Конспект лекций

по дисциплине **«КОМПЬЮТЕРНЫЕ СЕТИ»**
для студентов специальности
1-40 05 01 «Информационные системы и технологии (в проектировании и производстве)»

Тема 1. Определение компьютерной сети. Обобщенная схема. Классификация, характеристики компьютерных сетей.

Компьютер в настоящее время – это привычный атрибут как на рабочем месте в офисе, в научно-исследовательской лаборатории, так и в домашней обстановке.

Совместное использование нескольких компьютеров, терминалов, других периферийных устройств можно уже назвать компьютерной сетью.

Но компьютерные сети появились не сразу.

Эволюция комьютерных сетей.

В первые два десятилетия своего существования компьютерные системы были сильно централизованными и располагались, как правило, в пределах одного помещения.

Первые компьютера 50-х годов- большие, громоздкие и дорогие – предназначались для очень небольшого числа избранных пользователей. Часто эти монстры занимали целые здания.

Следующий важный период развития компьютерных систем относится к 1965-1975 годам.

В это время в технической базе вычислительных машин произошел переход от отдельных полупроводниковых элементов типа транзисторов к интегральным микросхемам, что открыло путь к появлению следующего поколения компьютеров. Большие функциональные возможности интегральных схем сделали возможным реализацию на практике сложных компьютерных архитектур, таких, например, как IBM/360.

Начали развиваться интерактивные многотерминальные системы разделения времени. В таких системах компьютер отдавался в распоряжение сразу нескольким пользователям. Каждый пользователь получал в свое распоряжение терминал, с помощью которого он мог вести диалог с компьютером. Причем время реакции вычислительной системы было достаточно мало для того, для того, чтобы пользователю была не слишком заметна параллельная работа с компьютером и других пользователей.

Алфавитно-цифровые терминалы располагались как правило в одном здании, но со временем возникла необходимость получать доступ к мощному компьютеру (мэйнфрейму) удаленно за сотни и тысячи километров.

Терминалы соединялись с компьютерами через телефонные сети с помощью модемов. Такие сети позволяли многочисленным пользователям получать удаленный доступ к разделяемым ресурсам нескольких мощных

компьютеров класса суперЭВМ. Затем появились системы, в которых наряду с удаленными соединениями типа терминал–компьютер были реализованы и удаленные связи типа компьютер–компьютер.

Таким образом, хронологически первыми появились глобальные вычислительные сети. Именно при построении глобальных сетей были впервые предложены и отработаны многие основные идеи и концепции современных вычислительных сетей. Такие, например, как многоуровневое построение коммуникационных протоколов, технология коммутации пакетов, маршрутизация пакетов в составных сетях.

В середине 70-х появились большие интегральные схемы. Их сравнительно невысокая стоимость и высокие функциональные возможности привели к созданию мини-компьютеров, которые стали реальными конкурентами мэйнфреймов. Многие предприятия стали приобретать несколько мини-компьютеров, по одному в каждый отдел. В конце 70-х, в начале 80-х стали стремиться соединять мини-компьютеры между собой, таким образом возникли первые локальные сети.

В середине 80-х годов положение дел в локальных сетях стало кардинально меняться. Утвердились стандартные технологии объединения компьютеров в сеть – Ethernet, Arcnet, Token Ring. Мощным стимулом для их развития послужили персональные компьютеры. Эти массовые продукты явились идеальными элементами для построения сетей – с одной стороны, они были достаточно мощными для работы сетевого программного обеспечения, а с другой – явно нуждались в объединении своей вычислительной мощности для решения сложных задач, а также разделения дорогих периферийных устройств и дисковых массивов.

Модель, в которой один компьютер выполнял всю необходимую работу по обработке данных, уступила место модели, состоящей из большого количество отдельных, но связанных между собой компьютеров. Такие системы называются компьютерными сетями.

Рассмотрим какие цели достигаются при применении компьютерных сетей и вкратце общие принципы, и методы обмена данными и построения компьютерных сетей.

В первую очередь.

Пользователи компьютерных сетей получают доступ к общим ресурсам, таким как сетевые принтеры, дисковые накопители, модемы и факс модемы, сканеры, устройства записи компакт-дисков и пр.

Но, наиболее более важной проблемой, является ***совместное использование информации***. В наше время любая компания, независимо от ее размеров, просто немыслима без данных, представленных в электронном виде. Большинство предприятий старается вести базу данных клиентов, товаров, счетов, финансовых операций, очень часто требуется налоговая информация и многое другое.

В маленьких компаниях все компьютеры обычно собраны в пределах одного офиса или, в крайнем случае, одного здания. Если же речь идет о больших фирмах, то и вычислительная техника, и служащие могут быть

разбросаны по десяткам представительств в разных регионах страны и за её пределами. Можно сказать, ***что одной из целей сетей является быстрый и надежный доступ к информационным ресурсам за многие сотни и тысячи км***.

Проще всего информационную систему организации можно представить себе как совокупность одной или более баз данных и некоторого количества работников, которым удаленно предоставляется информация. В этом случае данные хранятся на мощном компьютере, называемом **сервером.** Довольно часто сервер располагается в отдельном помещении и обслуживается системным администратором.

Вторая цель работы компьютерной сети это коммуникационная среда для совместной деятельности работников предприятия.

При помощи сети два или более удаленных друг от друга сотрудника могут легко составить совместный отчет, находящийся на сервере. К коммуникационной среде также можно отнести и электронную почту, видеоконференции, Skype, социальные сети, виртуальные доски и т.п.

Третья цель применения компьютерных сетей – это взаимодействие с другими компаниями. Особенно это касается взаимоотношений типа «поставщик-клиент». Заказы могут формироваться строго в соответствии с производственными нуждами, что позволяет резко повысить эффективность.

Четвертая цель – это интернет-коммерция. Эта область сейчас является очень перспективной и быстро развивающейся. Через Интернет уже можно приобретать практически любые товары.

Пятая цель – это Интернет – банкинг,. - платежи, переводы денег можно выполнить не выходя из дома - т.е. предоставление банковских услуг.

Шестая цель – создание и размещение различной рекламной информации на просторах Интернета виде WEB – сайтов.

Седьмая цель – дистанционное обучение – интерактивные WWW – сайты, содержащие учебные материалы, лекции, методические пособия, вопросы для само проверки, контрольные задания и зачастую выполняющая роль экзаменатора.

Определения и термины компьютерные сети

Компьютерная сеть (вычислительная сеть, сеть передачи данных)– это совокупность узлов и телекоммуникационного оборудования, объединенных между собой каким-либо способом с целью совместного доступа к ресурсам и обмена информацией обеспечивающая информационный обмен компьютеров в сети.

Компьютерные сети – объединение компьютеров и средств связи.

1. **Узел, абонент, хост** - устройство, непосредственно подключенное к сети. Сюда можно отнести сервер, рабочую станцию, ноутбук, планшет, смартфон, терминалы, периферийные устройства (принтера, сканеры, плоттеры и пр.);

2. **Телекоммуникационное оборудование** – концентраторы хабы (Hub's), коммутаторы (switch's), маршрутизаторы (router's), устройства первичной сети (мультиплексоры и пр. устройства), модемы (аналоговые и цифровые - ADSL).

3. **Сервер** - специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам свои ресурсы (файлы данных, накопители, процессорное время и т.д.).

4. **Клиентский компьютер (рабочая станция)** - компьютер пользователя сети, получающий доступ к ресурсам сервера (серверов).

5. **Среда передачи** (канал связи, линия связи) - физическая среда распространения сигналов от источника к приемнику.

6. **Пропускная способность** - максимально возможная скорость передачи данных по линии связи.

7. **Сегмент сети** - логически или физически обособленная часть сети.

8. Сегментация сети - разделения сети на сегменты с целью уменьшения **в** них количества узлов, увеличения пропускной способности в расчете на один узел и повышения безопасности.

Обобщенная схема.

Для того чтобы понять какие принципы лежат в основе построения и функционирования компьютерных сетей, рассмотрим простейший случай соединения двух компьютеров с целью общего доступа к файлам, принтерам и другим ресурсам называемое прямым соединением

Во-первых, автономно работающие компьютеры необходимо физически соединить друг с другом, т.е. создать между ними линию связи, по которой будут передаваться данные и команды в форме электрических сигналов. Для этого на каждый компьютер устанавливается специальный аппаратный модуль, называемый сетевым адаптером или сетевой картой (в пользовательских компьютерах они, как правило, встроены в материнские платы). Сетевые карты связываются между собой кабелем, который подсоединяется к ним через соответствующие разъемы.

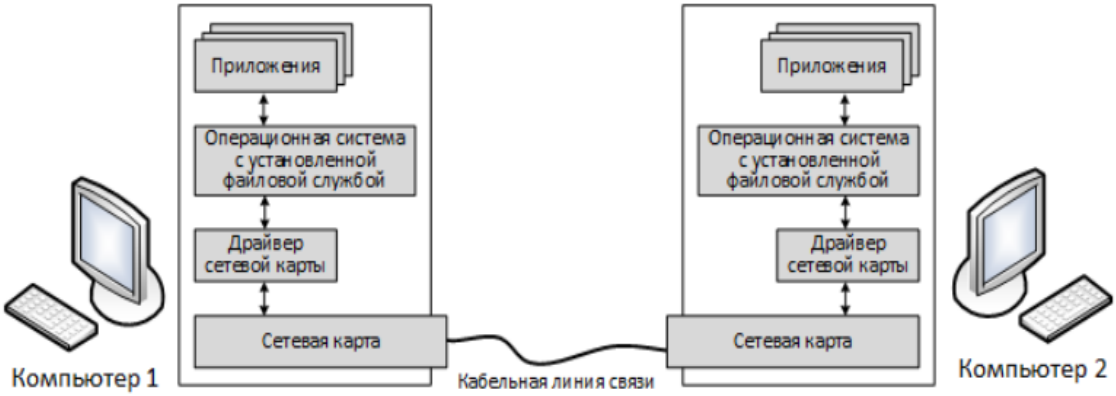


Рисунок 1.1. Прямое соединение двух компьютеров

Чтобы операционная система и другие программы могли управлять сетевой картой и пользоваться её функциями, на каждом компьютере устанавливается специальная служебная программа – драйвер сетевой карты. Кроме этого, как говорилось выше, для доступа приложений и пользователей к разделяемым ресурсам на компьютерах должны быть установлены клиентский и серверный программные модули. В нашем случае, когда разделяемыми ресурсами являются файлы, эти модули образуют сетевую файловую службу, которая в самом простом варианте может быть встроена в операционную систему.

Как видим (Рисунок 1.1), в каждом отдельно взятом компьютере взаимодействие между приложениями, операционной системой, файловой службой, драйвером сетевой карты, самим устройством и линией передачи данных осуществляется на разных уровнях. На каждом из уровней соответствующее устройство или программа выполняет свой набор функций: физическую передачу данных по линии связи, обработку электрических сигналов в информационные, обработку возникающих ошибок, объединение отдельных информационных сигналов в целые сообщения, передачу этих сообщений определенному приложению и т. п. Важно, чтобы весь обмен сообщениями между разными уровнями одного компьютера или одинаковыми уровнями разных компьютеров осуществлялся по определенным правилам. Наборы таких правил называются протоколами компьютерных сетей.

Таким образом, для создания компьютерной сети в общем случае необходимо: наличие линии связи между компьютерами, специальное аппаратное обеспечение - сетевое оборудование, специальные программные средства - сетевое программное обеспечение, и протоколы взаимодействия компонентов в сети.

Соединение двух автономных компьютеров является примером простейшей компьютерной сети. В действительности даже небольшая локальная сеть организации объединяет множество вычислительных устройств, а при создании протяженных сетей используется дополнительное сетевое оборудование и развитые технологии передачи данных.

Как видно из рисунка 1.3 передача данных в компьютерных сетях – это сложный процесс, который происходит поэтапно или как принято говорить по уровням.

Рассмотрим на каких уровнях и каким образом осуществляется взаимодействие компьютеров (пользователей) друг с другом.

На самом верхнем уровне компьютеров имеются сетевые приложения, такие как браузер, скайп, электронная почта, программы для скачивания файлов (например, Download Master), торрентов и др. Но чтобы наши сообщения, запросы достигали цели на самом нижнем уровне должна присутствовать физическая среда передачи данных: медный или оптический кабель и радиоволны.

Самый верхний уровень – уровень приложений принято называть «Прикладным уровнем», а самый нижний уровень «Физическим уровнем».

Между верхним – «Прикладным уровнем» и нижнем «Физическим уровнем», различает как минимум еще три промежуточных уровня: Транспортный, Сетевой (межсетевой) и Канальный (аппаратный) – Рисунок 1.4.

Представленная на рисунке 1.4. схема взаимодействия узлов (host) в сети является не много модифицированной моделью TCP/IP, разработанной инженерами и специалистами сообщество Интернет. (IETF – **Internet**

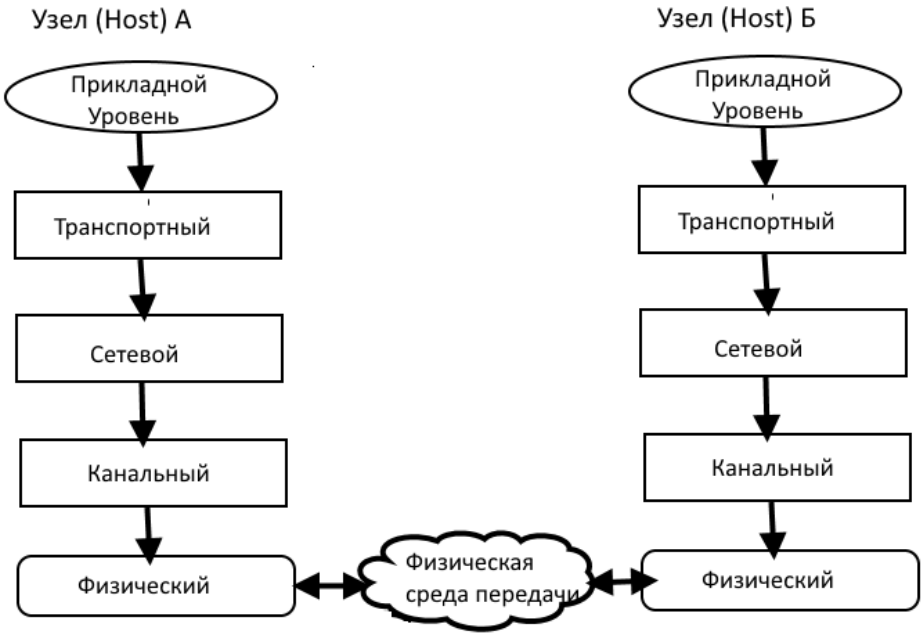


Рисунок 1.2 Схема взаимодействия узлов (host) в компьютерной сети.

Классификация компьютерных сетей.

Единой общепринятой системы, по которой классифицируются все информационные сети, не существует, однако есть ряд важных параметров, по которым можно определить к какому классу принадлежит сеть:

1. По типу технологии передачи;
2. По территориальному признаку;

3. По типу среды передачи;
4. По скорости передачи информации;
5. По типу функционального взаимодействия;
6. По типу сетевой топологии;
7. По функциональному назначению;
8. По сетевым операционным системам;

По типу технологии передачи

В общих чертах существует ***два типа технологии передачи***:

- - широковещательные сети;
- - сети с передачей от узла к узлу;

Широковещательные сети;

В ***широковещательной сети*** существует единый канал связи, для всех узлов сети – (ЭВМ, сетевых устройств). Короткие сообщения – (пакеты, кадры) посылаются одной машиной, их получают все машины. В поле адреса в пакете обозначается, адрес назначения. При получении пакета машина проверяет его адресное поле. Если пакет адресован этой машине, она его обрабатывает, остальные машины его игнорируют.

Широковещательные сети также позволяют адресовать пакет одновременно всем машинам с помощью специального кода в поле адреса (обычно все биты ="1". Такая операция называется **широковещательной передачей.**

Широковещательные системы также предоставляют возможность посылать сообщения подмножеству машин, и это называется **многоадресной передачей или групповой рассылкой.** В этом случае также применяется специфический адрес – адрес групповой рассылки.

Сети с передачей от узла к узлу;

Сети с передачей от узла к узлу, могут состоять из большого количества соединенных пар узлов (машин ЭВМ, сетевых устройств). В сети подобного типа пакету, чтобы добраться до пункта назначения, необходимо пройти через ряд промежуточных узлов. Часто при этом существует несколько возможных путей от источника до получателя, поэтому алгоритмы вычисления таких путей играют очень важную роль в сетях с передачей от узла к узлу.

Обычно небольшие, географически локализованные в одном месте сети используют широковещательную передачу, тогда как в более крупных сетях применяется передача от узла к узлу. В последнем случае имеется один отправитель и один получатель, и такую систему иногда называют **однонаправленной (одноадресной) передачей.**

По территориальному признаку.

По территориальному признаку сети делятся на:

Таблица 1-1

Расстояние между процессами	**Процессы расположены**	**Территориальная классификация**
1 м.	На одном квадратном метре	Персональная сеть.
10 м.	Комната	Локальная сеть
100 м.	Здание.	
1 км.	Кампус.	
10 км.	Город.	Глобальная сеть
100 км.	Страна.	
1000 км.	Континент.	
10 000 км.	Планета.	Интернет

В верхней строке таблицы помещаются **персональные сети,** то есть сети, предназначенные для одного человека. Далее в таблице следуют более протяженные сети.

- **Локальная сеть (Local Area Network, LAN)** - группа компьютеров, связанных друг с другом и расположенных на небольшой территории в одном офисе, здании или близко расположенных зданиях. Как правило, принадлежит одной организации.
- **Глобальная сеть (Wide Area Network, WAN)** - сеть, объединяющая компьютеры разных городов, регионов, государств. Пример: Интернет или крупная корпорация.
- **Городская сеть или сеть мегаполиса (Metropolitan Area Network, MAN)** - сеть, связывающая множество локальных сетей на территории одного города. Сочетает в себе признаки как локальной, так и глобальной сети. Пример: опорная сеть провайдера, сеть кабельного телевидения.

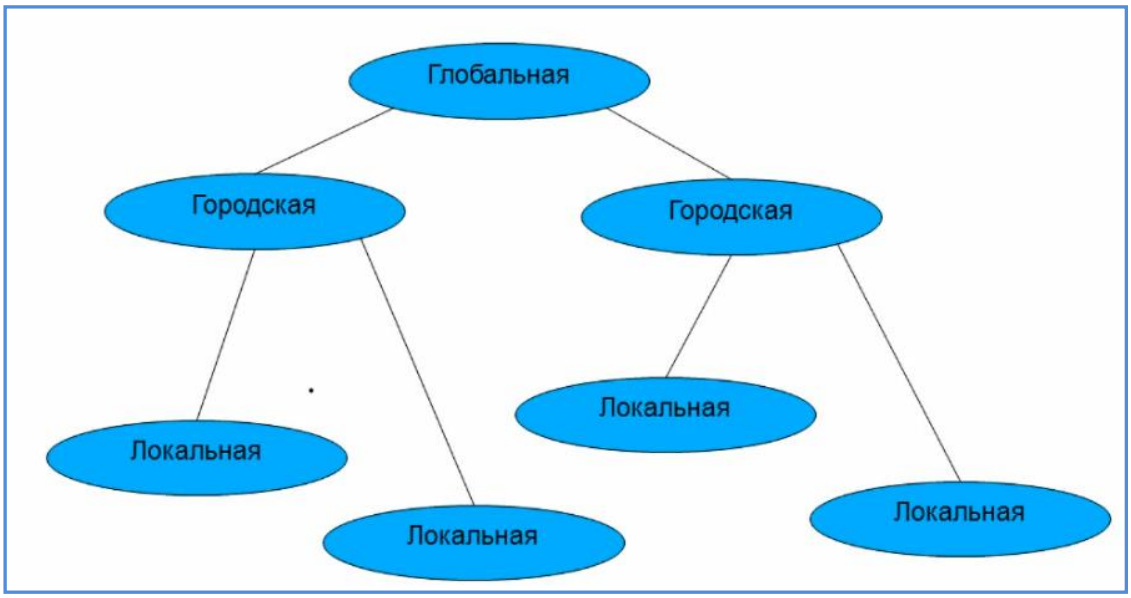


Рисунок 1.2 Пример объединения сетей.

Локальные, городские и глобальные, сети можно объединять в иерархии, т.е. хорошо масштабируемы. Локальные сети входят как абонент в городские, а городские в глобальные. (Рисунок 22.2).

Глобальные и городские сети также могут быть организованы в сложные структуры, причем на некоторых участках создаются не только иерархические, но и «петле образные» или кольцевые топологии. Самая большая сеть, которая объединяет все компьютеры в пределах планеты, является сеть Интернет.

Примером взаимодействия локальных и глобальных сетей является виртуальная частная сеть –VPN.

Виртуальная частная сеть (Virtual Private Network, VPN)- несколько

локальных сетей предприятия, объединенных через Интернет. Рисунок 22.3

Рисунок 1.3. Виртуальная частная сеть (VPN) - крупного предприятия, организованная через Интернет.

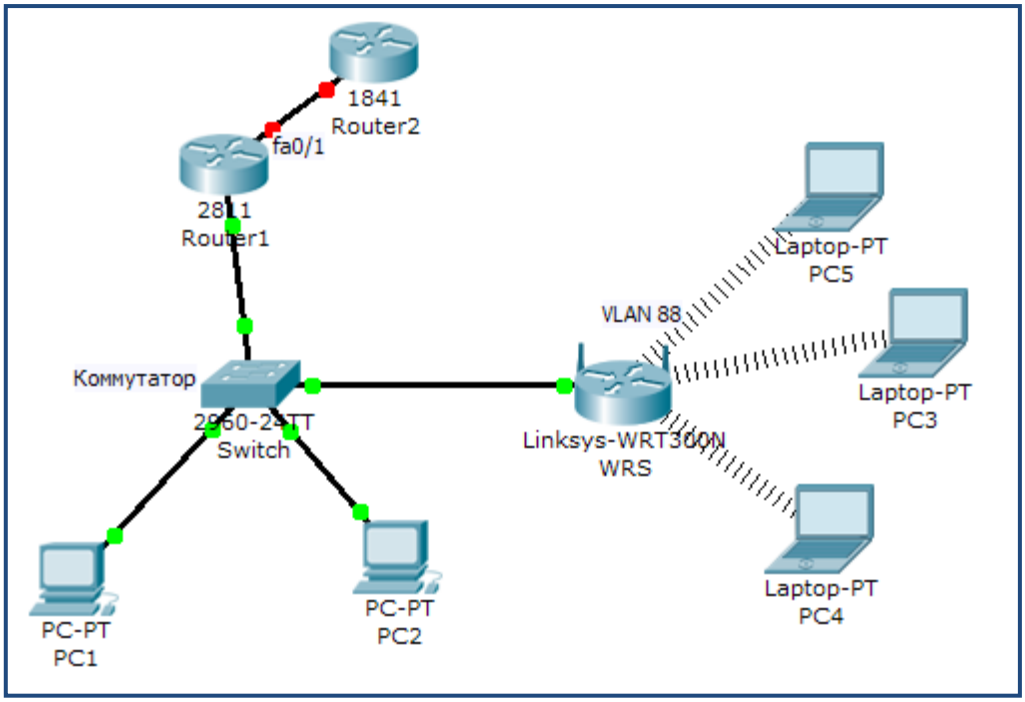


Рисунок 1.4. Фрагмент смешанной сети.

По типу среды передачи.

Компьютеры могут соединяться между собой, используя различные среды доступа:

В ***проводных сетях*** используется: телефонный кабель, витая пара, коаксиальный кабель или оптический кабель. Проводные сети используют технологии Ethernet, Token Ring, FDDI (оптические линии связи). Для соединения устройств проводных сетей часто используют телефонные линии и каналы связи, а также технологии SONET/SDH, DWDM с оптическим кабелем.

Беспроводные: Передача информации происходит по радиоволнам в определенном частотном диапазоне. Беспроводные технологии сетей - Wi-Fi, Bluetooth, GPRS, WiMax, 3G-модемы, а также радиорелейные и спутниковые каналы связи.

На практике чаще всего строятся сети смешанного типа с использованием проводных и беспроводных технологий

По скорости передачи информации.

Компьютерную сеть можно классифицировать по скорости передачи информации.

Рисунок 1.5. Классификация сетей по скорости передачи информации.

Сети делятся на низкоскоростные – до 10Мбит/с, среднескоростные до 100Мбит/с, и высокоскоростные свыше 1000 Мбит/с. К первым относятся сети LAN: классический Ethernet, Token Ring, ко вторым – Fast Ethernet, FDDI, и к третьим 1Gbit/s, 10Gb/s, 40Gb/s, 100Gb/s.

По типу функционального взаимодействия.

По типу взаимодействие сети можно разделить

- Одноранговая сеть
- Клиент-сервер
- Смешанная сеть
- Точка-точка
- Многоранговые сети

Классификация по типу сетевой топологии

Сетевая топология (от ***греч.*** τόπος, - место) – способ описания конфигурации **сети**, схема расположения и соединения сетевых устройств, схема прохождения электрических сигналов, описывающая направление потоков информации и принцип предоставления доступа к сети.

Сетевая топология может быть:

1. **физической** – описывает реальное расположение и связи между узлами сети - способ физического соединения компьютеров, узлов сети с помощью среды передачи, например, участками кабеля.
2. **логической** – описывает прохождение сигнала в рамках физической топологии. Таким образом, логическая топология описывает пути передачи потоков данных между сетевыми устройствами и определяет направление и способ передачи, а не схему соединения физических проводников.

Логическая топология в свою очередь подразделяется на:

- **информационную** – описывает направление потоков информации, передаваемых по сети;
- **и управления обменом** – это принцип передачи права на пользование сетью.

Существует множество способов соединения сетевых устройств.

Выделяют 3 базовых топологии:

- **Шина**
- **Звезда**
- **Кольцо**

И дополнительные (производные):

- ***Дерево***

- ***Двойное кольцо***
- ***Решётка***
- ***Полно связная***
- ***Ячеистая топология***

По функциональному назначению

- Сети хранения данных
- Серверные фермы
- Сети управления процессом
- Сети SOHO

По сетевым операционным системам ОС

- На основе Windows
- На основе UNIX
- На основе NetWare
- Смешанные

UNIX– группа переносимых, многозадачных и многопользовательских операционных систем.

Первая система UNIX была разработана в 1969 г. в подразделении Bell Labs компании AT&T. С тех пор было создано большое количество различных UNIX-систем. Юридически лишь некоторые из них имеют полное право называться «UNIX»; остальные же, хотя и используют сходные концепции и технологии, объединяются термином *«UNIX-подобные»* (*Unix-like*).

Некоторые отличительные признаки UNIX-систем включают в себя:

- использование простых текстовых файлов для настройки и управления системой;
- широкое применение утилит, запускаемых в командной строке;
- взаимодействие с пользователем посредством виртуального устройства – терминала;
- представление физических и виртуальных устройств и некоторых средств межпроцессового взаимодействия как файлов;
- использование конвейеров из нескольких программ, каждая из которых выполняет одну задачу.

В настоящее время UNIX используются в основном на серверах, а также как встроенные системы для различного оборудования. На рынке ОС для рабочих станций и домашнего применения UNIX уступили другим операционным системам, таким как Microsoft Windows и Mac OS, хотя существующие программные решения для Unix-систем позволяют реализовать

полноценные рабочие станции как для офисного, так и для домашнего использования.

В ходе разработки Unix-систем был создан язык Си.

NetWare – сетевая операционная система и набор сетевых протоколов, которые используются в этой системе для взаимодействия с компьютерами-клиентами, подключёнными к сети. Операционная система NetWare создана компанией Novell. NetWare является закрытой операционной системой, использующей кооперативную многозадачность для выполнения различных служб на компьютерах с архитектурой Intel x86. В основе сетевых протоколов системы лежит стек протоколов Xerox XNS. NetWare является одним из семейств XNS-систем.

Тема 2 Понятие протокола и применение сетевых протоколов для взаимодействия объектов сети.

Взаимодействие сетевых узлов состоит из множества достаточно сложных процессов и является сложной задачей.

Для решения сложных задач используется известный универсальный прием – декомпозиция, то есть разбиение одной сложной задачи на несколько более простых задач-модулей. Декомпозиция состоит в четком определении функций каждого модуля, а также порядка их взаимодействия (то есть межмодульных интерфейсов).

После представления исходной задачи в виде множества модулей эти модули можно сгруппировать и распределить **по уровням**, образующим иерархию. С учетом иерархии для каждого уровня можно указать непосредственно примыкающие к нему соседние вышележащий и нижележащий уровни и связи между ними. (Рисунок 2.1).

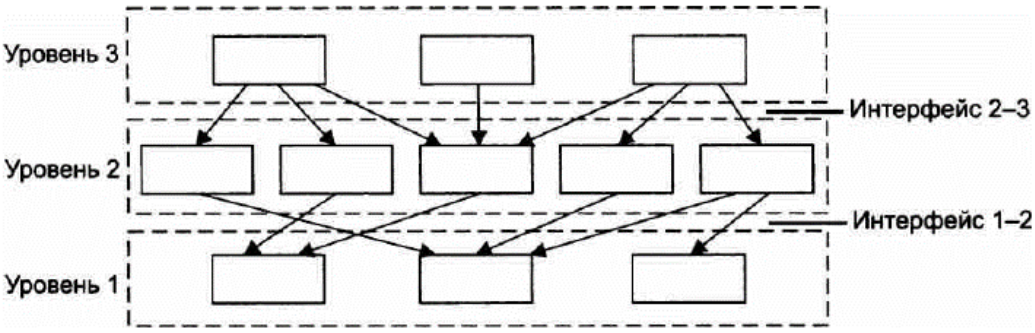


Рисунок 2.1 Многоуровневый подход – создание иерархии задач.

Протокол и стек протоколов

При рассмотрении средств сетевого взаимодействия, необходимо учитывать, что в процессе обмена сообщениями участвуют по меньшей мере две стороны, то есть в данном случае необходимо организовать согласованную работу двух иерархий аппаратных и программных средств на разных компьютерах. Оба участника сетевого обмена должны согласовать уровни и форму электрических сигналов, способ определения размера сообщений,

договориться о методах контроля достоверности и т. п. Другими словами, соглашения должны быть приняты на всех уровнях, начиная от самого низкого – уровня передачи битов, и заканчивая самым высоким, реализующим обслуживание пользователей сети.

На рисунке 3.2 показана модель взаимодействия двух узлов. С каждой стороны средства взаимодействия представлены четырьмя уровнями. Каждый уровень поддерживает интерфейсы двух типов. Во-первых, это интерфейсы услуг с выше и нижележащим уровнями «своей» иерархии средств (по вертикали). Во-вторых, это интерфейс со средствами взаимодействия другой стороны, расположенными на том же уровне иерархии (по горизонтали). ***Этот тип интерфейса называют протоколом***.

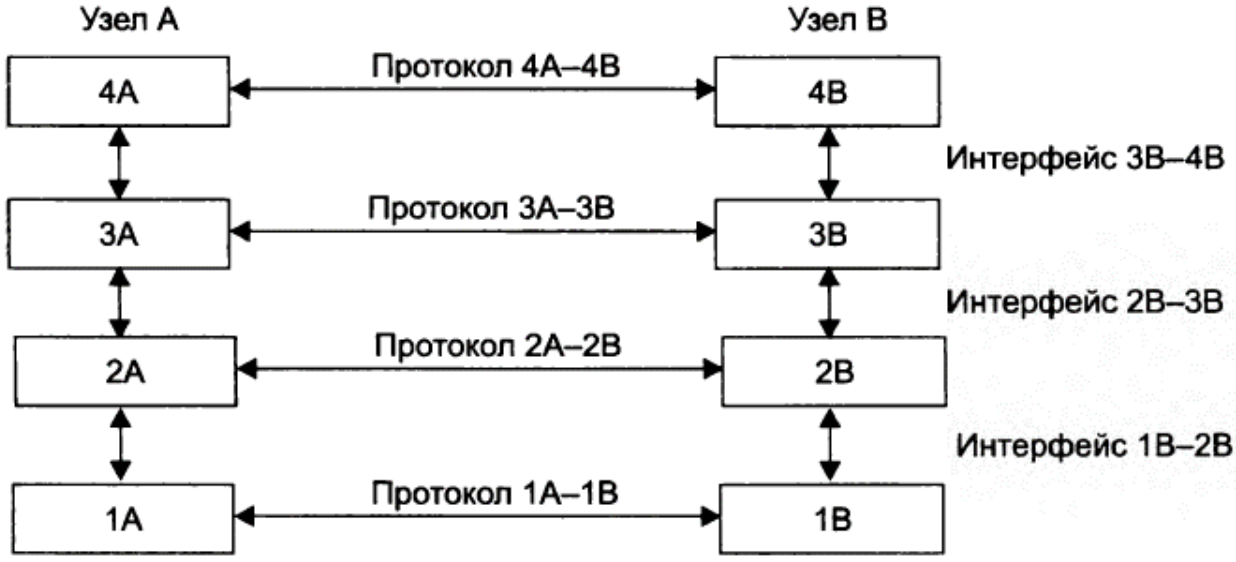


Рисунок 2.2 Взаимодействие двух узлов

Таким образом – ***протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы – правила взаимодействия модулей соседних уровней в одном узле***.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком протоколов.

Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, программными средствами.

Программный модуль, реализующий некоторый протокол, называют протокольной сущностью, или, для краткости, тоже протоколом.

При сравнении протоколов следует учитывать не только логику их работы, но и качество программной реализации. Более того, на эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, в частности то, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними.

Протокольные сущности одного уровня двух взаимодействующих сторон обмениваются сообщениями в соответствии с определенным для них протоколом. Сообщения состоят из заголовка и поля данных (иногда оно может отсутствовать). Обмен сообщениями является своеобразным языком общения, с помощью которого каждая из сторон «объясняет» другой стороне, что необходимо сделать на каждом этапе взаимодействия. Работа каждого протокольного модуля состоит в интерпретации заголовков, поступающих к нему сообщений и выполнении связанных с этим действий. Заголовки сообщений разных протоколов имеют разную структуру, что соответствует различиям в их функциональности. Понятно, что чем сложнее структура заголовка сообщения, тем более сложные функции возложены на соответствующий протокол.

Модель OSI

На практике при реализации сетей стремятся использовать стандартные протоколы. Это могут быть фирменные, национальные или международные стандарты.

В начале 80-х годов ряд международных организаций по стандартизации, в частности International Organization for Standardization (ISO), часто называемая International Standards Organization, а также International Telecommunications Union (ITU) и некоторые другие, разработали стандартную модель взаимодействия открытых систем (Open System Interconnection, OSI). Эта модель сыграла значительную роль в развитии компьютерных сетей.

Общая характеристика модели OSI

К концу 70-х годов в мире уже существовало большое количество фирменных стеков коммуникационных протоколов, среди которых можно назвать, например, такие популярные стеки, как DECnet, TCP/IP и IBM SNA. Подобное разнообразие средств межсетевого взаимодействия вывело на первый план проблему несовместимости устройств, использующих разные протоколы. Одним из путей разрешения этой проблемы в то время виделся всеобщий переход на единый, общий для всех систем стек протоколов, созданный с учетом недостатков уже существующих стеков. Такой академический подход к созданию нового стека начался с разработки модели OSI и занял семь лет (с 1977 по 1984 год). *Назначение модели OSI состоит в обобщенном представлении средств сетевого взаимодействия.* Она разрабатывалась в качестве своего рода универсального языка сетевых специалистов, именно поэтому ее называют справочной моделью.

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, утилитами, аппаратными средствами.

Модель OSI включает семь уровней: 7) Прикладной, 6) Представления, 5) Сеансовый, 4) Транспортный, 3) Сетевой, 2) Канальный, 1) Физический. (Рисунок 2.3).

Рассмотрим алгоритм взаимодействия двух узлов в концепции модели OSI.

Итак, пусть приложение узла А хочет взаимодействовать с приложением узла В (Рисунок 2.3). Для этого **приложение А** обращается с запросом к прикладному уровню, например к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата. После формирования сообщения прикладной уровень направляет его вниз по стеку уровню представления. Протокол уровня представления на основании информации, полученной из заголовка сообщения прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию – заголовок уровня представления, в котором содержатся указания для протокола уровня представления машины-адресата.

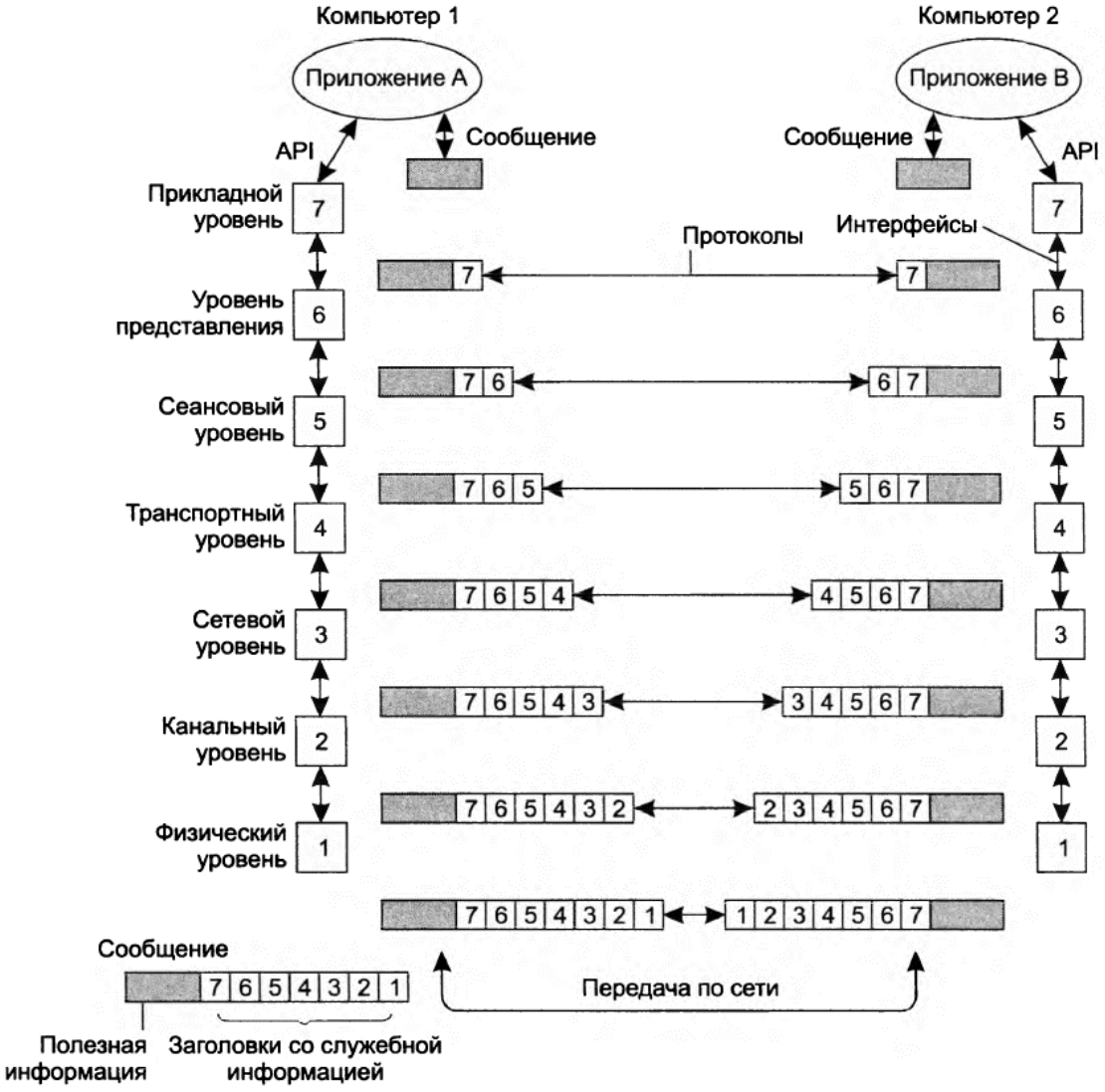


Рисунок 2.3 Модель взаимодействия открытых систем ISO/OSI

Полученное в результате сообщение передается вниз сеансовому уровню, который, в свою очередь, добавляет свой заголовок, и т. д. (Некоторые реализации протоколов помещают служебную информацию не только в начале сообщения в виде заголовка, но и в конце в виде так называемого концевика). Наконец, сообщение достигает нижнего, физического, уровня, который,

собственно, и передает его по линиям связи машине-адресату. К этому моменту сообщение «обрастает» заголовками всех уровней (Рисунок 2.3).

Физический уровень помещает сообщение на физический выходной интерфейс компьютера 1, и оно начинает свое «путешествие» по сети (до этого момента сообщение передавалось от одного уровня другому в пределах Компьютера 1.

Когда сообщение по сети поступает на входной интерфейс Компьютера 2, оно принимается его физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

Таблица 2.1. Уровни модели OSI, функции и типы данных.

Модель OSI		
Тип данных	**Уровень**	**Функции**
Данные	**7. Прикладной**	**Доступ к сетевым службам**
	6. Представления	**Представление и кодирование данных**
	5. Сеансовый	**Управление сеансом связи**
Сегменты	**4. Транспортный**	**Прямая связь между конечными пунктами и надежность**
Пакеты	**3. Сетевой**	**Определение маршрута и логическая адресация**
Кадры	**2. Канальный**	**Физическая/Аппаратная адресация**
Биты	**1. Физический**	**Работа со средой передачи, сигналами и двоичными данными**

Как видно из описания, протокольные сущности одного уровня не общаются между собой непосредственно, в этом общении всегда участвуют посредники – средства протоколов нижележащих уровней. И только

В стандартах ISO для обозначения единиц обмена данными, с которыми имеют дело протоколы разных уровней, используется общее название протокольная единица данных (Protocol Data Unit, PDU). Для обозначения единиц обмена данными конкретных уровней часто используются *специальные* названия, см. таблицу 2.1. – типы данных

физические уровни различных узлов взаимодействуют непосредственно.

Здесь следует обратить внимание на то что модель OSI не включает средства взаимодействия приложений конечных пользователей. Посмотрите внимательно на Рисунок 2.3. «Приложения» изображены отдельно. Важно различать уровень взаимодействия приложений и прикладной уровень семиуровневой модели.

Приложения могут реализовывать собственные протоколы взаимодействия, используя для этих целей многоуровневую совокупность системных средств. Именно для этого в распоряжение программистов предоставляется прикладной программный интерфейс (Application Program Interface, API). В соответствии с идеальной схемой модели OSI приложение может обращаться с запросами только к самому верхнему уровню – прикладному, однако на практике многие стеки коммуникационных протоколов предоставляют возможность программистам напрямую обращаться к сервисам, или службам, нижележащих уровней.

Например, некоторые СУБД имеют встроенные средства удаленного доступа к файлам. При наличии этих средств приложение, выполняя доступ к удаленным ресурсам, не использует системную файловую службу; оно обходит верхние уровни модели OSI и обращается непосредственно к ответственным за транспортировку сообщений по сети системным средствам, которые располагаются на нижних уровнях модели OSI.

Каждый уровень системы должен полагаться на услуги, предоставляемые ему смежными уровнями.

1. Физический уровень. На данном уровне выполняется передача битов по физическим каналам (коаксиальный кабель, витая пара, оптоволокно, Wi-Fi).

2. Канальный уровень. Данный уровень определяет методы доступа к среде передачи данных и обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией по физическому адресу сетевого устройства. Адреса, используемые на канальном уровне в локальных сетях, часто называют MAC-адресами (MAC – Media Access Control, управление доступом к среде передачи данных). В настоящее время наиболее известным протоколом канального уровня является протокол Ethernet/

3. Сетевой уровень. Обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом не гарантируется надежная доставка данных от узла-отправителя к узлу-получателю. На этом уровне выполняются такие функции как маршрутизация логических адресов сетевых узлов, создание и ведение таблиц маршрутизации, фрагментация и сборка данных. В настоящее время применяются две версии сетевого протокола IPv4 и IPv6. Каждый со своей системой адресации: IPv4 – 4 байта (32 бита), IPv6-

4. Транспортный уровень. Обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для выполнения этой задачи на транспортном уровне имеются механизмы установления соединения между

сетевыми узлами, нумерации, буферизации и упорядочивания пакетов, передаваемых между узлами сети.

5. Сеансовый уровень. Реализует средства управления сессией, диалогом, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями, контроля над ошибками, обработки транзакций, поддержки вызова удаленных процедур RPC.

6. Уровень представления. На этом уровне могут выполняться различные виды преобразования данных, такие как компрессия и декомпрессия, шифровка и дешифровка данных.

7. Прикладной уровень. Набор сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примеры таких сервисов — обмен сообщениями электронной почты, передача файлов между узлами сети, приложения управления сетевыми узлами.

Функционирование первых трех уровней, физического, канального и сетевого, обеспечивается, в основном, активным сетевым оборудованием и, как правило, реализуются следующими компонентами: сетевыми адаптерами, репитерами, мостами, концентраторами, коммутаторами, маршрутизаторами.

Тема 3 Требования, предъявляемые к современным сетям.

Компьютерная сеть должна обеспечить выполнение того набора услуг, для оказания которых она предназначена: это например, предоставление доступа к файловым архивам или страницам публичных Web-сайтов Internet, обмен электронной почтой в пределах предприятия или в глобальных масштабах, интерактивный обмен голосовыми сообщениями IP-телефонии, проведение WebInar, дистанционного обучения и пр.

Главным требованием, предъявляемым к сетям, является выполнение сетью ее основной функции – обеспечение пользователям потенциальной возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть. Все остальные требования – производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость – связаны с качеством выполнения этой основной задачи.

Хотя все эти требования весьма важны, часто понятие «качество обслуживания» (Quality of Service, QoS) компьютерной сети трактуется более узко — в него включаются только две самые важные характеристики сети — производительность и надежность.

Независимо от выбранного показателя качества обслуживания сети существуют два подхода к его обеспечению. Первый подход, очевидно, покажется наиболее естественным с точки зрения пользователя сети. Он состоит в том, что сеть (точнее, обслуживающий ее персонал) гарантирует пользователю соблюдение некоторой числовой величины показателя качества

обслуживания. Например, сеть может гарантировать пользователю A, что любой из его пакетов, посланных пользователю B, будет задержан сетью не более, чем на 150 мс. Или, что средняя пропускная способность канала между пользователями A и B не будет ниже 5 Мбит/с, при этом канал будет разрешать пульсации трафика в 10 Мбит на интервалах времени не более 2 секунд. Технологии Frame Relay и ATM позволяют строить сети, гарантирующие качество обслуживания по производительности.

Второй подход состоит в том, что сеть обслуживает пользователей в соответствии с их приоритетами. То есть качество обслуживания зависит от степени привилегированности пользователя или группы пользователей, к которой он принадлежит. Качество обслуживания в этом случае не гарантируется, а гарантируется только уровень привилегий пользователя. Такое обслуживание называется обслуживанием best effort – с наибольшим старанием. Сеть старается по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует. По такому принципу работают, например, локальные сети, построенные на коммутаторах с пиритизацией кадров.

Производительность

Потенциально высокая производительность — это одно из основных преимуществ распределенных систем, к которым относятся компьютерные сети. Это свойство обеспечивается принципиальной, но, к сожалению, не всегда практически реализуемой возможностью распределения работ между несколькими компьютерами сети.

Основные характеристики производительности сети:

- время реакции;
- скорость передачи трафика;
- пропускная способность;
- задержка передачи и вариация задержки передачи.

Время реакции сети является интегральной характеристикой производительности сети с точки зрения пользователя. Именно эту характеристику имеет в виду пользователь, когда говорит: "Сегодня сеть работает медленно".

В общем случае **время реакции** определяется как интервал между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на него.

Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети — загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т.п.

Поэтому имеет смысл использовать также и средневзвешенную оценку времени реакции сети, усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

Время реакции сети обычно складывается из нескольких составляющих. В общем случае в него входит:

- время подготовки запросов на клиентском компьютере;
- время передачи запросов между клиентом и сервером через сегменты сети и промежуточное коммуникационное оборудование;
- время обработки запросов на сервере;
- время передачи ответов от сервера клиенту и время обработки получаемых от сервера ответов на клиентском компьютере.

Очевидно, что разложение времени реакции на составляющие пользователя не интересует — ему важен конечный результат. Однако для сетевого специалиста очень важно выделить из общего времени реакции составляющие, соответствующие этапам собственно сетевой обработки данных, — передачу данных от клиента к серверу через сегменты сети и коммуникационное оборудование.

Знание сетевых составляющих времени реакции позволяет оценить производительность отдельных элементов сети, выявить узкие места и при необходимости выполнить модернизацию сети для повышения ее общей производительности.

Производительность сети может характеризоваться также скоростью передачи трафика.

Скорость передачи трафика может быть мгновенной, максимальной и средней.

средняя скорость вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени — час, день или неделя;

мгновенная скорость отличается от средней тем, что для усреднения выбирается очень маленький промежуток времени — например, 10 мс или 1 с;

максимальная скорость — это наибольшая скорость, зафиксированная в течение периода наблюдения.

Чаще всего при проектировании, настройке и оптимизации сети используются такие показатели, как средняя и максимальная скорость. Средняя скорость, с которой обрабатывает трафик отдельный элемент или сеть в целом, позволяет оценить работу сети на протяжении длительного времени, в течение которого в силу закона больших чисел пики и спады интенсивности трафика компенсируют друг друга. Максимальная скорость позволяет оценить, как сеть будет справляться с пиковыми нагрузками, характерными для особых периодов работы, например в утренние часы, когда сотрудники предприятия почти одновременно регистрируются в сети и обращаются к разделяемым файлам и

базам данных. Обычно при определении скоростных характеристик некоторого сегмента или устройства в передаваемых данных не выделяется трафик какого-то определенного пользователя, приложения или компьютера — подсчитывается общий объем передаваемой информации. Тем не менее, для более точной оценки качества обслуживания такая детализация желательна, и в последнее время системы управления сетями все чаще позволяют ее выполнять.

Пропускная способность — максимально возможная скорость обработки трафика, определенная стандартом технологии, на которой построена сеть. Пропускная способность отражает максимально возможный объем данных, передаваемый сетью или ее частью в единицу времени.

Пропускная способность уже не является, подобно времени реакции или скорости прохождения данных по сети, пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети — передачи пакетов данных между узлами сети через различные коммуникационные устройства. Зато она непосредственно характеризует качество выполнения основной функции сети — транспортировки сообщений — и поэтому чаще используется при анализе производительности сети, чем время реакции или скорость.

Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду.

Пропускная способность сети зависит как от характеристик физической среды передачи (медный кабель, оптическое волокно, витая пара) так и от принятого способа передачи данных (технология Ethernet, FastEthernet, ATM). Пропускная способность часто используется в качестве характеристики не столько сети, сколько собственно технологии, на которой построена сеть. Важность этой характеристики для сетевой технологии показывает, в частности, и то, что ее значение иногда становится частью названия, например, 10 Мбит/с Ethernet, 100 Мбит/с FastEthernet, 1000 Мбит/с GigabitEthernet, 10 Gb/s –10GE, 10GbE или 10 GigE.

В отличие от времени реакции или скорости передачи трафика пропускная способность не зависит от загруженности сети и имеет постоянное значение, определяемое используемыми в сети технологиями.

На разных участках гетерогенной сети, где используется несколько разных технологий, пропускная способность может быть различной. ***Для анализа и настройки сети очень полезно знать данные о пропускной способности отдельных ее элементов***. Важно отметить, что из-за последовательного характера передачи данных различными элементами сети общая пропускная способность любого составного пути в сети будет равна минимальной из пропускных способностей составляющих элементов маршрута. Для повышения пропускной способности составного пути необходимо в первую очередь обратить внимание на самые медленные элементы. Иногда полезно оперировать **общей пропускной способностью** сети, которая определяется как среднее количество информации, переданной между всеми узлами сети за

единицу времени. Этот показатель характеризует качество сети в целом, не дифференцируя его по отдельным сегментам или устройствам.

Задержка передачи определяется как задержка между моментом поступления данных на вход какого либо сетевого устройства или части сети и моментом появления их на выходе этого устройства.

Этот параметр производительности по смыслу близок ко времени реакции сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки конечными узлами сети.

Обычно качество сети характеризуют величинами максимальной задержки передачи и вариацией задержки. Не все типы трафика чувствительны к задержкам передачи, во всяком случае, к тем величинам задержек, которые характерны для компьютерных сетей, — обычно задержки не превышают сотен миллисекунд, реже — нескольких секунд. Такого порядка задержки пакетов, порождаемых файловой службой, службой электронной почты или службой печати, мало влияют на качество этих служб с точки зрения пользователя сети. С другой стороны, такие же задержки пакетов, переносящих голосовые или видеоданные, могут приводить к значительному снижению качества предоставляемой пользователю информации — возникновению эффекта "эха", невозможности разобрать некоторые слова, вибрации изображения и т. п.

Все указанные характеристики производительности сети достаточно независимы. В то время как пропускная способность сети является постоянной величиной, скорость передачи трафика может варьироваться в зависимости от загрузки сети, не превышая, конечно, предела, устанавливаемого пропускной способностью. Так в односегментной сети 10 Мбит/с Ethernet компьютеры могут обмениваться данными со скоростями 2 Мбит/с и 4 Мбит/с, но никогда — 12 Мбит/с.

Пропускная способность и задержки передачи также являются независимыми параметрами, так что сеть может обладать, например, высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета. Пример такой ситуации дает канал связи, образованный геостационарным спутником. Пропускная способность этого канала может быть весьма высокой, например 2 Мбит/с, в то время как задержка передачи всегда составляет не менее 0,24 с, что определяется скоростью распространения электрического сигнала (около 300000 км/с) и длиной канала (72000 км).

Надежность и безопасность

Одна из первоначальных целей создания распределенных систем, к которым относятся и вычислительные сети, состояла в достижении большей надежности по сравнению с отдельными вычислительными машинами.

Важно различать несколько аспектов надежности.

Для сравнительно простых технических устройств используются такие показатели надежности, как: среднее время наработки на отказ ; вероятность отказа ; интенсивность отказов.

Однако эти показатели пригодны для оценки надежности простых элементов и устройств, которые могут находиться только в двух состояниях — работоспособном или неработоспособном. Сложные системы, состоящие из многих элементов, кроме состояний работоспособности и неработоспособности, могут иметь и другие промежуточные состояния, которые эти характеристики не учитывают.

Для оценки надежности сложных систем применяется другой набор характеристик:

- готовность или коэффициент готовности;
- сохранность данных;
- согласованность (непротиворечивость) данных;
- вероятность доставки данных;
- безопасность;
- отказоустойчивость.

Готовность или **коэффициент готовности** (availability) означает период времени, в течение которого система может использоваться. Готовность может быть повышена путем введения избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие.

Чтобы компьютерную систему можно было считать высоконадежной, она должна как минимум обладать высокой готовностью, но этого недостаточно. Необходимо обеспечить сохранность данных и защиту их от искажений. Кроме того, должна поддерживаться согласованность (непротиворечивость) данных, например, если для повышения надежности на нескольких файловых серверах хранится несколько копий данных, то нужно постоянно обеспечивать их идентичность.

Так как сеть работает на основе механизма передачи пакетов между конечными узлами, одной из характеристик надежности является вероятность доставки пакета узлу назначения без искажений. Наряду с этой характеристикой могут использоваться и другие показатели: вероятность потери пакета (по любой из причин – из-за переполнения буфера маршрутизатора, несовпадения контрольной суммы, отсутствия работоспособного пути к узлу назначения и т. д.), вероятность искажения отдельного бита передаваемых данных, соотношение количества потерянных и доставленных пакетов.

Другим аспектом общей надежности является **безопасность** (security), то есть способность системы защитить данные от несанкционированного доступа. В распределенной системе это сделать гораздо сложнее, чем в централизованной. В сетях сообщения передаются по линиям связи, часто проходящим через общедоступные помещения, в которых могут быть установлены средства прослушивания линий. Другим уязвимым местом могут стать оставленные без присмотра персональные компьютеры. Кроме того,

всегда имеется потенциальная угроза взлома защиты сети от неавторизованных пользователей, если сеть имеет выходы в глобальные общедоступные сети.

Еще одной характеристикой надежности является отказоустойчивость (fault tolerance). В сетях под **отказоустойчивостью** понимается способность системы скрыть от пользователя отказ отдельных ее элементов. Например, если копии таблицы базы данных хранятся одновременно на нескольких файловых серверах, пользователи могут просто не заметить отказа одного из них. В отказоустойчивой системе выход из строя одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову. Так, при отказе одного из файловых серверов в предыдущем примере увеличивается только время доступа к базе данных из-за уменьшения степени распараллеливания запросов, но в целом система будет продолжать выполнять свои функции.

Расширяемость и масштабируемость

Расширяемость (extensibility)	Масштабируемость (scalability)
Возможность сравнительно легкого добавления отдельных элементов сети	Легкость расширения системы может обеспечиваться в некоторых весьма ограниченных пределах
Возможность добавления (необязательно легкого) элементов сети	Масштабируемость означает, что наращивать сеть можно в очень широких пределах, при сохранении потребительских свойств сети

Расширяемость

Расширяемость (extensibility) означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры более мощной. При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в весьма ограниченных пределах. Например, локальная сеть Ethernet, построенная на основе одного сегмента толстого коаксиального кабеля, обладает хорошей расширяемостью, в том смысле, что позволяет без труда подключать новые станции. Однако такая сеть имеет ограничение на число станций — оно не должно превышать 30–40. Хотя сеть допускает физическое подключение к сегменту и большего числа станций (до 100), но при этом чаще всего резко снижается производительность сети. Наличие такого ограничения и является признаком плохой масштабируемости системы при хорошей расширяемости.

Масштабируемость (scalability) означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть. Например, хорошей масштабируемостью обладает много сегментная сеть, построенная с использованием коммутаторов и маршрутизаторов и имеющая иерархическую структуру связей. Такая сеть может включать несколько тысяч компьютеров и при этом обеспечивать каждому пользователю сети нужное качество обслуживания.

Прозрачность

Прозрачность (transparency) сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени. Известный лозунг компании Sun Microsystems "Сеть — это компьютер" — говорит именно о такой прозрачной сети.

Прозрачность может быть достигнута на двух различных уровнях – на уровне пользователя и на уровне программиста. На уровне пользователя прозрачность означает, что для работы с удаленными ресурсами он использует те же команды и привычные процедуры, что и для работы с локальными ресурсами. На программном уровне прозрачность заключается в том, что приложению для доступа к удаленным ресурсам требуются те же вызовы, что и для доступа к локальным ресурсам. Прозрачности на уровне пользователя достичь проще, так как все особенности процедур, связанные с распределенным характером системы, скрываются от пользователя программистом, который создает приложение. Прозрачность на уровне приложения требует сокрытия всех деталей распределенности средствами сетевой операционной системы.

Прозрачность — свойство сети скрывать от пользователя детали своего внутреннего устройства, что упрощает работу в сети.

Сеть должна скрывать все особенности операционных систем и различия в типах компьютеров.

Пользователь компьютера Macintosh должен иметь возможность обращаться к ресурсам, поддерживаемым UNIX-системой, а пользователь UNIX/Linux – разделять информацию с пользователями Windows. Подавляющее большинство пользователей ничего не хочет знать о внутренних форматах файлов или о синтаксисе команд UNIX. Пользователь планшета (смартфона) должен иметь возможность обмениваться сообщениями с пользователями сети персональных компьютеров без необходимости вникать в секреты трудно запоминаемых адресов.

Концепция прозрачности применима к различным аспектам сети. Например, прозрачность расположения означает, что от пользователя не требуется знать местонахождение программных и аппаратных ресурсов, таких

как процессоры, принтеры, файлы и базы данных. Имя ресурса не должно включать информацию о месте его расположения, поэтому имена типа mashine1:prog.c или \\ftp_serv\pub прозрачными не являются.

Аналогично, прозрачность перемещения означает, что ресурсы могут свободно перемещаться из одного компьютера в другой без изменения имен. Еще одним из возможных аспектов прозрачности является прозрачность параллелизма, которая заключается в том, что процесс распараллеливания вычислений происходит автоматически, без участия программиста, при этом система сама распределяет параллельные ветви приложения по процессорам и компьютерам сети. В настоящее время нельзя сказать, что свойство прозрачности в полной мере присуще многим вычислительным сетям, это скорее цель, к которой стремятся разработчики современных сетей.

Поддержка разных видов трафика

Компьютерные сети изначально предназначались для совместного доступа к ресурсам компьютеров: файлам, принтерам и т. п. Трафик, создаваемый этими традиционными службами компьютерных сетей, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или, например, в сетях кабельного телевидения. Однако в 90-е годы в компьютерные сети проник трафик мультимедийных данных, представляющих в цифровой форме речь и видеоизображение. Компьютерные сети стали использоваться для организации видеоконференций, обучения на основе видеофильмов и т. п. Естественно, что для динамической передачи мультимедийного трафика требуются иные алгоритмы и протоколы, и, соответственно, другое оборудование. Хотя доля мультимедийного трафика пока невелика, он уже начал проникать как в глобальные, так и в локальные сети, и этот процесс, очевидно, будет активно продолжаться.

Главной особенностью трафика, образующегося при динамической передаче голоса или изображения, является наличие жестких требований к **синхронности** передаваемых сообщений. Для качественного воспроизведения непрерывных процессов, которыми являются звуковые колебания или изменения интенсивности света в видеоизображении, необходимо получение измеренных и закодированных амплитуд сигналов с той же частотой, с которой они были измерены на передающей стороне. При запаздывании сообщений будут наблюдаться искажения.

В то же время трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть при отсутствии жестких требований к синхронности доставки этих сообщений. Например, доступ пользователя, работающего с текстом на удаленном диске, порождает случайный поток сообщений между удаленным и локальным компьютерами, зависящий от действий пользователя, причем задержки при доставке в некоторых (достаточно широких с компьютерной точки зрения) пределах мало влияют на качество обслуживания пользователя сети. Все алгоритмы компьютерной связи, соответствующие протоколы и коммуникационное

оборудование были рассчитаны именно на такой "пульсирующий" характер трафика, поэтому необходимость передавать мультимедийный трафик требует внесения принципиальных изменений, как в протоколы, так и в оборудование. Сегодня практически все новые протоколы в той или иной степени предоставляют поддержку мультимедийного трафика.

Особую сложность представляет совмещение в одной сети традиционного компьютерного и мультимедийного трафика. Передача исключительно мультимедийного трафика компьютерной сетью хотя и связана с определенными сложностями, но доставляет меньше хлопот. А вот сосуществование двух типов трафика с противоположными требованиями к качеству обслуживания является намного более сложной задачей. Обычно протоколы и оборудование компьютерных сетей относят мультимедийный трафик к факультативному, поэтому качество его обслуживания оставляет желать лучшего. Сегодня затрачиваются большие усилия по созданию сетей, которые не ущемляют интересы одного из типов трафика. Наиболее близки к этой цели сети на основе технологии ATM, разработчики которой изначально учитывали случай сосуществования разных типов трафика в одной сети.

Управляемость

В идеале средства управления сетями представляют собой систему, осуществляющую наблюдение, контроль и управление каждым элементом сети – от простейших до самых сложных устройств, при этом такая система рассматривает сеть как единое целое, а не как разрозненный набор отдельных устройств.

Управляемость сети подразумевает возможность **централизованно** контролировать состояние основных элементов сети, выявлять и решать проблемы, возникающие при работе сети, выполнять **анализ** производительности и планировать развитие сети.

Хорошая система управления наблюдает за сетью и, обнаружив проблему, активизирует определенное действие, исправляет ситуацию и уведомляет администратора о том, что произошло и какие шаги предприняты. Одновременно с этим система управления должна накапливать данные, на основании которых можно планировать развитие сети. Наконец, система управления должна быть независимой от производителя и обладать удобным интерфейсом, позволяющим выполнять все действия с одной консоли.

Решая тактические задачи, администраторы и технический персонал сталкиваются с ежедневными проблемами обеспечения работоспособности сети. Эти задачи требуют быстрого решения, обслуживающий сеть персонал должен оперативно реагировать на сообщения о неисправностях, поступающих от пользователей или автоматических средств управления сетью. Постепенно становятся заметны общие проблемы производительности, конфигурирования сети, обработки сбоев и безопасности данных, требующие стратегического подхода, то есть **планирования сети**. Планирование, кроме этого, включает

прогноз изменений требований пользователей к сети, вопросы применения новых приложений, новых сетевых технологий и т. п.

Необходимость в системе управления особенно ярко проявляется в больших сетях: корпоративных или глобальных. Без системы управления в таких сетях требуется присутствие квалифицированных специалистов по эксплуатации в каждом здании каждого города, где установлено оборудование сети, что в итоге приводит к необходимости содержания огромного штата обслуживающего персонала.

В настоящее время в области систем управления сетями много нерешенных проблем. Явно недостаточно действительно удобных, компактных и многопротокольных средств управления сетью. Большинство существующих средств вовсе не управляют сетью, а всего лишь осуществляют наблюдение за ее работой. Они следят за сетью, но не выполняют активных действий, если с сетью что-то произошло или может произойти. Мало масштабируемых систем, способных обслуживать как сети масштаба отдела, так и сети масштаба предприятия, – очень многие системы управляют только отдельными элементами сети и не анализируют способность сети выполнять качественную передачу данных между конечными пользователями.

Совместимость

Совместимость или интегрируемость означает, что сеть может включать в себя разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от разных производителей. Сеть, состоящая из разнотипных элементов, называется неоднородной или гетерогенной, а если гетерогенная сеть работает без проблем, то она является интегрированной. Основной путь построения интегрированных сетей – использование модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

Качество обслуживания

Качество обслуживания (**Quality of Service, QoS**) определяет количественные оценки вероятности того, что сеть будет передавать определенный поток данных между двумя узлами в соответствии с потребностями приложения или пользователя.

Например, при передаче голосового трафика через сеть под качеством обслуживания чаще всего понимают гарантии того, что голосовые пакеты будут доставляться сетью с задержкой не более N мс, при этом

вариация задержки не превысит M мс, и эти характеристики станут выдерживаться сетью с вероятностью 0,95 на определенном временном интервале. То есть приложению, которое передает голосовой трафик, важно, чтобы сеть гарантировала соблюдение именно этого приведенного выше набора характеристик качества обслуживания. Файловому сервису нужны гарантии средней полосы пропускания и расширения ее на небольших интервалах

времени до некоторого максимального уровня для быстрой передачи пульсаций. В идеале сеть должна гарантировать особые параметры качества обслуживания, сформулированные для каждого отдельного приложения. Однако по понятным причинам разрабатываемые и уже существующие механизмы QoS ограничиваются решением более простой задачи — гарантированием неких усредненных требований, заданных для основных типов приложений.

Чаще всего параметры, фигурирующие в разнообразных определениях качества обслуживания, регламентируют следующие показатели работы сети:

- пропускная способность;
- задержки передачи пакетов;
- уровень потерь и искажений пакетов.

Качество обслуживания гарантируется для некоторого потока данных. Напомним, что поток данных – это последовательность пакетов, имеющих некоторые общие признаки, например адрес узла-источника, информация, идентифицирующая тип приложения (номер порта TCP/UDP) и т. п. К потокам применимы

такие понятия, как агрегирование и дифференцирование. Так, поток данных от одного компьютера может быть представлен как совокупность потоков от разных приложений, а потоки от компьютеров одного предприятия агрегированы в один поток данных абонента некоторого провайдера услуг.

Механизмы поддержки качества обслуживания сами по себе не создают пропускной способности. Сеть не может дать больше того, что имеет. Так что фактическая пропускная способность каналов связи и транзитного коммуникационного оборудования — это ресурсы сети, являющиеся отправной точкой для работы механизмов QoS. Механизмы QoS только управляют распределением имеющейся пропускной способности в соответствии с требованиями приложений и настройками сети. Самый очевидный способ перераспределения пропускной способности сети состоит в управлении очередями пакетов.

Поскольку данные, которыми обмениваются два конечных узла, проходят через некоторое количество промежуточных сетевых устройств, таких как концентраторы, коммутаторы и маршрутизаторы, то поддержка QoS требует взаимодействия всех сетевых элементов на пути трафика, то есть "из-конца-в-конец" ("end-to-end", "e2e"). Любые гарантии QoS настолько соответствуют действительности, насколько их обеспечивает наиболее "слабый" элемент в цепочке между отправителем и получателем. Поэтому нужно четко понимать, что поддержка QoS только в одном сетевом устройстве, пусть даже и магистральном, может лишь весьма незначительно улучшить качество обслуживания или же совсем не повлиять на параметры QoS.

Реализация в компьютерных сетях механизмов поддержки QoS является сравнительно новой тенденцией. Долгое время компьютерные сети

существовали без таких механизмов, и это объясняется в основном двумя причинами. Во-первых, большинство приложений, выполняемых в сети, были "нетребовательными", то есть для таких приложений задержки пакетов или отклонения средней пропускной способности в достаточно широком диапазоне не приводили к значительной потере функциональности. Примерами "нетребовательных" приложений являются наиболее распространенные в сетях 80-х годов приложения электронной почты или удаленного копирования файлов.

Во-вторых, сама пропускная способность 10-мегабитных сетей Ethernet во многих случаях не была дефицитом. Так, разделяемый сегмент Ethernet, к которому было подключено 10-20 компьютеров, изредка копирующих небольшие текстовые файлы, объем которых не превышает несколько сотен килобайт, позволял трафику каждой пары взаимодействующих компьютеров пересекать сеть так быстро, как требовалось породившим этот трафик приложениям.

В результате большинство сетей работало с тем качеством транспортного обслуживания, которое обеспечивало потребности приложений. Правда, никаких гарантий относительно контроля задержек пакетов или пропускной способности, с которой пакеты передаются между узлами, в определенных пределах эти сети не давали. Более того, при временных перегрузках сети, когда значительная часть компьютеров одновременно начинала передавать данные с максимальной скоростью, задержки и пропускная способность становились такими, что работа приложений давала сбой – шла слишком медленно, с разрывами сессий и т. п.

Существует два основных подхода к обеспечению качества работы сети. Первый состоит в том, что сеть гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания. Например, сети Frame Relay и ATM могут гарантировать пользователю заданный уровень пропускной способности. При втором подходе (Best Effort) сеть старается по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует.

Транспортный сервис, который предоставляли такие сети, получил название "best effort", то есть сервис "по возможности" (или "с максимальными усилиями"). Сеть старается обработать поступающий трафик как можно быстрее, но при этом никаких гарантий относительно результата не дает. Примерами может служить большинство технологий, разработанных в 80-е годы: Ethernet, Token Ring, IP, X.25. Сервис "с максимальными усилиями" основан на некотором справедливом алгоритме обработки очередей, возникающих при перегрузках сети, когда в течение некоторого времени скорость поступления пакетов в сеть превышает скорость продвижения этих пакетов. В простейшем случае алгоритм обработки очереди рассматривает пакеты всех потоков как равноправные и продвигает их в порядке поступления (First In – First Out, FIFO). В том случае, когда очередь становится слишком большой (не умещается в

буфере), проблема решается простым отбрасыванием новых поступающих пакетов.

Очевидно, что сервис "с максимальными усилиями" обеспечивает приемлемое качество обслуживания только в тех случаях, когда производительность сети намного превышает средние потребности, то есть является избыточной. В такой сети пропускная способность достаточна даже для поддержания трафика пиковых периодов нагрузки. Также очевидно, что такое решение не экономично — по крайней мере, по отношению к пропускным способностям сегодняшних технологий и инфраструктур, особенно для глобальных сетей. Тем не менее, построение сетей с избыточной пропускной способностью, будучи самым простым способом обеспечения нужного уровня качества обслуживания, часто применяется на практике. Например, некоторые провайдеры услуг сетей TCP/IP предоставляют гарантию качественного обслуживания, постоянно поддерживая определенный уровень превышения пропускной способности своих магистралей по сравнению с потребностями клиентов.

В условиях, когда многие механизмы поддержки качества обслуживания только разрабатываются, использование для этих целей избыточной пропускной способности часто оказывается единственно возможным, хотя и временным решением.

Тема 4. Классификация локальных сетей. Топологии локальных сетей: физическая и логическая. Достоинства и недостатки. Выбор топологии.

Локальные сети можно классифицировать по следующим параметрам:

1. **по классу** – локальные сети (LAN) делятся на одноранговые и клиент-серверные сети;
2. **по топологии сети** LAN делятся на шинные, кольцевые, звездообразные, гибридные;
3. **по типу физической среды передачи** - на витую пару, коаксиальный или оптоволоконный кабель, инфракрасный канал, радиоканал;
4. **по скорости доступа** - на низкоскоростные (до 10 Мбит/с), среднескоростные (до 100 Мбит/с), высокоскоростные (свыше 100 Мбит/с);

4.1. Одноранговые и клиент-серверные сети

Локальные вычислительные сети подразделяются на два кардинально различающихся класса: одноранговые (одноуровневые или Peer-to-Peer) сети и клиент-серверные (иерархические).

Клиентом называют тот компьютер (узел сети) и/или программное обеспечение, который использует ресурсы других компьютеров сети

(серверов). При этом клиент посылает запрос к серверу на получение доступа к ресурсу сети (файлу, Web-узлу, принтеру, модему и пр.)

Сервером называют тот компьютер (узел сети) и/или программное обеспечение, который предоставляет свои ресурсы клиентам. При этом сервер обрабатывает запросы клиентов и используя сетевые протоколы посылает (передает) необходимую информацию клиенту или позволяет клиенту управлять ресурсом, например, принтером.

Одноранговая сеть - это сеть равноправных компьютеров, каждый из которых имеет уникальное имя (имя компьютера) и обычно пароль для входа в него во время загрузки ОС (Рисунок 4.1). Имя и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером и клиентом сети, хотя вполне допустимо назначение одного компьютера только сервером, а другого только клиентом.

Такую сеть часто называют «**Рабочей Группой**» (***WORKGROUP***).

Рисунок 4.1. Пример одноранговой сети.

Одна из областей применения технологии одноранговых сетей — обмен файлами. Пользователи файл обменной сети выкладывают какие-либо файлы в папку общего доступа («расшаренную» от англ. share – делиться) на своём компьютере, содержимое которой доступно для скачивания другим пользователям. Аналогично пользователь компьютера, к которому подключен принтер, может открыть доступ пользователям сети к «своему» принтеру.

К основным достоинствам одноранговых сетей можно отнести:

- простоту работы в них;
- низкую стоимость, поскольку все компьютеры являются рабочими станциями;
- отсутствие необходимости в постоянном присутствии администратора сети и относительную простоту администрирования;
- возможность для пользователя контролировать ресурсы своего собственного компьютера;
- независимость отдельных компьютеров и их ресурсов друг от друга;

- легкость в установке и настройке;
- отсутствие необходимости в дополнительном программном обеспечении (кроме операционной системы);

Недостатки одноранговой архитектуры таковы:

- необходимость помнить столько паролей, сколько имеется разделенных ресурсов, либо имен и паролей для входа (для сетей на основе Windows NT/2000/XP/7/8/10);
- необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместно используемые данные;
- отсутствие возможности централизованного управления сетью и доступом к данным; как результат — низкая общая защищенность сети и данных;
- защита информации и безопасность зависит от настроек каждого компьютера;
- эффективность работы зависит от количества компьютеров в сети;

Сейчас считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10-20 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедлят работу компьютеров и создадут множество других проблем. Тем не менее, для небольшого офиса одноранговая сеть - оптимальное решение.

Клиент-серверные сети

Клиент-серверные (иерархические) локальные сети применяются в тех случаях, когда в сеть должно быть объединено много пользователей и возможностей одноранговой сети может не хватить. Тогда в сеть включается специализированный компьютер – сервер.

В клиент-серверных (иерархических) сетях выделяется один или несколько специальных ***компьютеров – серверов***. Серверы обычно представляют собой высокопроизводительные компьютер с серверной операционной системой (например, Windows Server 2003 – Windows Server 2019), отказоустойчивыми дисковыми массивами и системой защиты от сбоев. Как правило, на этих компьютерах локальные пользователи не работают, поэтому принято говорить о выделенном сервере. Серверы управляют сетью и хранят информацию, которую совместно используют остальные компьютеры сети. А компьютеры, с которых осуществляется доступ к информации на сервере, называются клиентами.

Рисунок 4.2. Пример клиент-серверный (иерархической) сети

Если рассматривать сети Windows, то по-настоящему иерархической сеть становится тогда, когда в ней задействуются службы ***Active Directory*** и создается домен Windows.

Преимущества и недостатки клиент-серверных сетей

К преимуществам Клиент-серверных сетей можно отнести:

- использование мощного серверного оборудования обеспечивает быстрый доступ к ресурсам и эффективную обработку запросов клиентов: один сервер может обслуживать тысячи пользователей;
- администрирование сети осуществляется централизованно – с сервера; централизация данных н ресурсов позволяет наладить четкое управление информацией и пользовательскими данными;
- размещение данных на сервере существенно упрощает процедуры резервного копирования;
- повышается общая защищенность сети и сохранность данных;
- выход из строя рабочих станций никак не сказывается на работоспособности сети в целом;

Недостатки Клиент-серверных сетей

- неисправность или сбой единственного сервера может парализовать всю сеть, а ресурсы – недоступными;
- наличие выделенных серверов повышает общую стоимость сети;
- сложность развертывания IT поддержки требует наличия квалифицированного персонала;
- IT-персонал должен обладать достаточными знаниями и навыками администрирования домена, что увеличивает общую стоимость сопровождения сети;
- стоимость сопровождения сети также увеличивается из-за потребности в выделенном оборудовании и специализированном программном обеспечении;

- требуется один (а чаще всего – несколько) постоянно присутствующих на рабочем месте администраторов.

4.2. Топология локальных сетей: физическая и логическая

Сетевая топология (от ***греч.*** τόπος, - место) — способ описания конфигурации **сети**, схема расположения и соединения сетевых устройств, схема прохождения электрических сигналов, описывающая направление потоков информации и принцип предоставления доступа к сети.

Сетевая топология может быть:

3. **физической** — описывает реальное расположение и связи между узлами сети - способ физического соединения компьютеров, узлов сети с помощью среды передачи, например, участками кабеля.
4. **логической** — описывает прохождение сигнала в рамках физической топологии. Таким образом, логическая топология описывает пути передачи потоков данных между сетевыми устройствами и определяет направление и способ передачи, а не схему соединения физических проводников.

Логическая топология в свою очередь подразделяется на:

- **информационную** — описывает направление потоков информации, передаваемых по сети;
- **и управления обменом** — это принцип передачи права на пользование сетью.

Существует множество способов соединения сетевых устройств.

Выделяют 3 базовых топологии:

- **Шина**
- **Звезда**
- **Кольцо**

И дополнительные (производные):

- ***Дерево***
- ***Двойное кольцо***
- ***Решётка***
- ***Полно связная***
- ***Ячеистая топология***
- ***Fat Tree***

Дополнительные способы являются комбинациями базовых. В общем случае такие топологии называются смешанными или гибридными, но некоторые из них имеют собственные названия, например «Дерево», «Двойное Кольцо», «Полно связная» и т.д.

4.2.1. Топология типа шина.

В этом случае подключение и обмен данными производится через общий канал связи, называемый общей шиной. Классической сетевой топологией шина является стандарт Ethernet-10Base-5 -толстый и 10Base-2-тонкий Ethernet. В качестве общего канала используется общий коаксиальный кабель, к которому по электрической схеме «ИЛИ» подключаются все компьютеры. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

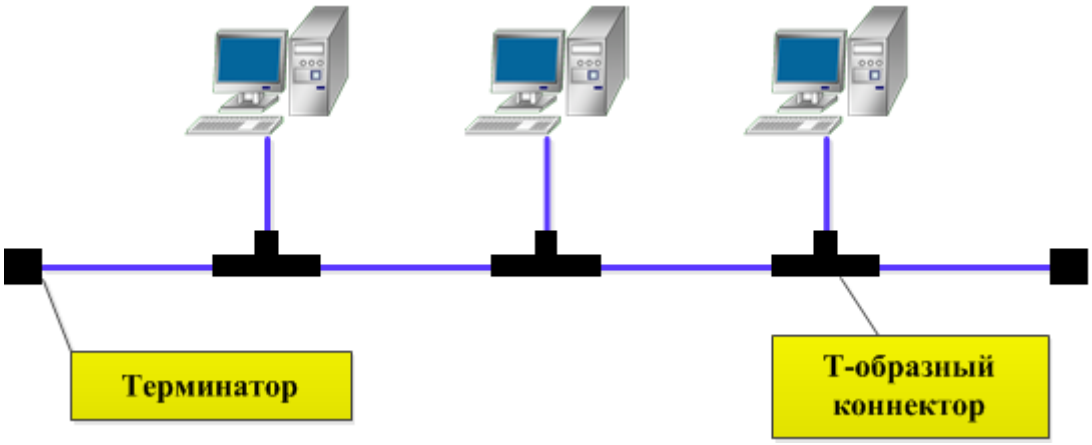


Рисунок 4.3. Топология типа шина**.**

В настоящее время топология шина считается устаревшей, но до сих пор используется.

В шине всегда реализуется режим так называемого полудуплексного (half duplex) обмена (в обоих направлениях, но по очереди, а не одновременно).

К первому компьютеру и к последнему, устанавливаются «Терминаторы»-согласующий резистор, который поглощает электрический сигнал, не давая ему отражаться и двигаться в обратном направлении по шине. Рисунок 4.3.

Работа в сети

Отправляемое рабочей станцией сообщение распространяется на все компьютеры сети. Каждая машина проверяет – кому адресовано сообщение и если ей, то обрабатывает. Существуют ограничения на длину кабеля, связанные с затуханием сигнала, в этом случае сеть разбивают на сегменты. Сегменты соединяются различными устройствами — повторителями, концентраторами или хабами. Например, технология Ethernet 10Base-2 позволяет использовать кабель длиной не более 185 метров Рисунок 4.4**.**

Сравнение с другими топологиями

Достоинства

- Небольшое время установки сети;
- Низкая стоимость (требуется меньше кабеля и сетевых устройств);
- Простота настройки;
- Выход из строя рабочей станции не отражается на работе сети;

Рисунок 4.4 Топология шина –«Тонкий Ethernet» 10Base-2

Недостатки

- Любые неполадки в сети, как обрыв кабеля, выход из строя терминатора полностью приводят к полной неработоспособности всей сети;
- Сложная локализация неисправностей;
- С добавлением новых рабочих станций падает производительность сети.

Часто используется топология, где каждый компьютер включается физически в концентратор (Hub) по схеме «Звезда». Концентратор, принимая сигнал от одного ПК тут же, по битно и одновременно направляет его на остальные порты, т.е. среда передачи данных единая для всей сети. **Такая сеть относится к топологии логическая шина**.

4.2.2. Топология типа Звезда.

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор, коммутатор), образуя **физический сегмент сети**. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило "дерево"). Топология звезда с концентратором (Рисунок 4.5 Б) в качестве центрального узла носит название пассивной звезды.

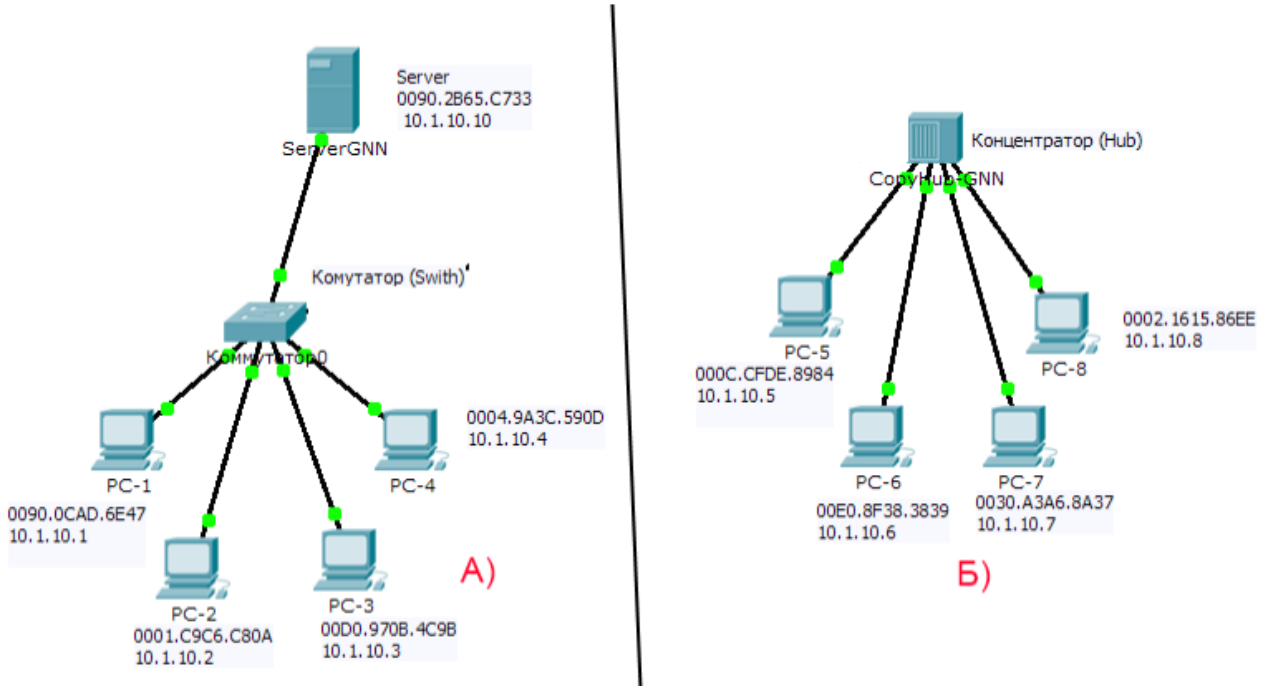


Рисунок 4.5. Топология звезда. А) «Активная звезда», Б) «Пассивная звезда»

Работа в сети

Различают топологии звезда А) «Активная звезда» и Б) «Пассивная звезда» Рисунок 4.5. В топологии активная звезда движением кадров (пакетов, сообщений) управляет центральный узел- это может быть компьютер, а чаще коммутатор (switch). **Одновременно может быть передаваться несколько пакетов.** В случае пассивной звезды, используются концентратор (hub). Задача hub транслировать каждый бит от входящего порта на все имеющиеся, т.е. передача происходит по битно. **Логически – это Шина**.

Сравнение с другими типами сетей

Достоинства

- выход из строя одной рабочей станции не отражается на работе всей сети в целом;
- хорошая масштабируемость сети;
- лёгкий поиск неисправностей и обрывов в сети;
- высокая производительность сети (при условии правильного проектирования);
- гибкие возможности администрирования.

Недостатки

- выход из строя центрального концентратора/коммутатора обернётся неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

Применение

Одна из наиболее распространённых топологий, поскольку проста в обслуживании. В основном используется в сетях, где носителем выступает кабель витая пара - UTP кат 3 или 5.

Конфликты в сети с топологией звезда в принципе невозможны, так как управление полностью централизовано.

Предельная длина каждой линии сети с топологией звезда обычно 100м.

4.2.3. Топология типа «Кольцо» (Ring).

Кольцо — базовая топология компьютерной сети, в которой каждый компьютер соединен линиями связи с двумя другими: от одного он получает информацию, а другому передает. Последний компьютер подключается к первому, и получается замкнутое кольцо.

Важная особенность кольца состоит в том, что каждый компьютер ретранслирует (восстанавливает, усиливает) приходящий к нему сигнал, то есть выступает в роли репитера. Поэтому, предельная длина кольца может достигать N*Lпр, где N — количество компьютеров в кольце, а Lпр предельная длина кабеля, ограниченная затуханием.

Полный размер сети в пределе будет N*Lпр/2, так как кольцо придется сложить вдвое. На практике размеры кольцевых сетей достигают десятков километров (например, в сети FDDI). Кольцо в этом отношении существенно превосходит любые другие топологии.

Четко выделенного центра при кольцевой топологии нет, все компьютеры могут быть одинаковыми и равноправными. Однако довольно часто в кольце выделяется специальный абонент, который управляет обменом или контролирует его. Передача информации в такой сети происходит следующим образом. Маркер (специальный служебный сигнал) последовательно, от одного компьютера к другому, передается до тех пор, пока его не получит тот, которому требуется передать данные. Получив маркер, компьютер создает так называемый «пакет», в который помещает адрес получателя и данные, а затем отправляет этот пакет по кольцу. Данные проходят через каждый компьютер, пока не окажутся у того, чей адрес совпадает с адресом получателя.

После этого принимающий компьютер посылает источнику информации подтверждение факта получения данных. Получив подтверждение, передающий компьютер создает новый маркер и возвращает его в сеть.

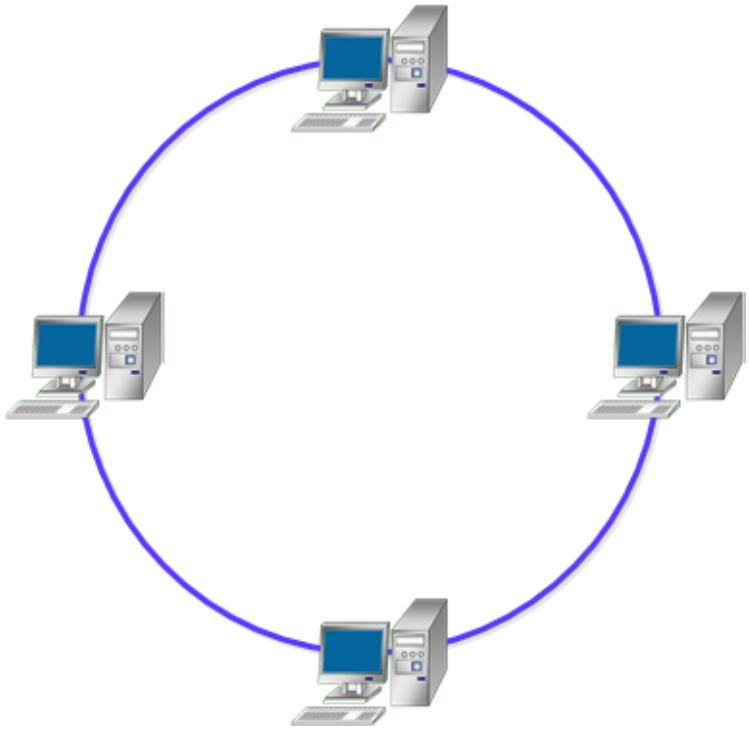


Рисунок 4.6. Сетевая топология кольцо

Достоинства топологии кольцо

- перегрузки в сети практически отсутствуют;
- протяженность сети может достигать до 100км.;
- сеть кольцо допускает включение большого количества абонентов.

Недостатки топологии кольцо

- Отказ одного узла или сетевой ведет к отказу всей сети;

- Обрыв или короткое замыкание в линии связи также приводит к остановке всей сети (то же самое если используются оптоволокно);
- Для включения нового абонента (узла) сети, необходимо останавливать всю сеть.

Для повышения надежности и производительности, часто прокладывают второе кольцо

Классическим вариантом этой технологии является Token Ring стандарт IEEE802.5. и FDDI.

4.2.5. Топология типа «Дерево» Tree.

Топология «Дерево» часто применяется на практике в сетях среднего и крупного масштаба, является производной топологией – комбинацией нескольких звезд, является иерархической топологией и широко применяется там, где технология обмена предусматривает иерархию (Ethernet).

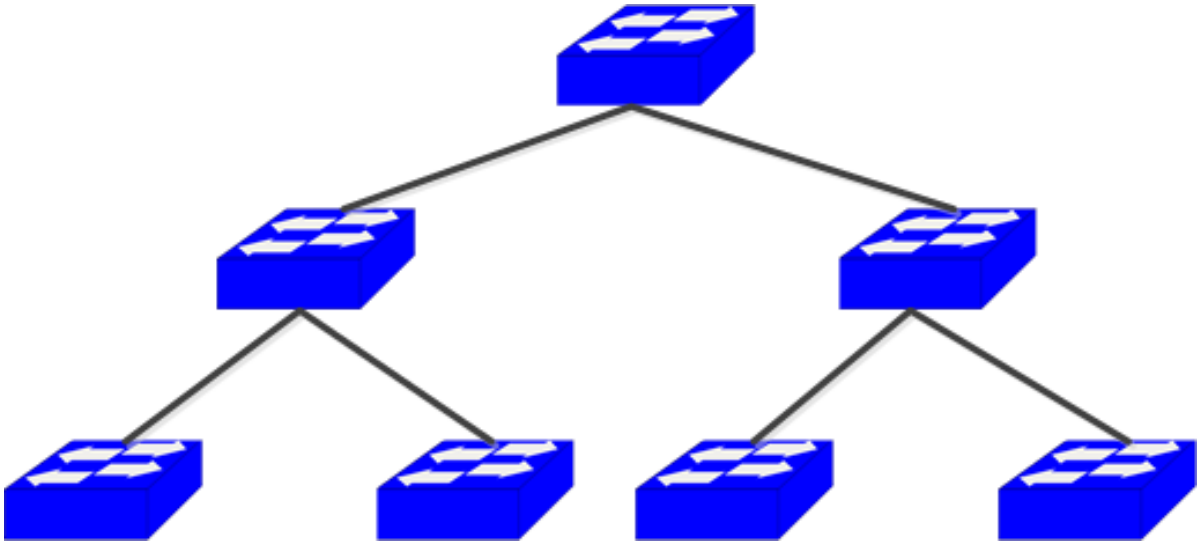


Рисунок 4.8. Сеть на коммутаторах по топологии дерево.

Причем, как и в случае звезды, дерево может быть активным или истинным (Рисунок 4.9) и пассивным (Рисунок 4.10). При активном дереве в центрах объединения нескольких линий связи находятся центральные компьютеры, коммутаторы, маршрутизаторы, а при пассивном — концентраторы (хабы).

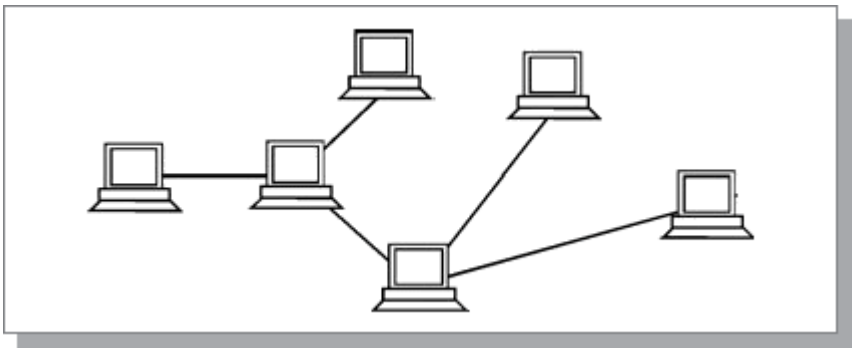


Рисунок 4.9. Топология активное дерево

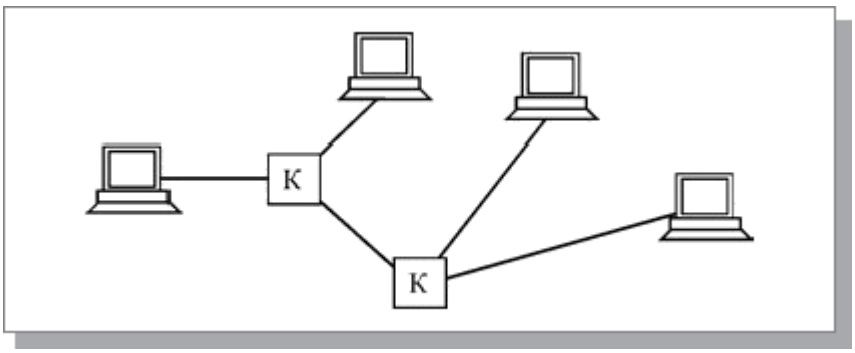


Рисунок 4.10 Топология пассивное дерево. К — концентраторы

В сетях с топологией «Дерево», можно включать любые устройства, – концентраторы, коммутаторы и маршрутизаторы или компьютер с несколькими сетевыми интерфейсами (сетевыми картами).

Таким образом пассивная топология «Дерево» логически – это топология «Шина», а активная топология имеет свойства активной «Звезды» или комбинации «Звезд»).

В локальных сетях Ethernet, чаще всего используются коммутаторы, т.е. «Активное дерево».

Достоинства топологии «Дерева»

- Хорошо масштабируемая сеть (большой потенциал для расширения);
- Легко контролировать и исправлять повреждения (поиск обрывов и неисправностей);
- Выход из строя на одной станции не влияет на работоспособность всей сеть;
- Производительность сети при активной топологии «Дерево» выше, чем у шинной, из-за отсутствия коллизий, т.к. применяется индивидуальное соединение между коммутаторами.

Недостатки топологии «Дерева»

- Зависимость нижестоящих узлов от вышестоящих, то есть отказ одного вышестоящего узла приведет к отказу всей ветки;
- Отказ корневого узла, приведет к неработоспособности всей сети;

- Большой расход кабеля;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в коммутаторе.

4.2.6. Топология типа «Решётка» (Mesh)

Решётка — понятие из теории организации компьютерных сетей. Это топология, в которой узлы образуют регулярную многомерную решетку. При этом каждое ребро решетки параллельно ее оси и соединяет два смежных узла вдоль этой оси.

Одномерная «решётка» — это цепь, соединяющая два внешних узла (имеющие лишь одного соседа) через некоторое количество внутренних (у которых по два соседа — слева и справа) (Рисунок 4.11). Двух- и трехмерные решетки используются в архитектуре суперкомпьютеров (Рисунок 4.12).

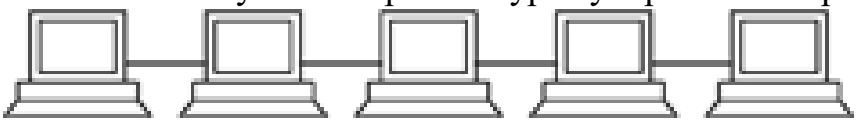


Рисунок 4.11 Топология типа одномерная «решётка»

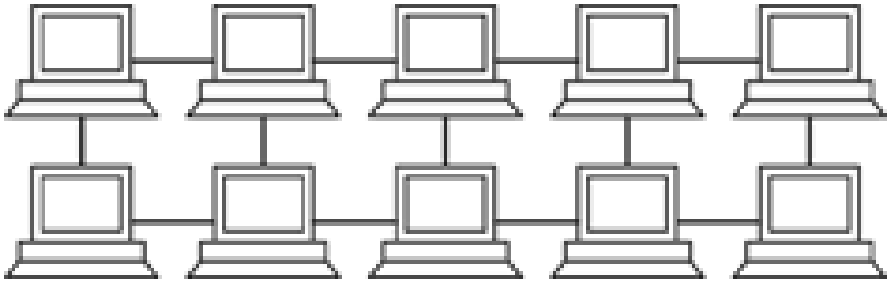


Рисунок 4.12Топология типа двумерная «решётка»

Достоинства топологии:

- высокая надежность;
- высокая отказоустойчивость.

Недостатки топологии:

- Сложность реализации;
- Стоимость реализации;
- Сложность в поддержке и обслуживании.

4.2.7. Полно связанная топология Каждый с каждым (Full Mesh)

Полносвязанная топология - топология компьютерной сети , в которой каждая рабочая станция подключена ко всем остальным. Этот вариант является громоздким и неэффективным, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько коммуникационных портов сколько компьютеров в сети. По этим причинам сеть может иметь только сравнительно небольшие конечные

размеры. Чаще всего эта топология используется в многомашинных комплексах.

Такая схема подключения является самой надежной, так как к одному узлу сразу подключены как минимум 2 соседних устройства. В то же время такая схема сети является и самой дорогой

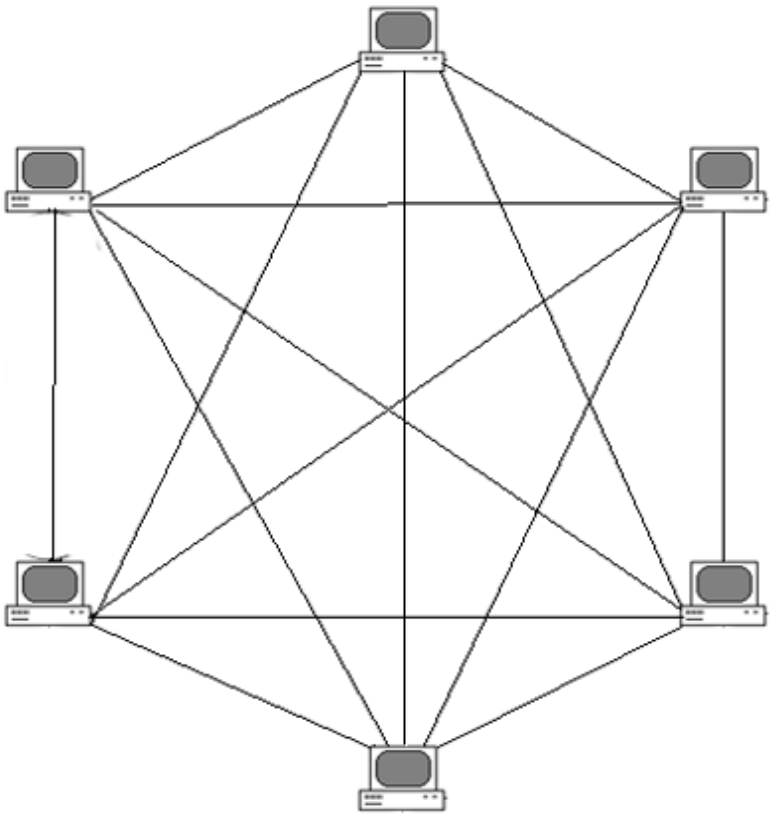


Рисунок 4.11 Полно связанная топология, узлы компьютеры

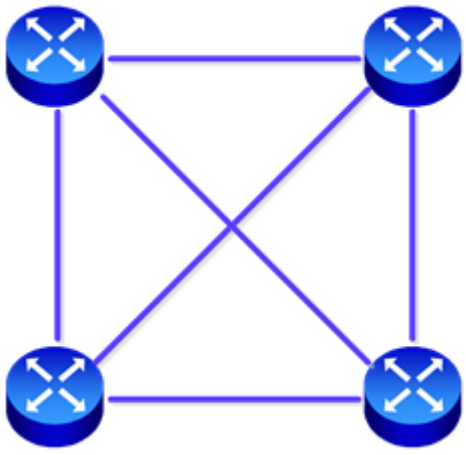


Рисунок 4.12 Полно связанная топология, узлы маршрутизаторы.

Этот вариант является громоздким и неэффективным, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько коммуникационных портов сколько компьютеров в сети. По этим причинам сеть может иметь только

сравнительно небольшие конечные размеры. Чаще всего эта топология используется в многомашинных комплексах или глобальных сетях при малом количестве рабочих станций.

Тема 5 Среда передачи: проводная и беспроводная. Методы доступа к среде передачи.

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами.

Информация в компьютерных сетях чаще всего передается в последовательном коде, то есть бит за битом.

В компьютерных сетях используются проводные и беспроводные линии связи, а также цифровые каналы операторов услуг связи и Интернет. В локальных сетях чаше всего применяются три типа кабельных линий связи.

5.1. Типы линий связи локальных сетей.

Коаксиальные кабели

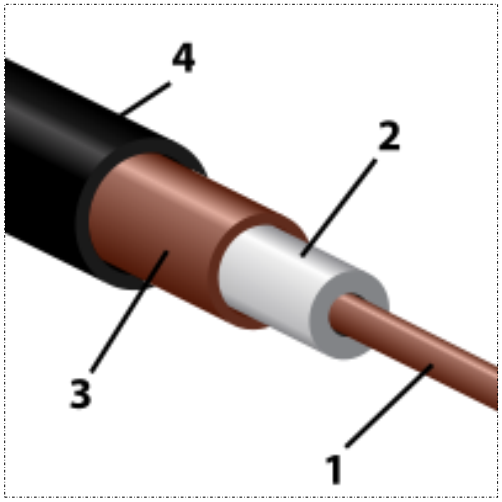


Рисунок.5.1. Коаксиальный кабель

1. Внутренний проводник (медная проволока),
2. Изоляция (сплошной полиэтилен),
3. Внешний проводник (оплётка из меди),
4. Оболочка (свето- стабилизированный полиэтилен).

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального медного провода и металлической оплетки (экрана), разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (Рисунок.5.1).

Коаксиальный кабель до недавнего времени был очень популярен, что связано с его высокой помехозащищенностью.

Основное применение коаксиальный кабель находит в сетях с топологией типа шина. При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен. Без заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех.

Чаще всего в локальных сетях применяются 50-омные (RG-58, RG-11, RG-8). В новых стандартах Ethernet не предусмотрено применение коаксиальных кабелей.

Существует два основных типа коаксиального кабеля:

- тонкий (thin) кабель, имеющий диаметр около 0,5-0,6 см, более гибкий;
- толстый (thick) кабель, диаметром около 1,2 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен современным тонким кабелем.

Толстый (thick) коаксиальный кабель называют «стандартный Ethernet», поскольку он был первым типом кабеля, применяемым в Ethernet. Медная жила этого кабеля толще, чем у тонкого коаксиального кабеля, поэтому затухание сигнала меньше. Толстый коаксиальный кабель передает сигналы дальше, чем тонкий, - до 500 м (около 1640 футов). Поэтому толстый коаксиальный кабель иногда используют в качестве основного кабеля магистрали (back-bone), который соединяет несколько небольших сетей, построенных на тонком коаксиальном кабеле. Для подключения к толстому коаксиальному кабелю применяют специальное устройство - трансивер (transceiver).

Тонкий (thin) коаксиальный кабель способен передавать сигнал на расстояние до 185 м (около 607 футов) без заметного искажения, вызванного затуханием (Рисунок.5.2.).

Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру (Рисунок.5.3), а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования.

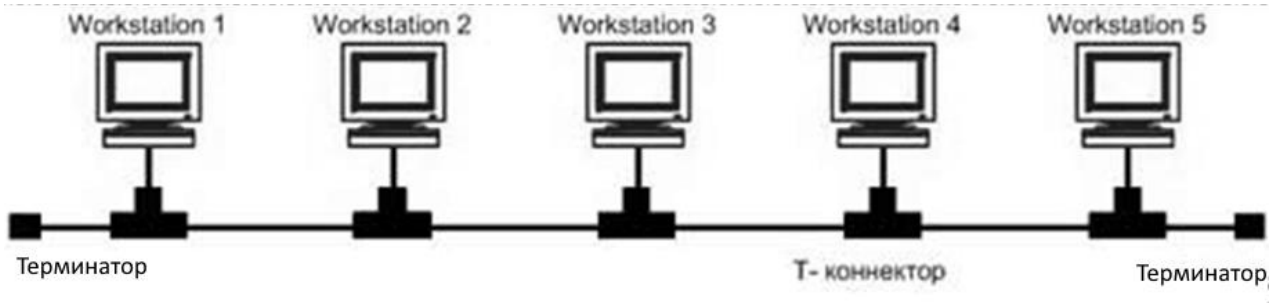


Рисунок.5.2. Сегмент локальной сети на тонком коаксиальном кабеле

В настоящее время считается, что коаксиальный кабель устарел, в большинстве случаев его вполне может заменить витая пара или оптоволоконный кабель. И новые стандарты Ethernet на кабельные системы уже не включают его в перечень типов кабелей.

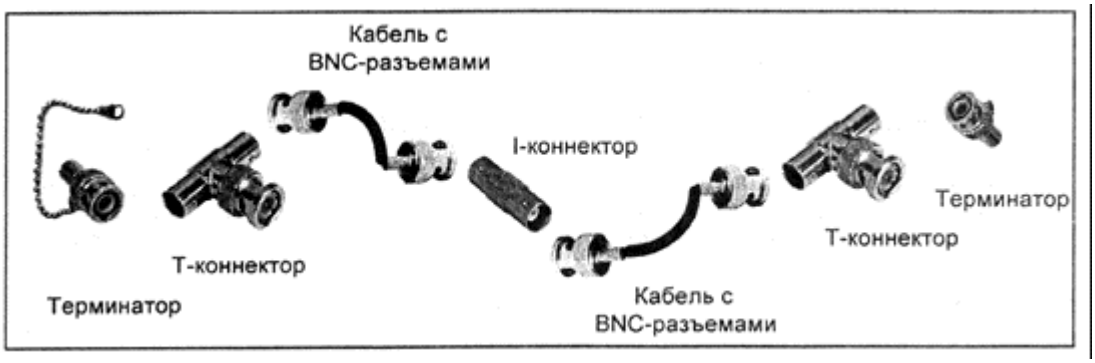


Рисунок.5.3. Пассивные элементы компьютерной сети с топологией общая шина на тонком коаксиальном кабеле.

Оптоволоконный (он же волоконно–оптический) кабель

Это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.

Структура оптоволоконного кабеля (Рисунок 5.4) очень проста и похожа на структуру коаксиального электрического кабеля. Только вместо центрального медного провода здесь используется тонкое (диаметром около 1 – 10 мкм) ***стекловолокно***, а вместо внутренней изоляции – ***стеклянная*** или ***пластиковая оболочка***, не позволяющая свету выходить за пределы стекловолокна.

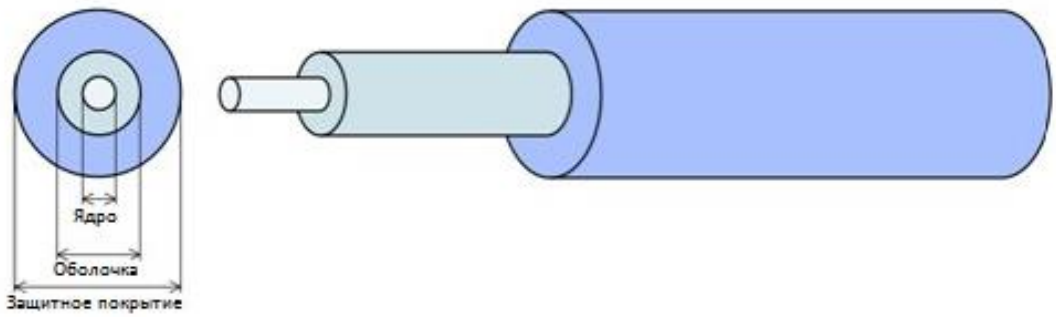


Рисунок 5.4 – Структура оптоволоконного кабеля

В данном случае речь идет о режиме так называемого полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Однако иногда ее все–таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым (бронированным), он может объединять под одной оболочкой несколько оптоволоконных кабелей).

Рисунок 5.4 Бронированный оптоволоконный кабель с множеством оптических волокон.

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания

сети практически невозможно, так как при этом нарушается целостность кабеля. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Однако оптоволоконный кабель имеет и некоторые недостатки:

1. Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме).

2. Использование оптоволоконного кабеля требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

3. Оптоволоконные кабели допускают разветвление сигналов (для этого производятся специальные пассивные разветвители (couplers) на 2–8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником.

4. Оптоволоконный кабель менее прочен и гибок, чем электрический.

5. Чувствителен оптоволоконный кабель и к ионизирующим излучениям, из–за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала.

6. Применяют оптоволоконный кабель только в сетях с топологией звезда и кольцо. Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели или, во всяком случае, сильно потеснит их.

Существуют два различных типа оптоволоконного кабеля:

1. ***многомодовый*** или ***мультимодовый кабель***, более дешевый, но менее качественный;
2. ***одномодовый кабель***, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.

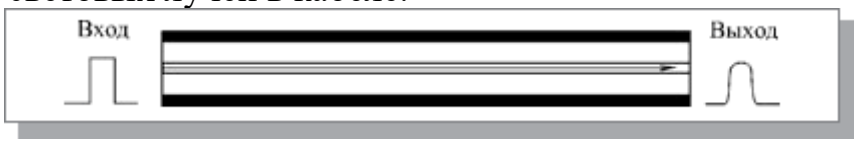


Рисунок 5.5– Распространение света в одномодовом кабеле

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля

применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Затухание сигнала в одномодовом кабеле составляет около 5 дБ/км и может быть даже снижено до 1 дБ/км.

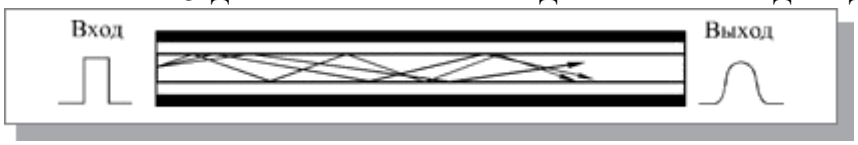


Рисунок 5.6– Распространение света в многомодовом кабеле

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм, при этом наблюдается разброс длин волн около 30 – 50 нм. Допустимая длина кабеля составляет 2 – 5 км. Многомодовый кабель – это основной тип оптоволоконного кабеля в настоящее время, так как он дешевле и доступнее. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5 – 20 дБ/км.

Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

Беспроводные линии связи Wi-Fi, Bluetooth

Кроме кабельных каналов в компьютерных сетях иногда используются также беспроводные линии связи и технологии. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, закреплять кабель в трубах и желобах, прокладывать его под фальшполами, над подвесными потолками или в вентиляционных шахтах, искать и устранять повреждения). К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарами, радиолюбительскими и профессиональными передатчиками и т.д.). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом сигнала несущей частоты.

Главным недостатком радиоканала является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

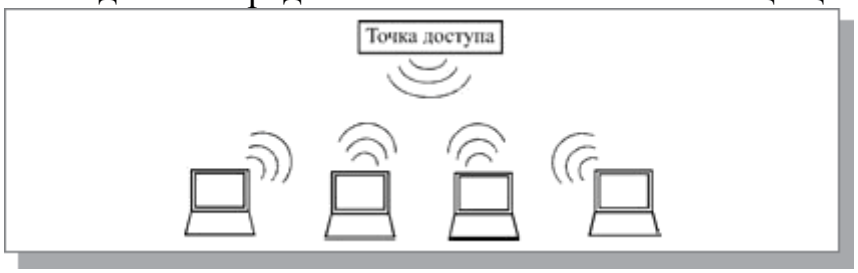


Рисунок 5.7 – Объединение компьютеров

Наиболее известные технологии с использованием радиоканала – это Wi-Fi и Bluetooth. Локальные сети с этими технологиями называются WLAN-сетей (Wireless Local Area Network).

Кабели на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Обычно в кабель входит две (рис. 3.7) или четыре витые пары.

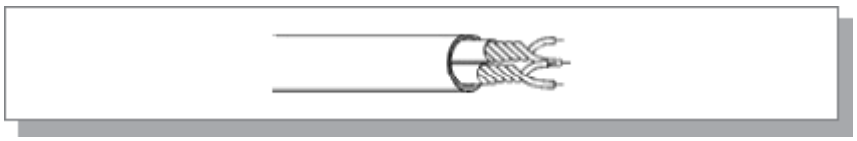


Рисунок 5.8. Кабель с витыми парами

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем перехват передаваемой по сети информации возможен как с помощью контактного метода (например, посредством двух иголок, воткнутых в кабель), так и с помощью бесконтактного метода, сводящегося к радиоперехвату излучаемых кабелем электромагнитных полей. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

В случае экранированной витой пары STP каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (cross talk – перекрестные наводки). Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов. Поэтому встречается она значительно реже, чем неэкранированная витая пара.

Основные достоинства неэкранированных витых пар – простота монтажа разъемов на концах кабеля, а также ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей. Например, при заданной скорости передачи затухание сигнала (уменьшение его уровня по мере прохождения по кабелю) у них больше, чем у коаксиальных кабелей. Если учесть еще низкую помехозащищенность, то понятно, почему линии связи на основе витых пар, как правило, довольно короткие (обычно в пределах 100 метров). В настоящее время витая пара используется для передачи информации на скоростях до 1000 Мбит/с, хотя технические проблемы, возникающие при таких скоростях крайне сложны.

Согласно стандарту EIA/TIA-568, существуют пять основных и две дополнительные категории кабелей на основе неэкранированной витой пары (UTP):

1. Кабель категории 1 – это обычный телефонный кабель (пары проводов не витые), по которому можно передавать только речь. Этот тип кабеля имеет большой разброс параметров (волнового сопротивления, полосы пропускания, перекрестных наводок).
2. Кабель категории 2 – это кабель из витых пар для передачи данных в полосе частот до 1 МГц. Кабель не тестируется на уровень перекрестных наводок. В настоящее время он используется очень редко. Стандарт EIA/TIA 568 не различает кабели категорий 1 и 2.
3. Кабель категории 3 – это кабель для передачи данных в полосе частот до 16 МГц, состоящий из витых пар с девятью витками проводов на метр длины. Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Это самый простой тип кабелей, рекомендованный стандартом для локальных сетей. Еще недавно он был самым распространенным, но сейчас повсеместно вытесняется кабелем категории 5.
4. Кабель категории 4 – это кабель, передающий данные в полосе частот до 20 МГц. Используется редко, так как не слишком заметно отличается от категории 3. Стандартом рекомендуется вместо кабеля категории 3 переходить сразу на кабель категории 5. Кабель категории 4 тестируется на все параметры и имеет волновое сопротивление 100 Ом. Кабель был создан для работы в сетях по стандарту IEEE 802.5. (Token Ring)
5. Кабель категории 5 – в настоящее время самый распространенный кабель, рассчитанный на передачу данных в полосе частот до 100 МГц. Состоит из витых пар, имеющих не менее 27 витков на метр длины (8 витков на фут). Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Рекомендуется применять его в современных высокоскоростных сетях типа Fast Ethernet и TPFDDI. Кабель категории 5 примерно на 30—50% дороже, чем кабель категории 3.
6. Кабель категории 6 – перспективный тип кабеля для передачи данных в полосе частот до 200 (или 250) МГц. в настоящее время рекомендуется для сетей 1000Мгц.
7. Кабель категории 7 – перспективный тип кабеля для передачи данных в полосе частот до 600 МГц.

Согласно стандарту EIA/TIA 568, полное волновое сопротивление наиболее совершенных кабелей категорий 3, 4 и 5 должно составлять 100 Ом ±15% в частотном диапазоне от 1 МГц до максимальной частоты кабеля. Требования не очень жесткие: величина волнового сопротивления может находиться в диапазоне от 85 до 115 Ом. Здесь же следует отметить, что волновое сопротивление экранированной витой пары STP по стандарту должно быть равным 150 Ом ±15%. Для согласования сопротивлений кабеля и оборудования в случае их несовпадения применяют согласующие трансформаторы (Balun). Существует также экранированная витая пара с волновым сопротивлением 100 Ом, но используется она довольно редко.

Методы доступа к среде передачи данных.

В технологии локальных сетей в основном осуществлено применение общей разделяемой физической среды и в этом случае существуют два основных метода доступа к разделяемой физической среде:

- Метод случайного доступа;
- Детерминированный доступ;

Метод случайного доступа является одним; из основных методов захвата разделяемой среды. Он основан на том, что узел, у которого есть кадр для передачи, пытается его отправить без какой бы то ни было предварительной процедуры согласования времени использования разделяемой среды с другими узлами сети.

Детерминированный доступ – это другой популярный подход к обеспечению доступа к разделяемой среде. Он получил свое название благодаря тому, что максимальное время ожидания доступа к среде всегда известно.

Алгоритмы детерминированного доступа используют два механизма - **передачу токена и опрос**.

В настоящее время основной технологией локальных вычислительных сетей является технология, а точнее семейство технологий Ethernet.

Метод доступа Ethernet к разделяемой физической среде – это множественный доступ с прослушиванием несущей и обнаружением коллизий, а именно: **CSMA/CD (Carrier Sense Multiple Access/Collision Detect).**

Суть метода состоит в следующем.

Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей (физическая среда свободна) он начинает передачу кадра, одновременно контролируя состояние линии. При обнаружении коллизии передача прекращается, и повторная попытка откладывается на случайное время. Коллизии — нормальное, хотя и не очень частое явление для CSMA/CD. Их частота связана с количеством и активностью подключенных узлов. Нормально коллизии могут начинаться в определенном временном окне кадра,

запоздалые коллизии сигнализируют об аппаратных неполадках в кабеле или узлах. Метод эффективнее, чем CSMA/CA, но требует более сложных и дорогих схем цепей доступа.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) — множественный доступ с прослушиванием несущей и избежанием коллизий. Узел, готовый послать кадр, прослушивает линию. При отсутствии несущей он посылает короткий сигнал запроса на передачу (RTS) и определенное время ожидает ответа (CTS) от адресата назначения. При отсутствии ответа (подразумевается возможность коллизии) попытка передачи откладывается, при получении ответа в линию посылается кадр. Метод не позволяет полностью избежать коллизий, но они обрабатываются на вышестоящих уровнях протокола. Метод применяется в сети Apple Local-Talk, характерен простотой и низкой стоимостью цепей доступа.

Функции технологий локальных сетей соответствую канальному уровню модели OSI/

Канальный уровень (Data Link) взаимодействует с верхним сетевым уровнем, обеспечивая инкапсуляцию пакетов сетевого уровня – IP (IPX, NETBIOS) в кадр и далее продвижение кадра на физическом уровне. Поэтому Канальный уровень разделен на 2 подуровня: верхний подуровень логической передачи данных ***LLC – Logical Link Control***, общий для всех технологий LAN, и нижний подуровень управления доступом к среде ***MAC – Media Access Control***

Функции уровня LLC обычно реализуются программно, соответствующим модулем операционной системы, а функции уровня MAC реализуются программно аппаратно: сетевым адаптером и его драйвером.

Уровень LLC выполняет две функции:

- организует интерфейс с прилегающим к нему сетевым уровнем;
- обеспечивает доставку кадров с заданной степенью надежности, через MAC уровень.

Интерфейсные функции LLC – обмен данными между уровнем MAC и сетевым уровнем.

При передаче данных *сверху вниз* LLC принимает от протокола сетевого уровня пакет (IP; IPX), в котором находятся пользовательские данные. Далее уровень LLC передает вниз — уровню MAC, при необходимости решает задачу **мультиплексирования**, передавая данные от нескольких протоколов сетевого уровня единственному протоколу уровня MAC.

При передаче данных *снизу вверх* LLC принимает от уровня MAC кадр с пакетом сетевого уровня, и выполняет обратную функцию — ***демультиплексирование***, то есть решает, какому из сетевых протоколов передать полученные от MAC данные.

- Уровень LLC предоставляет верхним уровням три типа транспортных услуг.

- **Услуга LLC1** — услуга ***без установления соединения и без подтверждения получения данных***
- **Услуга LLC2** —устанавливает ***логическое соединение*** перед началом передачи любого блока данных и, способна выполнить ***процедуры восстановления.***
- **Услуга LLC3** — услуга ***без установления соединения, но с подтверждением получения данных.***

Этот набор процедур является общим для всех методов доступа к среде, определенных стандартами 802.3-802.5.

Второй подуровень канального уровня это - MAC (Media Access Control) уровень, который выступает в качестве интерфейса между подуровнем LLC и физическим (первым) уровнем OSI. Интерфейсы и функции MAC уровня, взаимодействующие с физическим разнятся от технологий (Ethernet, Token Ring, FDDI) и применяемой физической среды (коаксиальный кабель, витая пара, оптоволокно, радиоэфир). Именно MAC уровень обеспечивает корректное совместное использование общую – разделяемую физическую среду.

В современных локальных сетях получили распространение несколько протоколов MAC уровня для технологий Ethernet, Token Ring, FDDI, но адресация MAC едина для всех.

MAC – уровень принимает кадр LLC, преобразует его в свой формат, а именно: добавляет физические (аппаратные) MAC адреса, данные пользователя, контрольную сумму и другие поля. MAC-уровень согласовывает дуплексный режим работы уровня LLC с полудуплексным режимом работы физического уровня и применяется только с полудуплексным режимом.

Механизм адресации уровня MAC называется физической адресацией или MAC-адресами. MAC-адрес представляет собой уникальный серийный номер, который присваивается каждому сетевому устройству (сетевая карта, в компьютере в коммутаторе) во время изготовления, и позволяет однозначно определить его среди других сетевых устройств в мире. Это гарантирует, что все устройства в сети будут иметь различные MAC-адреса.

Механизм контроля доступа к каналу, предоставляемый уровнем MAC, также известен, как протокол множественного доступа. Данный протокол позволяет нескольким станциям делить между собой одну среду передачи данных, к которой они подключены. Примерами разделяемой физической среды могут служить сети с топологиями типа «шина», «кольцо», а также сети, созданные с помощью сетевых концентраторов, беспроводные сети и сети с полудуплексным подключением «точка-точка». **Протокол множественного доступа может определять и предотвращать коллизии пакетов (кадров) данных**.

Механизм множественного доступа основан на методе мультиплексирования физического уровня.

Наиболее широко используемый – это протокол доступа CSMA/CD, используемом в Ethernet. Этот механизм используется только внутри сетевого домена коллизий, например, в шине Ethernet или в сетевом концентраторе (хабе). Сеть Ethernet может быть разделена на несколько доменов коллизий, соединенных мостами, коммутаторами или маршрутизаторами. Протокол множественного доступа не используется в коммутируемых полнодуплексных сетях, таких, как используемые сегодня коммутируемые сети Ethernet (коммутаторы и маршрутизаторы), но частично доступен в оборудовании для обеспечения совместимости. Т.е. интерфейсы Ethernet коммутаторов и маршрутизаторов могут его использовать.

На уровне MAC, для идентификации сетевых интерфейсов - узлов сети используются регламентированные стандартом **IEEE 802.3** уникальные 6-ти байтовые адреса, называемые MAC - адресами. Обычно MAC - адрес записывают в виде шести пар шестнадцатеричных цифр, разделенных тире или двоеточиями, например 11-A0-17-3D-BC-01. Каждый сетевой адаптер имеет, по крайней мере, один MAC -адрес.

Форматы кадров технологии Ethernet.

Существует четыре формата кадра Ethernet. Рассмотрим наиболее часто используемый формат, а именно: Кадр Ethernet DIX, или Ethernet II.

Кадр Ethernet DIX, или Ethernet II, появился в результате работы консорциума трех фирм Digital, Intel и Xerox в 1980 году, который представил на рассмотрение комитету 802.3 свою фирменную версию стандарта Ethernet в качестве проекта международного стандарта.

Однако комитет 802.3 принял стандарт, отличающийся в некоторых деталях от предложения DIX, причем отличия касались и формата кадра. Так возникли форматы кадров 802.3/LLC, 802.3/802.2, или Novell 802.2.

SСетевые эти отличия различают и корректно их обрабатывают, но формат кадра Ethernet II остался как основной (Рисунок 5.9)

6	6	2	46–1500	4
DA	SA	T	Data	FCS

Рисунок 5.9 Формат кадра Ethernet II

Формат кадра Ethernet является структурированной единицей данных канального уровня и разделен на следующие поля:

1. DA – (Destination Address) – Адрес назначения 6- байт;

2. SA – (Source Address) – Адрес источника 6- байт

3. T – (Type Protocol) – Тип протокола верхнего (сетевого) уровня 2-байта;

4. Data (Data) – Данные которые инкапсулируются (вкладываются) в это поле, например, пакет сетевого уровня IP протокола (или его часть) (46-1500 байт);

Если в поле Data вкладывается фрагмент сетевого протокола IP длинной меньше 46 байт, то в это поле добавляются «нулевые» байты в необходимом количестве до 46 байт в сумме с данными.

5. FCS – (Frame Check Sequence) – состоит из 4 байт, содержащих контрольную сумму. Это значение вычисляется по алгоритму CRC-32.

Перед каждым кадром поступает предварительно семь байт преамбулы, содержащей 10101010 и один байт ***Начальный ограничитель кадра*** (Start-of-Frame-Delimiter, SFD) состоит из одного байта 10101011.

Тема 6 Базовые технологии локальных сетей.

Локальными сетями (ЛВС - локальные вычислительные сети или LAN - Local Area Network) называют сети, размещающиеся, как правило, в одном здании или на территории какой-либо организации размерами до нескольких километров.

Технологии локальных компьютерных сетей стали разрабатываться и внедряться в 70-е года прошлого столетия.

Локальные сети технологии ARCnet

Attached Resource Computing Network (ARCnet) - сетевая архитектура, разработанная компанией Datapoint в середине 70-х годов. В качестве стандарта IEEE ARCnet принят не был, но частично соответствует IEEE 802.4 как сеть с передачей маркера (логическое кольцо). Пакет данных может иметь любой размер в пределах от 1 до 507 байт.

Из всех локальных сетей Arcnet обладает самыми широкими возможностями в области топологий. Кольцо, общая шина, звезда, дерево может быть использованы в одной сети. Плюс к этому можно использовать весьма протяженные сегменты (до нескольких километров). Такие же широкие возможности имеются и по использованию среды передачи - годится коаксиальный, оптоволоконный кабель, витая пара.

Доминировать на рынке этому недорогому стандарту помешало малое быстродействие - всего-то 2,5 Мбит/с. А также ограничение максимального числа клиентов в пределах одной сети - не более 256 и как правило необходимость выставлять сетевые адреса на сетевых картах с помощью джамперов, соблюдая при этом их уникальность. И когда в начале 90-х Datapoint разработала ArcNet PLUS со скоростью передачи до 20 Мбит/с, время было уже упущено. Fast Ethernet не оставил ArcNet ни малейшего шанса на широкое применение.

Тем не менее, в пользу большого (но так и не реализованного) потенциала этой технологии можно сказать, что в некоторых отраслях (обычно АСУТП) сети живут до сих пор (благодаря своей надежности и большой протяженности). Детерминированный доступ, возможности автоконфигурирования, согласования скорости обмена в диапазоне от 120

Килобит/с до 10 Мбит/с, в сложных условиях реального производства бывают просто незаменимы.

Кроме этого, Arcnet обеспечивает необходимую для систем управления возможность точно определять максимальное время доступа к любому устройству в сети при любой нагрузке по простой формуле: T = (TDP + TOBoNb)oND, где TDP и TOB -времена передачи пакета данных и одного байта, зависящие от выбранной скорости передачи, Nb - количество байтов данных, ND - количество устройств в сети. Как правило сеть состояла из системы активных (до 600 метров) и пассивных (до 200 метров) хабов, связанных коаксиальными линиями. В СССР эти сети получили большое распространение на промышленных предприятиях в 80-ых годах, благодаря использованию дешевого и массового кабеля РК-75 (антенный) и серверов Novell Netware 2.x-3.x

Топология Token Ring

Эта топология основана на топологии «физическое кольцо с подключением типа звезда». В данной топологии все рабочие станции подключаются к центральному концентратору (Token Ring Рисунок 4.7) как в топологии физическая звезда. Центральный концентратор - это интеллектуальное устройство, которое с помощью электронных «перемычек» обеспечивает последовательное соединение выхода одной станции со входом другой станции. Другими словами, с помощью концентратора каждая станция соединяется только с двумя другими станциями (предыдущей и последующей станциями). Таким образом, рабочие станции связаны петлей кабеля, по которой пакеты данных передаются от одной станции к другой, и каждая станция ретранслирует эти посланные пакеты.

В каждой рабочей станции имеется для этого приемо-передающее устройство, которое позволяет управлять прохождением данных в сети. Физически такая сеть построена по типу топологии «звезда». Концентратор создаёт первичное (основное) и резервное кольца. Если в основном кольце произойдёт обрыв, то его можно обойти, воспользовавшись резервным кольцом, так как используется четырёхжильный кабель. Отказ станции или обрыв линии связи рабочей станции не влечёт за собой отказ сети как в топологии кольцо, потому что концентратор отключит неисправную станцию и замкнет кольцо передачи данных.

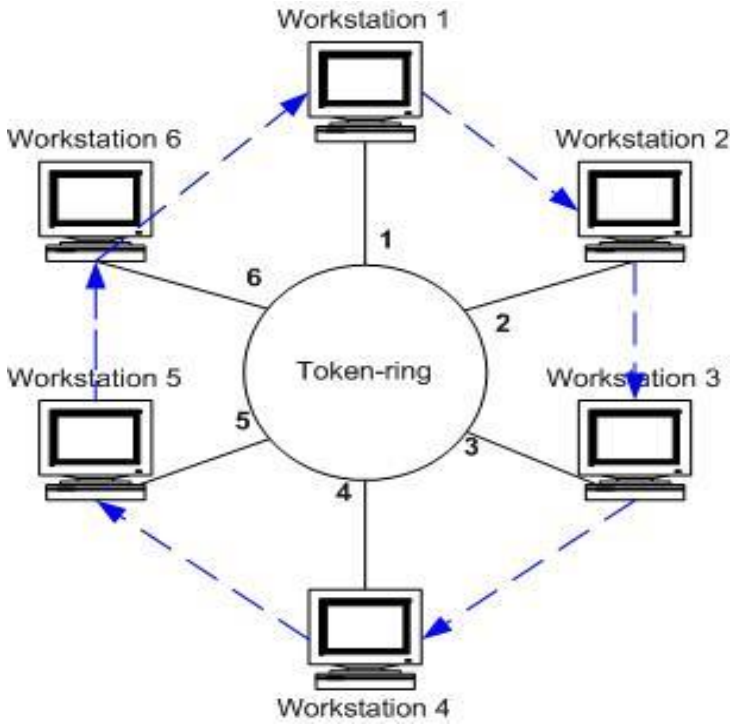


Рисунок 6.1. Сеть Token Ring

В архитектуре Token Ring маркер передаётся от узла к узлу по логическому кольцу, созданному центральным концентратором. Такая маркерная передача осуществляется в фиксированном направлении (направление движения маркера и пакетов данных представлено на рисунке стрелками синего цвета). Станция, обладающая маркером, может отправить данные другой станции. Для передачи данных рабочие станции должны сначала дождаться прихода свободного маркера. В маркере содержится адрес станции, пославшей этот маркер, а также адрес той станции, которой он предназначается. После этого отправитель передает маркер следующей в сети станции для того, чтобы и та могла отправить свои данные. Один из узлов сети (обычно для этого используется файл-сервер) создаёт маркер, который отправляется в кольцо сети.:

Изначальная скорость передачи, описанная в IEEE 802.5, составляет 4 Мбит/с, однако существует более поздняя реализация на 16 Мбит/с. Из-за более упорядоченного (детерминированного) метода доступа к среде, Token Ring на ранних этапах развития часто продвигался как более качественная замена Ethernet.

Преимущества сетей топологии Token Ring:

- топология обеспечивает равный доступ ко всем рабочим станциям;
- сеть устойчива к отказу узлов и к разрывам соединительных линий;
- значительно лучше держит высокий уровень нагрузки (более 40%)
- и обеспечивает гарантированное время доступа.

Недостатки сетей топологии Token Ring:

- большой расход кабеля.

- Аппаратура Token Ring более дорогая, чем Ethernet - Ввиду более сложного метода управления обменом.
- Сложность конфигурирования и настройки;
- Сложность поиска неисправностей;

Другой классический вариант применения топологии кольца – технология FDDI.

FDDI наиболее широкое применение получила в оптоволоконных сетях.

FDDI (англ. *Fiber Distributed Data Interface* — распределённый волоконный интерфейс данных) — стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 километров. Стандарт основан на протоколе Token Ring. Кроме большой территории, сеть FDDI способна поддерживать несколько тысяч пользователей.

В качестве топологии используется схема двойного кольца, при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе – вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Для контроля за состоянием кольца используется сетевой маркер, как и в технологии Token Ring. Поскольку такое дублирование повышает надёжность системы, данный стандарт с успехом применяется в магистральных каналах связи.

Технология FDDI была разработана в 1980 году комитетом ANSI. Это была первая компьютерная сеть, использовавшая в качестве среды передачи только оптоволоконный кабель. Причиной разработки была недостаточная в то время скорость (не более 10 Мбит/с) и надежность (отсутствие схем резервирования) локальных сетей. Так же, это была первая попытка вывести сети передачи данных на «транспортный» уровень, составив конкуренцию SDH.

Стандарт FDDI оговаривает передачу данных по двойному кольцу оптоволоконного кабеля со скоростью 100 Мбит/с, что позволяет получить надежный (зарезервированный) и быстрый канал. Расстояния вполне глобальные - до 100 км по периметру. Логически работа сети была построена на передачи маркера.

Дополнительно предусматривалась развитая схема приоритезации трафика. Сначала рабочие станции разделялись на два вида - синхронные (имеющие постоянную полосу пропускания), и асинхронные. Последние, в свою очередь, распределяли среду передачи с помощью восьмиуровневой системы приоритетов.

Несовместимость с сетями SDH не позволила FDDI занять сколь-нибудь значимую нишу в области транспортных сетей. Сегодня эта технология практически вытеснена ATM. С другой стороны, высокая стоимость не оставила шансов в борьбе с Ethernet в локальной нише. Не помогли стандарту и попытки прейти на более дешевый медный кабель. Технология CDDI,

основанная на принципах FDDI, но с применением в качестве среды передачи витой пары, популярностью не пользовалась, и сохранилась только в учебниках.

Технология 100VG-AnyLAN

Разработка AT&T и HP - 100VG-AnyLAN

Как и FDDI, эту технологию можно отнести ко второму поколению локальных сетей. Создавалась она в начале 90-х, совместными усилиями компаний AT&T и HP, как альтернатива технологии Fast Ethernet. Летом 1995 года она практически одновременно со своим конкурентом получила статус стандарта IEEE 802.12. И имела неплохой шанс на победу благодаря своей универсальности, детерминированности и более полной, чем Ethernet, совместимости с существующими кабельными сетями (витая пара Категор-и 3).

Схема квартетного кодирования Quartet Coding, использующая избыточный код 5B/6B, позволяла использовать 4-х парную витую пару Категории 3, которая была тогда распространена едва ли не более, чем современная 5 категория. Переходный период, по сути, не затронул Россию, в которой из-за более позднего начала строительства сети были повсеместно проложены уже с использованием 5 категории.

Кроме использования старой проводки, каждый концентратор 100VG-AnyLAN может быть настроен на поддержку кадров 802.3 (Ethernet), либо кадров 802.5 (Token Ring). Метод доступа к среде «Demand Priority» определяет простую двухуровневую систему приоритетов (высокий для мультимедийных приложений, и низкий для всех остальных).

Надо сказать, это была серьезнейшая заявка на успех. Подвела высокая стоимость, обусловленная большей сложностью и, в немалой мере, закрытостью технологии от тиражирования сторонними производителями. К этому прибавилось уже знакомое по Token Ring отсутствие реальных приложений, использующих преимущества системы приоритетов. В результате 100Base-T удалось надолго и безвозвратно захватить лидерство в отрасли.

Но новаторские технические идеи 100VG-AnyLAN немного позже нашли применение сначала в 100BaseT2 (IEEE 802.3u), а затем и «гигабитном» Ethernet 1000Base-T.

Технология Ethernet

Технология Ethernet на сегодняшний день является наиболее востребованной. Практически любой современный компьютер имеет встроенную сетевую карту GigabitEthernet.

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года, когда Роберт Меткалф (Robert Metcalfe) составил докладную записку для главы PARC о потенциале технологии Ethernet.

Первые сети Ethernet работали по коаксиальному кабелю со скоростью 10Mbit/s. Спецификации стандартов обозначались как 10Base-XX. Число 10 обозначало скорость 10Mb/s, Base – работа осуществлялась на одном несущей сигнале, XX – обозначения менялось в соответствии с применяемой физической средой, например: 10Base5 – в качестве физической среды использовался «толстый » коаксиальный кабель диаметром 0,5 дюйма (1,25см) – это был первый стандарт Ethernet. Далее были разработаны и широко применятся спецификации 10Base2, 10Base-T, 10Base-F.

10Base2 – стандарт IEEE 802.3a (называемый «Тонкий Ethernet» диаметр 0,2 дюма) — используется кабель RG-58, с максимальной длиной сегмента 185 метров, компьютеры присоединялись один к другому, для подключения кабеля к сетевой карте нужен Т-коннектор, а на кабеле должен быть BNC-коннектор. Требуется наличие терминаторов на каждом конце. Многие годы этот стандарт был основным для технологии Ethernet.

10Base-T- IEEE 802.3i – для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории 3 или категории-5. Максимальная длина сегмента — 100 метров.

10Base-F –IEEE 802.3j — Основной термин для обозначения семейства 10 Мбит/с Ethernet–-стандартов, использующих оптический кабель на расстоянии до 2 километров: 10BASE-FL, 10BASE-FB и 10BASE-FP. Из перечисленного только 10BASE-FL получил широкое распространение.

В 1995 году принят стандарт IEEE 802.3u Fast Ethernet со скоростью 100 Мбит/с. Для разных физических сред передачи данных также существует общее обозначение 100Base-X.

100BASE-TX обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из двух витых пар 5-й категории. Обычно передача данных в каждом направлении ведётся по одной витой паре, обеспечивая до 100 Мбит/с общей пропускной способности в дуплексе. Длина линии связи ограничена 100 метрами, но по одному стандартному кабелю, имеющему 4 пары, можно организовать два 100-мегабитных канала связи.

100BASE-T4 обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из четырёх витых пар 3-й категории.

100BASE-FX использует волоконно-оптический кабель и обеспечивает связь излучением с длиной волны 1310 нм по двум жилам — для приёма (RX) и для передачи (TX). Длина сегмента сети может достигать 400 метров в полудуплексном режиме (с гарантией обнаружения коллизий) и 2 километров в полнодуплексном при использовании многомодового волокна. Работа на больших расстояниях возможна при использовании одномодового волокна.

Гигабитный Ethernet (Gigabit Ethernet, 1 Гбит/с)

1000BASE-T, IEEE 802.3ab – основной гигабитный стандарт, опубликованный в 1999 году использует витую пару категории 5e. В передаче данных участвуют 4 пары, каждая пара используется одновременно для

передачи по обоим направлениям со скоростью – 250 Мбит/с. Используется метод кодирования PAM5 расстояние — до 100 метров.

1000BASE-TX был создан Ассоциацией Телекоммуникационной Промышленности (Telecommunications Industry Association, TIA) и опубликован в марте 2001 года как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000BASE-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001). Распространения не получил из-за высокой стоимости кабеля.

Спецификации для оптоволокна

1000BASE-SX, IEEE 802.3z – стандарт, использующий многомодовое волокно в первом окне прозрачности с длиной волны, равной 850 нм. Дальность прохождения сигнала составляет до 550 метров.

1000BASE-LX, IEEE 802.3z – стандарт, использующий одномодовое или многомодовое оптическое волокно во втором окне прозрачности с длиной волны, равной 1310 нм. Дальность прохождения сигнала зависит только от типа используемых приёмопередатчиков и, как правило, составляет для одномодового оптического волокна до 5 км и для многомодового оптического волокна до 550 метров.

1000BASE-LH (Long Haul) – стандарт использующий одномодовое волокно. Дальность прохождения сигнала без повторителя — до 100 километров1181.

10-гигабитный Ethernet (10G Ethernet, 10 Гбит/с)

Стандарт 10-гигабитного Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается поправкой IEEE 802.3ae.

В отличие от предыдущих стандартов Ethernet, в 10-гигабитных вариантах определены только полнодуплексные связи по схеме точка-точка, которые обычно подключаются к сетевым коммутаторам. Топологии с общей средой и алгоритмами CSMA/CD более не поддерживаются, в отличие от предыдущих поколений стандартов Ethernet, в 10GbE не реализована полудуплексная работа и не поддерживаются репитеры (хабы).

Стандарт 10G Ethernet определяет три группы физических интерфейсов:

10GBase-X, 10GBase-R4, 10GBase-W.

Они отличаются способом логического кодирования данных: в варианте 10Base-X применяется код 8B/10B, в остальных двух — код 64B/66B. Для передачи данных все они используют оптическую среду.

Группа 10GBase-X в настоящее время состоит из одного интерфейса подуровня PMD – 10GBase-LX4. Буква L говорит о том, что информация передается с помощью волн второго диапазона прозрачности, то есть 1310 нм.

Информация в каждом направлении передается одновременно с помощью четырех волн (что отражает цифра 4 в названии интерфейса),

мультиплексируемых на основе техники CWDM. Каждый из четырех потоков интерфейса XGMII передается в оптическом волокне со скоростью 2,5 Гбит/с. Максимальное расстояние между передатчиком и приемником стандарта 10GBase-LX4 на многомодовом волокне равно 200-300 м (в зависимости от полосы пропускания волокна), на одномодовом — 10 км.

В каждой из групп 10GBase-R и 10GBase-W может быть три варианта подуровня PMD: S, L и E в зависимости от используемого для передачи информации диапазона волн — 850, 1310 или 1550 нм соответственно. Таким образом, существуют интерфейсы lOGBase-SR, 10CBase-LR и 10GBase-ER, а также 10GBase-SW, 10GBase-LW, 10GBase-EW. Каждый из них передает информацию с помощью одной волны соответствующего диапазона.

10GBASE-SW 10GBASE-LW и 10GBASE-EW – эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192/STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.

10GBASE-T, IEEE 802.3ап-2006 — принят в июне 2006 года после 4 лет разработки. Использует витую пару **категории 6** (максимальное расстояние 55 метров) **6а** (максимальное расстояние 100 метров).

Построение LAN сетей с помощью мостов и коммутаторов Ethernet.

В первых сетях Ethernet, с применением общей разделяемой средой, с ростом количества узлов приводило к возникновению частых коллизий и падению производительности сети. Максимальное количество рабочих узлов в реалии достигало не более 30.

Преодолеть можно, выполнив логическую структуризацию сети с помощью мостов или коммутаторов (Рисунок 6.2).

Перечисленные устройства передают кадры с одного своего порта на другой, анализируя адрес назначения, помещенный в этих кадрах.

Логическая структуризация позволяет решить несколько задач, основные из них:

1) повышение производительности,
2) гибкости,
3) безопасности

и

4) управляемости сети.

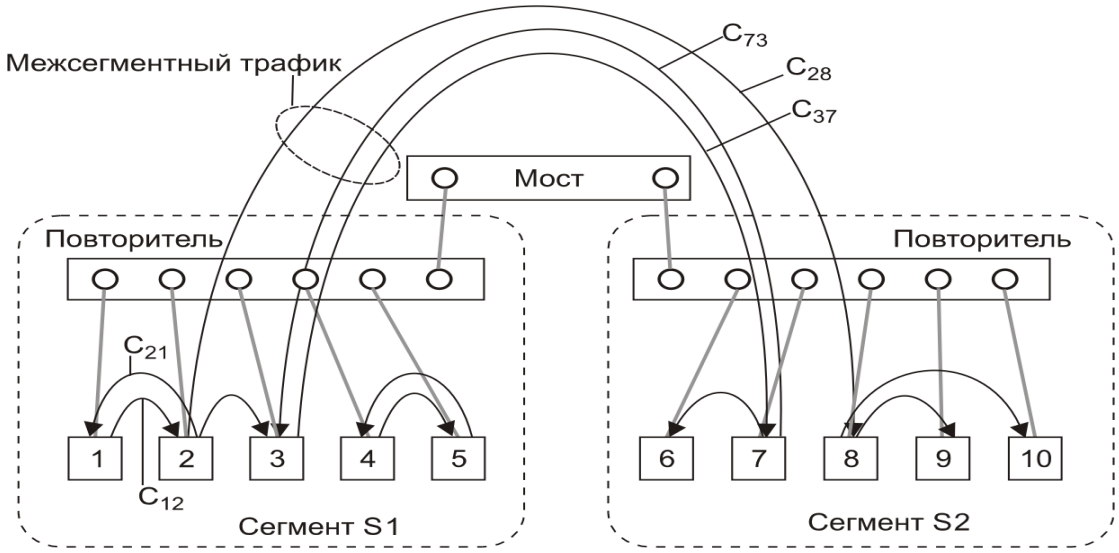


Рисунок 6.2 Логическая структуризация сети изменение нагрузки при делении сети на сегменты

Мост и коммутатор – это функциональные близнецы. Основное отличие коммутатора от моста заключается в том, мост имеет два порта и обрабатывает кадры последовательно, а коммутатор 4-48 портов и обрабатывает кадры параллельно.

Оба эти устройства продвигают кадры на основании одного и того же алгоритма, а именно **алгоритма прозрачного моста,** описанного в стандарте IEEE 802.1D.

Работа моста (коммутатора) заключается в том, что он принимает целый кадр в буфер, анализирует его и только потом перенаправляет кадр на соответствующий порт.

Для работы мост (коммутатор) применяет адресную таблицу. Причем коммутатор строит свою адресную таблицу на основании пассивного наблюдения за трафиком. При этом коммутатор учитывает адреса источников кадров данных, поступающих на порты коммутатора. По адресу источника кадра коммутатор делает вывод о принадлежности узла-источника тому или иному порту и сегменту сети.

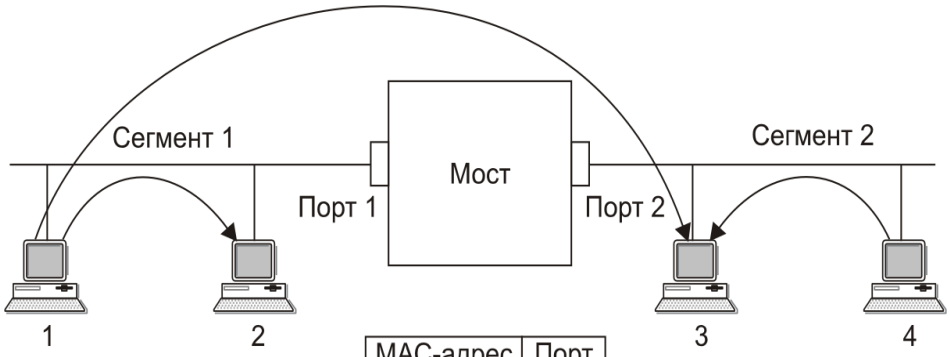
Алгоритм прозрачного моста IEEE 802.1D

Первый этап. В исходном состоянии коммутатор не знает о том, с какими MAC- адресами подключены компьютеры к каждому из его портов. В этой ситуации коммутатор просто передает любой захваченный и буферизованный кадр на все свои порты за исключением того порта, от которого этот кадр получен.

Одновременно с передачей кадра на все порты, коммутатор изучает адрес источника кадра и делает запись о его принадлежности к тому или иному порту и соответственно сегменту в своей адресной таблице.

Второй этап – анализ таблицы. Коммутатор проверяет, находятся ли компьютеры с адресами источника и назначения в одном сегменте. Если нет, то коммутатор выполняет операцию продвижения **(forwarding)** кадра – передает кадр на порт в сегмент получателя.

Если компьютеры принадлежат одному сегменту, то кадр просто удаляется из буфера. Такая операция называется фильтрацией (filtering).



MAC-адрес	Порт
1	1
2	1
3	2
4	2

Рисунок 6.3. Принцип работы прозрачного моста/коммутатора

Записи адресной таблицы могут быть динамическими, создаваемыми в процессе самообучения коммутатора, и статическими, создаваемыми вручную администратором сети**. Статические записи не имеют срока** жизни, что дает администратору возможность влиять на работу коммутатора.

Динамические записи имеют срок жизни — при создании или обновлении записи в адресной таблице ставится отметка времени. Это позволяет безболезненно переносить и подключать компьютер к другому сегменту сети.

Кадры с широковещательными MAC-адресами, как и кадры с неизвестными адресами назначения, передаются коммутатором на все его порты. Такой режим распространения кадров называется **затоплением сети** (flooding).

Нередко в результате каких-либо программных или аппаратных сбоев протокол верхнего уровня или сетевой адаптер начинают работать некорректно. Коммутатор в соответствии со своим алгоритмом передает ошибочный трафик во все сегменты. Такая ситуация называется **широковещательным штормом** (broadcast storm).

На Рисунке 6.4 показана типичная структура коммутатора. Функции доступа к среде при приеме и передаче кадров выполняют микросхемы MAC, которые идентичны микросхемам сетевого адаптера

Топологические ограничения коммутаторов в локальных сетях

Алгоритм прозрачного моста накладывает ограничение на топологию LAN с мостами и коммутаторами.

Серьезным ограничением функциональности мостов и коммутаторов является отсутствие поддержки петлеобразной конфигурации сети.

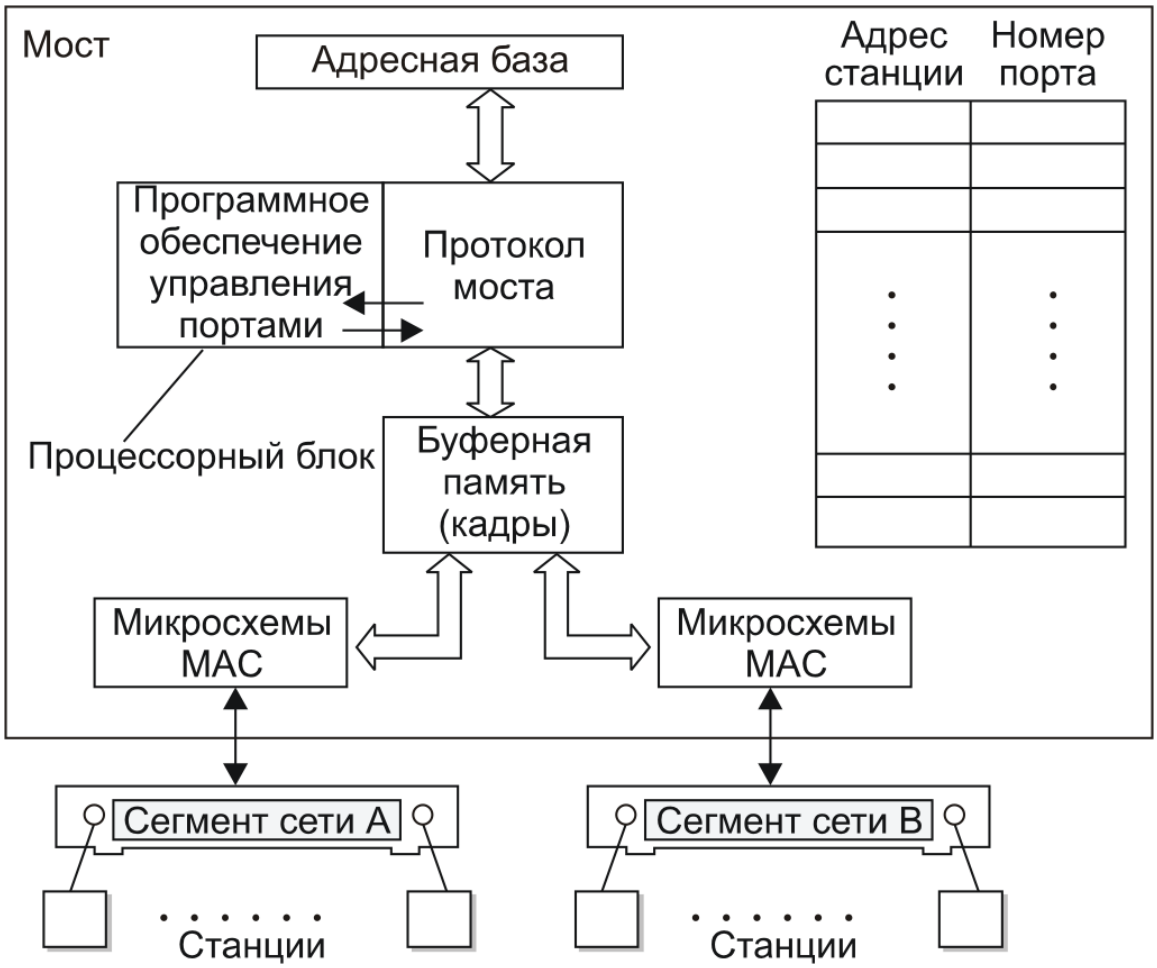


Рисунок 6.4. Структура моста/коммутатора

Например: Два сегмента Ethernet параллельно соединены двумя коммутаторами, так что образовалась петля. (Рисунок 6.5)

Последствия наличия петли в сети приводит к:

- «Размножение» кадра, то есть появление нескольких его копий
- Бесконечная циркуляция обеих копий кадра по петле в противоположных направлениях, а значит, засорение сети ненужным трафиком.
- Постоянная перестройка коммутаторами своих адресных таблиц, так как кадр с адресом источника (например 123 Рисунок 10.5) будет появляться то на одном порту, то на другом.
- В целях исключения всех этих нежелательных эффектов строить сеть с помощью коммутаторов, используя только древовидные структуры, гарантирующие наличие единственного пути между любыми двумя сегментами.
- Избыточные связи необходимо блокировать, то есть переводить их в неактивное состояние.

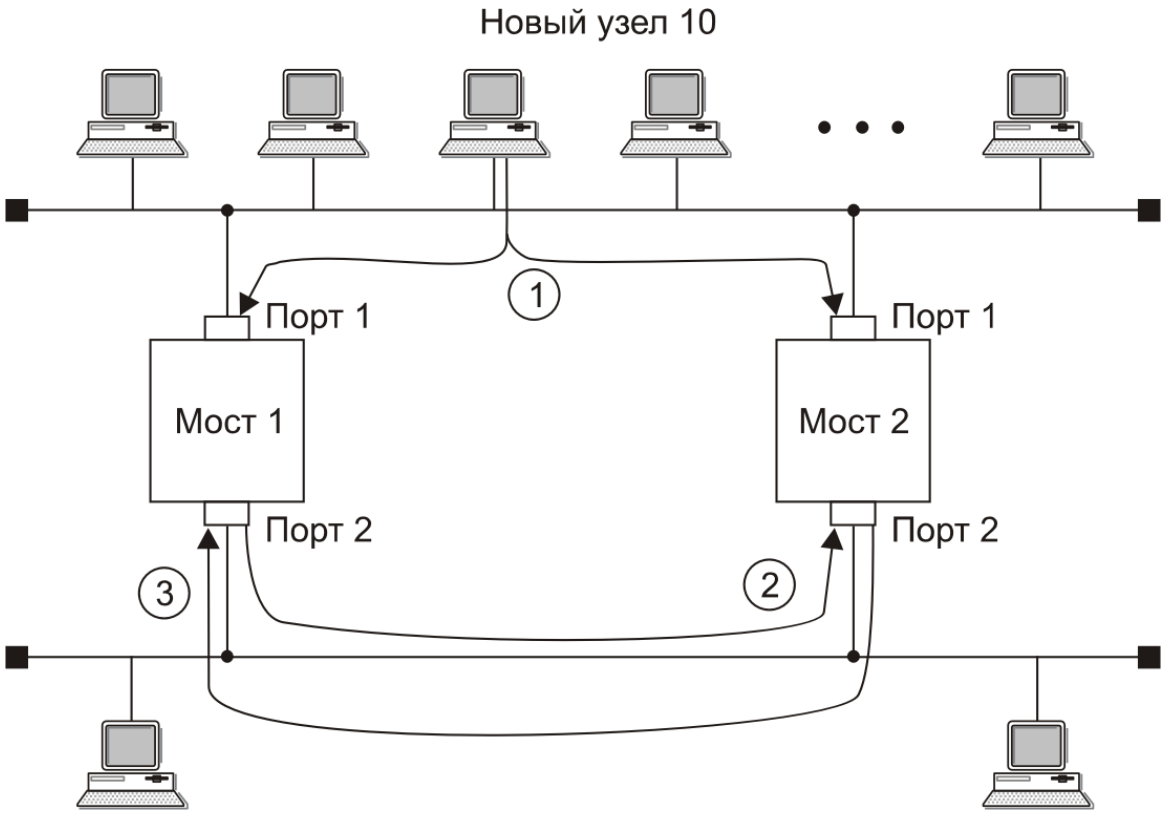


Рисунок 10.5. Влияние замкнутых маршрутов на работу коммутаторов

Два основных типа коммутации кадров коммутаторами.

Различают два основных типа коммутации кадров коммутаторами:

1) Коммутаторы с алгоритмом Kalpana (***Коммутаторы Cut-Through***) выполняют коммутацию "на лету" (on-the-*fly*), анализ кадра начинается сразу при поступлении первых шести байт кадра, после преамбулы и байта SFD.
2) Коммутаторы, которые полностью буферизируют кадр, анализирует его и только потом отправляют в другой порт. Такие коммутаторы носят название как коммутаторы **Ethernet Store-and-Forward.**

Коммутаторы Cut-Through коммутация "на лету" (on-the-*fly*).

Коммутаторы, работающие с коммутацией ***Cut-Through (***on-the-*fly)* "на лету" впервые были разработаны фирмой ***Kalpana.*** Алгоритм фирмы Kalpana состоит в следующем:

Эти коммутаторы начинают коммутацию после получения первых шести байтов кадра (6-байтовый адрес назначения). В результате время ожидания ретрансляции (задержка на коммутаторе), включающее как время буферирования, так и время коммутации (10 битовых интервалов), ***не превышает 150 битовых интервалов.***

Недостаток данного типа коммутатора состоит в том, что он ретранслирует любые пакеты как нормальные, так и заведомо ошибочные пакеты (например, с неправильной контрольной суммой) и карликовые пакеты (длиной менее 512

битовых интервалов), и ретранслирует их далее в другой сегмент, что приводит к снижению пропускной способности сети в целом.

Вторая проблема - коммутаторы данного типа часто перегружаются и плохо обрабатывают ситуацию перегрузки. Например, если из двух или более сегментов (портов) одновременно поступают пакеты, адресованные одному и тому же сегменту (порту), то в этом случае коммутатор не может одновременно передать несколько пакетов в один сегмент, поэтому часть пакетов пропадает.

Существуют коммутаторы, которые как и мост, полностью буферизируют кадр прежде чем отправить его в другой порт. Такие коммутаторы носят название как коммутаторы Ethernet Store-and-Forward (SAF).

Коммутаторы Store-and-Forward (SAF)

Коммутаторы Store-and-Forward (SAF) представляют собой наиболее дорогие, сложные и совершенные устройства данного типа.

Главное их отличие состоит в полном буферировании во внутренней буферной памяти FIFO всех ретранслируемых пакетов. Размер каждого буфера при этом должен быть не меньше максимальной длины пакета. Соответственно значительно возрастает и **задержка коммутации**. Карликовые пакеты (меньше 512 бит) и ошибочные пакеты (с неправильной контрольной суммой) таким *коммутатором* отфильтровываются, не пересылаются.

Буферная память (с организацией FIFO) может размещаться как на принимающей стороне всех портов (перед коммутацией), так и на передающей стороне портов (перед ретрансляцией), а также может быть общей для всех портов, причем эти методы часто комбинируются. Чем больше объем памяти, тем лучше *коммутатор* справляется с перегрузкой.

На Рисунке 6.6 показана идеальная в отношении производительности ситуация, когда четыре порта из восьми передают данные с максимальной для протокола Ethernet скоростью 10 Мбит/с.

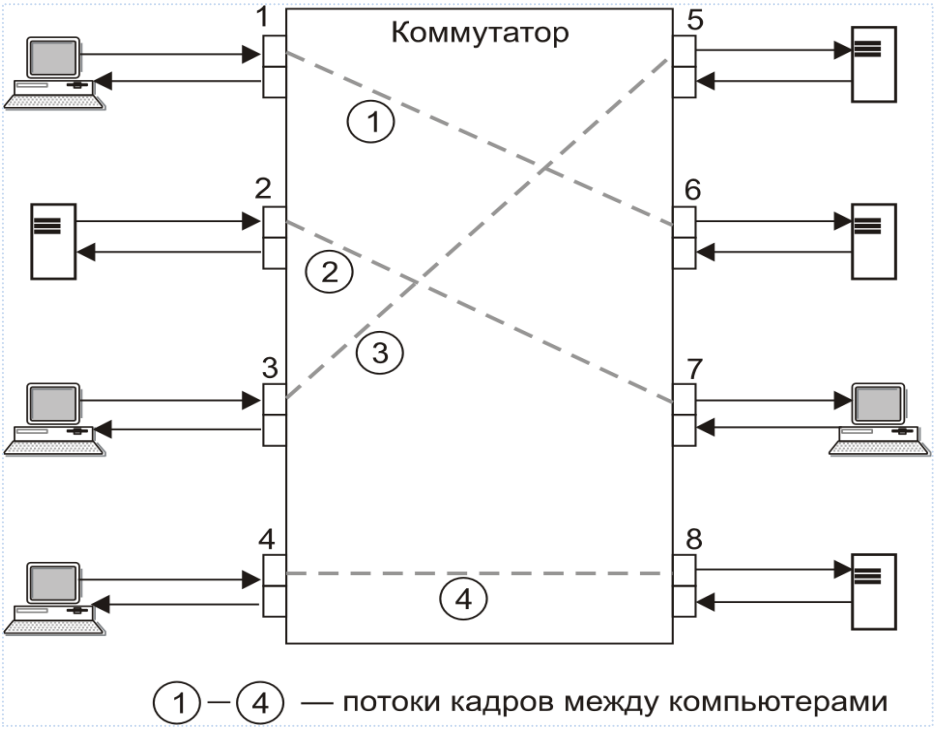


Рисунок 6.6. Параллельная передача кадров коммутатором.

Тема 7. Сети TCP/IP.

В прошлой 6-й лекции были рассмотрены различные протоколы канального уровня, таких протоколов достаточно много. Но необходимость соединять сети с различными технологиями канального уровня и глобальных сетей существовала достаточно давно, таким образом возникла необходимость в сетевом уровне, способном объединить данные сети в одну составную сеть.

Протоколов сетевого уровня также существует много, наиболее известны – это IP- протокол, NetBIOS (Network Basic Input/Output System) , IPX/SPX.

Наиболее хорошо известен, а также повсеместно применяемым является протокол IP – Internet Protocol и стек протоколов TCP/IP.

Модель TCP/IP описывает набор протоколов Интернета (RFC 1122). Название TCP/IP происходит из двух важнейших протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были первыми разработаны и описаны в данном стандарте.

Единицей данных в протоколе IP является пакет – структурированный набор байтов, состоящих из 32-битовых слов (Рисунок 7.1)

Рисунок 7.1 Структура заголовка IP-пакета версии v4.

Основными параметрами пакета являются IP- адрес отправителя и IP адрес получателя. IP-адрес состоит из двух логических частей -**номера сети** и **номера узла в сети**. IP-адрес версии IPv4 32-х битный, записывается в виде 4-х байтов, и разделенных точками, каждый байт отображается в десятичной форме, например: 128.10.2.30.

Чтобы разделить 4-х байтовый IP-адрес на адрес сети и адрес хоста используются два способа: первый использование классов **IP-адресов,** второй метод наиболее применяемый использование масок.

При классовой модели используется пять классов IP-адресов: **A, B, C, D, E.**

Таблица 7.1. Классы номеров IP

Класс	**Первые биты**	**Наименьший номер сети**	**Наибольший номер сети**	**Максимальное числю узлов в сети**
A	0	1.0.0.0 (0 - не используется)	126.0.0.0 **(127** — зарезервирован)	2^{24} поле 3 байта
B	10	128.0.0.0	191.255.0.0	2^{16}, поле 2 байта
C	110	192.0.0.0	223.255.255.0	2^{8}, поле 1 байт
D	1110	224.0.0.0	239.255.255.255	Групповые адреса
E	11110	240.0.0.0	247.255.255.255	Зарезервировано

- **Адреса класса A** назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат

идентификатор узла. Это позволяет иметь 2^7-2=126 сетей с числом узлов до 2^{24} =16 777 216 в каждой. Адреса сетей могут принимать значения от 1 до 126. Из-за ограничений, о которых будет говорится ниже, значение 0 (00000000) первого байта не используется, а значение 127 (01111111) зарезервировано для «внутренней петли».

- **К классу В** относятся все адреса, старшие два бита которых имеют значение 10. В адресах класса **В *под номер сети*** и **под номер узла** отводится по два байта. Сети, значения первых двух байтов адресов которых находятся в диапазоне от 128.0. (10000000 00000000) до 191.255 (10111111 11111111), называются сетями класса В. Ясно, что сетей класса В больше, чем сетей класса А, а размеры их меньше. Максимальное количество узлов в сетях класса В составляет 2^{16} = (65 536).
- **К классу С** относятся все адреса, старшие три бита которых имеют значение 110. **В адресах класса С под номер сети отводится 3 байта, а под номер узла 1 байт**. Сети, старшие три байта которых находятся в диапазоне от 192.0.0 (11000000 00000000 00000000) до 223.255 (11011111 11111111 11111111), называются сетями: класса С. Сети класса С наиболее распространены и имеют наименьшее максимальное число узлов-2^8 = (256).
- **Если адрес** начинается с последовательности **1110**, то он является адресом **класса D** и обозначает особый, групповой адрес (multicast address). В то время как адреса классов А, В и С используются для идентификации отдельных сетевых интерфейсов, то есть являются **индивидуальными адресами** (unicast address), **групповой адрес идентифицирует группу сетевых интерфейсов, которые в общем случае могут принадлежать разным сетям.**
- Если адрес начинается с последовательности 11110, то это значит, что данный адрес относится к **классу Е**. Адреса этого класса зарезервированы для будущих применений.

Использование масок для IP-адресации.

Схема разделения IP-адреса на номер сети и номер узла, основанная на понятии класса адреса, не является эффективной, поскольку предполагает всего 3 варианта (классы А, В и С). Например, в сети 10 компьютеров, значит необходимо использовать адреса класса С, а это диапазон 254 адреса, т. е. 244 адреса останутся незадействованными.

Для более гибкого определения границ между разрядами номеров сети и узла внутри IP-адреса используются так называемые маски подсети. Маска подсети – это 4-байтовое число специального вида, которое используется совместно с IP-адресом. "Специальный вид" маски подсети заключается в следующем: двоичные разряды маски, соответствующие разрядам IP-адреса, отведенным под номер сети, содержат единицы, а в разрядах, соответствующих разрядам номера узла – нули. Количество разрядов адреса подсети может быть различным и определяется **маской сети**.

Таким образом, **маска сети** также является 32-х разрядным двоичным числом. Разряды маски имеют следующий смысл:

1. если разряд маски равен 1, то соответствующий разряд адреса является разрядом адреса подсети;
2. если разряд маски равен 0, то соответствующий разряд адреса является разрядом хоста внутри подсети.

Все единичные разряды маски (если они есть) находятся в старшей (левой) части маски, а нулевые (если они есть) – в правой (младшей).

Для определения адреса сети на 32-х разрядный двоичный IP-адрес накладывается 32-х разрядная двоичная маска и выполняется по битно логическая операция & (И).

В компьютере каждая маска адреса хранится в виде 32-битового значения. Значения маски также могут быть представлены в виде 4-х байтов десятичными цифрами. разделенных точками, или новая синтаксическая форма, которая была разработана для адресации CIDR. (*Технология бесклассовой междоменной маршрутизации-Classless Inter-Domain Routing, CIDR*). Эта новая форма, получившая название системы обозначений CIDR, определяет, что маска, связанная с адресом, добавляется через косую черту; размер маски указывается в виде десятичного числа. Например, в первоначальной схеме на основе классов адрес 128.10.0.17 состоит из 16-битового префикса сети и 16-битового суффикса хоста. Маска сети в этом случае 255.255.0.0. С использованием адресации CIDR IP-адрес в месте с маской запишется более компактно: 128.10.0.17/16.

Разрешение IP адресов в Ethernet сетях.

Когда приложение компьютера А в локальной сети обращается к какому нибудь ресурсу в этой сети – компьютеру В, то запрос на первом этапе производится по IP-адресу компьютера В. Но в локальной сети продвижение кадров осуществляется протоколом канального уровня, т. е. для доступа к компьютеру В необходим MAC адрес компьютера В. Для получения MAC адресов, для разрешения IP адресов в MAC адреса, используются протокол **ARP (Address Resolution Protocol)**,), задача которого – преобразовать IP адрес в адрес локальной сети (для технологий Ethernet, Toking Ring, FDDI – это MAC адрес.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

Узел (компьютер, маршрутизатор и др.), которому нужно выполнить отображение IP-адреса на локальный адрес (на MAC адрес), формирует ARP запрос (Рисунок 14.3), вкладывает его в кадр протокола канального уровня (Рисунок 7.2), указывая в нем известный IP-адрес, и рассылает запрос

0 8 16 31

Тип сети		**Тип протокола**
Длина локального адреса	Длина сетевого адреса	Операция
Локальный адрес отправителя (байты 0 - 3)		
Локальный адрес отправителя (байты 4 - 5)		IP-адрес отправителя (байты 0-1)
IP-адрес отправителя (байты 2-3)		Искомый локальный адрес (байты 0 - 1)
Искомый локальный адрес (байты 2-5)		
Искомый IP-адрес (байты 0 - 3)		

широковещательно.

Рисунок 7.2 Формат пакета протокола ARP стека TCP/IP и канального Ethernet

Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета. Так как локальные адреса могут в различных типах сетей иметь различную длину, то формат пакета протокола ARP зависит от типа сети.

Маршрутизация IP-адресов.

Основная задача протокола IP – соединить разнородные локальные сети, отдельных пользователей, в единую составную, глобальную компьютерную сеть. Создание такой сети возможно только при наличии таких устройств как маршрутизаторы. Для подключения к локальным сетям или пользователям, в маршрутизаторе применяется сетевые интерфейсы (сетевые карты NIC) соответствующие тому или иному типу физической среды, стандарту и спецификации локальной сети. Каждому интерфейсу присваивается IP адрес, соответствующий IP адресу локальной сети. Маршрутизатор продвигает полученные пакеты на тот или иной интерфейс используя таблицу маршрутизации, как например Таблица 7.2.

Таблица маршрутизации обычно содержит:

- адрес сети или узла назначения, либо указание, что маршрут является маршрутом по умолчанию в этом случае значение в адресе = 0.0.0.0;
- маску сети назначения (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети);
- шлюз, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;
- интерфейс, через который доступен шлюз (в зависимости от системы, это может быть порядковый номер, GUID или символьное имя устройства; интерфейс может быть отличен от шлюза, если шлюз доступен через дополнительное сетевое устройство, например, сетевую карту);
- метрику — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

Таблица 7.2. Таблица маршрутизации

Адрес назначения	Маска	Шлюз	Метрика	Статус	TTL	Источник

198.21.17.0	255.255.255.0	198.21.17.5	0	Up		Подключена
213.34.12.0	255.255.255.0	213.34.12.3	0	Up	-	Подключена
56.0.0.0	255.0.0.0	213.34.12.4	14	Up	-	Статическая
116.0.0.0	255.0.0.0	213.34.12.4	12	Up	-	Статическая
129.13.0.0	255.255.0.0	198.21.17.6	1	Up	160	RIP

Таблица маршрутизации может быть создана вручную, либо с помощью протоколов маршрутизации. В первом случае говорят о статической маршрутизации во втором о динамической маршрутизации. Записи в таблице маршрутизации могут быть как статическими, так и динамическими.

Динамические записи создаются с помощью специальных протоколов маршрутизации – протоколов обмена маршрутной информацией.

Протоколы обмена маршрутной информацией стека TCP/IP

Все протоколы обмена маршрутной информацией стека TCP/IP относятся к классу адаптивных протоколов, которые в свою очередь делятся на две группы, каждая из которых связана с одним из двух следующих типов алгоритмов:

- дистанционно-векторный алгоритм (Distance Vector Algorithms, **DVA**);
- алгоритм состояния связей (Link State Algorithms, **LSA**).

В алгоритмах дистанционно-векторного типа каждый маршрутизатор периодически и широковещательно рассылает по сети вектор расстояний от себя до всех известных ему сетей. Под расстоянием обычно понимается число промежуточных маршрутизаторов через которые пакет должен пройти прежде, чем попадет в соответствующую сеть.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях. В больших сетях они засоряют линии связи интенсивным широковещательным трафиком. Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является **протокол RIP (Routing Information Protocol**). Преимуществом протокола RIP является его вычислительная простота, а недостатками - увеличение трафика при периодической рассылке широковещательных пакетов и не оптимальность найденного маршрута.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Широковещательная рассылка используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто. Маршрутизатор периодически обменивается короткими пакетами со своими ближайшими соседями. Этот трафик также широковещательный, но он циркулирует только между соседями и поэтому не так засоряет сеть.

Протоколом, основанным на алгоритме состояния связей, в стеке TCP/IP является **протокол OSPF.**

Протокол RIP относится к группе протоколов с дистанционно-векторным алгоритмом (DVA).

Для IP имеются две версии RIP — RIP v1 и RIP v2. Протокол RIP v1 не поддерживает масок. Протокол RIP v2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня.

Характерная таблица маршрутизации для протокола RIP представлена в Таблице 7.3.

Таблица 7.3. Таблица маршрутизации протоклла RIP

Сеть	Следующий переход	Метрика	Таймеры	Флаги
153.19.88.0	Router "A"	2	30-180-240	
198.63.35.0	Router "B"	6	30-180-240	
153.19.89.0	Router "C"	1	30-180-240	

Поля таблицы:

- ***Сеть:*** адрес сети назначения.

- ***Следующий переход:*** IP-адрес маршрутизатора, который является следующим звеном при перемещении к адресату.

- ***Метрика/Стоимость:*** Метрика маршрутизации ─ параметр критерий, по которому определяется наиболее предпочтительный маршрут.

- ***Таймер*** ─ поле на самом деле представляет три разных таймера, используемых RIP. Таймер обновления маршрутов (***routing update timer***) указывает интервал между обновлениями. Обычно RIP отсылает копию своей таблицы маршрутов каждые 30 секунд. Второй таймер – это тайм-аут для маршрута-таймера удержания (***route timeout***). Если от какой-то конкретной сети обновление маршрутов не получено в течение 180 секунд, то маршрут помечается как недостижимый. Последний таймер – это таймер удаления маршрута (***route removal timer***).

- ***Флаги:*** в поле хранятся различные необязательные данные (RIP используется нечасто).

Принцип действия протокола RIP можно пояснить следующим образом – Рисунок 7.3

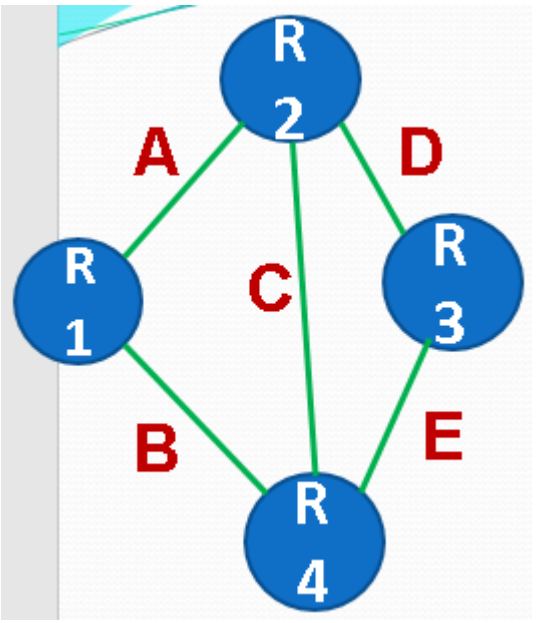


Рисунок 14.8 Принцип работы протокола RIP.

A, B, C, D, E – IP сети соответственно с IP адресами A, B, C, D, E ;

R1, R2, R3, R4– маршрутизаторы IP сетей

Вектором расстояний называется набор пар ("Сеть", "Расстояние до этой сети").

Первоначально каждый router рассылает векторы: R1: (A=1;B=1), R2: (A=1;C=1;D=1), R3:(D=1;E=1), R4: (B=1;C=1;E=1). Далее узел R1 получив по сети A вектор от R2 увеличивает расстояния на 1, т.е. (A=2;C=2;D=2), но так как в таблице имеется запись для A=1, а записи для сетей C и D отсутствуют, то в таблице маршрутизации R1 будут присутствовать записи (A=1;B=1;C=2;D=2). Аналогично вносятся записи для остальных сетей, а также в остальных узлах – routers. Ближайший маршрутизатор, который передал информацию о данном маршруте, отмечается в таблице маршрутизации как следующий (next hop).

Протокол OSPF (Open Shortest Path Firs) является достаточно современной реализацией алгоритма состояния связей (он принят в 1991 году) и обладает многими особенностями, ориентированными на применение в больших гетерогенных сетях.

OSPF имеет следующие преимущества:

- Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации;
- Поддержка сетевых масок переменной длины (VLSM);

Оптимальное использование пропускной способности с построением дерева кратчайших путей.

Принцип работы заключается в следующем:

1. После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения.
2. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. То есть они строят карту сети (топологию сети). Данная карта одинакова на всех маршрутизаторах.
3. На основе полученной информации запускается алгоритм SPF (Shortest Path First, «выбор наилучшего пути»), который

рассчитывает оптимальный маршрут к каждой сети. Данный процесс похож на построение дерева, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям. Данный процесс, то есть конвергенция, происходит очень быстро.

Протоколы DHCP

В компьютерной сети каждому интерфейсу компьютера, сервера, маршрутизатора, сетевого принтера, другого сетевого устройства необходимо назначать IP- адрес. Администратор может назначить вручную или динамически.

Если в сети 10 сетевых устройств, то такая задача достаточно простая, а когда счет идет о нескольких десятков, а то и сотен, то такая задача становится утомительной, затратной и часто приводит к ошибкам.

Для облегчения работы администраторов и был создан протокол DHCP (***Dynamic Host Configuration Protocol***).

Протокол DHCP работает в соответствии с моделью клиент-сервер. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса Рисунок 7.4. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфигурационные параметры.

Хотя основным назначением DHCP является динамическое назначение IP-адресов, но данный протокол может поддерживать и ручное назначение адресов.

При этом сервер DHCP может работать в разных режимах:

1) **ручное назначение статических адресов;**
2) **автоматическое назначение статических адресов;**
3) **автоматическое распределение динамических адресов.**

Во всех режимах работы администратор при конфигурировании DHCP-сервера сообщает ему один или несколько диапазонов IP-адресов, причем все эти адреса относятся к одной сети, то есть имеют одно и то же значение в поле номера сети.

1) В ручном режиме администратор, помимо пула доступных адресов, снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, всегда выдает определенному DHCP-клиенту один и тот же назначенный ему администратором IP-адрес (а также набор других конфигурационных параметров.

2) В режиме автоматического назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает клиенту IP-адрес из пула наличных IP-адресов. Адрес дается клиенту из пула в постоянное пользование, то есть между идентифицирующей

информацией клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает клиенту тот же самый IP-адрес.

3) При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, DHCP-клиент, удаляется из подсети, назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес.

Администратор управляет процессом конфигурирования сети, определяя два основных параметра конфигурации DHCP-сервера: **пул адресов**, доступных распределению, и **срок аренды**. Срок аренды диктует, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от DHCP-сервера. Срок аренды зависит от режима работы пользователей сети. Если это небольшая сеть учебного заведения, куда со своими компьютерами приходят многочисленные студенты для выполнения лабораторных работ, то срок аренды может быть равен длительности лабораторной работы. Если же это корпоративная сеть, в которой сотрудники предприятия работают на регулярной основе, то срок аренды может быть достаточно длительным — несколько дней или даже недель.

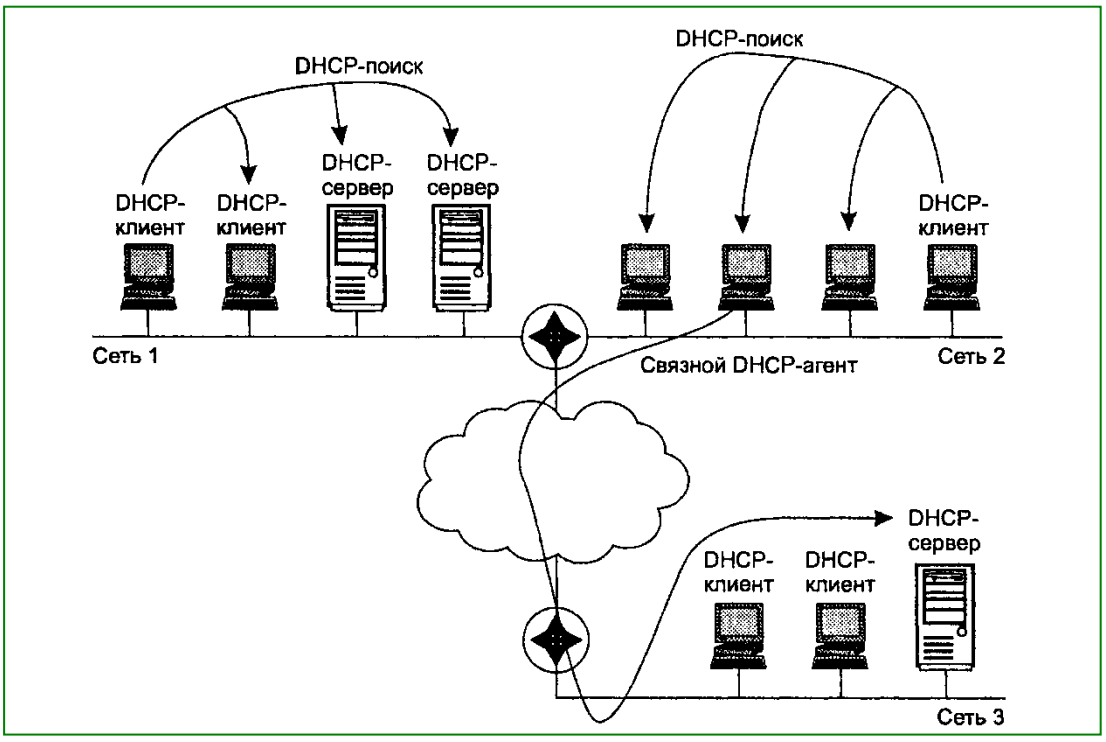


Рисунок 7.4. Схемы взаимного расположение серверов и клиентов DHCP

DHCP-сервер должен находиться в одной подсети с клиентами, учитывая, что клиенты посылают ему широковещательные запросы. Для снижения риска выхода сети из строя из-за отказа DHCP-сервера в сети иногда ставят резервный DHCP-сервер (такой вариант соответствует сети 1 на Рисунок 7.4).

Иногда наблюдается и обратная картина: в сети нет ни одного DHCP-сервера, его подменяет связной DHCP-агент — программное обеспечение, играющее роль посредника между DHCP-клиентами и DHCP-серверами (пример такого варианта — сеть 2 на Рисунке 7.4). Связной агент переправляет запросы клиентов из сети 2 DHCP-серверу сети 3. Таким образом, один DHCP-сервер может обслуживать DHCP-клиентов нескольких разных сетей.

Протокол ICMP.

Протокол обмена управляющими сообщениями ICMP (Internet Control Message Protocol) позволяет маршрутизатору сообщить конечному узлу об ошибках, с которыми маршрутизатор столкнулся при передаче какого-либо IP-пакета от данного конечного узла. Управляющие сообщения ICMP не могут направляться промежуточному маршрутизатору, который участвовал в передаче пакета, с которым возникли проблемы, так как для такой посылки нет адресной информации - пакет несет в себе только адрес источника и адрес назначения, не фиксируя адреса промежуточных маршрутизаторов. Протокол ICMP - это протокол сообщения об ошибках, а не протокол коррекции ошибок. Конечный узел может предпринять некоторые действия для того, чтобы ошибка больше не возникала, но эти действия протоколом ICMP не регламентируются. Каждое сообщение протокола ICMP передается по сети внутри пакета IP. Пакеты IP с сообщениями ICMP маршрутизируются точно так же, как и любые другие пакеты, без приоритетов, поэтому они также могут теряться. Кроме того, в загруженной сети они могут вызывать дополнительную загрузку маршрутизаторов. Для того, чтобы не вызывать лавины сообщения об ошибках, потери пакетов IP, переносящие сообщения ICMP об ошибках, не могут порождать новые сообщения ICMP.

Помимо диагностики ICMP также используется для мониторинга сети. Так, в основе популярных утилит для мониторинга IP-сетей ping и tracert лежат ICMP-сообщения. С помощью ICMP-сообщений приложение может определить маршрут перемещения данных, оценить работоспособность сети, определить время прохождения данных до заданного узла, сделать запрос о значении маски определенного сетевого интерфейса и т. п.

Все типы ICMP-сообщений могут быть разделены на два класса:

- диагностические сообщения об ошибках;
- информационные сообщения типа запрос/ответ.

ICMP-сообщение инкапсулируется в поле данных IP-пакета.

IPv6 как развитие стека TCP/IP.

За время существования протокола IPv4 были созданы множества новых протоколов для стека TCP/IP, которые решали новые задачи, как например защищенный протокол IP (IPSec), протокол коммутации меток (MPLS) и т. п. Однако было ясно, что только за счет добавления новых протоколов

технологию TCP/IP развивать нельзя – нужно решиться на модернизацию сердцевины стека, протокола IP. Наиболее очевидной проблемой такого рода была проблема дефицита IP-адресов, которую невозможно снять, не расширив размер полей адресов источника и приемника.

В результате сообщество Интернета после достаточно долгого обсуждения решило подвергнуть протокол IP серьезной переработке, выбрав в качестве *основных целей модернизации*:

создание масштабируемой схемы адресации;

сокращение объема работ, выполняемых маршрутизаторами;

предоставление гарантий качества транспортных услуг;

обеспечение зашиты данных, передаваемых по сети.

Документом, фиксирующим появление IPv6, стал RFC 1752. Базовый набор протоколов IPv6 был принят IETF в сентябре 1995 года. В августе 1998 года были приняты пересмотренные версии группы стандартов, определяющих как общую архитектуру IPv6 (RFC 2460), так и его отдельные аспекты, например систему адресации (RFC 2373).

Новая, шестая версия протокола IP (IPv6) внесла существенные изменения в систему адресации IP-сетей (RFC 2373). И, прежде всего, это коснулось увеличения разрядности адреса. **IPv6-адрес состоит из 128 бит**, **или 16 байт**. Это дает возможность пронумеровать огромное количество узлов:

340 282 366 920 938 463 463 374 607 431 762 211 456.

Главной целью изменения системы адресации было не механическое увеличение адресного пространства, а повышение эффективности работы стека TCP/IP в целом.

- Вместо прежних двух уровней иерархии адреса (номер сети и номер узла) в IPv6 имеется 4 уровня, из которых три уровня используются для идентификации сетей, а один — для идентификации узлов сети. За счет увеличения числа уровней иерархии в адресе новый протокол эффективно поддерживает технологию CIDR. Благодаря этому, а также усовершенствованной системе групповой адресации и введению нового типов адресов новая версия IP позволяет ***снизить затраты на маршрутизацию***.
- Произошли и чисто внешние изменения — разработчики стандарта предложили использовать вместо десятичной ***шестнадцатеричную*** форму записи IP-адреса. Каждые четыре шестнадцатеричные цифры отделяются друг от друга двоеточием. Вот как, например, может выглядеть адрес IPv6:
- **FEDC:0A98:0:0:0:0:7654:3210** ***(24-е шестиадцатеричных цифры)***.

Если в адресе имеется длинная последовательность нулей, то запись адреса можно сократить. Например, приведенный выше адрес можно записать и так:

FEDC:0A98::7654:3210. Сокращение в виде двух двоеточий (::) может употребляться в адресе только один раз. Можно также опускать незначащие нули в начале каждого поля адреса, например, вместо FEDC:0A98::7654:3210 можно писать FEDC:A98::7654:3210.

Для сетей, поддерживающих обе версии протокола (IPv4 и IPv6), разрешается использовать для младших 4 байт традиционную для IPv4 десятичную запись: 0:0:0:0:0:FFFF:129.144.52.38 или ::FFFF:129.144.52.38.

В новой версии IPv6 предусмотрено ***три основных типа адресов***: **индивидуальные адреса**, **групповые адреса** и **адреса произвольной рассылки**. Тип адреса определяется значением нескольких старших битов адреса, которые названы префиксом формата.

Типы адресов

- **Индивидуальный адрес (unicast)** определяет уникальный идентификатор отдельного интерфейса конечного узла или маршрутизатора. Назначение адреса этого типа совпадает с назначением уникальных адресов в версии IPv4 — с их помощью пакеты доставляются определенному интерфейсу узла назначения. Индивидуальные адреса делятся на несколько подтипов для отражения специфики некоторых часто встречающихся в современных сетях ситуаций.
- **Групповой адрес (multicast) IPv6** аналогичен по назначению групповому адресу IPv4. Он идентифицирует группу интерфейсов, относящихся, как правило, к разным узлам. Пакет с таким адресом доставляется ***всем*** интерфейсам с этим адресом. Групповые адреса используются в IPv6 для замены Широковещательных адресов – для этого вводится адрес особой группы, объединяющей все интерфейсы подсети.
- **Адрес произвольной рассылки (anycast)** — это новый тип адреса, который так же. как и групповой адрес, определяет группу интерфейсов. Однако пакет с таким адресом доставляется ***любому*** из интерфейсов группы, как правило, «ближайшему» в соответствии с метрикой, используемой протоколами маршрутизации. Синтаксически адрес произвольной рассылки ничем не отличается от индивидуального адреса и назначается из того же диапазона адресов. Адрес произвольной рассылки может быть назначен только интерфейсам маршрутизатора. Интерфейсы маршрутизаторов, входящие в одну группу произвольной рассылки, имеют индивидуальные адреса и, кроме того, общий адрес группы произвольной рассылки. Адреса такого типа ориентированы на маршрутизацию от источника, при которой маршрут прохождения пакета определяется узлом-отправителем путем указания IP-адресов всех промежуточных маршрутизаторов.

Например, поставщик услуг может присвоить всем своим маршрутизаторам один и тот же адрес произвольной рассылки и сообщить его абонентам. Если абонент желает, чтобы его пакеты передавались через сеть этого поставщика услуг, то ему достаточно указать этот адрес в цепочке

адресов маршрута от источника, и пакет будет передан через ближайший маршрутизатор данного поставщика услуг

Так же как и в IPv4, в IPv6 имеются так называемые частные адреса, предназначенные для использования в автономных сетях. В отличие от версии IPv4 в версии IPv6 эти адреса представлены двумя разновидностями:

- Адреса локальных сетей, не разделенных на подсети, содержат только 64-разрядное поле идентификатора интерфейса, а остальные разряды, кроме префикса формата, должны быть нулевыми, поскольку потребность в номере подсети здесь отсутствует.
- Адреса локальных сетей, разделенных на подсети, содержат по сравнению с предыдущими адресами дополнительное двухбайтовое поле номера подсети.

Основным подтипом индивидуального адреса является ***глобальный агрегируемый уникальный адрес***. Такие адреса могут агрегироваться для упрощения маршрутизации. В отличие от уникальных адресов узлов версии IPv4, которые состоят из двух полей — номера сети и номера узла, глобальные агрегируемые уникальные адреса IPv6 имеют более сложную структуру, включающую шесть полей (Рисунок 7.5)

Префикс формата (Format Prefix, FP) для этого типа адресов имеет размер три бита и значение 001. Следующие три поля — агрегирования верхнего (Top-Level Aggregation, TLA), следующего (Next-Level Aggregation, NLA) и местного (Site-Level Aggregation, SLA) уровней — описывают три уровня идентификации сетей.

3¤	13¤	8¤	24¤	16¤	64¤
Префикс·формата·(FP)¤	Агрегирование·верхнего·уровня·(TLA)¤	¤	Агрегирование·следующего·уровня(NLA)·¤	Агрегирование·местного·уровня(SLA)·¤	Идентификатор·интерфейса··(Interface·ID)¤

Рисунок 7.5 Структура глобального агрегируемого уникального адреса в пакете IPv6.

Поле TLA предназначено для идентификации сетей самых крупных поставщиков услуг. Конкретное значение этого поля представляет собой общую часть адресов, которыми располагает данный поставщик услуг. Сравнительно небольшое количество разрядов, отведенных под это поле (13). выбрано специально для ограничения размера таблиц маршрутизации в магистральных маршрутизаторах самого верхнего уровня Интернета. Это поле позволяет перенумеровать 8196 сетей поставщиков услуг верхнего уровня, а значит, число записей, описывающих маршруты между этими сетями, также будет ограничено значением 8196, что ускорит работу магистральных

маршрутизаторов. Следующие 8 разрядов зарезервированы на будущее для расширения при необходимости поля TLA.

Поле NLA предназначено для нумерации сетей средних и мелких поставщиков услуг. Значительный размер поля NLA позволяет путем агрегирования адресов отразить многоуровневую иерархию поставщиков услуг.

Поле SLA предназначено для адресации подсетей отдельного абонента, например подсетей одной корпоративной сети. Предполагается, что поставщик услуг назначает некоторому предприятию номер его сети, состоящий из фиксированного значения полей TLA и NLA. которые в совокупности являются аналогом номера сети версии IPv4. Остальная часть адреса — поля SLA и идентификатор интерфейса — поступает в распоряжение администратора корпоративной сети, который полностью берет на себя формирование адреса и не должен согласовывать этот процесс с поставщиком услуг. Причем поле идентификатора интерфейса имеет вполне определенное назначение — оно должно хранить физический адрес узла. На этом уровне также можно агрегировать адреса небольших подсетей в более крупные подсети, и размер поля SLA в 16 бит обеспечивает достаточную свободу и гибкость построения внутри-корпоративной иерархии адресов.

Идентификатор интерфейса является аналогом номера узла в IPv4. Отличием версии IPv6 является то, что в общем случае идентификатор интерфейса просто совпадает с его локальным (аппаратным) адресом, а не представляет собой произвольно назначенный администратором номер узла. Идентификатор интерфейса имеет длину 64 бита, что позволяет поместить туда MAC-адрес (48 бит), адрес X.25 (до 60 бит), адрес конечного узла ATM (48 бит) или номер виртуального соединения ATM (до 28 бит), а также, вероятно, даст возможность использовать локальные адреса технологий, которые могут появиться в будущем. Таким образом в большинстве случаев отпадает необходимость ручного конфигурирования конечных узлов, так как младшую часть адреса — идентификатор интерфейса — узел узнает от аппаратуры (сетевого адаптера и т. п.), а старшую — номер подсети — ему сообщает маршрутизатор.

В IP-пакета Ver 6 приобретает особое значение. Разработчики стандартов IPv6 считают, что агрегирование адресов является основным способом эффективного использования адресного пространства в новой версии протокола IP.

Пример

- Пусть клиент получил от поставщика услуг пул адресов IPv6, определяемый следующим префиксом:
- 20:0A:00:C9:74:05/48.

Давайте проведем анализ этого числа. Поскольку его первые 3 бита равны 001, следовательно, это ***глобальный агрегируемый уникальный адрес*** (Рисунок 7.6).

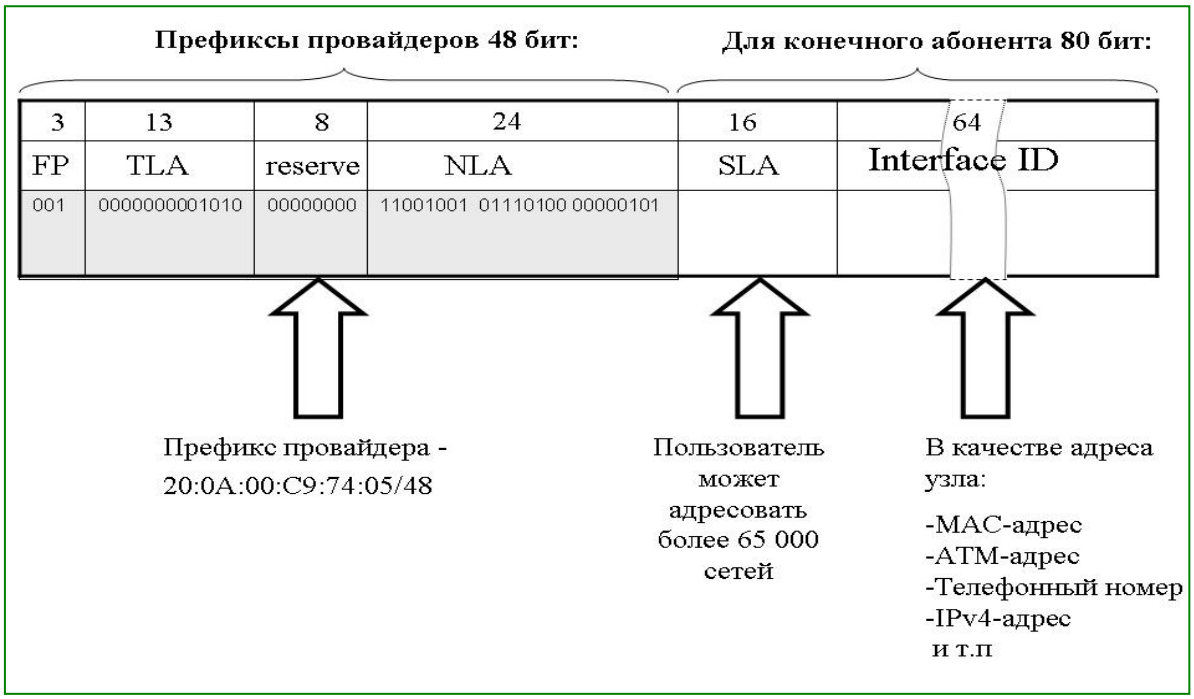


Рисунок 7.6 Пример глобального агрегируемого адреса

Пусть, например, следующий байт (01110100) в поле NLA поставщик услуг использовал для передачи поставщику услуг более низкого (третьего) уровня, а тот, в свою очередь, использовал последний байт поля NLA для назначения пула адресов клиенту. Таким образом, с участием поставщиков услуг трех уровней был сформирован префикс 20:OA:00:C9:74:05/48, который получил клиент.

Протокол IPv6 оставляет в полном распоряжении клиента 2 байта (поле SLA) для нумерации сетей и 8 байт (полем идентификатора интерфейса) для нумерации узлов. Имея такой огромный диапазон номеров подсетей, администратор может использовать его по-разному. Он может выбрать простую плоскую организацию своей сети, назначая каждой имеющейся подсети определенное значение из диапазона в 65 535 адресов, игнорируя оставшиеся.

Помимо подробно рассмотренного выше глобального агрегируемого адреса, существуют и другие разновидности индивидуального адреса.

Адрес обратной петли **0:0:0:0:0:0:0:1** играет в версии IPv6 ту же роль, что и адрес **127.0.0.1** в версии IPv4.

Неопределенный адрес, состоящий из одних нулей, является аналогом адреса **0.0.0.0** протокола IPv4. Этот адрес может появляться в IP-пакетах только в качестве адреса источника, и это означает, что пакет послан до того, как узел изучил свой IP-адрес (например, до получения его от DHCP-сервера).

Поддержка протокола IPv6 адресов IPv4

Предполагается, что довольно большое время будут сосуществовать островки Интернета, работающие по протоколу IPv6, и остальная часть Интернета, работающая на версии IPv4. Для того чтобы узлы, поддерживающие версию IPv6, могли использовать технику передачи пакетов IPv6 через сеть

IPv4 в автоматическом режиме, разработан специальный подтип адресов, которые переносят IPv4- адрес в младшие 4-х байтах IPv6- адреса, а в старших 12 байтах адреса содержат нули (Рисунок 7.7). Такие индивидуальные адреса делают очень простой процедуру преобразования адресов между двумя версиями протокола IP и называются IPv4-совместными IPv6-адресами.

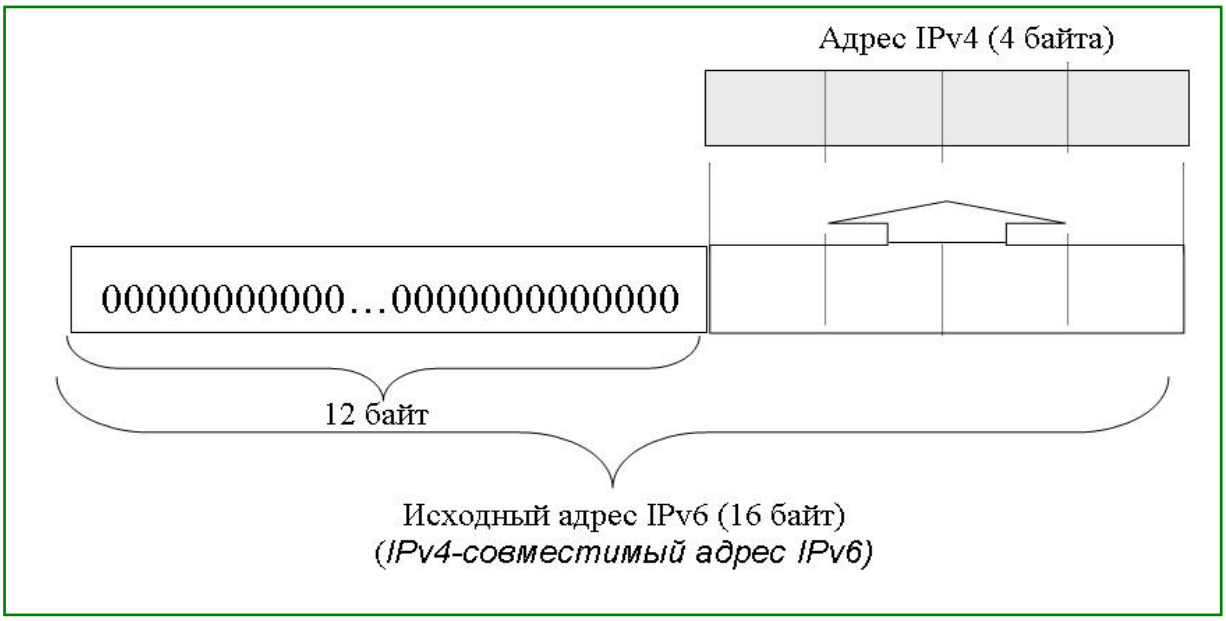


Рисунок 7.7. Преобразование IPv6 в IPv4.

Для решения обратной задачи — ***передачи IPv4-пакетов через части Интернета, работающие по протоколу IPv6, — предназначен IPv4-*** отображенный IPv6-адрес. Этот тип адреса по-прежнему содержит в 4-х младших байтах IPv4-адрес, и в старших 10-ти байтах — нули, а в 5-м и 6-м байтах IPv6-адреса — единицы, которые показывают, что узел поддерживает только 4-ю версию протокола IP (Рисунок 7.8.).

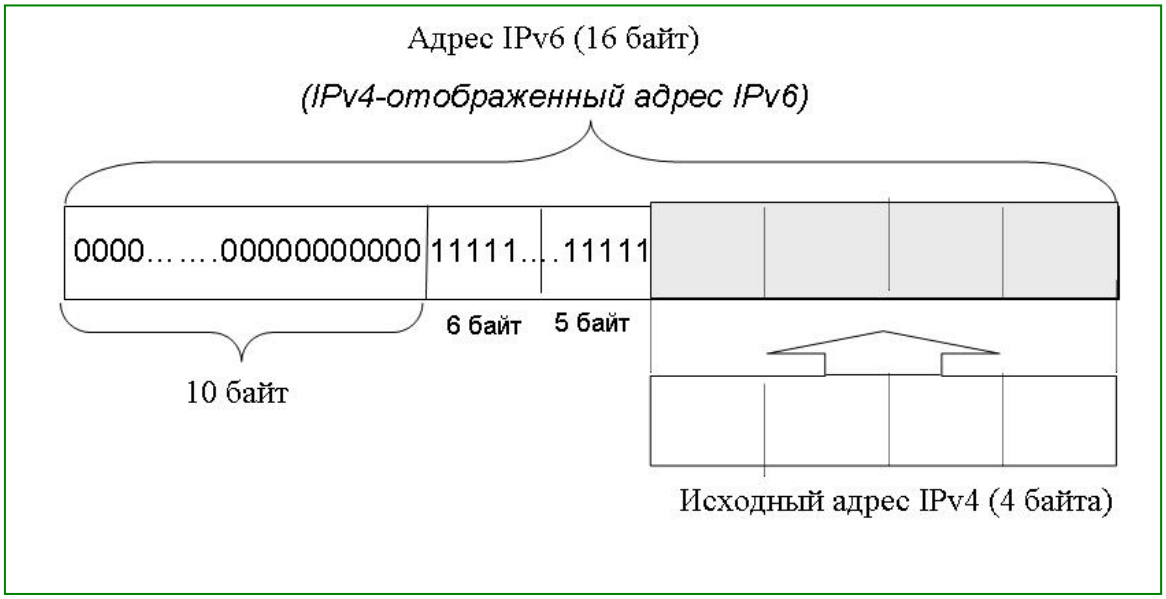


Рисунок 7.8. Преобразование IPv4 в IPv6

Тема 8. Глобальная сеть Интернет.

Интернет (Internet) – всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины (World Wide Web, WWW) и множества других систем (протоколов) передачи данных. Часто упоминается как Всемирная сеть и Глобальная сет.

В настоящее время под словом «Интернет» чаще всего имеется в виду Всемирная паутина и доступная в ней информация, а не физическая сеть.

В России День Интернета празднуется 30 сентября.

К середине 2008 года число пользователей, регулярно использующих Интернет, составило около 1,5 млрд человек (около четверти населения Земли). Вместе с подключёнными к нему компьютерами, Интернет служит основой для развития информационного общества.

Свое начало Интернет берет в 1957 году когда Министерство обороны США посчитало, что на случай глобальной войны США нужна надёжная система передачи информации. Агентство передовых оборонных исследовательских проектов США (DARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэнфордскому исследовательскому центру, Университету Юты и Университету штата Калифорния в Санта-Барбаре. Компьютерная сеть была названа ARPANET (англ. Advanced Research Projects Agency Network), и в 1969 году в рамках проекта сеть объединила четыре указанных научных учреждения. Все работы финансировались Министерством обороны США. Затем сеть ARPANET начала активно расти и развиваться, её начали использовать учёные из разных областей науки.

Первый сервер ARPANET был установлен 2 сентября 1969 года в Калифорнийском университете в Лос-Анджелесе. Компьютер Honeywell DP -516 имел 24 Кб оперативной памяти.

29 октября 1969 года в 21:00 между двумя первыми узлами сети ARPANET, находящимися на расстоянии в 640 км — в Калифорнийском университете Лос-Анджелеса (UCLA) и в Стэнфордском исследовательском институте (SRI) — провели сеанс связи. Чарли Клайн (Charley Kline) пытался выполнить удалённое подключение к компьютеру в SRI. Успешную передачу каждого введённого символа его коллега Билл Дювалль (Bill Duvall) из SRI подтверждал по телефону.

В первый раз удалось отправить всего три символа «LOG», после чего сеть перестала функционировать. LOG должно было быть словом LOGON (команда входа в систему). В рабочее состояние систему вернули уже к 22:30 и следующая попытка оказалась успешной. Именно эту дату можно считать днём рождения Интернета.

К 1971 году была разработана первая программа для отправки электронной почты по сети.

В 1973 году к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1970-х годах сеть в основном использовалась для пересылки электронной почты, тогда же появились первые списки почтовой рассылки, новостные группы и доски объявлений. Однако в то время сеть ещё не могла легко взаимодействовать с другими сетями, построенными на других технических стандартах. К концу 1970-х годов начали бурно развиваться протоколы передачи данных, которые были стандартизированы в 1982—83 годах. Активную роль в разработке и стандартизации сетевых протоколов играл Джон Постел. 1 января 1983 года сеть ARPANET перешла с протокола NCP на TCP/IP, который успешно применяется до сих пор для объединения сетей. Именно в 1983 году термин «Интернет» закрепился за сетью ARPANET.

В 1984 году была разработана система доменных имён (англ. Domain Name System, DNS).

В 1984 году у сети ARPANET появился серьёзный соперник: Национальный научный фонд США (NSF) основал обширную межуниверситетскую сеть NSFNet (англ. National Science Foundation Network), которая была составлена из более мелких сетей (включая известные тогда сети Usenet и Bitnet) и имела гораздо большую пропускную способность, чем ARPANET. К этой сети за год подключились около 10 тыс. компьютеров, звание «Интернет» начало плавно переходить к NSFNet.

В 1988 году был разработан протокол Internet Relay Chat (IRC), благодаря чему в Интернете стало возможно общение в реальном времени (чат).

В 1989 году в Европе, в стенах Европейского совета по ядерным исследованиям (фр. Conseil Européen pour la Recherche Nucléaire, CERN) родилась концепция Всемирной паутины. Её предложил знаменитый британский учёный Тим Бернерс-Ли, он же в течение двух лет разработал протокол HTTP, язык HTML и идентификаторы URI.

Соавтор Тима Бернерса-Ли по формулировке целей и задач проекта World Wide Web в CERN, бельгийский исследователь Роберт Кайо разъяснял позднее его понимание истоков этого проекта: «История всех великих изобретений, как это давно и хорошо известно, базируется на большом числе им предшествующих. В случае Всемирной паутины (WWW) следовало бы в этом контексте, видимо, отметить по крайней мере два важнейших для успеха проекта пути развития и накопления знаний и технологий: 1) история развития систем типа гипертекста …; 2) Интернет-протокол, который собственно и сделал всемирную сеть компьютеров наблюдаемой реальностью».

В 1990 году сеть ARPANET прекратила своё существование, полностью проиграв конкуренцию NSFNet. В процессе своего развития топология сети Интернет прошла развитие (Рисунок 8.1):

1. Централизованные сети передачи данных.

2. Ячеистые децентрализованные сети.

3. Сетевой децентрализованный принцип построения сети.

В том же году было зафиксировано первое подключение к Интернету по телефонной линии (т. н. «дозвон» – англ. Dialup access).

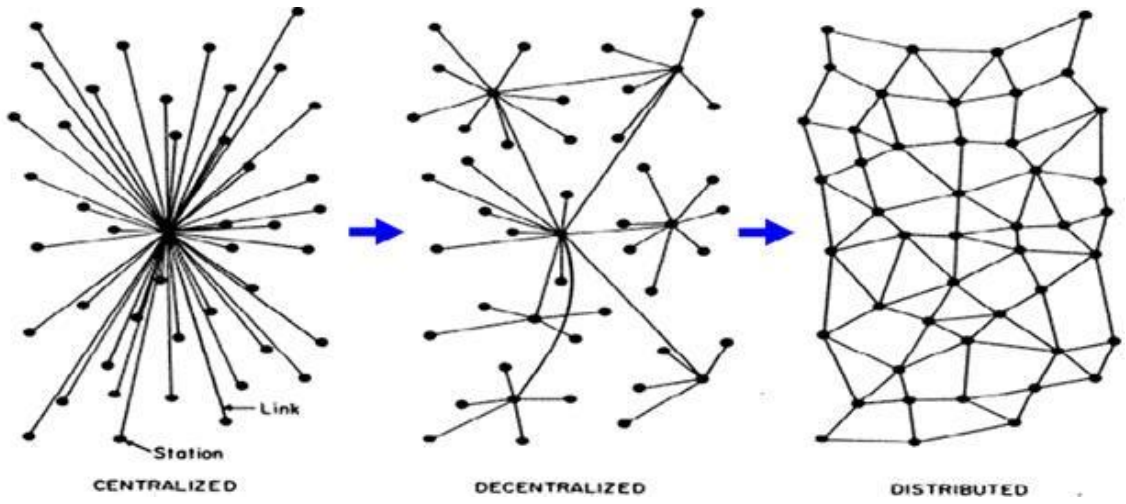


Рисунок 8.1 – Топологические изменения сети Интернет

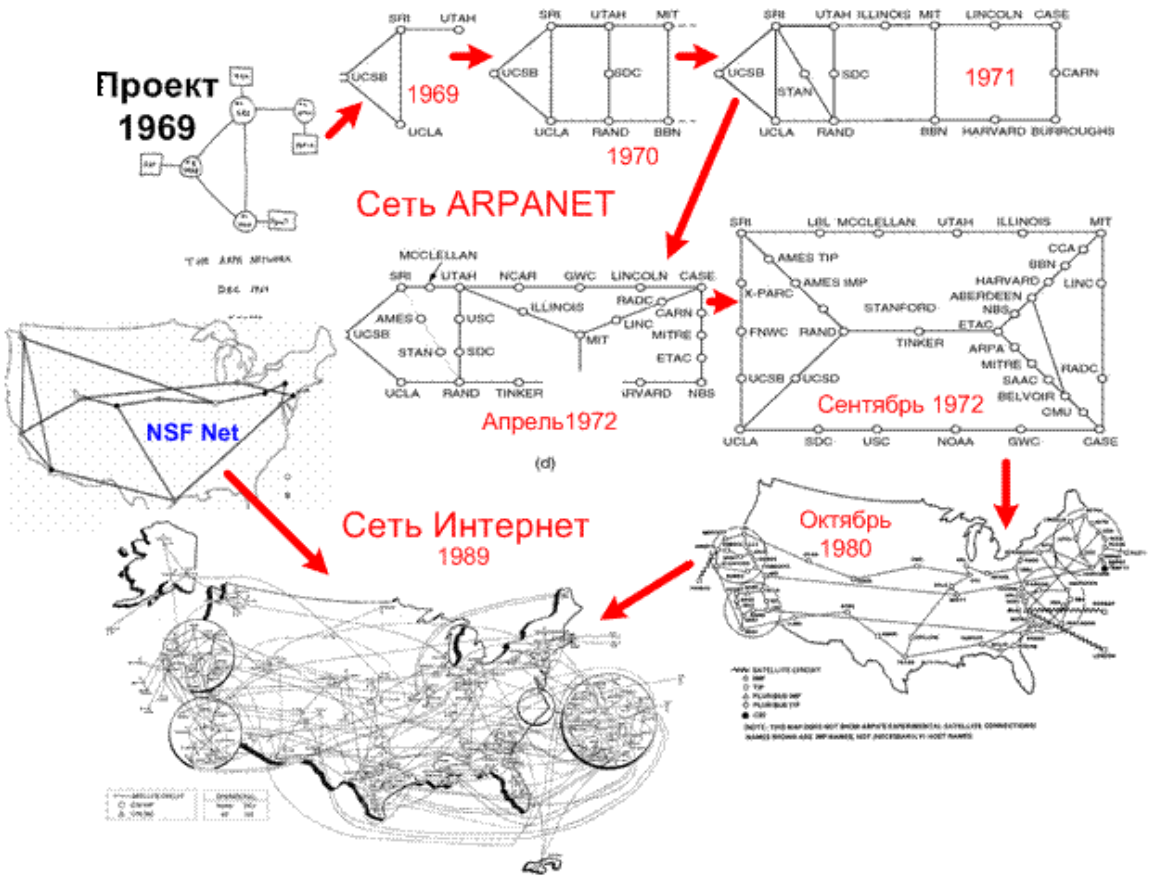


Рисунок 8.2 – Эволюционное развитие сети Интернет

В 1991 году Всемирная паутина стала общедоступна в Интернете, а в 1993 году появился веб-браузер NCSA Mosaic. Именно сочетание веб-протокола от Тима Бернерс-Ли, который обеспечивал коммуникацию, и браузера (Mosaic) от Марка Андриссена, который предоставил функционально совершенный пользовательский интерфейс, создало условия для активного интереса к Веб (WWW). За первые 24 месяца, истекшие после появления браузера Mosaic, Web прошел стадию от полной неизвестности до абсолютно мировой распространенности.

В 1995 году сеть NSFNet вернулась к роли исследовательской сети, маршрутизацией всего трафика Интернета теперь занимались сетевые провайдеры, а не суперкомпьютеры Национального научного фонда.

В том же 1995 году Всемирная паутина стала основным поставщиком информации в Интернете, обогнав по трафику протокол пересылки файлов FTP. Был образован Консорциум всемирной паутины (W3C). Можно сказать, что Всемирная паутина преобразила Интернет и создала его современный облик. С 1996 года Всемирная паутина почти полностью подменяет собой понятие «Интернет».

В 1990-е годы Интернет объединил в себе большинство существовавших тогда сетей (хотя некоторые, как Фидонет, остались обособленными). Объединение выглядело привлекательным благодаря отсутствию единого руководства, а также благодаря открытости технических стандартов Интернета, что делало сети независимыми от бизнеса и конкретных компаний.

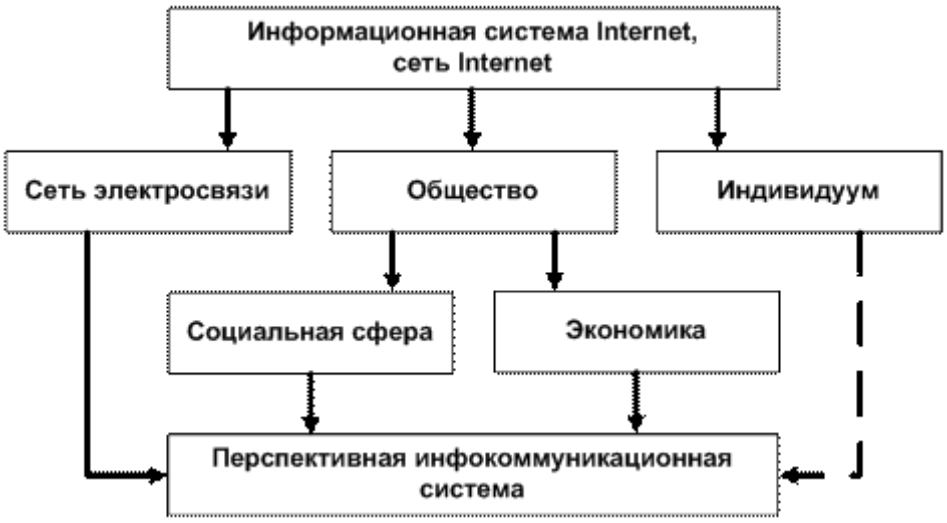


Рисунок 8.3 – Влияние сети Интернет

К 1997 году в Интернете насчитывалось уже около 10 млн компьютеров, было зарегистрировано более 1 млн доменных имён. Интернет стал очень популярным средством для обмена информацией. В настоящее время подключиться к Интернету можно через спутники связи, радио-каналы, кабельное телевидение, телефон, сотовую связь, специальные оптико-волоконные линии или электропровода. В течение 5 лет Интернет достиг аудитории свыше 50 миллионов пользователей. Другим средствам массовой

информации требовалось гораздо больше времени для достижения такой популярности: радио – 38 лет; телевидению – 13 лет. Всемирная сеть стала неотъемлемой частью жизни в развитых и развивающихся странах и оказывает существенно влияние на социальные, экономические и даже политические процессы на Земле.

В настоящее время Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей. Объединение сетей разной архитектуры и топологии стало возможно благодаря протоколу IP и принципу маршрутизации пакетов данных. Протокол IP на котором основано сетевое взаимодействие в Сети Интернет был специально создан независимым по отношению к физическим средам и каналам связи. Это позволило любой вычислительной системе или сети передачи данных, проводной или беспроводной, которая поддерживает инкапсуляцию IP-пакетов, подключаться и передавать трафик Интернет.

На стыках сетей специальные маршрутизаторы (программные или аппаратные) занимаются автоматической сортировкой и перенаправлением пакетов данных, исходя из IP-адресов получателей этих пакетов. Протокол IP образует единое адресное пространство в масштабах всего мира. Такая организация IP-адресов позволяет маршрутизаторам однозначно определять дальнейшее направление для каждого пакета данных. В результате между отдельными сетями Интернета не возникает конфликтов, и данные беспрепятственно и точно передаются из сети в сеть по всей планете.

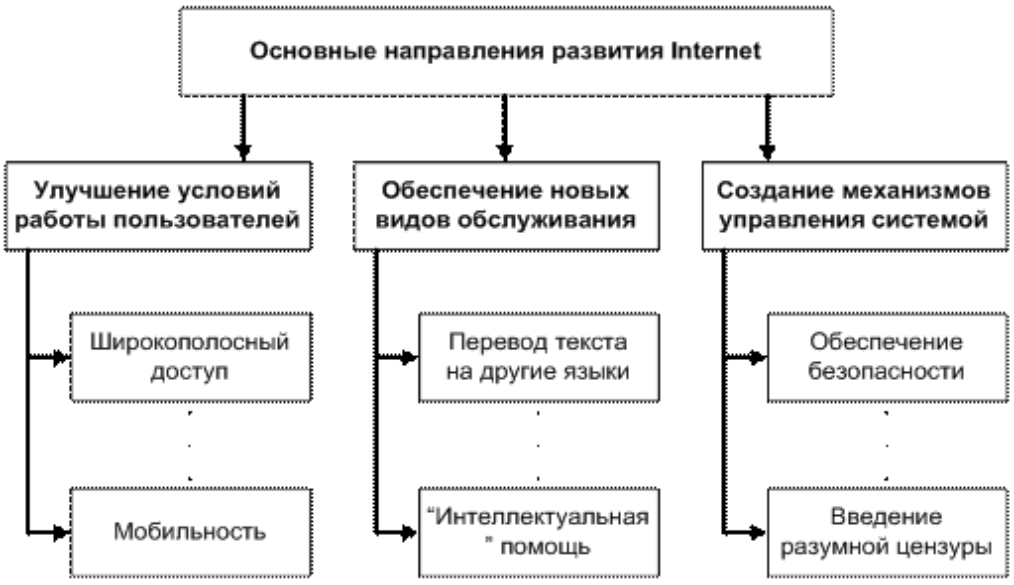


Рисунок 8.4 – Основные направления развития сети Интернет

Сам протокол IP был разработан в организации IETF (Internet Engineering Task Force) - «группе по решению задач проектирования Интернета». IETF и её рабочие группы по сей день занимаются развитием протоколов Всемирной сети. Комитеты IETF публикуют стандарты в виде документов RFC. В этих документах даются технические спецификации и точные объяснения по многим вопросам. Некоторым документам RFC организацией IAB (Internet Architecture

Board — Совет по архитектуре Интернета) присваивается статус обязательных стандартов Интернета. С 1992 года IETF, IAB и ряд других интернет-организаций входят в Общество Интернета (Internet Society, ISOC). Общество Интернета предоставляет организационную основу для исследовательских и консультативных групп, занимающихся развитием Интернета.

Однако развитие Интернета ведется не только в направление совершенствования технических систем. Идет интенсивное развитие синтаксического, информационного его наполнения, повышение интеллектуальности его сервисов Рисунок 8.4.

Сервисы сети Интернет

Когда говорят об использовании сети Интернет, то на самом деле речь идет об отдельных службах (сервисах), которые реализованы в этой сети. В зависимости от целей и задач клиенты сети используют те службы, которые им необходимы.

Разные службы имеют различные прикладные протоколы. Их соблюдение обеспечивается и поддерживается работой специальных программ, которые необходимо установить на компьютере. Такие программы называются клиентскими.

Терминальный режим (Telnet). Исторически одной из самых ранних служб сети Интернет является служба удаленного управления компьютером Telnet. Подключившись к удаленному компьютеру по протоколу этой службы, можно управлять его работой. Такое управление называют консольным или терминальным. Раньше эту службу широко использовали для проведения сложных математических расчетов на мощных вычислительных машинах. Название основных Telnet-клиентов указывать нецелесообразно, поскольку каждый сервер, предоставляющий такой сервис, предлагает свое клиентское обеспечение. Работа в этом случае напоминает работу за терминалом компьютера в режиме разделения времени. На практике этот режим используется редко.

Электронная почта

E-mail (Electronic mail) - электронная почта – аналог обычной почты, второй по популярности Internet сервис. С её помощью можно посылать и получать сообщения на определённый адрес. Такое общение не требует одновременного присутствия в Сети отправляющего и получающего – письма адресуются на адрес почтового сервера, который хранит их до получения абонентом.

Протоколы электронной почты, почтовые клиенты, безопасность.

Протоколы электронной почты– технические стандарты, определяющие правила взаимодействия клиентских и серверных программ между собой.

SMTP (Simple Mail Transfer Protocol) – служит непосредственно для транспортировки почты между двумя почтовыми серверами; в основном

работает в режиме on-line. Взаимодействие в рамках SMTP строится по принципу двусторонней связи, которая устанавливается между отправителем и получателем почтового сообщения. При этом отправитель инициирует соединение и посылает запросы на обслуживание, а получатель на эти запросы отвечает. Фактически, отправитель выступает в роли клиента, а получатель сервера. Пересылка сообщений между почтовыми серверами тоже происходит с помощью SMTP.

POP3 (Post Office Protocol, версия 3) – предназначен для разбора почты из почтовых ящиков пользователей на сервере в их локальные ящики при помощи программ - клиентов. Если по протоколу SMTP пользователи отправляют корреспонденцию через Internet, то по протоколу POP3 пользователи получают корреспонденцию из своих почтовых ящиков на почтовом сервере в локальные файлы.

Почтовый сервер – программа, установленная на сервере обеспечивающая работу электронной почты, по соответствующим протоколам.

Почтовый клиент– программа, установленная на компьютере пользователя, обеспечивающая совместную работу с почтовым сервером, используемая для отправки и получения сообщений электронной почты.

Почтовых программ, и клиентов, и серверов, существуют десятки. Часто почтовые серверы встроены в серверы доступа локальных сетей, системы сетевой безопасности, WWW-серверы. Почтовые клиенты встраиваются в браузеры (Opera, Firefox), программы онлайнового общения, органайзеры (MS Outlook), устанавливаются вместе с операционными системами. Также популярны отдельные почтовые клиенты, такие как TheBat!, EudoraPro.

Учетная запись электронной почты (почтовый ящик электронной почты) – совокупность настроек сервера, рассчитанных на работу с конкретным клиентом.

Регистрационное имя– запись, которую пользователь предъявляет серверу при подключении.

Пароль– секретная запись, которую пользователь предъявляет серверу при подключении.

Адрес электронной почты – запись, однозначно определяющая путь доступа к электронному почтовому ящику адреса. Адрес электронной почты в Internet выглядит так**: mailto:ivanov@mail.ru.**

И состоит из

- имени пользователя (ivanov),
- имени хоста или сетевой машины (mail.ru).

Сообщение электронной почты (письмо) – логическая совокупность данных, имеющая структуру, определенную используемым протоколом. Сообщение электронной почты – это не файл, а запись в базе данных на сервере и клиентском компьютере. К письму может быть пристыкован файл произвольного содержания. При пересылке файл кодируется специальным

образом и передаётся в тексте письма, отчего пересылаемый объём может быть в 2-3 раза больше объёма исходного файла. Поэтому пересылать большие файлы почтой не следует, лучше разместить их на каком-то сервере и переслать только URL на него.

Папки электронной почты – логические структуры, предназначенные для упорядочивания сообщений электронной почты. Большинство почтовых клиентов имеют возможность автоматической сортировки поступающей почты в соответствии с заданными пользователями правилами – например, помещать письма с определённых адресов в специально предназначенные для них папки, автоматически создавать сообщения, подтверждающие получение письма или отвечать на письма по заданному пользователем шаблону.

Почтовый робот (mail-bot) – серверная программа, автоматически рассылающая почту и служебные сообщения по списку адресов, или принимающая и обрабатывающая письма на определённый адрес, например, составленные по определённому шаблону заказы. Входит в состав многих почтовых клиентов и практически всех серверов. Например, при невозможности доставки письма адресату как правило создаётся сообщение почтового робота о причинах этого (нет такого сервера, нет такого адреса на сервере, сервер не принимает почту и так далее).

Рассылки– специальные серверы, рассылающие по заказу пользователей письма с определённой информацией – прогнозом погоды, курсами валют, новостями и т.п.

Спам – рассылки (SPAM, от названия фирмы, «прославившейся» назойливой рекламой) – почта, рассылаемая пользователям без их согласия, как правило рекламного характера.

Антиспам– программа или встроенная возможность почтового клиента, позволяющая отсортировать по задаваемым правилам или по спискам недобросовестных рассылок нежелательные сообщения и удалить или поместить в специальную папку.

Почтовый червь (mailworm) – род компьютерных вирусов, распространяющихся через электронную почту. Представляет собой сообщение особого рода, рассчитанное на автоматическую обработку почтовым клиентом таким образом, чтобы обеспечить дальнейшую рассылку заражённых писем и различные действия на компьютере пользователя. Не являются червями, но также могут вызвать заражение письма с прикреплёнными исполняемыми файлами (программами).

Списки рассылки (Mail List). Обычная электронная почта предполагает участие в переписке двух партнеров. Для расширения своего круга общения можно подписаться на получение почтовой информации по интересующей вас тематике на так называемые *списки рассылки*. Специальные тематические серверы, собирающие информацию по определенным темам, переправляют ее по вашему адресу электронной почты.

Службы телеконференций(Usenet). Это огромная, базирующаяся на сообщениях, электронная доска объявлений, которую называют *телеконференциями* или *группами новостей*. В отличие от электронной почты, информация в группах новостей доступна для всеобщего обозрения. Для удобства дискуссий образованы различные группы, участники которых посылают и принимают сообщения по определенной тематике.

Основной прием использования групп новостей состоит в том, чтобы задать вопрос, обращаясь ко всему миру, а затем получить ответ или совет от тех, кто с этим вопросом уже разобрался. Необходимо следить за тем, чтобы вопрос соответствовал теме конференции.

Для работы со службой телеконференций существуют специальные клиентские программы. Так, например, приложение Microsoft Outlook Express также позволяет работать со службой телеконференций. Для начала работы необходимо настроить программу на взаимодействие с сервером групп новостей, оформить подписку на определенные группы и периодически получать все сообщения, проходящие по выбранной теме.

Протокол передачи файлов FTP

Сервис FTP (File Transfer Protocol — Протокол передачи файлов). Этот сервис позволяет получать и передавать файлы и сегодня является самым распространенным для получения программных продуктов.

FTP (File Transfer Protocol) – протокол, определяющий правила передачи файлов между компьютером пользователя и FTP-сервером вне зависимости от типа операционной системы и места расположения компьютеров. Сервер может быть настроен как для свободного доступа, так и доступа по имени пользователя и паролю.

Редко используется как самостоятельный сервис, обычно работает вместе с HTTP, для чего большинство браузеров имеют возможность работать в качестве FTP-клиента. Есть и отдельные FTP-клиенты – программы для работы с FTP-серверами, также работа с FTP поддерживается некоторыми файловыми менеджерами – FAR, Total Commander

Сервис Archie. Позволяет найти файл в Интернет по его имени. Однако в последнее время этот сервис стал менее популярным, так как в WWW появились поисковые системы, позволяющие выполнить поиск более простым способом.

Gopher. Эта система доступа к информации посредством вложенных меню. Она является прообразом всемирной паутины, но в настоящее время постепенно отмирает, так как перемещение по WWW более простое и удобное.
WAIS (Wide Area Information Service—Информационный сервис широкой области). Эта система поиска информации по ключевому слову.

IRC. (Internet Relay Chat). Предназначена для прямого общения нескольких человек в режиме реального времени. Иногда эту службу называют *чат-конференциями* или *чатами*.

Существует несколько популярных клиентских программ для работы с серверами и сетями, поддерживающими сервис IRC. Одна из наиболее популярных программ– программа mIRC.exe.

ICQ. Эта служба предназначена для поиска сетевого IP-адреса человека, подключенного в данный момент к сети Интернет. Для пользования этой службой необходимо зарегистрироваться на центральном сервере (http://www.icq.com) и получить персональный идентификационный номер UIN (*Universal Internet Number*). Данный номер можно сообщить партнерам по контактам, и тогда служба ICQ приобретает характер Internet - пейджера.

Существует еще много интересных направлений использования Интернет, например, **телефонные переговоры**, **получение радио и телепередач**.

Всемирная паутина (WWW)

Всемирная паутина (сокращенно World Wide Web или WWW) — это единство информационных ресурсов, которые связаны между собой средствами телекоммуникаций и основаны на гипертекстовом представлении данных, разбросанных по всему миру.

Годом рождения Всемирной паутины считается 1989 год. Именно в этом году Тим Бернерс-Ли предложил общий гипертекстовый проект, который получил впоследствии название Всемирной паутины.

Создатель «паутины» Тим Бернес-Ли, работая в лаборатории физики элементарных частиц европейского центра ядерных исследований «CERN» В Женеве (Швейцария), совместно с партнером Робертом Кайо занимались проблемами применения идей гипертекста для построения информационной среды, которая упростила бы обмен информацией между физиками.

Итогом данной работы явился документ, в котором рассматривались понятия, имеющие принципиальное значение для «паутины» в ее современном виде, и были предложены идентификаторы URI, протокол HTTR и язык HTML. Без данных технологий уже нельзя представить современный Интернет.

Бернерс-Ли создал первый в мире веб-сервер и первый в мире гипертекстовый веб - браузер. На первом в мире веб-сайте он описал, что такое Всемирная паутина и как установить веб - сервер, как использовать браузер и т.п. Этот сайт являлся и первым в мире Интернет-каталогом.

Начиная с 1994 года самые главные задачи по развитию Всемирной паутины взял на себя Консорциум Всемирной паутины (*World Wide Web Consortium, W3C*), который организовал и до сих пор возглавляет Ким Бернес-Ли. Консорциум разрабатывает и внедряет технологические стандарты для Интернета и Всемирной паутины. Миссия W3C : **«Полностью раскрыть потенциал Всемирной паутины, путем создания протоколов и принципов, гарантирующих долгосрочное развитие Сети»**. W3C разрабатывает «Рекомендации», чтобы достичь совместимость между программными продуктами и аппаратурой различных компаний, что делает Всемирную сеть более совершенной, универсальной и удобной. Все рекомендации, которые разрабатывает Консорциум Всемирной паутины открыты, то есть не защищены

патентами и могут внедряться любым человеком без всяких финансовых отчислений консорциуму.

Для работы с WWW используется специальный протокол HTTP – Hyper Text Transfer Protocol (Протокол передачи гипертекста). Гипертекстовые документы создаются с помощью специального языка HTML – Hyper Text Markup Language (Язык разметки гипертекста). Документ, подготовленный с помощью этого языка и доступный для просмотра пользователем, называется Web-страницей. Программы для просмотра Web - страниц называются браузерами или обозревателями. Наиболее удачный термин для обозначения операции просмотра Web-страниц – навигация.

URL

URL (Uniform Resource Locator — унифицированный указатель ресурса) — это то, что отображается в строке браузера, когда вы заходите на тот или иной сайт. URL-адрес есть не только у сайтов, но и у различных файлов (документов, изображений, видео и так далее), загруженных в Интернет.

Протокол HTTP

Протокол передачи гипертекста (HTTP) - это протокол прикладного уровня в модели Internet protocol suite для распределенных, коллаборативных гипермедиа-информационных систем.

HTTP-это основа передачи данных для Всемирной паутины, где гипертекстовые документы включают гиперссылки на другие ресурсы, к которым пользователь может легко получить доступ, например, щелчком мыши или нажатием на экран в веб-браузере.

Сетевое управление в IP-сетях

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо имеющихся в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критически важна для выполнения сетью своих основных функций. Распределенный характер крупной сети делает невозможным поддержание ее работы без централизованной системы управления, которая бы в автоматическом режиме собирала информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляла эту информацию оператору сети.

Одной из первых систем сетевого управления, получившей широкое распространение, был программный продукт SunNet Manager, выпущенный в 1989 году компанией SunSoft. Система SunNet Manager была ориентирована на управление коммуникационным оборудованием и контроль трафика сети. Именно эти функции имеют чаще всего в виду, когда говорят о системе управления сетью (Network Management System, NMS).

Обычно система управления работает в автоматизированном режиме, выполняя наиболее простые действия по управлению сетью автоматически, а сложные решения предоставляя принимать человеку на основе подготовленной системой информации.

Сами системы управления представляют собой сложные программно-аппаратные комплексы, поэтому существует граница целесообразности их применения. В небольшой сети можно применять отдельные программы управления наиболее сложными устройствами, например, коммутатором, поддерживающим технику VLAN. Обычно каждое устройство, которое требует достаточно сложного конфигурирования, производитель сопровождает автономной программой конфигурирования и управления. Однако при росте сети может возникнуть проблема объединения разрозненных программ управления устройствами в единую систему управления, и для решения этой проблемы придется, возможно, отказаться от этих программ и заменить их интегрированной системой управления.

Литература

1) **Олифер, В. Г.** Компьютерные сети. Принципы, технологии, протоколы: учебное пособие / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – Санкт-Петербург: Питер, 2016. – 992 с. ил.

2) **Новиков, В. А**. Информационные системы и сети: учебное пособие / В. А. Новиков, А. В. Новиков, В. В. Матвеенко. – Минск: Изд-во Гревцова, 2014. – 448 с.

3) **Таненбаум Э.**, Компьютерные сети / Таненбаум Э.,Уэзеролл Д. 5-е изд. – Санкт-Петербург: Питер, 2013. – 960с. ил.

4) http://www.structuralist.narod.ru/it/internet/arpanet.htm