA** (**Sender Port Address**) - протокольный адрес отправителя, который имеет длину, равную PLen байтам;
- **Target HA** (**Target Hardware Address**) - аппаратный адрес получателя, который имеет длину, равную HLen байтам;
- **Target PA** (**Target Port Address**) - протокольный адрес получателя, который имеет длину, равную PLen байтам.

Рис. 9. Схема работы протокола RARP

Протокол RARP использует тот же формат пакета, что и протокол ARP. Однако значения MAC-заголовка и кода операции для RARP-запроса отличаются от аналогичных полей ARP-запроса. Формат пакета RARP содержит позиции для MAC-адресов отправителя и получателя, поле IP-адреса отправителя пусто. Широковещательный запрос адресуется всем абонентам в сети, для этого адрес получателя состоит из одних единиц.

Станция, использующая протокол RARP, содержит в своем ПЗУ программный код, который запускает процесс поиска адреса RARP (рис. 9).

Динамические адреса

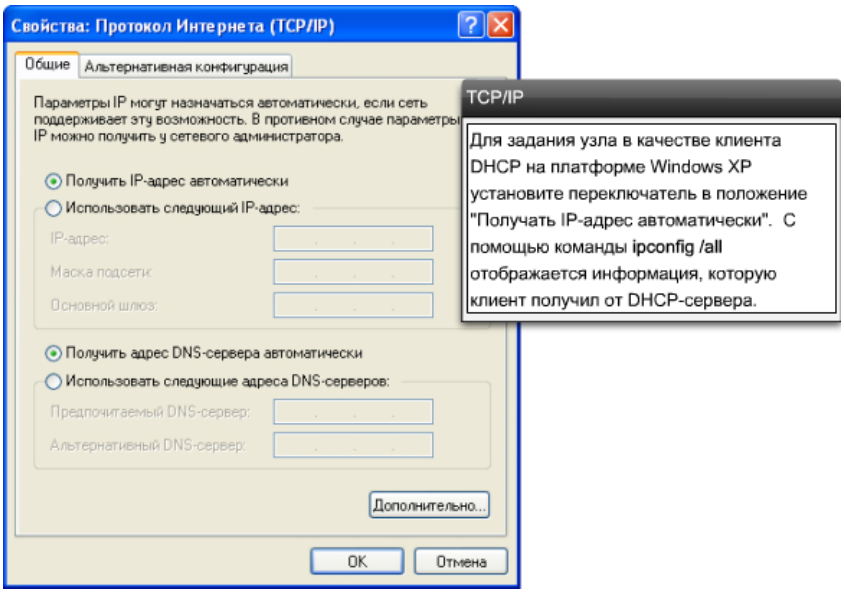


Рис. 10. Динамическое назначение IP-адресов

Список пользователей локальной сети часто меняется. Появляются новые пользователи с ноутбуками, которые нужно подключить. Другие устанавливают новые рабочие станции. Чтобы каждой станции не приходилось вручную присваивать IP-адреса, проще всего это сделать автоматически. Для этого используется протокол под названием Dynamic Host Configuration Protocol (DHCP).

DHCP предусматривает механизм автоматического присвоения информации об адресе, например, IP-адреса, маски подсети, шлюза по умолчанию и других настроек (рис. 10).

Это наиболее предпочтительный способ присвоения IP-адресов узлам в большой сети, поскольку он облегчает работу специалистов службы поддержки и практически устраняет возможность ошибки.

Другое преимущества DHCP состоит в том, что адреса присваиваются узлам временно. Если узел выключается или уходит из сети, его адрес возвращается в пул для повторного использования. Это особенно полезно для мобильных пользователей, которые, то подключаются, то отключаются.

Выделение адресов с помощью протокола DHCP

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol - DHCP) позволяет динамически получить IP-адрес, не прибегая к создаваемым администратором профилям для каждой конкретной машины. Все, что нужно, - это назначить диапазон доступных адресов на DHCP-сервере. Соединяющиеся с сетью узлы подключаются к DHCP-серверу и запрашивают необходимые им IP-адреса. Сервер выбирает один из незанятых адресов и выделяет его узлу. С помощью протокола DHCP вся необходимая информация о конфигурации протокола TCP/IP может быть передана клиенту в одном сообщении.

В качестве серверов DHCP могут выступать самые разные устройства при условии, что на них установлено служебное ПО DHCP. В большинстве средних и крупных сетей сервер DHCP - это локальный выделенный сервер на базе ПК (рис. 11).

В домашних сетях он обычно находится у Интернет-провайдера. Узел из домашней сети получает настройки IP непосредственно от Интернет-провайдера.

Во многих домашних и небольших корпоративных сетях для подключения к модему Интернет-провайдера используется встроенный маршрутизатор. В данном случае он выступает в качестве клиента и сервера DHCP. В качестве клиента он получает настройки IP от Интернет-провайдера, а затем, уже как сервер DHCP, передает их внутренним узлам локальной сети.

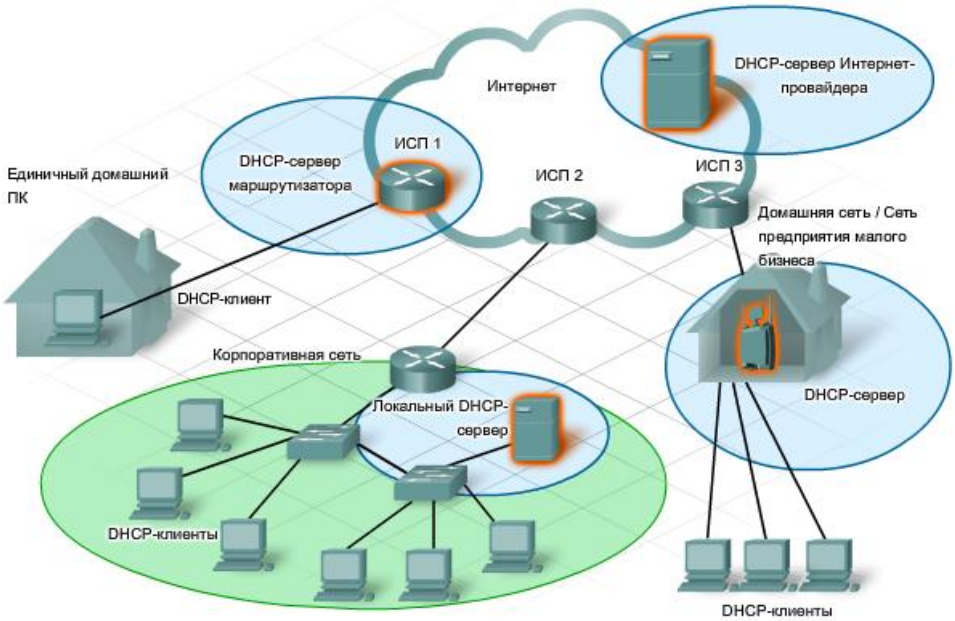


Рис. 11. Выделение адресов с помощью протокола DHCP

Основное преимущество протокола DHCP заключается в том, что этот протокол дает пользователям мобильность. Они могут свободно перемещаться с места на место, меняя точку подключения к сети. При использовании сервера DHCP больше нет необходимости в создании жестких профилей для каждого сетевого устройства. Такая гибкость достигается благодаря тому, что протокол DHCP может выделять IP-адрес одному устройству, а после его освобождения - передавать другому. Такой механизм работы означает, что для IP-адресов выполняется отношение «один ко многим» и, следовательно, адрес может быть доступен любому устройству, подключенному к сети.

Проблемы при определении адресов

Одной из основных проблем сетевых технологий является вопрос о том, как организовать взаимодействие между сетевыми устройствами. В TCP/IP-взаимодействиях дейтаграмма в локальной сети обязана содержать как MAC-адрес, так и IP-адрес получателя. На рис. 12 компьютер с адресом 176.10.16.1 хочет передать информацию компьютеру с адресом 176.10.16.4.

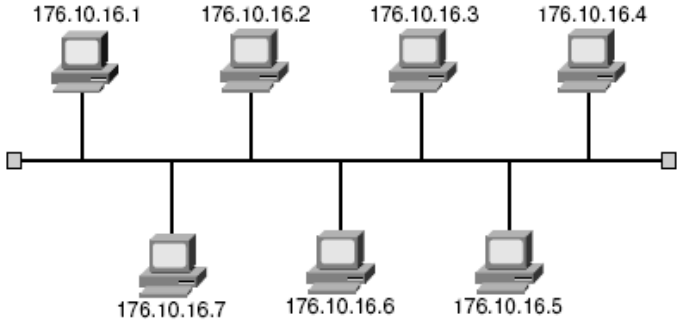


Рис. 12. Проблемы преобразования адресов

Каким же образом он получает необходимый для такого обмена данными MAC-адрес?

Все адреса должны быть корректными и в точности соответствовать MAC- и IP-адресу узла, в противном случае получатель просто отвергнет неправильные пакеты.

Таким образом, в локальной сети должен существовать механизм автоматического разрешения (или трансляции) IP-адресов в адреса физического уровня - MAC.

Выполнить такую задачу вручную было бы для пользователей обременительно и потребовало бы много времени. Такое решение применимо только для локальных сетей; в случае, когда данные адресуются за пределы локальной сети, появляются новые проблемы.

При взаимодействии с устройствами, не находящимися в локальном сетевом сегменте, возникают два вопроса:

- как получить MAC-адреса промежуточных устройств;
- как передавать пакеты с данными из одного сетевого сегмента в другой до тех пор, пока они не достигнут получателя.

Пример, приведенный на рис. 13, служит иллюстрацией такой проблемы. Компьютеру с адресом 192.168.10.34 необходимо передать информацию другому компьютеру с адресом 192.168.1.1. Каким образом он может получить MAC-адрес для IP-адреса 192.168.1.1? Следует помнить, что MAC-адрес может быть использован только в пределах локальной сети. От него будет мало пользы вне сети с адресом 192.168.10.0. Значит, для того чтобы передать данные из локальной сети в сеть глобальную, необходимо знать MAC-адрес маршрутизатора.

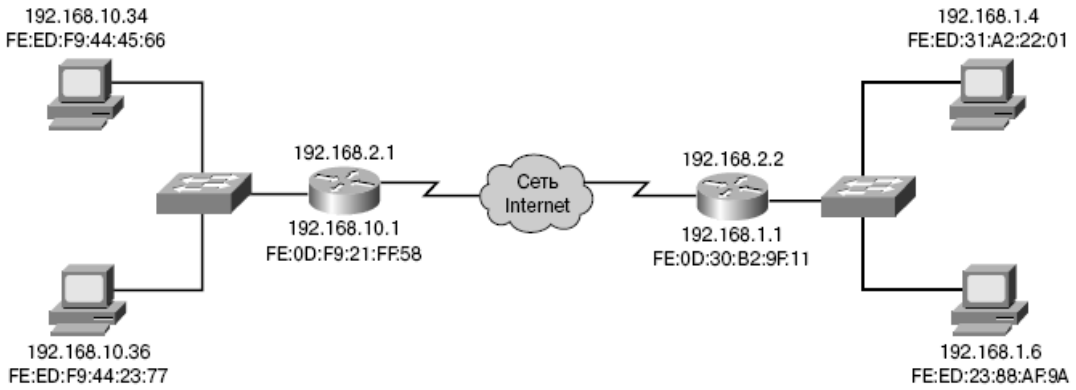


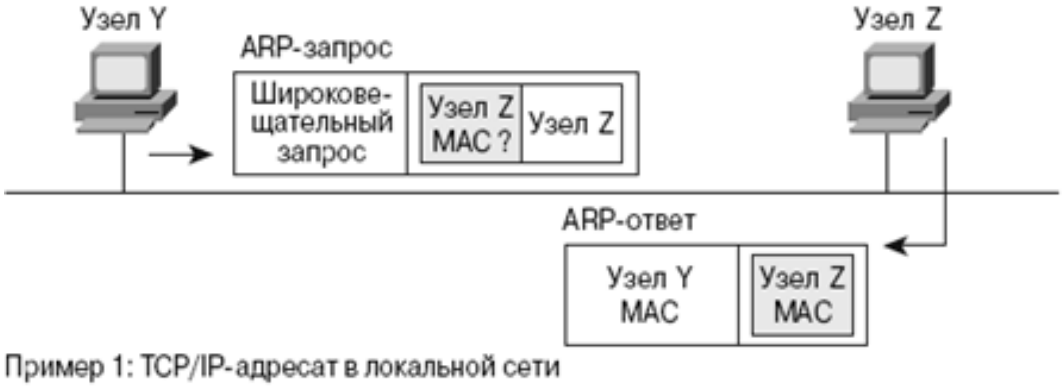
Рис. 13. Проблемы преобразования удаленных адресов

Протокол преобразования адресов (ARP)

Для взаимодействия устройств друг с другом необходимо, чтобы у передающего устройства был IP- и MAC-адреса получателя. Когда одно из устройств пытается установить связь с другим, с известным IP-адресом, ему необходимо определить MAC-адрес получателя. Набор протоколов TCP/IP имеет в своем составе специальный протокол, называемый ARP (Address Resolution Protocol - протокол преобразования адресов), который позволяет автоматически получить MAC-адрес. На рис. 14 проиллюстрирован процесс, позволяющий определить MAC-адрес, связанный с известным IP-адресом.

Некоторые устройства хранят специальные ARP-таблицы, в которых содержится информация о MAC- и IP-адресах других устройств, подключенных к той же локальной сети. ARP-таблицы позволяют установить однозначное соответствие между IP- и MAC-адресами. Такие таблицы хранятся в определенных областях оперативной памяти и обслуживаются автоматически на каждом из сетевых устройств (табл. 1 и 2). В редких случаях приходится создавать ARP-таблицы вручную.

Обратите внимание, что каждый компьютер в сети поддерживает свою собственную ARP-таблицу.



Пример 1: TCP/IP-адресат в локальной сети

Рис. 14. Получение IP-адресов через MAC-адреса

Таблица 1. Запись в ARP-таблице

Internet-адрес	**Физический адрес**	**Тип**
68.2.168.1	00-50-57-00-76-84	Динамический

Таблица 2. ARP-таблица для адреса 198.150.11.36

MAC-адрес	**IP-адрес**
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Куда бы ни передавались сетевым устройством данные, для их пересылки всегда используется информация, хранящаяся в ARP-таблице (рис. 15; одно из устройств хочет передать данные другому устройству).

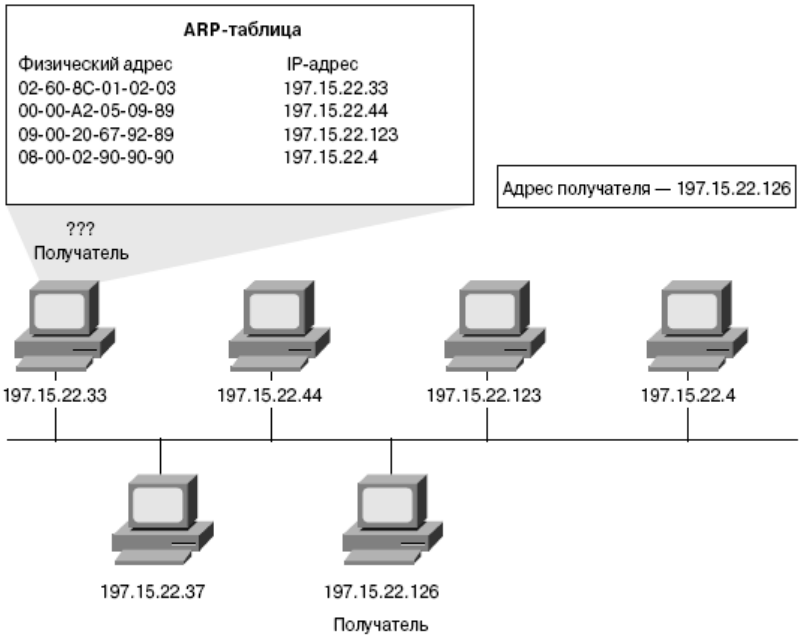


Рис. 15. ARP-таблицы

Функционирование протокола ARP в подсетях

Для передачи данных от одного узла другому отправитель должен знать IP- и MAC-адрес получателя. Если он не может получить искомый физический адрес из собственной ARP-таблицы, инициируется процесс, называемый ARP-запросом.

ARP-запрос позволяет узлу определить MAC-адрес получателя. Узел создает фрейм ARP-запроса и рассылает его всем сетевым устройствам. Фрейм ARP-запроса состоит из двух частей:

- заголовка фрейма;
- сообщения ARP-запроса.

Для того чтобы все устройства могли получить ARP-запрос, используется широковещательный MAC-адрес. В схеме MAC-адресации широковещательный адрес содержит во всех битах шестнадцатеричное число F и имеет, таким образом, вид FF_FF_FF_FF_FF_FF. Поскольку пакеты ARP-запроса передаются в широковещательном режиме, все сетевые устройства, подключенные к локальной сети, могут получить такие пакеты и передать их протоколам более высоких уровней для последующей обработки. Если IP-адрес устройства совпадает с IP-адресом получателя в широковещательном ARP-запросе, это устройство отвечает отправителю, сообщая свой MAC-адрес. Такое сообщение называется ARP-ответом.

После получения ARP-ответа устройство-отправитель широковещательного ARP-запроса извлекает MAC-адрес из поля аппаратного адреса отправителя и обновляет свою ARP-таблицу. Теперь это устройство может надлежащим образом адресовать пакеты, используя как MAC-, так и IP-адрес. Полученная информация используется для инкапсуляции данных на втором и третьем уровнях перед их отправкой по сети. Когда данные достигают пункта назначения, на канальном уровне проводится проверка на соответствие адреса, отбрасывается канальный заголовок, который содержит MAC-адреса, и данные передаются на сетевой уровень. На сетевом уровне проверяется соответствие собственного IP-адреса и IP-адреса получателя, содержащегося в заголовке третьего уровня. На сетевом уровне отбрасывается IP-заголовок, и инкапсулированные данные передаются на следующий уровень модели OSI - транспортный (уровень 4). Подобный процесс повторяется до тех пор, пока оставшиеся, частично распакованные, данные не достигнут приложения (уровень 7), в котором будет прочитана пользовательская часть данных.

Контрольные вопросы

1. В чем заключается основная задача IP-адресов?
2. Как определяется значение октетов IP-адресов?
3. Какие функции выполняет маска подсети?
4. Каким образом происходит деление сети на подсети?
5. Каким образом может быть назначен IP-адрес для оборудования в сети?

Лекция 12
Адресация в корпоративных сетях

1. **Управление адресами**
2. **Присвоение адреса**
3. **Адреса одноадресных, многоадресных и широковещательных рассылок**
4. **Использование схемы адресации иерархической IP-сети**
5. **Маска подсети переменной длинны (VLSM)**

Ключивые слова: управление адресами, DHCP сервер, стандартный шлюз, частный адрес, маршрутизатор, модем, рассылка, иерархическая сеть, подсеть, VLSM.

1. Управление адресами

Маршрутизатор создает шлюз, через который узлы одной сети могут обмениваться данными с узлами других сетей. Каждый интерфейс маршрутизатора подключается к отдельной сети.

Присвоенный интерфейсу IP-адрес идентифицирует непосредственно подключенную локальную сеть.

Каждый узел в сети обязательно использует в качестве шлюза в другие сети маршрутизатор. Соответственно, каждый узел должен знать IP-адрес интерфейса маршрутизатора, подключенного к его сети. Он называется адресом шлюза по умолчанию. Адрес можно статически настроить на уровне узла или получить динамически, с сервера DHCP.

Когда встроенный маршрутизатор превращается в сервер DHCP локальной сети, он автоматически рассылает всем узлам IP-адреса нужного интерфейса.

После этого все узлы в сети смогут использовать этот IP-адрес для передачи сообщений узлам Интернет-провайдера и получения доступа к узлам в Интернете. Обычно встроенные маршрутизаторы по умолчанию становятся серверами DHCP.

IP-адрес данного интерфейса локального маршрутизатора становится адресом шлюза по умолчанию в данной конфигурации узлов. Шлюз по умолчанию предоставляется статически или через DHCP.

Становясь сервером DHCP, встроенный маршрутизатор предоставляет клиентам DHCP свой внутренний IP-адрес в качестве шлюза по умолчанию. Кроме того, он рассылает узлам IP-адреса и маски подсети (рис. 1).

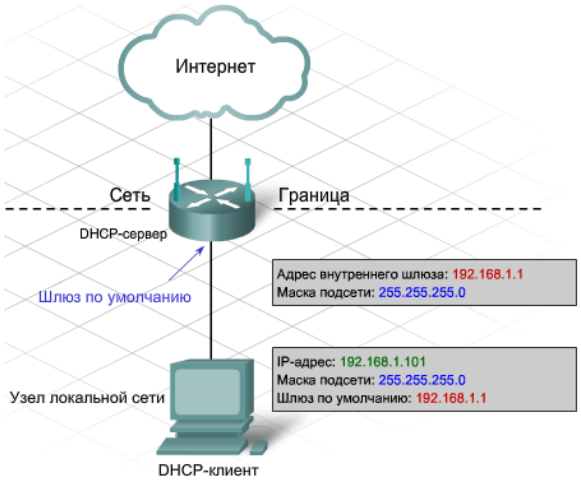


Рис. 1. Предоставление адресов DHCP сервером

Стандартный шлюз

Стандартным шлюзом называется IP-адрес интерфейса маршрутизатора, подключенного к локальной сети, в которой находится передающий узел. IP-адрес стандартного шлюза должен находиться в том же сетевом сегменте, в котором находится передающий узел (рис. 2).

Рис. 2. Стандартный шлюз

2. Присвоение адреса

Интегрированный маршрутизатор выступает в качестве сервера DHCP всех подключенных к нему кабелем Ethernet или по беспроводной связи локальных узлов. Считается, что эти узлы находятся во внутренней сети. Большинство серверов DHCP присваивают узлам из внутренней сети не маршрутизируемые общие адреса Интернет, а частные адреса. Это означает, что по умолчанию внутренняя сеть непосредственно из Интернета недоступна.

Обычно выбранный по умолчанию IP-адрес интерфейса локального встроенного маршрутизатора является частным адресом класса С. Внутренним узлам нужно присвоить адреса сети, в которой находится встроенный маршрутизатор (статически или через DHCP). Встроенный маршрутизатор, работающий как сервер DHCP, предоставляет адреса из этого диапазона. Кроме того, он предоставляет данные о маске подсети и IP-адресе своего интерфейса (шлюз по умолчанию).

Кроме того, многие Интернет-провайдеры с помощью серверов DHCP предоставляют IP-адреса для прямого выхода встроенного маршрутизатора пользователя в Интернет. Сеть, к которой маршрутизатор подключен в Интернете, называется внешней.

Подключенный к Интернет-провайдеру встроенный маршрутизатор работает как клиент DHCP, получая правильный IP-адрес внешней сети для интерфейса Интернет. Обычно Интернет-провайдер предоставляет маршрутизируемый в Интернете адрес, с помощью которого узлы могут подключаться к встроенному маршрутизатору и к Интернету.

Маршрутизатор разграничивает локальную внутреннюю сеть и внешнюю сеть (рис. 3.).

Узлы могут подключаться к Интернет-провайдеру и Интернету несколькими способами. Получение общего или частного адреса зависит от метода подключения узла.

Прямое подключение

У некоторых клиентов есть только один компьютер с непосредственным подключением к Интернет-провайдеру через модем. В данном случае общий адрес с сервера DHCP Интернет-провайдера присваивается только одному узлу.

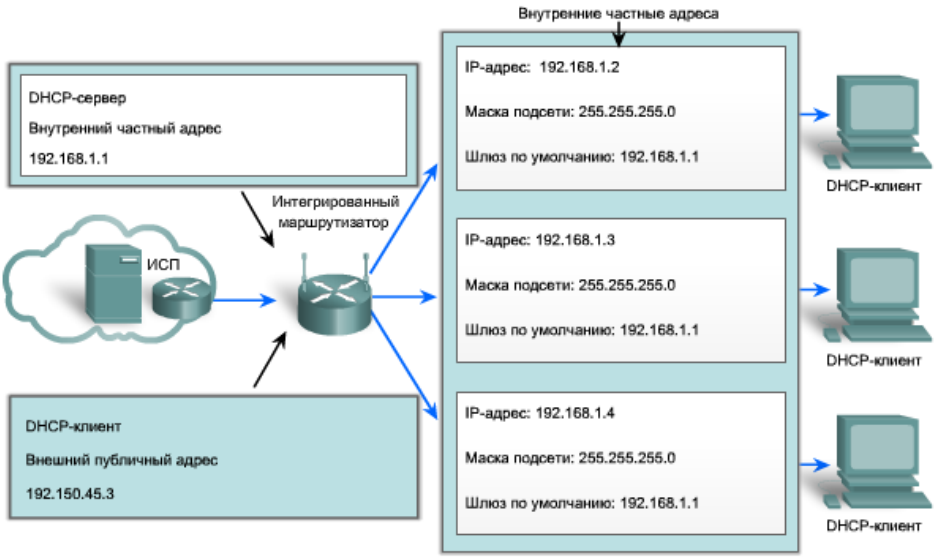


Рис. 3. Разграничение сети на локальную внутреннюю сеть и внешнюю сеть

Подключение через встроенный маршрутизатор

Если к Интернету нужно подключить несколько узлов, модем Интернет-провайдера можно соединить не с одним компьютером, а непосредственно со встроенным модемом. Таким образом создается домашняя или небольшая корпоративная сеть. Встроенный маршрутизатор получает от Интернет-провайдера общие адреса. Внутренние узлы получают от маршрутизатора частные адреса.

Подключение через шлюз

Шлюзы объединяют в себе встроенный маршрутизатор и модем и подключаются непосредственно к Интернет-провайдеру. Как и в случае со встроенными маршрутизаторами, шлюз получает от Интернет-провайдера общий адрес, а ПК во внутренней сети получают от шлюза частные адреса (рис. 4).

Рис. 4. Подключение через шлюз

3. Адреса одноадресных, многоадресных и широковещательных рассылок

Помимо классов, IP-адреса делятся на категории, предназначенные для одноадресных, широковещательных или многоадресных рассылок. С помощью IP-адресов узлы могут обмениваться данными в режиме «один к одному» (одноадресная пересылка), «один ко многим»; (многоадресная рассылка) или «один ко всем» (широковещательная рассылка).

Одноадресная рассылка

Адрес одноадресной рассылки чаще всего встречается в сети IP. Пакет с одноадресным получателем предназначен конкретному узлу. Пример: узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200 (адресат) (рис. 5)

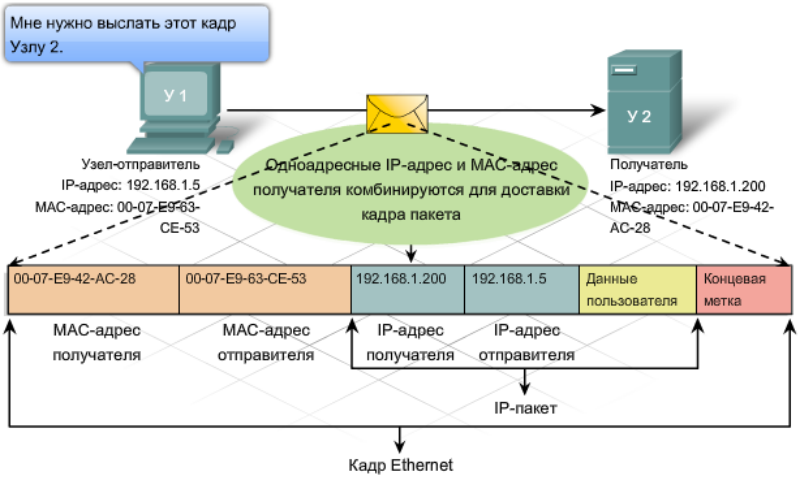


Рис. 5. Одноадрессная рассылка

Для отправки и приема одноадресного пакета IP-адрес получателя должен находиться в заголовке IP-пакета. Кроме того, в заголовке кадра Ethernet должен быть MAC-адрес получателя. IP-адрес и MAC-адрес - это данные для доставки пакета одному узлу.

Широковещательная рассылка

В пакете широковещательной рассылки содержится IP-адрес получателя, где в отведенной узлу части есть только единицы (1). Это означает, что пакет получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих Интернет-протоколах, например, ARP и DHCP (рис. 6).

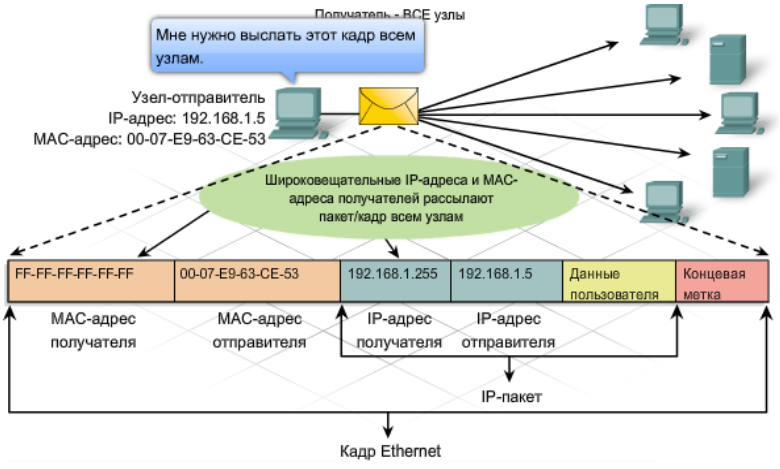


Рис. 6. Широковещательная рассылка

В сети класса C 192.168.1.0 с маской подсети по умолчанию 255.255.255.0 используется адрес широковещательной рассылки 192.168.1.255. В отведенной узлу части стоит 255, или двоичное 11111111.

В сети класса B 172.16.0.0 с маской подсети по умолчанию 255.255.0.0 используется адрес широковещательной рассылки 172.16.255.255.

В сети класса A 10.0.0.0 с маской подсети по умолчанию 255.0.0.0 используется адрес широковещательной рассылки 10.255.255.255.

Для сетевого IP-адреса широковещательной рассылки нужен соответствующий MAC-адрес в кадре Ethernet. В сетях Ethernet используется широковещательный MAC-адрес из 48 единиц, который в шестнадцатеричном формате выглядит как FF-FF-FF-FF-FF-FF.

Многоадресная рассылка

Адреса многоадресных рассылок позволяют источнику рассылать пакет группе устройств.

Устройства, принадлежащие к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов - от 224.0.0.0 до 239.255.255.255. Поскольку адреса многоадресных рассылок соответствуют группам адресов (которые иногда называются группами узлов), они используются только как адресаты пакета. У отправителя всегда одноадресный адрес (рис. 7).

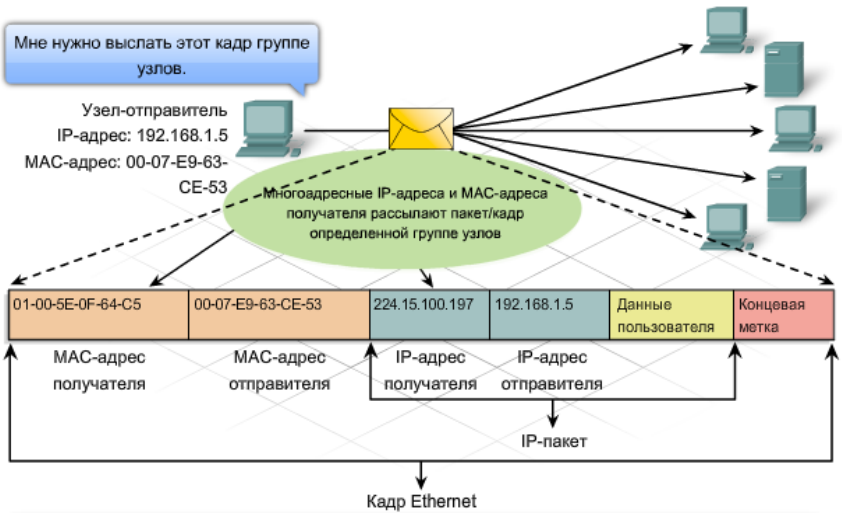


Рис. 7. Многоадресная рассылка

Как и одноадресным и широковещательным адресам, IP-адресам многоадресной рассылки нужен соответствующий MAC-адрес, позволяющий доставлять кадры в локальной сети. Многоадресный MAC-адрес - это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E. Нижние 23 бита IP-адреса многоадресной группы преобразуются в остальные 6 шестнадцатеричных символов адреса Ethernet.

4. Использование схемы адресации иерархической IP-сети

При использовании большого числа узлов плоская сеть становится менее эффективной. По мере увеличения числа узлов в коммутируемой сети увеличивается число передаваемых и получаемых широковещательных рассылок. Пакеты широковещательных рассылок занимают большую часть полосы пропускания, что приводит к задержкам при передаче трафика и тайм-аутам.

Решение - реализация иерархической сети с использованием маршрутизаторов (рис. 8).

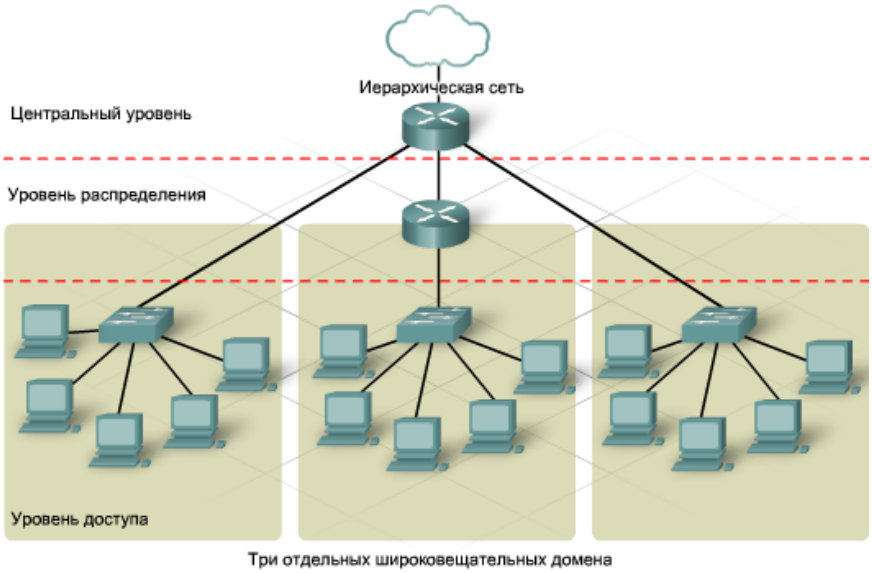


Рис. 8. Иерархическая сеть

Адресация в иерархических сетях

Большие корпоративные сети выигрывают от внедрения модели иерархической сети и соответствующей структуры адресов. Структура иерархической адресации логически делит сети на менее крупные подсети.

Эффективная схема иерархической адресации состоит из адреса классовой сети на центральном уровне, который подразделяется на менее крупные подсети на уровнях распределения и доступа (рис. 9).

Можно использовать иерархическую сеть без использования иерархической адресации. Хотя сеть продолжает функционировать, эффективность конструкции сети снижается, а определенные функции протокола маршрутизации работают некорректно.

В корпоративной сети, охватывающей множество географически разбросанных подразделений, модель и структура адресов иерархической сети упрощает управление сетью и устранение неисправностей, а также повышает масштабируемость и эффективность маршрутизации.

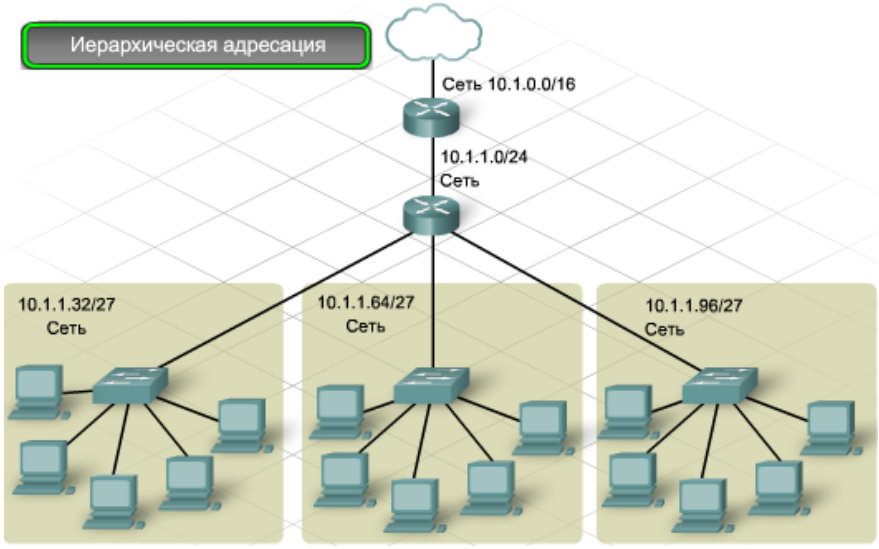
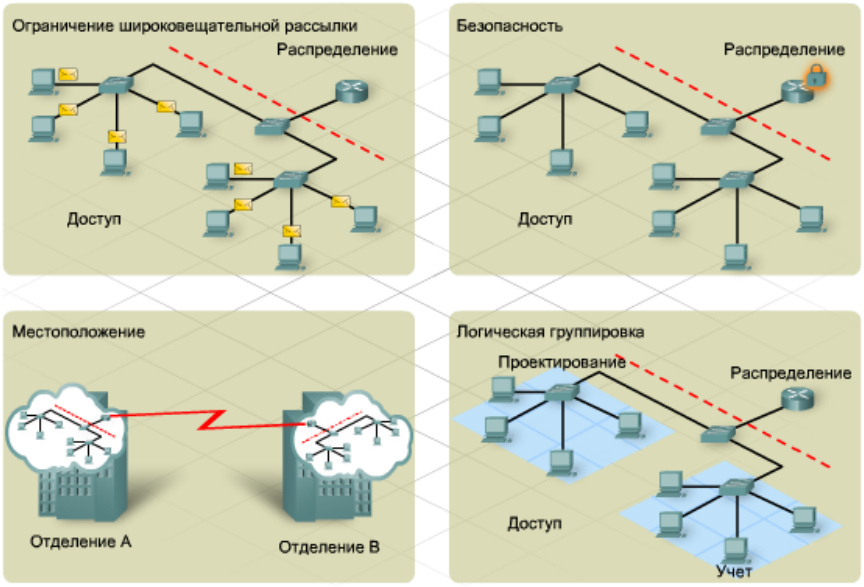


Рис. 9. Иерархичсекая адресация

Существует много причин разделить сеть на подсети, включая (рис. 10):

- физическое местоположение;
- логическую группировку;
- безопасность;
- требования приложений;
- ограничение широковещательной рассылки;
- модель иерархической сети.



Например, если в организации используется сеть 10.0.0.0 для всего предприятия, можно использовать схему адресации 10.X.Y.0, где X соответствует географическому местоположению, а Y - зданию или этажу в этом месте. Эта схема адресации позволяет использовать:

- 255 разных географических местоположений;

Рис. 10. Причины разделения сети на подсети

- 255 зданий в каждом местоположении;
- 254 узла в каждом здании.

Чтобы использовать разделение сети на подсети для создания иерархической модели, необходимо четко понимать структуру маски подсети.

Маска подсети указывает, находятся ли узлы в одной и той же сети. Маска подсети - это 32-битное значение для различения битов сети и битов узлов. Она состоит из строки единиц, за которой следует строка нулей. Единицы соответствуют сети, а нули - узлу.

В адресах класса А используется маска подсети по умолчанию вида 255.0.0.0 или запись с косой чертой вида /8.

В адресах класса В используется маска по умолчанию вида 255.255.0.0 или /16.

В адресах класса С используется маска по умолчанию вида 255.255.255.0 или /24.

Запись /x означает число битов в маске подсети, составляющую сетевую часть адреса.

В корпоративной сети маски подсети различаются длиной. Сегменты сети ЛВС часто содержат разное число узлов, следовательно, неэффективно использовать маску подсети одной и той же длины для всех создаваемых подсетей.

Процесс базового разбиения на подсети

Используя схему иерархической адресации, можно многое узнать, глядя на IP-адрес и запись маски подсети косой чертой (/x). Например, IP-адрес 192.168.1.75 /26 содержит следующие сведения:

Десятичная маска подсети

Обозначение /26 означает маску подсети 255.255.255.192.

Число создаваемых подсетей

Предположим, что мы начали с маски подсети по умолчанию /24, то тогда 2 дополнительных бита узла заимствованы для сети. Это позволяет создать 4 подсети (2^2 = 4).

Используя схему иерархической адресации, можно многое узнать, глядя на IP-адрес и запись маски подсети косой чертой (/x). Например, IP-адрес 192.168.1.75 /26 содержит следующие сведения:

Десятичная маска подсети

Обозначение /26 означает маску подсети 255.255.255.192.

Число создаваемых подсетей

Предположим, что мы начали с маски подсети по умолчанию /24, то тогда 2 дополнительных бита узла заимствованы для сети. Это позволяет создать 4 подсети (2^2 = 4).

Используя схему иерархической адресации, можно многое узнать, глядя на IP-адрес и запись маски подсети косой чертой (/x). Например, IP-адрес 192.168.1.75 /26 содержит следующие сведения:

Десятичная маска подсети

Обозначение /26 означает маску подсети 255.255.255.192.

Число создаваемых подсетей

Предположим, что мы начали с маски подсети по умолчанию /24, то тогда 2 дополнительных бита узла заимствованы для сети. Это позволяет создать 4 подсети (2^2 = 4).

Схема адресации: пример 4-х сетей

Подсеть	Сетевой адрес	Диапазон адресов узлов	Широковещательный адрес
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

5. Маска подсети переменной длинны (VLSM)

Базового разбиения на подсети достаточно для небольших сетей, но оно не обеспечивает гибкости, необходимой для крупных корпоративных сетей.

Маски подсети переменной длины (VLSM) обеспечивают эффективное использование адресного пространства. Они также позволяют использовать иерархическую IP-адресацию, за счет которой маршрутизаторы могут эффективно применять суммирование маршрутов. Суммирование маршрутов снижает размер таблиц маршрутизации в распределительных и основных маршрутизаторах. При уменьшении размера таблиц маршрутизации ЦПУ требуется меньше времени для поиска маршрутов.

VLSM - это концепция, используемая при разделении подсети на подсети. Они были изначально разработаны для повышения эффективности адресации. С внедрением частной адресации основное преимущество VLSM в настоящее время - организация и объединение.

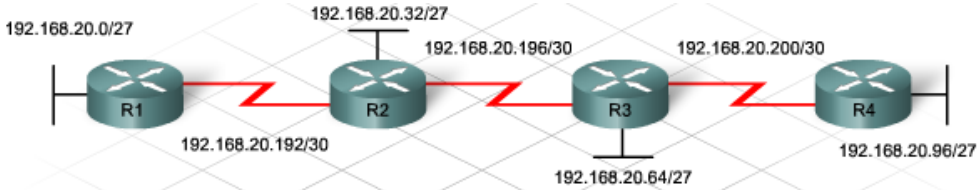
VLSM поддерживается не всеми протоколами маршрутизации. Классовые протоколы маршрутизации не включают поле маски подсети на обновление маршрутизации. Если маска

подсети назначена интерфейсу маршрутизатора, он считает, что всем пакетам одного класса назначена одна и та же маска подсети (рис. 11).

Бесклассовые протоколы маршрутизации поддерживают использование VLSM, поскольку маска подсети передается со всеми пакетами с обновлением маршрутизации. К бесклассовым протоколам маршрутизации относятся RIPv2, EIGRP и OSPF.

Преимущества VLSM:

- позволяет эффективно использовать адресное пространство;
- позволяет использовать маски подсети разной длины;
- разбивает блок адресов на менее крупные блоки;
- позволяет суммировать маршруты;
- обеспечивает большую гибкость при конструировании сети;
- поддерживает иерархические корпоративные сети.



Подсети 192.168.20.0	
Номер подсети	Адрес подсети
Подсеть 0	192.168.20.0/27
Подсеть 1	192.168.20.32/27
Подсеть 2	192.168.20.64/27
Подсеть 3	192.168.20.96/27
Подсеть 4	192.168.20.128/27
Подсеть 5	192.168.20.160/27
Подсеть 6	192.168.20.192/27
Подсеть 7	192.168.20.224/27

Подсети подсети 192.168.20.192	
Номер подсети	Адрес подсети
Подсеть 0	192.168.20.192/30
Подсеть 1	192.168.20.196/30
Подсеть 2	192.168.20.200/30
Подсеть 3	192.168.20.204/30
Подсеть 4	192.168.20.208/30
Подсеть 5	192.168.20.212/30
Подсеть 6	192.168.20.216/30
Подсеть 7	192.168.20.220/30

Рис. 11. Расбиение на подсети при помощи VLSM

VLSM позволяет использовать для каждой подсети свою маску. После разделения сетевого адреса на подсети при дальнейшем дроблении этих подсетей создаются под-подсети.

Например, сеть 10.0.0.0/8 с маской подсети /16 делится на 256 подсетей, каждая из которых может поддерживать 16 382 узла (рис. 12).

10.0.0.0/16

10.1.0.0/16

10.2.0.0/16 до 10.255.0.0/16

Рис.12. Разбиение на подсети с маской /16

Применив маску подсети /24 к любой из этих подсетей /16 (например, 10.1.0.0/16), можно получить разбиение на 256 подсетей. В каждой из этих новых подсетей можно поддерживать 254 узла (рис. 13).

10.1.1.0/24
10.1.2.0/24
10.1.3.0/24 до 10.1.255.0/24

Рис. 13. Разбиение на подсети с маской /24

Применив маску подсети /28 к любой из этих подсетей /24 (например, 10.1.3.0/28), можно получить разбиение на 16 подсетей. В каждой из этих новых подсетей можно поддерживать 14 узлов (рис. 14).

10.1.3.0/28
10.1.3.16/28
10.1.3.32/28 до 10.1.3.240/28

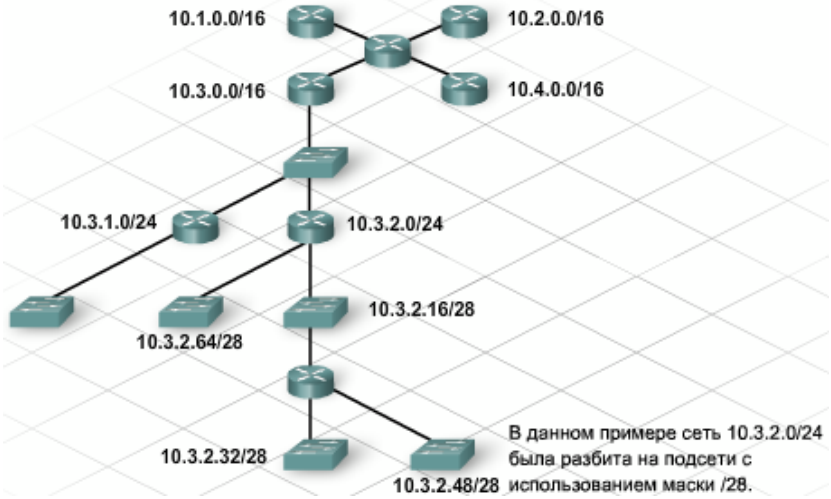


Рис. 14. Разбиение на подсети с маской /28

Контрольные вопросы

1. Какими способами осуществляется управление IP-адресами?
2. Что такое стандартный шлюз и какие требования к нему предъявляются?
3. Какие категории IP-адресов существуют?
4. Каким образом назнасаются IP-адреса в иерархических сетях?
5. Что такое VLSM и в каких случаях они используется?

Лекция 13
Технологии Ethernet

1. **Метод доступа CSMA/CD**
2. **Технология Ethernet и эталонная модель OSI**
3. **Ethernet-фреймы спецификации IEEE 802.3**
4. **Управление доступом к передающей среде**
5. **Три топологии сети Ethernet и их MAC-протоколы**

Ключивые слова: Ethernet, метод доступа, этапы доступа, преамбула, коллизия, фреймирование, спецификация IEEE 802.3, MAC-протоколы

Ethernet - это самый распространенный на сегодняшний день стандарт локальных сетей. Общее количество сетей, использующих в настоящее время Ethernet, оценивается в 5 миллионов, а количество компьютеров, работающих с установленными сетевыми адаптерами Ethernet - в 50 миллионов.

Ethernet - это сетевой стандарт, основанный на технологиях экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году.

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации - 10Base-5, 10Base-2, 10Base-T, 10Base-FL, 10Base-FB.

В 1995 году был принят стандарт Fast Ethernet, Аналогично, принятый в 1998 году стандарт Gigabit Ethernet описан в разделе 802.3z. основного документа.

Все виды стандартов Ethernet используют один и тот же метод разделения среды передачи данных.

1. Метод доступа CSMA/CD

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD).

Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод).

1. Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети.
2. Одновременно все компьютеры сети имеют возможность немедленно (с учетом задержки распространения сигнала по физической среде) получить данные, которые любой из компьютеров начал передавать на общую шину.

Простота схемы подключения - это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме *коллективного доступа (multiply-access, MA).*

Этапы доступа к среде

Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом станции назначения.

Чтобы получить возможность передавать кадр, станция должна убедиться, что разделяемая среда свободна. Это достигается прослушиванием основной гармоники сигнала, которая также называется несущей частотой (carrier-sense, CS). Признаком не занятости среды является отсутствие на ней несущей частоты, которая при манчестерском способе кодирования равна 5-10МГц, в зависимости от последовательности единиц и нулей, передаваемых в данный момент.

Если среда свободна, то узел имеет право начать передачу кадров. Узел 1 обнаружил, что среда свободна, и начал передавать свой кадр. В классической сети Ethernet на коаксиальном кабеле сигналы передатчика узла 1 распространяются в обе стороны, так что все узлы сети их получают. Кадр данных всегда сопровождается преамбулой (preamble), которая состоит из 7 байт, состоящих из значений 10101010, и 8-го байта, равного 10101011. Преамбула нужна для вхождения приемника в побитовый и побайтовый синхронизм с передатчиком.

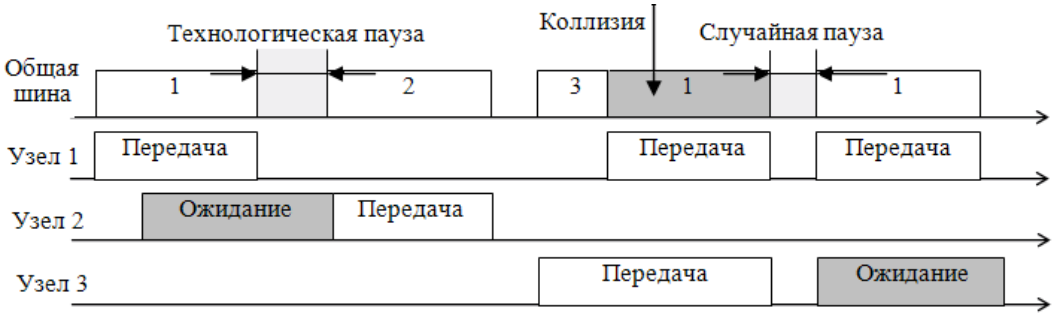


Рис.1 Пояснение метода случайного доступа CSMA/CD

Все станции, подключенные к кабелю, могут распознать факт передачи кадра, и та станция, которая узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес станции-источника также включен в исходный кадр, поэтому станция-получатель знает, кому нужно послать ответ.

Узел 2 во время передачи кадра узлом 1 также пытался начать передачу своего кадра, однако обнаружил, что среда занята - на ней присутствует несущая частота, - поэтому узел 2 вынужден ждать, пока узел 1 не прекратит передачу кадра.

После окончания передачи кадра все узлы сети обязаны выдержать технологическую паузу (Inter Packet Gap) в 9,6 мкс. Эта пауза, называемая также межкадровым интервалом, нужна для предотвращения монопольного захвата среды одной станцией. После окончания технологической паузы узлы имеют право начать передачу своего кадра, так как среда свободна. Из-за задержек распространения сигнала по кабелю не все узлы строго одновременно фиксируют факт окончания передачи кадра узлом 1.

Возникновение коллизии

При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общей среде. Говорят, что при этом происходит ***коллизия (collision)***, так как содержимое обоих кадров сталкивается на общем кабеле и происходит искажение информации.

Коллизия – это нормальная ситуация в работе сетей Ethernet. В примере, изображенном на рис.1, коллизию породила одновременная передача данных узлами 3 и 1. Для возникновения коллизии не обязательно, чтобы несколько станций начали передачу абсолютно одновременно,

такая ситуация маловероятна. Гораздо вероятней, что коллизия возникает из-за того, что один узел начинает передачу раньше другого, но до второго узла сигналы первого просто не успевают дойти к тому времени, когда второй узел решает начать передачу своего кадра. То есть коллизии - это следствие распределенного характера сети.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется ***обнаружение коллизии (collision detection, CD)***. Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети станция, которая обнаружила коллизию, прерывает передачу своего кадра (в произвольном месте, возможно, и не на границе байта) и усиливает ситуацию коллизии посылкой в сеть специальной последовательности из 32 бит, называемой ***jam-последовательностью***.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение короткого случайного интервала времени. Затем она может снова сделать попытку захвата среды и передачи кадра. Случайная пауза выбирается по следующему алгоритму:

Пауза =**L***(интервал отсрочки),

где интервал отсрочки равен 512 битовым интервалам (в технологии Ethernet принято все интервалы измерять в битовых интервалах; битовый интервал обозначается как bt и соответствует времени между появлением двух последовательностей бит данных на кабеле; для скорости 10 Мбит/с величина битового интервала равна 0,1 мкс или 100 нс).

L представляет собой целое число, выбранное с равной вероятностью из диапазона [0,2N], где N – номер повторной попытки передачи данного кадра: 1,2, …10.

После 10-й попытки интервал, из которого выбирается пауза, не увеличивается. Таким образом, случайная пауза может принимать значения от 0 до 52.4 мс.

Если 16 последовательных попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр.

Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети. При значительной интенсивности коллизий полезная пропускная способность сети Ethernet резко падает, так как сеть почти постоянно занята повторными попытками передачи кадров. Для уменьшения интенсивности возникновения коллизий нужно либо уменьшить трафик, сократив, например, количество узлов в сегменте или заменив приложения, либо повысить скорость протокола, например, перейти на Fast Ethernet.

Следует отметить, что метод доступа CSMA/CD вообще не гарантирует станции, что она когда-либо сможет получить доступ к среде. Другие методы доступа - маркерный доступ сети Token Ring и FDDI, метод Demand Priority сетей 100VG-AnyLAN - свободны от этого недостатка.

2. Технология Ethernet и эталонная модель OSI

Стандарты LAN-сетей определяют характеристики физической среды и разъемы, используемые для подсоединения устройств на физическом уровне эталонной модели OSI. Стандарты LAN также определяют способ коммуникации устройств на канальном уровне. Дополнительно стандарты LAN определяют зависящий от конкретного протокола тип инкапсуляции данных,

который позволяет соответствующим образом их обрабатывать по мере продвижения потоков данных между различными уровнями эталонной модели OSI.

Для выполнения этих функций канальный уровень технологии Ethernet Института IEEE имеет два подуровня:

- *подуровень управления доступом к среде (Media Access Control - MAC*) (802.3). Как указывает само название, MAC-подуровень определяет способ передачи фреймов в физическую передающую среду. На этом подуровне решаются вопросы физической адресации всех устройств, определения сетевой топологии и дисциплины канала;
- *подуровень управления логическим каналом (Logical Link Control - LLC*) (802.2). Как показывает само название, подуровень LLC отвечает за логическую идентификацию различных типов протоколов и последующую инкапсуляцию согласно им.

Как показано на рис. 2, стандарт *IEEE 802.3* определяет физический уровень (первый уровень) и MAC-часть канального (второго) уровня.

Рис. 2. Стандарт Ethernet и эталонная модель OSI

На рис. 2 изображены разнообразные технологии первого уровня модели OSI и нижняя половина второго уровня. Первый (физический) уровень эталонной модели OSI описывает интерфейс устройств со средой передачи, сигнализацию, перемещение битовых потоков по среде передачи, компоненты, передающие сигналы в передающую среду, и различные топологии сетей LAN. Физический уровень играет ключевую роль в коммуникации между отдельными компьютерами, однако его функций недостаточно для работы сети. Каждая из этих функций имеет свои ограничения.

Эти ограничения преодолеваются на втором уровне.

Как показано в табл. 1, для каждого ограничения первого уровня имеется соответствующее решение на втором уровне.

Таблица 1. Проблемы первого уровня, решаемые на втором

Ограничения первого уровня	**Решение на втором уровне**
Первый уровень не может осуществлять связь с верхними уровнями	Второй уровень осуществляет связь с верхними уровнями через подуровень LLC
Первый уровень не может идентифицировать отдельные компьютеры	Второй уровень идентифицирует отдельные компьютеры с помощью MAC-схемы адресации
Первый уровень оперирует только потоками битов	На втором уровне создаются фреймы для организации или группировки битов (в этом процессе группа битов приобретает определенное значение)

Первый уровень не может принять решение о том, какой компьютер из группы компьютеров, пытающихся передавать двоичные данные в данный момент, будет первым осуществлять передачу	Для принятия этого решения второй уровень использует MAC-подуровень

Подуровни LLC и MAC второго уровня являются действующими и полезными соглашениями, которые делают технологию совместимой, а связь между компьютерами - возможной. MAC-подуровень управляет физическими компонентами, которые будут использоваться для передачи информации. Как и другие уровни, подуровень LLC остается относительно независимым от физического оборудования, которое будет использоваться в процессе коммуникации. Подуровень LLC позволяет поддерживать несколько протоколов третьего уровня.

Фреймирование на втором уровне

Закодированные потоки битов в физической среде представляют собой огромное технологическое достижение, однако их недостаточно для осуществления коммуникации. Превращение этих битовых потоков во фреймы позволяет получать из них существенную информацию, которая не может быть получена из самих по себе закодированных битовых потоков. Дополнительная информация, которая может содержаться во фреймах, включает:

- сведения о том, какие компьютеры осуществляют связь друг с другом;
- сведения о том, когда начинается связь между двумя индивидуальными компьютерами и когда она заканчивается;
- она обеспечивает распознавание ошибок, которые могут произойти в процессе коммуникации;
- она содержит указания, чья очередь «говорить» в «диалоге» между двумя компьютерами;
- сведения о том, где во фрейме расположены собственно полезные данные.

После того как определен способ идентификации отдельных компьютеров, можно перейти к процессу создания фреймов. Создание фреймов происходит в процессе инкапсуляции данных на втором уровне эталонной модели OSI. Фрейм представляет собой модуль данных протокола второго уровня.

Отдельный фрейм в общем случае состоит из частей, называемых *полями (fields*), каждое из которых, в свою очередь, состоит из байтов (рис. 3). Во фрейме канального уровня обычно присутствуют следующие поля:

Рис. 3. Формат фрейма в самом общем случае

- поле начала фрейма (Frame Start);
- поле адреса (Address field);
- поле длины/типа/управляющее (Length/Type/Control field);
- поле данных (Data field);
- поле контрольной последовательности фрейма (Frame Check Sequence - FCS).

3. Ethernet-фреймы спецификации IEEE 802.3

Кроме рассмотренного выше типа фрейма 802.2, существует более простой тип фрейма 802.3, разработанный Институтом IEEE. Что касается спецификации 802.2, то в современных локальных Ethernet-сетях она используется достаточно редко.

На рис. 4 показан базовый формат Ethernet_фрейма спецификации IEEE 802.3.

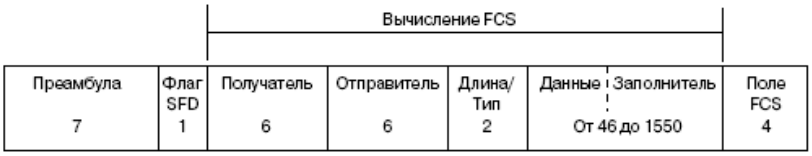


Рис. 4. Структура фрейма Ethernet спецификации 802.3 Института IEEE

Поля Ethernet-фрейма

Ниже описано большинство требуемых или разрешенных полей фрейма Ethernet 802.3.

- **Преамбула (Preamble**). Это поле содержит набор чередующихся нулей и единиц, которые использовались для временной синхронизации в асинхронной реализации технологии Ethernet со скоростью передачи 10 Мбит/с и в более медленных. Высокоскоростные версии технологии Ethernet являются синхронными, поэтому эта информация синхронизации избыточна, однако сохраняется для совместимости с предыдущими версиями. Преамбула имеет длину семь октетов и представляется следующим бинарным набором:
- **Флаг начала фрейма (Start Frame Delimiter - SFD**). Это поле имеет длину один октет и отмечает конец информации синхронизации. Оно представляется двоичным значением 10101011. Следует также отметить, что информация синхронизации, представленная в преамбуле и поле SFD, отбрасывается и не принимается в расчет, когда речь идет о минимальном и максимальном размерах фрейма.
- **Адрес получателя (Destination Address)**. Это поле содержит шестиоктетный MAC-адрес получателя. Адрес получателя может быть адресом одноадресатной рассылки (отдельный узел), многоадресатной рассылки (группа узлов) или широковещательным (рассылка всем узлам).
- **Адрес отправителя (Source Address)**. Это поле содержит шестиоктетный MAC-адрес отправителя. Предполагается, что адрес отправителя может быть только одноадресатным идентификатором передающей Ethernet-станции. Однако все чаще применяются виртуальные протоколы, которые иногда используют конкретный MAC-адрес для идентификации виртуального объекта.
- **Длина/Тип (Length/Type)**. Если это значение меньше десятичного числа 1536 (или шестнадцатеричного 0600), то оно указывает длину фрейма. Интерпретация поля как длины используется в тех случаях, когда уровень LLC обеспечивает идентификацию протокола.
- **Тип фрейма (тип Ethernet)**. Поле типа фрейма (Type) указывает протокол более высокого уровня, которому будут переданы данные после окончания обработки на уровне Ethernet.
- **Длина фрейма (длина IEEE 802.3)**. Поле длины фрейма указывает количество байтов данных, которые следуют за этим полем. Если это значение равно или больше десятичного числа 1536 (или шестнадцатеричного 0600), то оно указывает тип протокола, и в этом случае содержимое поля данных (Data field) декодируется согласно указанному протоколу.

- **Данные и биты заполнения (Data and Pad field)**. Это поле может иметь произвольную длину, не превосходящую максимально допустимый размер фрейма. Максимальный блок передачи (Maximum Transmission Unit - MTU) для технологии Ethernet составляет 1500 октетов, и объем данных не должен превосходить это значение.
- Согласно параметрам структуры фрейма, длина поля данных должна находиться в интервале от 46 до 1500 октетов.
- **Данные (IEEE 802.3)**. После того как обработка фрейма на физическом и канальном уровнях завершена, данные передаются протоколу более высокого уровня, который должен быть определен в поле данных фрейма. Если данных фрейма недостаточно для того, чтобы он имел минимальный размер 64 байта, то добавляются байты заполнителя, с тем чтобы фрейм имел длину как минимум 64 байта.
- **Контрольная последовательность фрейма (Frame Check Sequence - FCS)**. Эта последовательность содержит четырехбайтовое значение циклического избыточного кода (Cyclical Redundancy Check - CRC), которое вычисляется посылающим фрейм устройством, а затем повторно вычисляется получающим этот фрейм устройством для проверки того, не был ли фрейм поврежден в процессе передачи. В это четырехоктетное поле помещается результат выполнения - алгоритма проверки CRC. Передающая станция вычисляет контрольную сумму для передаваемого фрейма, а полученное значение вставляется за полем данных (или за битами заполнения). Приемная станция (станции) выполняет те же вычисления и сравнивает новую контрольную сумму с находящейся в конце пересылаемого фрейма. Если эти два значения совпадают, фрейм считается полноценным.

4. Управление доступом к передающей среде

Под управлением доступом к среде (Media Access Control - MAC) понимаются протоколы, которые в совместно используемой среде (коллизионном домене) определяют, какому компьютеру предоставить право передавать данные. Существуют два общих типа MAC-подуровня:

- детерминистический (существует очередность предоставления доступа);
- недетерминистический (право передачи предоставляется первому обратившемуся по принципу «первым пришел - первым обслужен» (first come, first served)).

Технологии Token Ring и FDDI являются детерминистическими, а Ethernet- недетерминистической (также называется вероятностной).

Детерминистические MAC-протоколы

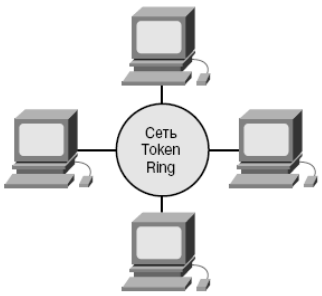


Рис. 5. Сеть Token Ring

Детерминистические MAC-протоколы при предоставлении права на передачу используют очередность, иногда шутливо называемую «передачей хода». Примером детерминистического протокола может служить протокол передачи маркера Token Ring. В сети Token Ring отдельные станции образуют кольцо, как показано на рис. 5. По такому кольцу циркулирует специальный маркер.

Если какой-то станции требуется передать данные, она захватывает маркер, в течение определенного времени передает данные, а затем передает маркер в кольцо, где он может быть перехвачен другой станцией.

Недетерминистические MAC-протоколы

Недетерминистические MAC-протоколы используют механизм доступа согласно принципу «первым пришел - первым обслужен» (first come, first served - FCFS).

Примером недетерминистического MAC-протокола является метод множественного доступа CSMA/CD.

При использовании этой технологии общего доступа среда Ethernet позволяет сетевым устройствам конкурировать за право передачи. Станции в сети, использующей метод CSMA/CD, прослушивают сеть и ожидают момента, когда она будет свободна для передачи данных. Однако если две станции начинают передачу одновременно, то происходит коллизия (столкновение), и попытки передачи обеих станций оказываются безуспешными. Все станции сети также узнают об этой коллизии и ожидают, когда канал передачи освободится. Передающие станции, в свою очередь, ожидают в течение некоторого случайным образом выбираемого промежутка времени перед попыткой повторной передачи, что уменьшает вероятность повторной коллизии.

5. Три топологии сети Ethernet и их MAC-протоколы

Тремя основными технологиями второго уровня являются Token Ring, FDDI и Ethernet. Ниже дается характеристика этих трех технологий.

- *Технология Ethernet* представляет собой логическую шинную топологию (информация проходит по линейной шине).
- *Технология Token Ring* представляет собой логическую кольцевую топологию (иными словами, информация перемещается по кольцу) и физическую звездообразную (соединения образуют звезду).
- *Технология FDDI* представляет собой логическую кольцевую (информационный поток перемещается по кольцу) и физическую топологию двойного кольца (соединения образуют двойное кольцо).

MAC-подуровень и обнаружение коллизий

Среда Ethernet представляет собой широковещательную технологию совместного доступа. Используемый в среде Ethernet метод доступа CSMA/CD выполняет три функции:

- передачу и получение пакетов данных;
- декодирование пакетов данных и проверку действительности содержащихся в них адресов перед передачей их более высоким уровням модели OSI;
- обнаружение ошибок в пакетах данных или в работе сети.

При использовании метода доступа CSMA/CD сетевые устройства, имеющие данные для передачи, находятся в режиме «прослушивание сети перед передачей» (*listen before transmit mode*), иначе называемом «контролем несущей» (*Carrier Sense - CS*). В технологии Ethernet совместного доступа такой подход означает, что когда устройству требуется передать данные, оно должно предварительно удостовериться в том, что сетевая среда свободна для передачи.

После того как устройство проверило, что в сетевой среде нет сигналов, оно начинает передавать данные. Передавая данные в виде сигналов, устройство продолжает прослушивание среды для того, чтобы быть уверенным в том, что другие устройства не ведут передачу одновременно с ним.

Если две станции ведут передачу одновременно, возникает коллизия (рис. 6).

После окончания передачи устройство возвращается в режим прослушивания сети.

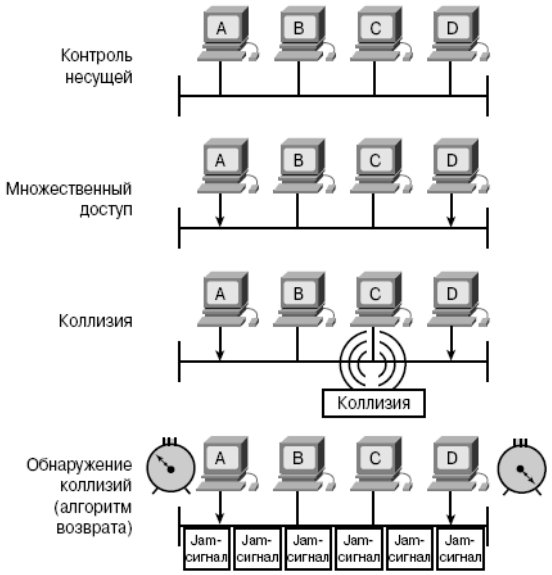


Рис. 6. Метод доступа CSMA/CD

Сетевые устройства способны обнаруживать возникновение коллизии, поскольку она сопровождается увеличением амплитуды сигнала в сетевой среде.

Такая функция называется обнаружением коллизий (Collision Detect - CD).

Когда возникает коллизия, каждое устройство, которое в данный момент осуществляет передачу, продолжает ее в течение короткого промежутка времени для того, чтобы коллизию могли увидеть все устройства в сети. Когда все устройства увидели, что в сети произошла коллизия, передающие устройства вызывают алгоритм, известный как алгоритм *возврата* (*backoff*).

После того как все передающие устройства осуществили возврат и воздержались от передачи в течение некоторого случайно выбранного (и, следовательно, разного у всех устройств) промежутка времени, любое устройство может попытаться вновь получить доступ к среде передачи. При возобновлении передачи устройства, которые были вовлечены в произошедшую коллизию, не имеют приоритета в передаче данных.

Ethernet представляет собой широковещательную технологию передачи данных. Это означает, что все устройства в сети могут «видеть» все фреймы, проходящие мимо них в сетевой среде. Однако не все устройства обрабатывают эти данные. Только устройство, MAC-адрес которого совпадает с MAC-адресом получателя, находящимся во фрейме, копирует этот фрейм в свой буфер. В технологии Ethernet адреса протоколов третьего уровня, таких, как IP или IPX, не просматриваются и не используются. Если MAC-адреса совпадают, то фрейм копируется в буфер и передается на третий уровень для проверки соответствия IP- или IPX-адреса получателя адресу устройства.

После того как устройство проверило MAC- и IP-адрес, содержащиеся в данных, пакет проверяется на наличие в нем ошибок. Если они обнаруживаются, пакет отбрасывается. Устройство-получатель не информирует об этом отправителя, независимо от того, прибыл ли пакет благополучно или нет. По этой причине Ethernet называется сетевой структурой *без установки соединения* (*connectionless*) и *негарантированной доставкой* (*best effort delivery*).

Контрольные вопросы

1. Какие модификации имеет стандарт IEEE 802.3 и каковы их характеристики?
2. Какой метод доступа к среде используется в стандарте Ethernet?
3. Что такое коллизия и каковы причины ее возникновения?
4. Какова структура Ethernet фрейма?
5. Каким образом осуществляется управление доступом к передающей среде?

Лекция 14
Начальные сведения о коммутации в локальных сетях

1. **Сегментация в локальных сетях**
2. **Основные операции коммутатора**
3. **Буфер памяти**

Ключивые слова: коммутация, латентность, режим, сегментация, коммутатор, симметричная коммутация, асимметричная коммутация, буфер памяти.

Коммутация представляет собой технологию, которая уменьшает нагрузку в локальной сети путем уменьшения количества передаваемых данных и увеличения полосы пропускания. В настоящее время в локальных сетях LAN концентраторы часто заменяются *коммутаторами (switch),* которые могут работать в уже существующей кабельной инфраструктуре и, таким образом, их установка не нарушает сложившегося характера работы сети. Для уменьшения количества коллизий и расширения полосы пропускания LAN коммутаторы используют микросегментацию. Коммутаторы LAN также поддерживают такие функции как дуплексная коммуникация и одновременные сеансы связи между несколькими устройствами. Дуплексная коммуникация позволяет двум устройствам одновременно получать друг от друга данные и посылать их. Фактически использование полного дуплекса удваивает пропускную способность сети LAN. В дуплексной коммутируемой LAN отсутствуют коллизии.

При пересылке данных через коммутатор возможны три режима коммутации: с *промежуточным хранением (store-and-forward), сквозной (cut-through)* и коммутация *без фрагментации (fragment-free switching).* Под *латентностью* или *задержкой (latency* или *delay)* понимается время прохождения пакета через коммутатор. Латентность каждого режима зависит от того, каким образом коммутатор обрабатывает и пересылает поступающие фреймы. Более быстрый режим коммутации уменьшает латентность коммутатора. Для выполнения функций коммутации коммутаторы и мосты LAN, функционирующие на 2-м уровне эталонной модели OSI, пересылают фреймы на основе MAC-адресов сетевых устройств. Если MAC-адрес 2-го уровня неизвестен, то устройство осуществляет лавинную рассылку, пытаясь таким путем достичь пункта назначения фрейма. Коммутаторы и мосты LAN также пересылают все широковещательные пакеты. Это может привести к лавинному шторму, т.е. ситуации, когда фреймы бесконечно циркулируют по образующимся в сети петлям. Для предотвращения петель используется протокол связующего дерева *(Spanning Tree Protocol).* Этот протокол представляет собой технологию, которая позволяет коммутаторам обмениваться друг с другом информацией и, таким образом, обнаруживать в сети петли. Протокол связующего дерева допускает существование в сети избыточных маршрутов, которые рассматриваются как резервные, однако для предотвращения петель временно отключает некоторые порты коммутаторов.

1. Сегментация в локальных сетях

Сегментация в сети LAN используется для двух целей: для изолирования потоков данных внутри сегментов и для увеличения полосы пропускания, приходящейся на одного пользователя, за счет уменьшения размеров коллизионных доменов.

При отсутствии сегментации сети LAN, превосходящие размерами небольшую рабочую группу, быстро становятся clogged и коллизии практически полностью закрывают полосу пропускания. Сегментация в сети LAN может быть реализована с помощью мостов, коммутаторов и маршрутизаторов. Каждое из этих устройств обладает своими достоинствами и недостатками. Сеть может быть подразделена на области меньшего размера, называемые сегментами. Каждый сегмент использует метод доступа *CSMA/CD* и поддерживает обмен данными между своими пользователями. На рис. 1 приведен пример сегментированной локальной сети Ethernet. Вся сеть состоит из 15 компьютеров (6 файловых серверов и 9 PC). Если разделить эту сеть на сегменты, то при коммуникации внутри сегмента на одни и те же 10 Мбит/с будет приходиться меньшее количество пользователей/устройств. Как показано на рис. 2, каждый сегмент рассматривается как отдельный коллизионный домен (collision domain).

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

Основной характеристикой LAN-коммутации является микросегментации, которая позволяет создавать выделенные сегменты и предоставляет выделенную полосу пропускания каждому пользователю сети. Каждый пользователь получает доступ сразу ко всей полосе пропускания сети и ему не приходится конкурировать за доступную полосу пропускания с остальными пользователями. Это означает что пары устройств, подсоединенные к одному коммутатору, могут осуществлять связь одновременно с минимальным количеством коллизий. Микросегментация уменьшает количество коллизий за счет уменьшения размера коллизионных доменов. Это увеличивает пропускную способность для каждого устройства, подсоединенного к сети.

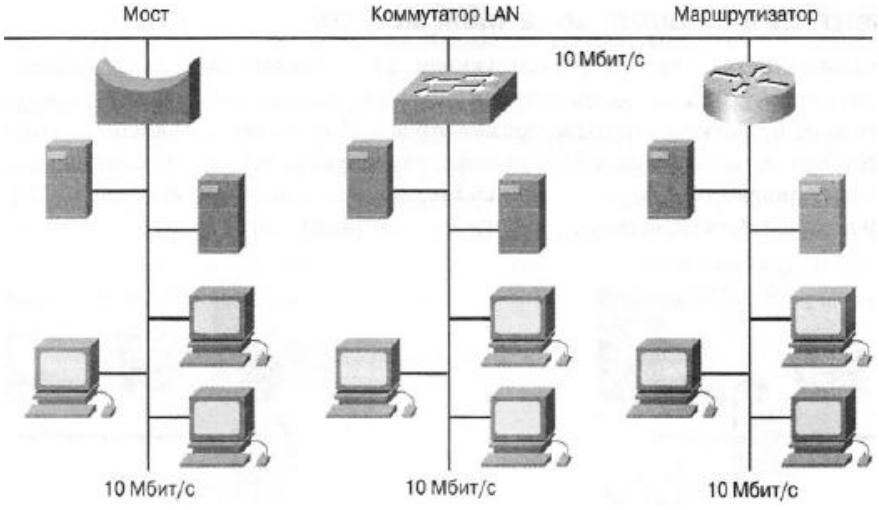


Рис. 1. Сегментированная сеть

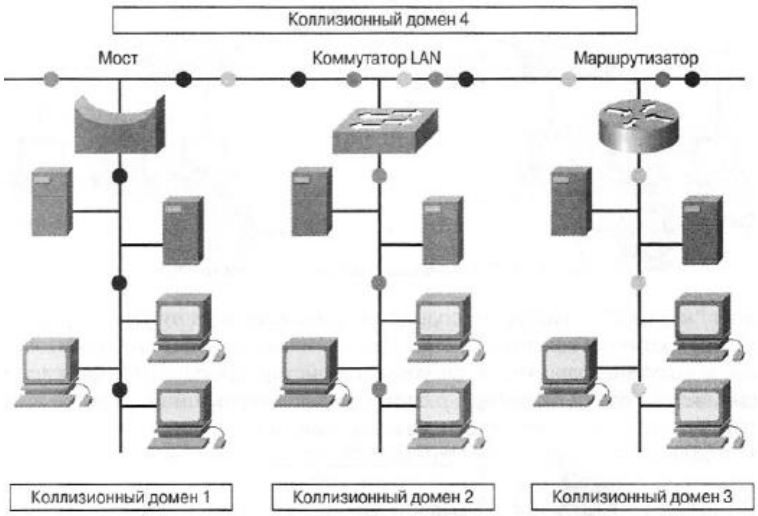


Рис. 2. Коллизионные домены

Сегментация с использованием мостов

Локальная сеть Ethernet, использующая для сегментации мосты, обеспечивает большую ширину полосы пропускания в расчете на одного пользователя, поскольку на один сегмент приходится меньше пользователей. И наоборот, локальные сети, в которых мосты не используются, обеспечивают меньшую полосу пропускания, поскольку в несегментированной LAN оказывается больше пользователей. На рис. 3 приведен пример локальной сети, сегментированной с помощью моста.

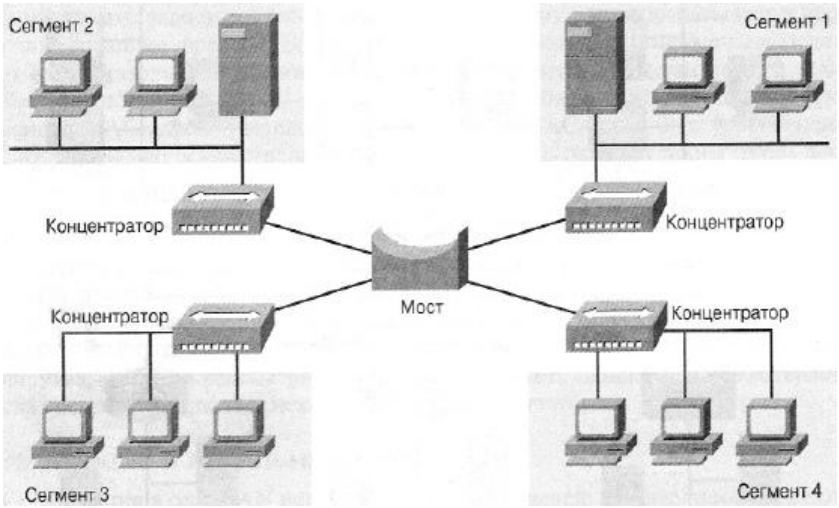


Рис. 3. Сегментация с использованием мостов

Мосты «изучают» характер расположения сегментов сети путем построения адресных таблиц, в которых содержатся адреса всех сетевых устройств и сегментов, необходимых для получения доступа к данному устройству. На рис. 4 приведен пример того, как мост использует адресную таблицу для идентификации всех узлов сети.

Мосты являются устройствами 2-го уровня, которые направляют фреймы данных в соответствии с MAC-адресами фреймов. Кроме того мосты являются «прозрачными» для всех остальных устройств сети.

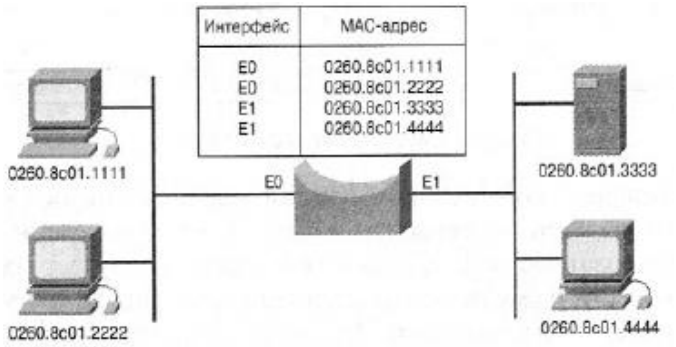


Рис. 4. Пример адресной таблицы

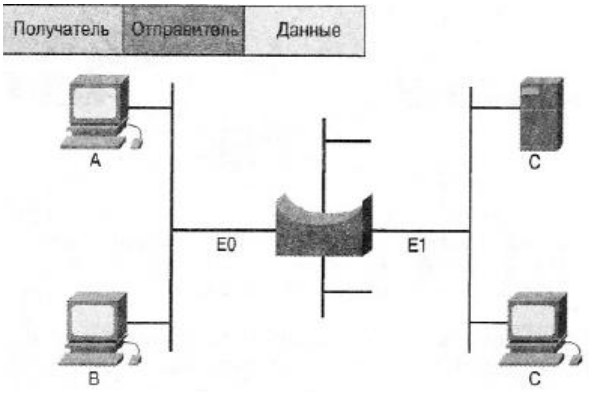


Рис. 5. Сегментация с использованием мостов

Как показано на рис. 5, мост узнает о расположении устройств A, B, C и D, изучая MAC-адреса отправителей. Если мост регистрирует поступление фрейма, но не знает ни адреса отправителя, ни адреса получателя, то он добавляет адрес отправителя в свою адресную таблицу и направляет фрейм на все интерфейсы, за исключением того, на который этот фрейм поступил.

При получении ответа мост исследует адрес отправителя и добавляет эту станцию в свою адресную таблицу. В дальнейшем для связи этих устройств мост использует данные адресной таблицы.

Мосты увеличивают латентность сети на 10-30%. Это увеличение латентности связано с тем, что мосту при передаче данных требуется дополнительное время на принятие решения. Если порт пункта назначения в данный момент занят, то мост может временно сохранить фрейм до освобождения порта.

Для выполнения этих операций требуется некоторое время, что замедляет процесс передачи и увеличивает латентность.

Сегментация с использованием маршрутизаторов

Маршрутизаторы представляют собой более современные устройства, чем обычные мосты. Мост является пассивным элементом сети и действует на уровне канала связи. Маршрутизатор действует на сетевом уровне *(network layer)* и в своих решениях относительно направления данных между сегментами опирается на адреса протокола сетевого уровня. Маршрутизаторы дают наивысший уровень сегментации, направляя данные на концентратор, к которому подсоединены рабочие станции. Маршрутизатор принимает решение о выборе сегмента для передачи данных, анализируя адрес пункта назначения, содержащийся в пакете данных, и используя таблицу маршрутизации (routing table) для выработки направляющих инструкций, как показано на рис. 6.

Сегментация с использованием коммутаторов

Использование коммутации (switching) в локальных сетях смягчает проблемы, связанные с недостаточной шириной полосы пропускания и с возможностью переполнений, которые могут возникать, например, между несколькими PC и удаленным файл-сервером. Коммутатор разделяет локальную сеть на микросегменты, состоящие из двух станций, как показано на рис. 7. При этом один большой коллизионный домен делится на несколько малых доменов, свободных от коллизий. Хотя LAN-коммутатор устраняет возможность коллизий между доменами, отдельные станции, находящиеся внутри сегмента, по-прежнему остаются в одном коллизионном домене.

Вследствие этого все узлы, подключенные к коммутатору, могут получить широковещательный сигнал всего от одного узла. Среди других преимуществ, стоит отметить малую латентность и высокую скорость пересылки на каждом порте интерфейса, а также совместимость с уже установленными сетевыми адаптерами, концентраторами и кабельной системой

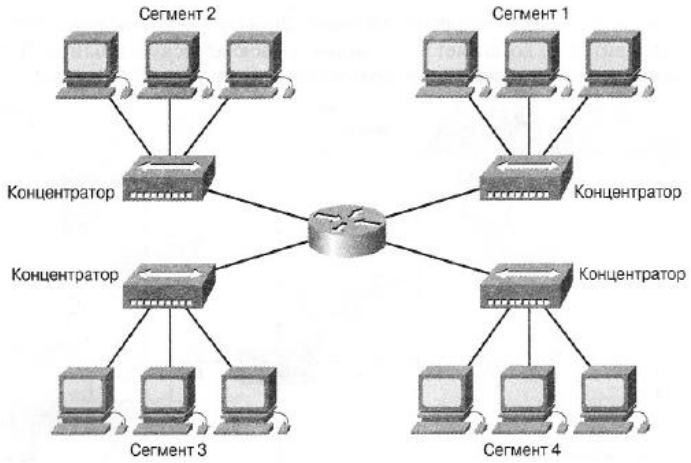


Рис. 6. Сегментация с использованием маршрутизаторов

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

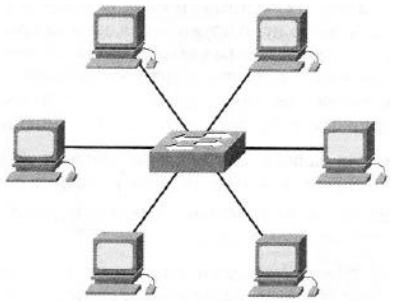


Рис. 7. Сегментация с помощью коммутаторов

Технология коммутируемого Ethernet (switched Ethernet) базируется на типовом Ethernet. При ее использовании каждый узел непосредственно соединен с одним из портов коммутатора или с сегментом, который, в свою очередь, соединен с одним из портов коммутатора. Таким образом на коммутаторе создается соединение с полосой пропускания 10 Мбит/с, 100 Мбит/с или 1000 Мбит/с между каждым узлом и соответствующим сегментом.

Компьютер, непосредственно соединенный с коммутатором, имеет собственный коллизионный домен и полную полосу пропускания в 10 Мбит/с.

Локальная сеть, использующая топологию (topology) коммутируемого Ethernet, ведет себя так, как если бы она имела только два узла — узел отправителя и узел получателя.

Этим двум узлам предоставляется полоса пропускания в 10 Мбит/с. Вследствие этого практически вся полоса пропускания может быть использована для передачи данных. За счет более эффективного использования полосы пропускания коммутируемый Ethernet обеспечивает более высокую скорость передачи, чем сети Ethernet, в которых используются только мосты и концентраторы. В коммутируемом Ethernet доступная ширина полосы пропускания может достигать величины, близкой к 100%.

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

2. Основные операции коммутатора

Коммутация представляет собой технологию, которая уменьшает вероятность переполнения в сетях Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI). В сетях LAN коммутаторы часто используются для замены совместно используемых концентраторов. Коммутаторы LAN разрабатываются таким образом, чтобы они могли быть установлены в уже существующие кабельные сетевые инфраструктуры без нарушения уже сложившегося характера работы сети. В современных коммуникациях все коммутирующие устройства выполняют две основные операции

- **Коммутация фреймов данных.** Эта операция состоит в получении фрейма из входной передающей среды и передаче его в выходную среду
- **Поддержка операций по коммутации.** При своей работе коммутатор строит и поддерживает таблицы коммутации

Под *мостовыми операциями (bridging)* понимается технология, в которой устройство, известное как мост, соединяет два или более сегментов сети LAN. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Мост передает дейтаграммы из одного сегмента к получателям, находящимся в других сегментах. Когда включается питание и начинается функционирование моста, он изучает MAC-адреса поступающих дейтаграмм и строит таблицу адресов известных ему получателей. Если мосту известно, что пункт назначения дейтаграммы находится в том же сегменте где и ее отправитель, то дейтаграмма отбрасывается, поскольку в ее передаче нет необходимости. Если мосту известно, что получатель находится в другом сегменте, то он передает ее только в этот сегмент. Если же сегмент пункта назначения неизвестен, то мост передает дейтаграмму во все сегменты, кроме того, в котором находится отправитель этой дейтаграммы. Такая передача называется лавинной рассылкой (flooding). Как мосты, так и коммутаторы соединяют между собой сегменты сети LAN, используют MAC-адреса для определения сегмента, в который требуется передать дейтаграмму и уменьшают объем передаваемых данных. В современных сетях коммутаторы выполняют большее количество функций, чем мосты, поскольку они позволяют осуществлять большее количество соединений, работают с гораздо большими скоростями, чем мосты, а также поддерживают новые функции, такие как виртуальные локальные сети (virtual LAN — VLAN). В мостах коммутацию обычно осуществляет программное обеспечение, в то время как в коммутаторах коммутация обычно выполняется аппаратно

На рис. 8 показана LAN-сеть с тремя рабочими станциями, LAN-коммутатор и адресная таблица этого коммутатора. LAN-коммутатор имеет четыре порта (или сетевых соединения). Станции A и C подсоединены к 3-му интерфейсу коммутатора, а станция B к 4-му интерфейсу. Вероятнее всего, что в реальной сети станции A и C будут подсоединены к концентратору, который будет подсоединен к 3-му интерфейсу. Как показано на рис. 8, станции A требуется передать данные станции B.

Операции, выполняемые LAN-коммутатором:

- Пересылает пакеты на основе данных таблицы пересылки
- Пересылает пакеты на основе MAC-адреса (2-й уровень)
- Функционирует на 2-м уровне модели OSI
- Узнает расположение станции путем исследования адреса отправителя

- Осуществляет рассылку со всех портов если адрес получателя является широковещательным, многоадресатным или неизвестен
- Осуществляет пересылку в том случае, если получатель расположен на другом интерфейсе

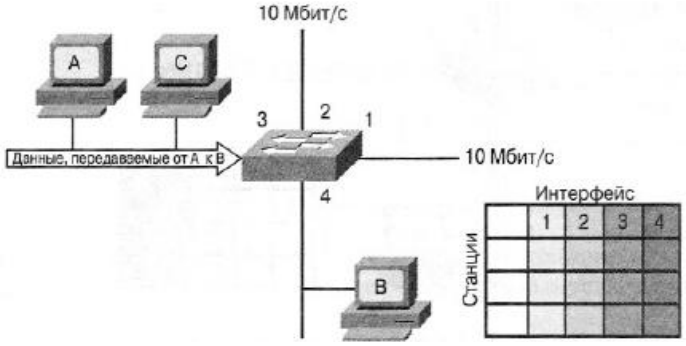


Рис. 8. Операции LAN-коммутатора

Следует помнить о том, что при прохождении потоков данных по сети коммутатор функционирует на 2-м уровне; это означает, что коммутатор просматривает адрес MAC-уровня. При передаче фреймов станцией A и получении их коммутатором, последний просматривает MAC-адрес отправителя и сохраняет его в адресной таблице, как показано на рис. 9. При прохождении данных через коммутатор в адресной таблице создается новая позиция, в которую заносится адрес станции-отправителя и интерфейс коммутатора, к которому она подсоединена. После этого коммутатору известно где подсоединена станция A. Как показано на рис. 10, после поступления фрейма данных на коммутатор он лавинным образом рассылается на все порты, поскольку станция-получатель пока неизвестна

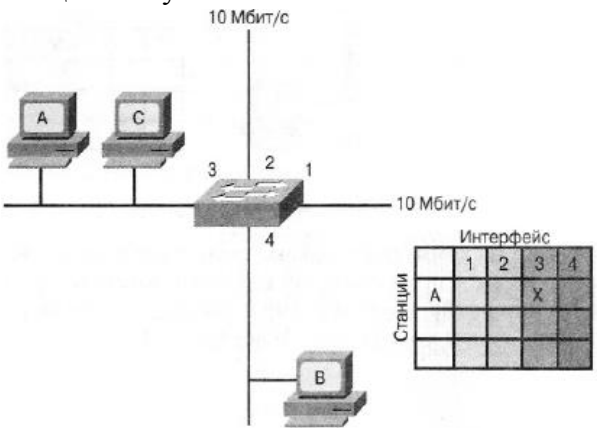


Рис. 9. Построение адресной таблицы

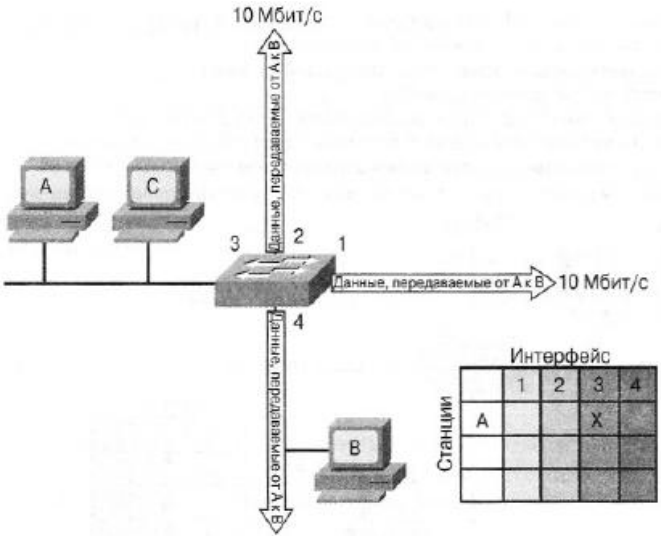


Рис. 10. Лавинная рассылка на все порты

Однако после создания соответствующей позиции в адресной таблице поступает ответ от станции B к станции A. Теперь коммутатору известно, что станция B подсоединена к 4-му интерфейсу, как показано на рис. 11.

Данные поступают на коммутатор, однако следует обратить внимание на то, что теперь коммутатор не выполняет лавинной рассылки. Коммутатор отправляет данные только на 3-й ин-

терфейс, поскольку ему известно, что станция А расположена в сегменте, подсоединенном к этому интерфейсу (рис. 12).

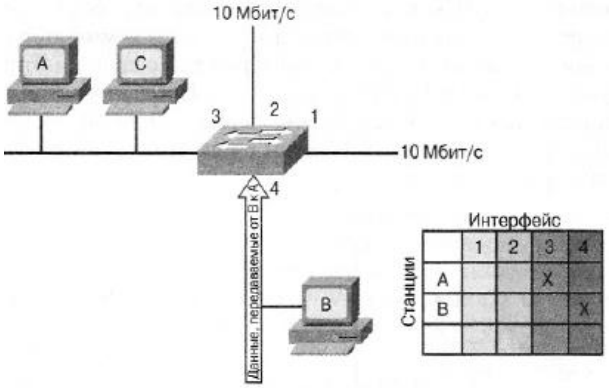


Рис. 11. Ответ на лавинную рассылку

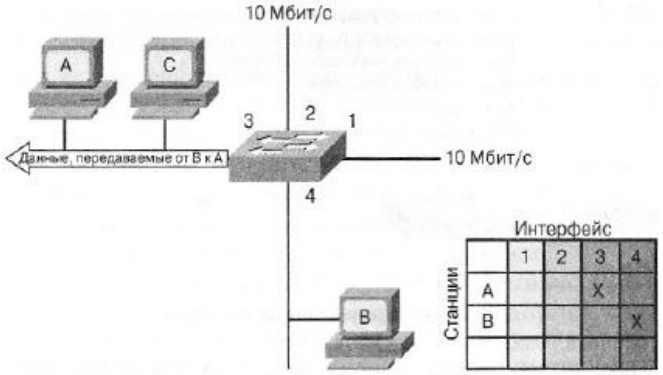


Рис. 12. Передача данных известной станции

Первоначальная передача указала MAC-адрес станции, от которой поступили данные, что позволило коммутатору более эффективно осуществлять передачу данных

Коммутация на 2-м и 3-м уровнях

В сетях используются два метода коммутации фреймов данных: коммутация на 2-м уровне, показанная на рис. 13, и коммутация на 3-м уровне, показанная на рис. 14. Под коммутацией понимается процесс приема входящего фрейма на одном интерфейсе и отправка его через другой интерфейс. Для маршрутизации пакетов маршрутизаторы используют коммутацию 3-го уровня, в то время как коммутаторы (имеются в виду коммутаторы 2-го уровня) используют для пересылки фреймов коммутацию 2-го уровня.

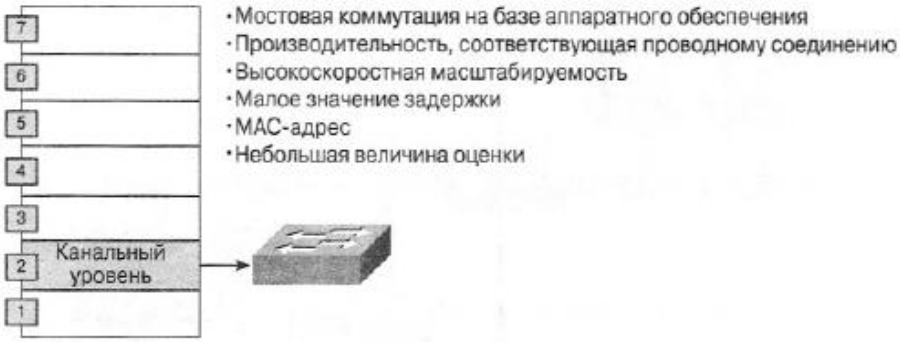


Рис. 13. Коммутация на 2-м уровне

Различие между коммутацией на 2-м уровне и на 3-м уровне определяется тем, какая находящаяся во фрейме информация используется для определения требуемого выходного интерфейса. При использовании коммутации 2-го уровня пересылка фреймов осуществляется на основе информации MAC-адреса. При использовании коммутации 3-го уровня пересылка фреймов осуществляется на основе информации сетевого адреса. При коммутации на 2-м уровне коммутатор просматривает во фрейме MAC-адрес пункта назначения. Если ему известно расположение адреса получателя, то коммутатор отправляет информацию на соответствующий интерфейс. При использовании коммутации 2-го уровня коммутатор строит и поддерживает таблицу коммутации, в которой фиксируется, какие MAC-адреса принадлежат определенным портам или интерфейсам.

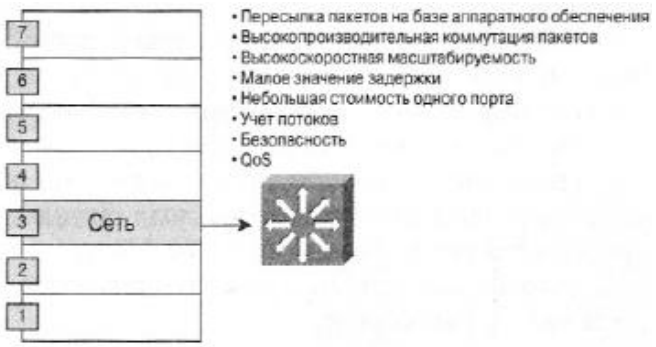


Рис. 14. Коммутация на 3-м уровне

Если коммутатор 2-го уровня не знает куда отправить фрейм, то он рассылает его широковещательно со всех своих портов для получения информации о пункте назначения. При получении ответного фрейма от получателя коммутатор узнает расположение нового адреса и добавляет эту информацию в свою таблицу коммутации.

Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Как показано на рис. 15, симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, в случаях когда все порты имеют ширину полосы пропускания 10 Мбит/с или 100 Мбит/с.

Как показано на рис. 16, асимметричный LAN-коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мбит/с и 100 Мбит/с или 100 Мбит/с и 1000 Мбит/с.

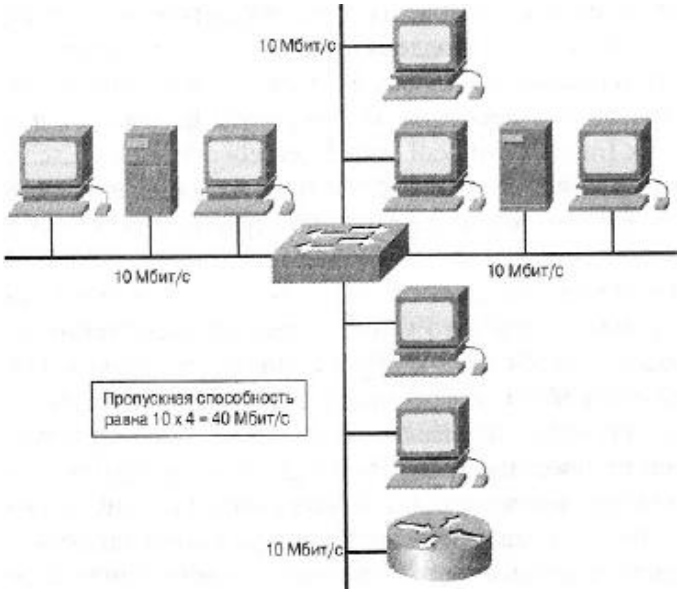


Рис. 15. Симметричная коммутация

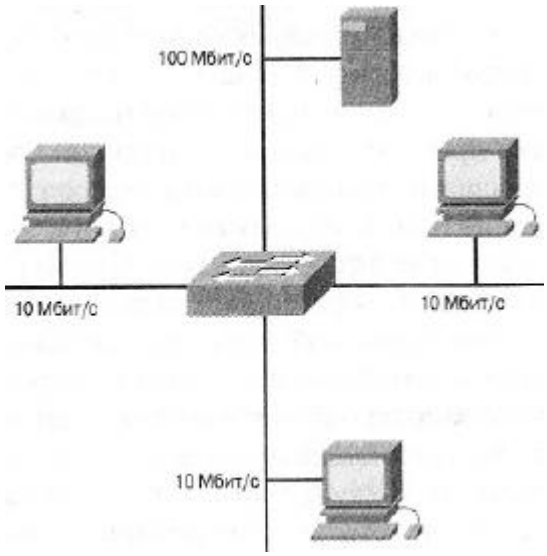


Рис. 16. Асимметричная коммутация

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент/сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к кото-

рому подсоединен сервер, с целью предотвращения переполнения на этом порте. Асимметричный коммутатор также необходим для обеспечения большой ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения или каналов между сегментами магистрали.

3. Буфер памяти

Для временного хранения пакетов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки пакетов — буферизация по портам и буферизация с обшей памятью.

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

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

Коммутатор поддерживает карту портов, в которые требуется отправить пакеты. Очистка этой карты происходит только после того, как пакет успешно отправлен. Поскольку память буфера является обшей, размер пакета ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные пакеты могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации.

Контрольные вопросы

1. Что такое коммутация?
2. Какие режимы коммутации возможны при пересылке данных?
3. Для каких целей осцществляется сигметация в локальных сетях?
4. Какие операции выполняет LAN-коммутатор?
5. Какие функции выплняет буфер памати?

Лекция 15
Коммутаторы

1. **Обзор коммутаторов**
2. **Коммутаторы сетей и иерархическое проектирование сети**
3. **Обзор уровня доступа в коммутируемых локальных сетях**

Ключивые слова: сетевое устройство, модульность, базовый уровень, уровень распределения, уровень доступа, фильтрация, интерфейс.

1. Обзор коммутаторов

Коммутаторы можно рассматривать как многопортовые мосты, которые являются стандартными для современных технологий локальных сетей Ethernet (local-area network — LAN), использующих звездообразную топологию. Коммутаторы обеспечивают выделенные виртуальные каналы типа «точка-точка» между каждыми двумя подсоединенными сетевыми устройствами, поэтому при одновременной передаче коллизий не происходит. Коммутаторы могут работать в дуплексном режиме; это означает, что они могут одновременно получать данные и отправлять их.

Локальные сети LAN охватывают пространство одного помещения, одного здания или нескольких близко расположенных зданий. Группа близко распложенных зданий, принадлежащих одной организации, в сетевой терминологии часто называется кампусом. При проектировании более крупных сетей LAN полезно исходить из следующих положений:

1. На уровне доступа осуществляется подключение конечных пользователей к сети LAN;
2. На уровне распределения осуществляется соединение между собой LAN-сетей конечных пользователей в котором реализуются определенные политики;
3. На базовом уровне осуществляется кратчайшее соединение между точками распределения.

По мере того, как сеть увеличивается до размеров кампуса, возникает необходимость в использовании различных типов коммутаторов локальных сетей. На каждом уровне требуется свой тип коммутатора, который наилучшим образом решает задачи данного уровня. Функции и технические характеристики каждого коммутатора зависят от того, для какого уровня предназначен этот коммутатор. Правильный выбор наилучшего для данного уровня коммутатора обеспечивает максимальную эффективность работы сети для ее пользователей

2. Коммутаторы сетей и иерархическое проектирование сети

Иерархический подход к проектированию сети состоит в разделении достаточно сложной задачи проектирования на ряд меньших и легче решаемых задач. Каждый уровень возникающей структуры решает свой собственный набор задач, что позволяет оптимизировать используемое аппаратное и программное обеспечение для решения конкретных, присущих этому уровню задач. Устройства самого нижнего уровня предназначены для приема данных и передачи их в сеть для последующей обработки на более высоких уровнях. Предлагается трехуровневый подход к решению задачи проектирования сети.

В этой трехуровневой модели проектирования сетевые устройства и соединения между ними группируются и подразделяются на три уровня: базовый уровень, уровень распределения

и уровень доступа, как показано на рис. 1. Как и эталонная модель OSI, эта трехуровневая модель является концептуальной конструкцией, т.е. абстрактной картиной сети.

Полезность уровневых моделей определяется их модульностью. Поскольку устройства одного уровня выполняют аналогичные и четко очерченные функции, сетевой администратор может легко добавлять, заменять и удалять отдельные элементы сети. Такая гибкость и адаптируемость позволяют в процессе проектирования создавать легко масштабируемую сеть.

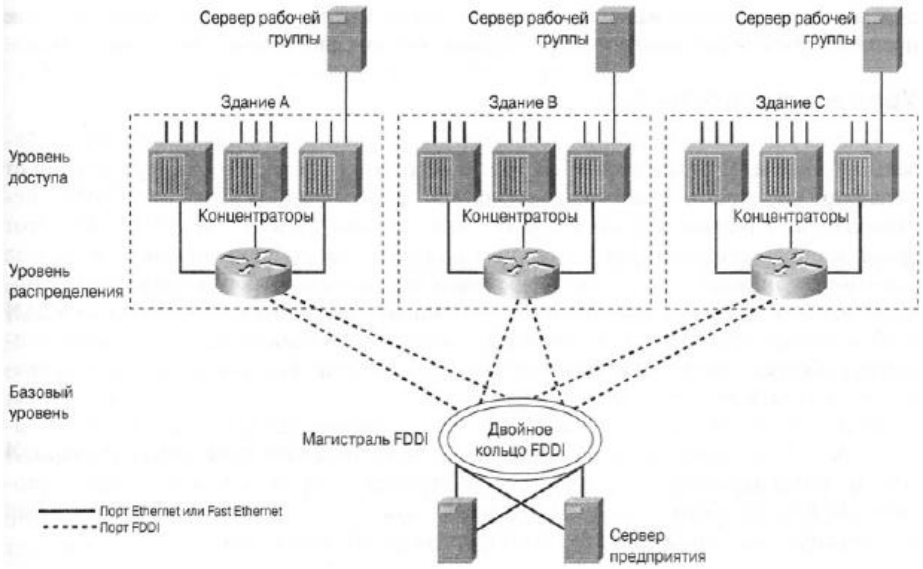


Рис. 1. Иерархическая модель проектирования сети

Этот подход может быть применен при проектировании любой сети. Необходимо принимать во внимание, что три вышеупомянутых уровня модели могут реализоваться в виде отдельных физических устройств, однако это не является обязательным. Эти уровни определяются для облегчения процесса проектирования и создания эффективной сети путем четкого определения требуемых функций сети.

В то же время, понимание уровневых моделей может осложняться тем, что конкретная реализация каждого уровня зависит от конкретной сети. Каждый уровень трехуровневой модели может воплощаться в виде маршрутизатора, коммутатора, соединения или их комбинации. В действительности функции каких-либо уровней могут быть объединены в одном устройстве или, наоборот, какой-либо из уровней может отсутствовать.

Базовый уровень

Назначение базового уровня состоит в создании оптимизированной и надежной транспортной структуры для передачи данных с большими скоростями. Иными словами, *базовый уровень (core layer)* должен передавать данные максимально быстро. Устройства этого уровня не должны быть загружены выполнением таких операций, как проверка списков доступа, шифрование данных, трансляция адресов и других функций, которые препятствуют *коммутации (switching)* пакетов с максимально возможной скоростью.

Уровень распределения

Уровень распределения (distribution layer) расположен между уровнем доступа и базовым уровнем. Его назначение состоит в отделении процессов базового уровня от остальной части сети. В частности, он должен создать границу входа в сеть путем использования списков доступа

и других фильтрующих средств. Таким образом, этот уровень определяет политику доступа к сети. Под политикой понимается подход к обработке определенных типов передаваемых данных, включая обновления маршрутов, обобщение маршрутов, данных, передаваемых по виртуальным сетям VLAN и обобщение (агрегирование) адресов. Различные политики могут быть использованы для обеспечения безопасности сети и для экономии ресурсов путем предотвращения передачи нежелательных данных.

Если в сети используются два или более протокола маршрутизации, такие, например, как протокол маршрутной информации (Routing Information Protocol - RIP) и протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol - IGRP), то обмен информацией между доменами с различными протоколами и се перераспределение также выполняются на уровне распределения.

Уровень доступа

На уровне доступа (access layer) происходит передача данных в сеть и осуществляется входной контроль. Через этот уровень конечные пользователи получают доступ к сети. Выступая в качестве «парадной двери « уровень доступа использует списки доступа, которые предназначены для предотвращения доступа к сети несанкционированных пользователей. Уровень доступа также предоставляет доступ к узлам удаленных сетей с использованием технологий распределенных сетей, таких как Frame Relay, ISDN или выделенные линии.

3. Обзор уровня доступа в коммутируемых локальных сетях

Создание LAN-сети, которая удовлетворит потребности средних и крупных организаций значительно облегчается, если при ее проектировании используется иерархическая модель. Использование такой модели также значительно облегчает внесение в сеть изменений по мере роста организации.

Уровень доступа является точкой входа в сеть для рабочих станций пользователей и серверов. В кампусной LAN в качестве устройства уровня доступа может выступать концентратор или коммутатор. Если используется концентратор, то доступная полоса пропускания используется совместно всеми устройствами. Если используется коммутатор, то полоса пропускания является выделенной для каждой пары устройств, осуществляющих соединение.

Если две или более рабочих станции или два сервер непосредственно подсоединены к портам коммутатора, то вся полоса пропускания соединения с коммутатором предоставляется компьютерам, осуществляющим соединение. Если два или более компьютера подсоединены к концентратору, то каждому компьютеру предоставляется полоса пропускания, равная обшей полосе пропускания, поделенной на количество подсоединенных к концентратору компьютеров. Концентратор может быть подсоединен к порту коммутатора. В этом случае полоса пропускания используется совместно всеми устройствами, подсоединенными к порту коммутатора через концентратор.

- Уровень доступа выполняет следующие функции:
- предоставление совместно используемой полосы пропускания;
- предоставление коммутируемой полосы пропускания;
- фильтрация на MAC-уровне;
- микросегментация.

Фильтрация на MAC-уровне позволяет коммутаторам направлять фреймы непосредственно на порт коммутатора, соединенный с требуемым устройством-получателем. Коммутатор создает небольшие сегменты 2-го уровня, называемые микросегментами. Эти коллизионные домены могут вктючать в себя всего лишь два устройства (т.е. устройство-получатель и соединенный с ним порт коммутатора). На уровне доступа используются коммутаторы 2-го уровня.

Коммутаторы уровня доступа

Как показано на рис. 2, коммутаторы уровня доступа функционируют на 2-м уровне эталонной модели OSI и, в частности, предостаатяют службу виртуальных локальных сетей (virtual LAN — VLAN). Главной целью коммутатора уровня доступа является соединение конечных пользователей с сетью. Коммутатор уровня доступа должен выполнять эту функцию с минимальными затратами и максимальной плотностью портов.

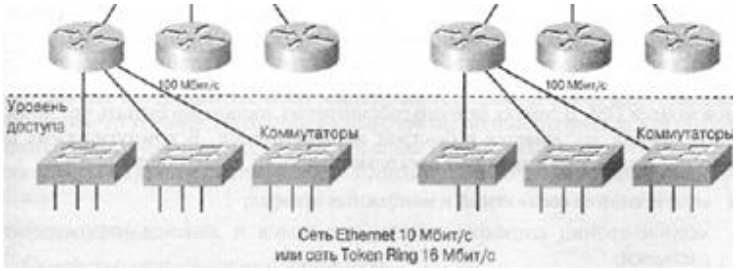


Рис. 2. Коммутаторы уровня доступа

Часто ошибочно полагают, что три рассматриваемых уровня (базовый, распределения и доступа) должны быть явно выражены конкретными физическими устройствами, однако это не является обязательным. На самом деле эти три уровня определяются для успешного проектирования сети и четкого определения функций, которые должна выполнять сеть. Конкретный способ реализации этих уровней зависит от потребностей проектируемой сети. Однако важно помнить, что для того, чтобы сеть оптимально функционировала и сохраняла масштабируемость по мере ее роста, в процессе ее проектирования должен быть соблюден иерархический принцип.

Обзор уровня распределения

Уровень распределения расположен между уровнем доступа и базовым уровнем и предназначен для определения и отделения базового уровня. Его функция состоит в задании границ, в которых может происходить какая-либо обработка пакетов. На этом уровне происходит сегментация сети на отдельные широковещательные домены. Здесь же с помощью списков доступа может определяться политика и производиться фильтрация пакетов. Этот уровень обеспечивает изоляцию основной части сети от проблем, которые могут возникать в рабочих группах, с тем чтобы они не затрагивали базовый уровень. Коммутаторы этого уровня могут работать на 2-м и 3-м уровнях эталонной модели OSI. В рамках данного рассмотрения достаточно считать что коммутация 3-го уровня заключается в быстрой маршрутизации. В коммутируемых сетях уровень распределения выполняет несколько функций, в частности.

- агрегирование соединений в монтажных шкафах;
- задание границ широковещательных доменов и доменов многоадресатной рассылки;
- VLAN-маршрутизация;
- все переходы из одной среды передачи в другую;
- обеспечение безопасности.

Коммутаторы уровня распределения

Коммутаторы уровня распределения представляют собой точки концентрации (агрегирования) нескольких коммутаторов уровня доступа. Эти коммутаторы должны быть способны обрабатывать весь объем данных, поступающих от устройств уровня доступа и поэтому должны иметь высокую производительность.

Коммутатор уровня распределения является граничной точкой широковещательного домена. На уровне распределения происходит объединение потоков данных виртуальных локальных сетей; этот уровень является фокусной точкой для принятия решений о политике доступа к сети и управления потоками данных. Коммутаторы уровня распределения работают как на 2-м, так и на 3-м уровнях эталонной модели OSI. По этой причине коммутаторы этого уровня часто называют многоуровневыми коммутаторами. Они соединяют в одном устройстве функции маршрутизатора и коммутатора, однако предназначены для коммутации потоков данных с большей скоростью, чем это делает обычный маршрутизатор. Если в таких многоуровневых коммутаторах отсутствует встроенный маршрутизирующий модуль, то для выполнения функций 3-го уровня используется внешний маршрутизатор.

Устройствам уровня распределения требуется меньшее количество *интерфейсов (interfaces)* и меньшая скорость коммутации, чем коммутаторам базового уровня, поскольку им приходится обрабатывать меньшие объемы данных.

Уровень распределения отделяет друг от друга уровень доступа и базовый уровень и помогает четко очертить их соответствующие функции (рис. 3). Этот уровень определяет границы функциональной области, в которой происходят операции с пакетами. Уровень распределения может выполнять несколько функций, в частности:

- агрегирование адресов или зон;
- управление доступом на уровне отдела или рабочей группы;
- определение границ широковещательной и многоадресатной рассылки;
- управление маршрутизацией сетей VLAN;
- все переходы из одной среды передачи в другую;
- обеспечение безопасности.

В средах, не являющихся сетями кампусов, уровень распределения может быть точкой перераспределения между доменами маршрутизации или точкой демаркации между протоколами статической и динамической маршрутизации. Он может также быть точкой доступа с удаленных узлов к корпоративной сети.

В целом уровень распределения можно охарактеризовать как уровень, на котором обеспечиваются соединения пользователей в соответствии с принятой в сети политикой.

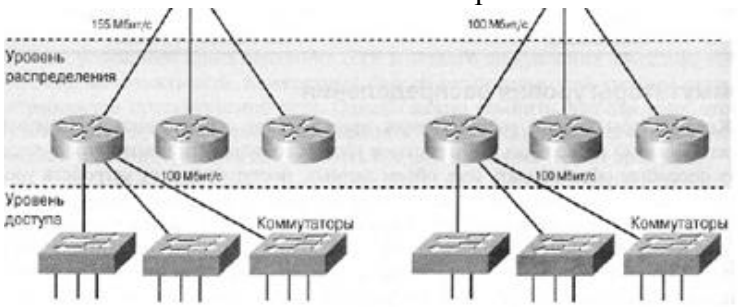


Рис. 3. Коммутатор уровня распределения

Обзор базового уровня

Поскольку базовый уровень является центральной частью сети, он должен быть спроектирован для быстрой и надежной работы. Использование на базовом уровне списков доступа нежелательно, поскольку они вносят дополнительную задержку. Более того, сам доступ конечных пользователей к базовому уровню весьма нежелателен. В иерархической сети данные конечных пользователей должны попадать на маршрутизаторы базового уровня только после того, как они прошли уровни доступа и распределения, где к ним могут быть применены списки доступа. Поскольку маршрутизация на базовом уровне осуществляется без использования списков доступа, трансляции адресов и других операций с пакетами, может показаться, что для выполнения столь простой задачи достаточно даже и маломощных маршрутизаторов. Однако верно как раз обратное — на этом уровне используются самые мощные маршрутизаторы, поскольку в них используются самые быстрые технологии коммутации и они имеют наибольшее количество физических интерфейсов.

Коммутаторы базового уровня

Как показано на рис. 4, базовый уровень является магистралью сети кампуса использующей коммутацию. Коммутаторы этого уровня могут использовать ряд технологий 2-го уровня. Если расстояния между коммутаторами базового уровня невелики, то для связи коммутаторов между собой может использоваться технология Ethernet. Также могут использоваться и другие технологии 2-го уровня, такие как асинхронный режим передачи ячеек (Asynchronous Transfer Mode — ATM). При проектировании сети в качестве базового уровня может быть использован уровень маршрутизации (3-й уровень). Коммутаторы базового уровня должны при необходимости обеспечивать эффективное выполнение функций 3-го уровня. Перед тем, как выбрать базовый коммутатор, следует рассмотреть такие факторы как потребности сети, стоимость коммутатора и его производительность.

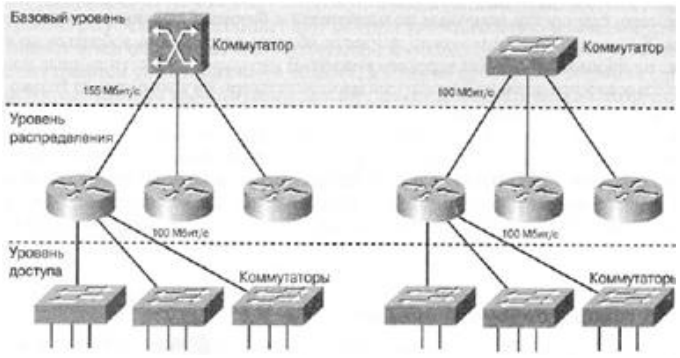


Рис. 4. Коммутаторы базового уровня

Контрольные вопросы

1. Что такое коммутатор и какие функции он выполняет?
2. На какие уровни делиться LAN при иерархическом подходе к прктированию?
3. Какие функции выполняются на уровне доступа?
4. Какие функции выполняются на уровне распределения?
5. Какие функции выполняются на базовом уровне?

Лекция 16
Начальные сведения о сетях VLAN

1. **Основные сведения о VLAN**
2. **Широковещательные домены в сетях VLAN и маршрутизаторы**
3. **Преимущества сетей VLAN**
4. **VLAN-сети и безопасность**
5. **Типы VLAN-сетей**

Ключивые слова: VLAN, масштабирование, сегментация, статические сети, динамические сети, сквозная VLAN-сеть, брандмауэр, концентратор, конфигурирование, магистральный протокол.

1. Основные сведения о VLAN

Одной из важных функций, реализуемых в технологии Ethernet, являются *виртуальные локальные сети VLAN,* в которых для объединения рабочих станций и серверов в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN-сети, возможна только с устройствами этой же сети, поэтому сеть с коммутацией функционирует как несколько индивидуальных, не соединенных друг с другом локальных сетей LAN. Трудно дать общее строгое определение сетей VLAN, поскольку разные производители используют различные подходы к созданию таких сетей.

Компании часто используют сети VLAN в качестве способа логической группировки пользователей. Это можно сравнить с традиционной организацией рабочих мест, в которой несколько отделов обычно группировались в локальный департамент и локальная сеть естественным образом решала задачи связи для этого департамента. В настоящее время сотрудники часто не связаны с конкретным физическим рабочим местом, поэтому сети VLAN создают не физическую, а логическую группу пользователей. Например, сотрудники, работающие в отделе маркетинга, объединены VLAN-сетью маркетинга, а сотрудники инженерного подразделения — VLAN-сетью инженерных служб.

Сети VLAN решают задачи масштабирования сети, обеспечения безопасности и сетевого управления. В сетях с топологией VLAN маршрутизаторы обеспечивают фильтрацию широковещания, решают задачи зашиты сети и упраыения потоками данных.

Сеть VLAN представляет собой группу сетевых устройств и служб, не ограниченную физическим сегментом или коммутатором. На рис. 1. показано логическое группирование рабочих станций в сети VLAN, в сравнении с физическим группированием рабочих станций в традиционной сети LAN.

Сети VLAN логически сегментируют сети, использующие коммутацию, на основе их организационных функций, принадлежности к различным рабочим коллективам (группам) или используемым приложениям, а не на базе физического или географического расположения. Например, все рабочие станции и серверы, используемые некоторой рабочей группой, могут быть объединены в одну и ту же сеть VLAN, независимо от их физического подсоединения к сети или расположения на территории предприятия.

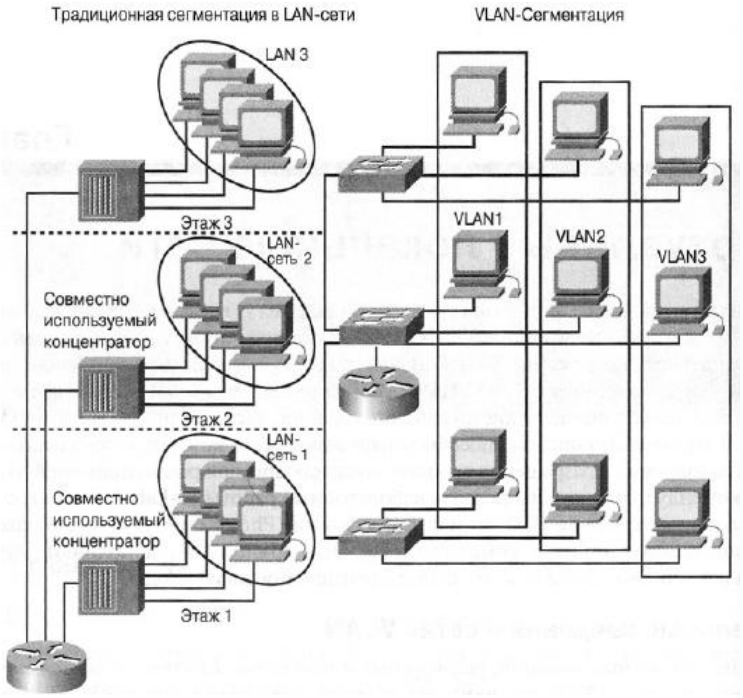


Рис. 1. Сети VLAN и физические границы

На рис. 2 приведен пример проектирования сети VLAN в физической сети. В данном случае создаются три сети VLAN, в которых рабочие станции соединены друг с другом через коммутаторы, а сами коммутаторы соединены друг с другом через маршрутизатор. Реконфигурирование системы может быть выполнено программным способом, без физического перемещения устройств и изменения подключения кабелей.

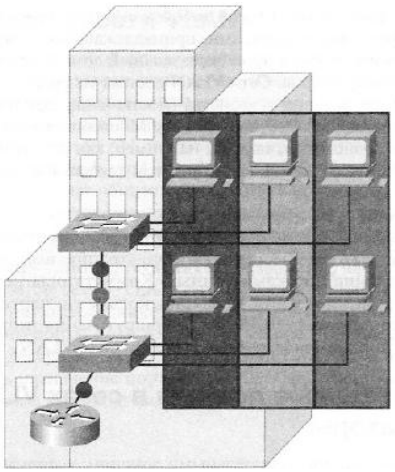


Рис. 2. Проектирование виртуальной локальной сети

На рис. 3 показано физическое проектирование сети VLAN, основанное на различных рабочих группах компании и их расположении на различных этажах офиса. В данном случае сеть VLAN создается для каждого отдела (инженерный отдел, отдел маркетинга и отдел учета), в каждом из которых имеется свой коммутатор.

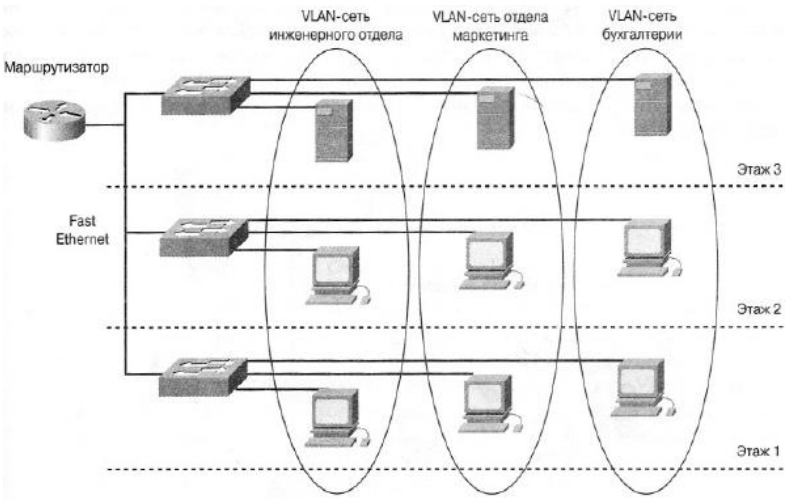


Рис. 3. Сети VLAN охватывают определенное физическое пространство

Как правило, соединения клиентской рабочей станции, находящейся в сети VLAN, ограничены только файловыми серверами, принадлежащими этой же сети VLAN. Сеть VLAN можно рассматривать как широковещательный домен, который существует в определенном наборе коммутаторов. Сети VLAN состоят из ряда конечных систем, таких как рабочие станции или сетевые устройства (мосты и маршрутизаторы), соединенных друг с другом через отдельный мостовой домен. Мостовой домен поддерживается различными сетевыми устройствами, такими, например, как коммутаторы сетей LAN, которые работают по мостовым протоколам; при этом для каждой сети VLAN имеется своя мостовая группа.

Сети VLAN создаются для реализации служб сегментации, которые в традиционных LAN-конфигурациях обычно обеспечиваются маршрутизаторами. В топологиях сетей VLAN маршрутизаторы обеспечивают фильтрацию *широковещания (broadcast).* защиту сети и управление потоками данных. Коммутаторы не могут осуществлять мостовые соединения между сетями VLAN, поскольку это нарушило бы целостность широковещательного домена сети VLAN. Маршрутизация потоков данных должна происходить только при передаче данных между сетями VLAN.

2. Широковещательные домены в сетях VLAN и маршрутизаторы

Сеть VLAN является широковещательными доменом, который создается одним или более коммутаторами. В приводимом ниже сценарии при проектировании сети требуется создать два отдельных широковещательных домена. На рис. 4 два отдельных широковещательных домена создаются с помощью трех отдельных коммутаторов — по одному на каждый широковещательный домен. Следует отметить, что маршрутизатор позволяет осуществлять маршрутизацию пакетов между широковещательными доменами, которые в данном случае подобны отдельным группам устройств 3-го уровня.

Это может быть сделано путем установки одного или нескольких соединений с маршрутизатором.

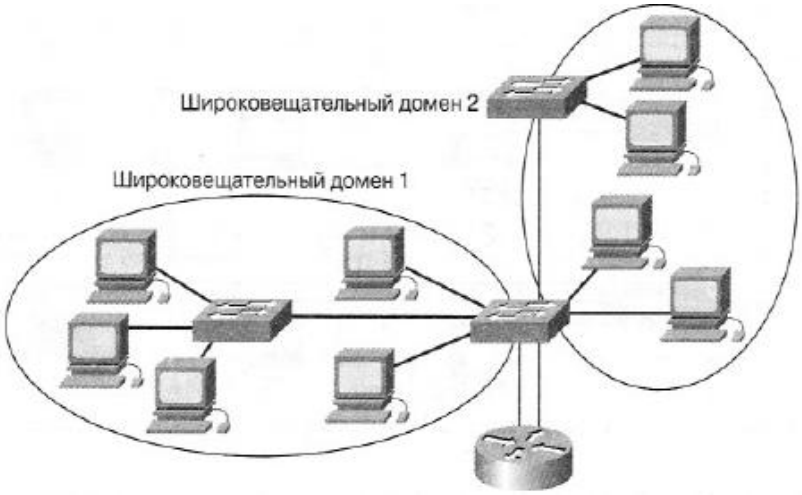


Рис. 4. Распределение широковещания в сети VLAN

3. Функционирование сети VLAN

Сеть VLAN представляет собой сеть коммутации, которая логически сегментируется в соответствии с выполняемыми функциями, объединением сотрудников в группы или согласно используемым приложениям, независимо от физического расположения пользователей. Сети VLAN может быть выделен любой порт коммутатора. Порты, выделенные одной и той же сети VLAN, имеют общее пространство широковещания.

Порты, не принадлежащие к этой сети VLAN, не получают эти широковещательные сообщения. Это повышает общую производительность сети, поскольку уменьшается количество ненужных широковещательных сообщений, которые потребляют полосу пропускания сети. Сети VLAN создаются двумя описанными ниже способами.

Статические сети - этот способ также называется членством на базе порта. Назначение портов сетям VLAN создает статическое распределение VLAN.

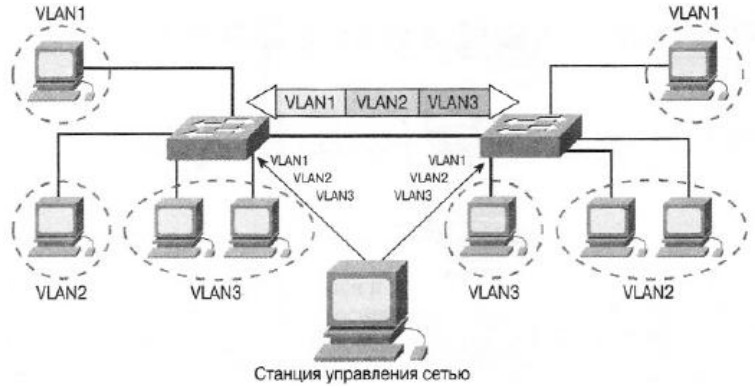


Рис. 5. Статические сети VLAN

Когда устройство подсоединяется к порту, оно автоматически попадает во VLAN-сеть этого порта. Если устройство меняет порт своего подключения, но ему требуется доступ к той же самой сети VLAN, то сетевой администратор должен сделать назначение порта сети VLAN для нового соединения. Пример такого назначения приведен на рис. 5.

Динамические сети VLAN — динамические сети VLAN создаются с использованием пакетного программного обеспечения, такого как CiscoWorks 2000. С помощью сервера политик управления сетями VLAN (VLAN Management Policy Server — VMPS) можно назначать порты коммутатора сетям VLAN динамически, на основе MAC-адреса устройства-источника, подсоединенного к данному порту. В настоящее время динамические VLAN позволяют присоединять к себе устройства на основе MAC-адреса источника. Когда устройство присоединяется к сети, оно делает запрос в базу данных на сервере VMPS относительно своей принадлежности к дан-

ной сети VLAN. Этот процесс показан на рис. 6, где каждый коммутатор имеет свой уникальный MAC-адрес.

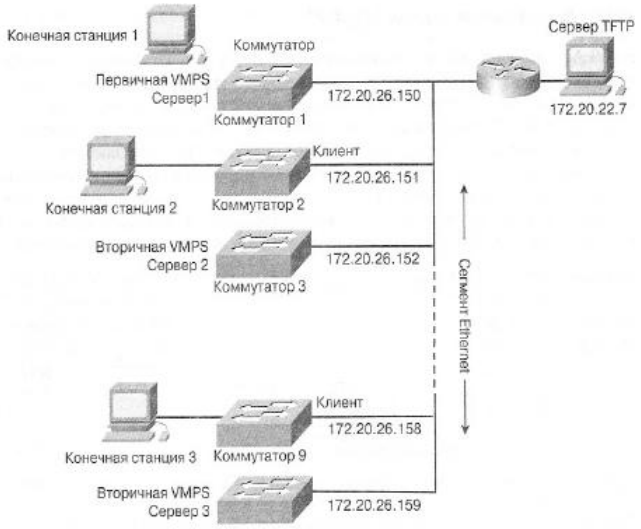


Рис. 6. Динамические сети VLAN

Принадлежность устройства к статической сети VLAN на основе портов проиллюстрировано на рис. 7. Конкретной сети VLAN назначается порт, который не зависит от пользователя или системы, подсоединенной к данному порту. Это означает, что все пользователи, подсоединенные к данному порту, должны быть членами одной и той же сети VLAN. Отдельная рабочая станция пользователя или концентратор, к которому подсоединены несколько рабочих станций, могут быть подсоединены к отдельному порту коммутатора. Назначение портов сетям VLAN обычно осуществляет сетевой администратор. Конфигурация порта в этом случае является статической и переключение порта на другую VLAN не может быть выполнено автоматически без реконфигурирования коммутатора. Следует обратить внимание на то, то каждая сеть VLAN находится в отдельной подсети, а маршрутизатор используется для связи между этими подсетями.

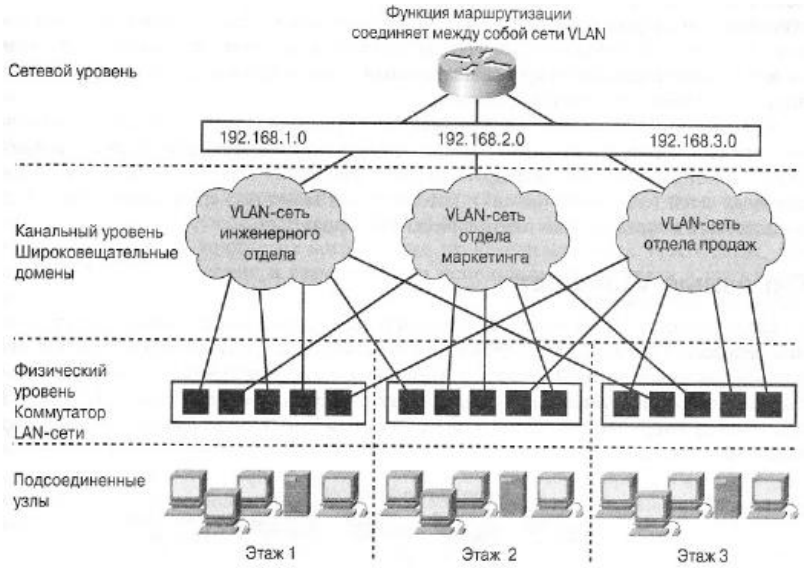


Рис. 7. Статические виртуальные сети на основе портов

Когда пользователи подсоединяются к этому совместно используемому сегменту, как это происходит в традиционных основанных на концентраторах сетях LAN, все они после этого используют общую полосу пропускания. На каждого дополнительного пользователя, который подсоединяется к совместно используемой среде передачи, приходится меньше доступной полосы пропускания, поскольку все пользователи находятся в одном и том же коллизионном домене. Если количество пользователей, использующих одну и ту же полосу пропускания становится слишком большим, то начинаются частые коллизии и работа приложения пользователя становится малопроизводительной. Коммутаторы уменьшают вероятность коллизий за счет обеспечения выделенной полосы пропускания между устройствами с помощью микросегментации; однако коммутаторы по-прежнему рассылают всем пользователям широковещательные сообщения, такие, как сообщения протокола ARP. Сети VLAN обеспечивают пользователям большую полосу пропускания в совместно используемой сети путем создания отдельных широковещательных доменов.

По умолчанию на каждом порте коммутатора имеется сеть VLAN1 или сеть VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Следует помнить о том, что каждый интерфейс коммутатора ведет себя как порт моста и в целом коммутатор можно рассматривать как многопортовый мост. Мосты отфильтровывают потоки данных, которые не требуется направлять в иные сегменты, кроме того, из которого они поступили. Если фрейм необходимо переслать через мост и MAC-адрес получателя известен, то мост направляет этот фрейм на соответствующий интерфейс и не направляет на все остальные. Если мосту или коммутатору не известно расположение получателя, то происходит лавинная рассылка фрейма со всех портов в данный широковещательный домен (VLAN), за исключением того порта, с которого этот фрейм поступил.

Каждой виртуальной сети VLAN должен быть присвоен уникальный адрес 3-го уровня (сети или подсети). Это помогает осуществлять коммутацию пакетов между сетями VLAN, в которых имеются маршрутизаторы. Сети VLAN могут выступать в качестве сквозных сетей (end-to-end network), которые охватывают всю среду коммутатора, или существовать в определенных географических границах.

Сквозные VLAN-сети

Сквозные сети VLAN позволяют группировать устройства на основе использования ресурсов. Оно включает в себя уровень использования сервера, рабочие группы по выполняемым проектам и отделы. Цель сквозных сетей VLAN состоит в том, чтобы не менее 80% данных передавались внутри локальной сети VLAN. На рис. 8 приведен пример сквозных сетей VLAN.

Географические VLAN-сети

По мере того, как корпоративные сети централизовали свои ресурсы, становилось все сложнее поддерживать сквозные VLAN-сети. Пользователям требовались различные ресурсы, многие из которых уже не находились в их VLAN-сетях. По причине такого изменения в размещении и использования ресурсов в настоящее время VLAN-сети все чаше создаются в определенных географических границах,|а не в границах сообщества. Эти географические границы могут быть целым зданием или всего лишь одним коммутатором в монтажном шкафу. В такой географической VLAN-структуре типичным является случай соотношения обмена данными

20% для локального использования и 80% — для удаленных соединений. Это соотношение прямо противоположно тому, которое обычно устанавливается при проектировании сквозных VLAN. Хотя такая топология означает, что пользователю приходится пересекать устройство 3-го уровня (маршрутизатор) для получения доступа к 80% ресурсов, она позволяет использовать в сети последовательный детерминистический способ получения доступа к ресурсам.

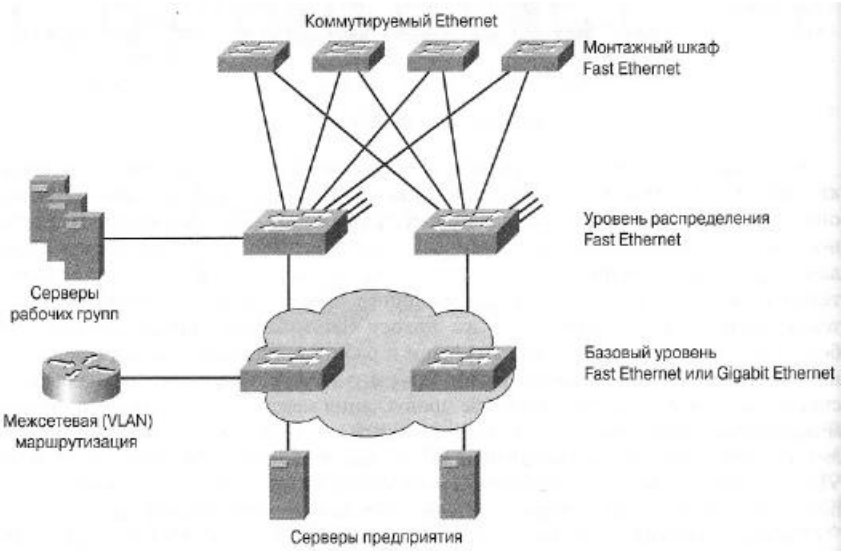


Рис. 8. Сквозные VLAN-сети

Географическими сетями VLAN также значительно легче управлять и концептуализировать их, чем VLAN-сетями, устройства которых находятся в географически различных областях.

3. Преимущества сетей VLAN

Коммерческие компании постоянно реорганизуются. В среднем 20-40% рабочей силы физически меняют место проживания каждый год. Эти переезды, добавление новых пользователей, и другие изменения являются одними из главных головных болей сетевых менеджеров и составляют одну из самых больших статей расходов, связанных с управлением сетью. Многие перемещения пользователей требуют прокладки новых кабелей и почти все перемещения требуют новой адресации станций и реконфигурирования концентраторов и маршрутизаторов.

Изменения в системе управления сетью

Сети VLAN предоставляют эффективный механизм для управления изменениями в топологии сети и значительно снижают затраты, связанные с реконфигурированием концентраторов и маршрутизаторов. Пользователи сети VLAN могут использовать одно и то же сетевое адресное пространство (т.е. IP-подсеть), независимо от их физического расположения. Когда пользователи сети VLAN перемещаются из одного места в другое, до тех пор пока они остаются в одной и той же VLAN и подсоединены к одному и тому же порту коммутатора, их сетевые адреса не изменяются. Изменение расположения пользователя требует лишь таких простых действий как включение штекера пользователя в соответствующий порт VLAN-коммутатора и конфигурирование порта коммутатора, к которому подсоединена данная VLAN. В динамических сетях VLAN при просматривании MAC-адреса сетевого адаптера переместившейся рабочей станции в

VMPS, коммутатор автоматически конфигурирует порт таким образом, чтобы он оказался в требуемой сети VLAN.

4. VLAN-сети и безопасность

VLAN сети являются эффективным механизмом расширения сферы действия брандмауэра от маршрутизаторов к среде коммутатора и защиты сети от потенциально опасных проблем, связанных с широковещанием. Кроме того, сети VLAN сохраняют все преимущества высокопроизводительной коммутации.

Рис. 9. Широковещательные домены

Брандмауэры создаются путем назначения портов коммутатора или пользователей в конкретные группы VLAN как на одном коммутаторе, так и на нескольких соединенных друг с другом коммутаторах. Широковещательные потоки данных не передаются за пределы сети VLAN. На рис. 9 приведен пример широковещательных доменов. В свою очередь смежные порты не получают широковещательных данных, которые генерируются другими сетями VLAN. Такой тип конфигурации значительно уменьшает общий объем широковещательных данных, освобождает полосу пропускания для действительно полезных данных и снижает общий уровень уязвимости сети в отношении широковещательных штормов. На рис. 10 показано как маршрутизатор может выполнять функции брандмауэра между сетями VLAN.

Одной из проблем совместно используемых сетей LAN является относительная легкость проникновения в них. Подключаясь к работающему порту несанкционированный пользователь получает доступ ко всем данным, передаваемым в сегменте. Чем больше группа пользователей, тем большие возможности создаются для потенциального несанкционированного доступа.

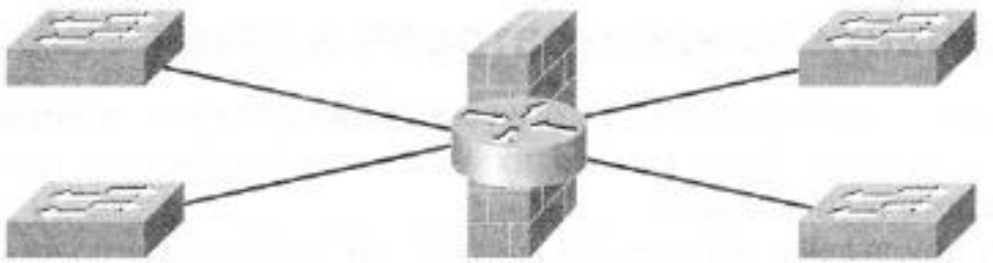


Рис. 10. Брандмауэр для широковещательных данных

Одним из экономически эффективных и легко административно реализуемых способов повышения уровня безопасности в сети является сегментация сети на несколько широковещательных групп. Это позволяет сетевому менеджеру решить следующие задачи:

- ограничить количество пользователей во VLAN-группе;
- предотвратить присоединение других полей без предварительного получения разрешения от приложения, управляющего сетью VLAN;
- сконфигурировать все неиспользуемые порты на принимаемую по умолчанию службу нижнего уровня VLAN.

Реализация такого типа сегментации относительно проста. Порты коммутатора объединяются в группы на основе типа приложения и привилегий при доступе. Ограниченные приложения и ресурсы обычно размещаются в защищенных VLAN-группах. В защищенных сетях VLAN коммутатор ограничивает доступ пользователей к группе. Ограничения могут основываться на адресах станций, типах приложений или типах протокола. Пример обеспечения безопасности в сети VLAN показан на рис. 11.

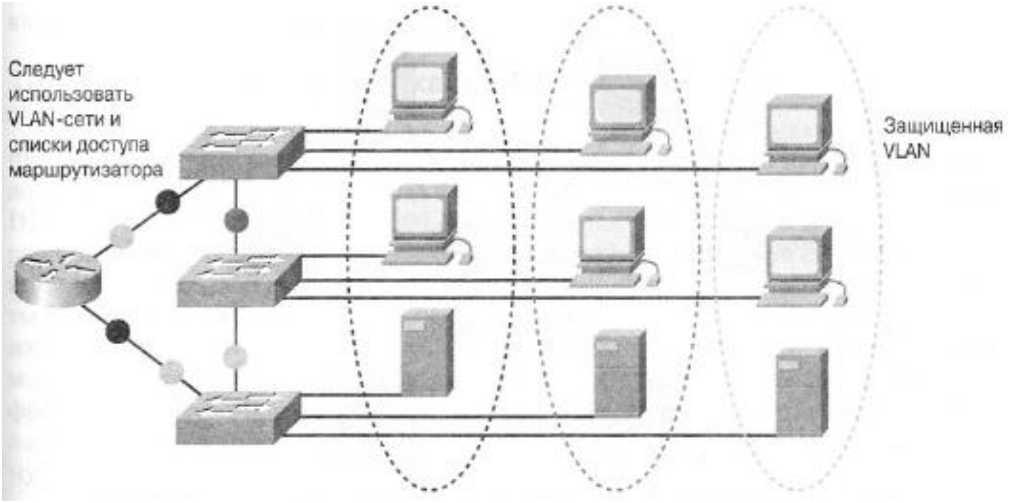


Рис. 11. Защищенная VLAN-сеть

Использование концентраторов в сетях VLAN

За последние несколько лет сетевые администраторы установили большое количество концентраторов. Многие из этих устройств заменяются настоящее время коммутирующими технологиями.

Непосредственно на рабочем столе, эти концентраторы по-прежнему выполняют полезные функции по многих уже существующих сетях. Сетевые менеджеры могут сэкономить средства. Подсоединив существующие концентраторы к коммутаторам. Пример такого использования концентраторов приведен на рис. 12. каждый сегмент концентратора, подсоединенный к порту коммутатора, может быть назначен только одной сети VLAN. Все станции, совместно использующие сегмент концентратора, становятся членами одной и той же группы VLAN. Коммутатор поддерживает несколько адресов доступа к среде передачи или MAC-адресов (Media Access Control — MAC), по одному на каждую станцию, которые логически связаны с портом, к которому подсоединен концентратор. Если требуется переназначить отдельную станцию в другую VLAN-сеть, то станцию необходимо подсоединить к соответствующему концентратору. Соеди-

ненные между собой коммутаторы обрабатывают передачу данных между портами коммутатора и автоматически определяют соответствующие принимающие сегменты. Чем больше мелких групп будет образовано на совместно используемом концентраторе, тем больше степень микросегментации и тем большая гибкость обеспечивается для назначения индивидуальных пользователей в группы VLAN. Путем подсоединения концентраторов к коммутаторам можно сконфигурировать концентраторы в качестве части архитектуры VLAN. Можно также обеспечить совместное использование передачи данных и сетевых ресурсов, непосредственно подсоединенных к коммутирующим портам с получателями VLAN.

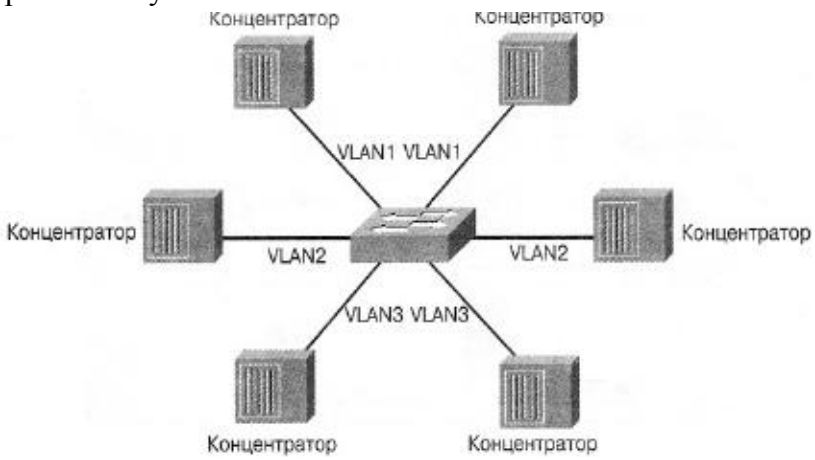


Рис. 12. Использование существующих концентраторов в среде коммутации сети VLAN

5. Типы VLAN-сетей

Три приведенных ниже базовых модели определяют назначение пакета сети VLAN и управляют его передачей.

- Сети VLAN, базирующиеся на портах (статические).
- VLAN-сети на основе MAC-адресов (динамические).
- Основанные на протоколах VLAN-сети.

Количество образованных на одном коммутаторе VLAN-сетей может изменяться в широких пределах, в зависимости от нескольких факторов. Среди этих факторов можно выделить типичный характер передачи данных, типы приложений, потребности сетевого управления и общей группы. Кроме того, важным фактором, определяющим количество VLAN-сетей на коммутаторе, является используемая схема IP-адресации. Например, предположим, что сеть использует 254-битовую маску для определения подсетей. В этом слу4чае в одной подсети можно использовать до 254 адресов для рабочих станций. Поскольку настоятельно рекомендуется устанавливать взаимно однозначное соответствие между сетями VLAN и IP-подсетями, в одной VLAN-сети может быть не более 254 устройств.

Конфигурирование VLAN

Первоначально сетевые администраторы полагали, что сети VLAN упростят их работу и сделают ненужными маршрутизаторы. К сожалению для них, эти надежды не оправдались. Сети VLAN не устранили *проблем, связанных с 3-м уровнем модели OSI. Сети VLAN позволяют легче решать задачи 3-го уровня, такие, например, как разработка более простых списков доступа, однако необходимость в маршрутизации на 3-м уровне не исчезла.*

Конфигурирование статических VLAN-сетей

Под статическими VLAN понимаются порты коммутатора, которым вручную назначаются сети VLAN путем использования управляющего программного обеспечения или непосредственным конфигурированием коммутатора. Эти порты поддерживают назначенную им конфигурацию VLAN сетей до тех пор пока она не будет изменена системным администратором. Хотя статические VLAN требуют в несения изменений вручную, они безопасны, легко конфигурируются и удобны для мониторинга. Этот тип VLAN хорошо работает в сетях, в которых соблюдаются следующие условия:

- перемещения станций легко контролируются и управляются;
- имеется надежное управляющее программное обеспечение для конфигурирования портов коммутатора;
- нежелательная дополнительная служебная нагрузка, требуемая для поддержки MAC-адресов конечных станций и типовых таблиц фильтрации.

Динамические VLAN, в отличие от статических, не полагаются на порты, котором назначаются конкретные VLAN сети. Вместо этого назначение VLAN-сетей портам основывается на MAC-адресах, логической адресации или типе протокола. При конфигурировании статических VLAN-сетей на маршрутизаторах следует помнить следующие основные положения:

- максимальное количество подключаемых VLAN-сетей зависит от типа коммутатора и ограничивается количеством его портов;
- сеть VLAN1 является одной из VLAN-сетей, создаваемых по умолчанию производителем;
- по умолчанию VLAN 1 является VLAN-сетью;
- по сети VLAN 1 рассылаются анонсирования маршрутов протокола обнаружения устройств *(Cisco Discovery Protocol — CDP)* и магистрального протокола VLAN (*VLAN Trunking Protocol — VTP);*
- на всех коммутаторных магистралях, принимающих участие в работе VLAN-сетей, должен быть сконфигурирован один и тот же протокол инкапсуляции, такой как 802.1Q или ISL;
- команды конфигурирования VLAN-сетей зависят от номера модели;
- IP-адреса находятся в широковещательном домене **VLAN;**
- при создании, добавлении и удалении VLAN-сетей коммутатор должен находиться в режиме VTP-сервера.

Создание на коммутаторе статической VLAN-сети является несложной задачей. При использовании коммутатора, работающего с командами IOS Cisco, следует войти в режим конфигурирования VLAN с помощью команды привилегированного EXEC-режима **vlan database.** Для создания VLAN-сети следует выполнить приведенные ниже команды.

Switcht# vlan database
Switch (vlan)# vlan vlan_number [vlan_name]
Switch(vlan)# exit

При необходимости следует также сконфигурировать имя VLAN-сети.

После выхода из режима конфигурирования на коммутаторе создается VLAN-сеть. Следующим этапом является назначение данной VLAN одному или более интерфейсам.

Протестировать конфигурацию можно с помощью команды show running-config.

Тестирование конфигурации VLAN-сети

Хорошей практикой является тестирование конфигурации VLAN-сети с помощью команд **show vlan**, **show vlan brief** или **show vlan id** *id_ntmber*

При работе с VLAN-сетями следует руководствоваться следующими положениями:

- созданная VLAN-сеть остается неиспользуемой до тех пор, пока она не будет логически связана с портами коммутатора;
- по умолчанию все порты Ethernet находятся в сети VLAN 1.
- между номерами портов не следует вводить пробелы. В этом случае коммутатор реагирует сообщением об ошибке, поскольку пробел отделяет другой аргумент, который не является структурной частью команды.

Контрольные вопросы

1. Что такое VLAN и когда они применяются?
2. По какому признаку делятся узды в VLAN?
3. Какими способами создаются VLAN?
4. В чем заключается приемущество VLAN?
5. Каким образом осущетвлятся безопасность VLAN?

Лекция 17
Магистральный протокол VLAN

1. **Магистральные соединения**
2. **Сети VLAN и магистральные каналы**
3. **Межсетевая VLAN-маршрутизация**

Ключивые слова: магистраль, trunk, виртуальный канал, фрейм, инкапсуляция, VLAN-сеть, процессор маршрутов, стандартный шлюз, логический интерфейс, подынтерфейс.

1. Магистральные соединения

История *магистральных соединений (trunking)* уходит своими корнями в радио- и телефонные технологии. В радиотехнологиях под магистралью понимается отдельная линия связи, по которой передается информация нескольких каналов радиосигналов.

В телефонии понятие магистрали связано с маршрутом телефонной связи или Каналом между двумя точками (одним из которых обычно является центральная АТС). Пример магистрали приведен на рис. 1. Магистрали общего пользования могут быть созданы для создания избыточности при связи между центральными АТС (central offices — CO) (рис. 2)

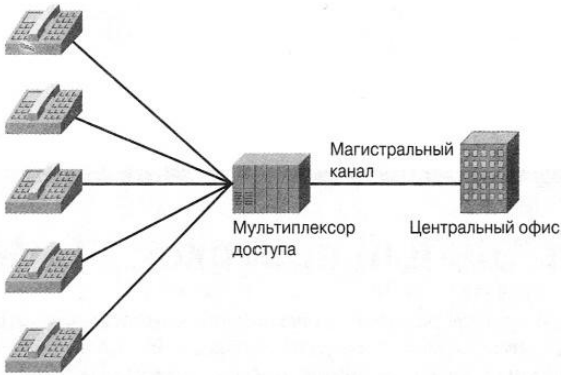


Рис.1. Магистральный канал

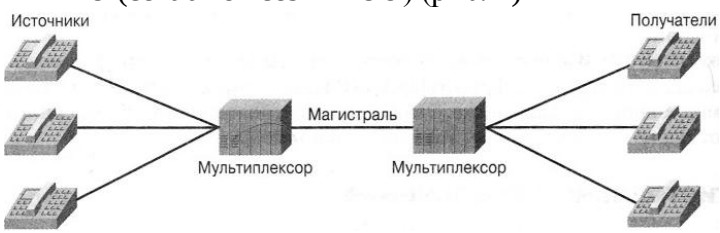


Рис.2. Общий магистральный канал

То же понятие магистрали, которое использовалось в телефонии и радиоиндустрии, было принято в аппаратном обеспечении телекоммуникаций. Примером этого может служить сегмент сети связи, в котором сходится несколько каналов, как показано на рис. 3. Магистраль состоит из нескольких магистральных каналов.

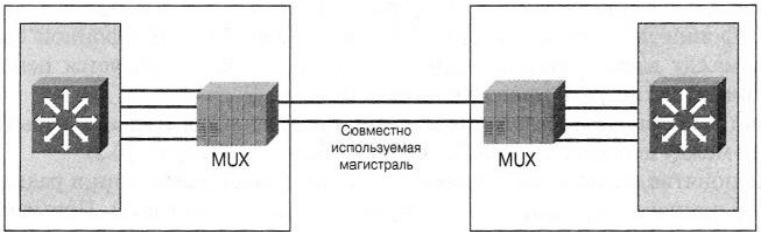


Рис. 3. Магистральные каналы, использующие мультиплексирование с разделением фреймов

В настоящее время этот же принцип создания магистралей применяется в технологиях коммутации, в которых под магистралью понимается физическое и логическое соединение между двумя коммутаторами, по которому передаются данные между сетями.

Понятие магистрали

Под *магистралью (trunk)* понимается отдельный канал передачи между двумя точками, которыми обычно являются центры коммутации. Магистраль представляет собой физическое соединение, по которому проходят логические каналы.

В контексте среды коммутации VLAN-сетей магистраль является каналом типа «точка-точка», который поддерживает несколько VLAN-сетей. Целью использования магистралей является экономия портов при создании канала связи между двумя устройствами, реализующими VLAN-сети, обычно этими устройствами являются два коммутатора. На рис. 4 показаны две VLAN-сети, которые выходят на коммутаторы Sa и Sb.

Рис. 4. Зачем нужна магистраль?

При использовании первого подхода, проиллюстрированного на рис. 4, создаются два физических канала между устройствами, по каждому из которых передаются данные для отдельной VLAN-сети. Такое решение трудно масштабировать. При добавлении третьей VLAN-сети придется пожертвовать двумя портами. Такой подход неэффективен также в плане распределения нагрузки, поскольку использование отдельного выделенного канала для некоторых VLAN может оказаться неоправданным. Магистраль объединяет несколько виртуальных (логических) каналов в один физический канал.

Функционирование магистрали

По мере увеличения числа VLAN-сетей, данные которых передаются по магистрали, использование существующих обычных таблиц коммутации на обоих концах магистрали, основанных на MAC-адресах, находящихся в передаваемых фреймах, становится медленным и сложным. Чем больше размер таблицы, которую требуется хранить коммутатору, тем медленнее становится процесс принятия решения об отправке фреймов на соответствующие порты. Для эффективного управления передачей фреймов от различных VLAN-сетей по одному физическому каналу или линии между двумя сетевыми устройствами требуется новый способ связи или язык коммуникации между этими двумя устройствами. Такой способ связи или протокол, используется для того, чтобы эти устройства могла «договориться» о передаче и последующем распределении фреймов на соответствующие порты на обоих концах магистрали. Для этой цели были созданы различные магистральные протоколы.

Эти магистральные протоколы позволяют осуществлять передачу фреймов от различных VLAN-сетей по одному физическому кагалу; они также управляют распределением фреймов на соответствующие логически связанные VLAN-порты. В настоящее время применяются два магистральных механизма: фильтрация фреймов и добавление ним тегов. На рис. 5 приведен пример магистральных каналов.

В магистральных протоколах используется механизм добавления тегов, который назначает фреймам некоторый идентификатор, что облегчает управление этими фреймами соответствен-

но, ускоряет их доставку получателям. Теги добавляются к фреймам на том конце магистрали и удаляются на другом. Такие фреймы не являются широковещательными (т.е. предназначены только одному устройству на другом конце магистрального канала).

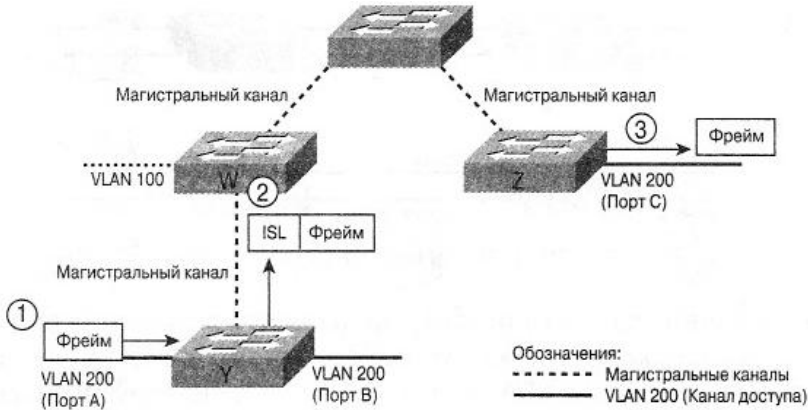


Рис. 5. Магистральные каналы

Уникальный физический канал между двумя коммутаторами может передавать данные, предназначенные для любой VLAN-сети.

2. Сети VLAN и магистральные каналы

Для реализации магистральных соединений требуется соблюдать некоторые правила или протоколы. Механизмы магистральных соединений облегчают расширение VLAN-сетей, использующих коммутацию. Сеть VLAN представляет собой группу устройств одной или более локальных сетей LAN, которые сконфигурированы (с использованием управляющего программного обеспечения) таким образом, чтобы они могли осуществлять между собой связь как если бы они были подключены к общей шине, тогда как в действительности они расположены в различных LAN-сегментах. Использование магистралей предоставляет эффективный метод распределения ID-информации VLAN сетей другим коммутаторам и связи между коммутаторами, как показано на рис. 6.

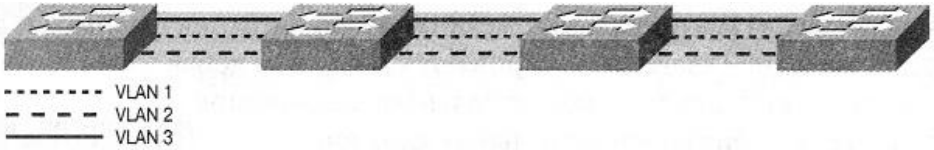


Рис. 6. Сети VLAN и магистральные каналы

Присвоение тегов является стандартным механизмом магистральных соединений; по сравнению с фильтрацией фреймов присвоение тегов предоставляет большие возможности масштабирования при реализации VLAN-сетей, которые могут быть реализованы в сети кампуса. Спецификация IEEE 802.1Q определяет присвоение тегов как способ реализации VLAN-сетей. Пример присвоения тегов приведен на рис.7.

Метод присвоения тегов фреймам виртуальных сетей VLAN был специально разработан для коммутируемых соединений. Операция добавления тега заключается в размещении в заголовке каждого фрейма уникального идентификатора для передачи его по сетевой магистрали. Каждый коммутатор просматривает и анализирует этот идентификатор перед тем как рассылать

его широковещательно или передать другим коммутаторам, маршрутизаторам или конечным станциям. Когда фрейм покидает сетевую магистраль, коммутатор удаляет идентификатор перед отправкой этого фрейма конечной станции-получателю. Идентификация фреймов осуществляется на 2-м уровне и не требует трудоемкой обработки или передачи служебной информации.

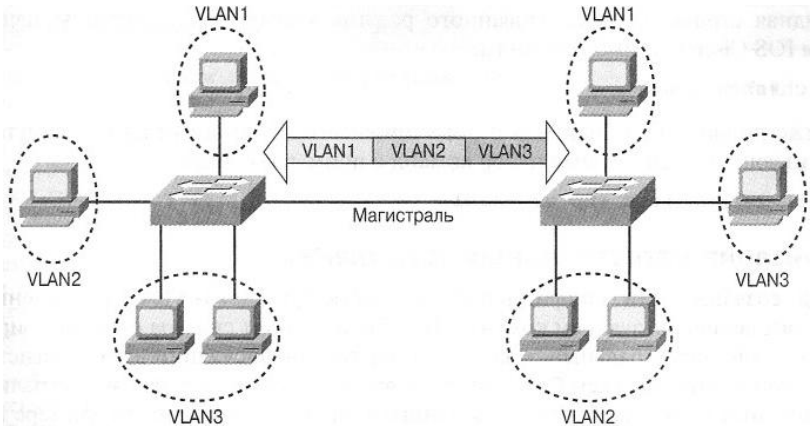


Рис. 7. Присвоение тегов

Магистральный канал не принадлежит ни одной конкретной VLAN-сети. Назначение магистрального канала состоит в том. чтобы обеспечить канал связи между коммутаторами и маршрутизаторами для VLAN-сетей

Коммутаторы на рис. 10.6 осуществляют связь друг с другом, используя протокол ISL, поддерживающий информацию о VLAN-сетях при передаче данных между коммутаторами. При использовании протокола ISL фрейм Ethernet инкапсулируется с заголовком, который содержит ID сети VLAN.

Реализация магистральных соединений

Для создания или конфигурирования магистрального VLAN-соединения на коммутаторе, использующем команды IOS Cisco, следует сначала сконфигурировать этот порт как магистральный, а затем указать тип инкапсуляции в этой магистрали. Тип инкапсуляции должен быть одним и тем же на обоих концах магистрали.

Перед конфигурированием VLAN-магистрали на порте коммутатора необходимо выяснить, какой тип инкапсуляции поддерживается этим портом. Это можно сделать, выполнив команду **show port capabilities** на коммутаторе, использующем специальный набор команд.

Для создания или конфигурирования магистрального VLAN-соединения на коммутаторе, использующем специальный набор команд, следует выполнить команду **set trunk** для конфигурирования портов на обоих концах канала как магистральных и указать VLAN-сети, данные которых будут передаваться по этому магистральному каналу.

Команда **set trunk** может быть также использована для изменения режима работы магистрали.

Ключевыми словами для магистральных режимов технологий Fast Ethernet и Gigabit Ethernet являются следующие:

- **on**. Этот режим переводит порт в постоянное состояние магистрального соединения. Порт становится магистральным даже в том случае, если соседний порт не соглашается на такое

изменение. Состояние on не позволяет обсуждать тип инкапсуляции; следовательно тип инкапсуляции должен быть указан в конфигурации.

- **off.** Этот режим переводит порт в постоянное немагистральное состояние. При этом обсуждается преобразование канала в немагистральный. При этом порт становится не магистральным даже в том случае, если соседний порт не согласен на такое изменение.

3. Межсетевая VLAN-маршрутизация

Если узлу в одном широковещательном домене требуется выполнить обмен данными с узлом другого широковещательного домена, то требуется использование маршрутизатора. Аналогичная ситуация возникает и в сетях VLAN.

Пример такой ситуации показан на рис. 8.

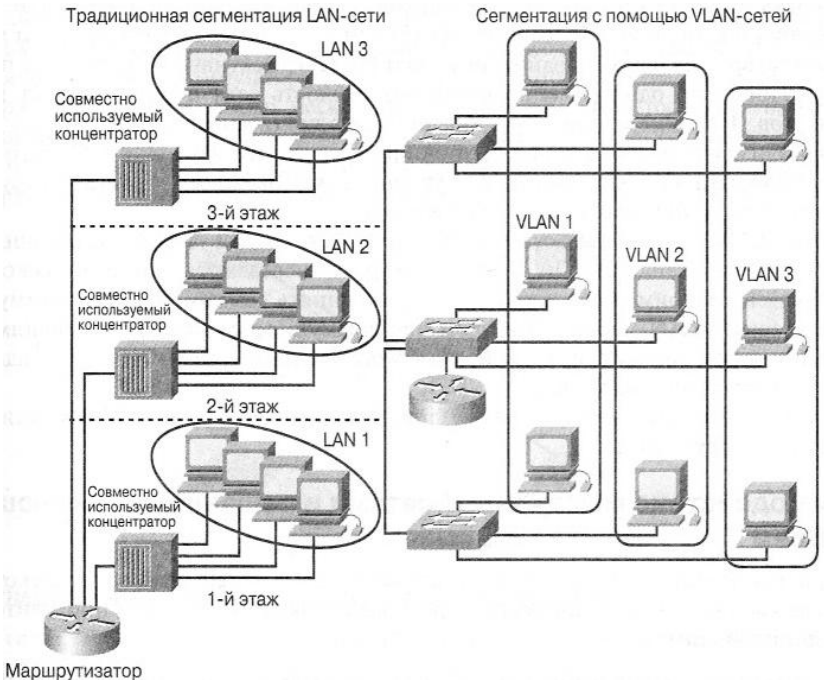


Рис. 8. Маршрутизаторы и виртуальные локальные сети VLAN

Порт 1 коммутатора является частью сети VLAN 1, а порт 2 — частью сети VLAN 200. Если бы все порты коммутатора принадлежали сети VLAN 1, то все узлы, подсоединенные к этим портам, могли бы осуществлять связь между собой. Однако в данном случае порты принадлежат различным VLAN-сетям: сети VLAN 1 и сети VLAN 200. Если узлы принадлежат различным VLAN-сетям и им требуется осуществить обмен данными, то требуется использование маршрутизатора, как показано на рис. 9.

Важным достоинством маршрутизации является ее проверенная временем способность облегчать поддержку работы сетей, особенно крупных. Наиболее очевидным примером этого является глобальная сеть Internet, однако это верно и для всех остальных типов сетей, таких, в частности, как магистрали крупной сети кампуса. Поскольку маршрутизаторы предотвращают распространение широковещательных сообщений и используют более интеллектуальные алгоритмы пересылки, чем мосты и коммутаторы, их использование позволяет более эффективно

использовать полосу пропускания. Это одновременно повышает гибкость сети и оптимизирует выбор маршрутов.

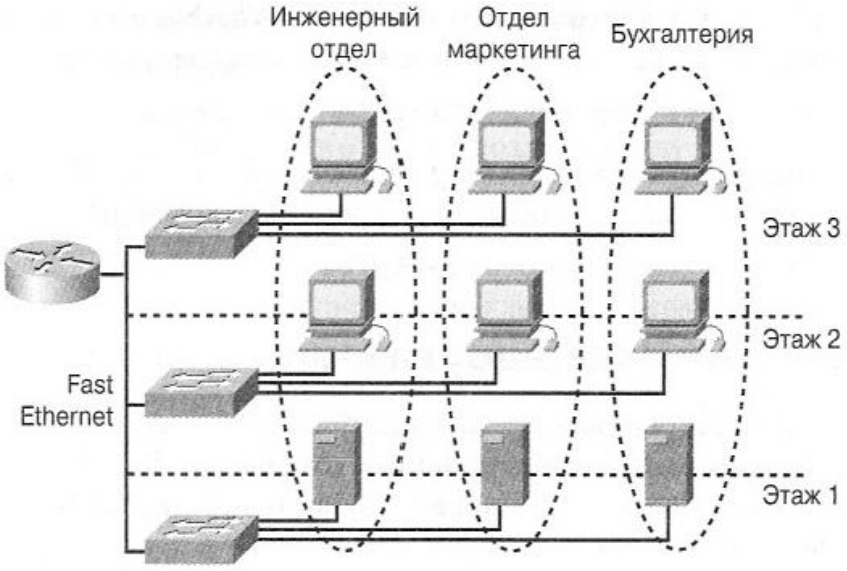


Рис. 9. Устранение физических границ

Если VLAN-сеть охватывает несколько устройств, то эти устройства соединяются магистральным канатом. По этой магистрали передаются данные нескольких VLAN-сетей. Например, магистраль может соединять два коммутатора, коммутатор с межсетевым VLAN-маршрутизатором или коммутатор с сервером, имеющим специальную карту сетевого интерфейса (network interface card — NIC) и поддерживающим магистральные каналы.

Следует учитывать, что для связи узлов, находящихся в разных VLAN-сетях, необходим маршрутизатор.

Взаимодействие между VLAN-сетями и решение возникающих проблем

При соединении между собой нескольких VLAN-сетей возникают некоторые технические проблемы. Чаще всего в среде нескольких VLAN-сетей приходится решать две проблемы:

- получение устройствами конечного пользователя доступа к нелокальным узлам;
- осуществление связи между узлами различных VLAN-сетей.

Когда устройству требуется осуществить обмен данными с удаленным узлом, оно просматривает свою таблицу маршрутизации в поисках известного маршрута. Если удаленный узел находится в известной подсети, то система проверяет, можно ли связаться с ним через данный интерфейс. Если все известные маршруты не позволяют осуществить связь, то у системы остается только один способ — использовать стандартный маршрут. Этот маршрут относится к специальному типу шлюзовых маршрутов и обычно в системе имеется только один такой маршрут.

Связь между различными VLAN-сетями может осущестатяться через логическое или физическое соединение. Логическое соединение осуществляется по отдельному или магистральному каналу от коммутатора к маршрутизатору. Этот магистральный канал может поддерживать передачу данных нескольких VLAN-сетей. Такая топология называется «приклеиванием маршрутизатора» («router on a stick»), поскольку при этом имеется лишь одно соединение с маршрутизатором, однако несколько логических соединений маршрутизатора с коммутатором.

Изолированные широковещательные домены

В сетях, использующих коммутацию, связь между различными VLAN-сетями осуществляется с помощью процессоров маршрутов (Route Processor).

Эти процессоры обеспечивают доступ VLAN-сетей к совместно используемым ресурсам и соединения с другими частями сети, которые либо логически сегментированы с помощью более традиционного деления на подсети, либо требуют доступа к удаленным узлам по каналам распределенных сетей. Процессоры маршрутов во многом аналогичны маршрутизаторам, однако они могут быть встроены в коммутатор.

Перед конфигурированием маршрутизации между VLAN-сетями необходимо определить VLAN-сети на коммутаторах сети. Вопросы, связанные с проектированием и определением VLAN-сетей, должны быть решены на этапе проектирования всей сети.

Рис. 10. Изолированные широковещательные домены

При этом должны быть решены следующие вопросы:

- совместное использование ресурсов VLAN-сетями;
- распределение нагрузки;
- избыточность каналов;
- логическая адресация;
- сегментирование сети с помощью VLAN-сетей.

На рис. 10 показаны изолированные широковещательные домены.

Нахождение маршрута между VLAN-сетями

Процессор маршрутов (Route Processor) содержит большинство компонентов системной памяти и главный процессор системы.

Стандартным шлюзом (default gateway) называется интерфейс маршрутизатора, который обычно идентифицируется своим IP-адресом. *Стандартным маршрутизатором или маршрутизатором по умолчанию (default router)* называется маршрутизатор, у которого есть хотя бы один интерфейс, выступающий в качестве стандартного шлюза. Для протокола DHCP стандартным считается маршрутизатор, предоставляющий пул IP-адресов. На рис. 11 показан стандартный шлюз.

При подсоединении отдельных подсетей через процессор маршрутов возникает вопрос о том, как осуществлять связь устройствам конечного пользователя с другими устройствами через несколько LAN-сегментов. Некоторые сетевые устройства используют таблицы маршрутизации для идентификации мест доставки пакетов, находящихся вне данного локального сегмента локальной сети.

Несмотря на то, что конечные устройства не отвечают за маршрутизацию данных, они могут оказаться способными отправлять данные по адресам подсетей, отличных от их собственных.

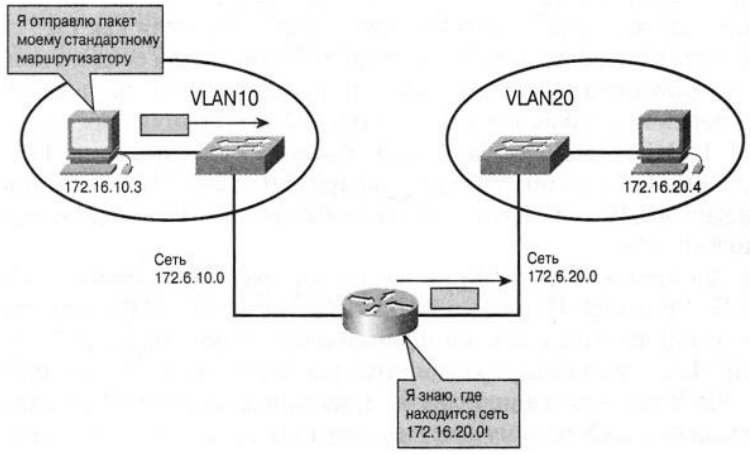


Рис. 11. Стандартный шлюз

Поэтому, хотя конечные устройства не обязаны управлять своими собственными таблицами маршрутизации, большинство этих устройств конфигурируются с IP-адресами назначенного процессора маршрутов. Этот назначенный процессор маршрутов представляет собой стандартный маршрутизатор, которому посылаются все пакеты, получатели которых не принадлежат данному локальному сегменту.

Физические и логические интерфейсы

В обычных ситуациях *сети,* имеющей, например, четыре VLAN-сети, требовались четыре физических соединения между коммутатором и внешним маршрутизатором. По мере того, как все шире использовались такие технологии как ISL, сетевые проектировщики стали использовать магистральные каналы для соединения маршрутизаторов с коммутаторами.

По мере того, как в сети увеличивается количество VLAN-сетей, физический подход, состоящий в выделении одного интерфейса маршрутизатора каждой VLAN-сети быстро становится неприемлемым. В сетях с большим количеством VLAN приходится использовать магистральные VLAN-соединения и назначать несколько VLAN одному физическому интерфейсу маршрутизатора.

Первичным преимуществом использования магистральных каналов является сокращение количества требуемых портов на коммутаторах и маршрутизаторах. Это не только сокращает расходы, но также уменьшает сложность конфигурирования сети. При таком подходе к маршрутизатору может быть подсоединено значительно большее количество VLAN-сетей чем при проектировании отдельных каналов для каждой VLAN-сети.

Создание подынтерфейсов на физическом интерфейсе

Подынтерфейсом (subinterface) называется логический интерфейс на физическом интерфейсеНа одном физическом интерфейсе могут быть созданы несколько подынтерфейсов.

Каждый подынтерфейс поддерживает одну VLAN-сеть и имеет свой IP-адрес. Для того, чтобы несколько устройств одной и той VLAN могли осуществлять связь друг с другом, их IP-адреса должны принадлежать одной и той же сети или подсети. Например, если подынтерфейс 2 имеет IP-адрес 192.168.1.1, то 192.168.1.2, 192.168.1.3 и 192.1.1.4 являются IP-адресами устройств, подсоединенных к подынтерфейсу 2. Для передачи данных между VLAN-сетями с подынтерфейсами необходимо создать подынтерфейсы для каждой.

Контрольные вопросы

1. Что такое магистраль?
2. Как осуществляется функционирование магстрали?
3. Какую функцию выполняют магитсральные каналы в VLAN?
4. Как осуществляется маршрутизация в VLAN?
5. Каким образом происходит находжение маршрута между VLAN?

Лекция 18
Технология глобальных сетей

1. **Аналоговые соединения удаленного доступа**
2. **Технология ISDN**
3. **Технология X.25**
4. **Технология Frame Relay**
5. **Технология ATM**
6. **Виртуальные каналы**

Ключивые слова: модем, телефонные линии, WAN-сеть, интерфейс, маршрутизатор, канал, пакет, абонент, широкополосная коммутация, скорость передачи, VPN-туннель.

1. Аналоговые соединения удаленного доступа

В тех случаях, когда по сети передаются небольшие объемы данных и потоки данных имеют пульсирующий характер, использование модемов и аналоговых телефонных линий позволяет осуществлять коммутируемые выделенные соединения с небольшой пропускной способностью (рис. 1).

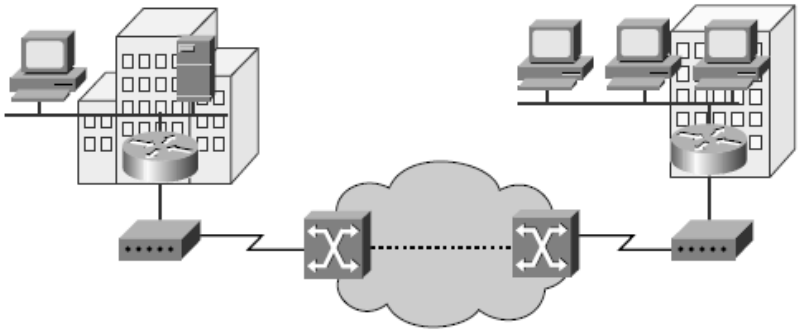


Рис.1. Сети WAN, использующие модемы

В традиционной телефонии телефонный аппарат пользователя соединен с сетью PSTN медным кабелем, называемым локальным ответвлением. Во время телефонного разговора сигнал в локальном ответвлении представляет собой электрическую копию голоса абонента и является непрерывно изменяющимся сигналом.

Локальное ответвление не позволяет непосредственно передавать двоичные компьютерные данные, однако при использовании модема компьютерные данные могут быть переданы по голосовой телефонной сети. Модем модулирует бинарные данные на аналоговых сигналах и, наоборот, демодулирует аналоговые сигналы в бинарные данные.

Скорость такого преобразования ограничена физическим характеристиками локального ответвления и его подсоединения к PSTN и не может превышать верхнего предела, равного примерно 33 Кбит/с. Эта скорость может быть повышено до примерно 56 Кбит/с при условии, что сигнал поступает из цифрового источника.

На небольших предприятиях эта скорость может оказаться удовлетворительной для таких операций, как обмен коммерческой информацией и для электронной почты. Для передачи

больших файлов или резервирования данных пользователь может воспользоваться преимуществами низкой стоимости такой связи в нерабочее время и в выходные дни. Тарифы такой связи зависят от расстояния между конечными точками, времени суток и продолжительности вызова.

Преимуществами использования модема и аналоговой линии являются простота и небольшая стоимость реализации. Недостатками являются невысокая скорость передачи и относительно большое время, затрачиваемое на установку соединения.

Часто в ситуациях, когда используются модемы, довольно длительное время установки соединения не вызывает проблем. Постоянная выделенная линия не вызывает задержки и дребезжания для данных, передаваемых по каналу «точка-точка», однако голосовые и видеоданные не могут адекватно передаваться при таких низких скоростях.

Технология ISDN

За прошедшее время передача по соединениям или магистралям сети PSTN аналоговых мультиплексированных сигналов с разделением частот уступила место передаче мультиплексированных цифровых сигналов с разделением времени (time division multiplexed - TDM). Очевидным следующим шагом является перевод локального ответвления на передачу цифровых сигналов, что обеспечивает коммутируемые соединения с большей полосой пропускания.

Служба цифровой сети интегрированных служб (Integrated Services Digital Network - ISDN) превращает локальное ответвление в цифровое соединение TDM. Это соединение имеет каналы носителя с полосой пропускания 64 Кбит/с (B-каналы) для передачи голоса и данных и сигнальный канал (дельта-канал или D-канал) для установки вызова и других целей.

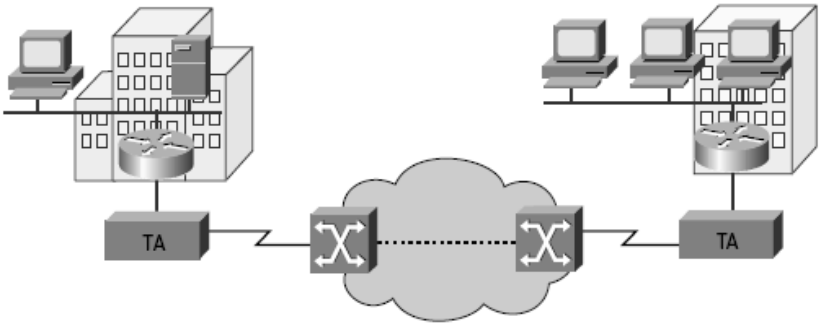
Интерфейс базовой скорости ISDN (Basic Rate Interface - BRI), предназначенный для домашних офисов и малых предприятий, обеспечивает два B-канала и один D-канал с полосой пропускания 16 Кбит/с. Для более крупных предприятий предназначен интерфейс первичной скорости передачи (Primary Rate Interface - PRI) ISDN.

Для небольших WAN-сетей BRI ISDN обеспечивает идеальный механизм связи. Интерфейс BRI имеет небольшое время установки вызова (менее одной секунды), а его B-канал 64 Кбит/с обеспечивает бо́льшую пропускную способность, чем аналоговый модемный канал. На рис. 2 показана WAN-сеть, в которой используется технология ISDN. Если требуется бо́льшая пропускная способность, то возможна активизация второго B-канала, что обеспечивает пропускную способность 128 Кбит/с. Хотя и недостаточное для передачи видео, такое повышение позволяет поддерживать в дополнение к передаче данных нескольких телефонных разговоров.

Другим возможным применением технологии ISDN является ее использование при необходимости в качестве дополнительного источника полосы пропускания для уже имеющегося соединения по выделенной линии. Выделенная линия проектируется для основных потоков нагрузки, а ISDN добавляется при пиковых нагрузках.

ISDN может быть также использована в качестве резервной линии в случае непредвиденных сбоев в выделенной линии.

Тарифы службы ISDN на каждый B-канал аналогичны тарифам голосовых соединений, т.е. два одновременных соединения 64 Кбит/с стоят вдвое больше, чем одно.



При использовании интерфейса PRI ISDN две конечные точки могут быть соединены несколькими B-каналами, что позволяет обеспечить видеоконференцию или несколько широкополосных соединений для передачи данных без задержки или дребезжания.

Рис. 2. WAN-сеть, использующая технологию ISDN

На больших расстояниях использование нескольких соединений может стать весьма дорогостоящим.

Выделенные линии

В тех случаях, когда требуются постоянные выделенные соединения, используются арендуемые линии с пропускной способностью до 2,5 Гбит/с.

Каналы «точка-точка» обеспечивают заранее установленные каналы связи сетей WAN от офиса пользователя к удаленной сети через несущую сеть, такую, например, как сеть телефонной компании. Каналы «точка-точка» обычно арендуются у оператора связи и поэтому часто называются арендованными линиями. Операторы связи предлагают выделенные линии с различными возможными значениями пропускной способности.

Стоимость выделенной линии обычно определяется требуемой полосой пропускания и расстоянием между соединяемыми точками. Каналы «точка-точка» обычно стоят дороже, чем службы совместного использования, такие как Frame Relay. Стоимость решений, использующих выделенные линии, значительно возрастает, если эти линии соединяют большое количество сетевых узлов. Пропускная способность выделенных линий обеспечивает отсутствие задержки и дребезжания. Для некоторых приложений, таких как электронная торговля, существенна постоянная доступность таких соединений.

Выделенные линии часто используются для построения WAN-сетей, как показано на рис. 3, поскольку обеспечивают постоянную выделенную полосу пропускания. Такие линии традиционно пользуются большим спросом, однако они имеют и ряд недостатков. Объем передачи данных по сети WAN часто изменяется, поэтому полоса пропускания канала редко соответствует конкретным потребностям пользователей.

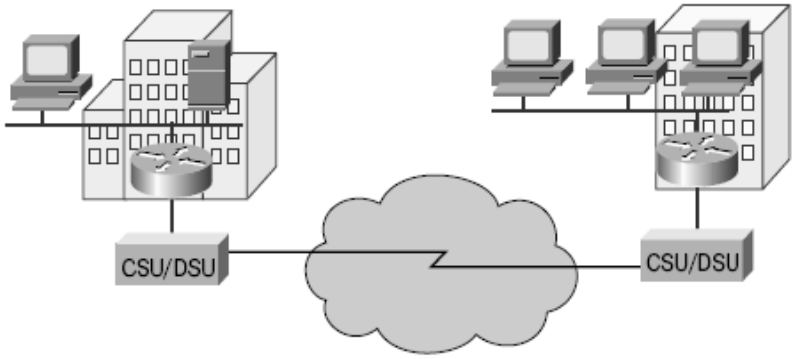


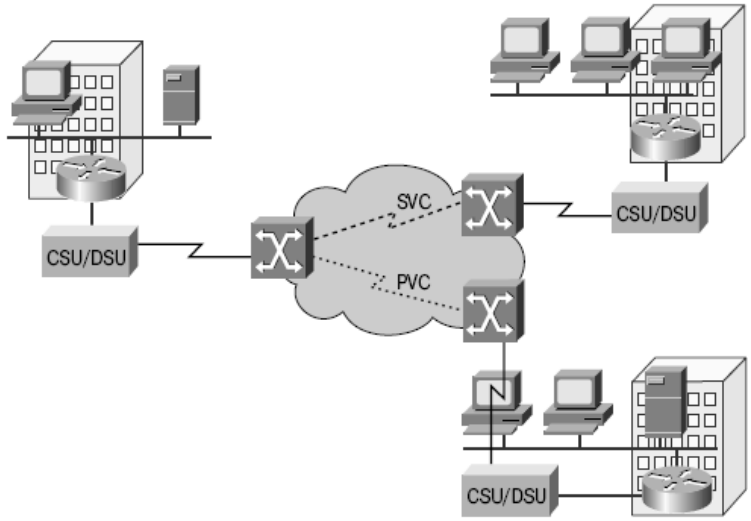
Рис. 3. WAN-сети с выделенными линиями

Кроме того, каждой конечной точке требуется отдельный интерфейс маршрутизатора, поэтому маршрутизатор в центральной точке звездообразной топологии оказывается весьма дорогостоящим. Любые изменения параметров выделенной линии, как правило, требуют посещения узла оператором для изменения пропускной способности.

Выделенные линии могут использоваться для создания непосредственных соединений типа «точка-точка» между сетями LAN предприятия. Они также используются для подсоединения отдельных филиалов к сети с коммутацией пакетов. В таком канале могут быть мультиплексированы несколько соединений, что уменьшает длину линии и требования к количеству интерфейсов центральных маршрутизаторов в топологии сети.

Технология X.25

В противовес дорогостоящим выделенным линиям провайдеры служб телекоммуникаций разрабатывают сети с коммутацией пакетов, в которых совместное использование каналов уменьшает затраты пользователей. Первой из таких сетей с коммутацией пакетов была группа протоколов, стандартизованная как X.25. Служба протокола X.25 обеспечивает низкоскоростное совместно используемое соединение с переменной пропускной способностью, которое может быть постоянным или коммутируемым. На рис. 4 показана WAN-сеть протокола X.25.



Пользователи службы получают сетевой адрес. В такой сети могут быть созданы виртуальные каналы, по которым получателям передаются пакеты запроса на установку соединения. Созданный канал SVC идентифицируется своим номером. Пакеты данных, отмеченные этим номером, доставляются по соответствующему адресу. В одном соединении могут быть активными несколько каналов.

Рис. 4. WAN-сеть протокола X.25

Абоненты службы подсоединяются к сети X.25 по выделенным линиям или по соединениям удаленного доступа. В сетях X.25 также могут присутствовать предварительно установленные соединения между пользователями, которые представляют собой постоянные каналы PVC.

Сети X.25 могут оказаться очень эффективными в отношении стоимости, поскольку тарифы в них основаны на объеме переданных данных, а не на расстоянии или времени соединения. Доставка данных может происходить с любой скоростью вплоть до максимальной для данного соединения. Это качество сети обеспечивает определенный уровень гибкости при ее использовании. Сети X.25 обычно имеют невысокую пропускную способность, с максимальным значением равным 48 Кбит/с.

Кроме того, передача пакетов данных часто сопровождается задержками, характерными для совместно используемых сетей.

Технология Frame Relay

В связи с увеличением спроса на широкополосную коммутацию пакетов с низкой задержкой провайдеры связи стали использовать технологию Frame Relay (Frame Relay - FR). Хотя общая структура такой сети похожа на сеть X.25, допустимые скорости передачи в ней достигают значений до 4 Мбит/с, а некоторые провайдеры предлагают и бо́льшие скорости (рис. 5).

Сети Frame Relay отличаются от сетей X.25 в нескольких аспектах. Наиболее важным отличием является то, что Frame Relay использует значительно более простой протокол на канальном уровне. Для обозначения модуля данных на канальном уровне используется термин *фрейм (frame)*.

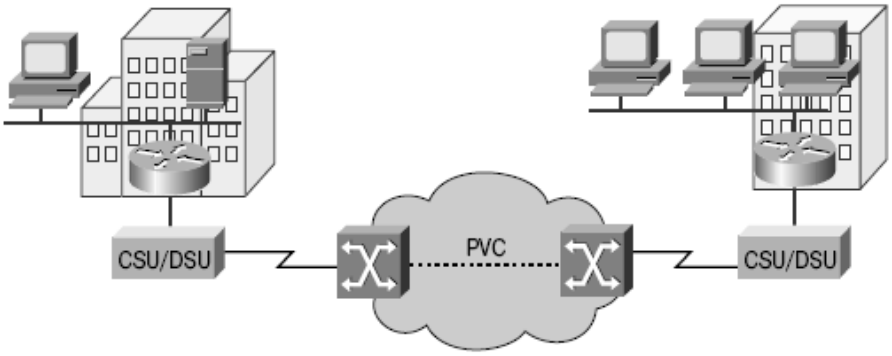


Рис. 5. WAN-сети протокола Frame Relay

Протокол Frame Relay не осуществляет контроля ошибок и управления потоками. Благодаря упрощенной обработке фреймов достигается малая задержка. Меры, принимаемые для предотвращения скопления фреймов на промежуточных коммутаторах, помогают уменьшить уровень дребезжания.

Большинство соединений Frame Relay используют постоянные каналы PVC, а не коммутируемые каналы SVC. Соединение с границей сети часто осуществляется по выделенной линии. Для установки канала SVC в одном или более B-каналов используется D-канал ISDN. Тарифы Frame Relay основываются на пропускной способности порта на границе сети и оговоренной в контракте полосе пропускания или согласованной скорости передачи информации (committed information rate - CIR) различных каналов PVC, проходящих через это порт.

Frame Relay обеспечивает постоянные, совместно используемые соединения со средней шириной полосы пропускания по которым передаются как обычные, так и голосовые данные. Технология Frame Relay является идеальным вариантом для соединения между собой LAN-сетей предприятия. Маршрутизатору LAN-сети требуется только один интерфейс, даже если используются несколько каналов VC, а короткая линия доступа или локальное ответвление к границе сети Frame Relay обеспечивает эффективные с точки зрения финансовых затрат соединения между разделенными большими расстояниями LAN-сетями.

Технология ATM

Параллельно с развитием технологии Frame Relay провайдеры служб связи осознали необходимость в технологии постоянного совместного использования с очень малой задержкой, низким уровнем дребезжания и полосой пропускания, значительно большей, чем была доступна ранее. Таким решением стала технология асинхронного режима передачи (Asynchronous Transfer Mode - ATM). В сетях ATM достигаются скорости передачи до 155 Мбит/с. Как видно из рис. 6, структура сети ATM аналогична структурам других сетей совместного доступа, таких как X.25 и Frame Relay, однако технология ATM обеспечивает соединения с очень высокими скоростями передачи данных. Эта технология особенно эффективна при передаче данных, для которых крайне нежелательна задержка, таких как видео.

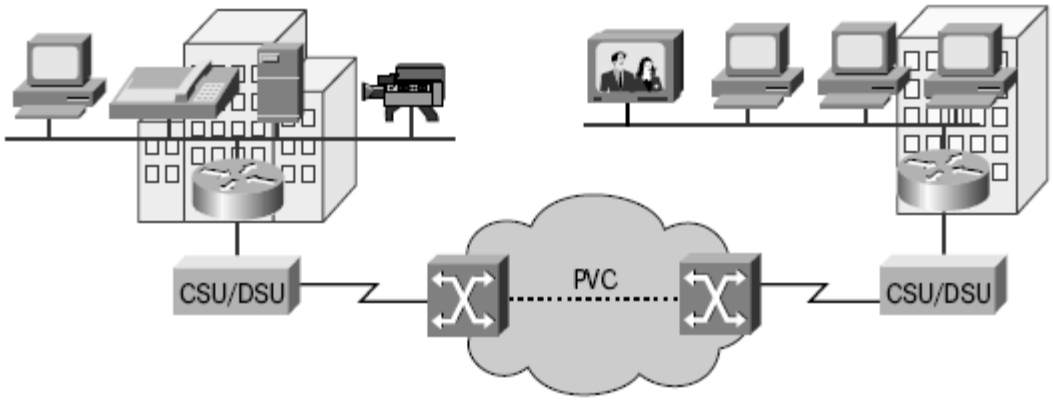


Рис. 6. WAN-сеть, в которой используется технология ATM

Режим асинхронной передачи (Asynchronous Transfer Mode - ATM) представляет собой технологию, позволяющую передавать голос, видео и обычные данные по открытым (общедоступным) и частным сетям. Основой архитектуры ATM являются не фреймы, а ячейки. Эти ячейки ATM имеют фиксированную длину 53 байта. Такая ячейка включает в себя 5-байтовый ATM-заголовок, за которым следуют 48 байтов полезной нагрузки. Используемые в ATM небольшие ячейки фиксированной длины 53 байта хорошо подходят для передачи голосовых и видеоданных, поскольку для таких данных недопустима задержка. Они не могут ожидать окончания передачи большого пакета данных. 53-байтовая ячейка ATM, в которой на 48 байтов полезной нагрузки приходится 5 байтов служебных данных, менее эффективна, чем имеющие больший размер фреймы и пакеты технологий Frame Relay и X.25. Если в ячейках передаются разбитые на части пакеты сетевого уровня, то уровень служебной нагрузки возрастает, поскольку коммутатор ATM должен быть способен собрать первоначальные пакеты в пункте назначения.

Для передачи одного и того же объема данных сетевого уровня типичной линии ATM требуется на 20% большая полоса пропускания, чем каналу Frame Relay.

В технологии ATM используются как каналы PVC, так и каналы SVC, хотя в WAN-сетях чаще используются постоянные каналы PVC. Как и в других технологиях совместного доступа, ATM позволяет реализовать несколько виртуальных каналов в одном соединении по выделенной линии с границей сети.

Виртуальные каналы

Технология Frame Relay, также, как X.25 и ATM, построена на концепции виртуальных каналов. Виртуальный канал — это полный набор программных отображений портов, содержащихся на двух взаимосвязанных устройствах Frame Relay. В роли таких устройств могут выступать как коммутаторы, так и конечные устройства, независимо от того, сколько между ними содержится коммутаторов. Каждому отображению, связанному с этим виртуальным каналом, соответствует идентификатор подключения канального уровня, который обсуждается в следующем подразделе текущего раздела. Каждый виртуальный канал обеспечивает двустороннюю передачу данных между конечными устройствами. Иными словами, виртуальный канал состоит из одного или нескольких (обычно из нескольких) соединений между устройствами Frame Relay, а каждое из этих соединений нумеруется идентификатором подключения канального уровня. В

свою очередь набор всех соединений между двумя конечными устройствами образует виртуальный канал.

Виртуальные каналы бывают трех типов: постоянные виртуальные каналы (Permanent Virtual Circuit — PVC), нежесткие каналы PVC (soft PVC — SPVC) и коммутируемые виртуальные каналы (Switched Virtual Circuit — SVC). Первоначально для технологии Frame Relay были предложены постоянные виртуальные каналы, которые до сих пор остаются самыми распространенными, однако в промышленности все большее распространение находят коммутируемые виртуальные каналы. Чтобы было легче различать постоянные и коммутируемые виртуальные каналы, канал PVC необходимо готовить или настраивать вручную во время заключения договора о предоставлении услуг. После того как канал PVC установлен, он работает постепенно (что следует из названия), до тех пор, пока абонент или поставщик услуг не прекратят контракт, который касается данного виртуального канала. Работа канала SVC также определяется контрактом между абонентом и поставщиком услуг, однако при этом такие каналы устанавливаются или разрываются (в них осуществляется переключение или установка связи) автоматически по требованию абонента. Как вы уже, наверное, догадались, если каналы используются не постоянно, то использование подключения SVC может оказаться дешевле, чем PVC. По мере увеличения загрузки виртуальных каналов экономическая эффективность коммутируемых виртуальных каналов снижается..

Несмотря на то, что для постоянных виртуальных каналов фактический маршрут передачи сигнала может меняться со временем (за исключением доступа к сети), как в случае с каналами SPVC, в которых при разрыве соединения или при возникновении значительной перегрузки происходит автоматическое изменение маршрута, при этом начальная и конечная точки такого виртуального канала остаются неизменными. Благодаря прочной связности конечных компонентов такие каналы называются постоянными. Виртуальные каналы получили свое название из-за выполнения в них статистического мультиплексирования с разделением времени (STDM), а также в силу того, что они фактически не предоставляются пользователю на постоянное время (в качестве примера можно привести такие TDM-каналы, как T1). Устройство коммутируемых виртуальных каналов позволяет по желанию изменять один из концов канала, что расширяет возможности абонента. Хотя работа коммутируемого виртуального канала более понятна конечному пользователю, устанавливать его в сети несколько сложнее, чем постоянный канал. Поэтому коммутируемые каналы приобрели популярность лишь в последнее время благодаря появлению приложений, управляющих их работой. Каждый поставщик услуг помимо настройки протокола обмена служебными сигналами (например, Q.933) должен установить соглашения относительно методов передачи сигналов для установления, поддержки и разрыва сквозного соединения в коммутируемом канале связи. Еще одно тонкое отличие коммутируемых виртуальных каналов от постоянных состоит в том, что для первых необходимо отслеживать интенсивность их использования и предъявлять абонентам счета в соответствии с этими показаниями. Для постоянных виртуальных каналов все необходимые моменты оговорены в исходном контракте, который остается неизменным в течение оговоренного срока его действия; напротив, контракт, заключенный по поводу условий предоставления коммутируемых виртуальных каналов, можно изменять. В следующем разделе мы рассмотрим подробно работу приложений для каналов SVC.

Нежесткие каналы PVC, как и обычные, характеризуются фиксированными соединениями в конечных точках, однако конфигурация внутрисетевых соединений для таких каналов может меняться (при каком-либо повреждении). В отличие от коммутируемых виртуальных каналов, нежесткие каналы PVC нельзя разрывать по требованию, поступившему от той или другой конечной точки соединения. Считается, что ни соединения PVC, ни SVC не являются такими устойчивыми при сбоях работы сети, как к.ыалы SPVC. По сути, каналы SPVC во всех отношениях сходны с каналами PVC, за исключением того, что для обеспечения межсетевого взаимодействия в канале SPVC нужно определить технические характеристики закрытого интерфейса между двумя коммутаторами Frame Relay (Private NNI — PNNI), а канал PVC можно обеспечить вручную, без применения протокола обмена служебными сигналами. Обеспечение совместимости оборудования, выпущенного различными производителями, было одним из препятствий на пути к реализации соединений SPVC.

Технология DSL

Телефонная система налагает ограничения на полосу пропускания локального ответвления. Отделение локального ответвления от телефонной системы позволяет обеспечить значительно большую полосу пропускания без прокладки нового кабеля. На рис. 7 показано DSL-соединение.

Рис. 7. DSL-соединение

Технология цифрового абонентского канала (Digital Subscriber Line - DSL) позволяет отделить локальное ответвление от коммутатора телефонной станции или аппаратуры локального оператора связи (local exchange). Вместо этого соединение DSL подсоединяет локальное ответвление данного абонента, вместе с локальными ответвлениями других абонентов данной зоны к мультиплексору доступа абонентского цифрового канала (Digital Subscriber Line Access Multiplexor - DSLAM), также расположенному на телефонной станции. Для поддержки обычной телефонной службы мультиплексор DSLAM подсоединяется к коммутатору телефонной станции. Он также обычно подсоединяется, обычно посредством соединения ATM, к Internet-службе провайдера DSL.

Канал DSL поддерживает постоянное соединение. Как только пользователь включает компьютер, подсоединенный к модему DSL, сразу же осуществляется DSL-соединение. При таком подходе не тратится время на набор номера и на установку соединения. Двумя основными типами технологий DSL являются асимметричная (asymmetric - ADSL) и симметричная (symmetric - SDSL). Все формы службы DSL попадают в одну из этих двух категорий; в каждой из них имеется несколько разновидностей. Для обобщенного обозначения всех различных форм службы DSL иногда используется аббревиатура xDSL. Асимметричная служба предоставляет большую полосу пропускания или загрузки в нисходящем направлении (к пользователю), чем в восходящем. Симметричная служба предоставляет одинаковую скорость в обоих направлениях.

Различные разновидности службы DSL предоставляют различную полосу пропускания; при этом у большинства из них полоса пропускания больше, чем у выделенных линий T1 и E1. Достигаемая при этом скорость передачи в значительной степени зависит от реальной длины локального ответвления, а также от типа и состояния кабеля. Для удовлетворительного качества службы длина локального ответвления не должна превышать 5,5 км (3,5 мили). Доступность DSL пока далека от универсальной и, вследствие обилия различных типов, уже существующих и разрабатываемых стандартов, служба DSL пока мало распространена в качестве средства связи компьютерных отделов предприятий с домашними работниками. Кроме того, абонент не может непосредственно подсоединиться к сети предприятия; для этого он должен сначала подсоединиться к Internet-провайдеру, а затем создать IP-соединение через сеть Internet с предприятием. Такой способ связи связан с определенным и угрозами безопасности информации.

Кабельные модемы

В городской среде для распространения телевизионных сигналов широко используется коаксиальный кабель. Сеть кабельного телевидения также может быть использована для доступа к сети, предоставляя значительно бо́льшую полосу пропускания, чем обычное локальное ответвление телефонной службы. На рис. 8 показаны кабельные модемные соединения.

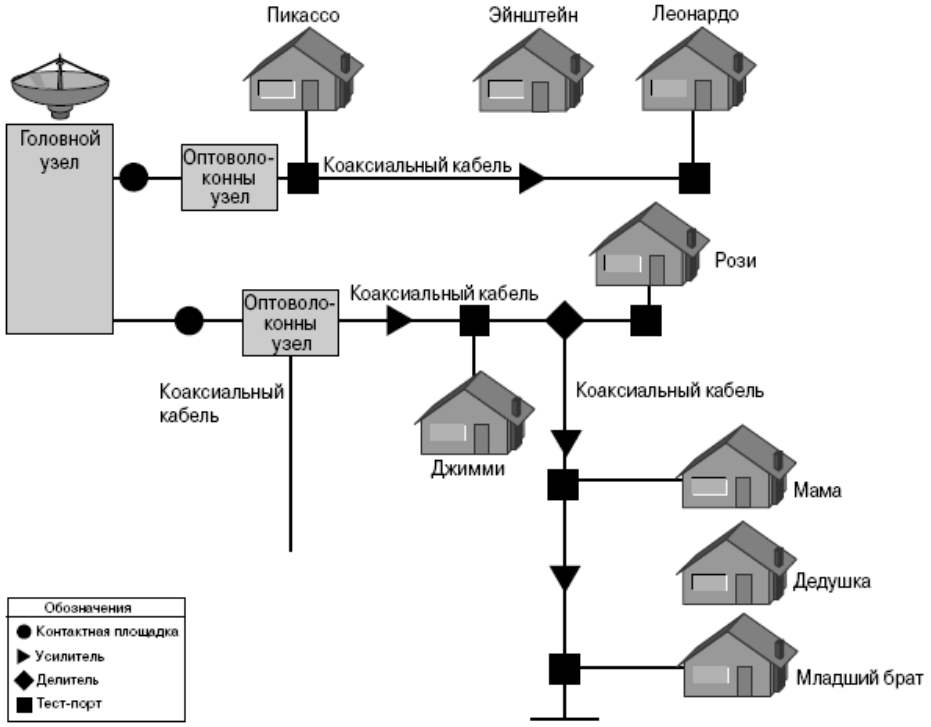


Рис. 8. Использование кабельных модемов

Кабельные модемы позволяют осуществлять двустороннюю передачу данных в обоих направлениях, используя те же коаксиальные линии, по которым передается кабельное телевидение. Некоторые провайдеры кабельных служб обещают скорости передачи в 6,5 раз превосходящие скорости выделенных линий T1. Такая скорость делает кабель привлекательной средой для быстрой передачи больших объемов цифровой информации, включая видеоклипы, аудиофайлы и большие объемы обычных цифровых данных. Объем информации, передача которой потребовала бы 2 минут для загрузки с использованием BRI ISDN, при использовании со-

единения кабельного модема может быть загружен за 2 секунды. Таким образом, кабельные модемы обеспечивают скорости, бо́льшие, чем у выделенных линий, с меньшими затратами и более простой установкой. Кабельные модемы обеспечивают круглосуточное соединение. Сразу после включения питания компьютера пользователь оказывается подключенным к сети Internet. Такая установка позволяет экономить время и усилия на набор номера для установки соединения. Однако постоянная включенность («always-on») кабельного соединения означает, что подсоединенный компьютер оказывается постоянно уязвимым в отношении атак хакеров и должен быть надежно защищен с помощью брандмауэра.

Кабельный модем способен обеспечить доставку данных со скоростью 30-40 Мбит/с по одному кабельному каналу 6 МГц. Это в 500 раз быстрее, чем модем 56 Кбит/с.

При использовании кабельного модема абонент может продолжать прием кабельного телевидения одновременно с получением данных на персональном компьютере. Это осуществляется с помощью простого делителя «один-к-двум», как показано на рис. 9.

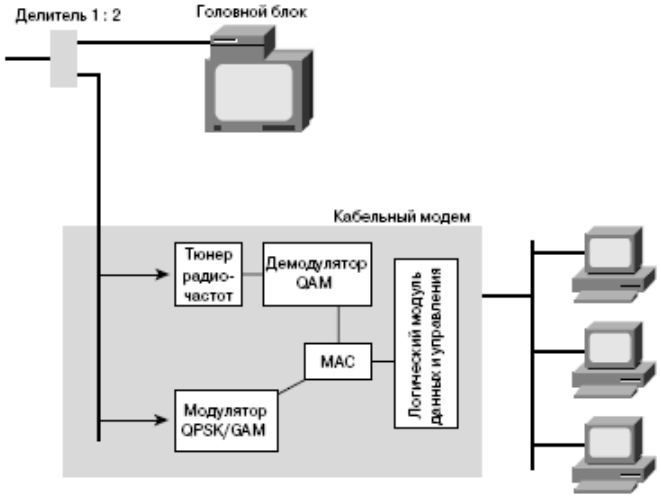


Рис. 9. Кабельный модем: двусторонний делитель

Как и в случае использования DSL, у абонента нет другого выбора, кроме как воспользоваться услугами Internet-провайдера (Internet service provider - ISP), предоставляющего службу кабельного модема и подсоединяться к сети своего предприятия с помощью приложения TCP/IP, такого как Telnet. Другим недостатком является то, что все локальные абоненты совместно используют полосу пропускания кабеля, так же, как это происходит в случае коаксиальных соединений Ethernet.

По мере того, как к службе подключается все большее количество пользователей, реальная полоса пропускания может оказаться значительно меньшей, чем ожидаемая. Еще более серьезной проблемой является обеспечение необходимого уровня безопасности.

Домашний компьютер пользователя оказывается уязвимым не только для всех пользователей сети Internet, но и для пользователей, подключенных к его собственному кабелю. Поэтому необходим определенный уровень защиты с помощью какого-либо типа брандмауэра.

Для решения проблем безопасности провайдеры модемных кабельных служб предоставляют возможность использования соединений виртуальных частных сетей (Virtual Private Network - VPN) для соединения с сервером VPN, который обычно расположен на корпоративном узле предприятия.

Виртуальная частная сеть

Виртуальная частная сеть (Virtual Private Network, VPN) – обобщённое название технологий, позволяющих обеспечить одно или несколько изолированных сетевых соединений (создать «виртуальную» сеть), используя в качестве транспорта любую реальную IP-сеть, в т.ч. Интернет. Благодаря применению средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от изменений передаваемых сообщений) эти техно-

логии позволяют организовать безопасный обмен данными с удаленной ЛВС через открытую сеть общего пользования. Под этой аббревиатурой скрывается группа технологий и протоколов позволяющих организовать логическую (виртуальную) сеть поверх обычной сети. Широко применяется для разграничения доступа и повышения безопасности корпоративных сетей, организации безопасного доступа к ресурсам корпоративной сети извне (через интернет) и, в последнее время, провайдерами городских сетей для организации доступа в интернет.

Схема организации VPN канала показана на рис. 10. Передача данных через Интернет выполняется путем создания потока шифрованного трафика - *VPN-туннеля* между VPN-клиентом и VPN-сервером, имеющими «реальные» (public) IP-адреса. При этом конечный пользователь и сервер могут использовать IP-адреса локального диапазона и «не знать» о наличии VPN-соединения. В качестве VPN-клиента и VPN-сервера могут использоваться как прикладное программное обеспечение, так и специальные устройства (шлюзы, маршрутизаторы), выполняющие шифрование трафика ЛВС при передаче в туннель и расшифровку данных при выходе из VPN-туннеля. В общем трафике Интернет, данные VPN-туннелей представляют собой поток пакетов специального формата с зашифрованным содержанием.

Рис. 10 Схема организации канала VPN

В зависимости от применяемого протокола VPN подразделяются на:

PPTP (Point-to-point tunneling protocol) -- туннельный протокол типа точка-точка, позволяет организовать защищенное соединение за счет создания специального туннеля поверх обычной сети. Основан на протоколе PPP1 и использует аналогичные механизмы проверки подлинности, выполнения сжатия и шифрования. Протокол PPTP интегрирован в пакет клиентского программного обеспечения Windows XP/7, как одно из стандартных средств удаленного доступа. Для организации соединения используется две сетевых сессии: для передачи данных устанавливается PPP сессия с добавления *туннельного заголовка* GRE2 и заголовка IP к данным, обработанным протоколом PPP и соединение на TCP порту 1723 для инициализации и управления соединением. Стандартно используется метод шифрования MPPE (Microsoft Point-to-Point Encryption).

При необходимости, данные могут передаваться без шифрования.

На рис. 11 показана структура PPTP-пакета, включающая следующие поля:

- *IP-дейтаграмма* – исходный пакет локальной сети, содержащий пользовательские данные и IP-заголовок локальной адресации;
- *PPP-заголовок* и - *GRE-заголовок* - данные, необходимые для создания и поддержания VPN-туннеля;

- *IP-заголовок* – реальный IP-адрес назначения и другие данные для передачи пакета через Интернет между входами туннеля.

Рис. 11. Структура PPTP-пакета

IPSec (IP Security Protocol) - это современный набор протоколов обеспечивающих создание VPN-соединения, аутентификацию, доступ и контроль. IPSec функционирует на сетевом уровне эталонной модели взаимодействия, позволяет создавать кодированные туннели VPN или кодировать трафик между двумя узлами. В состав службы IPSec входят протоколы: AH (Autentication Header) – аутентификация источника и проверка целостности сообщений, ESP (Encapsulating Security Payload) – шифрование сообщений, SA (Security Association) - обеспечение работы AH/ESP и управление ключами. Для шифрования данных в системе IPsec может быть применен любой симметричный алгоритм шифрования.

L2TP (Layer 2 Tunneling Protocol) -- протокол туннелирования второго уровня, более совершенный протокол, созданный на базе PPTP и L2F (протокол эстафетной передачи второго уровня). К его достоинствам относится гораздо более высокая безопасность за счет шифрования средствами протокола IPSec и объединения канала данных и канала управления в одну UDP сессию. L2TP интегрирован в клиента удаленного доступа Windows XP/7 и является протоколом по умолчанию при создании VPN-соединений. Аналогично PPTP, при формировании пакета, инкапсуляция данных происходит путем добавления заголовков L2TP и IPSec к данным обработанным протоколом PPP. Для шифрования данных используются алгоритмы DES (Data Encryption Standard) или 3DES.

SSTP (Secure Socket Tunneling Protocol) -- протокол безопасного туннелирования сокетов, основан на SSL и позволяет создавать защищенные VPN соединения посредством HTTPS. Требует для своей работы открытого порта 443, что позволяет устанавливать соединения из любого места, даже находясь за цепочкой прокси.

При организации VPN-соединения на основе вышеперечисленных протоколов, выполняются следующие операции:

1. Туннелирование (Tunneling) – прикрепление дополнительного заголовка и инкапсуляция исходных пакетов с локальной адресацией в IP-пакет, пригодный для передачи через чужую сеть в соответствии с ее правилами.

2. Проверка подлинности – механизм персонификации клиента при создании VPN-туннеля, использующий технологии PPP, IKE3, цифровые сертификаты.

3. Шифрование данных внутри созданного туннеля.

VPN-инфраструктура может строиться по схеме точка «точка-точка», для соединения двух сегментов ЛВС, или по топологии «звезда» для соединения произвольного количества узлов. В последнем случае VPN-узел называется VPN-шлюзом, а созданная им сеть - доменом шифрова-

ния. При наличии в ЛВС шлюза VPN, пользователи устанавливает соединение с ним, после чего получают доступ к ресурсам удаленного сегмента сети, как при локальном подключении.

По способу организации можно выделить следующие виды VPN-сетей:

- *Customer provided VPN* - организация VPN-соединений возлагается на потребителя. Данный тип VPN относится к сетевому уровню взаимодействия и получил широкое распространение благодаря тому, что может создаваться пользователями самостоятельно с использованием специализированного программного обеспечения. Преимуществом, является возможность для владельца распределенной компьютерной сети полностью контролировать работу VPN-шлюзов и обеспечить наилучшую конфиденциальность передачи информации.

- *Provider Provisioned VPN* - организация VPN силами провайдера телекоммуникационных услуг на основе существующих телефонных, телевизионных, мобильных и других сетей. Такие VPN строятся на сетевом и канальном (Layer 2) уровнях взаимодействия с использованием технологий MPLS4 и VLAN. Сети VPN, построенные с использованием услуг оператора имеет более высокую скорость работы и не требует специальных навыков пользователя, однако размер такой VPN ограничен сетью одного оператора и предполагает полный контроль над VPN-шлюзом и защищаемым трафиком со стороны персонала провайдера.

По назначению VPN решения можно классифицировать на следующие виды:

- *Intranet VPN*. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

- *Remote Access VPN*. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука.

- *Extranet VPN*. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

Рассмотрим несколько наиболее часто используемые применения VPN:

Доступ в интернет. Чаще всего применяется провайдерами городских сетей, но также весьма распространенный способ и в сетях предприятий. Основным достоинством является более высокий уровень безопасности, так как доступ в локальную сеть и интернет осуществляется через две разные сети, что позволяет задать для них разные уровни безопасности. При классическом решении - раздача интернета в корпоративную сеть - выдержать разные уровни безопасности для локального и интернет трафика практически не представляется возможным.

Доступ в корпоративную сеть извне, также возможно объединение сетей филиалов в единую сеть. Это собственно то, для чего и задумывали VPN, позволяет организовать безопасную работу в единой корпоративной сети для клиентов находящихся вне предприятия. Широко используется для объединения территориально разнесенных подразделений, обеспечения доступа в сеть для сотрудников находящихся в командировке или на отдыхе, дает возможность работать из дома.

Объединение сегментов корпоративной сети. Зачастую сеть предприятия состоит из нескольких сегментов с различным уровнем безопасности и доверия. В этом случае для взаимодействия между сегментами можно использовать VPN, это гораздо более безопасное решение, нежели простое объединение сетей. Например, таким образом можно организовать доступ сети складов к отдельным ресурсам сети отдела продаж. Так как это отдельная логическая сеть, для нее можно задать все необходимые требования безопасности не влияя на работу отдельных сетей.

Преимущества использования VPN-сетей при создании распределенных ЛВС:

1. *Масштабируемость* – подключение новых точек к сети может быть выполнено оперативно и не требует существенных затрат на строительство коммуникаций.

2. *Гибкость* – возможность подключения пользователя или сегмента ЛВС к VPN-сети существует в любой точке Интернет и не ограничено непосредственным местоположением удаленного пользователя.

3. *Защищенность* – все компьютеры VPN-инфраструктуры обмениваются данными изолированно, могут использовать IP-адресацию локального диапазона и использовать корпоративные средства обеспечения безопасности.

4. *Интеграция с IP-сервисами* – как правило, шлюзы доступа к VPN-сети представляют собой многофункциональные устройства, позволяющие выполнять маршрутизацию, фильтрацию, межсетевое экранирование и приоритетную обработку мультисервисного трафика.

Контрольные вопросы

1. Какие существуют технологии глобальных сетей?
2. Какие технологии относятся в концепции выделенного канала?
3. Какие технологии относятся к кабельной структуре канала?
4. Что подразумеыет под собой концепция вируальных сетей?
5. На каком принципе основана работа VPN?

Лекция 19
Основы маршрутизации и принципы построения подсетей

1. **Маршрутизируемые и маршрутизирующиеся протоколы**
2. **IP как маршрутизируемый протокол**
3. **Структура IP-пакета**
4. **Поиск оптимального маршрута**

Ключивые слова: протокол IP, маршрутизируемый протокол, протокол маршрутизации, дейтаграмма, IP-пакет, маршрут, стандартный маршрут, алгоритм, транзитный узел.

Протокол IP (Internet-протокол) является маршрутизируемым протоколом сети Internet. Пакеты маршрутизируются по оптимальному пути от отправителя к получателю на основе уникальных идентификаторов – IP-адресов. Данные могут быть правильно доставлены получателю в том случае, если в сети требуемым образом работают механизмы пересылки пакетов, устройства, преобразующие данные из одного формата в другой, а также протоколы с установлением и без установления соединения.

1. Маршрутизируемые и маршрутизирующиеся протоколы

Протоколом называется основанный на стандартах набор правил, определяющий принципы взаимодействия компьютеров в сети. Протокол также задает общие правила взаимодействия разнообразных приложений, сетевых узлов или систем, создавая таким образом единую среду передачи. Взаимодействующие друг с другом компьютеры обмениваются данными; чтобы принять и обработать сообщения с данными, компьютерам необходимо знать, как сформированы сообщения и что они означают.

Примерами использования различных форматов сообщений в разных протоколах могут служить установление соединения с удаленной машиной, отправка сообщений по электронной почте или передача файлов и данных; интуитивно понятно, что разные службы используют разные сообщения.

Протокол описывает:

- формат сообщения, которому приложения обязаны следовать;
- способ обмена сообщениями между компьютерами в контексте определенного действия, такого, как отправка сообщений по сети.

Схожее звучание терминов «маршрутизируемый протокол» и «протокол маршрутизации» нередко приводит к путанице. Приведенные ниже определения помогут прояснить ситуацию.

Маршрутизируемый протокол - это любой сетевой протокол, адрес сетевого уровня которого предоставляет достаточное количество информации для доставки пакета от одного сетевого узла другому на основе используемой схемы адресации. Такой протокол задает форматы полей внутри *пакета*. Пакеты обычно передаются от одной конечной системы другой. Маршрутизируемый протокол использует таблицу маршрутизации для пересылки пакетов. Примеры маршрутизируемых протоколов приведены на рис. 1. В их число входят:

- Internet-протокол (IP);

- протокол межсетевого пакетного обмена (Internetwork Packet Exchange - IPX);
- протокол AppleTalk.

Легче всего запомнить, что такое маршрутизируемые протоколы, если помнить, что это протоколы, которые связаны с передачей данных.

Протокол маршрутизации - это протокол, который поддерживает маршрутизируемые протоколы и предоставляет механизмы обмена маршрутной информацией. Сообщения протокола маршрутизации передаются между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией друг с другом для обновления записей и поддержки таблиц маршрутизации. Ниже приводятся некоторые примеры протоколов маршрутизации TCP/IP:

- протокол маршрутной информации (Routing Information Protocol - RIP);
- протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol - IGRP);
- усовершенствованный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol - EIGRP);
- протокол первоочередного обнаружения кратчайших маршрутов (Open Shortest Path First - OSPF).

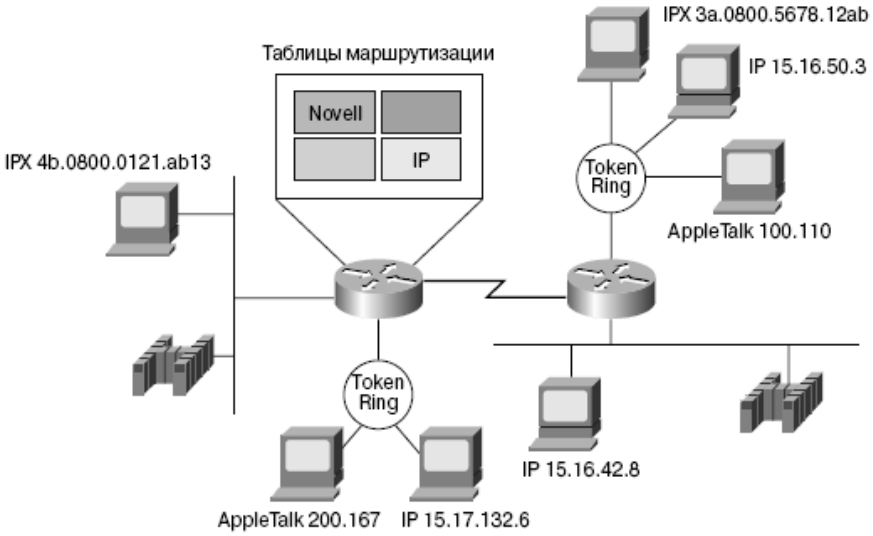


Рис. 1. Маршрутизируемые протоколы

Чтобы протокол был маршрутизируемым, в нем должны наличествовать механизмы назначения как номера сети, так и номера узла для каждого отдельного сетевого устройства. В некоторых протоколах, таких, как, например, IPX, необходимо назначить только адрес сети, поскольку в качестве адреса устройства эта технология использует физический адрес (MAC-адрес) устройства. Другие протоколы, такие, как IP, требуют, чтобы явно был задан весь адрес и сетевая маска.

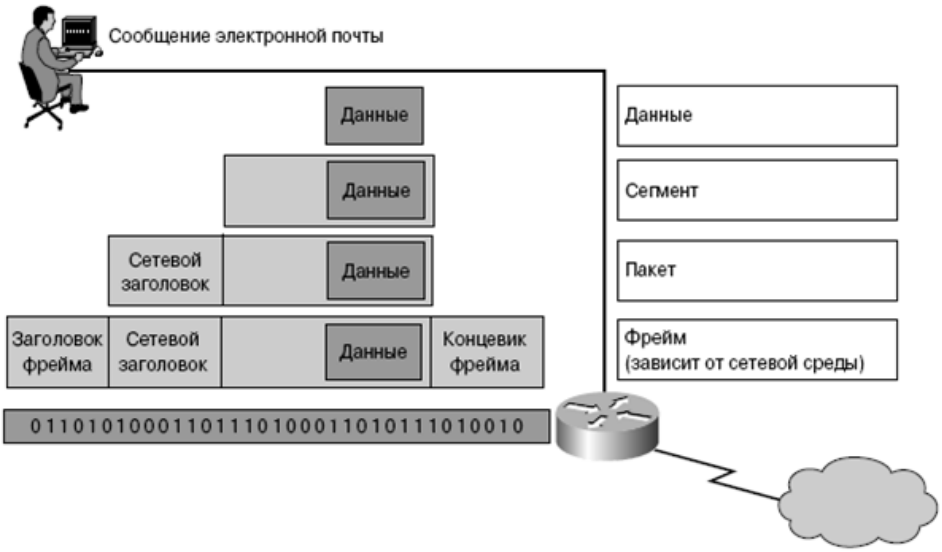
Для создания маршрутизируемой сети необходимы как *IP-адрес*, так и *маска сети*. Сетевая маска делит 32-битовый IP-адрес на сетевую часть и адрес узла. Протокол IPX использует MAC-адрес, объединенный с установленным администратором номером сети, для создания полного адреса и не требует использования сетевой маски. При использовании IP-технологий адрес сети вычисляется путем сравнения полного адреса и маски подсети.

Сетевая маска позволяет рассматривать группу последовательных IP-адресов как единое целое. Без такой возможности группировки адресов потребовался бы механизм маршрутизации для каждого отдельного узла. Такая схема была бы непригодна для миллионов узлов, работающих в сети Internet.

2. IP как маршрутизируемый протокол

Протокол IP является наиболее широко распространенной реализацией иерархической схемы сетевой адресации. Используемый в сети Internet, протокол IP не отвечает за установку соединений, не является надежным и позволяет реализовать только негарантированную доставку данных. Термин *протокол без установления соединения (connectionless*) означает, что для взаимодействия не требуется выделенный канал, как это происходит во время телефонного звонка, и не существует процедуры вызова перед началом передачи данных между сетевыми узлами. Протокол IP выбирает наиболее эффективный маршрут из числа доступных на основе решения, принятого протоколом маршрутизации. Отсутствие надежности и негарантированная доставка не означает, что система работает плохо и ненадежно, а указывает лишь на то, что протокол IP не предпринимает никаких усилий, чтобы проверить, был ли доставлен пакет по назначению. Эти функции делегированы протоколам верхних уровней.

Информация, проходя сверху вниз по уровням OSI-модели, на каждом из уровней надлежащим образом обрабатывается. На рис. 2 показано, что на сетевом уровне данные инкапсулируются внутрь *пакетов*, зачастую называемых *дейтаграммами*.



Протокол IP распознает формат заголовка пакета (включая адресную часть и другую служебную информацию), но никоим образом не заботится о фактических данных. Он принимает любые данные, переданные протоколами верхнего уровня (рис.3).

Рис. 2. Инкапсуляция

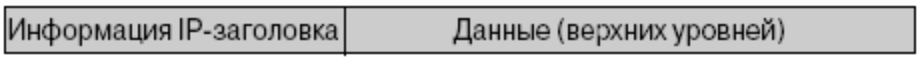


Рис. 3. IP-заголовок

Пересылка пакетов и коммутация внутри маршрутизатора

На рис. 4 показано, что заголовок и концевик фрейма отбрасываются и заменяются новыми каждый раз при прохождении движущимся по сети пакетом маршрутизирующего устройства третьего уровня. Причина этого состоит в том, что блоки информации второго уровня (фреймы)

используются для локальной доставки информации, в то время как блоки третьего уровня (пакеты) предназначены для сквозной передачи данных согласно схеме адресации.

Ethernet-фреймы второго уровня предназначены для работы внутри широковещательных доменов с назначенными каждому сетевому устройству MAC-адресами.

Фреймы второго уровня других типов, такие, как последовательные двухточечные соединения и Frame Relay распределенных сетей (сетей WAN), используют свою собственную схему адресации второго уровня. Принципиальным является то, что, независимо от используемой схемы адресации второго уровня, все они разработаны для использования внутри одного широковещательного домена второго уровня. При прохождении данными через устройство третьего уровня информация второго уровня изменяется.

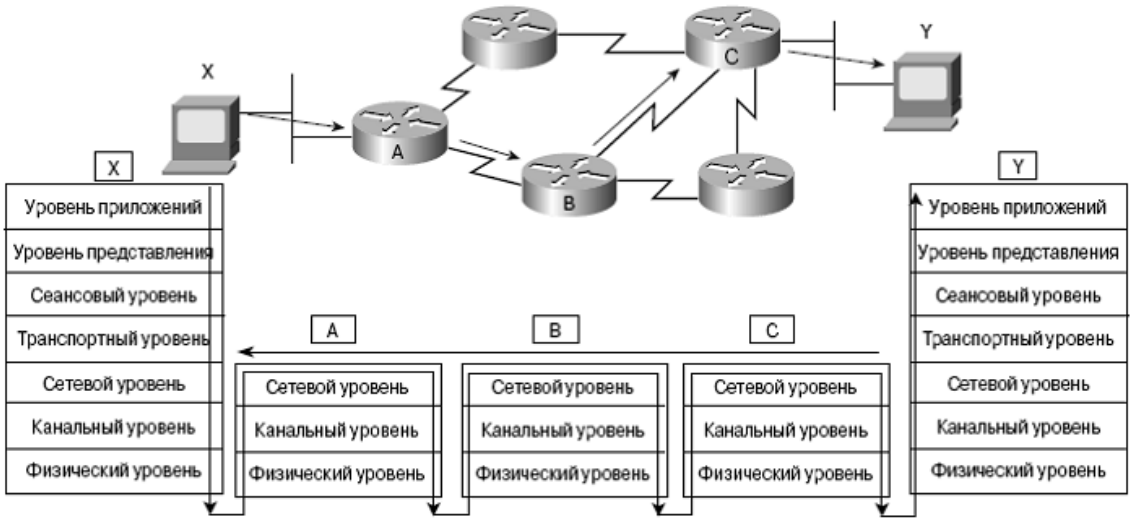


Рис. 4. Поток данных сетевого уровня

Сетевые службы с установлением соединения и без

Большинство сетевых служб модели OSI используют системы доставки без установления соединения (протокол UDP). Они работают с каждым пакетом в отдельности и пересылают их в нужном направлении через сеть.

Пакеты могут быть переданы по сетевым маршрутам и будут собраны вместе в сообщение только тогда, когда достигнут своего пункта назначения. В системах без установления соединения перед отправкой пакета контакт с получателем не происходит.

Сетевые службы без установления соединения часто называют процессами с *коммутацией пакетов*. В таких процессах пакеты могут проходить разными маршрутами от отправителя к получателю, а также (что вполне вероятно) прибывать в пункт назначения в другом порядке. Устройства выбирают маршрут для каждого пакета на основе различных критериев. Некоторые критерии (как, например, доступная полоса пропускания) могут быть разными для различных пакетов.

Сеть Internet - огромная объединенная сеть без установления соединения, в которой за доставку всех пакетов отвечает протокол IP. Протокол TCP (четвертый уровень модели) использует службы с установлением соединений поверх протокола IP (третьего уровня). Сегменты TCP инкапсулируются в IP-пакеты для передачи через сеть Internet.

Протокол IP является системой без установления соединений: каждый пакет в ней обрабатывается отдельно.

Каждый пакет может пойти своим маршрутом. Некоторые из них даже могут быть утеряны. Протокол IP полагается на протоколы транспортного уровня, чтобы определить, был ли доставлен пакет, и при необходимости организовать повторную передачу. Транспортный уровень также отвечает за сборку пакетов в сообщение в надлежащей последовательности.

В системах с *установлением соединения*, как следует из названия, соединение между отправителем и получателем устанавливается до начала передачи данных. В сетях с установлением соединения вначале организуется соединение с получателем и только после этого начинается фактическая передача данных. Все пакеты передаются последовательно, с использованием одного и того же физического канала или, в самом общем случае, одного виртуального канала.

3. Структура IP-пакета

Ранее было рассмотрено, как пакеты или дейтаграммы третьего уровня становятся данными второго уровня и инкапсулируются во фреймы.

Аналогично, как показано на рис. 5, IP-пакеты состоят из данных верхнего уровня и IP-заголовка.

- **Версия (Version)** - четырехбитовое поле, описывающее используемую версию протокола IP. Все устройства обязаны использовать протокол IP одной версии; устройство, использующее другую версию, будет отбрасывать пакеты.

Рис. 5. Структура IP-пакета

- **Длина IP-заголовка (IP Header Length - HLEN)** - четырехбитовое поле, описывающее длину заголовка дейтаграммы в 32-битовых блоках. Данное значение - это полная длина заголовка с учетом двух полей переменной длины.
- **Тип обслуживания (Type of Service - TOS)** - восьмибитовое поле, указывающее на степень важности информации, которая присвоена определенным протоколом верхнего уровня.
- **Полная длина (Total Length)** - шестнадцатибитовое поле, описывающее полную длину пакета в байтах, включая данные и заголовок. Чтобы вычислить длину блока данных, нужно из полной длины вычесть значение поля HLEN.
- **Идентификация (Identification)** - шестнадцатибитовое поле, хранящее целое число, описывающее данную дейтаграмму. Это число представляет собой последовательный номер.
- **Флаги (Flags)** - трехбитовое поле, в котором два младших бита контролируют фрагментацию пакетов. Первый бит определяет, был ли пакет фрагментирован, а второй - является ли этот пакет последним фрагментом в серии фрагментированных пакетов.

- **Смещение фрагментации (Fragment Offset)** - тринадцатибитовое поле, помогающее собрать вместе фрагменты дейтаграммы. Это поле позволяет использовать 16 битов для поля флагов.
- **Время жизни (Time to Live - TTL)** - восьмибитовое поле, в котором хранится последовательно уменьшающееся значение счетчика, вплоть до нуля. В последнем случае (счетчик равен нулю) дейтаграмма будет отброшена – таким образом предотвращается бесконечная циклическая пересылка пакета.
- **Протокол (Protocol)** - восьмибитовое поле, указывающее, какой протокол верхнего уровня получит пакет, после того как обработка протоколом IP будет закончена. Примерами значений в этом поле являются протоколы TCP и UDP.
- **Контрольная** - сумма заголовка (Header Checksum) - шестнадцатибитовое поле, которое помогает проверить целостность заголовка пакета.
- **IP-адрес отправителя (Source IP address)** – 32-битовое поле, содержащее IP-адрес узла-отправителя.
- **IP-адрес получателя (Destination IP address)** – 32-битовое поле, содержащее IP-адрес узла-получателя.
- **Опции (Options)** - поле переменной длинны, позволяющее протоколу IP реализовать поддержку различных опций, например, средств безопасности.
- **Дополнение (Padding)** - поле, используемое для вставки дополнительных нулей, чтобы гарантировать кратность IP-заголовка 32 битам.
- **Данные (Data)** - поле переменной длины (максимум 64 Кбит), содержащее информацию верхних уровней.

4. Сравнение маршрутизируемых протоколов и протоколов маршрутизации

Протоколы сетевого уровня делятся на две категории: маршрутизируемые и протоколы маршрутизации. Маршрутизируемые протоколы организуют передачу данных через сеть, а протоколы маршрутизации реализуют механизмы, с помощью которых маршрутизаторы определяют необходимое направление для доставки данных из одного пункта в другой.

Протоколы, способные передавать данные от одного узла другому, находящемуся за маршрутизатором, называются маршрутизируемыми, или просто протоколами передачи данных.

Принцип работы маршрутизируемого протокола проиллюстрирован на рис. 6.

- Маршрутизируемым является любой протокол или набор сетевых протоколов, которые предоставляют маршрутизаторам необходимую информацию в адресе сетевого уровня для передачи данных следующему узлу и конечному получателю.
- Маршрутизируемый протокол задает формат пакета и использование в нем отдельных полей. В большинстве своем пакеты передаются от одной конечной системы другой.

Примерами маршрутизируемых протоколов являются IP и IPX.

Маршрутизаторы используют протоколы маршрутизации для обмена таблицами маршрутизации и совместного использования информации о доступных маршрутах. Иными словами, *протоколы маршрутизации* дают возможность маршрутизаторам выбирать маршрут для *марш-*

рутизируемых протоколов, после того как будут обнаружены все возможные пути к получателю.

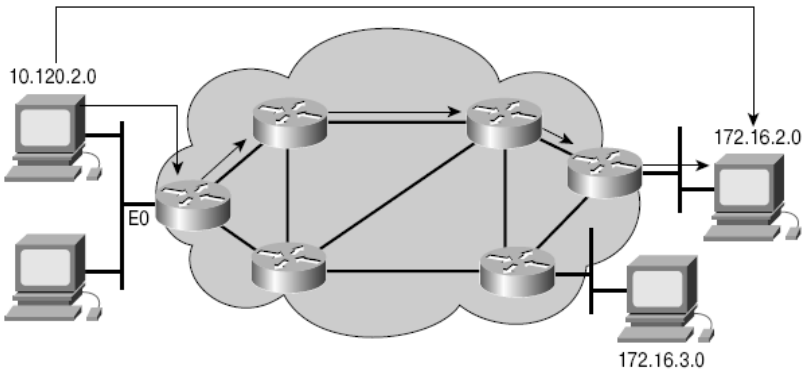
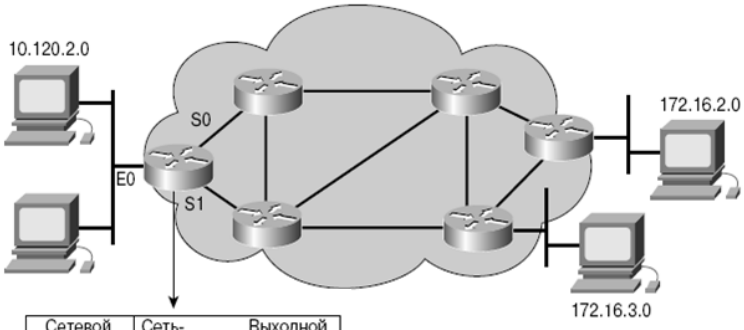


Рис. 6. Маршрутизируемый протокол



Сетевой протокол	Сеть-получатель	Выходной интерфейс
Подключена напрямую RIP IGRP	10.120.2.0	E0
	172.16.2.0	S0
	172.16.3.0	S1

Рис. 7. Протокол маршрутизации

Принцип работы протокола маршрутизации проиллюстрирован на рис. 7.

- Протокол маршрутизации обеспечивает работу процесса совместного использования информации о доступных маршрутах.
- Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией друг с другом для поддержки таблиц маршрутизации.

Примерами протоколов маршрутизации, которые поддерживают маршрутизируемый протокол IP, являются RIP, IGRP, OSPF, протокол граничного шлюза (Border Gateway Protocol - BGP) и EIGRP.

Поиск оптимального маршрута

Процесс нахождения оптимального пути, по которому следует передать пакет, выполняется на третьем уровне эталонной модели OSI (сетевом). Эта процедура позволяет маршрутизатору оценить существующие маршруты к получателю и выбрать среди них наиболее предпочтительный. Как показано на рис. 10.18, службы маршрутизации используют информацию о топологии сети в процессе анализа сетевых маршрутов. Определением пути называют процесс, используемый маршрутизатором для выбора следующего узла на пути следования пакета к своему конечному пункту назначения. Этот процесс также называется *маршрутизацией* пакета.

Маршрутизаторы могут принимать решения, основываясь на информации об интенсивности трафика и пропускной способности соединения. Маршрутизаторы принимают решение о выборе оптимального пути на основании загрузки, полосы пропускания, задержки, стоимости и надежности какого-либо канала. Процесс выбора маршрута для каждого пакета включает в себя следующие компоненты:

- адрес получателя берется непосредственно из заголовка пакета;
- сетевая маска первой записи в таблице маршрутизации применяется к адресу получателя в пакете;
- после того как маска умножается на адрес получателя (логическая операция «И»), полученная величина сравнивается с записью в таблице маршрутизации;

- если оба значения совпали, пакет пересылается на интерфейс (порт) маршрутизатора, с которым связана данная запись в таблице маршрутизации;
- если же совпадений значений нет, описанным выше образом проверяется следующая запись в таблице маршрутизации;
- если адрес пакета не соответствует ни одной из записей в таблице маршрутизации, маршрутизатор проверяет, есть ли у него стандартный маршрут;
- если в маршрутизаторе сконфигурирован стандартный маршрут, пакет передается на соответствующий ему порт маршрутизатора. *Стандартный маршрут* (default route) - это маршрут, который конфигурирует в устройстве системный администратор и который будет использоваться устройством в том случае, если не найдены соответствия ни одной записи в таблице маршрутизации;
- если же стандартного маршрута нет, то пакет будет отброшен маршрутизатором. Зачастую в обратном направлении устройство отправляет сообщение, которое сигнализирует о том, что сеть получателя недоступна.

Таблицы маршрутизации

Чтобы найти маршрут, по которому следует передавать данные, протоколы маршрутизации создают и поддерживают таблицы маршрутизации. Информация о маршруте может отличаться в зависимости от используемого протокола маршрутизации. Таблица маршрутизации заполняется соответствующим протоколом различной информацией.

Маршрутизаторы хранят и обновляют следующую важную информацию в таблицах маршрутизации:

- **тип протокола** - информацию о протоколе маршрутизации, создавшем запись в таблице маршрутизации;
- **связка получатель/следующий узел** сообщает маршрутизатору о том, что определенный получатель либо подключен непосредственно, либо может быть достигнут через другой маршрутизатор, называемый *следующим транзитным узлом (next hop)*, находящийся на пути к пункту назначения. Маршрутизатор анализирует адрес получателя во входящих пакетах и сравнивает его на соответствие с записями в таблице маршрутизации;
- **метрики маршрутизации**. Различные протоколы маршрутизации используют разные метрики, которые помогают определить предпочтительность маршрута. Например, протокол RIP использует *счетчик транзитных узлов (hop count)* в качестве метрики маршрутизации. Протокол IGRP использует пропускную способность, загрузку канала, суммарную задержку передачи и надежность для формирования комплексного значения метрики.
- **выходной интерфейс** - интерфейс, через который должны быть отправлены данные, чтобы достичь пункта назначения.

Маршрутизаторы взаимодействуют друг с другом посредством передачи сообщений-анонсов для поддержки таблиц маршрутизации. В зависимости от протокола маршрутизации такие обновления маршрутных таблиц могут отправляться либо периодически, либо при изменении топологии сети. Протокол также определяет, нужно ли в анонсе отправить полную таблицу маршрутизации или только информацию об изменившемся маршруте. Используя анонсы, получаемые от соседей, маршрутизатор создает и поддерживает свою таблицу маршрутизации в актуальном состоянии.

Алгоритмы маршрутизации и метрики

Протоколы маршрутизации выбираются, исходя из характеристик, перечисленных ниже.

- **Оптимальность** описывает способности протокола и алгоритма по выбору наиболее оптимального маршрута на основании метрик и их весовых значений, используемых при расчетах. Например, некий протокол может использовать счетчик узлов и задержки для определения метрик; задержки имеют более высокий вес при учете окончательного значения, но зато их сложнее рассчитать.
- **Простота и низкие накладные расходы.** Идеальная эффективность работы алгоритма маршрутизации может быть достигнута, когда загрузка процессора и памяти маршрутизатора минимальны. Эта характеристика важна для масштабируемости сети, которая в предельном случае может быть расширена до размеров сети Internet.
- **Устойчивость и надежность.** Алгоритм маршрутизации должен корректно функционировать даже при наличии нестандартных и непредвиденных обстоятельств, таких, как сбой оборудования, высокая загрузка и ошибки эксплуатации.
- **Быстрая конвергенция.** Конвергенцией называется процесс установления договоренности между всеми маршрутизаторами об имеющихся маршрутах. Когда в сети происходят события, оказывающие влияние на доступность маршрутизатора, для установления повторного соединения требуются перерасчеты. Алгоритмы маршрутизации, не обладающие быстрой конвергенцией, могут вызвать сбой или значительную задержку при доставке информации.
- **Гибкость.** Алгоритм и протокол маршрутизации должны быстро адаптироваться к разнообразным изменениям в сети. Изменениями в сети считаются изменения в состоянии устройств, в частности, маршрутизаторов, изменение пропускной способности каналов, изменение размера очередей или сетевой задержки.
- **Масштабируемость.** Некоторые протоколы разработаны таким образом, что могут быть масштабируемы лучше других. Важно помнить, что если планируется расширение сети (или такая возможность в принципе предусматривается), следует отдать предпочтение протоколу EIGRP, нежели RIP.

Первоочередная задача *алгоритма маршрутизации* при обновлении таблицы маршрутизации состоит в определении наилучшей информации, которая должна быть внесена в таблицу. Алгоритмы маршрутизации используют различные метрики для определения наилучшего маршрута, но каждый алгоритм интерпретирует выбор лучшего варианта пути по-своему. Алгоритм маршрутизации рассчитывает число, называемое метрикой, для каждого сетевого маршрута. Сложные алгоритмы маршрутизации могут основывать выбор маршрута на основе нескольких параметров, объединяя их в одну общую метрику. Чем меньше метрика, тем лучше выбранный маршрут.

Метрики могут быть вычислены на основе одной или нескольких характеристик.

Наиболее часто в алгоритмах маршрутизации используются параметры метрики, которые перечислены ниже.

- **Ширина полосы пропускания** представляет собой средство оценки объема информации, который может быть передан по каналу связи (канал Ethernet со скоростью 10 Мбит/с более предпочтителен, чем выделенная линия со скоростью 64 Кбит/с).

- **Задержка** - промежуток времени, необходимый для перемещения пакета по каждому из каналов связи от отправителя получателю. Задержка зависит от пропускной способности промежуточных каналов, размера очередей в портах маршрутизаторов, загрузки сети и физического расстояния.
- **Загрузка** - объем операций, выполняемых сетевым устройством, таким, как маршрутизатор, или средняя загруженность канала связи.
- **Надежность** обычно обозначает относительное значение количества ошибок для каждого из каналов связи.
- **Счетчик транзитных узлов —** количество маршрутизаторов, через которые должен пройти пакет, прежде чем достигнет пункта назначения. Когда пакет проходит через маршрутизатор, значение счетчика узлов увеличивается на единицу. Путь, для которого значение счетчика узлов равно четырем, означает, что данные, отправленные по этому маршруту, пройдут через четыре маршрутизатора, прежде чем будут получены адресатом. Если существует несколько путей, маршрутизатор выбирает тот, для которого значение счетчика узлов наименьшее.
- **Стоимость** — значение, обычно вычисляемое на основе пропускной способности, денежной стоимости или других единиц измерения, назначаемых администратором.

Контрольные вопросы

1. Что такое протокол и каковы его функции?
2. Каково назначение маршрутизируемых протоколов?
3. Какова структура IP-пакета?
4. Какие функции в сети выполняют протоколы маршрутизации?
5. Как осуществяется выбор оптимального маршрута?

Лекция 20
Применение маршрутизации и протоколы маршрутизации

1. **Маршрутизация**
2. **Протоколы внешней маршрутизации**

Ключевые слова: маршрутизация, значение получателя, маска, адрес шлюза, метрика маршрута, прямой маршрут, статический маршрут, динамический маршрут, маршрут по умолчанию, протокол, оптимальный путь, RIP, EIGRP, OSPF, автономная система.

1. Маршрутизация

Маршрутизация – это способ направления сообщений по различным сетям, посредством которого устройства доставляют сообщения получателям.

Все маршрутизаторы должны принимать решения о маршрутизации. В принятии решения маршрутизатор руководствуется заложенными в него таблицами маршрутизации. Каждый маршрутизатор содержит таблицу сетей, подключенных локально, и интерфейсов, через которые осуществляется подключение. В таблицах маршрутизации также содержатся сведения о маршрутах или путях, по которым маршрутизатор связывается с удаленными сетями, не подключенными локально.

Эти маршруты могут назначаться администратором статически или выделяться маршрутизатору динамически: посредством другого маршрутизатора или программного протокола маршрутизации.

Каждый маршрутизатор принимает решения о направлении пересылки пакетов на основании таблицы маршрутизации. Таблица маршрутизации содержит набор правил. Каждое правило в наборе описывает шлюз или интерфейс, используемый маршрутизатором для доступа к определенной сети.

Маршрут состоит из четырех основных компонентов:

- значение получателя;
- маска;
- адрес шлюза или интерфейса;
- стоимость маршрута или метрика маршрута.

Чтобы переслать сообщение получателю, маршрутизатор извлекает IP-адрес получателя из пакета и находит соответствующее правило в таблице маршрутизации.

Значения получателей в таблице маршрутизации соответствуют адресам сетей получателей.

Чтобы определить наличие маршрута к IP-адресу получателя в таблице, маршрутизатор сначала определяет число битов, задающих адрес сети получателя.

Затем маршрутизатор ищет в таблице маску подсети, присвоенную каждому из потенциальных маршрутов. Маршрутизатор применяет каждую из масок подсети к IP-адресу получателя в пакете и сравнивает полученный адрес сети с адресами отдельных маршрутов в таблице:

- при обнаружении совпадающего адреса пакет пересылается на соответствующий интерфейс или к соответствующему шлюзу;

- если адрес сети соответствует нескольким маршрутам в таблице маршрутизации, маршрутизатор использует маршрут с наиболее точным или наиболее длинным совпадающим фрагментом адреса сети;
- иногда для одной сети адресата существует несколько маршрутов с равной стоимостью: маршрут, используемый маршрутизатором, выбирается на основе правил протокола маршрутизации;
- в отсутствие совпадающих маршрутов маршрутизатор направляет сообщение на шлюз, указанный в маршруте по умолчанию, если он настроен.

В маршрутизаторах содержимое таблицы маршрутизации можно просмотреть по команде IOS show ip route. В таблице маршрутизации могут содержаться маршруты нескольких типов:

Прямые маршруты

При включении питания маршрутизатора активируются настроенные интерфейсы. После выхода этих интерфейсов в рабочий режим маршрутизатор будет хранить адреса непосредственно подключенных локальных сетей в виде прямых маршрутов в таблице маршрутизации. В маршрутизаторах Cisco такие маршруты обозначаются в таблице маршрутизации префиксом C. Они автоматически обновляются при перенастройке или отключении маршрута.

Статические маршруты

Сетевой администратор может вручную настроить статический маршрут в конкретную сеть. Статические маршруты не изменяются до тех пор, пока администратор не перенастроит их вручную. В таблице маршрутизации эти маршруты обозначаются буквой S.

Динамические (динамически обновляемые) маршруты

Динамические маршруты автоматически создаются и обновляются протоколами маршрутизации. Протоколы маршрутизации реализуются в программах, которые выполняются на маршрутизаторах и осуществляют обмен сведениями о маршрутизации с другими маршрутизаторами в сети. Динамически обновляемые маршруты обозначаются в таблице маршрутизации приставкой, характеризующей тип протокола, создавшего маршрут. Например, R обозначает информационный протокол маршрутизации (RIP).

Маршрут по умолчанию

Для сетей, путь к которым отсутствует в таблице маршрутизации, используется шлюз, указанный в маршруте по умолчанию. Маршрут по умолчанию является статическим маршрутом. Обычно маршруты по умолчанию указывают на следующий маршрутизатор на пути к Интернет-провайдеру. Если в подсети присутствует только один маршрутизатор, он автоматически выбирается для маршрута по умолчанию, поскольку обмен трафиком с локальной сетью в обоих направлениях может осуществляться только через него.

Протоколы маршрутизации

Маршруты могут меняться весьма резко. Проблемы с кабелями и оборудованием могут привести к недоступности получателей через установленные интерфейсы. Маршрутизаторам необходим способ быстрого обновления маршрутов без участия администратора.

Для динамического управления информацией, поступающей с собственных интерфейсов и других маршрутизаторов, маршрутизаторы используют протоколы маршрутизации. Можно также настроить протоколы маршрутизации для управления маршрутами, заданными вручную.

Динамическая маршрутизация позволяет исключить трудоемкую и ответственную процедуру настройки статических маршрутов. Динамическая маршрутизация позволяет маршрутизаторам реагировать на изменения в сети и корректировать таблицы маршрутизации без вмешательства сетевого администратора.

Протокол динамической маршрутизации определяет все доступные маршруты, помещает наилучшие маршруты в таблицу маршрутизации и удаляет маршруты, ставшие недействительными.

Способ, которым протокол маршрутизации определяет наилучший маршрут к сети назначения, называется алгоритмом маршрутизации (рис. 1).

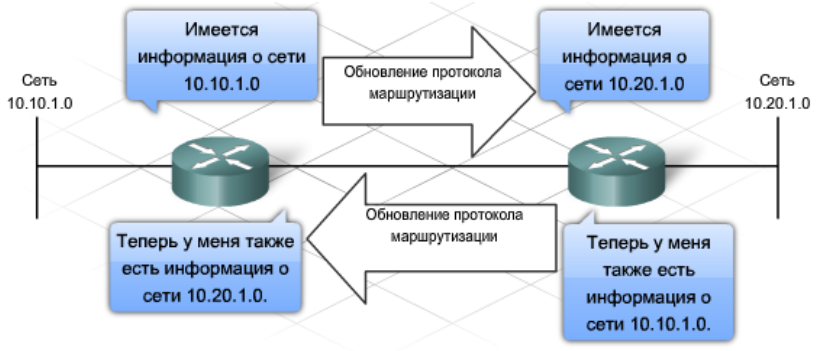


Рис. 1. Посторение таблиц маршрутизации

Алгоритмы маршрутизации подразделяются на два класса: вектор расстояния и состояние соединения. Каждый из них предполагает использование различных методов для определения оптимального маршрута в сеть назначения.

Выбор алгоритма маршрутизации крайне важен при динамической маршрутизации. При каждом изменении топологии сети в результате изменения конфигурации или сбоя также требуется перестройка таблиц маршрутизации в точном соответствии с новой топологией. Состояние обновления всех маршрутизаторов в сети с учетом нового маршрута называется схождением маршрутизаторов.

Для обмена маршрутами между двумя маршрутизаторами необходимо, чтобы они оба использовали один протокол и, следовательно, один алгоритм маршрутизации.

Алгоритм маршрутизации на основе вектора состояния предусматривает периодическую пересылку копий таблицы маршрутизации между маршрутизаторами для отражения изменений топологии.

Алгоритм маршрутизации на основе вектора расстояния анализирует информацию, поступающую от других маршрутизаторов, в свете двух основных критериев:

- расстояние – насколько удалена сеть от данного маршрутизатора;
- вектор – в каком направлении следует пересылать пакеты для данной сети?

Расстояние в маршруте представляется стоимостью или метрикой, которая может характеризовать один из следующих параметров:

- число участков маршрута;
- административные накладные расходы;
- полоса пропускания;
- скорость передачи;

- вероятность задержек;
- надежность.

Компонент вектора или направления в маршруте представляет собой адрес следующего участка пути к сети, указанной в маршруте.

Аналогией для векторов расстояния могут быть дорожные знаки с указанием направлений на развязках автострад. Знак указывает направление к месту назначения и сообщает расстояние до него. По мере движения по автостраде появляется следующий знак, указывающий на то же место назначения, но расстояние становится короче. Если расстояния сокращаются, трафик следует по оптимальному маршруту.

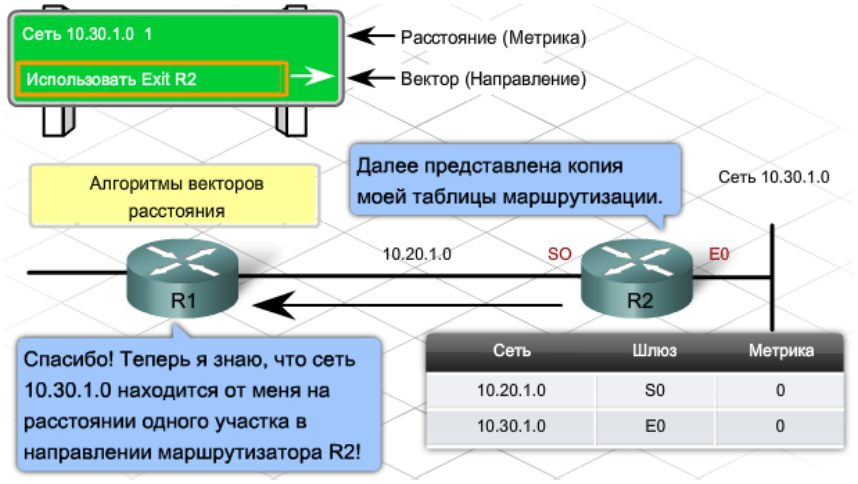


Рис. 2. Определение вектора расстояния

Каждый маршрутизатор, использующий векторы расстояний, сообщает сведения о маршрутизации своим соседям (рис. 2). Соседние маршрутизаторы являются участниками сети с прямым подключением. Интерфейс, ведущий в каждую сеть с прямым подключением, имеет расстояние, равное 0.

Каждый маршрутизатор получает таблицу маршрутизации с непосредственно подключенных соседних маршрутизаторов.

Для примера, маршрутизатор R2 получает информацию с маршрутизатора R1.

Рис. 3. Обмен таблицами маршрутизации

Маршрутизатор R2 увеличивает значение метрики (в данном случае – число участков маршрута), отражая тот факт, что теперь путь к сети назначения стал на один участок длиннее. Затем маршрутизатор R2 рассылает новую таблицу маршрутизации своим соседям, включая маршрутизатор R3. Этот поэтапный процесс продолжается во всех направлениях между соседними маршрутизаторами (рис. 3).

В конечном итоге каждый маршрутизатор получит от соседних маршрутизаторов информацию о других, более удаленных, сетях. Каждой записи сети в таблице маршрутизатора соответствует вектор накопленного расстояния, указывающий удаленность сети в данном направлении.

Продолжая процесс определения в сети векторов расстояния, маршрутизаторы находят оптимальный путь к сетям, подключенным не напрямую, на основе накопленных метрик от каждого из соседей.

Оптимальный путь – это путь с кратчайшим расстоянием или наименьшей метрикой.

Обновление таблиц маршрутизации также происходит при изменении топологии, например, при добавлении новой сети или выходе из строя маршрутизатора, в результате которого сеть становится недостижима. Как и при обнаружении сетей, обновление топологии происходит поэтапно и состоит в обмене копиями таблиц маршрутизации между маршрутизаторами.

Внутренние и внешние протоколы маршрутизации

Маршрутизаторы используют протоколы маршрутизации для обмена маршрутной информацией. Иными словами, протоколы маршрутизации определяют, как маршрутизируются протоколы передачи данных (т.е. маршрутизируемые). Как показано на рис. 4, двумя семействами протоколов маршрутизации являются *протоколы внутренних шлюзов (Interior Gateway Protocol - IGP*) и *протоколы внешних шлюзов (Exterior Gateway Protocols - EGP*). Классификация всех протоколов по этим двум семействам основана на принципе их работы по отношению к автономным системам.

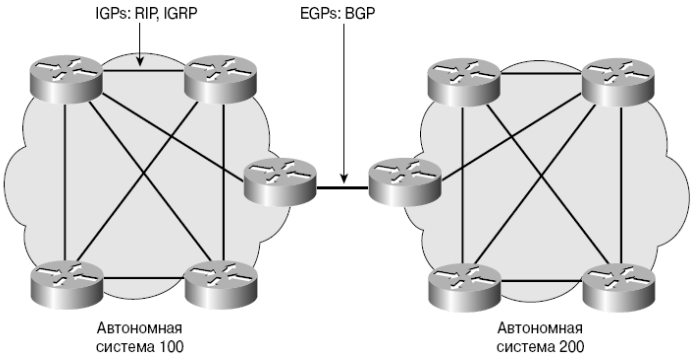


Рис. 4. Протоколы EGP и IGP

Автономной системой (Autonomous System - AS) называется сеть или группа сетей, находящихся под единым административным контролем. Автономная система состоит из маршрутизаторов, которые для внешнего мира (т.е. для других сетей) выглядят как единая сеть.

Такие автономные системы описываются шестнадцатибитовым номером. При настройке таких протоколов маршрутизации, как BGP, требуется указать назначенный уникальный номер автономной системы.

Протоколы класса IGP маршрутизируют данные внутри автономных систем.

К классу IGP относятся следующие протоколы маршрутизации:

- протоколы RIP и RIP V2;
- IGRP;
- EIGRP;
- OSPF;
- протокол обмена данными между промежуточными системами (Intermediate system-to-Intermediate System – IS-IS).

Протоколы класса EGP маршрутизируют данные между автономными системами.

Протокол BGP является наиболее широко известным представителем класса EGP.

Протоколы маршрутизации по состоянию каналов

Маршрутизаторы, использующие алгоритм маршрутизации на основе вектора расстояния, располагают ограниченными сведениями об удаленных сетях и совсем не имеют информации об удаленных маршрутизаторах. Алгоритм маршрутизации, основанный на состоянии канала, ведет полную базу данных об удаленных маршрутизаторах и схеме их соединений.

В маршрутизации на основе состояния канала присутствуют следующие атрибуты:

1. таблица маршрутизации – список известных маршрутов и интерфейсов;

Объявление о состоянии канала (LSA) – компактный пакет для обмена сведениями о маршрутизации между маршрутизаторами. LSA описывает состояние интерфейсов (каналов связи) маршрутизатора и содержит другие сведения, например IP-адрес каждого канала;

2. топологическая база данных – концентрирует информацию, извлеченную маршрутизатором из всех LSA;
3. алгоритм SPF (первоочередное определение кратчайших маршрутов) – расчет дерева SPF на основании информации из базы данных. Дерево SPF представляет собой карту сети с точки зрения конкретного маршрутизатора. Содержимое этого дерева используется при построении таблицы маршрутизации.

При получении LSA с других маршрутизаторов алгоритм SPF путем анализа информации в базе данных создает дерево SPF. Руководствуясь деревом SPF, алгоритм SPF вычисляет кратчайшие пути к другим сетям. При изменении базы данных о состоянии каналов связи, вызванном поступлением нового пакета LSA, алгоритм SPF повторно рассчитывает оптимальные пути и обновляет таблицу маршрутизации.

Примерами протоколов, использующих алгоритм с учетом состояния каналов, являются OSPF и IS-IS (рис. 5).

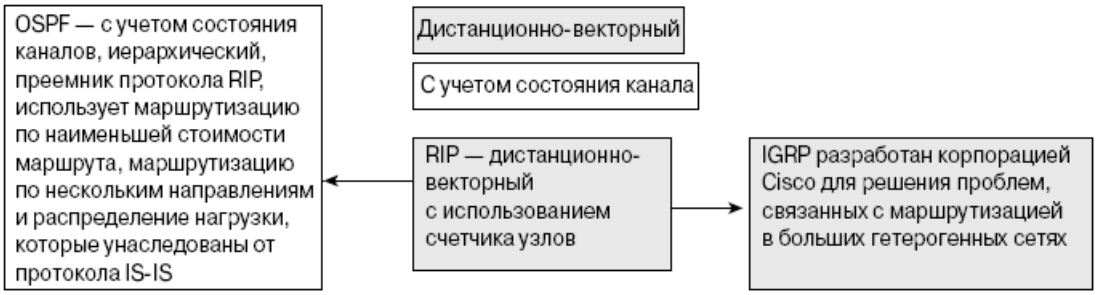


Рис. 5. Протоколы, использующие алгоритм с учетом состояния каналов

Протокол RIP

Протокол маршрутной информации (Routing Information Protocol - RIP) использует счетчик количества транзитных узлов для определения направления и расстояния для любого из каналов сети. Если существуют несколько маршрутов к получателю, протокол RIP выберет тот из них, который имеет наименьшее значение счетчика транзитных узлов. Поскольку счетчик является единственной метрикой, используемой протоколом RIP, выбранный маршрут далеко не всегда оказывается кратчайшим. Протокол RIP версии 1 позволяет использовать только классовую (classfull) маршрутизацию. Это означает, что все сетевые устройства должны иметь одинаковую маску сети, поскольку RIP версии 1 не включает в маршрутные обновления информацию о ней.

Протокол RIP версии 2 использует так называемую *префиксную маршрутизацию (prefix routing*) и пересылает маску сети вместе с анонсами таблиц маршрутизации: именно за счет этой функции обеспечивается поддержка бесклассовой маршрутизации. Благодаря протоколам бесклассовой маршрутизации можно использовать подсети с разной длины масками внутри одной и той же сети. Использование масок подсети разной длины внутри одной сети называется технологией масок переменной длины (Variable Length Subnet Mask -VLSM).

Протокол RIP имеет простую логику, несложен в реализации и доступен без дополнительной платы в большинстве маршрутизаторов. Эти преимущества принесли RIP широкую популярность.

Однако RIP обладает и недостатками:

1. допускается не более 15 участков маршрута, т.е. сеть может содержать не более 16 последовательно соединенных маршрутизаторов;
2. непосредственно подключенным соседним маршрутизаторам периодически рассылаются полные копии всей таблицы маршрутизации – в крупных сетях каждое обновление может сопровождаться значительным всплеском трафика;
3. длительное схождение после изменений в крупных сетях.

В настоящее время существуют две версии RIP: RIPv1 и RIPv2. RIPv2 имеет ряд преимуществ по сравнению с RIPv1. RIPv1 обычно используется в тех случаях, когда оборудование не поддерживает RIPv2. Наиболее значимым различием двух версий протокола является поддержка бесклассовой маршрутизации в RIPv2 за счет включения маски подсети в обновления маршрутов. RIPv1 не предусматривает отправку масок подсетей в обновлениях и руководствуется масками, принятыми для различных подсетей по умолчанию.

Протокол EIGRP

Расширенный протокол маршрутизации внутреннего шлюза (EIGRP) – это собственный усовершенствованный протокол маршрутизации Cisco с использованием вектора расстояния. EIGRP был разработан с целью преодоления ограничений других протоколов маршрутизации с вектором расстояний, таких как RIP. К этим ограничениям относятся использование числа участков маршрута в качестве метрики и предел в 15 участков.

Вместо числа участков в EIGRP используется несколько метрик, включая значение полосы пропускания, настраиваемое вручную, и задержка при прохождении пакета по конкретному маршруту.

Основные характеристики EIGRP:

- расчет стоимости маршрута на основе нескольких метрик;
- возможности протоколов на основе вектора расстояния, связанные со следующим участком и метрикой, объединены с дополнительными функциями баз данных и обновлений;
- максимальное число участков маршрута – 224

EIGRP формирует таблицу топологии на основе извещений от соседних маршрутизаторов. Таблица топологии содержит все маршруты, объявленные соседними маршрутизаторами. Для расчета кратчайшего пути по сети к месту назначения в протоколе EIGRP применяется алгоритм диффузионного обновления (DUAL). Рассчитанный путь помещается в таблицу маршрутизации. Таблица топологии позволяет маршрутизатору, на котором используется протокол EIGRP, определять оптимальный альтернативный маршрут при изменениях в сети. Если в таблице

маршрутизации отсутствуют альтернативные маршруты, EIGRP опрашивает соседние маршрутизаторы для нахождения нового маршрута к месту назначения.

В отличие от протокола RIP, предназначенного для небольших сетей, в которых число участков между маршрутизаторами не превышает 15, протокол EIGRP наилучшим образом подходит для крупных более сложных сетей, объединяющих до 224 участков и требующих быстрого схождения.

Выбор конкретного протокола маршрутизации может стать сложной задачей даже для опытных проектировщиков сетей. При проектировании сети полезно учесть следующие рекомендации.

Статические маршруты бывают приемлемы для небольших сетей только с одним шлюзом в Интернет. В такой топологии динамическая маршрутизация требуется редко.

По мере роста организации и появления новых маршрутизаторов в топологии можно перейти к использованию протокола RIPv2, не требующему сложной настройки и успешно работающему в небольших сетях. RIP может применяться до тех пор, пока размер сети не превысит 15 маршрутизаторов.

В более крупных сетях широкое применение нашли протоколы EIGRP и OSPF, однако простых правил для выбора одного из них не существует. При выборе протокола следует рассматривать каждую сеть в отдельности, руководствуясь тремя основными критериями.

Простота управления. Какую информацию о собственном состоянии хранит протокол? Какие команды «show» доступны?

Простота настройки. Сколько команд в среднем требуется выполнить для настройки? Можно ли задать одинаковую конфигурацию сразу для нескольких маршрутизаторов в сети?

Эффективность. Какую долю полосы пропускания отнимает протокол маршрутизации в установившемся режиме и каков верхний предел используемой полосы пропускания при схождении в результате крупных событий?

Протокол OSPF

Открытый протокол поиска кратчайшего пути (Open Shortest Path First - OSPF) использует алгоритм маршрутизации по состоянию каналов. OSPF является протоколом IGP-типа, что означает, что он распространяет маршрутную информацию между маршрутизаторами, находящимися в единой автономной системе.

Протокол OSPF был разработан для использования в больших сетях, в которых невозможно использование протокола RIP.

Его основными характеристиками являются:

- использование алгоритма SPF для расчета пути к месту назначения с наименьшей стоимостью;
- рассылка обновлений маршрутов только при изменении топологии; периодическая рассылка полной таблицы маршрутизации не производится;
- ускоренная сходимость;
- поддержка VLSM и изолированных подсетей;
- аутентификация маршрутов.

В сетях с поддержкой OSPF маршрутизаторы обмениваются извещениями о состоянии каналов связи, информируя друг друга о таких изменениях, как:

- добавление нового соседнего маршрутизатора;
- выход из строя канала;
- восстановление канала.

При изменении топологии сети, например, при выходе из строя одного из каналов или при добавлении нового маршрутизатора, все маршрутизаторы, на которых влияет данное изменение, рассылают остальным маршрутизаторам сети извещения LSA для обновления маршрутов. Все маршрутизаторы вносят соответствующие изменения в базы данных топологий, перестраивают деревья SPF для поиска кратчайшего пути к каждой сети и обновляют маршруты в своих таблицах маршрутизации.

2. Протоколы внешней маршрутизации

Автономные системы

Архитектура маршрутизации за годы существования Интернета эволюционировала в распределенную систему взаимосвязанных сетей. При сегодняшнем масштабе Интернета и многообразии составляющих его сетей ни одна организация не справится с управлением информацией обо всех маршрутах к каждому получателю в мире.

Для преодоления этой сложности Интернет поделен на объединения сетей, называемые автономными системами (AS), контролируемые разными независимыми организациями и компаниями.

AS представляет собой несколько сетей в ведении одного административного органа, для которых применяется единая внутренняя политика маршрутизации. Идентификатором AS служит уникальный номер автономной системы (ASN). ASN в Интернете подчиняются правилам контроля и регистрации.

Самым распространенным примером AS является Интернет-провайдер (ISP). Большинство предприятий, подключенных к Интернету через провайдера, входят в состав домена маршрутизации этого провайдера. AS администрируется провайдером и содержит не только маршруты для собственных сетей, но и маршруты ко всем сетям корпоративных и других клиентов, подключенных к провайдеру.

Один и тот же номер ASN распространяется на все сетевые устройства в домене маршрутизации AS.

Провайдер A представляет собой автономную систему, чей домен маршрутизации включает в себя местное предприятие, напрямую подключенное к провайдеру для доступа в Интернет. Это предприятие не имеет отдельного ASN, а использует в данных о маршрутизации номер автономной системы провайдера A (ASN 100).

Также на иллюстрации показана крупная корпорация с офисами в Гонконге и Нью-Йорке. Поскольку эти офисы расположены в разных странах, каждый из них для доступа в Интернет подключается к местному провайдеру. Следовательно, корпорация пользуется услугами двух различных провайдеров. К какой AS и с каким номером ASN она будет принадлежать?

Наличие двух провайдеров – B и C, через которые компания подключена к Интернету, создает сложности с организацией маршрутов. Для трафика из Интернета нет информации, на основе которой можно было бы выбрать одну из AS, используемых глобальной корпорацией. Что-

бы решить эту проблему, корпорация регистрирует собственную AS, которой присваивается ASN 400 (рис. 6).

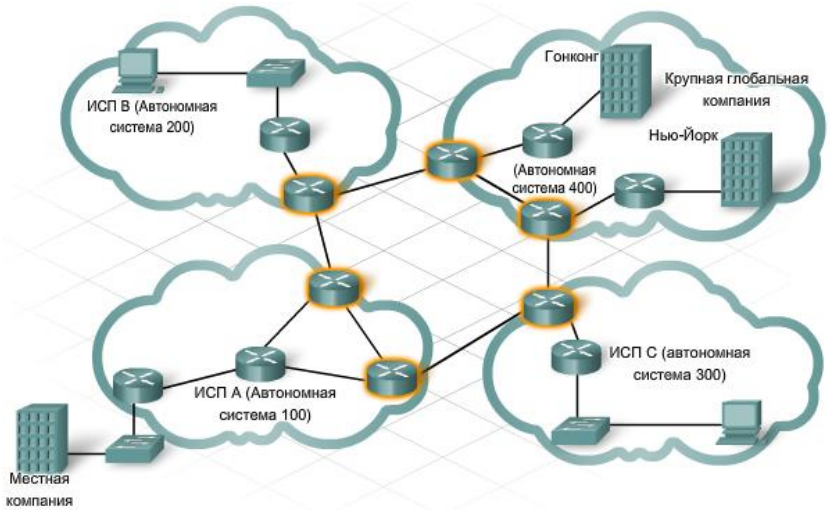


Рис. 6. Автономные системы

Маршрутизация между автономными системами

Протоколы внутренних шлюзов (IGP) используются для обмена сведениями о маршрутизации с автономной системой или отдельной организацией. Цель протокола внутренней маршрутизации – нахождение оптимального пути во внутренней сети. IGP реализуется внутренними маршрутизаторами, т.е. маршрутизаторами внутри организации. Примеры протоколов внутренних шлюзов – RIP, EIGRP и OSPF.

В отличие от IGP, протоколы внешних шлюзов (EGP) предназначены для обмена информацией между различными автономными системами. Поскольку разные автономные системы находятся в компетенции разных администраторов и могут использовать различные внутренние протоколы, то протокол, применяемый на межсетевом уровне, должен обеспечивать взаимодействие разнородных систем. EGP отвечает за преобразование информации о внешних маршрутах, делая возможной ее успешную обработку в каждой сети автономной системы.

Протоколы EGP выполняются на внешних маршрутизаторах, расположенных на границе автономной системы. Внешние маршрутизаторы также называются граничными шлюзами (рис. 7).

В отличие от внутренних маршрутизаторов, которые обмениваются друг с другом информацией об отдельных маршрутах по протоколам IGP, внешние маршрутизаторы обмениваются информацией о путях к различным сетям, используя внешние протоколы. Назначение внешних протоколов маршрутизации – поиск оптимального пути через Интернет в виде последовательности автономных систем.

Самый распространенный внешний протокол маршрутизации в Интернете сегодня – протокол граничного шлюза (BGP). По оценкам 95% автономных систем используют BGP.

Каждая автономная система отвечает за информирование других автономных систем о сетях, которые через нее доступны. Обмен этими сведениями о достижимости осуществляется по внешним протоколам маршрутизации, которые реализуются выделенными маршрутизаторами – граничными шлюзами.

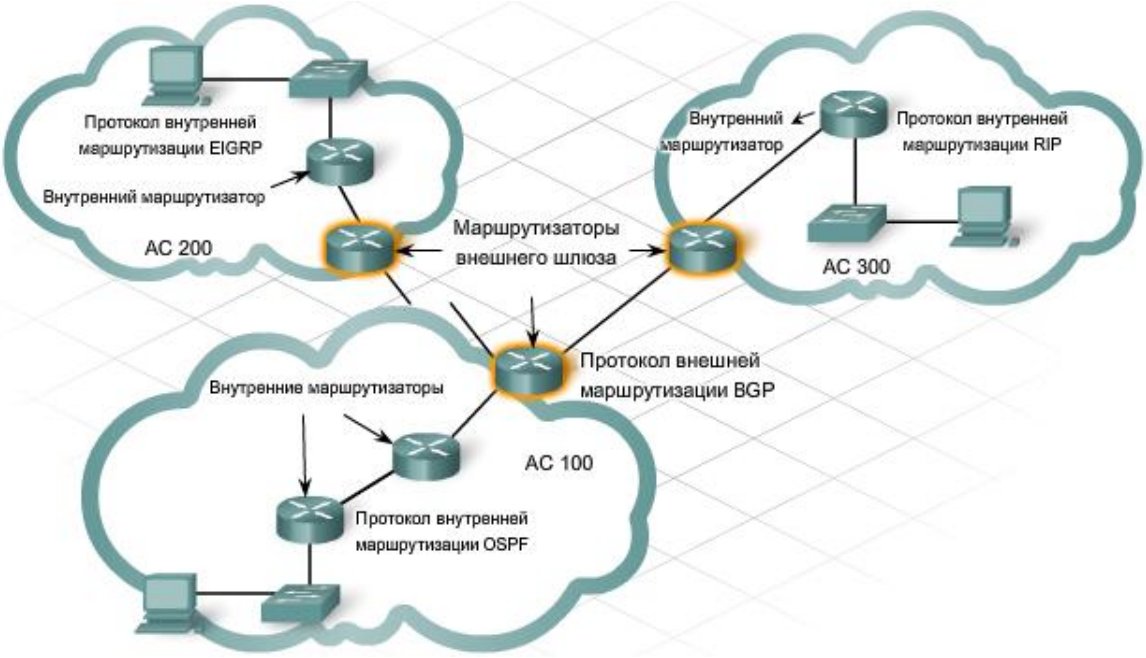


Рис. 7. Маршрутизация между автономными системами

Маршрутизация пакетов через Интернет осуществляется в несколько этапов

1. Узел-источник отправляет пакет, предназначенный для удаленного узла в другой автономной системе.

2. Поскольку IP-адрес адресата пакета находится за пределами локальной сети, внутренние маршрутизаторы продолжают передавать пакет, выбирая маршруты по умолчанию, пока в итоге пакет не достигнет внешнего маршрутизатора на границе локальной автономной системы.

3. Внешний маршрутизатор ведет базу данных по всем автономным системам, с которыми он связан. Эта база данных достижимости сообщает маршрутизатору, что путь к сети адресата проходит через несколько AS и что следующий участок пути проходит через напрямую подключенный внешний маршрутизатор на соседней автономной системе.

4. Внешний маршрутизатор направляет пакет на следующий участок пути, которым является внешний маршрутизатор в соседней автономной системе.

5. Пакет достигает соседней автономной системы, где внешний маршрутизатор обращается к собственной базе данных достижимости и пересылает пакет к следующей автономной системе в пути.

6. Процесс повторяется на каждой автономной системе до тех пор, пока внешний маршрутизатор автономной системы-адресата не распознает IP-адрес получателя пакета как относящийся к внутренней сети данной автономной системы.

7. Конечный внешний маршрутизатор направляет пакет маршрутизатору на следующем внутреннем участке, присутствующему в его таблице маршрутизации. С этого момента пакет обрабатывается так же, как любой локальный пакет и пересылается посредством внутренних протоколов маршрутизации через несколько внутренних участков до узла-получателя.

Внешние протоколы маршрутизации и Интернет-провайдеры

Протоколы внешних шлюзов предоставляют много полезных функций Интернет-провайдерам. Внешние протоколы не только позволяют пересылать трафик через Интернет уда-

ленным получателям, но они также служат для провайдера механизмом установки и реализации политик и локальных настроек, позволяющих оптимизировать пересылку трафика через провайдера и исключить перегрузку внутренних маршрутов (рис. 8).

Корпоративные клиенты требуют надежного предоставления услуг доступа в Интернет, и провайдеры стремятся обеспечить непрерывную работу Интернет-канала для этих клиентов. Для этого они предусматривают запасные маршруты и маршрутизаторы на случай отказа основного маршрута. При нормальной работе Интернет-провайдер сообщает другим автономным системам основной маршрут. Если этот маршрут прекращает функционировать, провайдер рассылает по внешнему протоколу сообщение с обновлением маршрута, указывая запасной маршрут.

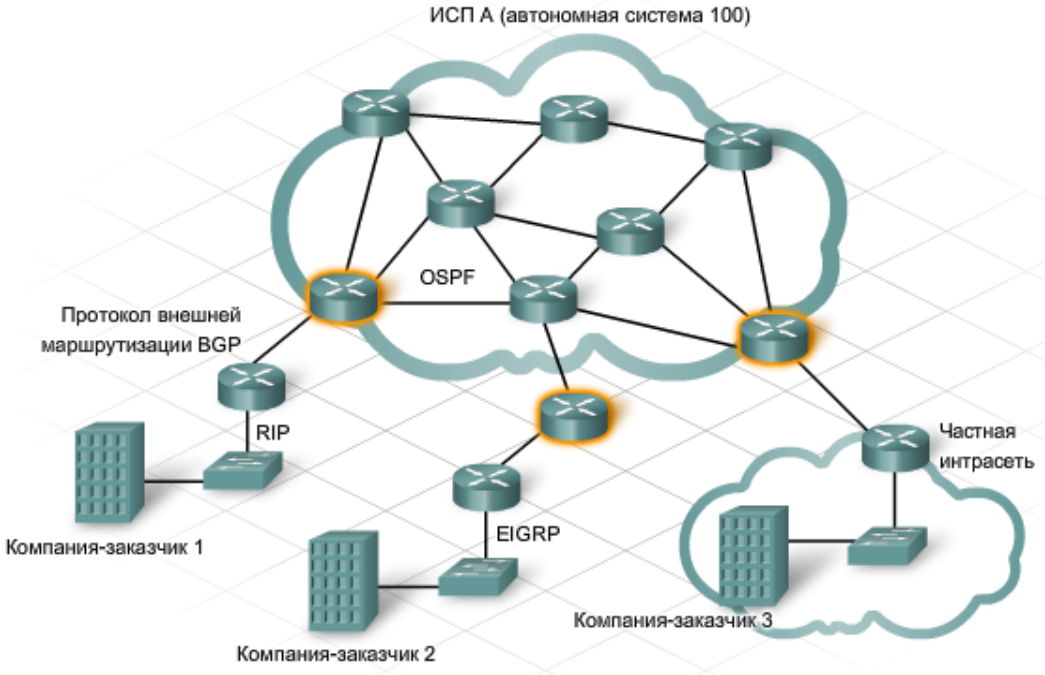


Рис. 8. Внешние протоколы маршрутизации и Интернет-провайдеры

Движение сообщений в Интернете называется трафиком. Интернет-трафик может быть отнесен к одной из двух категорий.

Локальный трафик – трафик, пересылаемый внутри автономной системы и изначально возникший в ее пределах или адресованный получателю в пределах этой автономной системы. Аналогия – движение транспорта в пределах улицы.

Транзитный трафик - трафик, возникший за пределами автономной системы, который может пересылаться по сетям внутри автономной системы получателям за ее пределами. Аналогия – сквозное движение по улице.

Пересылка трафика между автономными системами надежно контролируется. Важно иметь возможность ограничения или запрета обмена определенными видами сообщений с автономной системой – по соображениям безопасности или для предотвращения перегрузки (рис. 9).

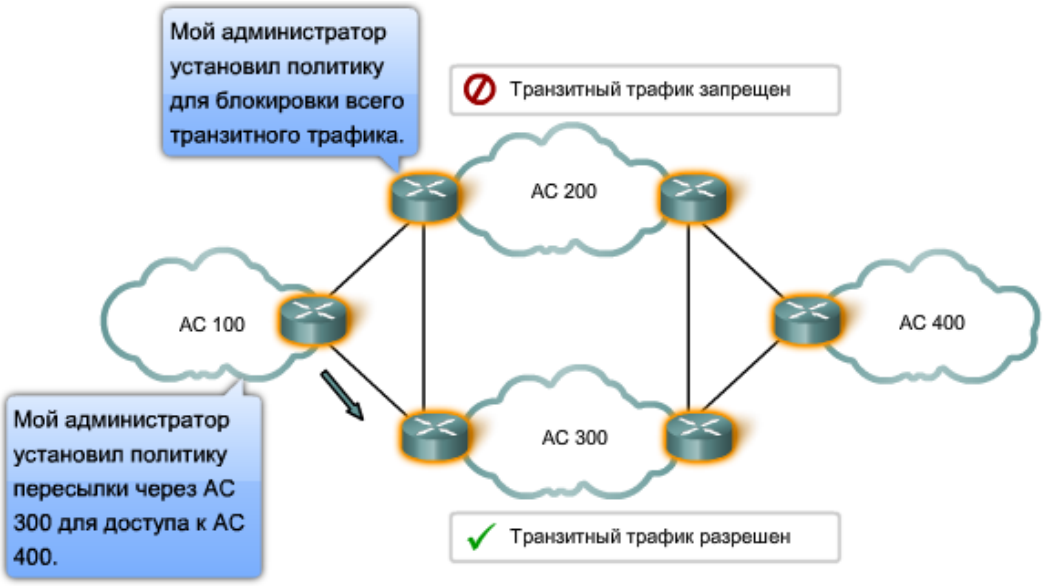


Рис. 9. Транзит трафика через автономные системы

Многие автономные системы не предназначены для транзитного трафика. Транзитный трафик может привести к перегрузке и выходу из строя маршрутизаторов, если их ресурсов окажется недостаточно для обработки большого объема трафика.

Контрольные вопросы

1. Что такое маршрутизация и когда они применяется?
2. Какие типы маршрутов могут содержаться в таблице маршрутизации?
3. Какие протоколы относятся к внутренним и внешним протоколам маршрутизации?
4. Для чего используются автономные системы?
5. Какие функции выполняют внутренние и внешние шлюзы?

Лекция 21
Списки управления доступом

1. **Введение в списки управления доступом**
2. **Конфигурирование списков управления доступом**
3. **Стандартные списки ACL**
4. **Расширенные списки управления доступом**
5. **Использование именованных списков управления доступом**

1. Введение в списки управления доступом

Сетевой администратор должен уметь запрещать несанкционированный доступ к сети и в то же время обязан обеспечить доступ к сети авторизированных пользователей. Несмотря на то, что средства безопасности, такие, как пароли, средства установления обратного вызова и физические устройства безопасности, достаточно полезны, им часто не хватает гибкости при фильтрации потока данных и специализированных управляющих средств, которые чаще всего предпочитают администраторы.

Например, бывают ситуации, когда сетевой администратор готов предоставить пользователям локальной сети выход в сеть Internet, но при этом не хочет разрешать пользователям сети Internet, находящимся вне такой локальной сети, входить в сеть предприятия средствами протокола telnet.

Маршрутизаторы предоставляют администраторам основные возможности фильтрации, такие, как блокирование потока данных из сети Internet с использованием *списков управления доступом (Access Control List - ACL*). Список управления доступом представляет собой последовательный набор разрешающих или запрещающих директив, которые относятся к адресам или протоколам верхнего уровня.

Правила списка ACL, которые принадлежат одному и тому же списку управления доступом, всегда содержат один и тот же номер-идентификатор списка. Например, представим себе такой набор списков и правил:

- список управления доступом 1
  - правило списка ACL 1,
  - правило списка ACL 1,
- список управления доступом 2
  - правило списка ACL 2,
  - правило списка ACL 2,

В приведенной структуре списков ACL правило, номер которого совпадает с номером списка, относится к определенному нумерованному списку. Сами правила выполняются в процессе отработки списка последовательно.

Администратору и техническому специалисту необходимо уметь правильно конфигурировать списки управления доступом и знать, где их следует разместить в сети.

Основные функции списков управления доступом включают в себя:

- фильтрацию внутренних пакетов;
- защиту внутренней сети от несанкционированного доступа;

- ограничение доступа к портам виртуального терминала.

Списки управления доступом (ACL) представляют собой набор инструкций, применяемых к интерфейсу маршрутизатора. Они указывают маршрутизатору, какие пакеты следует принять, а какие - отбросить. Решение о том, как поступить с пакетом, может быть основано на определенных критериях, таких, как адреса отправителя и получателя или номер порта TCP/UDP.

Списки управления доступом позволяют администратору управлять потоками данных и сканировать определенные пакеты. Любые потоки данных, которые проходят через интерфейс маршрутизатора, проверяются на соответствие условиям списка.

Списки управления доступом могут быть созданы для всех маршрутизируемых сетевых протоколов, таких, например, как Internet-протокол (Internet Protocol - IP) или протокол межсетевого пакетного обмена (Internetwork Packet Exchange - IPX), с целью фильтрации пакетов по мере их поступления на маршрутизатор. Для списков ACL может быть установлена конфигурация, позволяющая управлять доступом к сети или подсети.

Алгоритм списков управления доступом при фильтрации потока данных принимает решение о том, направить пакет далее или заблокировать его на интерфейсе.

Каждый пакет исследуется на соответствие условиям, которые указаны в списке; в качестве условий могут выступать адреса отправителя и получателя, идентификатор протокола верхнего уровня или другая информация.

Список ACL должен составляться для каждого отдельного протокола. Иными словами, для *каждого* используемого на интерфейсе маршрутизатора протокола должен быть составлен список, который будет регулировать трафик именно *на этом* интерфейсе. (Отметим, что в некоторых протоколах списки управления доступом называются *фильтрами*). Списки могут быть использованы в качестве гибкого средства фильтрации пакетов, поступающих на интерфейс маршрутизатора или отправляемых с него (рис. 1).

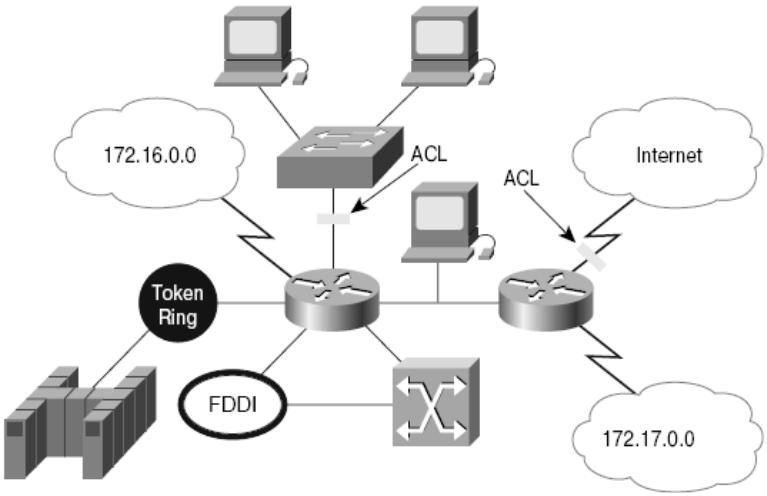


Рис. 1. Пример использования списков управления доступом

Для создания списков управления доступом существует множество причин; некоторые из них перечислены ниже.

- Списки ACL можно использовать для ограничения потока данных в сети и повышения ее производительности. В частности, списки могут быть использованы для того, чтобы некоторые

пакеты какого-либо протокола обрабатывались маршрутизатором ранее других. Такая функция называется *установкой очередности (queuing*) и используется для того, чтобы маршрутизатор не обрабатывал пакеты, которые в данный момент не являются жизненно необходимыми. Установка пакетов в очередь ограничивает поток данных в сети и уменьшает вероятность перегрузки.

- Списки ACL можно использовать для управления потоком данных. Например, с помощью списков можно ограничить или уменьшить количество сообщений об изменениях в сети. Такие ограничения используются для предотвращения распространения информации об отдельных сетях на всю сеть.

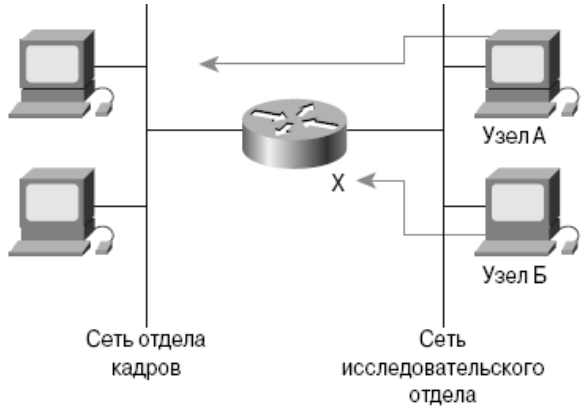


Рис. 2. Пример ограничения сетевого трафика

- Списки ACL можно использовать для обеспечения базового уровня защиты от несанкционированного доступа. Например, списки доступа позволяют разрешить одному узлу доступ к некоторому сегменту сети, а другому закрыть доступ к этой же области. На рис. 2 показано, что узлу А разрешен доступ к сети пользователей, а узлу Б такой доступ запрещен. Если на маршрутизаторе не установлен список управления доступом, то все пакеты, проходящие через него, поступают во все сегменты сети.

- Списки ACL можно использовать для указания данных, которые будут направляться далее или блокироваться на интерфейсе маршрутизатора

Например, можно разрешить маршрутизацию трафика электронной почты и в то же время заблокировать весь поток данных протокола telnet.

Принцип работы списков управления доступом

Список управления доступом представляет собой набор директив, которые определяют то, как пакеты

- поступают на входной интерфейс маршрутизатора,
- доставляются внутри маршрутизатора,
- пересылаются далее через выходной интерфейс маршрутизатора.

Начальная стадия процесса установления связи не зависит от того, используются ли списки управления доступом или нет. Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить - на маршрутизатор или на мост (т.е. являются ли пакеты маршрутизируемыми или коммутируемыми). Если пакет по какой-либо причине не может быть обработан маршрутизатором или мостом, он отбрасывается. Далее операционная система проверяет, связан ли со входным интерфейсом какой-либо список доступа. Если список есть, то операционная система сверяет параметры пакета с записями такого списка ACL. Если пакет соответствует разрешающему правилу и подвергается маршрутизации, то в таблице маршрутизации выполняется поиск сети-получателя, определяется метрика маршрута или состояние и интерфейс, через который следует отправить пакет. Список управления доступом не фильтрует пакеты, которые возникают внутри маршрутизатора, но фильтрует пакеты из иных источников.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка управления доступом. Если его там нет, то пакет может быть направлен на интерфейс получателя непосредственно; например, при использовании интерфейса E0, который не связан со списками управления доступом, пакет отправляется непосредственно через такой интерфейс.

Директивы списка исполняются в последовательном логическом порядке. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, пакет передается далее или отбрасывается в соответствии с конфигурацией. Если заголовок пакета не соответствует ни одной директиве списка, то к нему применяется стандартное правило, размещенное в конце списка, которое запрещает передачу любых пакетов. Даже если такая директива не отображается в последней строке списка управления доступом, она стандартно там присутствует. В примере, который проиллюстрирован на рис. 4, пакет соответствует условию первой директивы и ему отказано в доступе. Он отбрасывается, соответствие пакета последующим условиям не проверяется. Для уничтожения пакета используется *битовая корзина (bit bucket*). Если пакет не соответствует условию первой директивы, он проверяется на соответствие второй директиве из списка управления доступом, и т.д.

Списки ACL позволяют контролировать, каким пользователям разрешен доступ к конкретной сети. Условия в списке контроля доступа позволяют:

- просмотреть адреса определенных узлов для того, чтобы разрешить или заблокировать им доступ к некоторой части сети;
- разрешить или запретить доступ пользователям только к определенным видам приложений, таким, как службы FTP и HTTP.

2. Конфигурирование списков управления доступом

Списки ACL создаются в режиме глобальной конфигурации устройства. Существует великое множество разных типов списков управления доступом: стандартные, расширенные, списки протокола IPX, списки AppleTalk и многие другие. При создании списков ACL в маршрутизаторе каждому списку следует назначить уникальный номер. Такой номер идентифицирует тип списка и не должен выходить за границы диапазона номеров, который выделен для определенной разновидности списков.

После того как администратор переводит режим командной строки в нужный и принято решение о том, из какого диапазона следует выбрать номер списка, он последовательно вводит директивы списка ACL, начиная с ключевого слова **access-list** и заканчивая правильными параметрами. Создание списка управления доступом - это только половина дела. Вторая, и не менее важная часть процесса, - это привязка списка к интерфейсу.

Списки ACL могут быть привязаны к одному и более интерфейсам и могут фильтровать как входные, так и выходные потоки данных. Привязка списка к интерфейсу (интерфейсам) осуществляется посредством команды **access-group**. Команда **access-group** вводится в режиме конфигурирования интерфейса. Список управления доступом привязывается к интерфейсу во входном или выходном направлении: для входящего или исходящего трафика. Чтобы определить, в каком направлении должен воздействовать список ACL на проходящие через интерфейс потоки данных, следует «взглянуть на интерфейс изнутри маршрутизатора», т.е. представить себе, что вы находитесь внутри устройства. Такой подход поможет разобраться в потоках тра-

фика во многих ситуациях, когда необходимо понять, какие потоки данных, в каком направлении передаются. С точки зрения «наблюдателя внутри маршрутизатора», трафик, который входит из внешнего мира внутрь устройства через интерфейс, может быть отфильтрован входным списком управления доступом; соответственно, поток данных, который направлен из устройства во внешнюю сеть через интерфейс, может быть отфильтрован выходным списком. После того как нумерованный список ACL создан, его следует привязать к нужному интерфейсу. Чтобы изменить порядок следования директив в нумерованном списке управления доступом, необходимо удалить весь список с помощью команды **no access-list** номер списка и создать его заново.

На практике команды списков управления доступом представляют собой длинные символьные строки. Основные задачи, решение которых описано в этом разделе, включают в себя следующие действия:

- необходимо сконфигурировать список управления доступом в режиме глобальной конфигурации маршрутизатора;
- следует назначить номер списку управления доступом в диапазоне от 1 до 99, если требуется создать стандартный список для протокола IP;
- следует назначить номер списку управления доступом в диапазоне от 100 до 199, если требуется создать расширенный список ACL для протокола IP;
- при создании списка ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. В списке должны быть указаны разрешенные IP-протоколы; все данные других протоколов должны быть запрещены;
- необходимо выбрать IP-протоколы, которые следует проверять; все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя;
- после того как будет создан необходимый список контроля доступа, его следует привязать к определенному интерфейсу.

Несмотря на то, что каждый протокол выдвигает свои специфические требования и правила, выполнение которых необходимо для фильтрации трафика, в целом создание списков управления доступом требует выполнения всего двух основных действий, которые указаны ниже.

Этап 1. Создать список доступа ACL.

Этап 2. Применить список доступа на конкретном интерфейсе.

Списки управления доступом применяются к одному или нескольким интерфейсам и выполняют фильтрацию входящих или исходящих потоков данных, в зависимости от установленной конфигурации. Списки для исходящего трафика обычно более эффективны, поэтому предпочтительнее использовать именно их. Маршрутизатор, в котором сконфигурирован список ACL для входящего трафика, должен проверять каждый пакет на его соответствие условиям списка перед тем, как отправить пакет на выходной интерфейс.

Использование шаблона any

Работа с десятичным представлением битов шаблона может показаться утомительной3. Во многих случаях ключевые слова (или зарезервированные шаблоны) значительно упростят работу со списками ACL. Прежде всего, такие ключевые слова уменьшают количество символов, которое приходится набирать на клавиатуре при записи условий проверки для отдельных адресов. Одним из таких шаблонов является ключевое слово **any** (переводится как *любой*). Например, ес-

ли требуется разрешить доступ для всех адресов получателей, можно указать маску 0.0.0.0 (рис. 3); кроме этого, список управления доступом должен игнорировать (т.е. пропускать их без проверки) любые значения битов адреса, поэтому все биты инвертированной маски должны быть равны единице (т.е. 255.255.255.255).

Рис. 3. Шаблон **any**

Для указания описанного выше условия можно также использовать ключевое слово **any**. Вместо того чтобы набирать на клавиатуре 0.0.0.0 255.255.255.255, достаточно указать простое и короткое ключевое слово **any**.

Например, вместо использования строки

Router(config)# **access_list 1 permit 0.0.0.0 255.255.255.255**

можно просто набрать

Router(config)# **access_list 1 permit any**

Использование шаблона host

Второй случай, когда можно использовать ключевое слово в списке ACL, — это ситуация, когда необходимо соответствие всех битов адреса одного узла заданному шаблону. Предположим, требуется заблокировать доступ конкретному узлу. Чтобы указать один узел, надо полностью ввести его IP-адрес (например, 172.30.16.29 (рис. 4), а затем указать, что в списке должны быть проверены все биты адреса, т.е. инвертированная маска должна состоять только из нулей (0.0.0.0).

Рис. 4. Шаблон **host**

Можно использовать ключевое слово **host**, которое укажет операционной системе Cisco IOS, что нужно проверять только один полный адрес. В приведенном ниже примере показано, что вместо ввода длинной строки **172.30.16.29 0.0.0.0** перед адресом можно записать ключевое слово **host**.

Например, вместо строки

Router(config)# **access_list 1 permit 172.30.16.29 0.0.0.0**

можно записать

Router(config)# **access_list 1 permit host 172.30.16.29**

Стандартные списки ACL

Посредством списков управления доступом маршрутизаторы предоставляют простые средства фильтрации потоков данных, например, возможность блокирования Internet»трафика. Список ACL представляет собой упорядоченный набор выражений на основе ключей **permit** (разрешить) и **deny** (заблокировать), которые применяются к адресам протоколов верхних уровней. В текущем разделе подробно рассматриваются стандартные и расширенные списки управления доступом и методы их применения в качестве средства сетевого трафика. В нем также обсуждается вопрос использования списков ACL в качестве механизма обеспечения безопасности в сети.

Стандартный список управления доступом позволяет проверять и сравнивать адреса отправителей пакетов с директивами, как показано на рис. 5.

Стандартные списки управления доступом используются тогда, когда необходимо заблокировать или разрешить доступ всему набору протоколов на основании адреса сети, подсети или узла.

Например, для пакетов, поступивших на интерфейс E0 или Fa0/0, проверяются адреса отправителя и протоколы. Затем они сравниваются с директивами списка управления доступа. Если соответствие найдено, выполняется указанное действие (разрешение или запрет). Если пакеты соответствуют разрешающему правилу (**permit**), они перенаправляются через маршрутизатор к выходному интерфейсу, который логически связан со списком управления доступом. Если же пакеты соответствуют запрещающему правилу (**deny**), они отбрасываются.

Полный синтаксис директивы стандартного списка ACL имеет вид:

Router(config)# **access_list** *access_list_number* {**permit** | **deny** |**remark**} **source** [*source_wildcard*] [**log**]

Ключевое слово **remark** используется для внесения в список комментария, который впоследствии поможет разобраться в списке управления доступом. Длина такой строки-комментария не может превышать ста символов.

Стандартная версия команды **access-list** списка доступа в режиме глобальной конфигурации задает стандартный список управления доступом с номером в диапазоне от 1 до 99. Следует помнить, что даже если пакеты не отвечают ни одному из правил (т.е. записям или директивам) списка доступа, они попадают под неявное правило в конце списка доступа ACL, которое запрещает передачу всех пакетов (это правило не отображается в конфигурации).

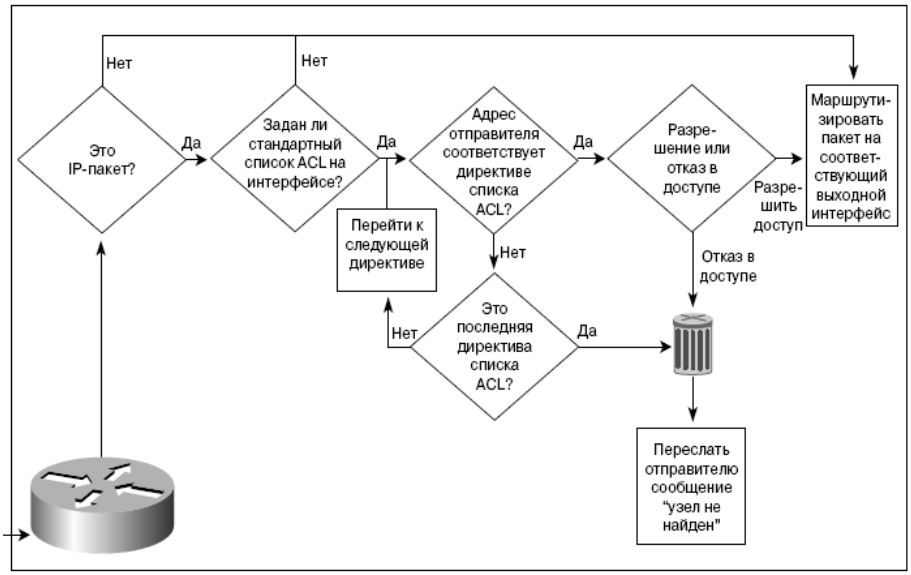


Рис. 5. Принцип работы стандартных списков управления доступом

Команда **ip access-group** используется для привязки созданного списка управления доступом к интерфейсу. Отметим, что для каждого порта, протокола и направления допускается использовать только один список. Команда имеет следующий формат:

Router(config)# **ip access_group** *номер списка* {**in** | **out**}

Расширенные списки управления доступом

Расширенные списки управления доступом (extended access control list — extended ACL) используются чаще, чем стандартные, поскольку они обеспечивают бо́льшие возможности кон-

троля. Расширенный список управления доступом проверяет как адрес отправителя, так и адрес получателя. Список может также проверять конкретные протоколы, номера портов и другие параметры. Процесс обработки трафика маршрутизатором для проверки пакетов на соответствие правилам расширенных списков управления доступом проиллюстрирован на рис. 6.

Отправка пакета может быть разрешена или же может быть отказано в передаче в зависимости от того, откуда был переслан пакет и куда направлен, какой протокол, адрес порта и тип приложения при этом были использованы. Расширенные списки управления доступом, например, позволяют пересылать трафик электронной почты из интерфейса Fa0/0 в интерфейс S0/0 и в то же время могут запрещать передачу файлов и потоки данных от Web-сайтов. Когда маршрутизатор уничтожает пакеты, некоторые протоколы посылают эхо-сообщения отправителю, уведомляющие, что получатель недоступен.

Расширенные списки управления позволяют более точно контролировать и управлять пакетами, нежели стандартные. Стандартные списки управления доступом предназначены для того, чтобы запрещать весь набор или стек протоколов; расширенные списки позволяют точно указать, какой из протоколов необходимо разрешить или запретить. Например, с помощью такого списка ACL можно разрешить трафик HTTP, но запретить доступ к ресурсам по протоколу FTP.

В одном списке управления доступом может быть указано несколько директив.

Каждая из записей списка должна содержать один и тот же *номер* списка доступа, чтобы относиться к одному и тому же списку. В одном списке управления доступом может быть указано столько директив, сколько требуется. Количество директив ограничено только доступной памятью маршрутизатора.

Чем больше записей содержится в каждом списке управления доступом, тем сложнее будет поддерживать и управлять списками ACL в маршрутизаторе.

Расширенные списки управления доступом являются практически универсальным инструментом и, по существу, позволяют использовать практически любые опции и параметры, которые характерны для любого используемого протокола. Порядок следования записей в списке может быть различным и зависит от используемого протокола. Основные применяемые на практике протоколы перечислены ниже.

- Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol - ICMP).
- Межсетевой протокол управления группами (Internet Group Management Protocol - IGMP).
- Протокол управления передачей (Transmission Control Protocol - TCP).
- Протокол пользовательских дейтаграмм (User Data Protocol - UDP).

В коротких разделах ниже описаны вариации расширенных списков управлением доступом в зависимости от используемого протокола.

Использование именованных списков управления доступом

Именованные списки управления доступом позволяют обращаться к стандартным и расширенным спискам управления доступом посредством символьной строки – имени списка. Именованным спискам управления доступом присущи следующие преимущества:

- в символьном имени можно указать краткое интуитивно понятное описание списка;
- исключен лимит в 99 стандартных и 100 расширенных списков управления доступом;

- администратор может изменять списки управления доступом без их удаления и повторного введения.

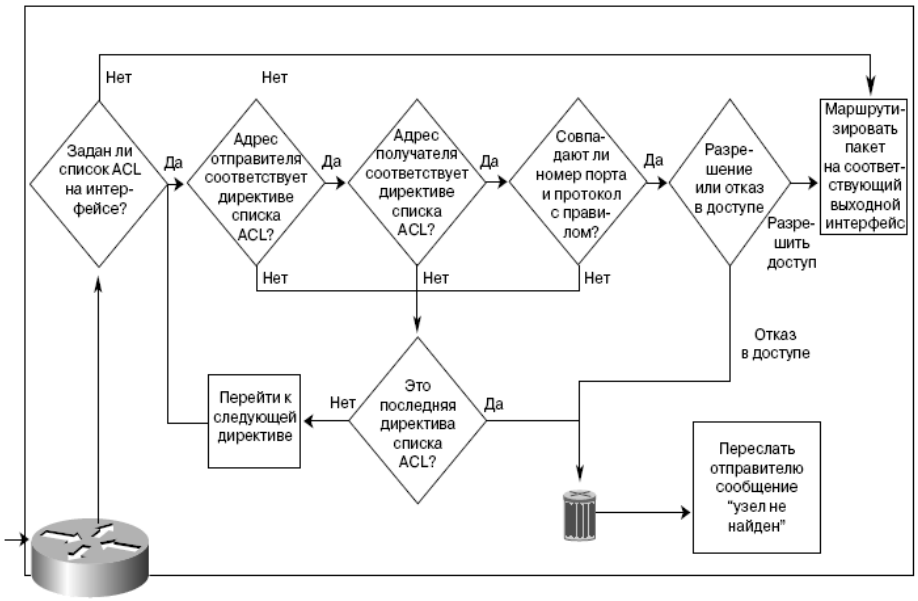


Рис. 6. Принцип работы расширенного списка управления доступом

Именованные списки управления доступом создаются с помощью команды **ip access-list**. Синтаксис именованных списков управления доступом выглядит следующим образом:

ip access_list {**extended** | **standard**} *name*

В режиме конфигурирования списка доступа можно указать одно или несколько условий (так называемых директив) для разрешения или блокирования доступа. При конфигурировании именованного списка доступны следующие опции:

Router(config-std-nacl)#**permit** | **deny** {*source* [*source-wildcard*]| **any** [**log**]

Операнд разрешения или запрета (**permit** или **deny**) указывает маршрутизатору, какие действия следует выполнять, когда пакеты будут проверяться на соответствие другим критериям, указанным в директиве списка управления доступом, т.е. отправить или отбросить пакет.

Контрольные вопросы

1. Сто такое ACL-списки и каково их предназначение?
2. Каков принцип работы ACL-списков?
3. Каким образом конфигурируются ACL-списки?
4. Какие существуют типы списков управления доступом?
5. Каков алгоритм работы ACL-списков?

Лекция 22
Internet. Назначение, протоколы, принципы работы

1. **Общие сведения**
2. **Подключение**
3. **Структура сети Internet**

Ключевые слова: Интернет, HTML, URI, URL, HTTP, CGI, протокол, узел, подключение, коммутация, NAT, PAT.

1. Общие сведения

Интернет - это сеть, состоящая из равноправных и независимых узлов, объединённых между собой каналами связи.

Internet берет свое начало с 1969 года с создания системы ARPANet (сеть передовых исследовательских проектов) при министерстве обороны США. В 80-ые годы Национальный научный фонд США основал сеть (NFSNet), которая была разработана для того, чтобы обеспечить доступ к нескольким суперкомпьютерам для своих главных пользователей, и в 1988 года она заменила сеть ARPANet, став общенациональной сетью на всей территории США.

В марте 1989 года Тим Бернерс-Ли предложил руководству исследовательского центра CERN концепцию новой распределенной информационной системы, которую он назвал WorldWideWeb.

Проект был успешно реализован, в частности, к 1991 году был создан первый браузер (программа просмотра гипертекста), получивший название «www» и работавший в режиме командной строки. С этого момента основными элементами технологии WWW являются:

- язык гипертекстовой разметки документов HTML;
- универсальный способ адресации ресурсов в сети (URI и URL);
- протокол обмена гипертекстовой информацией HTTP;
- универсальный интерфейс шлюзов CGI, добавленный позже сотрудниками Национального Центра Суперкомпьютерных приложений (NSCA).

Чтобы получить файл из Internet, браузер (browser, программа для просмотра Web, клиент) должен знать, где находится файл и как общаться с компьютером, на котором этот файл находится. Поэтому требуется, чтобы программа-клиент WWW передала имя определенного файла, его местоположение в Internet (адрес хоста) и метод доступа (обычно протокол типа HTTP или FTP). Комбинация этих элементов формирует универсальный идентификатор ресурса (Universal Resource Identifier, URI). URI определяет способ записи адресов различных информационных ресурсов. В основу URI были заложены идеи расширяемости, полноты и читаемости. Реализация URI для WWW называется URL (Universal Resource Locator).

Общий формат ссылки URL:

протокол://узел/путь/файл[#метка]

- ***протокол (или метод доступа)*** определяет способ взаимодействия с информационным ресурсом;

- ***узел*** - любое вычислительное устройство (иногда свой собственный IP-адрес имеет даже принтер), включённое в сеть и имеющее свой уникальный IP-адрес;
- ***путь*** - имя каталога (возможно виртуального) или цепочки вложенных каталогов Web-сервера или файловой системы;
- ***файл*** - простое имя файла с расширением, содержащее гипертекст, графический образ, прикладную программу или другую информацию;
- ***метка***- имя закладки в гипертекстовом файле, позволяет осуществлять внутренние переходы к разным фрагментам одного документа.

2. Подключение

Как уже говорилось выше, в качестве каналов для подключения к Интернету могут использоваться обычные и оптоволоконные кабели, радиоканалы и каналы спутниковой связи.

При модемном соединении с INTERNET - провайдером (так называемом Dial-Up соединении) характерна следующая схема работы:

Ваш модем по дозвону устанавливает соединение с модемом провайдера по телефонным линиям. Вначале запрос пересылается непосредственно к серверу провайдера (proxy - серверу). Роль proxy - сервера заключается в пересылке запроса и доставки ответа именно на Ваш компьютер, также он производит соответствие сетевого адреса компьютера его IP-адресу.

От proxy - сервера запрос переходит к следующему серверу и т.д. В среднем пакет совершает от 15 до 25 переходов по пути к адресату. Если запрос доходит до своего места назначения, запрашиваемый сервер посылает ответ, который идет по такой же схеме.

Ответ может содержать код WEB-страницы, рисунки, файлы и т.д. Как видно из приведенного выше, количество переходов, при получении ответа, составляет в среднем 50. По такой же схеме работает и выделенная линия. (рис. 1.)

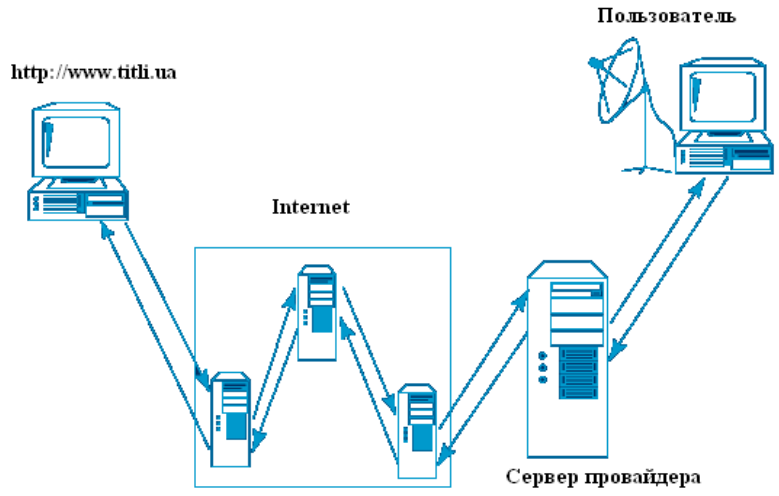


Рис .1. Модемное соединение с INTERNET.

Недостатками такого соединения являются низкая скорость и несовершенство некоторых старых АТС, которые не могут длительное время поддерживать соединение и корректно работать с данными. Иными словами и прием и передача ограничены пропускной способностью Ваших телефонных линий и скоростью канала провайдера. В этом случае соотношение 5%/95% (запрос/ответ) работает по одному и тому же каналу.

Это сказывается не в лучшую сторону при просмотре страниц, насыщенных графикой, переписывании любых архивов и т.д.

При переписывании нескольких файлов из INTERNET общая скорость соединения падает пропорционально количеству переписываемых файлов.Также при организации общего доступа

в INTERNET нескольких компьютеров через одно соединение наблюдается аналогичная картина снижения скорости.

Принцип работы спутникового INTERNET:

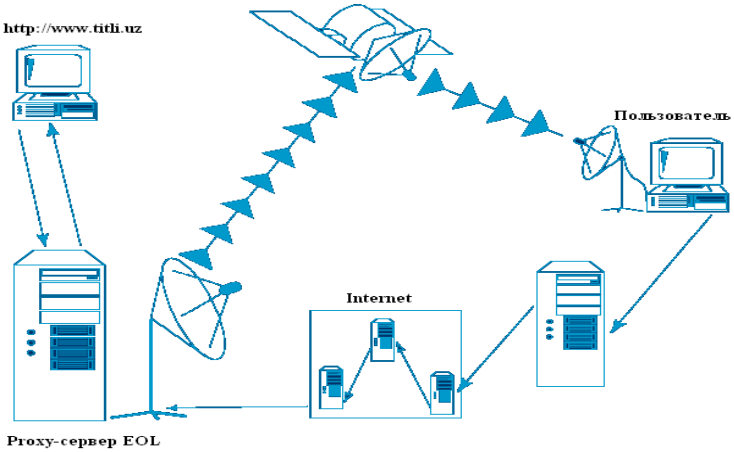


Рис .2. Спутниковое соединение с INTERNET.

Как и в первом случае, запрос направляется через провайдера, но в этом варианте сервер провайдера не является proxy - сервером. Им выступает сервер, способный передавать данные на спутник. Далее при получении ответа, который попадает на сервер, происходит передача данных на спутник. Со спутника данные передаются прямо на Вашу спутниковую антенну. Скорость передачи данных может достигать 2Mbit/c.(рис 2.).

Так же возможно подключение не отдельного компьютера, а всей локальной сети, или ее части. В этом случае модемное соединение или соединение посредством выделенной кабельной системы производится с одним хостом (сервером в локальной сети), на котором устанавливается прокси-сервер. Все пользователи локальной сети в зависимости от настроек установленных системным администратором далее подключаются к этому серверу и получают доступ к сети Интернет.

Структура сети Internet

При всей сложности сети Internet можно выделить несколько базовых идей, на которых построена работа этой глобальной сети. Такая сеть представляет из себя объединение множества сетей и позволяет практически мгновенно обмениваться информацией в глобальных масштабах между любыми пользователями где угодно и когда угодно. На рис. 3 показано, что компьютеры X и Y подключены к такой сети и могут обмениваться информацией, находясь в разных точках земного шара.

Рис. 3. Маршрутизаторы, соединяющие две сети

Одним из недостатков локальных сетей являются ограничения, связанные с их масштабируемостью:

- по количеству рабочих станций;
- по географической протяженности сети.

Выдающийся прогресс был достигнут в вопросе о допустимом количестве узлов, которые эффективно могут быть подключены к иерархической сети благодаря использованию преимуществ таких технологий, как Metro Optical (магистральные оптические сети), Gigabit- и 10-Gigabit-Ethernet. Однако каждая из станций в конечном итоге нуждается в службе глобального взаимодействия или службе распределенной сети, т.е. в технологии коммутации пакетов.

Основой структуры сети Internet является принцип независимости подробностей работы компьютеров и сетей, к которым они подключены, от механизмов доставки сообщений между отдельными сетями.

Одним из подходов к глобальному принципу построения сети Internet являлась идея взаимодействия уровней приложений передающего и принимающего компьютеров, а также всех компьютеров на пути их взаимодействия. Идентичные приложения, работающие на всех компьютерах, могли бы осуществить доставку сообщений в глобальных масштабах. Однако такой подход плохо расширяем. Добавление новых функций в используемые приложения потребовало бы обновления программного обеспечения на всех компьютерах, работающих в сети; новые возможности аппаратных платформ требовали бы изменений в программных приложениях. Сбой в работе одного из компьютеров или выполняемого в нем приложения могут вызвать обрыв цепочки, по которой следует сообщение.

Вместо описанного выше подхода в сети Internet применяется принцип взаимодействия сетевых уровней. Используя в качестве руководства эталонную модель OSI, ставится цель создать сеть, состоящую из независимых модулей. Такой мотив продиктован желанием сохранить разнообразие допустимых технологий локальных сетей на уровнях 1 и 2. В приложениях, функционирующих на уровнях 5, 6 и 7, также используются разнообразные технологии. Необходимо реализовать систему, где подробности организации верхних и нижних уровней будут скрыты от промежуточных сетевых устройств, передающих сетевой трафик, которым нет необходимости заботиться о тонкостях технологий локальных сетей (управляемых локально, так что вся сеть выглядит глобальной) или приложений, инициирующих сетевой обмен.

Перечисленные идеи являются основой концепции *межсетевого взаимодействия* - объединения малых сетей в крупные. Сеть, состоящая из других сетей, называется *internet* (с маленькой буквы). Большая заглавная «I» используется, когда подразумевают сеть, в которой работают службы WWW, - Internet. Межсетевое взаимодействие обязано отвечать следующим требованиям:

- оно должно быть масштабируемым по количеству используемых сетей и подключенных компьютеров;
- должно содержать механизмы транспортировки данных на огромные расстояния, включая всю Землю и околоземное пространство;
- должно быть гибким и обеспечивать использование постоянно развивающихся новых и изменяющихся старых технологий;
- оно должно уметь приспосабливаться к динамическому характеру сети;
- должно быть экономически выгодным;
- обязано быть системой, позволяющей передать данные в любой момент времени, откуда и куда угодно.

На рис. 3 показано соединение двух физических сетей посредством специально предназначенного для этой цели устройства, называемого маршрутизатором. Показанные на рисунке сети называются *непосредственно* -подключенными (directly connected) к маршрутизатору.

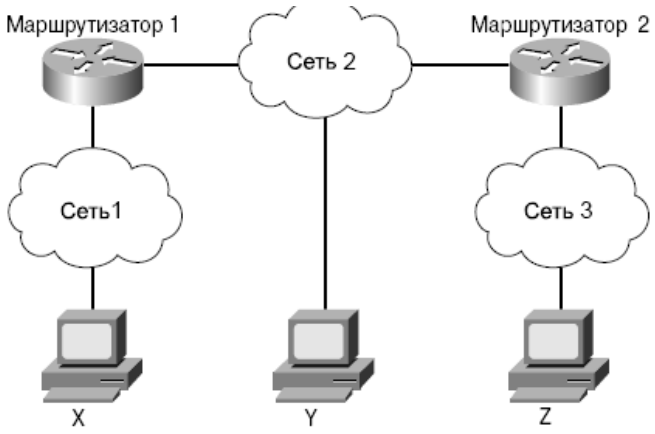


Рис. 4. Локальные и удаленные сети

В этой схеме маршрутизатор выполняет все необходимые преобразования для обмена данными между сетями. Однако, поскольку пользователи всегда и везде нуждаются в соединении с произвольными точками в глобальной сети, такая схема соединения только двух сетей быстро стала неадекватной.

На рис. 4 изображены два маршрутизатора, объединяющие три физические сети.

В такой ситуации маршрутизаторы должны принимать более сложное решение.

Поскольку все пользователи хотят передавать данные друг другу, даже не будучи подключенными напрямую, маршрутизатор должен иметь средства для перенаправления пакетов.

Одним из вариантов решения могло бы быть использование хранящегося у маршрутизатора списка всех компьютеров и путей к ним. Таким образом, маршрутизатор получил бы возможность принимать решения о необходимости пересылки данных, принимая во внимание список всех пользователей и информацию о компьютере-получателе. Однако очень быстро такой подход вызвал бы существенные проблемы по мере роста числа пользователей - он не масштабируем. Что произойдет, если маршрутизатор вместо полного списка будет хранить только список всех сетей, а проблемой локальной доставки предоставит заниматься локальной физической сети? Такое решение лучше и более масштабируемо - пересылка осуществляется на основе информации о сети назначения. В таком случае маршрутизаторы только передают сообщения. В принципе описанная идея может быть распространена и на большое количество маршрутизаторов, если они могут обмениваться необходимой информацией о том, с какими сетями соединены.

На рис. 5 представлен результат использованного расширенного подхода и проиллюстрирована наиболее предпочтительная для потребителей ситуация: осуществляется универсальное межсетевое взаимодействие; информация, которую необходимо знать о конечных пользователях для доставки их данных через сетевую среду, минимальна.

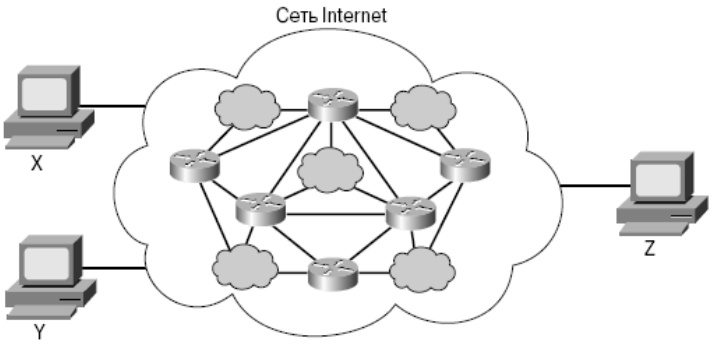


Рис. 5. Физические детали сети скрыты от пользователя

Тем не менее, физическая и логическая иерархия подобной структуры могут быть чрезвычайно сложны.

Таким образом, два компьютера, расположенные в произвольных точках мира, имеющие определенное аппаратное и программное обеспечение, соответствующие спецификациям необходимых протоколов, могут надежно взаимодействовать друг с другом («где угодно/когда угодно/кто угодно»).

4. Способы коммутации LAN и WAN

IP-адрес требуется любому устройству, имеющему соединения с Internet. Количество устройств, которым требуются IP-адреса, быстро увеличивается. Однако количество этих адресов ограниченно. В качестве предлагаемых решений рассматривается трансляция сетевых адресов (network address translation - NAT), трансляция адресов портов (port address translation - NAT).

Основы NAT

Адресация NAT представляет собой менханизм ограничения количесва зарегестрированных IP-адресов в крупных сетях и упращения задачи управления, связанных с IP-адресацией. Преобразование сетевых адресов (NAT) позволяет большой группе частных пользователей подключаться к Интернету через небольшой пул публичных IP-адресов (рис. 6).

Одна из основных причин создания NAT - возможность сэкономить зарегистрированные IP-адреса. Кроме того, NAT обеспечивает безопасность компьютеров, серверов и сетевых устройств, блокируя непосредственный доступ в Интернет с реального IP-адреса узла.

При прохождении пакета через маршрутизатор с функциями NAT, IP-адрес источника, присвоенный в частной внутренней сети, преобразуется в официально зарегистрировнный IP-адрес для того, чтобы его можно было передать по открытой внешней сети, такой как Internet.

Адреса ответных пакетов так же преобразуются в обратном порядке для доставки их конкретному получателю во внутренней сети.

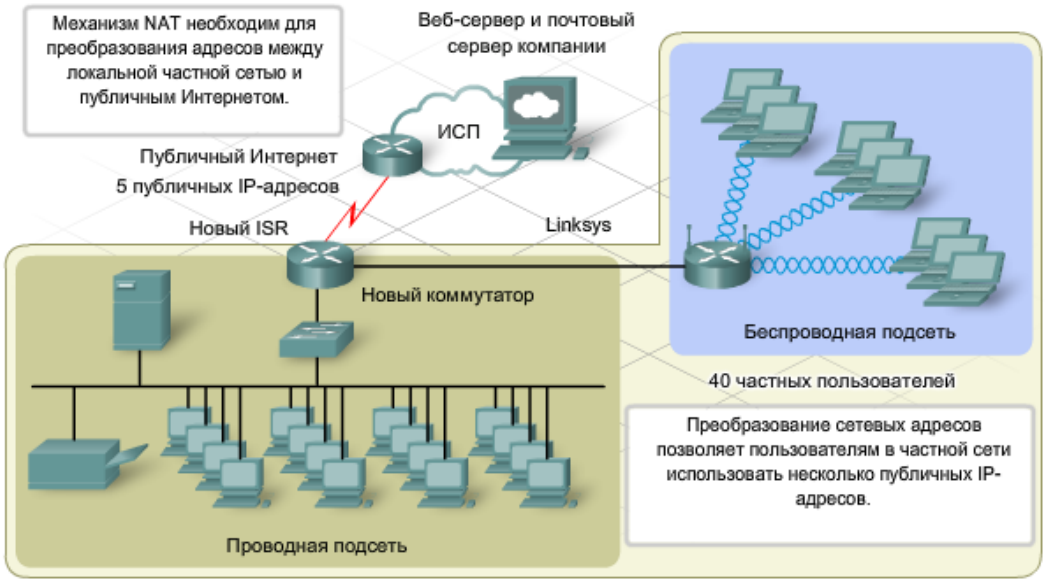


Рис. 6. Преобразование сетевых адресов

Основное преимущество NAT - возможность повторного использования IP-адресов и совместного использования уникальных в глобальном масштабе IP-адресов многочисленными узлами внутри одной ЛВС. Кроме того, NAT обеспечивает прозрачность работы пользователей. Другими словами, для того, чтобы выйти в Интернет из частной сети, им не нужно знать о NAT. Наконец, NAT позволяет заблокировать доступ к частной сети извне.

У NAT есть определенные недостатки, в частности:

Воздействие на определенные приложения, где в информационном наполнении сообщения используются IP-адреса. Такие IP-адреса также нужно преобразовывать, увеличивая нагрузку на процессор маршрутизатора. Дополнительная нагрузка снижает эффективность сети.

NAT прячет частные IP-адреса от общедоступных сетей. Контроль доступа в некоторых случаях желателен, но может оказаться и недостатком в том случае, если нужен удаленный доступ к устройству в частной сети из Интернета.

Преимущества NAT:	Недостатки NAT:
• совместное использование публичных IP-адресов; • прозрачность для конечных пользователей; • повышенная безопасность; • расширяемость или масштабируемость локальной сети; • локальное управление при подключении посредством Интернет-провайдера.	• несовместимость с некоторыми приложениями; • затрудняет удаленный доступ; • снижение производительности по причине увеличения обработки маршрутизатором.

Термины IP NAT

В процессе настройки NAT на маршрутизаторе используется несколько терминов, помогающих интерпретировать процесс реализации NAT.

«Внутренней локальной сетью» называется любая сеть, подключенная к интерфейсу маршрутизатора и входящая в ЛВС с частной адресацией. IP-адреса узлов во внутренних сетях преобразуются до передачи внешним адресатам.

Внешняя глобальная сеть - это любая сеть, подключенная к внешнему по отношению к ЛВС маршрутизатору и не распознающая частные адреса узлов в ЛВС.

Внутренний локальный адрес - это частный IP-адрес узла по внутренней сети. До передачи за пределы структуры адресации локальной сети его нужно преобразовать.

Внутренний глобальный адрес - это IP-адрес внутреннего узла, который используется во внешней сети. Это преобразованный IP-адрес.

Внешний глобальный адрес - это реальный частный IP-адрес внешнего узла. Адрес выделяется из пространства глобально маршрутизируемых адресов или сетевых адресов.

Внешний локальный адрес - это адрес узла назначения пакета, находящегося в локальной сети. Обычно он совпадает с внешним глобальным адресом.

Статическое и динамическое преобразование NAT

Одно из преимуществ использования NAT состоит в том, что отдельные узлы недоступны из Интернета напрямую. А что, если один или несколько узлов сети используют службы, к которым необходимо подключаться через Интернет-устройства, и устройства, находящиеся в локальной частной сети?

Один из способов это сделать - присвоить устройству статическое преобразование адреса. Статические преобразования гарантируют, что частный IP-адрес отдельного узла будет всегда преобразовываться в один и тот же зарегистрированный глобальный адрес. Кроме того, благодаря этому адрес никогда не получит другой локальный узел (рис. 7).

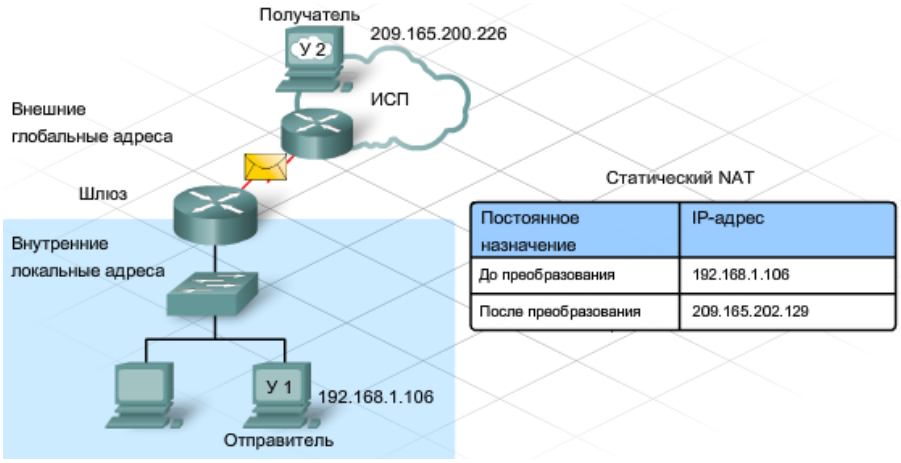


Рис. 7. Статическое преобразование NAT

Динамическое преобразование NAT происходит в том случае, если маршрутизатор присваивает IP-адреса из доступного пула внешних глобальных адресов (рис. 8). Пока сессия открыта, маршрутизатор отслеживает внутренние глобальные адреса и отправляет подтверждения внутренним устройствам. В конце сеанса он просто возвращает внутренний глобальный адрес в пул.

Рис. 8. Динамическое преобразование NAT

Динамическое преобразование NAT позволяет узлам с частными IP-адресами из Интранета подключаться к общедоступной сети, например, сети Интернет. Статическое преобразование сетевых адресов (NAT) позволяет узлам из общедоступной сети подключаться к отдельным узлам из частной сети. Это означает, что при настройке NAT для внешнего доступа следует использовать динамический вариант NAT. Если устройство из внутренней сети должно быть доступно извне, используйте статический вариант NAT.

При необходимости оба метода можно использовать одновременно.

Основы PAT

Если зарегистрированный пул IP-адресов организации очень небольшой или если у нее есть всего один IP-адрес, к общедоступной сети все равно могут одновременно подключаться несколько пользователей, с использованием механизма, который называется перегрузкой NAT или преобразованием адресов портов (PAT) (рис. 9).

PAT преобразует несколько локальных адресов в один глобальный IP-адрес. Когда узел источника отправляет сообщение узлу назначения, он использует сочетание IP-адреса и номера порта и таким образом отслеживает каждый отдельный сеанс связи с адресатом. В режиме PAT шлюз преобразует адрес локального источника и номер порта из пакета в один глобальный IP-адрес и уникальный номер порта выше 1024. Хотя каждый узел получает одинаковый глобальный IP-адрес, номер порта остается уникальным.

Ответный трафик адресуется на преобразованный IP-адрес и номер порта узла. В таблице маршрутизатора находится список внутренних IP-адресов и номеров портов, которые преобразуются во внешние адреса. Ответный трафик направляется на соответствующий внутренний адрес и номер порта. Поскольку в наличии есть более 64 000 портов, маршрутизатору вряд ли не хватит адресов, как это могло бы случиться при динамическом преобразовании NAT.

Рис. 9. Преобразованием адресов портов (PAT)

Преобразование на основе локального адреса и локального порта выполняется отдельно для каждого соединения, при котором генерируется новый порт источника. Преобразование действует только на время соединения, так что после завершения обмена данными пользователь не сохраняет данное сочетание глобального адреса и порта.

Пользователи из внешней сети не смогут установить надежное соединение с узлом сети, где используется PAT. Дело не только в том, что локальный или глобальный номер порта невозможно прогнозировать, но и в том, что шлюз даже не создает преобразование, пока внутренний узел не установит соединение.

Контрольные вопросы

1. Что такое Internet и какова его концепция?
2. Что является основными элементами технологии WWW?
3. Какие существуют способы подключения к Internet?
4. Какова структура Internet?
5. Какими способами осуществляется коммутация LAN и WAN?

Лекция 23
Сервисы Internet

1. **Интернет и стандарты**
2. **Подключение к Интернет**
3. **Иерархия Интернет**
4. **Сервисы Интернет**

Ключевые слова: стандарт, подключение, DSL, модем, спутник, иерархия, сервис, DNS, HTTP, FTP, SMTP, POP3, IMAP4.

1. Интернет и стандарты

Интернет - это общедоступная общемировая сеть сетей. С ее помощью через взаимосвязанные компьютерные сети частные лица и предприятия могут воспользоваться совместным доступом к информации, ресурсам и службам.

Первоначально Интернет предполагалось использовать исключительно для научных, образовательных и военных целей.

В 1991 г. ситуация изменилась. Теперь к Интернету могут подключаться предприятия и частные лица. Интернет быстро разросся и превратился в глобальную сеть. Постоянно возникают новые технологии, упрощающие работу в Интернете и делающие ее более привлекательной. Для пользователей Интернета существуют интерактивные приложения, позволяющие, например, работать с электронной почтой, просматривать веб-страницы, скачивать музыку и видео в потоковом режиме, играть в игры в режиме онлайн и обмениваться мгновенными сообщениями (рис. 1).

Рис. 1. Ресурсы Internet

Такие стандарты разрабатывают, публикуют и обновляют самые разные организации. Благодаря этим организациям, миллионы людей могут подключаться к Интернету с различных устройств, включая персональные компьютеры, мобильные телефоны, карманные компьютеры (КПК) и даже телевизоры.

В процессе непрерывного развития глобальной сети методы взаимодействия между людьми, общего доступа к информации и даже ведения коммерческой деятельности меняются. Например, в Интернете ведется следующая деятельность:

- электронная торговля;
- информационное взаимодействие;
- организация совместной работы и обучение.

Что бы справиться со всеми изменениями и обеспечить бесперебойную работу служб, с учетом того, что количество устройств и технологий с выходом в Интернете постоянно растет была осуществлена стандартизация Интернета.

Стандарт представляет собой набор правил выполнения определенных заданий. Сетевые и Интернет-стандарты гарантируют, что все устройства будут подключаться к сети с использованием одного и того же набора правил. При наличии стандартов устройства различных типов могут обмениваться информацией через Интернет. Например, сообщения электронной почты одинаково форматируются, отправляются и получаются при использовании любых устройств. Отправленное с персонального компьютера письмо можно получить и прочесть с мобильного телефона, если он использует те же стандарты.

2. Подключение к Интернет

Чтобы получить доступ в Интернет, прежде всего, необходимо физическое подключение к Интернет-провайдеру. Поставщики предлагают различные варианты подключения. Для дома и небольших компаний обычно используются следующие методы (технологии) подключения:

Коммутируемый доступ

Коммутируемый доступ - это недорогой вариант подключения с использованием любой телефонной линии и модема (рис. 2). Для подключения к Интернет-провайдеру пользователь вызывает определенный номер телефона. Между оборудованием пользователя и оборудованием доступа в Интернет средствами телефонной сети создается временный канал связи, по характеристикам аналогичный каналу для организации телефонного соединения. Однако, теперь этот канал используется для связи с Интернет. Этот вариант отличает самая низкая скорость подключения, и его обычно используют мобильные сотрудники или пользователи, находящиеся в местах, где нет других возможностей.

Рис. 2. Коммутируемый доступ

DSL

DSL - это более дорогой, но и более быстрый метод. При DSL-подключении также используется обычная телефонная линия. Однако, теперь между оборудованием пользователя и оборудованием доступа в Интернет формируется выделенный информационный канал, не проходящий через коммутаторы телефонной сети (рис. 3). Специальный высокоскоростной модем, разделяет компьютерные данные от сигнала телефона, обеспечивая одновременную работу на телефонной линии компьютера и телефона. Модем предусматривает Ethernet-порт для подключения компьютера и ЛВС.

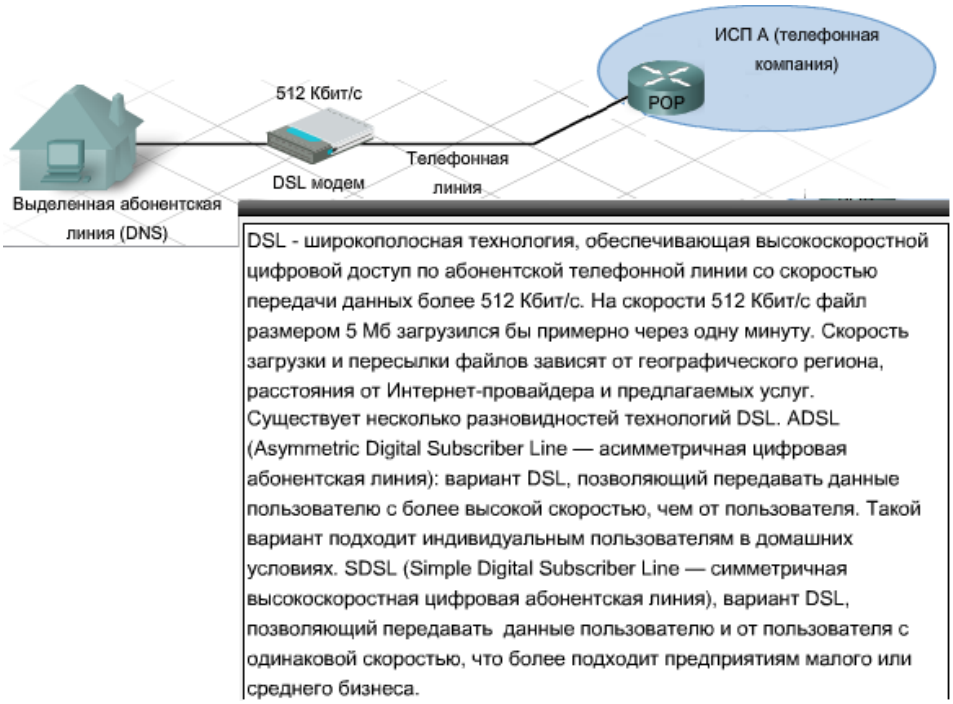


Рис. 3. DSL-подключение

Кабельный модем

Подключение через кабельный модем предоставляют поставщики услуг кабельного телевидения. Сигнал передается в дома и офисы по тому же коаксиальному кабелю, что и телевизионный сигнал. Специальный кабельный модем отделяет сигналы Интернета от других и имеет Ethernet-порт для подключения компьютера или ЛВС (рис. 4).

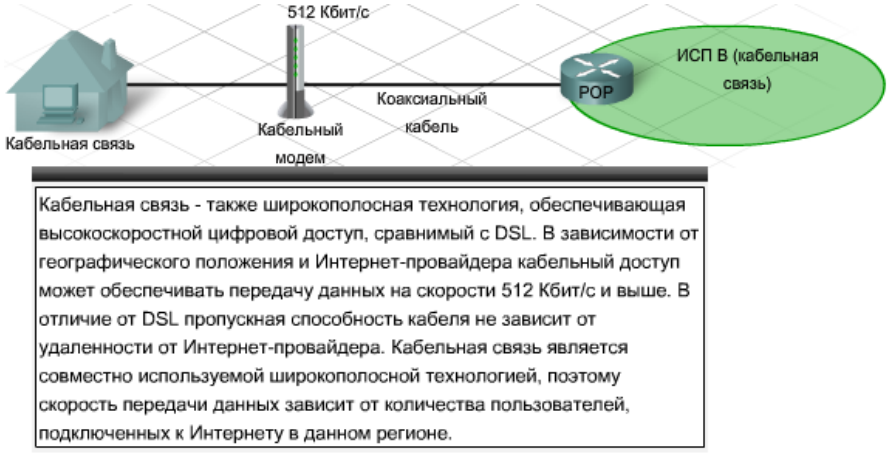


Рис.4. Кабельный модем

Спутник

Спутниковое подключение предоставляет поставщик услуг спутниковой связи. Компьютер пользователя через Ethernet подключается к спутниковому модему, который передает радиосигналы на ближайшую POP со спутниковой связью (рис.5).

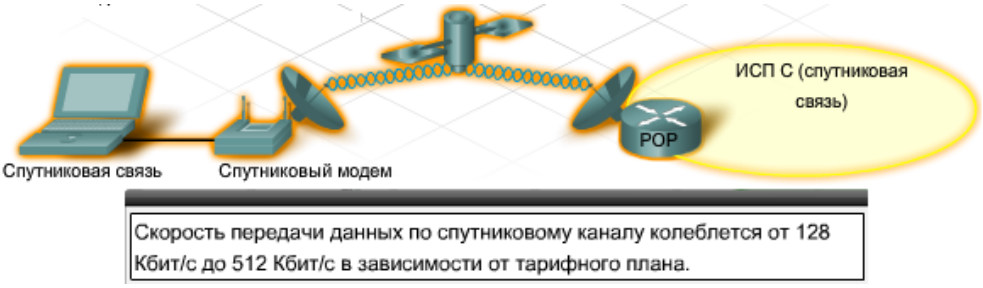


Рис. 5. Спутник

Полоса пропускания измеряется в битах в секунду (бит/с). Большие полосы пропускания измеряются в килобитах в секунду (кбит/с), мегабитах в секунду (Мбит/с) или гигабитах в секунду (Гбит/с).

Существует три основных вида коммерческих подключений с широкой полосой пропускания:

Соединения T1 передают данные со скоростью до 1,544 Мбит/с. T1 - это симметричное соединение (то есть полоса пропускания при загрузке и выгрузке совпадает). Предприятиям среднего размера достаточно одного соединения T1. E1 - это европейский стандарт передачи данных со скоростью 2,048 Мбит/с.

Соединения T3 передают данные со скоростью до 45 Мбит/с. Хотя такие каналы заметно дороже каналов T1, они могут понадобиться крупным предприятиям с многочисленными сотрудниками. Большие компании с несколькими офисами могут параллельно использовать каналы T1 и T3. E3 - это европейский стандарт передачи данных со скоростью 34,368 Мбит/с (рис. 6).

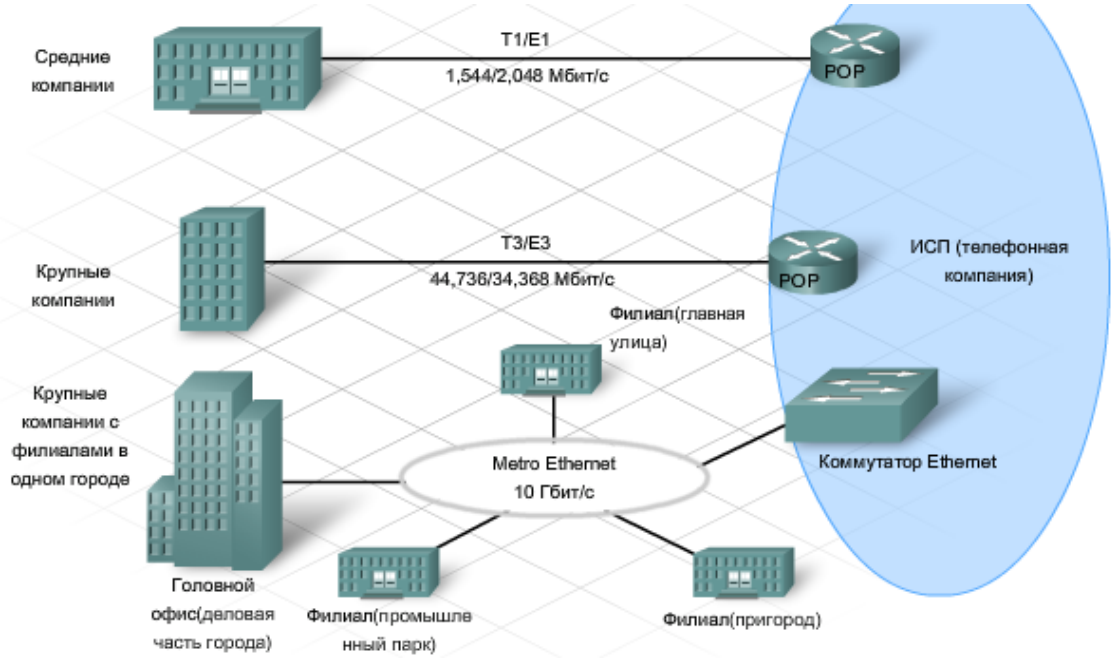


Рис. 6. Основные виды подключений с широкой полосой пропускания

Городская сеть Ethernet предлагает широкий ассортимент высокоскоростных соединений, включая гигабитные каналы. Metro Ethernet используют крупные компании с многочисленными

офисами в одном и том же городе. Metro Ethernet соединяет головной офис со всеми филиалами с использованием коммутируемой технологии. Такое подключение позволяет передавать большие объемы данных. Оно дешевле других высокоскоростных соединений.

Выбрав тип соединения, можно подключиться к Интернет-провайдеру и получить доступ в Интернет. Место, через которое компьютеры и отдельные корпоративные сети подключаются к Интренет-провайдеру, называется точкой присутствия POP. Точки POP расположены на краю сети Интернет-провайдера и обслуживают определенный географический район. Точки присутствия используются для локального подключения и проверки подлинности (пароля) для многочисленных конечных пользователей. У Интернет-провайдера может быть несколько точек присутствия POP, в зависимости от их мощности и размера обслуживаемого провайдером региона.

Внутренняя сеть Интернет-провайдера реализована с помощью высокопроизводительных маршрутизаторов и коммутаторов, соединенных между собой высокоскоростными линиями связи. Внутренняя сеть связывает между собой все точки присутствия провайдера, обеспечивая высокоскоростную и надежную передачу данных между ними. Резервные и дублирующие линии связи обеспечивают обходные и запасные пути передачи данных в случае перегрузки или сбоя канала.

3. Иерархия Интернет

Сеть Интернет имеет иерархическую структуру. На верхнем уровне этой иерархии находятся организации Интернет-провайдеров. Через свои точки присутствия POP Интернет-провайдеры подключаются к узлу обмена (обменнику) Интернет-трафиком, называемую также точкой обмена (IXP). В некоторых странах они называются точками доступа в сеть (NAP). IXP, или NAP, - это место, где соединяются несколько Интернет-провайдеров для получения доступа к сетям друг друга и обмена информацией (рис.7).

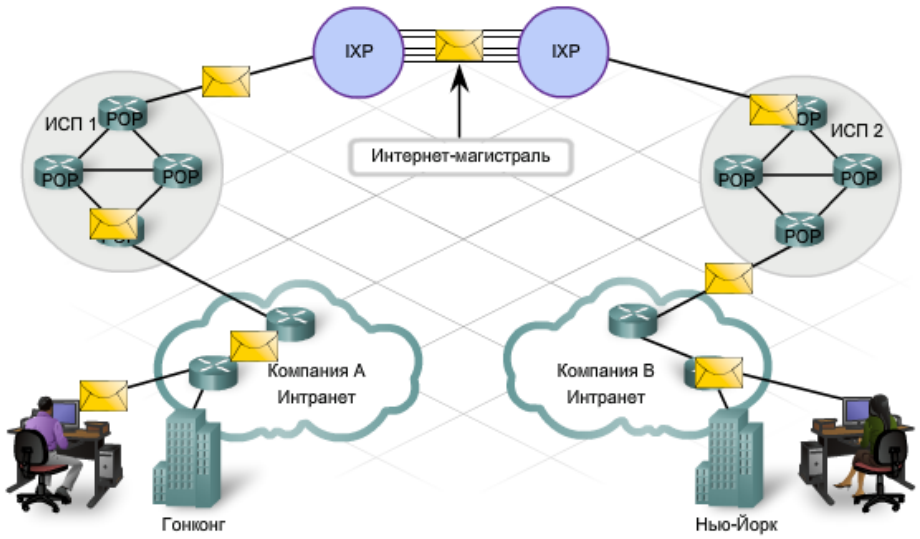


Рис. 7. Отправка сообщения через Интернет

Магистраль Интернета состоит из группы сетей, принадлежащих различным организациям и соединенных друг с другом через точки IXP и частные одноранговые соединения.

Магистраль - это нечто вроде информационного шоссе, состоящее из высокоскоростных каналов, которые соединяют POP и IXP в крупных городах мира (рис. 8).

Элементы магистрали чаще всего соединяются оптоволоконными кабелями. Как правило, кабель прокладывается под землей и соединяет города на континенте. Кабели, соединяющие континенты, проходят по дну моря.

Интернет-провайдеры классифицируются по уровням, в зависимости от метода доступа к магистрали.

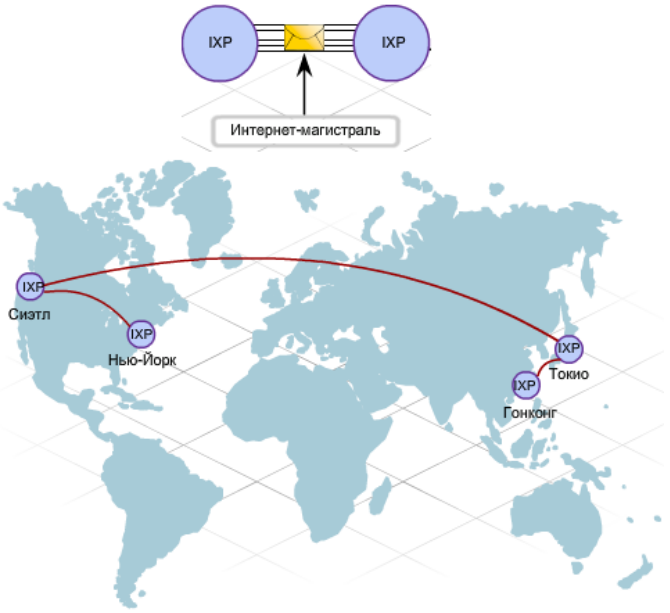


Рис.8. Магистраль Интернета

Интернет-провайдеры уровня 1 представляют собой верхнюю ступень иерархии. Интернет-провайдеры уровня 1 - это огромные организации, непосредственно соединенные друг с другом в режиме частной одноранговой связи. Магистрали их сетей физически соединены друг с другом и образуют глобальную магистраль Интернет. Интернет-провайдеры уровня один владеют внутрисетевыми маршрутизаторами, высокоскоростными каналами данных и другим оборудованием, необходимым для связи с аналогичными Интернет-провайдерами. Им же принадлежат подводные кабели, соединяющие континенты.

Интернет-провайдеры уровня 2 - это следующая ступень с точки зрения доступа к магистрали. Это также очень большие организации, часто работающие в нескольких странах, но у них редко бывают сети, распространенные на весь континент или, хотя бы, межконтинентальные. Чтобы обеспечить своим клиентам доступ в глобальную сеть Интернет, Интернет-провайдеры уровня 2 иногда платят Интернет-провайдерам уровня 1 за передачу трафика в другие части света. Некоторые Интернет-провайдеры уровня 2 обмениваются глобальным трафиком с другими Интернет-провайдерами с использованием более дешевого частного одноранговое подключения в точках IXP. Большая точка IXP может связывать сотни Интернет-провайдеров и обеспечивать доступ к многочисленным сетям через общее соединение.

Интернет-провайдеры уровня 3 дальше всего от магистрали. Обычно они работают в крупных городах, предоставляя клиентам локальный доступ в Интернет. Интернет-провайдеры уровня 3 платят Интернет-провайдерам уровней 1 и 2 за доступ в глобальную сеть и пользование Интернет-службами.

4. Сервисы Интернет

После подключения к Интернет-провайдеру (ISP) предприятие или клиент могут выбрать необходимые им сервисы.

Провайдеры работают на нескольких рынках. Частные домашние пользователи составляют потребительский рынок. Крупные транснациональные корпорации составляют Предприятие рынок. Между ними существует несколько более узких рынков, например, малые и средние предприятия или крупные некоммерческие организации. Требования к сервисам на каждом из этих рынков различны.

Растущие ожидания клиентов и обостряющаяся конкурентная борьба побуждают провайдеров предлагать своим клиентам новые сервисы, направленные на увеличение дохода и дифференциацию в конкурентной среде.

Электронная почта, хостинг веб-сайтов, мультимедиа-трансляции, IP-телефония и передача файлов – основные виды сервисов, которые провайдеры могут предоставлять всем клиентам. Эти услуги важны для потребительского рынка провайдера и для предприятий малого и среднего бизнеса, не располагающих штатом квалифицированных специалистов для реализации собственных сервисов.

DNS

Служба доменных имен (DNS) представляет собой систему разрешения имен узлов без недостатков, которые были свойственны файлу HOSTS. DNS имеет иерархическую структуру. Распределенная база данных привязок имен узлов к IP-адресам распространяется по множеству DNS-серверов во всем мире. В этом состоит отличие от файла HOSTS, все привязки в котором редактировались централизованно на одном сервере (рис. 9).

Иерархическая структура DNS строится по именам доменов и подразделяется на небольшие управляемые зоны. У каждого DNS-сервера имеется файл с базой данных для конкретной зоны. Сервер управляет привязкой имен к IP-адресам только в небольшой части общей структуры DNS. Получив запрос на преобразование имени, не относящегося к собственной зоне DNS, DNS-сервер может переслать этот запрос на обработку другому DNS-серверу в соответствующей зоне.

Возможность разнесения функции преобразования имен узлов по нескольким серверам стала залогом чрезвычайно высокой масштабируемости DNS.

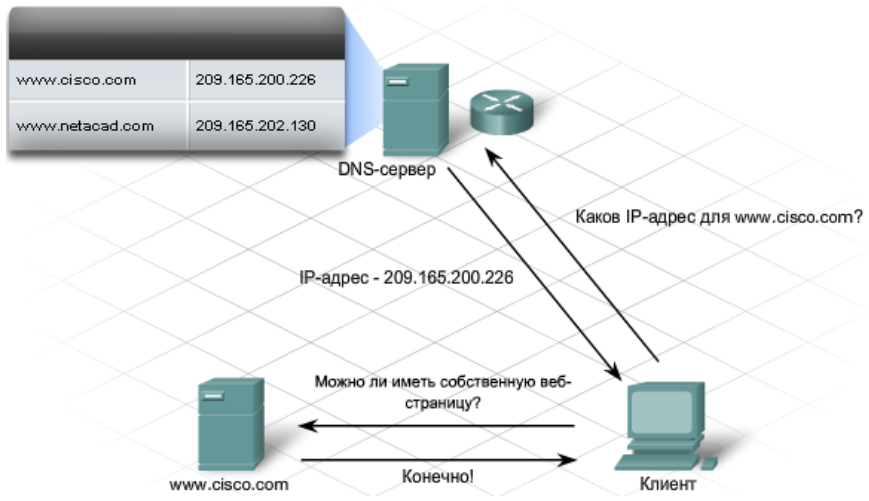


Рис. 9. Структура DNS

Запись ресурса – это запись в файле базы данных зоны DNS. Она идентифицирует тип узла, IP-адрес узла и параметры базы данных DNS. Пространство доменных имен – иерархическая структура именования, используемая при организации записей ресурсов. Пространство доменных имен состоит из различных доменов (групп) и записей ресурсов в каждой группе.

DNS-серверы

Эти серверы отвечают за ведение баз данных, в которых хранятся записи ресурсов и сведения о структуре пространства доменных имен. DNS-серверы начинают обработку запросов клиентов с поиска в пространстве доменных имен и записях ресурсов, хранящихся в файлах базы данных зоны. Если DNS-сервер не находит требуемой информации в базе данных зоны DNS, сервер обращается к дополнительным предопределенным DNS-серверам для обработки запроса преобразования имени в IP-адрес.

Преобразователи

Преобразователь (resolver) – это приложение или функция операционной системы, выполняемая на DNS-клиентах и DNS-серверах. Если в запросе используется доменное имя, преобразователь обращается к DNS-серверу и преобразует это имя в IP-адрес. Преобразователь реализуется на стороне DNS-клиента и служит для создания запроса имени DNS, отсылаемого на DNS-сервер. Преобразователи также размещаются на DNS-серверах. Если DNS-сервер не располагает данными о запрашиваемой привязке имени к IP-адресу, он с помощью преобразователя передает запрос другим DNS-серверам.

В системе DNS используется иерархическая структура преобразования имен. Эта иерархия выглядит как перевернутое дерево с корнем наверху и ветвями, растущими вниз.

Во главе иерархии находятся корневые серверы, которые располагают записями, позволяющими обратиться к серверам доменов верхнего уровня, которые в свою очередь содержат записи, указывающие на серверы вторичных доменов.

Различные домены верхнего уровня представляют либо определенный вид организации, либо страну происхождения. Примеры серверов верхнего уровня:

.au – Австралия

.co - Колумбия

.com – коммерческие и промышленные предприятия

.jp - Япония

.org – некоммерческие организации

Под доменами верхнего и второго уровней имеются домены более низких уровней.

Корневой DNS-сервер может не располагать точным адресом узла H1.cisco.com, но он имеет запись о домене верхнего уровня .com. Аналогично, на серверах домена .com также может отсутствовать запись узла H1.cisco.com, но обязательно будет иметься запись домена cisco.com. DNS-серверы в домене cisco.com имеют запись для узла H1.cisco.com и способны преобразовать адрес.

Именно эта иерархия децентрализованных серверов в системе DNS отвечает за хранение и ведение записей ресурсов. Записи содержат имена доменов, которые может преобразовать сервер, а также ссылки на альтернативные серверы, которые могут также обрабатывать запросы.

Имя H1.cisco.com называется полным доменными именем (FQDN) или DNS-именем, поскольку оно точно характеризует конкретный компьютер в иерархическом пространстве имен DNS.

Преобразование имен в DNS

Если узлу требуется преобразовать имя DNS, он с помощью преобразователя обращается к DNS-серверу в собственном домене. Преобразователю известен IP-адрес DNS-сервера, к которому требуется обратиться – этот адрес был предварительно настроен в составе конфигурации IP узла.

Получив запрос от клиентского преобразователя, DNS-сервер сначала проверяет локальные записи DNS, хранящиеся в его кэше. Если серверу не удается преобразовать имя в IP-адрес локально, сервер с помощью собственного преобразователя пересылает запрос другому DNS-серверу, адрес которого был предварительно настроен. Этот процесс продолжается до тех пор,

пока не будет получен IP-адрес. Результат преобразования имени возвращается исходному DNS-серверу, который использует его для ответа на изначально отправленный запрос.

В процессе преобразования имени DNS каждый DNS-сервера кэширует, или запоминает, получаемые им ответы на запросы. Кэширование информации позволяет DNS-серверу быстрее отвечать на последующие запросы преобразователя, проверяя наличие записей в кэше перед отправкой запросов на другие DNS-серверы.

DNS-серверы кэшируют информацию в течение ограниченного времени. Срок нахождения записей в кэше DNS-сервера должен быть ограничен, поскольку записи имен узлов могут время от времени изменяться. Наличие устаревшей информации в кэше DNS-сервера может привести к тому, что клиентам будут сообщаться неверные IP-адреса компьютеров.

В старых реализациях DNS все записи ресурсов для узлов добавлялись и обновлялись вручную. Однако рост сетей привел к необходимости следить за все большим числом узлов, и ручное управление записями ресурсов перестало быть практичным. Кроме того, при использовании DHCP требуется еще более частое обновление записей ресурсов в зоне DNS. Для упрощения обновления информации о зонах в протокол DNS был добавлен механизм динамического обновления, позволяющий системам обновлять свои записи в зоне DNS (рис. 10).

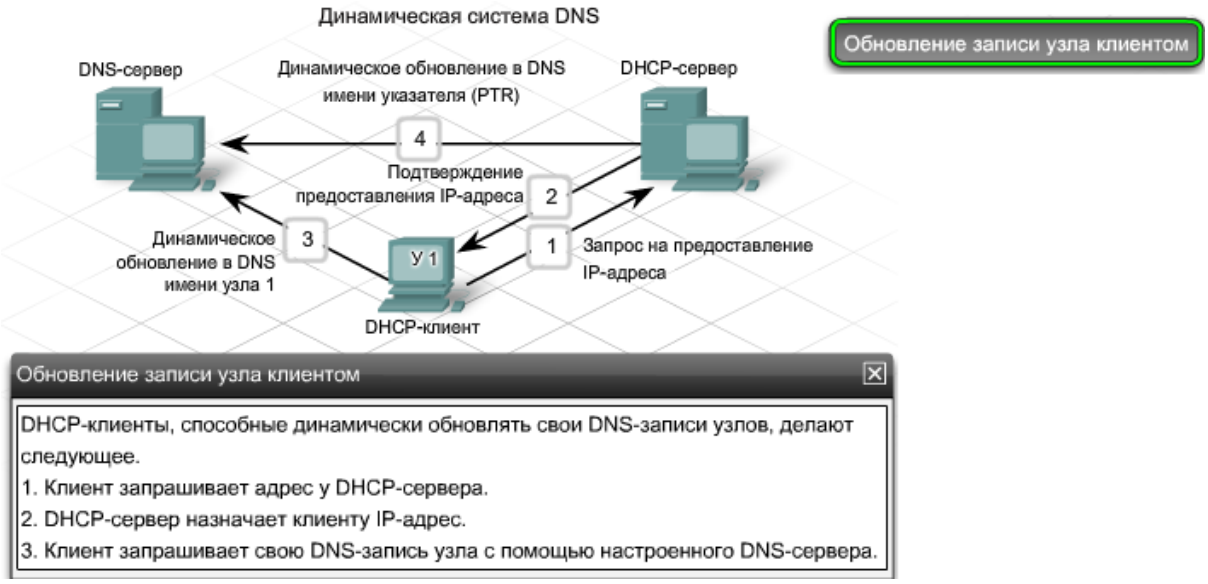


Рис. 10. Динамическая система DNS. Обновление записи узла клиентом

Динамические обновления дают возможность компьютерам DNS-клиентов регистрировать и динамически обновлять свои записи ресурсов на DNS-сервере при каждом изменении. Для использования динамического обновления DNS-сервер и DNS-клиенты (или DHCP-сервер) должны поддерживать функцию динамического обновления. Динамические обновления на DNS-сервере по умолчанию отключены и должны быть включены в явном виде. Поддержка динамических обновлений имеется в текущих версиях операционных систем (рис. 11).

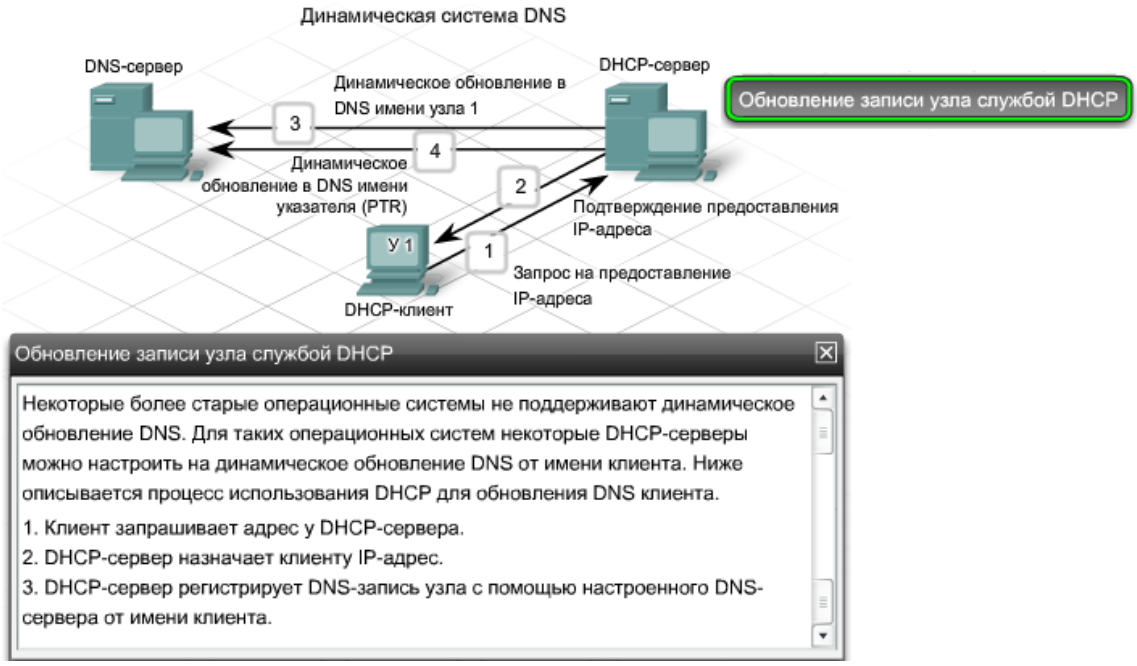


Рис. 11. Динамическая система DNS. Обновление записи узла службой DHCP

Помимо подключения к сети и доступа к службе DNS, предлагаемых всем клиентам, Интернет-провайдеры предлагают ряд дополнительных сервисов, ориентированных на бизнес. Эти сервисы реализуются программным обеспечением, установленным на серверах. В их числе:

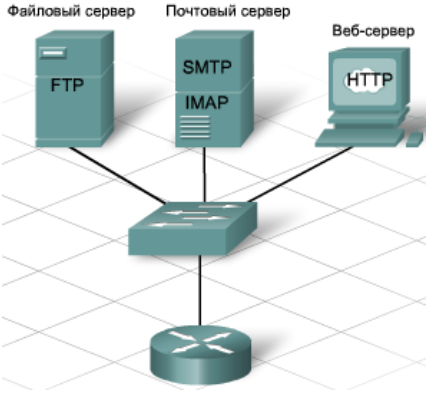


Рис. 12. Сервисы Интернет

- размещение серверов электронной почты;
- размещение веб-сайтов (веб-хостинг);
- организация сайтов для электронной коммерции;
- хранение и передача файлов;
- форумы и веб-журналы;
- потоковая передача аудио- и видеоматериалов.

Такое многообразие сервисов и приложений реализуется провайдерами на основе протоколов TCP/IP прикладного уровня. Наиболее распространенными из протоколов TCP/IP прикладного уровня являются HTTP, FTP, SMTP, POP3 и IMAP4 (рис. 12).

Некоторые клиенты предъявляют повышенные требования к безопасности, и для них разработаны защищенные протоколы прикладного уровня, такие как FTPS и HTTPS.

Контрольные вопросы

1. Какими ресурсами обладает Internet?
2. Какой из способов подключения обладает наилучшими характеристиками?
3. Какими характеристиками обладают виды подключения с широкой полосой пропускания?
4. Какие сервисы являются основными для Internet?
5. Какова иерархия Internet?

Лекция 24
Протоколы Интернет

1. Поддержка протоколов HTTP и HTTPS
2. Службы FTP и TFTP
3. Поддержка SMPT, POP3, IMAP
4. Протокол SNMP

Ключевые слова: Протокол, имя домена, HTTP, HTTPS, FTP, TFTP, электронная почта, SMPT, POP3, IMAP, SNMP.

1. Поддержка протоколов HTTP и HTTPS

Протокол передачи гипертекста (HTTP) входит в состав семейства протоколов TCP/IP. Изначально он был разработан для загрузки веб-страниц с HTML-разметкой. Он используется для распределенной совместной работы с информацией. По мере развития появилось несколько версий протокола HTTP. В отличие от прежних версий, эта версия позволяет организовать несколько сайтов на одном веб-сервере и использовать постоянные соединения для поточной обработки нескольких запросов и откликов.

Протокол HTTP использует схему «запрос-отклик». Протокол HTTP определяет типы сообщений, отправляемых клиентом (обычно – веб-браузером) серверу при запросе веб-страницы. В протоколе также определены типы сообщений с откликом сервера.

Несмотря на примечательную гибкость, протокол HTTP не является защищенным. Сообщения запроса передаются серверу открытым текстом, который может быть перехвачен и прочитан. Отклики от сервера, обычно представляющие собой HTML-страницы, также передаются в незашифрованном виде.

Для защищенного двустороннего обмена данными с веб-серверами в Интернете разработана защищенная модификация протокола HTTP (HTTPS) (рис. 1). HTTPS позволяет использовать аутентификацию и шифрование для защиты данных, пересылаемых между клиентом и сервером. HTTPS определяют дополнительные правила передачи данных между прикладным и транспортным уровнями.

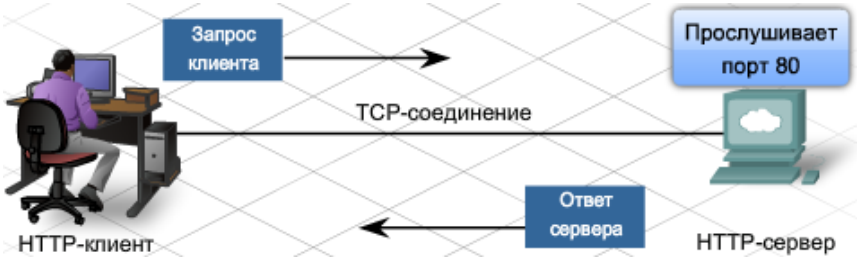


Рис. 1. Обмен данными с веб-серверами в Интернете

При соединении с HTTP-сервером для загрузки веб-страницы местонахождение сервера и конкретного ресурса указывается универсальным идентификатором ресурса (URL) (рис. 2).

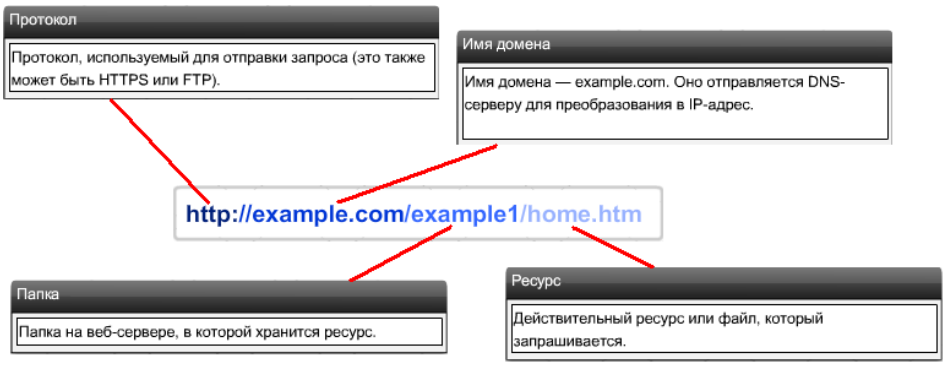


Рис. 2. Структура URL

В URL содержится следующая информация:

- используемый протокол;
- имя домена сервера, к которому производится обращение;
- местонахождение ресурса на сервере, например:

HTTP поддерживает прокси-серверы, позволяющие клиентам устанавливать соединения с другими сетевыми устройствами через посредника. Прокси-сервер – это устройство в цепочке передачи данных, которое выступает сервером по отношению к клиенту и клиентом по отношению к серверу.

Клиент подключается к прокси-серверу и запрашивает у него ресурс, расположенный на другом сервере (рис. 3). Прокси-сервер подключается к указанному серверу и получает у него запрошенный ресурс, который затем возвращает клиенту.

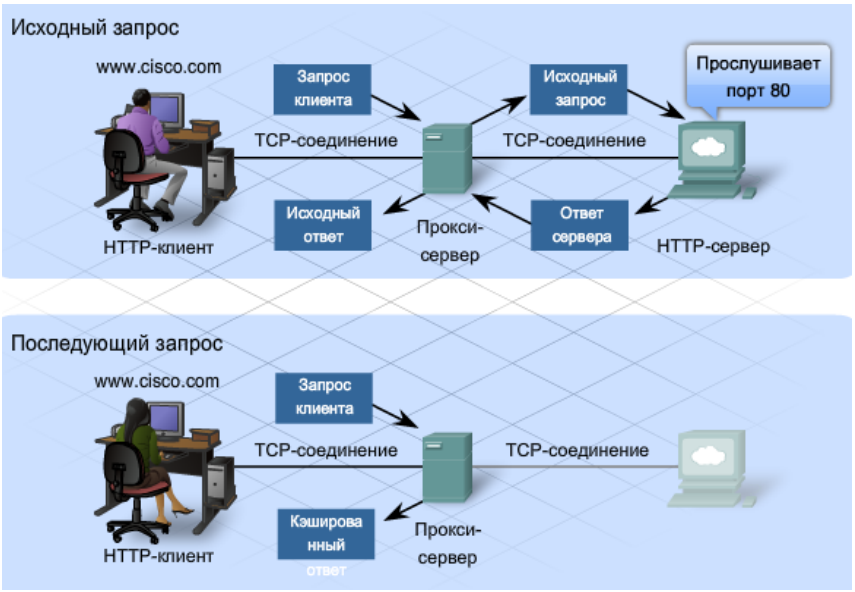


Рис. 3. Типы запросов

Прокси-сервер может кэшировать полученную страницу или ресурс в течение настраиваемого периода времени. Благодаря кэшированию клиенты в дальнейшем смогут быстрее получать доступ к веб-странице, поскольку обращаться к серверу, на котором физически находится страница, не потребуется. Прокси-серверы используются по трем причинам:

Скорость - кэширование позволяет сделать ресурсы, запрошенные одним пользователем, доступными другим пользователям, не обращаясь повторно к серверу, на котором фактически находится страница.

Безопасность - прокси-серверы способны перехватывать компьютерные вирусы и другие вредоносные объекты, не пересылая их клиентам.

Фильтрация - прокси-серверы могут просматривать входящие HTTP-сообщения и фильтровать контент неприемлемого или непристойного содержания.

В HTTP обмен сообщениями между клиентом и сервером осуществляется открытым текстом. Такие текстовые сообщения не защищены от несанкционированного перехвата. Для защиты данных, особенно конфиденциальной информации, многие провайдеры предлагают защищенные веб-сервисы. Защищенные веб-сервисы реализуются провайдерами посредством протокола HTTPS (HTTP с протоколом SSL для шифрования на уровне сокетов). В HTTPS используется тот же процесс «запрос-отклик», что и в HTTP, но поток данных зашифровывается посредством SSL перед передачей по сети.

При поступлении на сервер поток данных HTTP переходит с уровня TCP на прикладной уровень сервера, где он расшифровывается посредством SSL.

При использовании HTTPS сервер способен поддерживать меньшее число одновременных соединений, чем при использовании HTTP. HTTPS создает дополнительную нагрузку и требует более длительной обработки на сервере из-за необходимости шифрования и расшифровки трафика. Чтобы поддерживать производительность сервера на требуемом уровне, протокол HTTPS следует использовать только в случае необходимости, например при обмене конфиденциальной информацией.

2. Службы FTP и TFTP

Протокол FTP (File Transfer Protocol - протокол передачи файлов) был разработан для загрузки файлов (получаемых от узла из сети Internet) или передачи файлов на удаленный компьютер (пересылка информации узлу в сети Internet). Возможность загружать и передавать на удаленный компьютер файлы является одной из самых востребованных функций в Internet. Протокол FTP является идеальным средством для людей, которые используют компьютер для многих целей и которым часто нужно обновлять драйверы и программное обеспечение. Подобно программам для работы с электронной почтой и терминальным соединением telnet, служба FTP является приложением типа «клиент-сервер». Для работы клиентского программного обеспечения требуется наличие запущенного где-либо сервера.

FTP – протокол с установлением соедине-ния, в котором обмен данными между процессами FTP-клиента и сервера осуществляется по TCP-соединению. Реализация FTP предусматривает разделение функций между интер-претатором протокола (PI) и процессом пере-дачи данных (DTP). При передаче файлов PI и DTP существуют парал-лельно как два взаимодействующих процесса.

В результате протокол FTP требует установления двух соединений между клиентом и сервером: одно соединение используется для передачи управляющей информации и команд, а второе – для непосредственной передачи содержимого файлов (рис. 4)

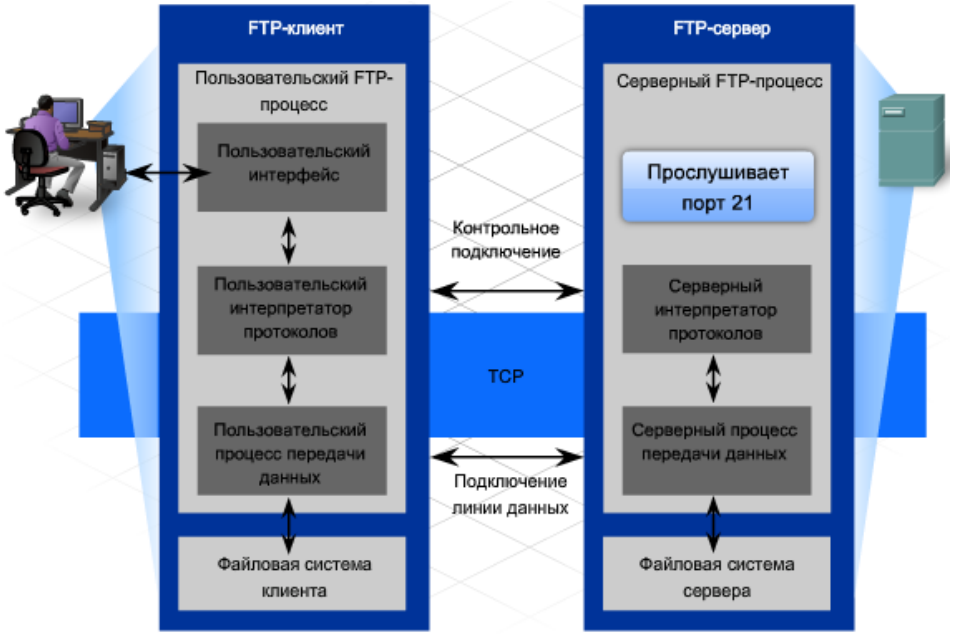


Рис. 4. Структура FTP-запроса

Основным назначением протокола FTP является копирование файлов с одного компьютера на другой или передача файлов от сервера клиенту, а также от клиента серверу. При копировании файлов с сервера устанавливается дополнительное FTP-соединение, или канал связи, посредством которого и передаются данные.

Интерпретатор протокола (PI)

PI играет роль основного управляющего соединения между FTP-клиентом и FTP-сервером. Он устанавливает TCP-соединение и передает управляющую информацию серверу. К управляющей информации относятся команды, используемые, в частности, для перемещения по иерархии каталогов, переименования и переноса файлов. Управляющее соединение, или управляющий поток, остается открытым до закрытия пользователем. При подключении пользователя к FTP-серверу:

1. Пользовательский PI отправляет запрос соединения серверному PI на известном порту 21.
2. Серверный PI возвращает отклик, и соединение считается установленным.
3. После открытия управляющего TCP-соединения серверный PI начинает выполнять последовательность входа в систему.
4. Пользователь вводит реквизиты доступа в пользовательском интерфейсе и проходит аутентификацию.
5. После этого может начинаться процесс передачи данных.

Процесс передачи данных (DTP)

DTP – отдельная функция передачи данных. Эта функция приводится в действие только в том случае, если пользователь в явном виде запрашивает передачу файлов на FTP-сервер или с FTP-сервера. В отличие от соединения PI, которое остается открытым постоянно, соединение DTP автоматически закрывается по завершении передачи файла.

FTP поддерживает установление соединений для передачи данных в двух режимах: активном и пассивном.

Активные соединения для передачи данных

В активном соединении для передачи данных клиент инициирует запрос к серверу и открывает порт для ожидаемых данных (рис. 5). Непосредственный процесс передачи данных начинается после того, как сервер подключится к клиенту на этом порту.

Рис. 5. Активные соединения для передачи данных

Пассивные соединения для передачи данных

В данном случае FTP-сервер открывает произвольный порт источника (с номером выше 1023). Сервер пересылает свой IP-адрес и номер этого произвольного порта FTP-клиенту в управляющем потоке. Затем сервер ожидает подключения к нему FTP-клиента, чтобы начать передачу файла (рис. 6).

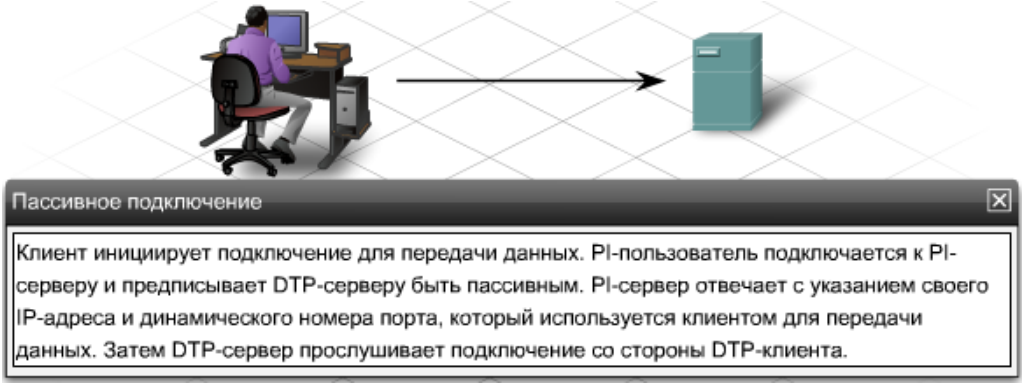


Рис. 6. Пассивные соединения для передачи данных

Провайдеры обычно поддерживают пассивные подключения к своим FTP-серверам. Межсетевые экраны часто не допускают установления активных FTP-соединений с узлами во внутренней сети.

Протокол TFTP (Trivial File Transfer Protocol — простейший протокол передачи файлов) является протоколом без установления соединения, который использует механизм UDP. Служба TFTP используется для передачи конфигурационных файлов и образов операционных систем Cisco IOS в маршрутизаторах и коммутаторах. Протокол разрабатывался маленьким и легким в использовании и установке, поэтому в нем отсутствует большинство функций протокола FTP. Единственное, что может выполнять данный протокол, - это читать и записывать файлы (или электронную почту) с или на удаленный сервер. Протокол TFTP не позволяет просмотреть список каталогов, и в настоящее время в нем не реализована аутентификация пользователей. Однако в некоторых локальных сетях этот протокол широко используется, поскольку он работает быстрее стандартного протокола FTP.

3. Поддержка SMPT, POP3, IMAP

Один из основных сервисов, предлагаемых провайдерами – размещение серверов электронной почты. Электронная почта – это набор средств для доставки, хранения и извлечения электронных сообщений в сети. Сообщения электронной почты хранятся на серверах электронной почты в базах данных. Провайдеры часто устанавливают у себя серверы электронной почты, содержащие учетные записи множества клиентов.

Клиенты электронной почты для отправки и получения сообщений обращаются к серверам электронной почты. Серверы электронной почты взаимодействуют с другими серверами электронной почты для обмена сообщениями между доменами. Другими словами, почтовый клиент не соединяется непосредственно с другим почтовым клиентом для отправки сообщения. Оба клиента должны доверить транспортировку сообщений серверу электронной почты. Это верно даже в том случае, если оба пользователя находятся в одном домене.

Клиенты электронной почты отправляют сообщения на сервер, указанный в настройках приложения. Получив сообщение, сервер проверяет, присутствует ли указанный в нем домен получателя в локальной базе данных сервера. Если домен отсутствует в базе данных, сервер отправляет запрос DNS для определения сервера электронной почты в домене получателя. Как только становится известен IP-адрес сервера электронной почты получателя, сообщение пересылается на соответствующий сервер.

Электронная почта может быть реализована с использованием трех самостоятельных протоколов: SMTP, POP3 и IMAP4. Процесс прикладного уровня, пересылающий сообщения от клиента на сервер или между серверами, реализует протокол SMTP. Клиент извлекает сообщения с сервера с помощью одного из двух протоколов прикладного уровня: POP3 или IMAP (рис. 7).

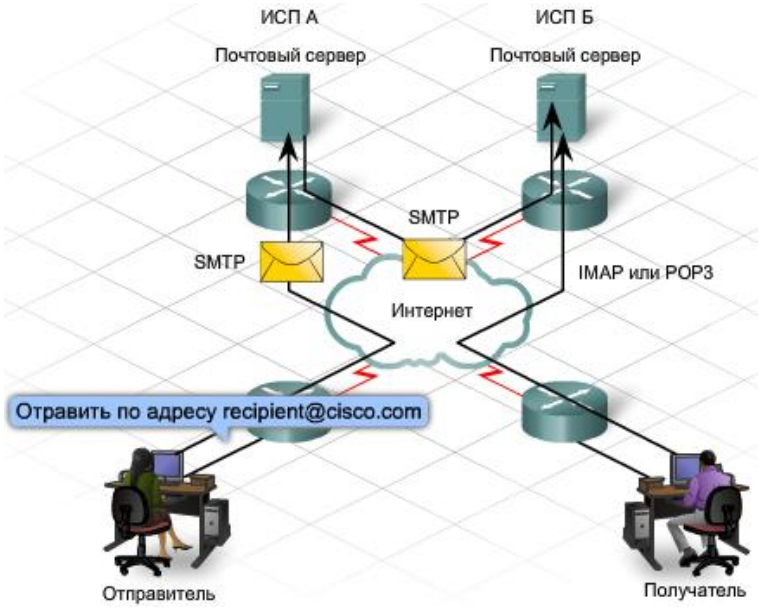


Рис. 7. Протоколы SMPT, POP3, IMAP

Функции, реализуемые упрощенным протоколом передачи электронной почты (SMTP), обеспечивают надежную и эффективную доставку сообщений, но SMTP-приложения требуют выполнения двух условий:

- должны соблюдаться требования к формату сообщения;
- на клиенте и сервере должны функционировать процессы SMTP.

В формате SMTP сообщение состоит из заголовка и тела сообщения.

В то время как тело сообщения может содержать текст произвольной длины, заголовок должен содержать адреса электронной почты получателя и отправителя в правильном формате. Все другие элементы заголовка являются необязательными.

Когда клиент отправляет сообщение по электронной почте, процесс SMTP клиента подключается к процессу SMTP сервера на известном порту 25. Установив соединение, клиент пытается отправить по нему сообщение серверу. Как только сервер получит сообщение, он помещает его в очередь сообщений локальной учетной записи или пересылает другому серверу, выполняя такой же процесс установления SMTP-соединения.

Целевой сервер электронной почты в момент доставки сообщения может оказаться недоступен или перегружен. На этот случай в SMTP предусмотрено временное хранение сообщений с последующей повторной отправкой. Периодически сервер проверяет очередь сообщений и пытается отправить их повторно. Если сообщение не удается доставить в течение установленного времени, оно возвращается отправителю с уведомлением о невозможности доставки.

Одним из обязательных полей в заголовке сообщения является адрес электронной почты получателя. Адрес электронной почты состоит из имени или псевдонима учетной записи, а также имени домена почтового сервера. Пример адреса электронной почты (рис. 8):

Рис. 8. Структура адреса электронной почты

Символ «@» разделяет в адресе имя учетной записи и имя домена сервера.

При отправке сообщения на адрес recipient@cisco.com имя домена отправляется DNS-серверу для получения IP-адреса сервера электронной почты, обслуживающего данный домен. Серверы электронной почты в DNS помечены индикатором записи MX. Получив сообщение, сервер-адресат помещает его в почтовый ящик соответствующего пользователя. Местоположение почтового ящика определяется исходя из учетной записи, указанной в первой части адреса электронной почты.

Протокол работы с почтовым ящиком версии 3 (POP3) позволяет рабочим станциям получать сообщения электронной почты с серверов электронной почты. При использовании POP3 сообщения загружаются клиентом с сервера и удаляются на сервере.

Сетевая служба POP3 на сервере пассивно ожидает запросов подключения клиентов к TCP-порту 110. Для использования этой сетевой службы клиент запрашивает TCP-соединение с сервером. Как только соединение установлено, сервер POP3 посылает приветствие. Затем клиент и сервер POP3 обмениваются командами и откликами, пока подключение не будет закрыто или прервано.

Поскольку сообщения электронной почты загружаются клиентом и удаляются с сервера, это означает, что они не хранятся централизованно. По этой причине протокол POP3 нецелесообразен в решении для малого бизнеса с централизованным резервным копированием.

Протокол POP3 подходит Интернет-провайдерам, поскольку он снимает с провайдера ответственность за хранение большого объема данных на серверах электронной почты (рис. 9).

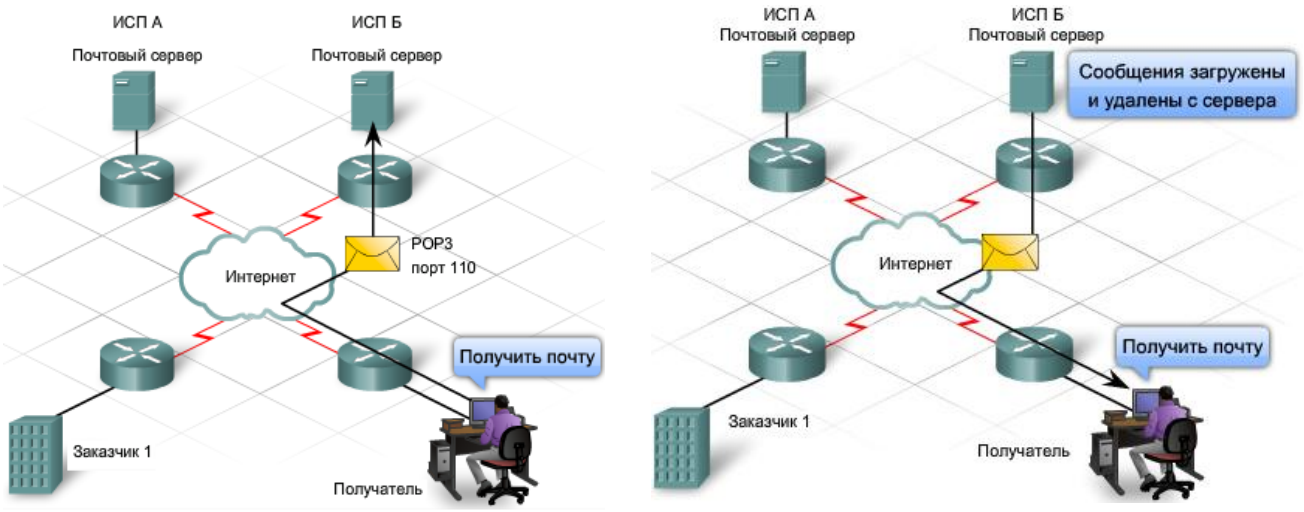


Рис. 9. Работа почтового протокола POP

Протокол доступа к сообщениям в Интернете (IMAP4) предусматривает другой метод извлечения почтовых сообщений с сервера. Его отличие от POP3 состоит в том, что при подключении пользователя к серверу IMAP в клиентское приложение загружаются только копии сообщений. Исходные сообщения остаются на сервере до тех пор, пока они не будут удалены вручную. Пользователи просматривают копии сообщений в клиентах электронной почты.

Пользователи могут организовать на сервере иерархическую файловую структуру для упорядочения и хранения почты. Эта структура также дублируется клиентом электронной почты. Если пользователь решает удалить сообщение, оно синхронно удаляется из клиента и с сервера.

Малым и средним предприятиям протокол IMAP предоставляет множество преимуществ. IMAP обеспечивает долгосрочное хранение почтовых сообщений на серверах электронной почты и их централизованное резервное копирование. Он также позволяет сотрудникам работать с сообщениями из любого места, используя различные устройства и клиентское ПО. Привычная для пользователя структура папок почтового ящика доступна всегда независимо от того, как пользователь обращается к почтовому ящику.

Для Интернет-провайдера протокол IMAP может быть не лучшим выбором. Могут потребоваться существенные затраты на приобретение и обслуживание крупных дисковых хранилищ для большого объема корреспонденции. Кроме того, если клиенты требуют регулярного резервного копирования своих почтовых ящиков, затраты провайдера возрастут еще сильнее (рис. 10).

4. Протокол SNMP

Протокол SNMP (Simple Network Management Protocol - простой протокол управления сетью) является протоколом уровня приложений, который позволяет облегчить обмен управляющей информацией между сетевыми устройствами. Протокол SNMP помогает администраторам сети контролировать ее производительность, отыскивать и устранять проблемы в ее работе и планировать дальнейшее развитие сети.

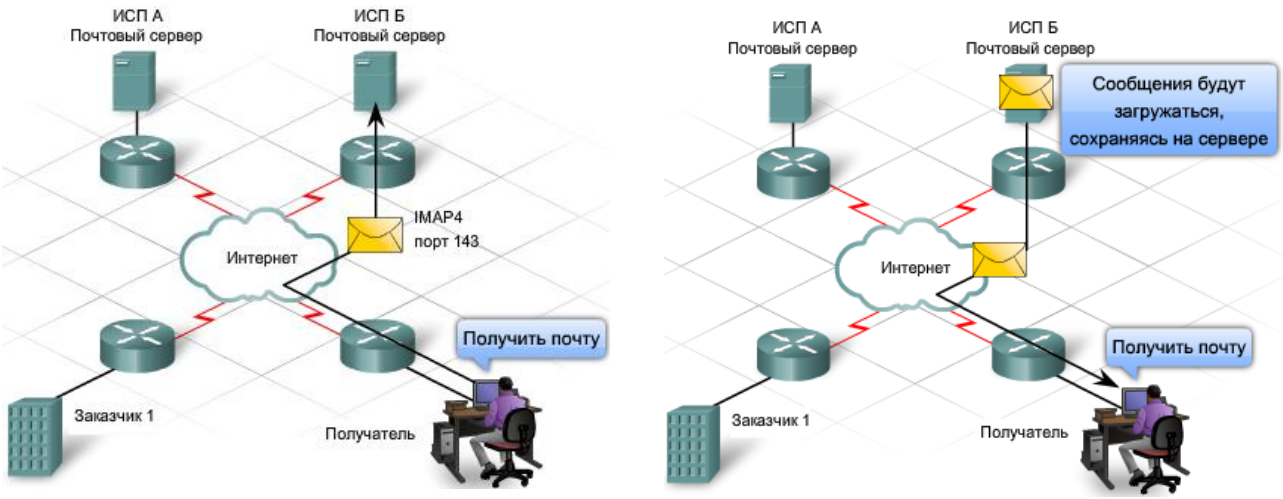


Рис. 10. Работа постового протокола IMAP4

Протокол SNMP состоит из следующих трех компонентов:

- **управляемого устройства** - сетевого узла, на котором установлен агент протокола SNMP и который расположен в управляемой сети. Управляемые устройства собирают и сохраняют информацию об управлении и предоставляют доступ к ней устройствам NMS при помощи протокола SNMP. Иногда управляемое устройство называют сетевым элементом. Сетевым элементом может быть маршрутизатор, сервер доступа, коммутатор, шлюз, компьютер или принтер;
- **агента** - модуля программного обеспечения, который размещен на управляемом устройстве. У агента имеется локальная база информации управления, он производит трансляцию этой информации в форму, совместимую с протоколом SNMP;
- **станции управления сетью (Network Management Station - NMS).** Она выполняет приложения, которые управляют сетевыми устройствами. Система NMS предоставляет процессорные ресурсы и выделяет память, необходимую для сетевого управления. В управляемой сети должны работать несколько систем NMS для повышения отказоустойчивости системы.

Контрольные вопросы

1. Каково назначение протокола HTTP?
2. Какова структура URL запроса?
3. Каково назначение протокола FTP?
4. Что такое электронная почта?
5. На каких протоколах реализована электронная почта?

Лекция 25
Беспроводные сети

1. **Беспроводные технологии и устройства**
2. **Структура и стандарты беспроводных сетей**
3. **Обеспечение безопасности беспроводных локальных сетей**

Ключевые слова: электромагнитные волны, инфракрасный диапазон, радиочастотный диапазон, Bluetooth, роуминг, SSID, WLAN, WPAN, WWAN, Wi-Fi, аутентификация, подключение, шифрование, WPA, VPN, EAP, LEAP.

Когда появились первые компьютеры, они были доступны только для больших корпораций, государственных учреждений и университетов. С того времени технологии ушли далеко вперед, и теперь производительность карманного персонального компьютера ни в чем не уступает первым компьютерам. То же можно сказать и о сетевых технологиях.

Различные типы сетей, требуют наличия физических соединений для их функционирования. Преимуществами таких сетей являются высокая скорость передачи данных, надежность и обеспечение доступа к сети в заранее заданных областях. Физическое соединение позволяет увеличить производительность и обеспечить совместное использование принтеров, серверов и программного обеспечения. Тем не менее, такие сетевые решения требуют от сетевых устройств постоянного местоположения, передвижение устройств разрешено только в пределах установленных кабельных систем и в пределах офиса.

Появление беспроводных технологий связи позволило избежать вышеуказанных ограничений и ощутить компьютерному миру настоящую мобильность. Несмотря на то, что беспроводная связь не обеспечивает высоких скоростей передачи данных, а также безопасности и постоянной доступности, ее гибкость оправдывает ее использование.

Беспроводные сети доступа очень просты в установке. Самая простая беспроводная сеть может быть настроена и запущена уже через несколько минут после включения рабочей станции. Соединение с поставщиком услуг сети Internet осуществляется посредством кабельных соединений, маршрутизатора, модема для кабельных сетей либо модема для выделенных линий, а беспроводная точка доступа выступает в роли концентратора для беспроводных устройств.

1. Беспроводные технологии и устройства

Беспроводные технологии предусматривают передачу информации между устройствами с помощью электромагнитных волн. Электромагнитная волна переносит радиосигналы без проводов.

Некоторые электромагнитные волны неприемлемы для передачи данных. Остальные области этого спектра регламентируются правительствами и предоставляются различным организациям по лицензии для определенных целей. Для общедоступных беспроводных сетей используется инфракрасный спектр и часть радиочастотного (РЧ) диапазона.

Инфракрасный диапазон

Инфракрасное излучение (IR) отличается относительно слабым энергетическим уровнем и не может проникать через стены или прочие препятствия. Тем не менее, оно обычно используется для установления соединений и передачи данных между устройствами, такими как КПК и ПК. Для обмена информацией между устройствами с помощью инфракрасного излучения используется специализированный коммуникационный порт IrDA (Infrared Direct Access). Передача данных по ИК-излучению предусматривает установление соединения только одного типа.

ИК-излучение применяется также в устройствах дистанционного управления, в беспроводных манипуляторах «мышь» и в беспроводных клавиатурах. Оно обеспечивает связь в пределах малой дальности и в пределах видимости. При этом ИК-сигналы могут отражаться от поверхности объектов, что увеличивает радиус действия. Для большего радиуса действия требуются более высокие частоты электромагнитного излучения.

Радиочастотный диапазон (RF)

Радиоволны могут проникать через стены и прочие препятствия, что позволяет добиться большего радиуса действия, чем у ИК-излучения.

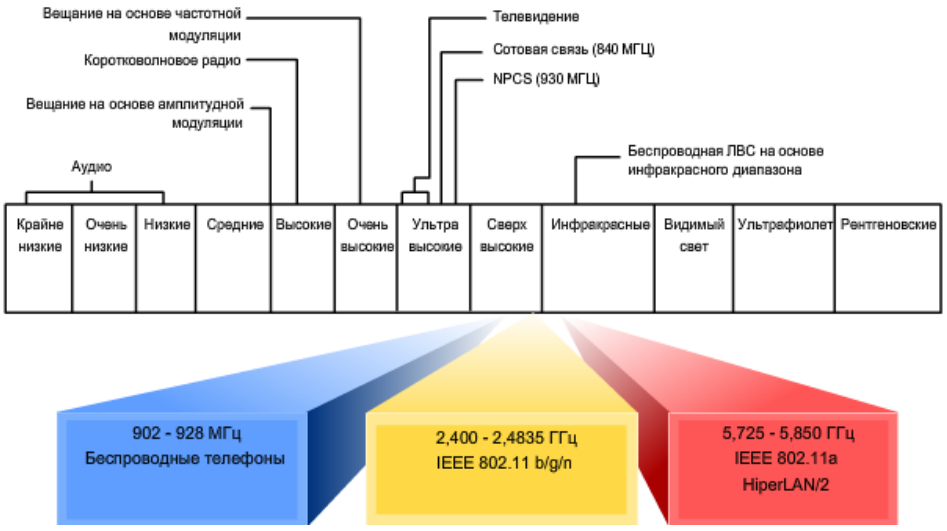


Рис. 1. Частоты и стандарты беспроводных сетей

Некоторые области радиочастотного диапазона зарезервированы для работы таких нелицензируемых систем, как беспроводные локальные сети, беспроводные телефоны и периферийные устройства компьютеров. Это устройства работают в диапазонах частот 900 МГц, 2,4 ГГц и 5 ГГц (рис. 1).

Эти полосы называются ISM-полосами (Indu-strial, Scientific, Medical) и используются с очень незначительными ограничениями.

Технология Bluetooth работает в полосе частот 2,4 ГГц.

Скорость передачи данных и радиус действия этой технологии ограничен, но ее преимущество заключается в том, что она позволяет обмениваться данными между несколькими устройствами одновременно. Благодаря возможности устанавливать связь одного устройства со многими технология Bluetooth более предпочтительна по сравнению с ИК-технологией, так как она позволяет обеспечивать связь с периферийными компьютерными устройствами, такими как мыши, клавиатуры и принтеры.

К числу прочих технологий, использующих полосы частот 2,4 ГГц и 5 ГГц, относятся современные технологии беспроводных локальных сетей, отвечающие требованиям различных стандартов IEEE 802.11. В отличие от технологии Bluetooth их мощность передачи выше и соответственно больше радиус действия.

Устройства и структуры беспроводных сетей

Наименьшее количество устройств, из которых может состоять беспроводная сеть, - это два устройства с беспроводными сетевыми адаптерами. Беспроводные устройства могут быть установлены как в настольные, так и в портативные или карманные компьютеры.

Оборудованные адаптерами беспроводной связи, они создают *сеть сопряженных устройств*, которая очень схожа с одноранговой кабельной сетью. Оба устройства в такой среде работают и как сервер, и как клиент. Несомненно, такая конфигурация позволяет объединить несколько устройств и установить между ними связь, но обеспечивает низкий уровень безопасности, как, впрочем, и малую пропускную способность. Для беспроводных соединений существует проблема совместимости устройств; если приходится использовать сетевые адаптеры различных производителей, то в большинстве случаев они не могут работать друг с другом.

Наиболее часто для доступа отдельных устройств к беспроводной сети в сеть помещают точку доступа (Access Point —AP), которая выступает в роли концентратора для беспроводных устройств. Точка доступа подключена к кабельной сети и предоставляет беспроводным устройствам доступ к остальной сети, обеспечивает подключение к сети Internet. Точка доступа комплектуется антенной, которая предоставляет возможность доступа беспроводным устройствам к сети в некой области (называемой областью покрытия); такая область называется *ячейкой*.

В зависимости от типа помещения, в котором установлена точка доступа, размеры одной ячейки могут колебаться от нескольких десятков метров до десятков километров. В большинстве случаев размер ячейки составляет от 90 до 150 метров. Для создания беспроводной сети в более широких пределах необходимо установить несколько точек доступа с перекрывающимися ячейками, а также разрешить *роуминг (roaming*) между ячейками, как показано на рис. 2.

Перекрытие отдельных ячеек очень важно, т.к. позволяет беспроводному устройству свободно перемещаться без потери соединения в пределах беспроводной локальной компьютерной сети. Рекомендуемый процент перекрытия ячеек должен составлять около 20-30. Такое перекрытие позволяет осуществлять процедуру роуминга, позволяя при этом устройству отсоединяться от одной точки доступа и соединяться со второй без потери соединения с беспроводной сетью.

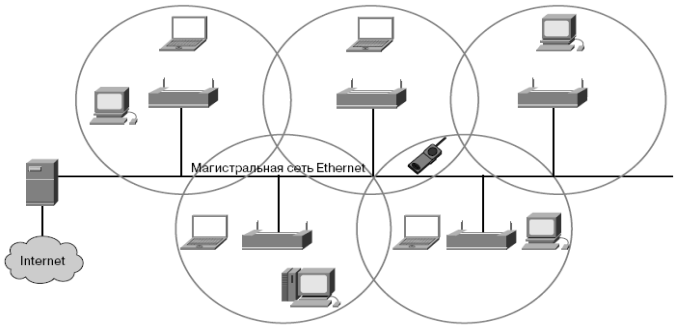


Рис. 2. Роуминг

Если устройство-клиент было включено в пределах беспроводной локальной сети, оно прослушивает эфир для нахождения совместимых устройств, с которыми можно было бы соединиться. Такой процесс называют сканированием. Процесс сканирования может быть как пассивным, так и активным.

В активном режиме сканирования устройство посылает зондирующие запросы, с помощью которых пытается найти совместимое устройство и использовать его для подключения к сети. В зондирующем запросе содержится идентификационный номер набора служб (Service Set Identifier — SSID) для той сети, к которой хочет подключиться устройство. Если была найдена точка доступа с нужным идентификационным номером, она отвечает устройству зондирующим ответом и, соответственно, выполняет этапы аутентификации и подключения устройства к сети.

Устройства, которые находятся в пассивном режиме сканирования, прослушивают эфир и принимают сигнальные фреймы. Источником таких фреймов являются точки доступа и беспроводные станции. Когда устройство получает сигнальный фрейм с необходимым ему идентификатором SSID, оно пытается подсоединиться к беспроводной сети. Процесс пассивного сканирования является непрерывным, устройство может соединяться или разъединяться с точками доступа, в зависимости от изменения уровня их сигналов.

Преимущества и ограничения беспроводной технологии

По сравнению с традиционными проводными сетями беспроводная технология имеет целый ряд преимуществ (рис. 3).

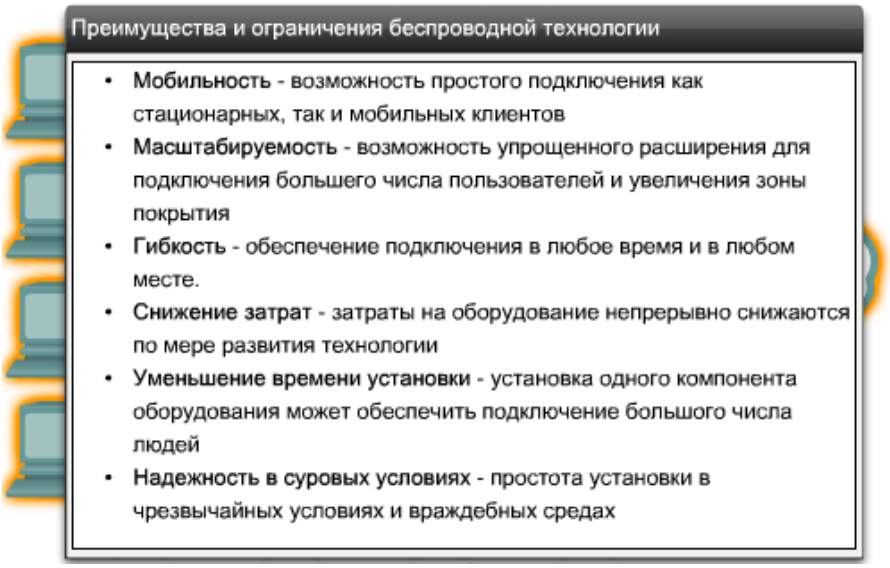


Рис. 3. Преимущества и ограничения беспроводной технологии

Одним из главных преимуществ является возможность установления связи в любое время и из любой точки.

Беспроводная технология довольно проста и недорогая в установке.

Беспроводная технология расширяет границы сетей без ограничений, свойственных кабельным соединениям.

Она позволяет быстро и удобно устанавливать сетевые соединения постоянно растущему числу пользователей.

Несмотря на гибкость и значительные преимущества, для беспроводных сетей свойственны некоторые ограничения и риски.

Во-первых, в технологиях беспроводных локальных сетей (WLAN) используются нелицензируемые области радиочастотного спектра. Поскольку эти области диапазона не регламентируются, в них используется множество различных устройств. Это приводит к переполнению областей спектра и помехам от различных устройств. Кроме того, эти частоты используются многими устройствами, например, микроволновыми печами и беспроводными телефонами, которые могут создавать помехи работе беспроводных локальных сетей.

Другая проблема беспроводной связи - безопасность. Доступ в беспроводные сети открыт. Каждый может получить доступ к данным, передаваемых в сеансе широковещательной рассылки. При этом уровень защиты данных в беспроводной сети также ограничен. Каждый может перехватывать потоки данных даже непреднамеренно. Для обеспечения безопасности данных в беспроводных сетях был разработан ряд методов, таких как шифрование и аутентификация.

Типы беспроводных сетей и их границы

Беспроводные сети делятся на три основные категории: персональные сети (Wireless Personal Area), беспроводные локальные сети (Wireless Local Area, WLAN) и глобальные беспроводные сети (Wireless Wide Area, WWAN) (рис. 4).

Несмотря на эти четкие категории, трудно разграничить рамки реализации беспроводных технологий. Это связано с тем, что в отличие от проводных сетей для беспроводных сетей не требуются четко определенные границы. Диапазон передачи данных в беспроводных сетях может меняться под воздействием различных факторов. Беспроводные сети чувствительны к внешним источникам помех - естественных или искусственных. Перепады температуры и влажности могут значительно влиять на зону покрытия беспроводных сетей. Препятствия в среде беспроводных сетей также влияют на диапазон их действия.

WPAN

Беспроводные сети этого типа применяются для подключения различных периферийных устройств, таких как мыши, клавиатуры и КПК, к компьютеру и имеют наименьший диапазон действия. Все эти устройства подключаются к одному узлу с использованием технологий ИК или Bluetooth.

WLAN

Сети WLAN расширяют границы локальных проводных сетей (LAN). Сети WLAN используют технологию радиочастотного доступа (RF) и соответствуют требованиям стандартов IEEE 802.11. В таких сетях пользователи могут подключаться к проводной сети с помощью устройств, именуемых точками доступа (Access Point, AP). Точка доступа обеспечивает связь между беспроводными узлами и узлами в проводной сети Ethernet.

WWAN

Сети WWAN обеспечивают зону покрытия на очень больших территориях. Наиболее наглядным примером сети WWAN является сеть сотовой связи. В этих сетях используются такие технологии, как многостанционный доступ с кодовым разделением каналов (CDMA) или Глобальная система мобильной связи (GSM), и их деятельность обычно регламентируется правительственными организациями.

	WPAN	WLAN	WWAN
Стандарты	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Скорость	< 3 Мбит/с	1-540 Мбит/с	10-384 кбит/с
Диапазон	Короткие	Средние	Длинные
Приложения	От равноправного устройства к устройству	Домашние сети, сети для малых предприятий и корпоративные сети	Карманные ПК, мобильные телефоны, сотовый доступ

** EDR — Enhanced Data Rate

Скорость и диапазоны постоянно расширяются в результате появления новых технологий.

Рис. 4. Типы беспроводных сетей

2. Структура и стандарты беспроводных сетей

Взаимодействие беспроводных устройств регламентируется целым рядом стандартов. В них указывается спектр радиочастотного диапазона, скорость передачи данных, способ передачи данных и прочая информация. Главным разработчиком технических стандартов беспроводной связи является Институт инженеров по электротехнике и электронике (IEEE), а его стандарты соответствуют нормам, которые установлены федеральной комиссией связи США (FCC).

Стандарт IEEE 802.11 регламентирует работу устройств в сетях WLAN. С учетом различных характеристик беспроводной связи в стандарт IEEE 802.11 были внесены четыре поправки. На сегодняшний день действуют следующие поправки - 802.11a, 802.11b, 802.11g и 802.11n (поправка 802.11n не ратифицирована на момент написания материала). Все эти технологии отнесены к категории Wi-Fi (Wireless Fidelity).

В качестве основной технологии, которая описана в стандарте 802.11, выступает технология DSSS. Беспроводные устройства, работающие на скоростях от 1 до 2 Мбит/с, используют технологию DSSS, которая теоретически может обеспечить максимальную скорость передачи данных вплоть до 11 Мбит/с, но, тем не менее, обычно ее не используют для получения скоростей выше 2 Мбит/с. Следующий (т.е. более новый) стандарт 802.11b позволяет увеличить скорость передачи данных до 11 Мбит/с. Несмотря на то что теоретически технологии DSSS и FHSS могут использоваться в одной беспроводной сети, на практике возникают проблемы совместимости между устройствами различных производителей, поэтому Институт IEEE создал ряд стандартов, отвечающих запросам производителей.

- 802.11a:
- использует полосу частот 5 ГГц;
- не совместим со спектром частот 2,4 ГГц, т.е. с устройствами стандарта 802.11 b/g/n;
- диапазон действия примерно 33% от такового для устройств 802.11 b/g;
- относительно дорогой в реализации по сравнению с другими технологиями;
- оборудование, соответствующее требованиям стандарта 802.11a, встречается все реже.

Организация «Wi-Fi Alliance» отвечает за тестирование устройств для локальных сетей (LAN) от разных производителей. Логотип Wi-Fi на корпусе устройства означает, что это оборудование может взаимодействовать с другими устройствами того же стандарта.

Общие стандарты IEEE WLAN

Стандарт	Дата выпуска	Частота	Скорость передачи данных (макс.)	Максимальный диапазон*
802.11	Июль 1997 г.	2.4 ГГц	2 Мбит/с	не определено
802.11a	Октябрь 1999 г.	5 ГГц	54 Мбит/с	50 м
802.11b	Октябрь 1999 г.	2,4 ГГц	11 Мбит/с	100 м
802.11g	Июнь 2003 г.	2,4 ГГц	54 Мбит/с	100 м
**802.11n	Принятие чернового варианта 1.06 - ноябрь 2006 г. Одобренный черновой вариант 2.0 - март 2007 г.	2,4 ГГц или 5 ГГц	540 Мбит/с	250 м

*Максимальный диапазон - это значение может широко меняться. ~ Стандарт 802.11n остается в черновом варианте, поэтому соответствующие значения могут меняться.

Стандарт IEEE 802.11b носит название Wi-Fi (высокоскоростные беспроводные сети) и описывает взаимодействие устройств с использованием технологии DSSS на скоростях 1, 2, 5,5 и 11 Мбит/с. Все устройства, соответствующие стандарту 802.11b, совместимы с устройствами, отвечающими стандарту 802.11 и использующими систему DSSS. Такая совместимость очень важна, поскольку позволяет модернизировать беспроводную сеть без замены всех сетевых плат и точек доступа. Устройства, соответствующие стандарту 802.11b, позволяют достигать более

высоких скоростей передачи данных благодаря использованию технологии кодирования данных, которая отличается от базового стандарта 802.11, позволяя передавать Устройства, соответствующие стандарту 802.11b, позволяют достигать более высоких скоростей передачи данных благодаря использованию технологии кодирования данных, которая отличается от базового стандарта 802.11, позволяя передавать.

Компоненты беспроводных локальных сетей (Wireless LAN)

После выбора стандарта необходимо убедиться в том, что все компоненты в сети WLAN отвечают его требованиям или, по крайней мере, совместимы с ним. В сети WLAN должно быть несколько обязательных компонентов: беспроводной клиент или STA, точка доступа (рис. 5), беспроводной мост (рис. 6.) и антенна (рис. 7).

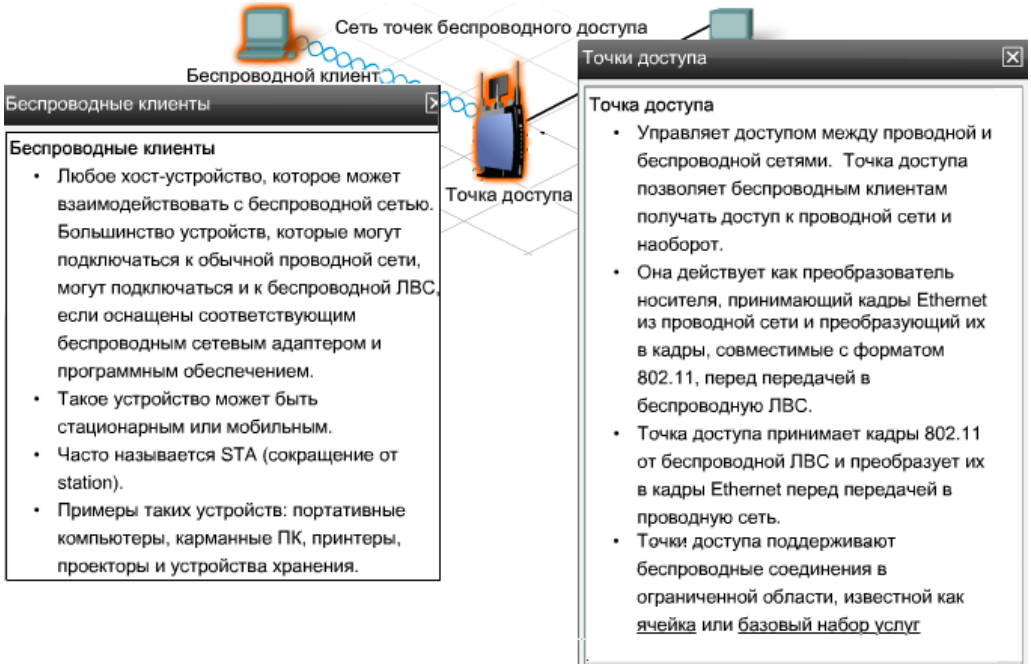


Рис. 5. Беспроводной клиени и точка доступа

Рис. 6. Беспроводной мост

Антенны:

- используются в точках доступа и в беспроводных мостах;
- повышает мощность выходного сигнала с беспроводного устройства;
- принимает сигналы с других устройств, например, STA;

- увеличение мощности сигнала с антенны называется усилением;
- более высокий уровень усиления сигнал позволяет добиться большего расстояния передачи.

Антенны классифицируются по способу излучения сигнала. Направленные антенны концентрируют мощность сигнала в одном направлении. Всенаправленные антенны излучают сигнал во всех направлениях с равной интенсивностью.

Рис. 7. Антенна

Концентрируя сигнал в одном направлении, направленные антенны могут передавать сигналы на большие расстояния. Направленные антенны обычно используются для объединения систем, а всенаправленные антенны используются в точках доступа.

Сети WLAN и имена SSID

При построении беспроводной сети важно, чтобы беспроводные компоненты были подключены к соответствующей сети WLAN. Для этого используется идентификатор набора услуг (SSID).

SSID – это имя беспроводной сети, представляющее собой буквенно-цифровую строку, чувствительную к регистру, имеющее длину до 32 символов. Этот идентификатор пересылается в заголовке всех кадров, передаваемых по сети WLAN. Идентификатор SSID сообщает беспроводным устройствам, к какой беспроводной сети WLAN они принадлежат и с какими устройствами они взаимодействуют.

Для обеспечения связи все беспроводные устройства в сети WLAN должны иметь общий идентификатор SSID, независимо от типа установки сети WLAN.

Применяются два основных вида установки сетей WLAN: специальный (ad-hoc) и инфраструктурный режимы.

Рис. 8 Независимый базовый набор услуг (IBSS)

Специальный режим (Ad-hoc)

Простейшая беспроводная сеть создается посредством объединения двух или более беспроводных клиентов в одноранговой сети. Беспроводная сеть, построенная таким образом, называется специализированной сетью и в ней нет ни одной точки доступа. Все клиенты внутри специализированной сети равноправны. Зона покрытия этой сети называется независимым базовым набором услуг (IBSS) (рис. 8). Простая специализированная сеть может использоваться для обмена файлами и информацией между устройствами без дополнительных затрат и необходимости покупки и настройки точки доступа.

Инфраструктурный режим

Хотя для малых сетей более предпочтительными являются специализированные конфигурации, в сетях более высокого уровня необходимо использовать единое устройство, управляющее взаимодействием в беспроводной соте. Если в сети имеется точка доступа, то она берет эти функции на себя: определяет, какие узлы и в какое время могут устанавливать связь. Такой ре-

жим называется инфраструктурным режимом беспроводной связи; чаще всего они используется в домашних условиях и в условиях бизнеса. При такой форме организации беспроводных локальных сетей WLAN отдельные STA-устройства не могут взаимодействовать между собой напрямую. Чтобы эти устройства могли взаимодействовать между собой, им необходимо разрешение от точки доступа. Точка доступа управляет всеми взаимодействиями и обеспечивает равный доступ в среду всем STA-устройствам. Зона покрытия одной точки доступа называется базовым набором услуг (BSS) или сотой.

Базовый набор услуг (BSS) (рис. 9) – это наименьший строительный блок сети WLAN. Точка доступа имеет ограниченную зону покрытия. Для расширения зоны покрытия можно объединить несколько базовых наборов услуг через систему распределения (DS). Таким образом создается расширенный набор услуг (ESS). В ESS используется несколько точек доступа. Каждая точка доступа представляет собой отдельный базовый набор услуг.

Рис. 9. Вазовый набор услуг (BSS)

Чтобы обеспечить обмен данными между сотами без потерь сигналов, базовые наборы услуг должны пересекаться между собой примерно на 10%. Это позволяет клиенту подключаться ко второй точке доступа перед тем, как отключиться от первой точки доступа.

В большинстве домашних и коммерческих сетей имеется только один базовый набор услуг. Тем не менее, при необходимости увеличения зоны покрытия и числа узлов может потребоваться создать расширенный набор услуг.

Взаимодействие в беспроводной сети

После установления соединения устройства с беспроводной сетью дальнейшее взаимодействие осуществляется посредством фреймов, которые идентичны фреймам сетей стандарта 802.2. Беспроводные локальные сети не используют фреймы стандарта 802.3, поэтому термин *беспроводная сеть Ethernet* не совсем корректен.

В беспроводных локальных сетях существуют три типа фреймов: контрольные, управляющие и фреймы данных. Ниже приведен список фреймов, относящихся к каждому из указанных типов.

Управляющие фреймы:

- фрейм запроса на соединение;
- фрейм-ответ на запрос об установлении соединения;
- фрейм зондирующего запроса;
- фрейм зондирующего ответа;
- сигнальный фрейм;
- фрейм аутентификации.

Контрольные фреймы:

- готовность к передаче (Request To Send - RTS);
- готовность к приему (Clear To Send - CTS);
- подтверждение (Acknowledgement).

Фреймы данных.

Только фреймы данных схожи с фреймами стандарта 802.3. Размер поля данных спецификации 802.3 ограничен 1500 байтами, поэтому общий размер фрейма не может превышать 1518 байтов. В то же время размеры фрейма в беспроводных сетях могут достигать 2346 байтов, но обычно модули передачи данных беспроводных локальных сетей не превышают 1518 байтов по той причине, что точки доступа соединяются с проводной сетью стандарта Ethernet.

Исходя из того, что связь на основе радиоволн осуществляется с использованием общей среды передачи данных, в беспроводных локальных сетях могут возникать коллизии, так же, как и в кабельной сети с общим доступом к среде передачи данных. Из-за такой ситуации в беспроводных сетях используется множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA). Этот тип доступа к среде передачи данных немного похож на множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection — CSMA/CD), который используется в технологии Ethernet.

Если одно из устройств передает фрейм, принимающее устройство должно отправить в ответ позитивное подтверждение (acknowledgment — ACK), поэтому эффективная скорость передачи данных в такой сети падает до 50% от номинальной.

Непроизводительные затраты в сумме с затратами на реализацию протокола предотвращения коллизий уменьшают актуальную скорость передачи данных до 5,0-5,5 Мбит/с для беспроводных сетей, соответствующих стандарту 802.11b, с номинальной пропускной способностью 11 МБит/с.

Качество беспроводных сетей данных также зависит от силы сигнала и понижения качества сигнала вследствие его передачи на большие расстояния или из-за наличия помех. Как только сигнал становится слабым либо зашумленным, активируется алгоритм адаптивного выбора скорости передачи данных (Adaptive Rate Selection — ARS), и скорость передачи данных начинает уменьшаться с 11 МБит/с до 5,5 МБит/с, с 5,5 МБит/с до 2 МБит/с, либо с 2 МБит/с до 1 МБит/с.

Беспроводные каналы.

Независимо от того, как взаимодействуют беспроводные клиенты - внутри IBSS, BSS или ESS, – необходимо управлять связью между отправителем и получателем. Одним из средств управления связью являются каналы.

Каналы создаются посредством деления доступного радиочастотного спектра. Каждый канал может использоваться в качестве несущей для другого сеанса связи. Это можно сравнить с передачей нескольких телевизионных каналов по одному тракту. Несколько точек доступа могут работать в непосредственной близости одна к другой, если они используют разные каналы связи (рис. 10).

К сожалению, частоты, выбранные для некоторых каналов, могут пересекаться с каналами, занятыми другими устройствами. Разные сеансы связи должны использоваться на непересекающихся каналах. Количество и распределение каналов зависит от региона и выбора технологий. Канал для отдельного сеанса связи можно настраивать вручную или автоматически, учитывая его загруженность и пропускную способность.

Обычно для каждого сеанса беспроводной связи выделяется отдельный канал. В некоторых новейших технологиях предусмотрено объединение каналов в единый канал повышенной пропускной способности с более высокой скоростью передачи данных.

Отсутствие четких границ в сети WLAN не позволяет выявлять конфликты в процессе передачи данных. Поэтому необходимо использовать такой метод доступа, который бы гарантировал отсутствие конфликтов.

Для этого в беспроводных технологиях применяется множественный доступ с контролем несущей и предотвращением конфликтов (CSMA/CA).

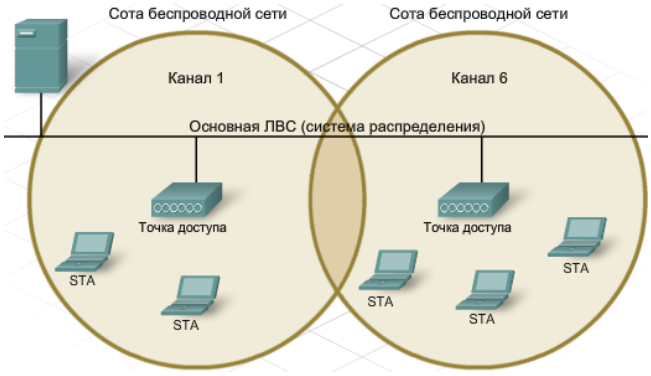


Рис. 10. Беспроводные каналы

CSMA/CA резервирует канал для отдельного сеанса связи. Если канал зарезервирован, никакое другое устройство не сможет передавать по нему данные, что позволит избежать возможных конфликтов.

Как работает процесс резервирования? Если устройству требуется специальный канал связи в базовом наборе услуг, оно обращается к точке доступа за разрешением. Это называется протокол готовности к передаче (RTS). Если канал свободен, точка доступа отправит устройству сообщение о готовности к приему (Clear to Send, CTS), показывающее, что устройству разрешена передача по данному каналу. Сообщение CTS передается всем устройствам в базовом наборе услуг (BSS). Поэтому все устройства в базовом наборе услуг знают, что запрашиваемый канал в данный момент занят.

После завершения сеанса связи устройство, запросившее канал, отправляет в точку доступа еще одно сообщение, именуемое (ACK) (подтверждение). Сообщение ACK сообщает точке доступа, что канал может быть освобожден. Это сообщение также рассылается всем устройствам в сети WLAN. Все устройства в базовом наборе услуг получают сообщение ACK и таким образом извещаются о том, что данный канал снова свободен.

3. Обеспечение безопасности беспроводных локальных сетей

Одним из главных преимуществ беспроводных сетей является удобство в подключении устройств. Но оборотной стороной удобства подключения и возможности передачи информации без проводов является уязвимость вашей сети для перехвата информации и атак со стороны злоумышленников (рис. 11).

Взломщику не требуется физического подключения к вашему компьютеру или к любому другому устройству для получения доступа в вашу сеть. Злоумышленник может настраиваться на сигналы вашей беспроводной сети точно так же как на волну радиостанции.

Взломщик может получить доступ в вашу сеть из любой точки в пределах действия беспроводной связи. Получив доступ к вашей сети, злоумышленники смогут бесплатно воспользоваться вашими Интернет-сервисами, а также получить доступ к компьютерам в сети и повредить файлы, либо украсть персональную или конфиденциальную информацию.

Для защиты от этих уязвимостей беспроводной связи необходимы специальные функции обеспечения безопасности и методы защиты беспроводной локальной сети (WLAN) от внешних атак.

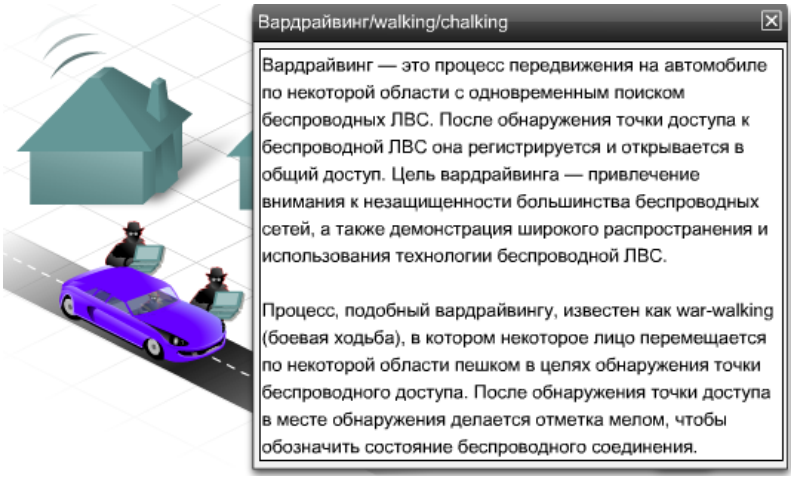


Рис. 11. Вардрайвинг

Для этого достаточно выполнить несколько несложных операций в процессе исходной настройке беспроводного устройства, а также настроить дополнительные параметры обеспечения безопасности.

Один из простейших способов доступа в беспроводную сеть - использовать имя сети или SSID.

Все компьютеры, подключенные к беспроводной сети, должны использовать ее SSID. По умолчанию, беспроводные маршрутизаторы и точки доступа рассылают идентификаторы SSID всем компьютерам в пределах действия беспроводной сети. Если функция рассылки SSID активирована, то любой беспроводной клиент сможет обнаружить сеть и подключиться к ней, если не настроены другие функции обеспечения безопасности.

Функцию рассылки SSID можно отключать. Если она отключена, то сведения о доступности сети уже не являются общедоступными. Любой компьютер, подключаемый в сеть, должен использовать ее SSID.

В качестве дополнительной меры защиты настоятельно рекомендуется изменить настройки, заданные по умолчанию. Беспроводные устройства поставляются с предварительно настроенными SSID, паролями и IP-адресами. Используя настройки по умолчанию, злоумышленник сможет легко идентифицировать сеть и получить доступ.

Даже если отключена рассылка SSID, существует вероятность проникновения в сеть, если злоумышленнику стал известен SSID, заданный по умолчанию (рис. 11). Если не изменить другие настройки по умолчанию, а именно пароли и IP-адреса, то взломщики могут проникнуть в точку доступа и внести изменения в ее конфигурацию. Настройки, заданные по умолчанию, должны быть изменены на более безопасные и уникальные.

Эти изменения сами по себе еще не гарантируют безопасности вашей сети. Например, SSID передаются открытым текстом. Но сегодня имеются устройства для перехвата беспроводных сигналов и чтения сообщений, составленных открытым текстом. Даже если функция рассылки SSID отключена и значения по умолчанию изменены, взломщики могут узнать имя беспроводной сети с помощью таких устройств. Используя эту информацию, они смогут подключиться к сети. Для обеспечения безопасности беспроводной локальной сети (WLAN) следует использовать комбинацию из нескольких методов защиты (рис. 13).

Рис. 12. Назащищенная сеть

Рис. 13. Защещенная сеть

Один из способов ограничения доступа в беспроводную сеть – определить устройствам разный уровень привилегий доступа в сеть. Для этого применяется фильтрация MAC-адресов.

Фильтрация MAC-адресов

Фильтрация MAC-адресов позволяет задать перечень устройств, имеющим разрешение на соединение с беспроводной сетью, с помощью их MAC-адресов. При каждой попытке беспроводного клиента установить соединение или ассоциироваться с точкой доступа он должен передать свой MAC-адрес. Если включена функция фильтрация по MAC-адресам, то беспроводной маршрутизатор или точка доступа выполнит поиск MAC-адреса этого устройства по своему предварительно заданному списку. Разрешение на соединение получат только те устройства, чьи MAC-адреса были заранее прописаны в базе данных маршрутизатора (рис. 14).

Если MAC-адрес не найден в базе данных, устройству будет отказано в установлении соединения или в доступе в беспроводную сеть.

Такой тип обеспечения безопасности имеет некоторые недостатки. Например, он предполагает, что MAC-адреса всех устройств, которым должен быть предоставлен доступ в сеть, включены в базу данных до того, как будет выполнена попытка соединения. Устройство, не распознанное по базе данных, не сможет выполнить соединение. При этом взломщик может создать клон MAC-адреса устройства, имеющего доступ в сеть.

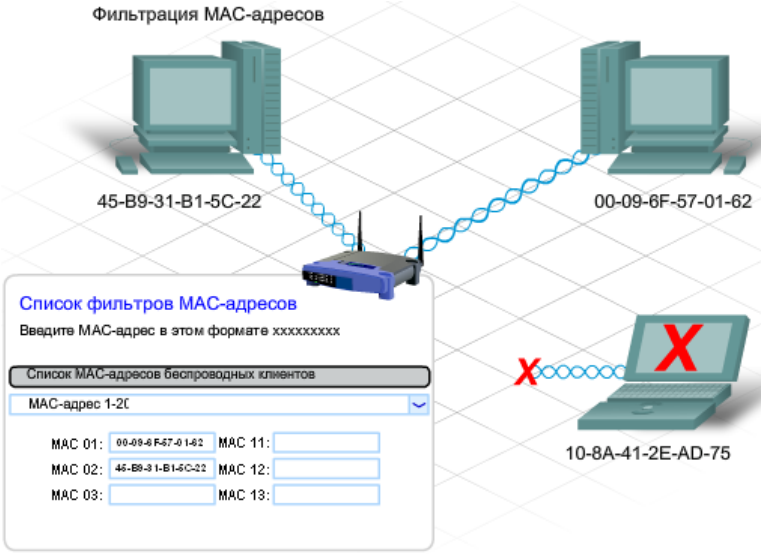


Рис. 14. Обеспечение защиты при помощи фильтнации MAC-адресов

Аутентификация и подключение

Аутентификация в беспроводных локальных сетях осуществляется на втором уровне модели OSI, и этот процесс является процессом аутентификации устройства, а не пользователя. Данный момент - принципиальный вопрос безопасности в беспроводных сетях, необходим для поиска неисправностей и общего обслуживания беспроводных сетей.

Процесс аутентификации беспроводного устройства состоит из обмена фреймами аутентификации между сетевым адаптером и точкой доступа. Клиент посылает точке доступа фрейм запроса на аутентификацию. Точка доступа принимает такой фрейм, обрабатывает его и выносит решение об аутентификации клиента.

Сетевой адаптер будет извещен о вынесенном решении посредством фрейма-ответа. Точка доступа может также быть настроена на выполнение процедуры аутентификации клиентов посредством сервера аутентификации, который может провести расширенную проверку параметров и прав клиентского устройства.

Процесс подключения беспроводного устройства к точке доступа выполняется после прохождения аутентификации. После подключения клиентские устройства могут использовать услуги точки доступа для передачи данных.

Методы аутентификации

В стандарте IEEE 802.11 предусмотрено использование двух методов аутентификации:

аутентификация по методу открытой системы (Open system). В таком процессе аутентификации проверяется только значение SSID. Этот метод может быть использован в средах с безопасным и небезопасным окружением, но несмотря на это, программы захвата и анализа трафика нижних уровней могут получить значение SSID для конкретной беспроводной локальной сети;

По умолчанию для беспроводных устройств аутентификация не требуется. Всем устройствам разрешено устанавливать соединения независимо от их типа и принадлежности. Это называется открытой аутентификацией. Открытая аутентификация должна использоваться только в общедоступных беспроводных сетях, например, в школах и Интернет-кафе (ресторанах). Она может использоваться в сетях, где аутентификация будет выполняться другими средствами после подключения к сети.

аутентификация по методу общего ключа (Shared key). Этот процесс аутентификации требует использования алгоритма криптования WEP (Wired Equivalent Privacy - протокол обеспечения безопасности для беспроводных сетей). Механизм WEP является довольно простым алгоритмом, в котором используются 64- или 128-битовые ключи. Точка доступа настраивается с использованием зашифрованного ключа; любому устройству для подключения к соответствующей беспроводной локальной сети через такую точку доступа необходимо иметь совпадающий ключ. Статически установленные ключи WEP обеспечивают намного более высокий уровень безопасности, чем метод открытой системы, но не могут обеспечить полной защиты от взлома.

Режим предварительных ключей (Pre-shared keys, PSK)

При использовании режима PSK точка доступа и клиент должны использовать общий ключ или кодовое слово (рис. 15). Точка доступа отправляет клиенту случайную строку байтов. Клиент принимает эту строку, шифрует ее (или скремблирует), используя ключ, и отправляет ее обратно в точку доступа. Точка доступа получает зашифрованную строку и для ее расшифровки использует свой ключ. Если расшифрованная строка, принятая от клиента, совпадает с исходной строкой, отправленной клиенту, то клиенту дается разрешение установить соединение.

PSK выполняет односто-роннюю аутентификацию, то есть, точка доступа проверяет подлинность подключаемого узла.

PSK не подразумевает проверки узлом подлинности точки доступа, а также не про-веряет подлинности пользователя, подключа-ющегося к узлу.

Рис. 15. Режим предварительных ключей (Pre-shared keys, PSK)

Расширяемый протокол проверки подлинности (Extensible Authentication Protocol, EAP)

EAP обеспечивает взаимную или двухстороннюю аутентификацию, а также аутентификацию пользователя. Если на стороне клиента установлено программное обеспечение EAP, клиент взаимодействует с внутренним сервером аутентификации, таким как сервер дистанционной аутентификации мобильного пользователя коммутируемой сети (RADIUS) (рис. 16). Этот обслуживающий сервер работает независимо от точки доступа и ведет базу данных пользователей, имеющих разрешение на доступ в сеть. При применении EAP пользователь, а не только узел, должен предъявить имя и пароль, которые затем проверяются по базе данных сервера RADIUS. Если предъявленные учетные данные являются допустимыми, пользователь рассматривается как прошедший проверку подлинности.

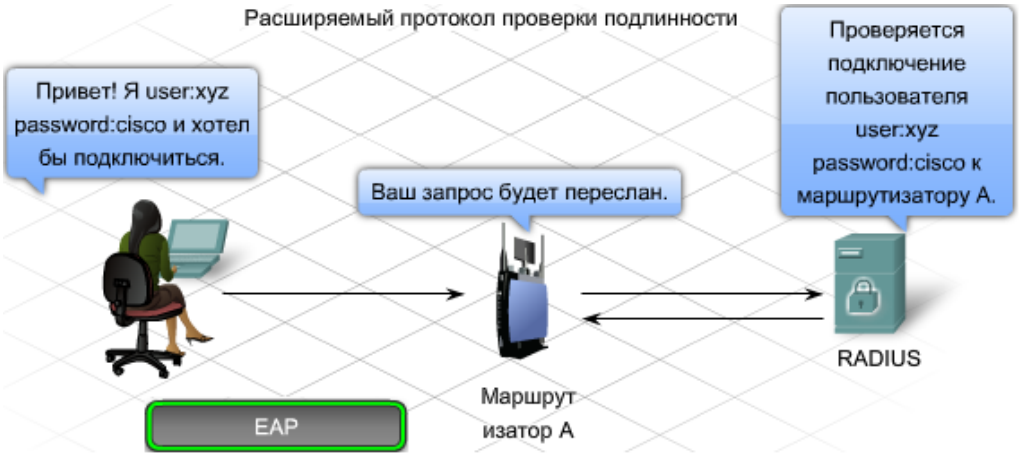


Рис. 16. Расширяемый протокол проверки подлинности

Если функция аутентификации включена, то независимо от применяемого метода клиент должен успешно пройти аутентификацию до того, как ему будет предоставлено разрешение на вход в точку доступа. Если включены функции аутентификации и фильтрации MAC-адресов, то в первую очередь выполняется аутентификация.

Если аутентификация прошла успешно, точка доступа затем проверяет MAC-адрес по таблице MAC-адресов. После выполнения проверки точка доступа добавляет MAC-адрес этого узла в свою таблицу узлов. Таким образом, предполагается, что клиент ассоциирован с точкой доступа и имеет разрешение на подключение к сети.

Безопасность в беспроводных сетях

В связи с бурным развитием сетей, в том числе и беспроводных, значительно возросли требования к безопасности. Увеличение безопасности приводит к увеличению времени обслуживания системы в целом.

Беспроводные точки доступа излучают радиоволны на большие площади, которые не ограничиваются физическими строениями, что делает радиосигналы доступными для подслушивания. Это приводит к повышенной уязвимости беспроводных сетей.

Радиоволны от беспроводных мостов сконцентрированы в одном луче. Взломщик должен находиться на пути следования луча, чтобы перехватить информацию в процессе передачи данных. Исходя из этого, беспроводные точки доступа требуют большей безопасности, чем мосты.

Шифрование в сети WLAN

Аутентификация и фильтрация MAC-адресов могут блокировать взломщику доступ в беспроводную сеть, но не смогут предотвратить перехват передаваемых данных. Поскольку не существует четких границ беспроводных сетей и весь трафик передается без проводов, то взломщик может легко перехватывать или прочитать кадры данных беспроводной сети. Шифрование – это процесс преобразования данных таким образом, что даже перехват информация оказывается бесполезным.

Протокол конфиденциальности, эквивалентной проводной связи - Wired Equivalency Protocol (WEP)

Протокол WEP – это усовершенствованный механизм безопасности, позволяющий шифровать сетевой трафик в процессе передачи. В протоколе WEP для шифрования и расшифровки данных используются предварительно настроенные ключи.

WEP-ключ вводится как строка чисел и букв длиной 64 или 128 бит. В некоторых случаях протокол WEP поддерживает 256-битные ключи. Для упрощения создания и ввода этих ключей во многих устройствах используются фразы-пароли. Фраза-пароль – это простое средство запоминания слова или фразы, используемых при автоматической генерации ключа (рис. 17).

Для эффективной работы протокола WEP точка доступа, а также каждое беспроводное устройство, имеющее разрешение на доступ в сеть, должны использовать общий WEP-ключ. Без этого ключа устройства не смогут распознать данные, передаваемые по беспроводной сети.

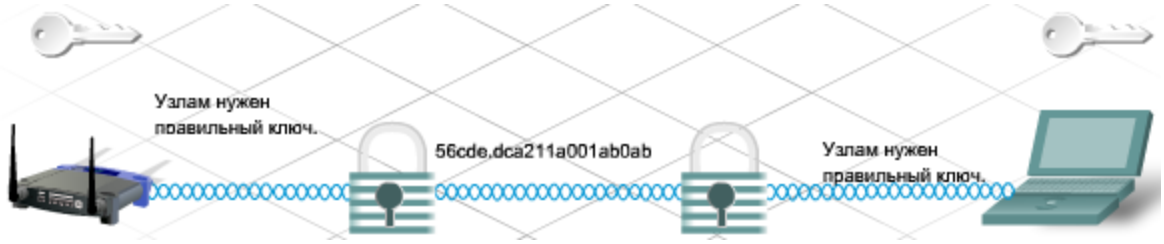


Рис. 17. Шифрование в сети WLAN

Протокол WEP – это эффективное средство защиты данных от перехвата. Тем не менее, протокол WEP также имеет свои слабые стороны, одна из которых заключается в использовании статического ключа для всех устройств с поддержкой WEP. Существуют программы, позволяющие взломщику определить WEP-ключ. Эти программы можно найти в сети Интернет. После того, как взломщик получил ключ, он получает полный доступ ко всей передаваемой информации.

Одним из средств защиты от такой уязвимости является частая смена ключей. Существует усовершенствованное и безопасное средство шифрования – протокол защищенного доступа Wi-Fi (Wi-Fi Protected Access, (WPA)).

Защищенный доступ к Wi-Fi (WPA)

В протоколе WPA используются ключи шифрования длиной от 64 до 256 бит. При этом WPA, в отличие от WEP, генерирует новые динамические ключи при каждой попытке клиента установить соединение с точкой доступа. По этой причине WPA считается более безопасным, чем WEP, так как его значительно труднее взломать.

Решения на основе технологий VPN, EAP и LEAP

Чтобы избежать многих ограничений беспроводных сетей, было разработано большое количество решений и протоколов для обеспечения безопасности в беспроводных сетях, таких, как виртуальные частные сети (Virtual Private Network — VPN) и расширяемый протокол аутентификации (Extensible Authentication Protocol — EAP). Точка доступа, использующая протокол EAP, не выполняет аутентификации пользователей; для этой цели служит выделенный сервер, способный провести более тщательную проверку параметров клиента. При использовании интегрированного сервера VPN данная технология создает туннель, применяя существующий протокол, например, IP. Такой туннель представляет собой соединение на третьем уровне эталонной модели, в отличие от соединения второго уровня между сетевой платой и точкой доступа.

Ниже приведено краткое описание протоколов EAP и LEAP.

EAP-MD5 Challenge (Запрос MD5-хэша протокола EAP). Механизм EAP является одним из первых методов аутентификации и во многом похож на протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP), который используется в проводных сетях для защиты паролей. Протокол EAP позволяет клиентским сетевым адаптерам, поддерживающим различные типы аутентификации, выполнять процедуру аутентификации с различными конечными серверами, такими, как RADIUS.

Упрощенный расширяемый протокол аутентификации (Lightweight Extensible Authentication Protocol - LEAP). Корпорация Cisco разработала разновидность протокола EAP, который базируется на обоюдной аутентификации, названной LEAP. При обоюдной аутентификации должны быть аутентифицированы как сетевой адаптер клиента, так и точка доступа, через которую клиент пытается подключиться к корпоративной сети. При использовании такого типа аутентификации корпоративная сеть будет защищена от использования неавторизированных точек доступа для подключения к сети. Аутентификация LEAP стандартно используется на всех беспроводных точках доступа корпорации Cisco. Технология LEAP предоставляет безопасность в процессе обмена данными, шифрование данных с использованием динамических ключей WEP и поддерживает обоюдную аутентификацию.

Механизмы безопасности технологии VPN включают несколько методов:

аутентификация пользователя позволяет только авторизованным пользователям подключаться, передавать и принимать данные, используя беспроводную сеть;

шифрование предоставляет средства обеспечения конфиденциальности данных и дополнительную защиту данных от злоумышленников;

аутентификация данных проверяет целостность данных, позволяет аутентифицировать устройство-отправитель и получателя данных.

Технология VPN эффективно увеличивает уровень безопасности в беспроводных сетях по той причине, что свободные беспроводные локальные сети автоматически пересылают данные между клиентами, которые находятся в пределах одной беспроводной сети. Зона покрытия беспроводных сетей не ограничена стенами здания, и без использования дополнительных технологий увеличения уровня безопасности неавторизованные пользователи могут проникать в сеть без особых проблем. Поэтому необходимо устанавливать минимальную низкоуровневую безопасность в беспроводной локальной сети.

Контрольные вопросы

1. Какие существуют технологии беспроводных сетей?
2. Какие существуют типы беспроводных сетей и в чем их особенности?
3. Укажите наименоване и характеристики компанентов беспроводных сетей?
4. Что такое SSID и в чем его назначение?
5. Какими методами осуществляется безопасность беспроводных сетей?

Лекция 26
Проектирование локальных сетей

1. **Цели проекта локальной сети**
2. **Методика проектирования сети**
3. **Фильтрация трафика на уровне распределения**

Ключевые слова: проектирование, требования, компоненты, архитектура, модуль, методика, технология, топология, оборудование, доступность, службы

1. Цели проекта локальной сети

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

- **Функциональность.** Сеть должна обеспечить связь пользователей друг с другом и с приложениями с соответствующей требованиям скоростью и надежностью.
- **Расширяемость.** Сеть должна обладать способностью к росту. Это означает, что первоначально реализованная сеть должна увеличиваться без каких-либо существенных изменений общего устройства.
- **Адаптируемость.** Сеть должна быть разработана с учетом технологий будущего и не должна включать элементы, которые в дальнейшем ограничивали бы внедрение технологических новшеств.
- **Управляемость.** Сеть нужно сконструировать так, чтобы облегчить текущий контроль и управление для обеспечения стабильности ее работы.
- **Безопасность.** Безопасность — характеристика, которая должна учитываться при разработке сети, а не после ее завершения. Планирование размещения устройств, обеспечивающих безопасность, фильтров и межсетевых экранов очень важно для защиты сетевых ресурсов.
- **Масштабируемость.** Масштабируемые сети способны расширяться для добавления новых групп пользователей и удаленных узлов, а также поддерживать новые приложения без ухудшения уровня обслуживания существующих пользователей.
- **Доступность.** Сеть, разработанная для обеспечения доступности, должна обеспечивать постоянную надежную работу. Кроме того, сбой одного канала или одного компонента оборудования не должен значительно влиять на производительность сети.

Компоненты сетевого проекта

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

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

Чтобы выполнить основные задачи проекти-рования, в основе сети должна лежать архитектура, предусматривающая универсальность при-менения и расширение.

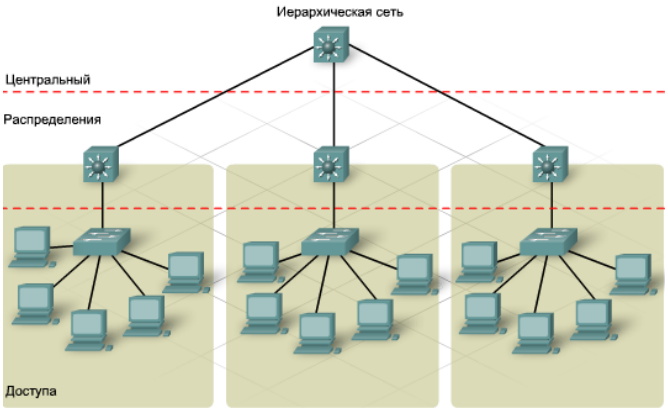


Рис. 1. Иерархическая архитектура сети

Иерархическая архитектура сети

В сетевом проектировании, иерархическая архитектура служит для группировки устройств в несколько сетей. Существует три (рис. 1) основных уровня:

1. центральный уровень - соединяет устройства уровня распределения;
2. уровень распределения - соединяет между собой малые локальные сети;
3. уровень доступа - обеспечивает соединение сетевых узлов и конечных устройств.

Преимущества перед сетями плоского типа

Иерархические сети имеют ряд преимуществ перед сетями с плоской архитектурой. Преимущество разделения плоской сети на более мелкие и лучше управляемые блоки заключается в том, что локальный трафик остается локальным. На верхний уровень попадает только трафик, предназначенный для других сетей.

Устройства второго уровня в плоской сети обладают малой возможностью управлять широковещательными рассылками и фильтровать нежелательный трафик. По мере добавления в плоскую сеть устройств и приложений время отклика увеличивается до тех пор, пока сеть не становится непригодной к применению.

Корпоративные архитектуры можно использовать для дополнительного разделения трехуровневой иерархической архитектуры на модульные участки. Модули представляют собой участки с разными физическими или логическими возможностями подключения. Они обозначают функциональное разделение в сети. Эта модульность обеспечивает гибкость применения сетевой архитектуры. Она облегчает внедрение, а также поиск и устранение неполадок. В модульной сетевой архитектуре существует три ключевых области (рис. 2):

- комплекс зданий предприятия - эта область включает сетевые элементы, предназначенные для независимого функционирования в комплексе зданий или в филиале;
- серверная ферма - компонент комплекса зданий предприятия, серверная ферма центра обработки данных защищает ресурсы сервера и обеспечивает возможность надежного резервного высокоскоростного подключения;
- граница предприятия - когда трафик поступает в сеть комплекса зданий, эта область отфильтровывает трафик из внешних ресурсов и направляет его в корпоративную сеть. В нее включены все элементы, необходимые для эффективного и безопасного обмена данными между комплексом зданий предприятия и удаленными объектами, удаленными пользователями и сетью Интернет.

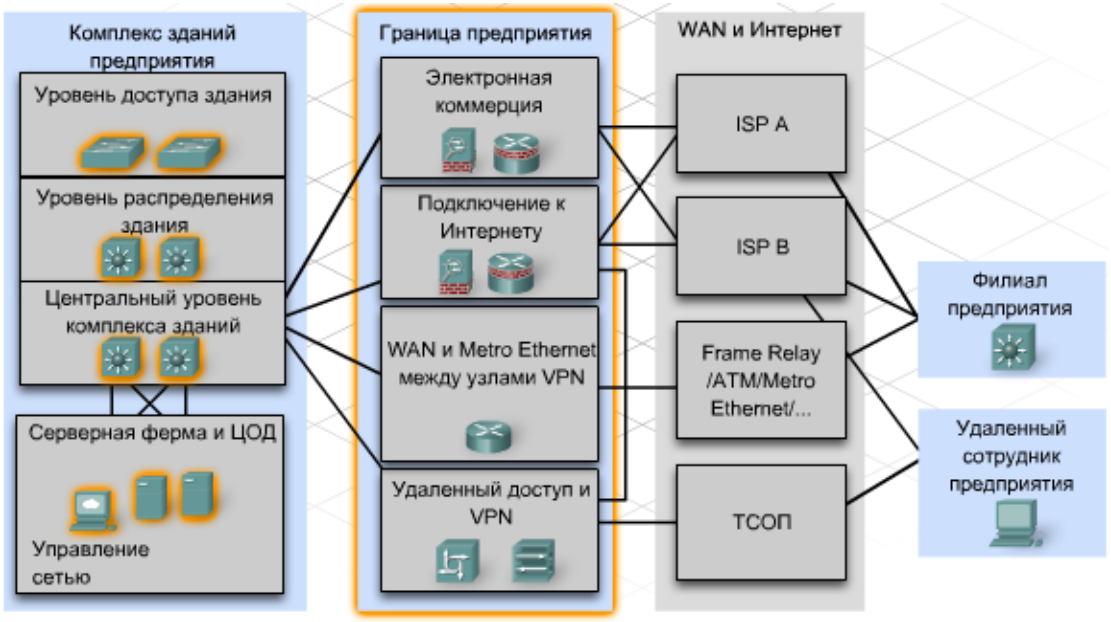


Рис. 2. Модульная сетевая архитектура

Модульная структура корпоративных архитектур имеет следующие преимущества.

1. Она создает детерминированную сеть с четко определенными границами между модулями. Это предполагает ясные точки разграничения, которые позволяют разработчикам сети с точностью определять, откуда происходит трафик и куда он поступает.
2. Подобная структура облегчает задачу проектирования, делая каждый модуль независимым. Разработчик может сконцентрироваться на потребностях каждой отдельной области.
3. Она обеспечивает масштабируемость, облегчая добавление модулей в корпоративную сеть. По мере усложнения сети разработчик может добавлять новые функциональные модули.
4. Она позволяет разработчику добавлять службы и решения, не изменяя базовую архитектуру сети.

Методика проектирования сети

Проектирование больших сетей обычно разбивается на три отдельных шага.

Шаг 1. Определение требований к сети

Разработчик сети работает в тесном контакте с клиентом для документирования целей проекта. Цели обычно подразделяются на две категории:

бизнес-цели - ориентированы на то, как сделать бизнес более успешным;

технические требования - ориентированы на то, как реализована технология в сети.

Шаг 2. Описание существующей сети

Собираются и подвергаются анализу сведения о текущей сети и сервисах. Необходимо сравнить функциональные возможности существующей сети с определенными целями нового проекта. Разработчик определяет, можно ли повторно использовать текущее оборудование, инфраструктуру и протоколы и какое новое оборудование и протоколы необходимы для завершения проекта.

Шаг 3. Проектирование топологии сети

Общей стратегией при проектировании сетей является метод нисходящего порядка, или метод «сверху вниз». В соответствии с этим методом сначала определяются требования к сетевым приложениям и службам, а потом, согласно им, проектируется сеть.

По завершении проекта выполняется тестирование прототипа или пробной версии. Такой подход позволяет удостовериться, что новый проект функционирует как положено перед его непосредственным внедрением.

Частой ошибкой, которую совершают разработчики сети, является неверное определение объема проекта сети.

Определение объема проекта

Выявляя требования, разработчик определяет те из них, которые отражаются на всей сети, и те, что проявляются только на конкретных участках. Неспособность понять влияние того или иного требования часто влечет за собой превышение объемом проекта первоначальной сметы. Из-за этого упущения могут значительно возрасти финансовые и временные затраты, необходимые для внедрения нового проекта.

Влияние на всю сеть

В число сетевых требований, действующих на всю сеть, входят:

- добавление новых сетевых приложений и значительное изменение существующих, например изменения базы данных или структуры DNS;
- повышение эффективности сетевой адресации или изменение протоколов маршрутизации;
- интеграция новых мер безопасности;
- добавление новых сетевых служб, например, голосового трафика, сетей распространения контента или сетевого хранения;
- перемещение серверов в серверную ферму центра обработки данных.

Влияние на участок сети

К числу требований, которые влияют только на участок сети, относятся:

- улучшение подключения к сети Интернет и увеличение пропускной способности;
- обновление кабельных каналов LAN уровня доступа;
- обеспечение резервирования для ключевых служб;
- поддержка беспроводного доступа на определенных участках;
- модернизация пропускной способности WAN.

Эти требования не обязательно отражаются на многих пользователях и не требуют больших изменений для установленного оборудования. Иногда можно интегрировать изменения архитектуры в существующую сеть, не прерывая ход сетевых операций большинства пользователей сети. Этот метод позволяет сократить издержки, связанные с простоями, и ускорить модернизацию сети.

Центральный уровень сети

Центральный уровень иногда называют сетевая магистраль (рис. 3). Маршрутизаторы и коммутаторы на центральном уровне обеспечивают высокоскоростное подключение. В корпоративной LAN на центральном уровне могут быть соединены несколько зданий или объектов, а также обеспечиваться подключение к серверной ферме. В центральный уровень входят одно

или несколько подключений к устройствам на границе предприятия для поддержки сети Интернет, виртуальные частные сети (VPN), сети экстранет и доступа к WAN.

Внедрение центрального уровня позволяет снизить сложность сети, поскольку упрощает ее управление, а также поиск и устранение неполадок.

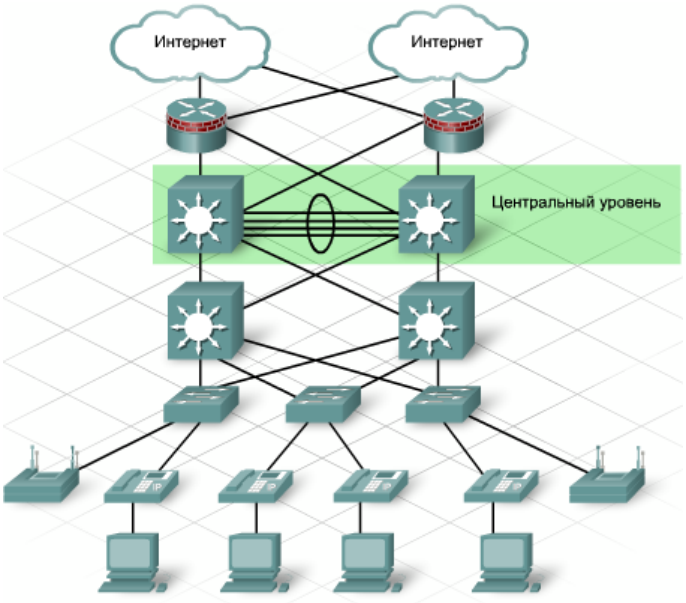


Рис. 3. Центральный уровень сети

Цели центрального уровня

Проектирование центрального уровня предусматривает эффективную высокоскоростную передачу данных между участками сети. Основными целями проектирования на центральном уровне являются:

- обеспечение 100% времени работы;
- доведение до максимума пропускной способности;
- упрощение расширения сети.

Технологии центрального уровня

В число технологий, используемых на центральном уровне, входят:

- маршрутизаторы или многоуровневые коммутаторы, которые сочетают функции маршрутизации и коммутации в одном устройстве
- резервирование и распределение нагрузки;
- высокоскоростные и агрегированные каналы;
- протоколы маршрутизации с возможностью хорошего масштабирования и быстрой конвергенции, например усовершенствованный протокол внутренней маршрутизации между шлюзами протокол EIGRP и протокол алгоритм выбора кратчайшего пути (OSPF).

Резервные каналы

При внедрении резервных каналов на центральном уровне сетевые устройства всегда могут найти альтернативные маршруты для отправки данных в случае сбоя.

Если устройства уровня 3 разместить на центральном уровне, эти резервные каналы можно использовать как для резервирования, так и для распределения нагрузки. В сети с плоской архитектурой уровня 2 протокол связующего дерева (STP) отключает резервные каналы, если нет сбоя основного канала (рис. 4). Режим STP не допускает распределения нагрузки с помощью резервных каналов.

Ячеистая топология

Большинство центральных уровней в сети связаны либо в полносвязанную топологию, либо в частично-ячеистую. В полносвязанной топологии каждое устройство подключается ко всем остальным устройствам. Несмотря на то, что полносвязанные топологии дают преимущества сети с полным резервированием, возможны сложности при их соединении и управлении, а также они требуют больших затрат. Для установок большего размера используется модифицированная частично-ячеистая топология. В частично-ячеистой топологии каждое устройство соединено, по

крайней мере, с двумя другими, при этом создается достаточное резервирование и удается избежать сложности полносвязанной топологии.

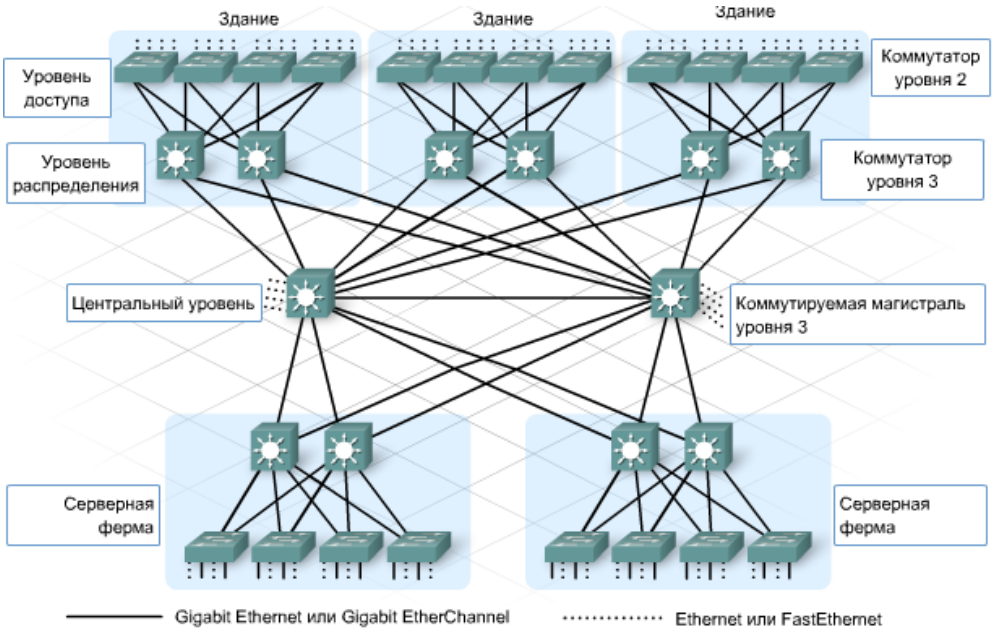


Рис. 4. Резервные каналы в ячеистой топологии

Уровень распределения

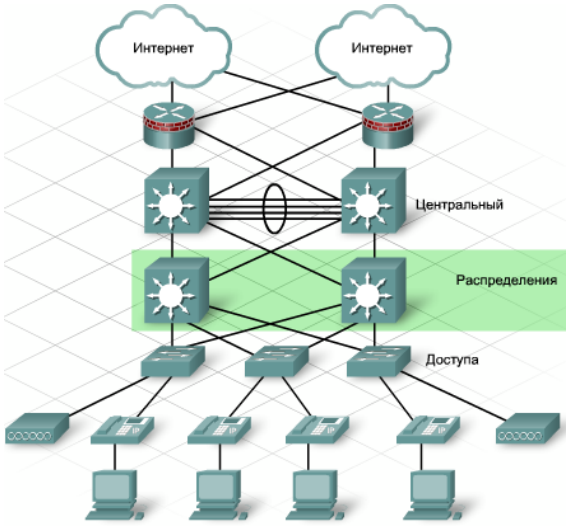


Рис. 5. Уровень распределения

Уровень распределения представляет собой границу маршрутизации между уровнем доступа и центральным уровнем (рис. 5). Кроме того, он служит точкой соединения между удаленными узлами и центральным уровнем.

Маршрутизация на уровне распределения

Уровень доступа обычно создается с помощью технологии коммутации уровня 2. Уровень распределения формируется с помощью устройств уровня 3. Маршрутизаторы или многоуровневые коммутаторы, размещенные на уровне распределения, предусматривают многие функции, необходимые для выполнения целей архитектуры сети. В число этих целей входят:

- фильтрация и управление потоками трафика;
- внедрение политик контроля доступа;
- объединение маршрутов перед объявлением их на центральный уровень;
- изолирование центрального уровня от сбоев и неполадок на уровне доступа;
- маршрутизация между сетями VLAN на уровне доступа.

Кроме того, устройства уровня распределения служат для управления очередями и определения приоритетов для трафика перед передачей его через центральный уровень комплекса зданий.

Магистральные каналы

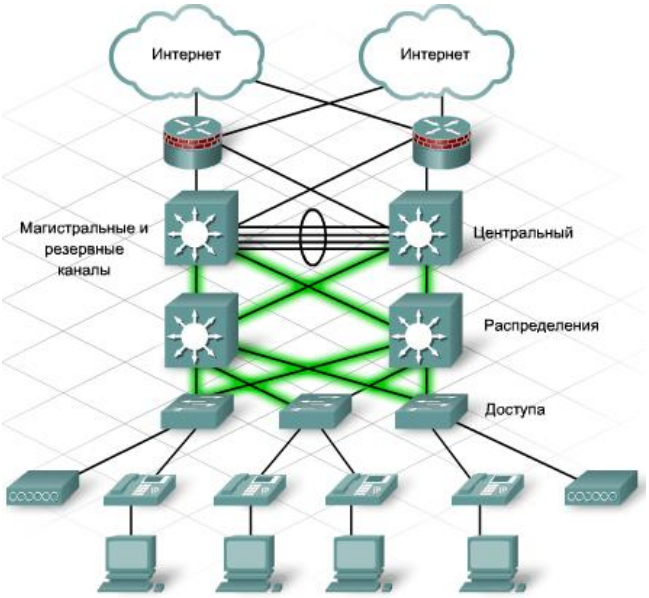


Рис. 6. Магистральные каналы

Часто между сетевыми устройствами уровня доступа и распределения устанавливают магистральные каналы. Магистральные каналы служат для передачи трафика, относящегося к нескольким сетям VLAN, между устройствами по одному и тому же каналу. При проектировании магистральных каналов разработчик сети принимает во внимание общую стратегию сетей VLAN и шаблоны сетевого трафика (рис. 6).

Резервные каналы

Если между устройствами на уровне распределения существуют резервные каналы, устройства можно настроить для распределения нагрузки трафика в каналах. Распределение нагрузки увеличивает пропускную способность, доступную для приложений.

Топология уровня распределения

Сети уровня распределения обычно соединяются в частично-ячеистую топологию. Эта топология предусматривает достаточное количество резервных маршрутов, чтобы сеть продолжала работу при сбое канала или устройства. Когда устройства уровня распределения располагаются в одном коммутационном отсеке или центре обработки данных, они соединяются с помощью гигабитных каналов. Если устройства отделяются друг от друга большими расстояниями, используется оптоволоконный кабель.

Ограничение области сбоя сети

Домен возникновения сбоя означает участок сети, который оказывается затронутым при отказе сетевого приложения или устройства (рис.7).

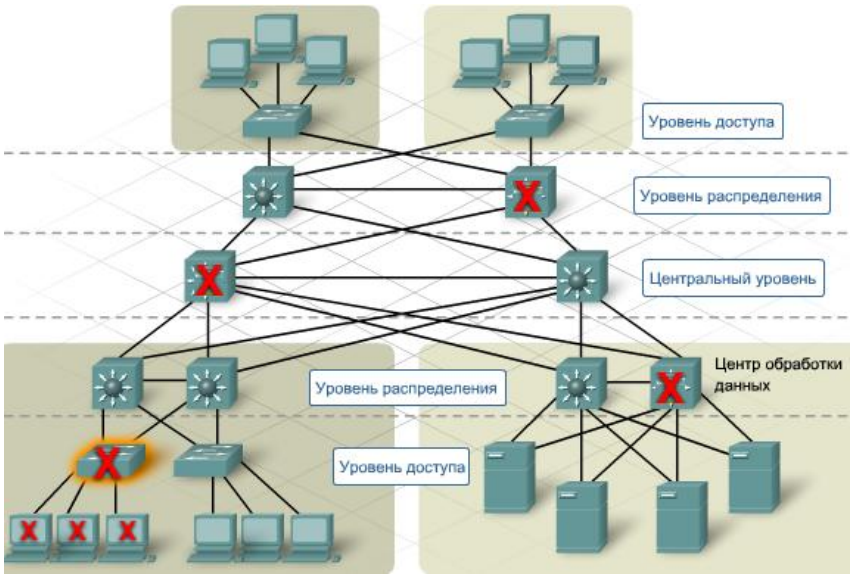


Рис. 7. Ограничение размера доменов возникновения сбоя

Ограничение размера доменов возникновения сбоя

Поскольку сбои на центральном уровне сети оказывают значительное воздействие, разработчики сетей часто уделяют особое внимание предотвращению сбоев. В модели с иерархической архитектурой легче и дешевле всего контролировать размер домена возникновения сбоя на уровне распределения.

На уровне распределения ошибки сети можно ограничить небольшой областью, и они будут затрагивать небольшое число пользователей.

При использовании устройств уровня 3 на уровне распределения каждый маршрутизатор выступает в качестве шлюза для ограниченного числа пользователей уровня доступа.

Развертывание блока коммутаторов

Маршрутизаторы или многоуровневые коммутаторы обычно развертываются парами, при этом коммутаторы уровня доступа поровну распределяются между ними. Эта конфигурация называется блоком коммутации здания или отдела. Каждый блок коммутации функционирует независимо от других. Поэтому в случае отказа отдельного устройства не будет сбоя всей сети. Более того, даже сбой всего блока коммутации отражается лишь на некотором числе конечных пользователей.

Создание резервной сети

Чтобы сократить время простоя, разработчики сети предусматривают в сети резервирование.

Резервирование на уровне распределения

Устройства на уровне распределения имеют резервные подключения к коммутаторам уровня доступа и к устройствам центрального уровня. При отказе канала или устройства эти подключения обеспечивают альтернативные маршруты. С помощью соответствующего протокола маршрутизации на уровне распределения устройства уровня 3 быстро откликаются на сбои канала, вследствие чего последние на работу сети влияния не оказывают.

Если не включен протокол STP, наличие нескольких подключений к коммутаторам уровня 2 может вызвать нестабильность в работе сети. Без протокола STP резервные каналы в сети уровня 2 могут вызвать широковещательные штормы. Коммутаторам не удается верно выучить порты, поэтому трафик переполняет коммутатор. При отключении одного из каналов протокол STP гарантирует, что активным между двумя устройствами будет только один маршрут. При отказе одного из каналов коммутатор перерассчитывает топологию связующего дерева и автоматически начинает использовать альтернативный канал.

3. Фильтрация трафика на уровне распределения

Списки контроля доступа (ACL-списки) - это средство, которое можно использовать на уровне распределения для ограничения доступа и предотвращения поступления нежелательного трафика из сети центрального уровня. ACL-список - это список условий, служащих для проверки сетевого трафика, который поступает через интерфейс маршрутизатора. Инструкции ACL-списка определяют, какие пакеты следует принять, а какие – отклонить.

Фильтрация сетевого трафика

Для фильтрации сетевого трафика маршрутизатор анализирует каждый пакет и либо пересылает его, либо отклоняет, исходя из условий, указанных в ACL-списке. Существуют разные типы ACL-списков для разных назначений. Стандартные ACL-списки фильтруют трафик, исходя из адреса источника. Расширенные ACL-списки позволяют фильтровать на основе нескольких критериев, в том числе:

- адрес источника;

- адрес назначения;
- протоколы;
- номера портов и приложения;
- входит ли пакет в установленный поток TCP.

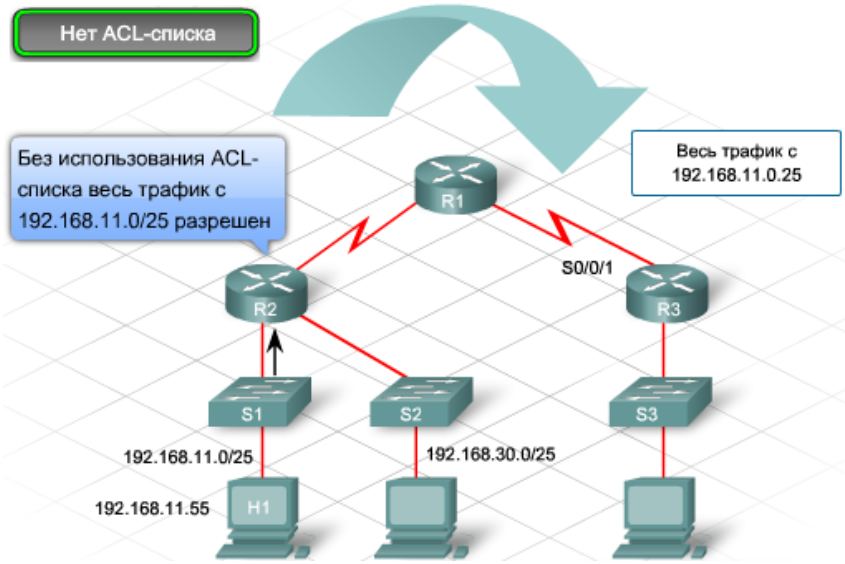


Рис. 8. Сеть без фильтрации

Стандартный и расширенный ACL-списки можно настроить либо в форме нумерованного, либо в форме именованного списка доступа.

Сложные ACL-списки

Стандартные (рис. 9) и расширенные (рис. 10) ACL-списки служат основой для более сложных типов ACL-списков. Можно настроить три сложных ACL-функции: динамическую, рефлексивную и синхронизируемую.

Динамический ACL-список - пользователь должен использовать протокол Telnet для подключения к маршрутизатору и аутентификации. После аутентификации будет разрешено поступление трафика от пользователя. Динамические ACL-списки иногда называются «замок и ключ», поскольку пользователю необходимо войти в систему, чтобы получить доступ.

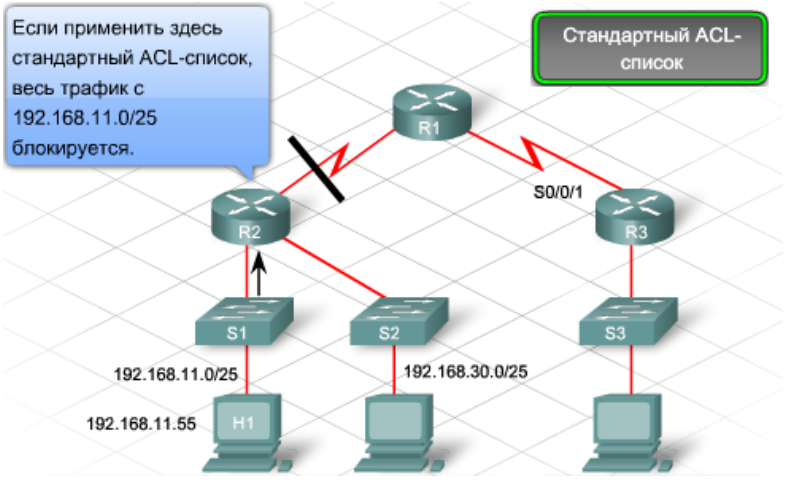


Рис. 9. Стандартный ACL-список

Рефлексивный ACL-список - разрешает исходящий трафик, после чего ограничивает входящий только откликами на эти разрешенные запросы. Это напоминает использование в инструкциях расширенного ACL-списка установленного ключевого слова, за исключением того, что эти ACL-списки могут проверять не только трафик по протоколу TCP, но и по UDP и ICMP.

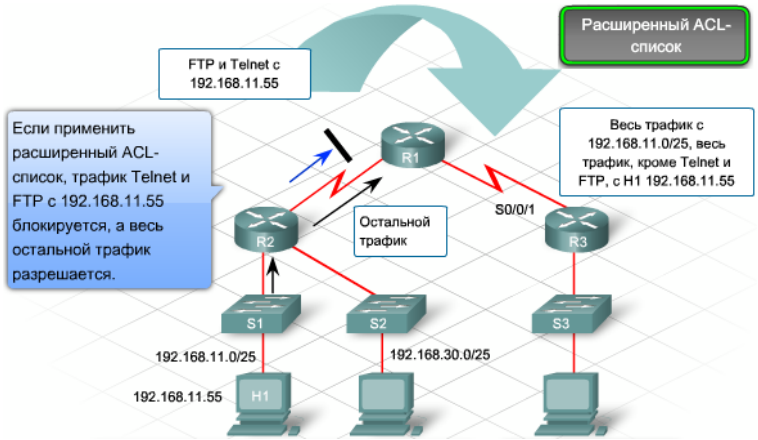


Рис. 10. Расширенный ACL-список

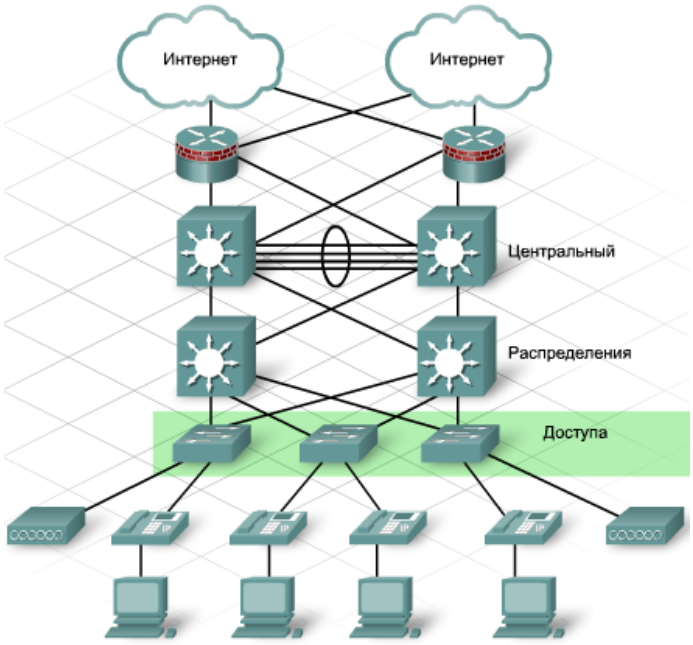


Рис. 11. Размещение ACL-списков

Синхронизируемый ACL-список - разрешает и отклоняет определенный трафик, исходя из времени дня или дня недели.

Размещение ACL-списков

Трафик, который поступает в интерфейс, фильтруется входящим ACL-списком. Исходящий из интерфейса трафик фильтруется исходящим списком контроля доступа.

Чтобы достичь требуемых результатов, разработчик сети должен решить, где размещать ACL-списки в сети.

Уровень доступа

Уровень доступа представляет границу сети, где соединяются конечные устройства. Службы и устройства уровня доступа размещаются внутри каждого здания комплекса, каждого удаленного узла и серверной фермы, а также на границе предприятия (рис. 11).

Физические факторы уровня доступа

На уровне доступа инфраструктуры комплекса зданий используется технология коммутации уровня 2 для обеспечения доступа к сети.

Доступ может предоставляться либо через постоянную проводную инфраструктуру, либо через беспроводные точки доступа. Сеть Ethernet с использованием медной проводки имеет ограничения по расстоянию. Поэтому одной из основных проблем при проектировании уровня доступа в инфраструктуре комплекса зданий является физическое расположение оборудования.

Коммутационные отсеки

Коммутационными отсеками могут быть действительно отсеки или небольшие телекоммуникационные комнаты, выступающие в качестве конечной точки для кабельной проводки инфраструктуры в зданиях или на их этажах. Размещение и физический размер коммутационных отсеков зависит от размера сети и планов на расширение.

Оборудование в коммутационных отсеках обеспечивает питанием конечные устройства, в частности, IP-телефоны и беспроводные точки доступа.

В отличие от стандартного коммутационного отсека на серверной ферме или в центре обработки данных устройства уровня доступа - это, как правило, резервные многоуровневые коммутаторы, сочетающие функциональные возможности маршрутизации и коммутации.

Воздействие конвергированной сети

Современная компьютерная сеть состоит не только из персональных компьютеров и принтеров, подключенных к уровню доступа. К IP-сети могут подключаться множество разных устройств, в том числе:

IP-телефоны;

видеокамеры;

системы видеоконференций.

Все эти службы могут быть сведены в единой физической инфраструктуре уровня доступа. Однако для их поддержки усложняется проектирование логической сети из-за таких факторов, как служба QoS, разделение трафика и фильтрация. Эти новые типы конечных устройств и связанные приложения и службы изменяют требования к масштабируемости, доступности, безопасности и управляемости на уровне доступа.

Требование доступности

В ранних сетях высокая доступность наблюдалась обычно только на центральном уровне сети, на границе предприятия и в сетях центра обработки данных. С появлением IP-телефонии ожидается, что каждый телефон должен быть доступен 100% времени.

Резервные компоненты и стратегии переключения при отказе можно реализовать на уровне доступа для повышения надежности и доступности конечных устройств.

Управление уровнем доступа

Главная проблема, стоящая перед разработчиком сетей, - это улучшение управляемости уровня доступа. Управление уровнем доступа важно по следующим причинам:

- увеличение количества и разнообразия типов подключенных устройств на уровне доступа;
- внедрение беспроводных точек доступа в LAN.

Проектирование возможностей управления.

Помимо обеспечения базовой возможности подключения на уровне доступа разработчик сети должен принимать во внимание:

- структуру именования;
- архитектуру VLAN;
- модели трафика;
- стратегии определения приоритетов.

Очень важными являются настройка и применение систем управления сетями в крупной конвергентной сети. Кроме того, важно стандартизировать конфигурации и оборудование, где это возможно.

При соблюдении принципов успешного проектирования улучшается управляемость и текущая поддержка сети за счет:

- недопущения излишней усложненности сети;
- упрощения поиска и устранения неполадок при их возникновении;
- упрощения последующего добавления новых функций и служб.

Топологии сети на уровне доступа

В большинстве современных сетей Ethernet используется топология типа «звезда», которую иногда называют топологией «ступица и спица». В топологии типа «звезда» все конечные устройства напрямую подключены к одному сетевому устройству. Этим единым сетевым

устройством обычно бывает коммутатор уровня 2 или многоуровневый коммутатор. В проводной топологии типа «звезда» на уровне доступа обычно отсутствует резервирование между отдельными конечными устройствами и коммутатором. Для многих предприятий затраты на дополнительную проводку при создании резервирования слишком высоки.

К преимуществам топологии типа «звезда» относятся:

- простая установка;
- минимальная настройка.

Недостатки топологии типа «звезда» значительны.

- Центральное устройство представляет единую точку сбоя.
- Возможности центрального устройства могут ограничивать общую производительность для доступа к сети.
- Топология не восстанавливается в случае сбоя, если нет резервных каналов.

Топологии типа «звезда» для сети Ethernet обычно имеют в сочетании следующие кабели:

- кабель типа витой пары для подключения к отдельным конечным устройствам;
- оптоволоконный кабель для соединения коммутаторов доступа с устройствами уровня распределения.

Использование VLAN для разделения трафика

Использование сетей VLAN и IP-подсетей - это наиболее распространенный способ разделения пользовательских групп и трафика в сети уровня доступа.

Сегодня сети VLAN служат для разделения и классификации потоков трафика и управления широковещательным трафиком в едином коммутационном отсеке или здании (рис. 12). Несмотря на то, что не рекомендуется использовать большие VLAN, охватывающие целые сети, они могут использоваться для поддержки определенных приложений, например, беспроводного роуминга и беспроводных IP-телефонов.

Рекомендуется размещать сети VLAN в одном коммутационном отсеке. При таком подходе увеличивается количество сетей VLAN в сети, что в свою очередь приводит к увеличению числа отдельных IP-подсетей. Рекомендуется соединять одну IP-подсеть с одной сетью VLAN. Важной задачей проектирования становится IP-адресация на уровне доступа, которая влияет на масштабируемость всей сети.

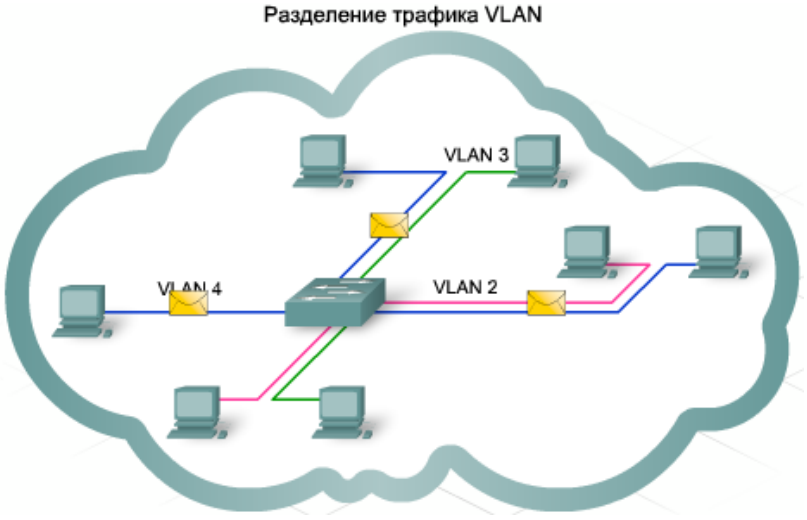


Рис. 12. Использование VLAN для разделения трафика

Службы на границе сети

Обеспечение качества обслуживания сетевых приложений

Сети должны предоставлять безопасные, стабильные, измеримые, а иногда и гарантированные службы. Кроме того, сетям необходимы механизмы отслеживания перегрузок при увеличении трафика. Перегрузка канала возникает, когда спрос на сетевые ресурсы превышает допустимую пропускную способ-

ность.

Ресурсы во всех сетях ограничены. Вследствие этого сети должны быть оснащены механизмами службы QoS. Возможности службы QoS зависят от классификации трафика и назначенного приоритета.

Классификация

Перед проектированием стратегий службы QoS необходимо классифицировать приложения, исходя из определенных требований служб. Классификация данных в источнике (или около него) позволяет назначать им соответствующий приоритет по мере перемещения их по всей сети. Отбор трафика со сходными свойствами и группировка его по классам с последующей маркировкой являются функциями сетевых устройств на уровнях доступа и распределения (рис.13). В качестве примера этой стратегии можно привести помещение голосового трафика из коммутатора доступа в одну сеть VLAN. Далее, устройство маркирует трафик, поступивший из голосовой VLAN, и присваивает ему наивысший приоритет.

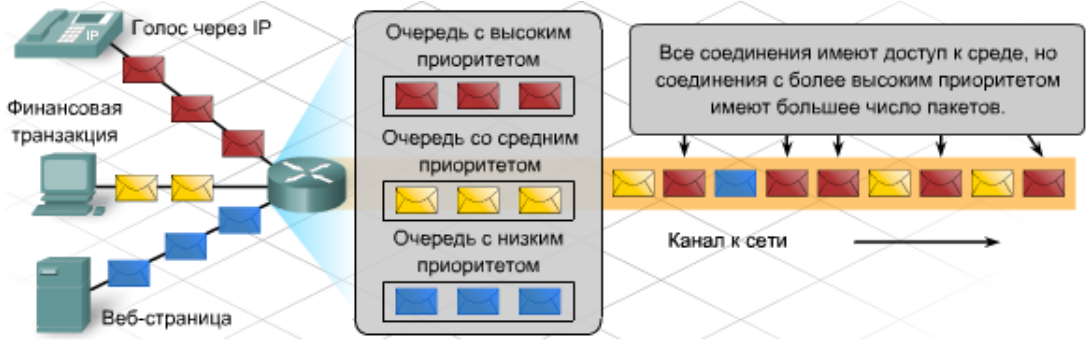


Рис. 13. Маркировка и изменение приоритета трафика

Контрольные вопросы

1. Какие требования характерны доля большенства проектов LAN?
2. В чем заключается приемущество иерархической архитектуры?
3. В чем приемущества модульной структуры корпоратвной архитектуры?
4. Какие технологии используются при проектировании уровней иерархии?
5. На каком уровне при проектировании разрабатывются методы обеспечения безопасности?

Лекция 27
Защита локальных сетей

1. Серверные фермы
2. Методы атак
3. Разработка мер обеспечения безопасности в сети

Ключевые слова: службы, доступность, безопасность, сервер, трафик, вторжения, атака, хакер, вирус, червь, «Троянский конь», DoS, cookie, механизм, защита, аутентификация, авторизация, ключ

Большинство корпоративных сетей предоставляют пользователям службы с доступом в Интернет, например, электронную почту и электронную коммерцию. Для успешной деятельности предприятия очень важны доступность и безопасность этих служб.

1. Серверные фермы

Управление и защита многочисленных распределенных серверов с разным расположением в сети предприятия представляют определенную сложность. Рекомендуется централизовать серверы на серверных фермах. Серверные фермы обычно располагаются в машинных залах и центрах обработки данных.

При создании серверной фермы открываются следующие преимущества.

Сетевой трафик поступает и покидает серверную ферму в определенной точке. Это упрощает защиту, фильтрацию и назначение приоритетов трафика.

Резервные каналы с высокой пропускной способностью можно установить как для серверов, так и между сетью серверной фермы и основной LAN. Эта конфигурация более экономична по сравнению с обеспечением подобного уровня подключения для серверов, распределенных в сети.

Распределение нагрузки и переключение при отказе можно предусмотреть между серверами и между сетевыми устройствами.

Количество коммутаторов с высокой пропускной способностью и устройств защиты сокращается, что позволяет снизить затраты на предоставление сервисов.

Риски вторжения в сеть

Компьютерные сети – как проводные, так и беспроводные – стремительно приходят в повседневную жизнь. Индивидуальные пользователи и организации в равной мере зависят от надежной работы компьютеров и сетей в таких задачах, как электронная почта, учет, организационное управление и работа с файлами. Несанкционированное вторжение в сеть может привести к чрезвычайно затратным перебоям и потере ценных результатов работы. Атака на сеть может иметь разрушительные последствия с потерей времени и денег в результате повреждения или хищения важной информации и ресурсов.

Злоумышленники могут получить доступ в сеть, эксплуатируя уязвимости в ПО, атакуя оборудование или даже используя такие изящные приемы, как угадывание чужого имени поль-

зователя и пароля. Злоумышленники, которые получают доступ, изменяя программное обеспечение или эксплуатируя уязвимости в программном обеспечении, часто именуются хакерами.

Хакер, получивший доступ в сеть, сразу становится источником четырех видов угроз:

1. хищение информации;
2. хищение личных данных;
3. уничтожение/изменение данных;
4. нарушение работы.

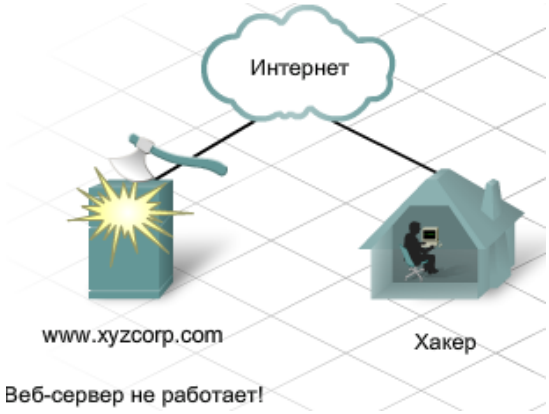


Рис. 1. Внешние угрозы

Рис. 2. Внутренние угрозы

Источники вторжения в сеть

Угроза вторжения в сеть исходит от злоумышленников, расположенных как внутри, так и за пределами организации (рис.1).

Внешние угрозы

Внешние угрозы исходят от лиц, находящихся за пределами организации и не обладающих санкционированным доступом к компьютерным системам и сетям. В этом случае атаки совершаются главным образом из Интернета, по беспроводным сетям или через серверы коммутируемого доступа.

Внутренние угрозы

Внутренние угрозы исходят от пользователей, имеющих официально разрешенный доступ в сеть с учетной записью или физический доступ к сетевому оборудованию (рис. 2). Злоумышленники, атакующие сеть изнутри, знакомы с внутренней политикой и персоналом. Кроме того, они обычно знают, какая информация представляет ценность и наиболее уязвима, а также – как получить к ней доступ.

Однако не все атаки являются преднамеренными.

В некоторых случаях, внутренняя угроза исходит от добросовестного сотрудника, который, находясь за пределами компании, стал жертвой вируса или нарушения безопасности и, впоследствии, неосознанно принес эту угрозу во внутреннюю сеть.

2. Методы атак

Вирусы

Вирус – программа, которая функционирует и распространяется путем изменения других программ и файлов. Вирус не запускается сам – он должен быть активирован. После активации действия вируса могут ограничиться простым размножением и распространением. Даже такие вирусы при всей своей простоте опасны, поскольку они способны быстро заполнить всю сво-

бодную память и остановить работу системы. Более серьезные вирусы могут быть запрограммированы на удаление или повреждение конкретных файлов перед дальнейшим распространением. Вирусы могут распространяться через вложения в электронной почте, загружаемые из Интернета файлы, системы мгновенного обмена сообщениями, а также через дискеты, компакт-диски и USB-устройства

Черви

Червь аналогичен вирусу, но, в отличие от вируса, он не присоединяется к существующей программе. Червь рассылает копии самого себя по сети на все подключенные узлы. Черви могут функционировать независимо и интенсивно распространяться. Для их работы не требуется ни активация, ни вмешательство человека. Ущерб от саморазмножающихся сетевых червей может значительно превышать последствия одного вируса. Черви способны быстро поражать значительную часть Интернета.

«Троянские кони»

«Троянским конем» называют неразмножающуюся программу, представляющую собой инструмент для атаки, замаскированный под некоторую легитимную программу. Успешное выполнение троянского коня зависит от успешности его маскировки под программу, которую пользователь согласится запустить. Троянские кони могут быть сравнительно безвредными или могут содержать код, способный повредить файлы на жестком диске пользователя. Некоторые «троянские кони» также открывают «черный ход» в систему для хакера.

В некоторых случаях злоумышленник заинтересован воспрепятствовать нормальному функционированию сети. Этот вид атак обычно выполняется с целью нарушить работу организации.

Отказ в обслуживании (DoS)-атаки

DoS-атаки представляют собой агрессивные атаки с отдельных компьютеров или групп компьютеров, препятствующие обслуживанию легитимных пользователей. DoS-атаки могут быть нацелены на пользовательские системы, серверы, маршрутизаторы и сетевые соединения.

Обычно DoS-атаки предполагают следующие вредоносные действия:

- заполнение системы или сети посторонним трафиком, блокирующим доставку легитимного трафика;
- нарушение соединения клиента с сервером для предотвращения доступа к сервису.

DoS-атаки подразделяются на несколько видов. Администраторы, отвечающие за вопросы безопасности, должны знать о видах DoS-атак, которые угрожают их сетям, и обеспечить защиту сетей. Два наиболее распространенных вида DoS-атак:

Насыщение пакетами синхронизации (SYN Flood) – к серверу направляется поток пакетов от клиента, запрашивающего установление соединения. Пакеты содержат неверные IP-адреса источников. Сервер, занятый обработкой этих фиктивных запросов, теряет способность обрабатывать легитимные запросы.

Деструктивный эхо-запрос (Ping of Death) – устройству направляется пакет эхо-запроса, размер которого превышает максимум, предусмотренный протоколом IP (65 535 байт), что может привести к сбою системы-приемника.

Распределенная DoS-атака (DDoS)

DDoS представляет собой развитие DoS-атаки со значительно большим вредоносным потенциалом. Цель состоит в насыщении и переполнении сетевых каналов бесполезными данными, но DDoS действует в гораздо большем масштабе, чем простые DoS-атаки. Жертва обычно становится получателем громадного потока трафика от сотен тысяч источников атаки. Источниками могут быть компьютеры неподозревающих пользователей, на которые ранее проникло вредоносное ПО, открывающее DDoS-атаку на целевой сайт после получения определенного сигнала.

Атаки методом грубой силы

Не все атаки, приводящие к нарушению работы сети, относятся к категории DoS. Атака методом грубой силы – другой распространенный вид атак, часто приводящий к отказу в обслуживании.

В атаках методом грубой силы используется быстродействующий компьютер для подбора паролей или дешифровки. Злоумышленник активно перебирает большое число возможных вариантов для получения доступа или извлечения ключа шифрования. Атаки методом грубой силы могут стать причиной отказа обслуживания в результате перенасыщения трафиком определенного ресурса или блокирования учетной записи пользователя.

Не все атаки ведут к ущербу или лишению легитимных пользователей доступа к ресурсам. Многие угрозы связаны со сбором сведений о пользователях, которые в дальнейшем могут использоваться для рекламы, маркетинга и анализа. Источниками таких угроз являются шпионское ПО, сеансовые идентификаторы (cookies), рекламное ПО и всплывающие окна. Не приводя к непосредственным сбоям в работе компьютера, они вторгаются в личные данные пользователя и могут раздражать своей работой.

Шпионское ПО

Шпионское ПО – программы, собирающие личные данные с компьютера пользователя без его ведома. Эти данные поступают в распоряжение рекламных агентств или других пользователей Интернета. В их числе могут оказаться пароли и банковские реквизиты.

Шпионское ПО обычно устанавливается незаметно для пользователя при загрузке файла, установке другой программы или щелчке мышью во всплывающем окне. Оно может замедлить работу компьютера и изменить внутренние параметры настройки, сделав систему более уязвимой для других угроз. Кроме того, при удалении шпионского ПО часто возникают сложности.

Сеансовые идентификаторы

Сеансовые идентификаторы (cookie) считаются одним из видов шпионского ПО, но не всегда являются вредоносными. Они фиксируют информацию о посещении сайтов определенным пользователем Интернета. Сеансовые идентификаторы могут быть полезны для персонализации настроек и других применений, экономящих время. Многие веб-сайты при подключении пользователя требуют, чтобы сеансовые идентификаторы были разрешены.

Рекламное ПО

Рекламное ПО – вид шпионского ПО для сбора сведений о пользователях, посещающих веб-сайты. Собранные сведения в дальнейшем используются для целевой рекламы. Часто рекламное ПО попадает к пользователю вместе с «бесплатным» продуктом.

Всплывающие и фоновые окна

Всплывающие и фоновые окна – это дополнительные рекламные окна, которые появляются на экране при посещении веб-сайта. В отличие от рекламного ПО, всплывающие и фоновые окна не служат для сбора сведений о пользователе и обычно связаны только с конкретным просматриваемым веб-сайтом.

Всплывающие окна: открываются перед текущим окном браузера.

Фоновые окна: отрываются за текущим окном браузера.

Они могут раздражать и обычно рекламируют продукты и услуги, не представляющие интереса.

Спам представляет собой существенную угрозу для сети и ведет к перегрузке Интернет-провайдеров, серверов электронной почты и отдельных пользовательских систем. Лица и организации, ведущие рассылку спама, называются спамерами. Для рассылки спамеры часто пользуются незащищенными серверами электронной почты. Спамеры могут взламывать домашние компьютеры посредством таких приемов, как вирусы, черви и троянские кони. После этого компьютеры начинают рассылать спам без ведома владельца.

3. Разработка мер обеспечения безопасности в сети

Обеспечение безопасности в сети является одним из наиболее важных аспектов сетевого проектирования. Безопасность часто упускается из виду при проектировании сети, поскольку она рассматривается как вопрос, относящийся скорее к функционированию сети, чем к ее проектированию. Однако рассмотрение вопросов безопасности еще до проектирования сети позволяет избежать проблем масштабирования сети и ее эффективности, которые возникают в том случае, если средства безопасности добавляются к уже законченному проекту сети.

В настоящее время для проектировщиков промышленных сетей вопросы безопасности приобретают особенную важность, поскольку значительно увеличивается количество Internet- и экстраиет-соединений, значительно вырос объем торговли в Internet и все большее количество телеработников и мобильных пользователей осуществляют доступ к сети предприятия с удаленных узлов.

Ниже перечислены этапы проектирования сети, в которых учтены требования обеспечения безопасности.

Этап 1. Идентификация оборудования сети

Этап 2. Анализ возможных рисков

Этап 3. Анализ требований безопасности и возможных компромиссных решений

Этап 4. Разработка плана мер обеспечения безопасности

Этап 5. Определение политики в сфере безопасности

Этап 6. Разработка процедур применения политики безопасности

Этап 7. Разработка стратегии технической реализации

Этап 8. Достижение соглашений о совместных действиях между пользователями, менеджерами и техническим персоналом

Этап 9. Обучение пользователей, менеджеров и технического персонала

Этап 10. Реализация технической стратегии и процедур обеспечения безопасности

Этап 11. Тестирование сети в плане безопасности и решение обнаруженных проблем

Этап 12. Поддержка комплекса мер безопасности путем периодических независимых аудитов, изучения журналов регистрации входа в сеть, принятия соответствующих мер в случае возникновения инцидентов в сфере безопасности, изучения современной литературы и уведомлений соответствующих агентств, непрерывного тестирования сети и обучения персонала, обновления плана и политики безопасности.

Идентификация сетевого оборудования и анализ рисков

Риски для сети могут вызываться разнообразными ситуациями: от враждебного вторжения в сеть до неопытного и неосторожного пользователя, который загружает Internet-приложения, содержащие вирусы. Злоумышленник, вторгшийся в есть, может похитить данные, изменить их или вызвать отказ в обслуживании легитимных пользователей (такого рода атаки, называемые «отказом в обслуживании» [denial-of-service - DoS], становятся в последние годы все более распространенными).

Кроме того, обеспечение безопасности оказывает влияние на производительность сети. Выполнение функций безопасности, таких как фильтрация пакетов и шифрование данных потребляют мощность процессора CPU и память рабочих станций, маршрутизаторов и серверов.

Шифрование может уменьшить уровень избыточности сети. если все данные должны проходить через шифрующее устройство, то оно становится узловой точкой при возможном сбое, что затрудняет решение вопросов доступности сети.

Компоненты политики безопасности

В целом в политике безопасности должны быть отражены приведенные ниже вопросы

- Политика в сфере доступа к сети (An access policy). Определяет права доступ привилегии пользователей. Она должна задавать основные правила подключения к внешним сетям, подключения к сети новых устройств и установка нового программного обеспечения в системах сети.
- Политика в сфере отчетности (An accountability policy). Определяет ответственность пользователей, операционного персонала и менеджеров. В ней должны быть описаны возможности аудита сети и способы информирования о проблемах в сфере безопасности сети.
- Политика в вопросах аутентификации (An authentication policy). С помощью эффективной политики паролей определяет, каким пользователям разрешен вход в сеть и устанавливает способы аутентификации пользователей удаленного доступа.
- Правила приобретения компьютерных технологий (Computer-technology purchasing guidelines). Описывает требования, которые должны выполняться при приобретении, конфигурировании и аудите компьютерных систем и сетей для того, чтобы они соответствовали политике безопасности компании.

Разработка процедур обеспечения безопасности

Процедуры обеспечения безопасности реализуют политику безопасности. Эти процедуры определяют процессы конфигурирования, задание имен пользователей в сети (login), аудита и поддержки сети. Процедуры безопасности должны быть написаны для конечных пользователей, сетевых администраторов и администраторов по вопросам безопасности. Эти процедуры определять действия сотрудников в случае возникновения проблем с безопасностью сети.

Механизмы обеспечения безопасности

Политика безопасности должна обеспечить централизацию мер по защите, контролю, испытанию и развитию сети. Политика безопасности реализуется посредством процедур безопасности. Процедуры регламентируют порядок настройки, регистрации пользователей, аудита и обслуживания узлов и сетевых устройств. К ним относятся как предварительные меры для снижения риска, так и активное противодействие известным угрозам безопасности. В состав процедур входят как простые и малозатратные операции (например, регулярное обновление версий ПО), так и сложные задачи создания межсетевых экранов и систем обнаружения вторжения.

Укрепление безопасности сети достигается, в частности, следующими средствами:

- исправления и обновления ПО;
- антивирусная защита;
- защита от шпионского ПО;
- средства блокировки спама;
- средства блокировки всплывающих окон;
- межсетевые экраны.

Защита, межсетевые экраны и демилитаризованные зоны

Серверы центров обработки данных могут стать целью атак злоумышленников, поэтому им необходимо обеспечить защиту.

Атаки на серверные фермы могут привести к потере сделок в приложениях типа электронной коммерции и «бизнес-бизнес», а также к утечке сведений. Необходимо обеспечить защиту как для локальных сетей (LAN), так и для сетей хранения данных (SAN), чтобы ограничить тем самым возможность таких атак. Злоумышленники используют ряд средств для наблюдения за сетями, вторжения и произведения атак типа отказ в обслуживании (DoS).

Защита серверных ферм от атак

Развертывание межсетевых экранов часто производится для обеспечения базового уровня защиты - при попытке внутренних и внешних пользователей выйти в сеть Интернет через серверную ферму (рис. 3). Для надежной защиты серверных ферм необходим более основательный подход. При таком подходе используются возможности следующих сетевых продуктов, которые можно развернуть на серверной ферме:

- межсетевые экраны;
- функции защиты коммутаторов LAN;
- системы обнаружения и предотвращения узловых и сетевых вторжений;
- средства распределения нагрузки;
- устройства анализа сети и управления сетью.

Межсетевые экраны

Помимо защиты отдельных компьютеров и серверов, подключенных к сети, необходимо контролировать прохождение трафика через сеть в различных направлениях.

Межсетевой экран представляет собой одно из наиболее эффективных средств безопасности, защищающее пользователей сети от внешних угроз. Межсетевой экран разделяет две сети или более и контролирует проходящий между ними трафик, одновременно предотвращая несанкционированный доступ. Решения для межсетевых экранов разрешают или запрещают прохождение пакетов в сеть, используя различные технологии контроля.

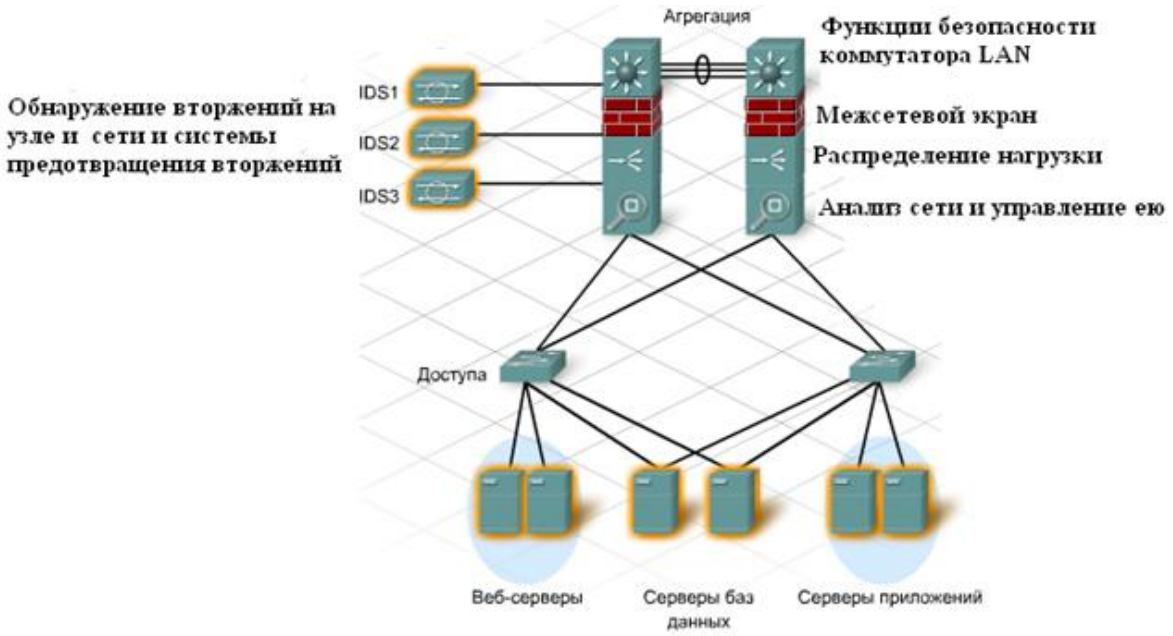


Рис. 3. Защита серверных ферм

Фильтрация пакетов - запрет или разрешение доступа на основе IP- или MAC-адресов.

Фильтрация по приложениям и веб-сайтам - запрет или разрешение доступа в зависимости от приложений. Предусмотрено блокирование веб-сайтов с указанием их URL-адреса или ключевых слов.

Динамический анализ пакетов (SPI) - входящие пакеты должны представлять собой легитимные отклики на запросы внутренних узлов. Незапрошенные пакеты блокируются, если они не разрешены в явном виде. SPI также позволяет распознавать и блокировать конкретные виды атак, например DoS.

Межсетевые экраны поддерживают один или несколько подобных механизмов фильтрации и блокирования. Кроме того, межсетевые экраны часто выполняют трансляцию сетевых адресов (NAT). NAT преобразует внутренние адреса и группы адресов во внешние глобальные адреса, используемые для пересылки по сети. При этом внутренние IP-адреса скрываются от внешних пользователей.

Решения для межсетевых экранов поставляются в различных формах:

Аппаратные межсетевые экраны. Аппаратный межсетевой экран – это выделенное устройство, называемое устройством защиты.

Серверные межсетевые экраны. Серверный межсетевой экран представляет собой приложение межсетевого экрана, выполняемое в сетевой операционной системе (NOS), например UNIX, Windows или Novell.

Интегрированные межсетевые экраны. Интегрированный межсетевой экран дополняет возможности существующего устройства (например, маршрутизатора) функциями межсетевого экрана.

Персональные межсетевые экраны. Персональные межсетевые экраны размещаются на узлах и не рассчитаны на защиту локальной сети в целом. Они могут быть реализованы в ОС по умолчанию или установлены сторонним поставщиком.

Использование межсетевых экранов

Конфигурация с одним межсетевым экраном

Один межсетевой экран делит сетевое пространство на три зоны: внешняя сеть, внутренняя сеть и DMZ. Весь трафик поступает на межсетевой экран из внешней сети. Межсетевой экран должен контролировать трафик и принимать решение о его пересылке в DMZ или во внутреннюю сеть, либо о запрете пересылки (рис.4).

Конфигурация с двумя межсетевыми экранами.

В конфигурации с двумя межсетевыми экранами предусмотрены внутренний и внешний межсетевой экраны, между которыми располагается DMZ (рис. 5). Внешний межсетевой экран применяет менее строгие ограничения и разрешает доступ пользователей из Интернета в DMZ, а также сквозное прохождение трафика, запрошенного внутренними пользователями.

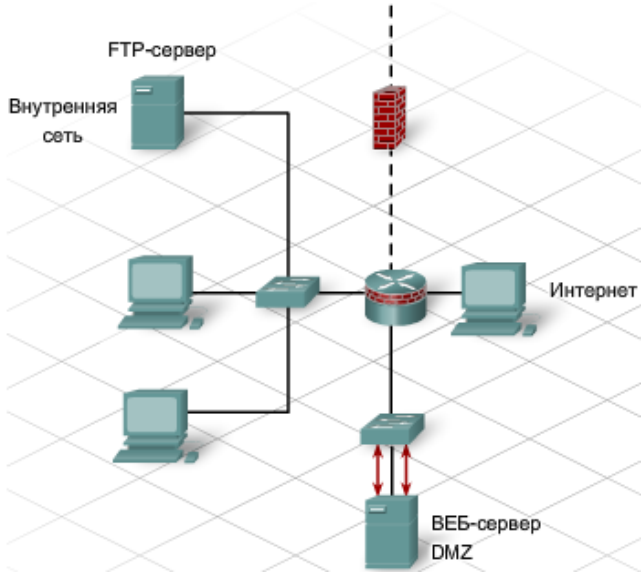


Рис. 4. Настрока одного межсетового экрана

Внутренний межсетевой экран применяет более строгие ограничения и защищает внутреннюю сеть от несанкционированного доступа.

Для небольших сетей с низким трафиком подходит конфигурация на основе одного межсетевого экрана, который, однако, является критической точкой отказа и может оказаться перегруженным.

Конфигурация с двумя межсетевыми экранами целесообразна для крупных и сложных сетей со значительно большими объемами трафика.

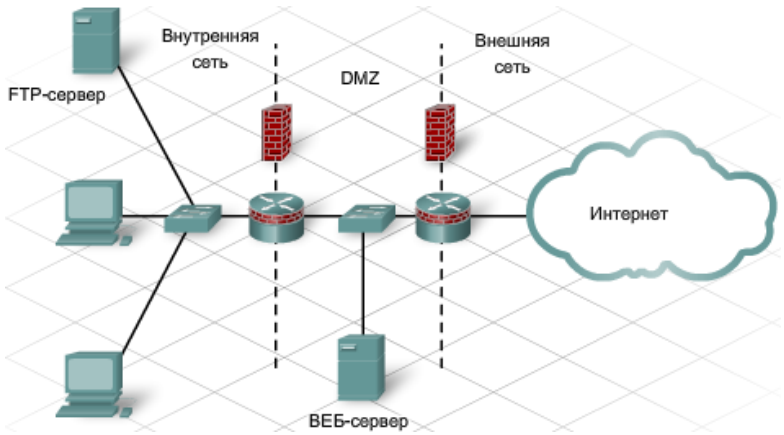


Рис. 5. Настрока двух межсетовых экранов

Во многих устройствах для домашних сетей, например интегрированных маршрутизаторах, часто имеются многофункциональные программные межсетевые экраны. Такие межсетевые экраны обычно реализуют трансляцию сетевых адресов (NAT), динамический анализ пакетов (SPI), а также фильтрацию по IP-адресам, приложениям и веб-сайтам. Дополнительно они поддерживают функции DMZ.

Интегрированный маршрутизатор позволяет настроить примитивную DMZ для доступа к внутреннему серверу с узлов за пределами сети. Для этого сервер должен иметь статический IP-адрес, который указывается в конфигурации DMZ. Интегрированный маршрутизатор изолирует трафик, пересылаемый на указанный IP-адрес. Этот трафик пропускается только на тот порт

коммутатора, к которому подключен сервер. На все остальные узлы по-прежнему распространяется защита межсетевого экрана.

При активации DMZ в простейшем виде внешние узлы получают доступ ко всем портам сервера, например 80 (HTTP), 21 (FTP) и 110 (POP3 для электронной почты).

Функция переадресации портов позволяет настроить более строгую конфигурацию DMZ. В этом случае указываются порты, которые должны быть доступны на сервере. Пропускается только трафик, направленный на эти порты. Весь остальной трафик исключается.

Беспроводная точка доступа в составе интегрированного маршрутизатора часто считается частью внутренней сети. Необходимо осознавать, что при работе точки доступа в незащищенном режиме все подключившиеся к ней пользователи получают доступ к внутренней защищенной сети без прохождения межсетевого экрана. Злоумышленники могут таким образом получить доступ к внутренней сети, минуя все средства защиты.

Демилитаризованные зоны

При традиционном проектировании межсетевых экранов серверы, вход на которые производился из внешних сетей, размещались в демилитаризованной зоне (DMZ). Пользователям, которые входили на эти серверы из сети Интернет или других ненадежных внешних сетей, не разрешался просмотр ресурсов, размещенных во внутренней LAN. Пользователи LAN считались надежными пользователями, и обычно у них не было больших ограничений при входе на серверы в DMZ.

Размещение межсетевого экрана в качестве граничного устройства между внутренней сетью (интранетом) и Интернетом позволяет контролировать весь исходящий и входящий Интернет-трафик и управлять его прохождением. Между внутренней и внешней сетью создается четкий защитный рубеж. Однако некоторым внешним клиентам может потребоваться доступ к внутренним ресурсам. Для этого можно предусмотреть демилитаризованную зону (DMZ).

Демилитаризованная зона – военно-политический термин, означающий территорию между двумя сторонами конфликта, в которой запрещено военное присутствие. В компьютерных сетях демилитаризованной зоной называется участок сети, доступный как внутренним, так и внешним пользователям. Он более защищен по сравнению с внешней сетью, но менее защищен по сравнению с внутренней сетью. DMZ создается посредством одного или нескольких межсетевых экранов, разграничивающих внутреннюю сеть, DMZ и внешнюю сеть. В DMZ часто размещаются веб-серверы, открытые для доступа извне.

Защита от внутренних атак

Сегодня атаки, исходящие из внутренней сети, более распространены, чем атаки из внешних источников. Вследствие этого обеспечение защиты серверных ферм отличается от прошлой модели DMZ. Между серверами и внутренними сетями, а также между серверами и внешними пользователями должен быть предусмотрен уровень функций межсетевых экранов и защиты от вторжений. Кроме того, может понадобиться дополнительный уровень защиты между серверами.

Политика безопасности для серверной фермы обусловлена секретностью данных, которые хранятся на серверах и содержатся в операциях сети.

Высокая доступность

Обеспечение высокой доступности

Помимо дополнительного уровня защиты серверным фермам обычно требуется высокая доступность для сетевых приложений и служб. Сеть с высокой доступностью - это сеть, в которой устранено или снижено потенциальное воздействие сбоев. Эта защита позволяет сети выполнять требования относительно доступа к приложениям, системам и данным из любой точки и в любое время.

Создание резервирования

Чтобы достичь высокой доступности, серверы подключаются с резервированием к двум отдельным коммутаторам на уровне доступа. Это резервирование обеспечивает маршрут от сервера к вторичному коммутатору при отказе первичного. С резервированием подключаются и устройства на уровне распределения и центральном уровне в сети серверной фермы. Протоколы связующего дерева, подобные быстрому протоколу связующего дерева (RSTP+), управляют резервными каналами уровня 2. Протокол маршрутизатора горячего резервирования (HSRP) и протоколы маршрутизации уровня 3 поддерживают резервирование и переключение при отказе.

Аутентификация

В процессе аутентификации определяется кто запрашивает сетевые службы. Термин *аутентификация (authentication)* обычно относится к аутентификации пользователей, однако может также относиться к процессам, выполняемым программным обеспечением. Например, некоторые протоколы маршрутизации поддерживают *аутентификацию маршрутов,* в процессе которой маршрутизатор, рассылающий обновления маршрутизации, должен удовлетворять некоторым критериям, чтобы эти обновления были приняты другим маршрутизатором.

В большинстве случаев политика безопасности требует, чтобы пользователь ввел свой идентификатор ID (login ID) и пароль, по отношению к которым сервер безопасности выполняет аутентификацию.

Авторизация

Аутентификация контролирует, кто имеет право доступа к сетевым ресурсам, а *авторизация (authorization)* определяет, какие действия разрешены пользователю или процессу после получения доступа к сетевым ресурсам. Авторизация позволяет администратору в сфере безопасности управлять отдельными частями сети, такими как каталоги и файлы на серверах.

Шифрование данных

Под *шифрованием* понимается процесс кодировки данных для того, чтобы они могли быть прочитаны только предполагаемым получателем. *Шифрующее устройство* выполняет такую кодировку перед передачей данных в сеть. *Дешифрующее устройство* осуществляет операцию, обратную первоначальной кодировке данных перед передачей их приложению. В качестве шифрующего или дешифрующего устройства может выступать маршрутизатор, сервер, конечная система или выделенное устройство.

Шифрование включает в себя два перечисленных ниже компонента.

Алгоритм шифрования (Encryption algorithm). Набор инструкций, используемых для кодирования и декодирования данных

Ключ шифрования (Encryption key). Код, используемый алгоритмом для кодировки и декодирования данных.

Фильтры пакетов

Фильтры пакетов могут устанавливаться на маршрутизаторах и серверах для того, что бы принимать или отвергать пакеты с конкретных адресов или от заданных служб. Фильтры пакетов усиливают действие механизмов аутентификации и авторизации. Они помогают защитить сетевые ресурсы от несанкционированного использования, кражи информации, от разрушения данных и DoS-атак.

Брандмауэры

Брандмауэром (firewall) называют систему или комбинацию систем, которые усиливают политику безопасности на границе между двумя или более сетями. В качестве брандмауэра может выступать маршрутизатор со списками управления доступом, выделенное аппаратное устройство или программное обеспечение, работающее на персональном компьютере или UNIX-системе. Применение брандмауэров особо важно на границе между сетью предприятия и глобальной сетью Internet.

Обнаружение вторжений в сеть

Под обнаружением вторжений (Intrusion Detection) понимается мониторинг работы сети в реальном времени и анализ получаемых данных для нахождения уязвимых мест и регистрации возможных атак на сеть. Также могут быть обнаружены в реальном времени и немедленно пресечены несанкционированные действия внутренних, авторизованных пользователей, такие как попытки передать конфиденциальные документы по сети Internet или незаконно изменить привилегии доступа к сети. Аналогичные меры могут «быть предприняты против внешнего злоумышленника, пытающегося «взломать» сеть.

Эффективная система защиты от вторжений имеет приведенные ниже характеристики.

1. Она должна постоянно функционировать без вмешательства человека. Система должна быть достаточно надежна, чтобы работать в фоновом режиме системы, за которой ведется наблюдение.
2. Она должна быть устойчива к ошибкам, т.е. не утрачивать работоспособность в случае сбоев в системе и не требовать повторного построения базы данных при перезагрузке системы.
3. Система должна противостоять попыткам вывести ее из строя. Для того, чтобы удостовериться в том, что такие попытки не предпринимаются, система может осуществлять мониторинг себя самой.
4. Она должна вызывать минимальный объем передачи по системе служебных данных. Не следует использовать системы, значительно замедляющие работу компьютера.
5. Система должна фиксировать отклонения от нормального поведения и немедленно информировать требуемых лиц в случае ненормального поведения.
6. Она должна корректировать свое функционирование в соответствии с изменениями в работе сети, происходящими с течением времени в результате добавления новых приложений.

Антивирусное ПО (выявление вирусов)

Даже с текущими обновлениями и исправлениями ОС и приложения остаются уязвимы для атак. Любое устройство, подключенное к сети, подвержено воздействию вирусов, червей и «троянских коней». Это вредоносное ПО может повреждать код операционной системы, ухудшать производительность компьютера, модифицировать приложения и уничтожать данные.

Присутствие вируса, червя или «троянского коня» иногда можно опознать по ряду признаков:

- в работе компьютера происходят необъяснимые изменения;
- программа перестает реагировать на перемещение мыши и нажатие клавиш;
- программы самопроизвольно запускаются или прекращают работать;
- почтовая программа начинает рассылать большие объемы электронной почты;
- центральный процессор сильно загружен;
- возникают неопознанные процессы или сильно увеличивается число процессов;
- компьютер работает медленно или со сбоями.

Антивирусное ПО

Антивирусное ПО может использоваться как для профилактики, так и для реагирования. Оно предотвращает заражение, а также обнаруживает и удаляет вирусы, черви и «троянских коней». Антивирусное ПО должно быть установлено на всех компьютерах, подключенных к сети. Существует большое число антивирусных программ.

Функции, реализуемые антивирусными программами:

- проверка электронной почты: сканирование входящей и исходящей электронной почты, выявление подозрительных вложений;
- динамическое сканирование в резидентном режиме: проверка исполнимых файлов и документов при обращении к ним;
- сканирование по графику: можно составить график регулярного сканирования на предмет вирусов с проверкой конкретных накопителей;
- автоматическое обновление: проверка выхода и автоматическая загрузка описаний характеристик и признаков известных вирусов. Проверка выхода обновлений может осуществляться автоматически по графику.

Антивирусное ПО для удаления вируса должно знать его характеристики. Поэтому при выявлении вируса или признаков вируса важно сообщить об этом сетевому администратору. Это обычно делается в форме сообщения об инциденте в сети согласно политике сетевой безопасности компании.

Антиспам

Программное обеспечение для защиты узлов от спама (антиспам) обнаруживает спам и нейтрализует его, например, путем удаления или помещения в папку для несанкционированных рассылок. ПО может быть установлено локально на компьютере или на почтовом сервере. Кроме того, многие Интернет-провайдеры предлагают услуги фильтрации спама. ПО для защиты от спама неспособно распознать все виды спама, поэтому открывать поступившие сообщения следует осторожно. Другой недостаток состоит в том, что легитимные сообщения могут быть отнесены к спаму и обработаны соответствующим образом.

Помимо программных средств, для предотвращения распространения спама могут использоваться другие предупредительные меры:

- своевременное обновление ОС и приложений;
- регулярный запуск антивируса и обновление описаний вирусов;
- воздержание от пересылки подозрительной корреспонденции другим пользователям;
- воздержание от открытия вложений, в особенности если отправитель неизвестен;

- настройка правил в почтовой программе для удаления спама, преодолевшего антиспам;
- выявление источников спама и информирование системного администратора для их блокирования;
- предоставление сведений об инцидентах органам власти, расследующим несанкционированные массовые рассылки.

Защита от шпионского и рекламного ПО

Шпионское и рекламное ПО проявляет некоторые симптомы, свойственные вирусам. Осуществляя несанкционированный сбор информации, они расходуют необходимые ресурсы компьютера и ухудшают производительность. Программы для защиты от шпионского ПО способны обнаруживать и удалять шпионские приложения, а также не допускать их установки в будущем. Многие средства защиты от шпионского ПО дополнительно позволяют находить и удалять сеансовые идентификаторы, а также рекламное ПО. Защита от шпионского ПО встроена в некоторые антивирусы.

Средства блокировки всплывающих окон

ПО для блокировки всплывающих окон позволяет предотвратить появление всплывающих и фоновых окон. Функция блокирования всплывающих окон по умолчанию встроена во многие браузеры. Следует отметить, что некоторые программы и веб-страницы создают всплывающие окна, необходимые для взаимодействия с пользователем, которые не должны блокироваться. Для этого в большинстве средств блокировки предусмотрена функция отмены блокировки.

Контрольные вопросы

1. На какие виды делятся все угрозы вторжения?
2. Какие требования безопасности учитываются при проектировании сети?
3. Какие аспекты должнв учитываться в политике безопасности сети?
4. Какие существуют механизны обеспечения безопасности?
5. В чем заключаются функции DMZ и межсетевых экранов?

Глоссарий

1000BASE-LX - спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи данных 1000 Мбит/с, в которой используются длинноволновой лазер и одномодовый оптический кабель. Максимальная длина сегмента составляет 10 000 м.

1000BASE-SX - спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используется коротковолновой лазер и многомодовый оптический кабель. Максимальная длина сегмента составляет 550 м.

1000BASE-T - спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используются четыре пары UTP-кабеля категории 5 и максимальная длина сегмента составляет 100 м.

100BASE-FX - спецификация узкополосной технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используются два волокна многомодового оптического кабеля для соединений. Для нормальной синхронизации сигнала в 100BASE-FX соединение не должно превышать 400 м. Описывается стандартом IEEE 802.3.

100BASE-TX - спецификация узкополосной технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используется две пары кабеля UTP или STP. Первая пара используется для приема данных, вторая - для передачи. Для нормальной синхронизации сигнала в 100BASE-OX соединение не должно превышать 100 м. Описывается стандартом IEEE 802.3.

10BASE2 - спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется тонкий коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 185 м.

10BASE5 - спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется толстый коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 500 м.

10BASE-T - спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используются две пары кабеля типа витая пара (категории 3, 4, 5): одна пара - для передачи данных, другая - для приема. Она является частью стандарта IEEE 802.3; максимальная длина сегмента равна 100 м.

DNS (Domain Name System) - система доменных имен. Система, используемая в сети Internet для трансляции имен узлов в сетевые адреса. *IEEE (Институт инженеров по электротехнике и электронике - Institute of Electrical and Electronic Engineers)* - это профессиональная организация, деятельность которой включает в себя разработку коммуникационных и сетевых стандартов. Стандарты для LAN-сетей, разработанные Институтом IEEE, в настоящее время являются преобладающими при проектировании и эксплуатации сетей.

IP-адрес - это 32-битовый адрес, назначаемый узлу при использовании протокола TCP/IP. IP-адрес принадлежит одному из пяти классов (A, B, C, D или E) и записывается в виде четырех октетов, разделенных точками (такой формат называется точечно-десятичным). Каждый адрес состоит из номера сети, необязательного номера подсети и номера узла. Адреса сети и подсети совместно используются для маршрутизации, а адрес узла необходим для доставки информации определенному сетевому узлу внутри сети или подсети. Маска подсети используется для извлечения из IP-адреса информации о сети и подсети. Механизм бесклассовой

междоменной маршрутизации (Classless InterDomain Routing - CIDR) предоставляет новый способ представления IP-адресов и маски подсети.

MAC-адрес - это стандартизованный адрес канального уровня, необходимый каждому устройству, подключенному к локальной сети. Все устройства используют MAC-адреса, чтобы найти определенные устройства в сети, а также для создания и обновления таблиц коммутации и структур данных. Длина MAC-адресов составляет 6 байтов, контролируются они Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers - IEEE). Этот тип адреса также называют *аппаратным адресом* (hardware address), *адресом MAC-уровня* (MAC-layer address) и *физическим адресом* (physical address).

ping (Packet Internet Groper — запросчик сети Internet) - команда, используемая для отправки эхо-запроса протокола ICMP и получения на него ответа. Часто используется в IP-сетях для проверки достижимости сетевого устройства.

Автономная система - это отдельная сеть или набор сетей, находящихся под единым административным контролем

Адрес подсети - это часть IP-адреса, задающая подсеть с помощью маски подсети.

Байт. Единица измерения, которая служит для описания размеров файлов данных, размера места на диске или другом носителе информации, для описания количества данных, переданных через сеть. 1 байт равен 8 битам.

Брандмауэр (firewall) маршрутизатор или сервер доступа, выполняющий роль буфера между подсоединенными общедоступными сетями и частной корпоративной сетью.

Декапсуляция (de-encapsulation) - освобождение данных от заголовка конкретного протокола.

Домен коллизий (collision domain): в сетях Ethernet - область сети, в которой распространяются столкнувшиеся и поврежденные фреймы. Повторители и концентраторы не отфильтровывают такие поврежденные фреймы, в то время как коммутаторы локальных сетей LAN, мосты и маршрутизаторы их не пропускают.

Дуплексная передача (full duplex) - это возможность одновременной передачи данных между отправляющей и принимающей станциями в двух направлениях.

Инкапсуляция (encapsulation) - упаковка данных в заголовок конкретного протокола.

Коллизия (collision): в сетях Ethernet коллизия - столкновение фреймов, произошедшее вследствие попытки одновременной их передачи. В результате оба фрейма повреждаются при встрече в физической среде.

Коммутатор (switch) - устройство, соединяющее сегменты локальной сети LAN и использующее таблицу MAC»адресов для определения сегментов, в которые следует переслать фреймы. Такой принцип работы позволяет существенно уменьшить объем нецелесообразно рассылаемых данных. Коммутаторы работают с гораздо бо́льшими скоростями, чем мосты.

Концентратор (hub) - общая точка соединений устройств сети. Обычно концентраторы используются для подсоединения к локальной сети отдельных сегментов. Концентратор может иметь несколько портов. Когда на один из них поступает пакет, он копируется и направляется на все остальные порты концентратора, поэтому такой пакет поступает во все сегменты LAN-сети.

Локальная сеть (local area network — LAN) - высокоскоростная сеть передачи цифровых данных с низким уровнем ошибок, охватывающая относительно небольшую географическую об-

ласть (до нескольких километров). Локальные сети включают в себя рабочие станции, периферийные устройства, терминалы и другие устройства, расположенные в одном здании или в другой географически ограниченной области.

Маршрутизатор (router) - это применяемое в объединенных сетях устройство, которое передает пакеты данных между сетями на основе адреса третьего уровня (сетевого адреса). Маршрутизатор может принимать решение о выборе наилучшего маршрута доставки данных по сети.

Маршрутизация (routing) представляет собой процесс нахождения маршрута к узлуполучателю. В крупных сетях маршрутизация является весьма сложным процессом, поскольку на пути следования пакета к конечному узлу-получателю может находиться большое количество промежуточных узлов.

Маска подсети – 32-битовые маски в протоколе IP, служат для указания битов IP-адреса, использующихся в адресе подсети. Иногда их называют просто *маской*.

Материнская плата. Основная печатная плата компьютера.

Микропроцессор. Кремниевый кристалл, содержащий интегральные схемы.

Модем (modem). Устройство, которое преобразует цифровые и аналоговые сигналы. В качестве устройства передачи данных модем преобразует цифровые сигналы в аналоговые, которые затем передаются через аналоговые системы передачи данных.

В качестве приемника данных модем преобразует аналоговый сигнал в начальную цифровую форму.

Пакет - логически сгруппированная единица информации, включающая заголовок, который содержит контрольную информацию, и (зачастую) пользовательские данные. Чаще всего о пакете говорят как о модуле передачи информации сетевого уровня. Термины *дейтаграмма*, *фрейм* и *сегмент* также описывают различные логические единицы информации на разных уровнях модели OSI и на разных технологических стадиях.

Повторитель (repeater) - сетевое устройство, функционирующее на первом (физическом) уровне эталонной модели OSI. Назначение повторителя состоит в регенерации и ресинхронизации сетевых сигналов на битовом уровне, что позволяет передавать их по передающей среде на бо́льшее расстояние.

Подсеть. 1. В IP-сетях - часть сети с общим адресом подсети. Сеть делится на подсети произвольно сетевым администратором; при этом обеспечивается многоуровневая, иерархическая структура маршрутизации, в то же время нет необходимости в сложной адресации присоединенных сетей. 2. В сетях OSI – набор систем ES и IS, находящихся под контролем одного административного домена и использующих один протокол сетевого доступа.

Полудуплексная передача (half duplex) представляет собой возможность передачи данных между передающей и принимающей станциями в каждый конкретный момент времени только в одном направлении.

Постоянное запоминающее устройство (Read only memory - ROM). Тип компьютерной памяти, в которой данные предварительно записаны.

Протокол (protocol) формальное описание набора правил и соглашений, управляющих обменом информацией между устройствами сети.

Протокол Internet (Internet Protocol - IP). Протокол сетевого уровня в стеке протоколов TCP/IP; обеспечивает передачу данных между сетями без предварительной установки соединения.

Распределенная сеть (Wide Area Network - WAN) представляет собой сеть передачи данных, охватывающую значительное географическое пространство. В ней часто используются передающие устройства, предоставленные открытыми операторами связи, например, местными или государственными телефонными компаниями.

Сегмент (segment). 1. Часть сети, ограниченная мостами, маршрутизаторами или коммутаторами. 2. В спецификации протокола TCP - логически сгруппированная информация на транспортном уровне эталонной модели OSI.

Служба Telnet — стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол telnet используется для организации соединений с удаленного терминала и позволяет пользователям входить в удаленную систему и использовать ее ресурсы так, словно они подключены к локальной системе.

Таблица маршрутизации (routing table) - представляет собой некоторую разновидность базы данных, хранящуюся в маршрутизаторе или другом устройстве объединенной сети, в которой содержится информация о маршрутах к конкретным сетямполучателям и, в большинстве случаев, метрики, связанные с этими маршрутами.

Фрейм (frame) - логически сгруппированная информация, пересылаемая в виде блока данных канального уровня по среде сети.

Шина (Bus). Набор электрических цепей, через которые передаются данные от одной части компьютера другой.

ЛИТЕРАТУРА

1. Бройдо В.Л. Архитектура ЭВМ и систем. Учебник. – М.: Питер, 2009. – 720 с.
2. Олифер В., Олифер Н. Основы компьютерных сетей. Учеб.пособие. -М.: Питер, 2009. -350 с.
3. Ручкин В.Н. Архитектура компьютерных сетей. Учеб.пособие.-М.:Диалог.Мифи,2009.-340 с.
4. Пескова С.А.,Кузин А.В. Сети и телекоммуникации.Учеб.пособие.-М.:Академия,2008.-352 с.
5. Брайдо В.Л., Ильина О.П. Архитектура ЭВМ и систем. Учебник. – М.: Питер, 2008. -720 с.
6. Qaxxorov A.A. Tarmoqlarni rejalashtirish va qurish. O`quv qo`llanma. – T.: Noshir, 2012, 224 b.
7. Таненбаум Э. Архитектура компьютера. Учебник. – М.: Питер, 2007. –844 с.
8. Кушнер А.Н.Сборка сервера. Учеб.пособие. – М.: ЭКСМО, 2007. -404 с.
9. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. Учеб.пособие. -М.: Питер, 2007. -540 с.
10. Ватаманюк В. Создание, обслуживание и администрирование сетей. Учеб.пособие. – СПб, Питер, 2007. -232 с.
11. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. Учебник. -М.: Питер, 2007,-668 с.
12. Смирнова Е.В., Козик П.В. Технология современных сетей Ethtrnet. Учеб.пособие. - СПб.: БХВ-Петербург, 2012. -272 с.
13. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. Учеб.пособие. -М.: Питер, 2007. -512 с.
14. Программа сетевой академии Cisco CCNA 1 и 2 Вспомогательное руководство. Третье издание, исправленное и дополненное. Пер. с англ. – М.:- Издательский дом «Вильямс», 2008. – 1168с.: ил – парал. тит. англ.
15. Программа сетевой академии Cisco CCNA 3 и 4 Вспомогательное руководство. Третье издание, исправленное и дополненное. Пер. с англ. – М.:- Издательский дом «Вильямс», 2008. – 900с.: ил – парал. тит. англ.
16. Основы организации сетей Cisco, том 1.: Пер. с англ. — М. : Издательский дом «Вильямс», 2002. — 569 с.: ил. — Парал. тит. англ.
17. Основы организации сетей Cisco, том 2.: Пер. с англ. — М. : Издательский дом «Вильямс», 2002. — 464 с.: ил. — Парал. тит. англ.
18. Электронный Учебный курс Cisco Network Academy. CCNA Discovery 1. Сети для домашних пользователей и малых предприятий. 2007 г.
19. Электронный Учебный курс Cisco Network Academy. CCNA Discovery 2. Работа на малых и средних предприятиях и у Интернет-провайдера. 2007 г.
20. Электронный Учебный курс Cisco Network Academy. CCNA Discovery 3. Введение в маршрутизацию и коммутацию на предприятии. 2007 г.
21. Электронный Учебный курс Cisco Network Academy. CCNA Discovery 4. Проектирование и поддержка компьютерных сетей. 2007 г.