История развития компьютерных сетей.

Развитие компьютерных сетей связано как с развитием собственно ЭВМ, входящих в состав сети, так и с развитием средств телекоммуникаций.
Работы по созданию компьютерных сетей начались ещё в 60-х годах XX века.
Прообразом компьютерных сетей явились системы телеобработки данных (СТД), построенные на базе больших (а позже и миниЭВМ).
В качестве средств передачи данных использовалась существующая телефонная сеть.
Основными элементами СТД являются модемы, абонентские пункты и устройства коммутации. Система СТД оперировала только аналоговыми сигналами.
Основным недостатком СТД является невысокое быстродействие (9600 бит/с, реально 2400 бит/с). Поэтому одним из направлений совершенствования СТД явилась разработка цифровых телефонных коммутаторов.
Вторым существенным недостатком СТД является возможность передачи данных по каналу связи в один и тот же момент времени только с одной скоростью. Этот недостаток был преодолен использованием впервые в 70-х годах в США коммуникаций кабельного телевидения, позволяющих вести широкополосную передачу (ШП).
Третьим направлением перехода к сетям была разработка высокоскоростных шин для обеспечения взаимодействия нескольких больших ЭВМ.
Четвёртым направлением развития сетей была реализация распределённой обработки данных.
К середине 80-х годов, с появлением ПЭВМ все отмеченные тенденции развития сетей стали сближаться, что привело к разработке современных компьютерных сетей.

Программные средства компьютерных сетей.

Программы - это упорядоченные последовательности команд. Конечная цель любой компьютерной программы - управление аппаратными средствами. Даже если на первый взгляд программа никак не взаимодействует с оборудованием, не требует никакого ввода данных с устройств ввода и не осуществляет вывод данных на устройства вывода, все равно ее работа основана на управлении аппаратными устройствами компьютера.

Программное и аппаратное обеспечение в компьютере работают в неразрывной связи и в непрерывном взаимодействии. Между ними существует диалектическая связь.

Состав программного обеспечения вычислительной системы называют программной конфигурацией. Между программами, как и между физическими узлами и блоками существует взаимосвязь - многие программы работают, опираясь на другие программы более низкого уровня, то есть можно говорить о межпрограммном интерфейсе. Возможность существования такого интерфейса тоже основана на существовании технических условий и протоколов взаимодействия, а на практике он обеспечивается распределением программного обеспечения на несколько взаимодействующих между собой уровней.

При подключении к вычислительной системе нового оборудования на системном уровне должна быть установлена программа, обеспечивающая для других программ взаимосвязь с этим оборудованием. Конкретные программы, отвечающие за взаимодействие с конкретными устройствами, называются драйверами устройств - они входят в состав программного обеспечения системного уровня.

Другой класс программ системного уровня отвечает за взаимодействие с пользователем. Именно благодаря им он получает возможность вводить данные в вычислительную систему, управлять ее работой и получать результат в удобной для себя форме. Эти программные средства называют средствами обеспечения пользовательского

интерфейса. От них напрямую зависит удобство работы с компьютером и производительность труда на рабочем месте.

Совокупность программного обеспечения системного уровня образует ядро операционной системы компьютера. Если компьютер оснащен программным обеспечением системного уровня, то он уже подготовлен к установке программ более высоких уровней, к взаимодействию программных средств с оборудованием, самое главное, к взаимодействию с пользователем.

Служебный уровень. Программное обеспечение этого уровня взаимодействует как программами базового уровня, так и с программами системного уровня. Основное назначение служебных программ, их называют утилитами, состоит в автоматизации работ по проверке, наладке и настройке компьютерной системы. Во многих случаях они используются для расширения или улучшения функций системных программ.

Прикладной уровень. Программное обеспечение прикладного уровня представляет собой комплекс прикладных программ, с помощью которых на данном рабочем месте выполняются конкретные задания. Спектр этих заданий необычайно широк: от производственных до творческих и развлекательно-обучающих. Огромный функциональный диапазон возможных приложений средств вычислительной техники условлен наличием прикладных программ для разных видов деятельности.

Между прикладным программным обеспечением и системным существует непосредственная взаимосвязь (первое опирается на второе), следовательно, универсальность вычислительной системы, доступность прикладного программного обеспечения и широта функциональных возможностей компьютера напрямую зависят от типа используемой операционной системы, от того, какие системные средства содержит ее ядро, как она обеспечивает взаимодействие триединого комплекса человек - программы - оборудование.

Системы управления базами данных. Базами данных называют огромные массивы данных, организованных в табличные структуры. В связи с широким распространением сетевых технологий к современным системам управления базами данных предъявляется также требование возможности работы с удаленными и распределенными ресурсами, находящимися на серверах всемирной компьютерной сети.

Web-редакторы. Это особый класс редакторов, объединяющих в себе свойства текстовых и графических редакторов. Они предназначены для создания и редактирования так называемых Web-документов (Web-страниц Интернета). Web-документы - это электронные документы, при подготовке которых следует учитывать ряд особенностей, связанных с приемом/передачей информации в Интернете.

Программы этого класса можно также эффективно использовать для подготовки электронных документов и мультимедийных изданий.

Браузеры (обозреватели, средства просмотра Web). К этой категории относятся программные средства, предназначенные для просмотра электронных документов, выполненных в формате HTML (документы этого формата используются в качестве Web-документов). Современные браузеры воспроизводят не только текст и графику. Они могут воспроизводить музыку, человеческую речь, обеспечивать прослушивание радиопередач в Интернете, просмотр видеоконференций, работу со службами электронной почты, с системой телеконференций (групп новостей) и многое другое.

Интегрированные системы делопроизводства. Представляют собой программные средства автоматизации рабочего места руководителя. К основным функциям подобных систем относятся функции создания, редактирования и форматирования простейших документов, централизация функций электронной почты, факсимильной и телефонной

связи, диспетчеризация и мониторинг документооборота предприятия, координация деятельности подразделений, оптимизация административно-хозяйственной деятельности и поставка по запросу оперативной и справочной информации.

Финансовые аналитические системы. Программы этого класса используются в банковских и биржевых структурах. Они позволяют контролировать и прогнозировать ситуацию на финансовых, товарных и сырьевых рынках, производить анализ текущих событий, готовить сводки и отчеты.

Средства коммуникации (коммуникационные программы). С появлением электронной связи и компьютерных сетей программы этого класса приобрели очень большое значение. Они позволяют устанавливать соединения с удаленными компьютерами, обслуживают передачу сообщений электронной почты, работу с телеконференциями (группами новостей), обеспечивают пересылку факсимильных сообщений и выполняют множество других операций в компьютерных сетях.

Средства обеспечения компьютерной безопасности. К этой весьма широкой категории относятся средства пассивной и активной защиты данных от повреждения, а также средства защиты от несанкционированного доступа, просмотра и изменения данных.

В качестве средств пассивной защиты используют служебные программы, предназначенные для резервного копирования. Нередко они обладают и базовыми свойствами диспетчеров архивов (архиваторов). В качестве средств активной защиты применяют антивирусное программное обеспечение. Для защиты данных от несанкционированного доступа, их просмотра и изменения служат специальные системы, основанные на криптографии.

Аппаратные средства компьютерных сетей.

Физическая среда передачи данных

Определяет:
1) Скорость передачи данных в сети;
2) Размер сети
3) Требуемый набор служб (передача данных, речи, мультимедиа и т.д.), который необходимо организовать.
4) Требования к уровню шумов и помехозащищенности;
5) Общую стоимость проекта, включающая покупку оборудования, монтаж и последующую эксплуатацию.

Кабельный сегмент сети - цепочка отрезков кабелей, электрически соединенных друг с другом.

Логический сегмент сети, или просто сегмент - группа узлов сети, имеющих непосредственный доступ друг к другу на уровне пакетов канального уровня. В интеллектуальных хабах Ethernet группы портов могут объединяться в логические сегменты для изоляции их трафика от других сегментов в целях повышения производительности и защиты.

Коммутирующие устройства предназначены для связи сегментов сети.

Концентратор- хаб (Hub) - устройство физического подключения нескольких сегментов или лучей, обычно с возможностью соединения сетей различных архитектур.

Интеллектуальный хаб (Intelligent Hub) имеет специальные средства для диагностики и управления, что позволяет оперативно получать сведения об активности и исправности узлов, отключать неисправные узлы и т. д. Стоимость существенно выше, чем у обычных.

Активный хаб (Active Hub) усиливает сигналы, требует источника питания.
Peer Hub - хаб, исполненный в виде платы расширения PC, использующей только источник питания PC.
Пассивный хаб (Passive Hub) только согласует импедансы линий (в сетях ArCnet).
Standalone Hub - самостоятельное устройство с собственным источником питания (обычный вариант).
Повторитель (repeater) - устройство для соединения сегментов одной сети, обеспечивающее промежуточное усиление и формирования сигналов.Позволяет расширять сеть по расстоянию и количеству подключенных узлов.
Мост (Bridge) - средство передачи пакетов между сетями (локальными), для протоколов сетевого уровня прозрачен. Осуществляет фильтрацию пакетов, не выпуская из сети пакеты для адресатов, находящихся внутри сети, а также переадресацию - передачу пакетов в другую сеть в соответствии с таблицей маршрутизации или во все другие сети при отсутствии адресата в таблице. Таблица маршрутизации обычно составляется в процессе самообучения по адресу источника приходящего пакета.
Маршрутизатор (router) - средство обеспечения связи между узлами различных сетей, использует сетевые (логические) адреса. Сети могут находиться на значительном расстоянии, и путь, по которому передается пакет, может проходить через несколько маршрутизаторов. Сетевой адрес интерпретируется как иерархическое описание местоположения узла. Маршрутизаторы поддерживают протоколы сетевого уровня: IP, IPX, X.25, IDP. Мультипротокольные маршрутизаторы (более сложные и дорогие) поддерживают несколько протоколов одновременно для гетерогенных сетей. Brouter (Bridging router) - комбинация моста и маршрутизатора, оперирует как на сетевом, так и на канальном уровне.

Основные характеристики маршрутизатора:

- тип: одно- или многопротокольный, LAN или wAN, Brouter;
- поддерживаемые протоколы;
- пропускная способность;
- типы подключаемых сетей;
- поддерживаемые интерфейсы (LAN и wAN);
- количество портов;
- возможность управления и мониторинга сети.

Шлюз (Gateway) - средство соединения существенно разнородных сетей. В отличие от повторителей, мостов и маршрутизаторов, прозрачных для пользователя, присутствие шлюза заметно. Шлюз выполняет преобразование форматов и размеров пакетов, преобразование протоколов, преобразование данных, мультиплексирование. Обычно реализуется на основе компьютера с большим объемом памяти.
Примеры шлюзов:
Fax: обеспечивает доступ к удаленному факсу, преобразуя данные в факс-формат;
E-mail: обеспечивает почтовую связь между локальными сетями. Шлюз обычно связывает MHS, специфичный для сетевой операционной системы с почтовым сервисом по X.400;
Internet: обеспечивает доступ к глобальной сети Internet.

Процесс передачи данных. Принципы пакетной передачи данных.

Коммутация пакетов

Под ***коммутацией*** в сетях передачи данных понимается совокупность операций, обеспечивающих в узлах коммутации передачу информации между входными и выходными устройствами в соответствии с указанным адресом.

При ***коммутации пакетов*** (КП) передаваемое сообщение разбивается на меньшие части, называемые пакетами, каждый из которых имеет установленную максимальную длину. Пакеты снабжаются служебной информацией, необходимой для доставки пакета, и передаются по сети.

Каждый пакет снабжается следующей служебной информацией (заголовком):

- коды начала и окончания пакета,
- адреса отправителя и получателя,
- номер пакета в сообщении,
- информация для контроля достоверности передаваемых данных в промежуточных узлах связи и в пункте назначения.

Множество пакетов одного и того же сообщения может передаваться одновременно. Приемник в соответствии с заголовками пакетов выполняет сборку пакетов в исходное сообщение и отправляет его получателю. Благодаря возможности не накапливать сообщения целиком, в узлах коммутации не требуется внешних запоминающих устройств, следовательно, можно вполне ограничиться оперативной памятью, а в случае ее переполнения использовать различные механизмы задержки передаваемых пакетов в местах их генерации.

Части одного и того же сообщения могут в одно и то же время находиться в различных каналах связи, более того: когда начало сообщения уже принято, его конец отправитель может еще даже не передавать в канал.

При пакетной коммутации приходится находить компромиссное решение, удовлетворяющее двум противоречивым требованиям:
- уменьшение задержки пакета в сети, обеспечиваемое уменьшением его длины;
- обеспечение повышения эффективности передачи информации, достигаемое, наоборот, увеличением длины пакета (при малой длине пакета длина его заголовка становится неприемлемо большой, что снижает экономическую эффективность передачи).

В сети с пакетной коммутацией максимальный размер пакета устанавливается на основе 3-х факторов:
- распределение длин пакетов,
- характеристика среды передачи (главным образом, скорость передачи),
- стоимость передачи.

Для каждой передающей среды выбирается свой оптимальный размер пакета.

Процесс передачи данных в сети с коммутацией пакетов

Процесс передачи данных в сети с КП можно представить в виде следующей последовательности операций:

- вводимое в сеть сообщение разбивается на части - пакеты, содержащие адрес конечного пункта получателя;

- в узле КП пакет запоминается в оперативной памяти (ОЗУ) и по адресу определяется канал, по которому он должен быть передан;
- если этот канал связи с соседним узлом свободен, то пакет немедленно передается на соседний узел КП, в котором повторяется та же операция;
- если канал связи с соседним узлом занят, то пакет может какое-то время храниться в ОЗУ до освобождения канала;
- сохраняемые пакеты помещаются в очередь по направлению передачи, причем длина очереди не превышает 3-4 пакета; если длина очереди превышает допустимую, пакеты стираются из ОЗУ и их передача должна быть повторена.

Пакеты, относящиеся к одному сообщению, могут передаваться по разным маршрутам в зависимости от того, по какому из них в данный момент они с наименьшей задержкой могут пойти к адресату. В связи с тем, что время прохождения по сети пакетов одного сообщения может быть различным (в зависимости от маршрута и задержки в узлах коммутации), порядок их перехода к получателю может не соответствовать порядку пакетов.

Методы пакетной коммутации

Существует два метода пакетной коммутации: дейтаграммный (датаграммный) и способ виртуальных соединений.

Дейтаграммный метод

Этот метод эффективен для передачи коротких сообщений. Он не требует громоздкой процедуры установления соединения между абонентами.

Термин "дейтаграмма" (датаграмма, datagram) применяют для обозначения самостоятельного пакета, движущегося по сети независимо от других пакетов. Пакеты доставляются получателю различными маршрутами. Эти маршруты определяются сложившейся динамической ситуаций на сети. Каждый пакет снабжается необходимым служебным маршрутным признаком, куда входит и адрес получателя.

Пакеты поступают на прием не в той последовательности, в которой они были переданы, поэтому приходится выполнять функции, связанные со сборкой пакетов. Получив дейтаграмму, узел коммутации направляет ее в сторону смежного узла, максимально приближенного к адресату. Когда смежный узел подтверждает получение пакета, узел коммутации стирает его в своей памяти. Если подтверждение не получено, узел коммутации отправляет пакет в другой смежный узел, и так до тех пор, пока пакет не будет отправлен.

Все узлы, окружающие данный узел коммутации, ранжируются по степени близости к адресату, и каждому присваивается 1, 2 и т.д. ранг. Пакет сначала посылается в узел первого ранга, при неудаче - в узел второго ранга и т.д. Эта процедура называется алгоритмом маршрутизации. Существуют алгоритмы, когда узел передачи выбирается случайно, и тогда каждая дейтаграмма будет идти по случайной траектории.

Виртуальный метод

Этот метод предполагает предварительное установление маршрута передачи всего сообщения от отправителя до получателя с помощью специального служебного пакета - запроса вызова.

Для этого пакета выбирается маршрут, который в случае согласия получателя этого пакета на соединение закрепляется для прохождения по нему всего трафика. Пакет запроса на соединение как бы прокладывает через сеть путь , по которому пойдут все пакеты, относящиеся к этому вызову.

Метод называется виртуальным потому, что здесь не коммутируется реальный физический тракт (как, например, в телефонной сети), а устанавливается логическая связка между отправителем и получателем, - т.е. коммутируется виртуальный (воображаемый) тракт.

В виртуальной сети абоненту-получателю направляется служебный пакет, прокладывающий виртуальное соединение. В каждом узле этот пакет оставляет распоряжение вида: пакеты *k*-го виртуального соединения, пришедшие из *i*-го канала, следует направлять в *j*-й канал. Тем самым виртуальное соединение существует только в памяти управляющего компьютера. Дойдя до абонента-получателя, служебный пакет запрашивает у него разрешение на передачу, сообщив, какой объем памяти понадобится для приема. Если его компьютер располагает такой памятью и свободен, то посылается согласие абоненту-отправителю на передачу сообщения. Получив подтверждение, абонент-отправитель приступает к передаче сообщения обычными пакетами.

Пакеты беспрепятственно проходят друг за другом по виртуальному соединению и в том же порядке попадают абоненту-получателю, где, освободившись от заголовков и концевиков, образуют передаваемое сообщение.

Виртуальное соединение может существовать до тех пор, пока отправленный одним из абонентов специальный служебный пакет не сотрет инструкции в узлах.

Режим виртуальных соединений эффективен при передаче больших массивов информации.

Преимущества режима виртуальных соединений перед дейтаграммным заключается в обеспечении упорядоченности пакетов, поступающих в адрес получателя, и сравнительной простоте управления потоком данных вдоль маршрута в целях ограничения нагрузки в сети, в возможности предварительного резервирования ресурсов памяти на узлах коммутации.

К недостаткам следует отнести отсутствие воздействия изменившейся ситуации в сети на маршрут, который не корректируется до конца связи. Виртуальная сеть в значительно меньшей степени подвержена перегрузкам и зацикливанию пакетов, за что приходится платить худшим использованием каналов и большей чувствительностью к изменению топологии сети.

Организация сетей различных типов.

С точки зрения организации взаимодействия компьютеров, сети делят на одноранговые (Peer-to-Peer Network) и с выделенным сервером (Dedicated Server Network).

Одноранговые сети

Все компьютеры одноранговой сети равноправны. Любой пользователь сети может получить доступ к данным, хранящимся на любом компьютере.

Одноранговые сети могут быть организованы с помощью таких операционных систем, как LANtastic, windows'3.11, Novell Netware Lite. Указанные программы работают как с DOS, так и с windows. Одноранговые сети могут быть организованы также на базе всех

современных 32-разрядных операционных систем - windows 9x\ME\2k, windows NT workstation версии, OS/2) и некоторых других.
Достоинства одноранговых сетей:

1. Наиболее просты в установке и эксплуатации.
2. Операционные системы DOS и windows обладают всеми необходимыми функциями, позволяющими строить одноранговую сеть.

Недостатки:
В условиях одноранговых сетей затруднено решение вопросов защиты информации. Поэтому такой способ организации сети используется для сетей с небольшим количеством компьютеров и там, где вопрос защиты данных не является принципиальным.

Иерархические сети
В иерархической сети при установке сети заранее выделяются один или несколько компьютеров, управляющих обменом данных по сети и распределением ресурсов. Такой компьютер называют *сервером.*
Любой компьютер, имеющий доступ к услугам сервера называют клиентом сети или рабочей станцией.
Сервер в иерархических сетях - это постоянное хранилище разделяемых ресурсов. Сам сервер может быть клиентом только сервера более высокого уровня иерархии. Поэтому иерархические сети иногда называются сетями с выделенным сервером.
Серверы обычно представляют собой высокопроизводительные компьютеры, возможно, с несколькими параллельно работающими процессорами, с винчестерами большой емкости, с высокоскоростной сетевой картой (100 Мбит/с и более).
Иерархическая модель сети является наиболее предпочтительной, так как позволяет создать наиболее устойчивую структуру сети и более рационально распределить ресурсы.
Также достоинством иерархической сети является более высокий уровень защиты данных.
К недостаткам иерархической сети, по сравнению с одноранговыми сетями, относятся:

1. Необходимость дополнительной ОС для сервера.
2. Более высокая сложность установки и модернизации сети.
3. Необходимость выделения отдельного компьютера в качестве сервера.

Две технологии использования сервера
Различают две технологии использования сервера: технологию *файл-сервера* и архитектуру *клиент-сервер*.
В первой модели используется *файловый сервер*, на котором хранится большинство программ и данных. По требованию пользователя ему пересылаются необходимая программа и данные. Обработка информации выполняется на рабочей станции.
В системах с архитектурой клиент-сервер обмен данными осуществляется между *приложением-клиентом* (front-end) и *приложением-сервером* (back-end). Хранение данных и их обработка производится на мощном сервере, который выполняет также контроль за доступом к ресурсам и данным. Рабочая станция получает только результаты запроса. Разработчики приложений по обработке информации обычно используют эту технологию.
Использование больших по объему и сложных приложений привело к развитию многоуровневой, в первую очередь трехуровневой архитектуры с размещением данных на отдельном сервере базы данных (БД). Все обращения к базе данных идут через сервер приложений, где они объединяются.

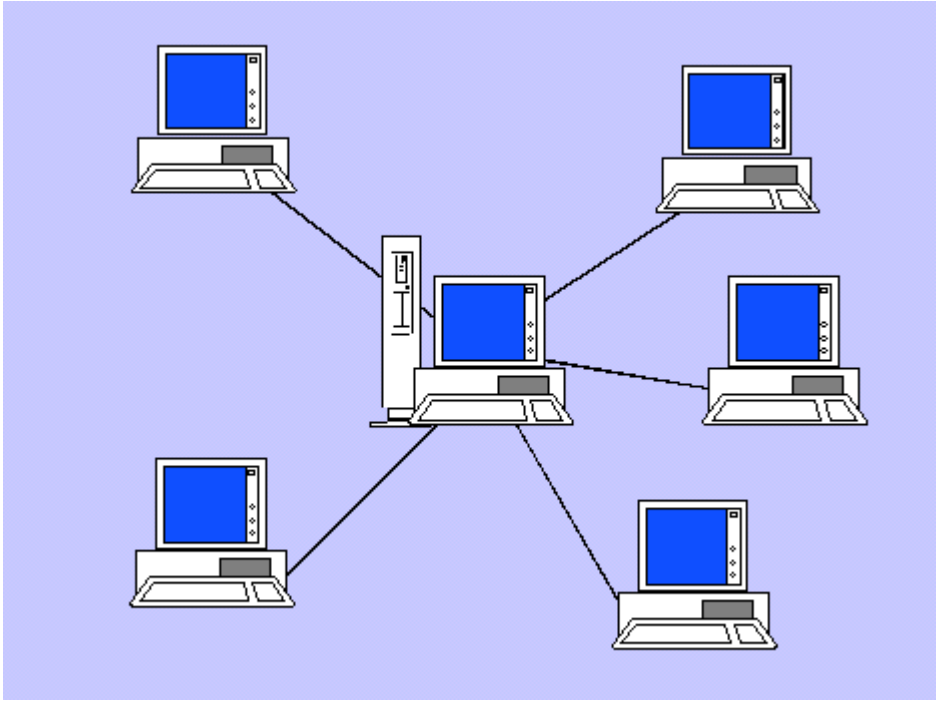
Базовые сетевые топологии и комбинированные топологические решения.

Топология - это конфигурация сети, способ соединения элементов сети (то есть компьютеров) друг с другом. Чаще всего встречаются три способа объединения компьютеров в локальную сеть: **"звезда", "общая шина"** и **"кольцо"**.

Соединение типа "звезда". Каждый компьютер через специальный сетевой адаптер подключается отдельным кабелем к объединяющему устройству. При необходимости можно объединить вместе несколько сетей с топологией "звезда", при этом конфигурация сети получается разветвленной.

Достоинства: При соединении типа "звезда" легко искать неисправность в сети.

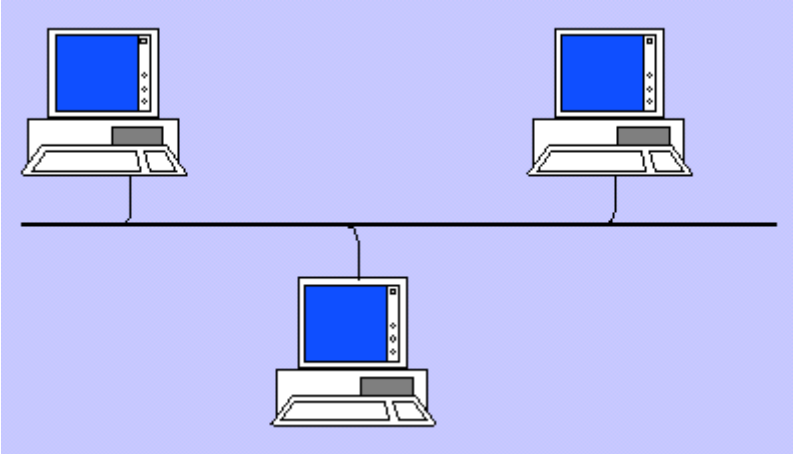
Недостатки: Соединение не всегда надежно, поскольку выход из строя центрального узла может привести к остановке сети.



Соединение "общая шина". Все компьютеры сети подключаются к одному кабелю; этот кабель используется совместно всеми рабочими станциями по очереди. При таком типе соединения все сообщения, посылаемые каждым отдельным компьютером, принимаются всеми остальными компьютерами в сети.

Достоинства: в топологии "общая шина" выход из строя отдельных компьютеров не приводит всю сеть к остановке.

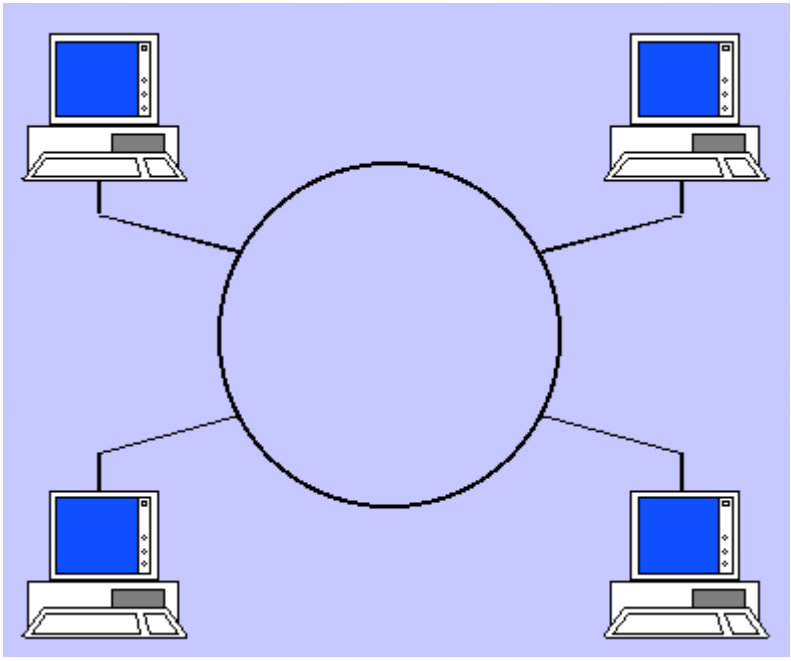
Недостатки: несколько труднее найти неисправность в кабеле и при обрыве кабеля (единого для всей сети) нарушается работа всей сети.



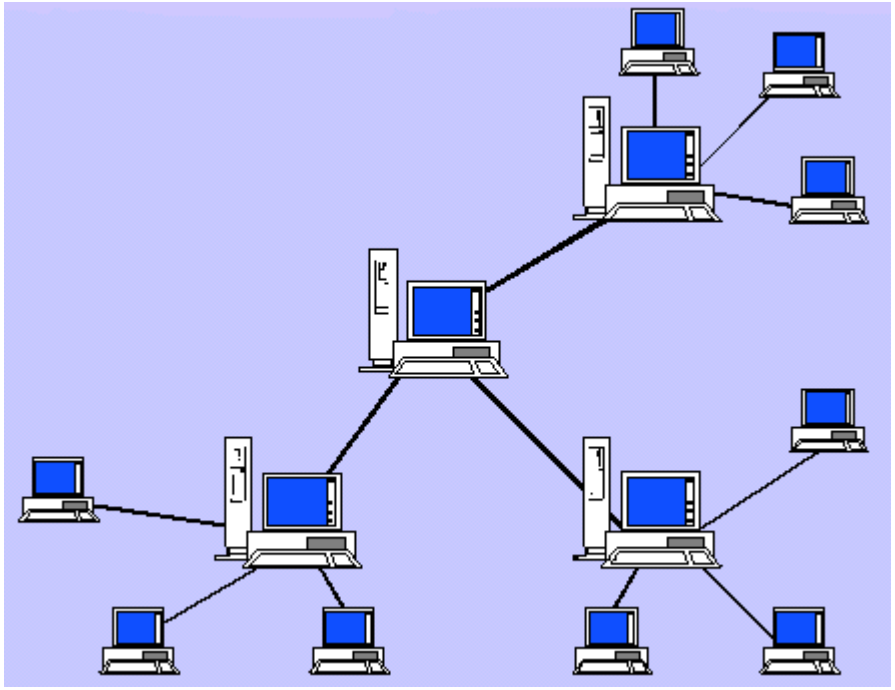
Соединение типа "кольцо". Данные передаются от одного компьютера к другому; при этом если один компьютер получает данные, предназначенные для другого компьютера, то он передает их дальше (по кольцу).

Достоинства: балансировка нагрузки, возможность и удобство прокладки кабеля.

Недостатки: физические ограничения на общую протяженность сети.



От схемы зависит состав оборудования и программного обеспечения. Топологию выбирают, исходя из потребностей предприятия. Если предприятие занимает многоэтажное здание, то в нем может быть применена схема **"снежинка"**, в которой имеются файловые серверы для разных рабочих групп и один центральный сервер для всего предприятия.



Базовые технологии локальных сетей: Ethernet, ArcNet, Token-Ring, 100BaseVG-AnyLAN, FDDI.

Архитектура сети определяет технологию передачи данных в сети.
Наиболее распространены следующие архитектуры:

- Ethernet,
- Token ring,
- ArCNET,
- FDDI.

Ethernet
Появилась технология Ethernet - во второй половине 70-х годов. Ее разработали совместно фирмы DEC, Intel и Xerox. В настоящее время эта технология наиболее доступна и популярна.

- *Топология* - шина, звезда
- *Среда передачи данных* - коаксиал, витая пара.
- *Скорость передачи данных* - до 100 Мбит/с
- *Длина кабельного сегмента сети* - не более 100 м до хаба

Принципы работы сети Ethernet:

1. Никому не разрешается посылать сообщения в то время, когда этим занят уже кто-то другой (слушай перед тем, как отправить).
2. Если два или несколько отправителей начинают посылать сообщения примерно в один и тот же момент, рано или поздно их сообщения "столкнутся" друг с другом в проводе, что называется коллизией. Коллизии нетрудно распознать, поскольку они всегда вызывают сигнал помехи, который не похож на допустимое сообщение. Ethernet может распознать помехи и заставляет отправителя приостановить передачу, подождать некоторое время, прежде, чем повторно отправить сообщение.

Достоинства Ethernet:

1. Дешевизна.
2. Большой опыт использования.
3. Продолжающиеся нововведения.
4. Богатство выбора. Многие изготовители предлагают аппаратуру построения сетей, базирующуюся на Ethernet.

Недостатки Ethernet:

1. Возможность столкновений сообщений (коллизии, помехи).
2. В случае большой загрузки сети время передачи сообщений непредсказуемо.

Token ring

Token ring - маркерное кольцо

Более молодой, по сравнению с Ethernet, является технология Token ring (?en. 2.8). Она была разработана фирмой IBM. Технология ориентирована на кольцо, по которому постоянно движется маркер. Маркер представляет собой особого рода пакет, предназначенный для синхронизации передачи данных.

- *Топология* - кольцо
- *Среда передачи данных* - коаксиал, витая пара.
- *Скорость передачи данных* - до 100 Мбит/с
- *Длина кабельного сегмента сети* - не более 185 м до коммутатора.

Принципы работы сети Token ring:

Каждый абонент сети работает в Token ring согласно принципу "Ждать маркера, если необходимо послать сообщение, присоединить его к маркеру, когда он будет проходить мимо. Если проходит маркер, снять с него сообщение и послать маркер дальше".

Достоинства Token ring:

- Гарантированная доставка сообщений;
- Высокая скорость.

Недостатки Token ring:

1. Необходимы дорогостоящие устройства доступа к сети.
2. Высокая сложность технологии реализации сети.
3. Необходимы 2 кабеля (для повышения надежности): один входящий, другой исходящий от компьютера к концентратору (2-я модификация кольца, коммутатор).
4. Высокая стоимость (160-200% от Ethernet).

ArCNET

ArCNET Attached resource Computer Network - маркер шины

Технология ArCNET была разработана фирмой Datapoint Corporation. Принцип работы сети ArCNET аналогичен Token ring, т.е. используется маркер для разрешения АбС передать информацию в соответствующий момент времени.

Однако "способ" реализации маркера здесь отличен от Token ring. Кроме того, технология ArCNET ориентирована на шину (в случае коаксиального кабеля) или звезду (при наличии витой пары проводов).

- *Топология* - шина, звезда
- *Среда передачи данных* - коаксиал, витая пара.

- *Скорость передачи данных* - до 10 Мбит/с
- *Длина кабельного сегмента сети* - не более 185м

Достоинства ArCNET:

1. Невысокая стоимость(самая дешевая);
2. Простота использования;
3. Гибкость.

Недостатки ArCNET:

1. Низкое быстродействие (1/4 Ethernet, 1/2 - 1/7 Token ring);
2. Плохо работает в условиях мультимедиа, режиме реального времени;
3. Отсутствуют перспективы развития.

FDDI

FDDI Fiber Distributed Data Interface- волоконно-оптический распределенный механизм передачи данных.
Технологи FDDI появилась в середине 80-х годов и ориентирована на волоконную оптику. FDDI поддерживает сеть с передачей маркера. FDDI опирается на 1-ю модификацию циклического кольца (2 кольца: в первом сообщения передаются по часовой стрелке; во втором - против).

- *Топология* - кольцо
- *Среда передачи данных* - оптоволоконные линии.
- *Скорость передачи данных* - от 100 Мбит/с
- *Длина кабельного сегмента сети* - не более 200км.

Достоинства:

1. Очень высокая скорость передачи;
2. Кольцо может быть окружностью до 200 км. и включать до 1000 устройств.

Недостаток:
высокая стоимость (подключение одной рабочей станции $1000-2000).

Методы маркерной шины и маркерного кольца.

Метод доступа с контролем несущей и определением коллизий

Множественный доступ с контролем несущей и определением коллизий (*CSMA/CD, Carrier Sense Multiple Access/Collision Detect) - самый распространенный метод случайного доступа, что применяются в локальных сетях. Все узлы сети постоянно прослушивают канал (контроль несущей). Если узел имеет данные для передачи, он ожидает тишины в канале и начинает передачу. При этом может оказаться так, что другой узел тоже обнаружил, что канал свободен и тоже начал передачу. Такая ситуация называется* ***коллизией****. Поскольку все узлы, передавая данные, продолжают прослушивать канал, они могут обнаружить наложение сигналов от разных источников. При выявлении коллизии передаточные узлы выдают в канал специальную последовательность битов - "затор", который служит для оповещения других узлов о коллизии. Потом все передаточные узлы прекращают передачу и планируют ее на более позднее время. Величина паузы выбирается случайным образом.*

Маркерные методы доступа

Метод передачи маркера относится к селективным детерминированным одноранговым методам доступа. Сети с шинной топологией, которые используют передачу маркера, называются сетями типа "маркерная шина" (token bus), а кольцевые сети - сетями типа "маркерное кольцо" (token ring).

*В сетях типа "**маркерная шина"** маркер являет собой кадр, который содержит поле адреса, в которое записывается адрес узла, который предоставляется право доступа к среде передачи. После передачи кадру данных узел, который передает, записывает в маркер адрес следующего узла и выдает маркер в канал.*

*Сети типа "**маркерное кольцо",** будучи сетями с кольцевой топологией, имеют последовательную конфигурацию: каждая пара узлов связана отдельным каналом, а для функционирования сети необходимо функционирование всех узлов. В таких сетях маркер не содержит адреса узла, которому разрешена передача, а содержит только полет занятости, которая может содержать одно из двух значений: "занятый" и "свободный". Когда узел, который имеет данные для передачи, получает свободный маркер, он меняет состояние маркера на "занятый", а затем передает в канал маркер и свой кадр данных. Станция-получатель, распознав свой адрес в кадре данных, считывает назначенные ей данные, но не меняет состояния маркера. Изменяет состояние маркера на "свободный" (после полного оборота маркера с кадром данных по кольцу) тот узел, что его занял. Кадр данных при этом удаляется из кольца. Узел не может повторно использовать маркер для передачи другого кадра данных, а должен передать свободный маркер далее по кольце и дождаться его получения после одного или нескольких оборотов.*

Равноранговые приоритетные системы включают приоритетные слоту системы, системы с контролем несущей без коллизий и системы с передачей маркера с приоритетами.

***Приоритетные слоты системы** подобны системам с мультиплексной передачей со временным делением, но выдача слотов происходит с учетом приоритетов узлов. Критериями для установления приоритетов могут быть: предыдущее владение слотом, время ответа, объем переданных данных и др.*

***Системы с контролем несущей без коллизий** (CSMA/CA, Carrier Sense Multiple Access/Collision Avoidance) отличаются от систем с выявлением коллизий наличием у узлов таймеров, которые определяют безопасные моменты передачи. Длительности таймеров устанавливаются в зависимости от приоритетов узлов: станции из больше высоким приоритетом имеют меньшую длительность таймера.*

***Приоритетные системы с передачей маркера** определяют приоритеты узлов таким образом, что чем меньше номер узла, тем выше его приоритет. Маркер при этом содержит поле резервирования, в которое узел, который собирается передавать данные, записывает свое значение приоритета. Если в кольце встретится узел с высшим приоритетом, который тоже имеет данные для передачи, этот узел запишет свое значение приоритета в поле резервирования, чем перекроет предыдущую заявку (сохранив старое значение поля резервирования в своей памяти). Если маркер, который поступил на узел, содержит в поле резервирование значения приоритета данного узла, данный узел может передавать данные. После оборота маркера по кольцу и его освобождения узел, который передавал, должен возобновить в маркере значение поля резервирование, сохраненное в памяти.*

Методы доступа к среде передачи.

Топология сети определяет правила, по которым каждое передающее устройство получает доступ к общей среде передачи – метод доступа.

Метод доступа -

это способ "захвата" передающей среды, способ определения того, какая из рабочих станций сети может следующей использовать ресурсы сети. Каждый метод доступа определяется набором правил (алгоритмом), используемым сетевым оборудованием, чтобы направлять поток сообщений чрез сеть. Метод доступа является одним из основных признаков, по которым различают сетевое оборудование.

Методы доступа к передающей среде могут быть разделены на следующие классы:

Селективные методы

При реализации селективных методов рабочая станция осуществляет передачу только после получения разрешения, которое либо направляется каждой рабочей станции по очереди центральным управляющим органом сети (такой алгоритм называется циклическим опросом), либо передается от станции к станции (алгоритм передачи маркера).

Метод опроса

Эта технология доступа к передающей среде применяется в многоточечных линиях глобальных сетей. Суть ее заключается в том, что первичный узел последовательно предлагает вторичным узлам подключиться к общему каналу передачи. В ответ на такой запрос вторичный узел, имея подготовленные данные, осуществляет передачу. Если подготовленных данных нет, выдается короткий пакет данных типа «данных нет», хотя в современных системах, как правило, реакцией в таких случаях является «молчание».

Наиболее распространенный способ организации запроса – циклический опрос, т.е. последовательное обращение к каждому вторичному узлу в порядке очередности, определяемой списком опроса. Цикл завершается после опроса всех вторичных узлов из списка. Для сокращения потерь времени, связанных с опросом неактивных вторичных узлов (т.е. узлов, по той или иной причине не готовых к передаче данных), применяются специальные варианты процедуры опроса: наиболее активные вторичные узлы опрашиваются несколько раз в течение цикла; наименее активные узлы – один раз в течение нескольких циклов; частота, с которой опрашиваются отдельные узлы, меняется динамически в соответствии с изменением активности узлов.

Метод запроса на передачу

При использовании этого метода инициатива в подаче запроса на обслуживание принадлежит вторичному узлу, причем запрос подается первичному узлу, если действительно имеется необходимость в передаче данных или в получении данных от другого узла.

Эффективность этого метода по сравнению с методом опроса будет тем выше, чем в большей степени вторичные узлы отличаются друг от друга по своей активности, т.е. по частоте подачи запросов на обслуживание. При одних и тех же исходных данных и при

условии, когда все абоненты сети являются активными, в сетях без опроса максимальное время реакции на запрос почти в 2 раза меньше, чем в сетях с опросам, а максимально допустимое число активных абонентов при ограничении времени реакции на запрос – почти в 2 раза больше.

Метод передачи маркера

Этот метод широко используется в сетях с магистральной (шинной), звездообразной и кольцевой топологией. Право на передачу данных станции получают в определенном порядке, задаваемом с помощью маркера, который представляет собой уникальную последовательность бит информации (уникальный кадр). Магистральные сети, использующие этот метод, называются сетями типа "маркерная шина", а кольцевые сети – сетями типа "маркерное кольцо".

В сетях типа ***"маркерная шина"*** доступ к каналу обеспечивается таким образом, как если бы канал был физическим кольцом, причем допускается использование канала некольцевого типа (шинного, звездообразного).

Право пользования каналом передается организованным путем. Маркер (управляющий кадр) содержит адресное поле, где записывается адрес станции, которой предоставляется право доступа в канал. Станция, получив маркер со своим адресом, имеет исключительное право на передачу данных (кадра) по физическому каналу. После передачи кадра станция отправляет маркер другой станции, которая является очередной по установленному порядку владения правом на передачу. Каждой станции известен идентификатор следующей станции. Станции получают маркер в циклической последовательности, при этом в физической шине формируется так называемое логическое кольцо. Все станции "слушают" канал, но захватить канал для передачи данных может только та станция, которая указана в адресном поле маркера. Работая в режиме прослушивания канала, принять переданный кадр может только та станция, адрес которой указан в поле адреса получателя этого кадра.

В сетях типа "маркерная шина", помимо передачи маркера, решается проблема потери маркера из-за повреждения одного из узлов сети и реконфигурации логического кольца, когда в кольцо добавляется или из него удаляется один из узлов.

Преимущества такого метода доступа:

- не требуется физического упорядочения подключенных к шине станций, т.к. с помощью механизма логической конфигурации может быть обеспечен любой порядок передачи маркера станции, т.е. с помощью этого механизма осуществляется упорядочение использования канала станциями;
- имеется возможность использования в загруженных сетях;
- возможна передача кадров произвольной длины.

В сетях типа ***"маркерное кольцо"*** (сети с кольцевой топологией) сигналы распространяются через однонаправленные двухточечные пути между узлами. Узлы и однонаправленные звенья соединяются последовательно, образуя физическое кольцо. В отличие от сетей с шинной структурой, где узлы действуют только как передатчики или приемники и отказ узла или удаление его из сети не влияет на передачу сигнала к другим узлам, здесь при распространении сигнала все узлы играют активную роль, участвуя в ретрансляции, усилении, анализе и модификации приходящих сигналов.

Как и в случае маркерной шины, в качестве маркера используется уникальная последовательность битов. Однако маркер не имеет адреса. Он снабжается полем занятости, в котором записывается один из кодов, обозначающих состояние маркера - свободное или занятое. Если ни один из узлов сети не имеет данных для передачи, свободный маркер циркулирует по кольцу, совершая однонаправленное (обычно против часовой стрелки) перемещение. В каждом узле маркер задерживается на время, необходимое для его приема, анализа (с целью установления занятости) и ретрансляции. В выполнении этих функций задействованы кольцевые интерфейсные устройства.

Свободный маркер означает, что кольцевой канал свободен и что любая станция, имеющая данные для передачи, может его использовать. Получив свободный маркер, станция, готовая к передаче кадра с данными, меняет состояние маркера на "занятый", передает его дальше по кольцу и добавляет к нему кадр. Занятый маркер вместе с кадром совершает полный оборот по кольцу и возвращается к станции-отправителю. По пути станция-получатель, удостоверившись по адресной части кадра, что именно ей он адресован, снимает копию с кадра. Изменить состояние маркера снова на свободное может тот узел, который изменил его на занятое. По возвращении занятого маркера с кадром данных к станции-отправителю кадр удаляется из кольца, а состояние маркера меняется на свободное, после чего любой узел может захватить маркер и начать передачу данных. С целью предотвращения монополизации канала станция-отправитель не может повторно использовать возвращенный к ней маркер для передачи другого кадра данных. Если после передачи свободного маркера в кольцо он, совершив полный оборот, возвращается к станции-отправителю в таком же состоянии ()это означает, что все другие станции сети не нуждаются в передаче данных), станция может совершить передачу другого кадра.

В кольцевой сети в передачей маркера также решается проблема потери маркера в результате ошибок при передаче или при сбоях в узле. Отсутствие передач в сети означает потерю маркера. Функции восстановления кольца в таких случаях выполняет сетевой мониторный узел.

Основные преимущества сетей типа "маркерное кольцо":

- имеется возможность проверки ошибок при передаче данных: станция-отправитель. получив свой кадр от станции-получателя, сверяет его с исходным вариантом кадра. В случае наличия ошибки кадр передается повторно;
- канал используется полностью, его простои отсутствуют;
- метод может быть реализован в загруженных сетях;
- имеется принципиальная возможность (и в некоторых сетях она реализована) осуществлять одновременную передачу несколькими станциями сети.

Недостатки такого подхода:

- невозможность передачи кадров произвольной длины;
- в простейшем (описанном выше) исполнении не предусматривается использование приоритетов, вследствие чего станция, имеющая для передачи важную информацию, вынуждена ждать освобождения маркера, что сопряжено с опасностью несвоевременной доставки данных адресату;
- протокол целесообразно использовать только в локальных сетях с относительно небольшим количеством узлов, т.к. в противном случае время на передачу данных может оказаться неприемлемо большим.

Методы случайного доступа

Методы, основанные на соперничестве (методы случайного доступа, методы "состязаний" абонентов), предполагают, что каждая рабочая станция пытается "захватить" передающую среду. При этом могут использоваться несколько способов передачи данных: базовый асинхронный, синхронизация режима работы канала путем тактирования моментов передачи кадров, прослушивание канала перед началом передачи данных по правилу "слушай, прежде чем говорить", прослушивание канала во время передачи данных по правилу "слушай, пока говоришь". Эти способы используются вместе или раздельно, обеспечивая различные варианты загруженности канала стоимости сети.

Метод множественного доступа с прослушиванием несущей и разрешением коллизий

Этот метод применяется, в основном, в локальных сетях. Все станции сети, будучи равноправными, перед началом передачи работают в режиме прослушивания канала. Если канал свободен, станция начинает передачу; если занят, – станция ожидает завершения передачи. Через некоторое случайное время она снова обращается к каналу.

Поскольку сеть CSMA/CD является равноранговой, в результате соперничества за канал могут возникнуть коллизии: станция В может передать свой кадр, не зная, что станция А уже захватила канал, поскольку от станции А к станции В сигнал распространяется за конечное время. В результате станция В, начав передачу, вошла в конфликт со станцией А (коллизия со станцией А).

Каждая станция способна одновременно и передавать данные, и «слушать» канал. При наложении двух сигналов в канале начинаются аномалии (в виде аномального изменения напряжения), которые обнаруживаются станциями, участвующими в коллизии.

Для разрешения коллизий используется так называемое «окно коллизий», представляющее собой интервал времени, необходимый для распространения сигнала по каналу и обнаружения его любой станцией сети. В наихудших для одноканальной сети условиях время, необходимое для обнаружения столкновения сигналов (коллизии), в два раза больше задержки распространения, так как сигнал, образовавшийся в результате коллизии, должен распространяться обратно к передающим станциям. Чтобы окно коллизии было меньше, такой способ доступа целесообразно применять в сетях с небольшими расстояниями между станциями, т.е. в локальных сетях. Кроме того, вероятность появления коллизий возрастает с увеличением расстояния между станциями сети.

Коллизия является нежелательным явлением, т.к. приводит к ошибкам в работе сети и поглощает много канального времени для ее обнаружения и ликвидации последствий. Поэтому желательно реализовать некоторый алгоритм, позволяющий либо избежать коллизий, либо минимизировать их последствия.

В сети CSMA/CD эта проблема решается на уровне управления доступом к среде путем прекращения передачи кадра сразу же после обнаружения коллизии.

При обработке коллизии компонент управления доступом к среде передающей станции выполняет две функции:
– усиливает эффект коллизии путем передачи специальной последовательности битов, называемой *затором*. Цель затора – сделать коллизию настолько продолжительной, чтобы ее смогли заметить все другие передающие станции, которые вовлечены в коллизию. В локальных сетях затор состоит по меньшей мере из 32 бит, но не более 48

бит. Ограничение длины затора сверху необходимо для того, чтобы станции ошибочно не приняли его за действительный кадр. Любой кадр длиной менее 64 байт считается фрагментом испорченного сообщения и игнорируется принимающими станциями сети;
– после посылки затора прекращает передачу и планирует ее на более позднее время, определяемое на основе случайного выбора интервала ожидания.

Системы с доступом в режиме соперничества реализуются достаточно просто и при малой загрузке обеспечивают быстрый доступ к передающей среде, а также позволяют легко подключать и отключать станции. Они обладают высокой живучестью, поскольку большинство ошибочных и неблагоприятных условий приводит либо к молчанию, либо к конфликту, а обе эти ситуации поддаются обработке. Кроме того, нет необходимости в центральном управляющем органе сети. Их основной недостаток: при больших нагрузках время ожидания доступа к передающей среде становится большим и меняется непредсказуемо, следовательно, не гарантируется обеспечение предельно допустимого времени доставки кадров. Такие системы применяются в незагруженных локальных сетях с небольшим числом абонентских станций (с увеличением числа станций увеличивается вероятность возникновения конфликтных ситуаций).

Методы резервирования времени

Методы, основанные на резервировании времени, принадлежат к числу наиболее ранних и простых. Любая рабочая станция осуществляет передачу только в течение временных интервалов (слотов), заранее для нее зарезервированных. Все слоты распределяются между станциями либо поровну (в неприоритетных системах), либо с учетом приоритетов, когда некоторые рабочие станции за фиксированные интервал времени получают большее число слотов. Станция, владеющая слотом, получает канал в свое полное распоряжение. Такие методы целесообразно применять в сетях с малым числом абонентских систем, так как канал используется неэффективно.

Множественный доступ с временным разделением

Этот метод широко используется в спутниковых сетях связи. Главная (эталонная) станция принимает запросы от вторичных (подчиненных) станций на предоставление канала связи и, реализуя ту или иную дисциплину обслуживания запросов, определяет, какие именно станции и когда могут использовать канал в течение заданного промежутка времени, т.е. предоставляет каждой станции слот. Получив слот, вторичная станция осуществляет временную подстройку, чтобы произвести передачу данных за заданный слот.

Мультиплексная передача с временным разделением

Здесь используется жесткое расписание работы абонентов: каждой станции выделяется интервал времени (слот) использования Канада связи, и все интервалы распределяются поровну между станциями. Во время слота станция получает канал в свое полное распоряжение. Этот способ отличается простотой в реализации и широко применяется в глобальных и локальных сетях.

К недостаткам метода можно отнести возможность неполного использования канала, когда станция, получив слот, не может загрузить канал полностью из-за отсутствия необходимого объема данных для передачи; нежелательные задержки в передаче данных, когда станция, имеющая важную и срочную информацию, вынуждена ждать своего слота или когда выделенного слота недостаточно для передачи подготовленных данных и необходимо ждать следующего слота.

Кольцевые методы

Кольцевые методы предназначены специально для ЛВС с кольцевой топологией, хотя большинство из вышеперечисленных методов могут также использоваться в таких сетях. К кольцевым относятся два метода – вставка регистров и сегментированная передача (метод временны*х* сегментов).

Вставка регистра

При реализации метода вставки регистра рабочая станция ожидает межкадрового промежутка в моноканале. С его появлением регистр включается в кольцо (до этого он был отключен от кольца) и содержимое регистра передается в линию. Если во время передачи станция получает кадр, он записывается в буфер и передается вслед за кадром, передаваемым этой станцией. Такой метод допускает «подсадку» в кольцо нескольких кадров.

Сегментированная передача

При использовании в ЛВС с кольцевой топологией сегментированной передачи временные сегменты формируются управляющей станцией сети. Они имеют одинаковую протяженность и циркулируют по кольцу. Каждая станция, периодические обращаясь в сеть, может дождаться временного сегмента, помеченного меткой «свободный». В этот сегмент станция помещает свой кадр фиксированной длины, при этом в сегменте метка «свободный» заменяется меткой «занятый». После доставки кадра адресату сегмент вновь освобождается. Важным преимуществом такого метода является возможность одновременной передачи кадров несколькими рабочими станциями. Однако передача допускается только кадрами фиксированной длины.

Мониторинг и анализ компьютерных сетей.

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль — это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную. Процесс контроля работы сети обычно делят на два этапа — мониторинг и анализ.

На *этапе мониторинга* выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап *анализа,* под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как

экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Функциональная организация компьютерных сетей.

Серверы и сетевые сервисы

Как уже говорилось ранее (см. Лекция 2, п.2), основными компонентами сети являются коммуникационное оборудование, рабочие станции и серверы сети. На рабочих станциях пользователями сети реализуются прикладные задачи, для решения которых приходится обращаться к общим сетевым ресурсам. Управление тем или иным ресурсом осуществляется серверами.

Каждый конкретный сервер определяется видом того ресурса, которым он владеет. Например, назначением сервера баз данных является обслуживание запросов клиентов, связанных с обработкой данных; файловый сервер управляет доступом к файлам и т.д. Этот принцип распространяется и на взаимодействие программ. Программа, выполняющая предоставление соответствующего набора услуг, рассматривается в качестве сервера, а программы, пользующиеся этими услугами, называют клиентами.

Таким образом, серверы сети - это аппаратно-программные системы, выполняющие функции управления распределение сетевых ресурсов общего доступа, которые могут работать и как обычная абонентская система. В качестве аппаратной части сервера используются достаточно мощный ПК или компьютер, спроектированный специально как сервер. В локальной компьютерной сети может быть несколько различных серверов для управления сетевыми ресурсами. С другой стороны, на одном компьютере может быть запущено несколько серверов (сетевых служб), решающих различные сетевые задачи.

Рассмотрим некоторые виды сервисов, которые могут функционировать как на одном выделенном для этих целей компьютере, так и по отдельности.

Файловый сервер (file server) -

обеспечивает одновременный доступ пользователей к общим данным.

Функции файл-сервера:

- хранение данных;
- архивирование данных;
- согласование изменений данных, выполняемых разными пользователями;
- передача данных.

Как правило, под файл-сервер выделяют специальный компьютер с большим объемом дискового пространства.

Сервер баз данных (database server) -

обеспечивает хранение, обработку и управление файлами баз данных.

Функции сервера баз данных:

- хранение баз данных, поддержка их целостности, полноты, актуальности;
- прием и обработка запросов к базам данных, а также пересылка результатов обработки на рабочую станцию;

- обеспечение авторизированного доступа к базам данных, поддержка системы ведения и учета пользователей, разграничение доступа пользователей;
- согласование изменений данных, выполняемых разными пользователями;
- поддержка распределенных баз данных, взаимодействие с другими серверами баз данных, расположенными в другом месте.

Сервер прикладных программ (application server) -
обеспечивает выполнение прикладных программ для пользователей, работающих на своих рабочих станциях.

Коммуникационный сервер (communications server) -
предоставляет пользователям локальной сети прозрачный доступ к своим последовательным портам ввода/вывода. С помощью коммуникационного сервера можно создать разделяемый модем, подключив его к одному из портов сервера. Пользователь, подключившись к коммуникационному серверу, может работать с таким модемом так же, как если бы модем был подключен непосредственно к рабочей станции.

Сервер доступа (access server) -
позволяет выполнять удаленную обработку заданий. Программы, инициируемые с удаленной рабочей станции, выполняются на этом сервере. От удаленной рабочей станции принимаются команды, введенные пользователем с клавиатуры, а возвращаются результаты выполнения задания.

Факс-сервер (fax server) -
выполняет рассылку и прием факсимильных сообщений для пользователей локальной сети.

Сервер резервного копирования данных (backup server) -
обеспечивает создание, хранение и восстановление копий данных, расположенных на файловых серверах и рабочих станциях.

Еще раз отметим, что все перечисленные типы серверов могут функционировать на одном выделенном для этих целей компьютере.

Организация управления в компьютерных сетях

По организации управления локальные вычислительные сети различаются на сети с централизованным и децентрализованным управлением.

Сети с централизованным управлением

В сетях с централизованным управлением выделяются одна или несколько машин, управляющих работой сети. Диски выделенных машин (файл-серверов или серверов баз данных) доступны всем другим компьютерам (рабочим станциям) сети. На серверах работает сетевая операционная система. Рабочие станции имеют доступ к дискам серверов и совместно используемым принтерам, но, как правило, не могут работать непосредственно с дисками других ПК. Серверы могут быть выделенными, и тогда они выполняют только задачи управления сетью и не используются как ПК, или невыделенными, когда параллельно с задачей управления сетью выполняют пользовательские программы (при этом снижается производительность сервера и надежность работы всей сети из-за возможной ошибки в пользовательской программе,

которая может привести к остановке работы сети). В сетях с централизованным управлением большая часть информационно-вычислительных ресурсов сосредоточена в центральной системе. Они отличаются также более надежной системой защиты информации.

В сетях с централизованным управлением сетевая операционная система (ОС сервера), обеспечивает выполнение базовых функций, таких, как поддержка файловой системы, планирование задач, управление памятью. Сетевая операционная система и ОС рабочей станции решают разные задачи, поэтому для обеспечения взаимодействия сервера и ПК в рабочую станцию вводится специальная программа, называемая сетевой оболочкой. Она воспринимает прикладные запросы пользователей сети и определяет место их обработки - в локальной ОС станции или в сетевой ОС на сервере. Если запрос должен обрабатываться в сети, оболочка преобразует его в соответствии с принятым протоколом, обеспечивая тем самым передачу запроса по нужному адресу.

Одноранговые сети

Если информационно-вычислительные ресурсы локальной компьютерной сети равномерно распределены по большому числу абонентских станций сети, централизованное управление малоэффективно из-за резкого увеличения служебной (управляющей) информации. В этом случае эффективными оказываются сети с децентрализованным (распределенным) управлением, или одноранговые сети.

В таких сетях нет выделенных серверов, функции управления сетью передаются по очереди от одного ПК к другому. Рабочие станции имеют доступ к дискам и принтерам других ПК. Это облегчает совместную работу групп пользователей, но производительность сети несколько понижается. Такие сети отличаются простотой обеспечения функций взаимодействия между абонентскими станциями ЛКС, но их применение целесообразно при сравнительно небольшом числе абонентских станций в сети. Недостатки одноранговых сетей: зависимость эффективности функционирования сети от количества абонентских станций, сложность обеспечения защиты информации от несанкционированного доступа.

В одноранговых сетях объединяются компьютеры, каждый из которых может быть и сервером, и клиентом. В такой сети любой компьютер работает под управлением обычной дисковой ОС, а для выполнения сетевых функций в его оперативную память загружаются программы одноранговой сетевой ОС.

Ведение баз данных в компьютерных сетях

Эффективность функционирования локальных компьютерных сетей в значительной степени определяется способами создания и ведения баз данных. В локальных сетях для создания БД реализованы две архитектуры: *файл-сервер* и *клиент-сервер*. Кроме того, могут использоваться распределенные базы данных.

Архитектура "файл-сервер"

В случае использования архитектуры "файл-сервер" файлы базы данных располагаются на дисках файл-сервера (в качестве файл-сервера применяется мощный ПК), и все рабочие станции получают к нему доступ, т.е. на рабочую станцию устанавливаются сетевые версии широко распространенных СУБД персональных компьютеров. Основной недостаток такой архитектуры заключается в необходимости

пересылки по линиям связи сети фрагментов файлов базы данных значительных объемов, что приводит к быстрому насыщению сетевого трафика и возрастанию времени реакции информационной системы. Следователь, не обеспечивается достаточная производительность сети (особенно при большом количестве рабочих станций).

Архитектура "клиент-сервер"

В архитектуре "клиент-сервер" этот недостаток устранен, в связи с чем обеспечивается совместная работа многих пользователей с большими БД в реальном масштабе времени. Помимо файл-сервера к сети подключается еще один мощный компьютер (сервер баз данных, на котором размещается серверная СУБД) исключительно для работы с БД. Сама база данных может располагаться на дисках сервера баз данных или файл-сервера. Принимая запросы от рабочей станции на поиск данных в БД, сервер баз данных сам осуществляет поиск и его результаты отсылает через сеть в запросившую их рабочую станцию. Следовательно, по сети передаются только запрос и найденные данные. Серверная СУБД обычно работает в среде многозадачной ОС, которая сама занимается распределением ресурсов при поступлении одновременно нескольких запросов от рабочих станций.

Распределенные базы данных

Важным фактором в обеспечении высокой эффективности функционирования локальной компьютерной сети является организация распределенной базы данных, представляющей собой логически единую базу данных, отдельные физические части которой размещены на нескольких ЭВМ сети. Основная особенность распределенной БД - ее "прозрачность", означающая независимость пользователей и прикладных программ от способа размещения информации на ЭВМ сети. Локализация данных, декомпозиция запросов и композиция результатов должны выполняться системой без участия пользователей. В процессе работы пользователи не должны учитывать, что их запросы будут обрабатываться в сети, возможно, на нескольких ЭВМ.

Протокол Telnet. Программа-клиент Telnet.

Главная задача Интернета и его набора протоколов *TCP/IP* — это обеспечить сервис для пользователя. Например, *пользователь*хочет иметь возможность выполнять различные прикладные программы на удаленном сайте и создать результат, который может быть передан к его местному сайту. Один из путей удовлетворения такой потребности — создать различные прикладные программы клиент-*сервер* для каждой услуги. Уже доступны программы передачи файлов (*FTP* и *TFTP*), электронной почты (*SMTP*) и так далее. Однако все конкретные программы клиентсервер для каждого применения описать невозможно.

Лучшее решение — общецелевая *программа* клиент-*сервер*, которая позволяет пользователю иметь *доступ* к любой прикладной программе на удаленном компьютере. После входа в систему *пользователь* может использовать услуги, доступные на удаленном компьютере, и принимать результаты на местном компьютере.

TELNET — это сокращение от Terminals *NETwork*. Это *стандартный протокол TCP/IP* для услуг виртуального терминала. *TELNET*дает возможность устанавливать соединение с удаленным компьютером таким образом, что создается впечатление, как будто местный *терминал* – это *терминал* удаленной системы.

Концепция

TELNET основан на концепциях, которые обсуждаются ниже.

Внешняя среда с разделением времени

TELNET был разработан в эпоху, когда большие операционные системы, такие как UNIX, работали с внешней средой по принципу разделения времени. Согласно этому принципу, большой компьютер поддерживал множество пользователей, предоставляя им часть общего времени. Взаимодействие между пользователем и компьютером осуществляется с помощью терминала, который обычно состоит из комбинации клавиатуры, монитора и мышки. Даже *микрокомпьютер* может моделировать терминал с помощью терминального эмулятора.

В среде с разделением времени вся обработка информации проводится в центральном компьютере. Когда пользователь печатает символ на клавиатуре, символ обычно посылается компьютеру и отражается на мониторе. Разделение по времени создается средой, в которой для каждого пользователя создается иллюзия специализированного компьютера. Пользователь выполняет программу доступа к системным ресурсам, переключается от одной программы к другой и так далее.

Логин

В среде с разделением времени *пользователь* — это часть системы с некоторыми правами и, вероятно, с паролем. Каждый полномочный *пользователь* имеет *идентификатор* и *пароль*.
Пользовательская *идентификация* определяет пользователя как часть системы. Для доступа к системе *пользователь* начинает *сеанс* с пользовательского идентификатора (id) или с регистрационного имени (*login name*). Система помогает проверке пароля, чтобы предотвратить *доступ* к ресурсу неполномочного пользователя.

Местный логин

Когда пользователь входит в местную систему с разделением времени, это называется местный логин. Как только пользователь напечатает некое слово на терминале или рабочей станции, выполняющей эмуляцию терминала, сразу начинает работать терминальная программа (драйвер), которая распознает значение введенных символов. Терминальный драйвер передает символы операционной системе, в рамках этой системы комбинация символов интерпретируется и вызывает желаемую прикладную программу или утилиту (рис. 12.1).

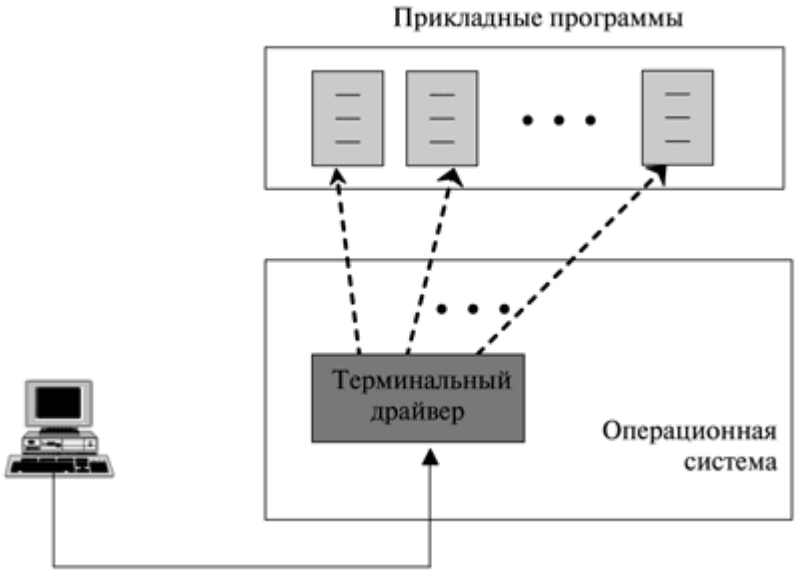


Рис. 12.1. Местный login

Однако этот механизм не такой простой, как кажется, потому что операционная система может назначить специальные значения для специальных символов. Скажем, в UNIX некоторые комбинации символов имеют специальное значение, например, комбинации управляющих символов с символом "z", которые означают прекращение действия; комбинации управляющих символов с символом "c" означают остановку; и так далее. Несмотря на то что эти специальные ситуации не создают никаких проблем в местном вхождении в систему (login), потому что терминальный эмулятор и терминальный драйвер знают точно значение каждого символа и комбинации символов, они могут создавать проблемы при удаленном входе в систему. Какой процесс должен интерпретировать специальные символы? Клиент или сервер? Эта ситуация будет рассмотрена в этой лекции позднее.

Удаленный логин

Когда пользователь хочет иметь доступ к прикладной программе или утилите, размещенным на удаленном компьютере, он выполняет дистанционный вход в систему (логин). Здесь TELNET берет на себя функции клиента и сервера. Пользователь посылает сигнал нажатия кнопки терминальному драйверу, где местная операционная система принимает символы и интерпретирует их. Эти символы посылает TELNET-клиент, который преобразует символы к универсальному набору, называемому символы виртуального сетевого терминала (Network *Virtual Terminal* Characters), и доставляет их к местному стеку протоколов TCP/IP (рис. 12.2).

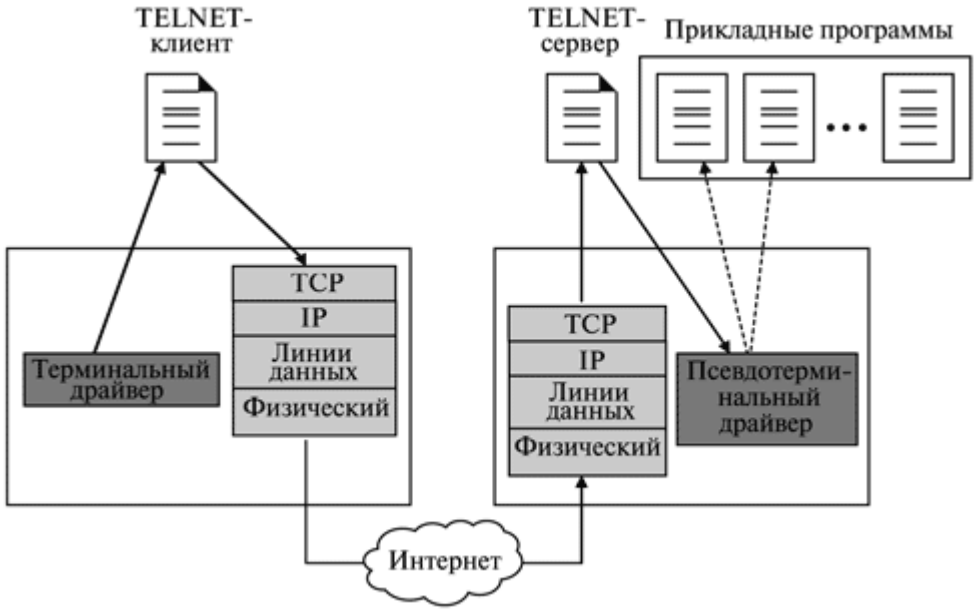


Рис. 12.2. Дистанционный login

Команды или текст в форме сетевого виртуального терминала (*NVT*) перемещаются через Интернет и прибывают на стек протоколов TCP/IP в удаленной машине. Здесь символы доставляются операционной системе и проходят к TELNET-серверу, который преобразует их в символы, понятные удаленному компьютеру. Однако символы не могут пройти прямо на операционную систему, потому что удаленная операционная система не разработана для получения трактовки этих символов от TELNET. Она спроектирована так, чтобы принимать символы от драйвера терминала. Решение, добавляющее необходимое программное обеспечение, называется псевдотерминальным драйвером, который преобразовывает поступившие символы как символы, поступающие от местного терминала. Операционная система затем предает символы к соответствующей прикладной программе.

Сетевой виртуальный терминал (NVT)

Механизм для доступа удаленного компьютера должен быть комплексным с учетом специфики каждой операционной системы. Например, для некоторых операционных систем знак конца — это Ctrl+z, в то время как в других операционных системах — этоCtrl+d.

Если мы хотим иметь *доступ* к любому удаленному компьютеру в мире, мы должны сначала знать специфику терминального эмулятора, используемую этим компьютером. *TELNET* решает эти проблемы определением *универсального интерфейса*, называемого *NVT* (*Network Virtual Terminal* — виртуальный сетевой *терминал*). Для каждого интерфейса *TELNET* переводит символы (данные или команды), которые получает от местного терминала, в *NVT*-форму и доставляет их в *сеть*. С другой стороны, *сервер TELNET* переводит команды из формы *NVT* в форму, доступную удаленному компьютеру. Все иллюстрации этой концепции смотрите на рисунке 12.3.

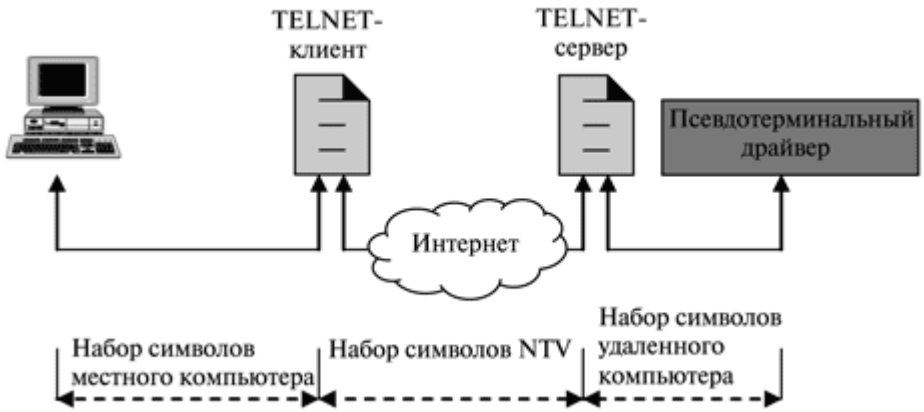


Рис. 12.3. Концепция NVT

Проводные и беспроводные компьютерные сети.

Технология WI-FI История беспроводных технологий передачи информации началась в конце XIX века с передачей первого радиосигнала и появлением в 20-х годах XX века первых радиоприемников с амплитудной модуляцией. В 1930-е годы появилось радио с частотной модуляцией и телевидение. В 1970-е годы были созданы первые беспроводные телефонные системы. Сначала это были аналоговые сети, в начале 1980-х появился стандарт GSM, ознаменовавший начало перехода на цифровые стандарты как обеспечивающие лучшее распределение спектра, лучшее качество сигнала и большую безопасность. С 90-х годов XX века происходит укрепление позиций беспроводных сетей. Беспроводные технологии прочно входят в нашу жизнь. Развиваясь с огромной скоростью, они стимулируют создание новых устройств и услуг.

WI-FI – это **современная беспроводная технология** соединения компьютеров в локальную сеть и подключения их к Internet. Именно благодаря этой технологии Internet становится мобильным и дает пользователю свободу перемещения не то что в пределах комнаты, но и по всему миру. Представьте себе такую картину: вы пользуетесь своим компьютером так же, как сейчас - мобильным телефоном; вам не нужны провода, вы можете взять свой ноутбук в любую точку Москвы и войти в Internet практически отовсюду.

Режимы и особенности организации технологии Wi-Fi Беспроводные сети Wi-Fi поддерживают несколько различных режимов работы, реализуемых для конкретных целей. Каждый режим сопровождается пояснительным рисунком для лучшего представления взаимодействия элементов сети. Большим плюсом является подробное описание настройки подключения, используя как встроенные в Windows службы, так и утилиту D-Link AirPlus XtremeG Wreless Utility, которая идет в комплекте с оборудованием D-Link. Очень интересно будет ознакомиться с режимами WDS и WDS WITH AP, которые образуют мостовое соединение.

Беспроводная технология WiMAX WiMAX – очень перспективное направление в развитии беспроводных технологий. Характеристики технологии WiMAX во многом превосходят стандарт IEEE 802.11. Довольно интересно будет ознакомиться с архитектурой работы системы WiMAX. Несомненно, существует несколько режимов работы стандарта IEEE 802.16. Как ни странно, у новой технологии есть несколько сдерживающих факторов, ограничивающих ее быстрое распространение.

Технология Smart Antenna, поддерживающая субканалы и эстафетную передачу сессии между каналами, что позволяет использовать сложные системы антенн, включая формирование диаграммы направленности, пространственно-временное маркирование, пространственное мультиплексирование (уплотнение).

Электронная почта. Протоколы электронной почты.

Служба электронная почта - предназначена для обмена сообщениями (письмами).

Клиент (MS Outlook, The bat ...) готовит ("упаковывает") и посылает серверу (почтовое отделение) сообщения, принимает и просматривает сообщения.

Сервер электронной почты (Sendmail, MS Exchange ...) обрабатывает сообщения (сортирует) и отправляет локальному адресату или удаленному серверу (почтовому отделению).

Электронная почта во многом похожа на обычную почтовую службу.

Основные протоколы:

- SMTP (Simple Mail Transfer Protocol) - простой протокол передачи почты, используется для **отправки** почты, как клиентом на сервер, так и сервером на другой сервер.
- POP3 (Post Office Protocol) - используется для **приема** почты клиентом с сервера.
- IMAP 4 (Internet Message Access Protocol) -
- UUCP (Unix-Unix-CoPy) - используется для **отправки и приема** почты, как клиентом на(с) сервер(а), так и сервером на другой сервер. В данное время почти не используется, поэтому рассматривать не будем.

Физическая передающая среда локальной вычислительной сети: коаксиальный кабель, витая пара, оптоволокно.

Передающие среды

Итак, передача сигнала может происходить либо по кабелю, либо посредством радиосвязи. Основным параметром любого канала связи является его пропускная способность (см. выше). На уровень пропускной способности, в свою очередь, влияют:

- *частотный диапазон канала* - интервал частот синусоидальных колебаний, передаваемых без повреждений;
- *динамический диапазон* или отношение "сигнал/шум", измеряемый обычно в децибелах (дБ) - логарифмическая мера ослабления/усиления сигнала (20 дБ - ослабление или усиление в 10 раз, 40 дБ - в 100 раз, 60 дБ - в 1000 раз и т.д.).

Кабель "витая пара"

Витая пара (twisted pair) **-**

проводное соединение, состоящее из двух перевитых медных проводов, заключенных в оболочку. Проводники скручиваются с определенным шагом для уменьшения влияния помех.

Кабель "витая пара" позволяет передавать информацию со скоростью до 100 Мбит/с, легко наращивается, однако отличается слабой устойчивостью к помехам. Длина кабеля не может превышать 1000 м при скорости передачи 10 Мбит/с.

Типы витых пар:

- по количеству витых пар:
  - одинарные,
  - объединенные в многопарный кабель,
  - оформленные в виде плоского ленточного кабеля;

- по устойчивости к помехам:
  - экранированные (STP, Shielded Twisted Pair)
    применяются, когда локальная сеть прокладывается в помещениях с высоким уровнем электромагнитных помех, либо требуется повысить точность передачи информации за счет снижения перекрестных нгаводок в кабеле. Как правило, экран выполняется из металлической фольги. При этом существует несколько различных вариантов экранирования: фольгой может быть обернута каждая из четырех пар, плюс все они защищены сверху дополнительным слоем фольги, расположенным под внешней изоляцией (STP), либо внутри кабеля предусмотрен один общий для всех пар экран (FTP).
  - неэкранированные (UTP, Unshielded Twisted Pair);

- по категории:
  исходя из функциональных характеристик, таких как пропускная способность и устойчивость к помехам, различные марки кабеля "витая пара" принято делить на несколько категорий, в соответствии с международными стандартами.

  Категории обозначаются номерами: 1, 2, 3, 4, 5, 5+, 6. Номер категории указывает на скорость передачи. Чем выше номер категории, тем большую скорость передачи поддерживает кабель. Кабели 1 и 2 категорий применяются для телефонных линий и не подходят для передачи данных в компьютерных сетях.

  Кабели, изготовленные из витых пар категории 5 с частотной полосой 100 МГц, обеспечивают пропускную способность до 155 Мбит/с. При четырех витых парах это позволяет осуществлять передачу до 622 Мбит/с. Кабели категории 6 сертифицируются до частот 300 МГц, а экранированные и до 600 МГц. Такой кабель может иметь пропускную способность более 1 Гбит/с.

Для локальных сетей наиболее часто используют неэкранированный кабель категории 5. Сетевые адаптеры, работающие с витой парой, имеют разъем RJ-45, по внешнему виду похожий на телефонный разъем RJ-11. Локальные сети, построенные на витой паре, имеют, как правило, топологию "звезда". Центром звезды является концентратор (Hub). Максимальное расстояние от концентратора до рабочей станции составляет 100 м.

Достоинства и недостатки

Кабели "витая пара" легко наращиваются, дешевы, системы на витой паре менее уязвимы, по сравнению с коаксиальными кабелями, к внешним наводкам. Однако отличаются слабой устойчивостью к помехам; длина кабеля не может превышать 1000 м при скорости передачи 10 Мбит/с. Поэтому возникают серьезные ограничения на количество станций в сети на витой паре и на ее длину: максимальное расстояние между узлами составляет 100 м.

Коаксиальный кабель

Коаксиальный кабель (coaxial cable)-

"коаксиальный" означает "соосный". Сигнал в кабеле распространяется по центральной медной жиле, контур тока замыкается через внешний экранирующий слой.

Коаксиальные кабели вызывают минимальное внешнее электромагнитное излучение. При заземлении экрана в нескольких точках по нему начинают протекать выравнивающие токи. Такие токи могут стать причиной внешний наводок (иной раз достаточных для выхода из строя интерфейсного оборудования). Именно это обстоятельство является причиной требования заземления кабеля локальной сети только в одной точке.

Виды коаксиального кабеля:

- *Широкополосный коаксиальный кабель* не восприимчив к помехам, легко наращивается, но цена его высока. Скорость передачи данных равна 500 Мбит/с. При передаче информации в базисной полосе частот на расстояние более 1,5 км требуется усилитель (репитер, повторитель). Поэтому суммарное расстояние при передаче данных увеличивается до 10 км. Для компьютерных сетей с топологией "шина" или "дерево" коаксиальный кабель должен иметь на конце согласующий резистор (терминатор).

- *Ethernet-кабель* также является коаксиальным кабелем с волновым сопротивлением 50 см. Его называют еще *толстый Ethernet* (*thick*) или *желтый кабель* (*yellow cable*). Он использует 15-контактное стандартное включение. Вследствие повышенной помехозащищенности является дорогой альтернативой обычным коаксиальным кабелям.
  Максимально доступное расстояние без повторителя не превышает 500 м (если общая длина сети больше 500 м, ее необходимо разбить на сегменты, соединенные друг с другом через репитеры), а общее расстояние сети Ethernet - около 3000 м.

- *Cheapernet-кабель* является более дешевым, чем Ethernet-кабель. Его называют также *тонкий (thin) Ethernet*. Это также 50-омный коаксиальный кабель со скоростью передачи информации в 10 Мбит/с.
  При соединении сегментов Cheapernet-кабеля также требуются повторители. Соединения сетевых плат производится с помощью малогабаритных байонетных разъемов СР-50. Дополнительное экранирование не требуется.
  Расстояние между двумя рабочими станциями без повторителей может составлять максимум 300 м, а общее расстояние для сети на Cheapernet-кабеле - около 1000 м. Приемопередатчик Cheapernet расположен на сетевой плате как для гальванической развязки между адаптерами, так и для усиления внешнего сигнала. Сеть Ethernet на тонком кабеле существенно проще, чем на толстом.

Достоинства и недостатки

Коаксиальный кабель имеет среднюю цену, хорошо помехозащищен и применяется для связи на относительно большие расстояния (несколько км). Коаксиальный кабель используется для основной и широкополосной передачи информации. В настоящее время коаксиальный кабель не применяется как основная транспортная среда локальных сетей. Коаксиальные кабели используются для построения магистральных линий в компьютерных сетях, а также там, где требуется высокий уровень защиты от радиоэлектронных помех.

Оптоволоконные кабели

Оптоволоконный кабель (fiber optic) -

в волоконно-оптическом кабеле данные передаются с помощью световых импульсов, проходящих по оптическому волокну. Сердечник такого кабеля изготовлен из стекла или пластика. Сердечник окружается слоем отражателя, который направляет световые импульсы вдоль кабеля.

Свет (длина волны $\lambda \sim 1350$ или 1500 нм) вводится в оптоволокно (диаметром менее 100 μ - микрон, микрометров) с помощью светоизлучающего диода или полупроводникового лазера. Центральное волокно покрывается слоем (клэдинг), коэффициент преломления которого меньше, чем у центрального ядра (стрелками условно показан ход луче2й света в волокне). Для обеспечения механической прочности извне волокно покрывается полимерным слоем.

Характеристика оптоволокон

Существует несколько типов оптических волокон, обладающих различными свойствами. Они отличаются друг от друга зависимостью коэффициента преломления от радиуса центрального волокна.

Понятие «открытая архитектура». ISO.

Требования к организации сети

Основными требованиями, которым должна удовлетворять организация ИВС, являются следующие:

1. **Открытость** - возможность включения дополнительных абонентских, ассоциативных ЭВМ, а также линий (каналов) связи без изменения технических и программных средств существующих компонентов сети. Кроме того, любые две ЭВМ должны взаимодействовать между собой, несмотря на различие в конструкции, производительности, месте изготовления, функциональном назначении.
2. **Гибкость** - сохранение работоспособности при изменении структуры в результате выхода из строя ЭВМ или линии связи.
3. **Эффективность** - обеспечение требуемого качества обслуживания пользователей при минимальных затратах.

Модель OSI

Международной организацией стандартов утверждены определённые требования к организации взаимодействия между системами сети.
Эти требования получили название *OSI (Open System Interconnection)* - "эталонная модель взаимодействия открытых систем".
Согласно требованиям эталонной модели, каждая система сети должна осуществлять

взаимодействие посредствам передачи кадра данных. Согласно модели OSI образование и передача кадра осуществляется с помощью 7-ми последовательных действий, получивших название "уровень обработки".
Основная идея этой модели заключается в том, что каждому уровню отводится конкретная ролью в том числе и транспортной среде. Благодаря этому общая задача передачи данных расчленяется на отдельные легко обозримые задачи.
Так как пользователи нуждаются в эффективном управлении, система вычислительной сети представляется как комплексное строение, которое координирует взаимодействие задач пользователей.
Отдельные уровни базовой модели проходят в направлении вниз от источника данных (от уровня 7 к уровню 1) и в направлении вверх от приемника данных (от уровня 1 к уровню 7). Пользовательские данные передаются в нижерасположенный уровень вместе со специфическим для уровня заголовком до тех пор, пока не будет достигнут последний уровень.
На приемной стороне поступающие данные анализируются и, по мере надобности, передаются далее в вышерасположенный уровень, пока информация не будет передана в пользовательский прикладной уровень.

Уровень 1. Физический.
На физическом уровне определяются электрические, механические, функциональные и процедурные параметры для физической связи в системах. Физическая связь и неразрывная с ней эксплуатационная готовность являются основной функцией 1-го уровня. Стандарты физического уровня включают рекомендации V.24 МККТТ (CCITT), EIA rS232 и X.21. Стандарт ISDN (Integrated Services Digital Network) в будущем сыграет определяющую роль для функций передачи данных. В качестве среды передачи данных используют трехжильный медный провод (экранированная витая пара), коаксиальный кабель, оптоволоконный проводник и радиорелейную линию.

Уровень 2. Канальный.
Канальный уровень формирует из данных, передаваемых 1-м уровнем, так называемые "кадры", последовательности кадров. На этом уровне осуществляются управление доступом к передающей среде, используемой несколькими ЭВМ, синхронизация, обнаружение и исправление ошибок.

Уровень 3. Сетевой.
Сетевой уровень устанавливает связь в вычислительной сети между двумя абонентами. Соединение происходит благодаря функциям маршрутизации, которые требуют наличия сетевого адреса в пакете. Сетевой уровень должен также обеспечивать обработку ошибок, мультиплексирование, управление потоками данных. Самый известный стандарт, относящийся к этому уровню, - рекомендация X.25 МККТТ (для сетей общего пользования с коммутацией пакетов).

Уровень 4. Транспортный.
Транспортный уровень поддерживает непрерывную передачу данных между двумя взаимодействующими друг с другом пользовательскими процессами. Качество транспортировки, безошибочность передачи, независимость вычислительных сетей, сервис транспортировки из конца в конец, минимизация затрат и адресация связи гарантируют непрерывную и безошибочную передачу данных.

Уровень 5. Сеансовый.
Сеансовый уровень координирует прием, передачу и выдачу одного сеанса связи. Для координации необходимы контроль рабочих параметров, управление потоками данных промежуточных накопителей и диалоговый контроль, гарантирующий передачу, имеющихся в распоряжении данных. Кроме того, сеансовый уровень содержит

дополнительно функции управления паролями, подсчета платы за пользование ресурсами сети, управления диалогом, синхронизации и отмены связи в сеансе передачи после сбоя вследствие ошибок в нижерасположенных уровнях.

Уровень 6. Представления данных.

Уровень представления данных предназначен для интерпретации данных; а также подготовки данных для пользовательского прикладного уровня. На этом уровне происходит преобразование данных из кадров, используемых для передачи данных в экранный формат или формат для печатающих устройств оконечной системы.

Уровень 7. Прикладной.

В прикладном уровне необходимо предоставить в распоряжение пользователей уже переработанную информацию. С этим может справиться системное и пользовательское прикладное программное обеспечение.

Коммуникационное оборудование сетей.

Коммутирующие устройства предназначены для связи сегментов сети.
Концентратор- хаб (Hub) - устройство физического подключения нескольких сегментов или лучей, обычно с возможностью соединения сетей различных архитектур.
Интеллектуальный хаб (Intelligent Hub) имеет специальные средства для диагностики и управления, что позволяет оперативно получать сведения об активности и исправности узлов, отключать неисправные узлы и т. д. Стоимость существенно выше, чем у обычных.
Активный хаб (Active Hub) усиливает сигналы, требует источника питания.
Peer Hub - хаб, исполненный в виде платы расширения PC, использующей только источник питания PC.
Пассивный хаб (Passive Hub) только согласует импедансы линий (в сетях ArCnet).
Standalone Hub - самостоятельное устройство с собственным источником питания (обычный вариант).
Повторитель (repeater) - устройство для соединения сегментов одной сети, обеспечивающее промежуточное усиление и формирования сигналов.Позволяет расширять сеть по расстоянию и количеству подключенных узлов.
Мост (Bridge) - средство передачи пакетов между сетями (локальными), для протоколов сетевого уровня прозрачен. Осуществляет фильтрацию пакетов, не выпуская из сети пакеты для адресатов, находящихся внутри сети, а также переадресацию - передачу пакетов в другую сеть в соответствии с таблицей маршрутизации или во все другие сети при отсутствии адресата в таблице. Таблица маршрутизации обычно составляется в процессе самообучения по адресу источника приходящего пакета.
Маршрутизатор (router) - средство обеспечения связи между узлами различных сетей, использует сетевые (логические) адреса. Сети могут находиться на значительном расстоянии, и путь, по которому передается пакет, может проходить через несколько маршрутизаторов. Сетевой адрес интерпретируется как иерархическое описание местоположения узла. Маршрутизаторы поддерживают протоколы сетевого уровня: IP, IPX, X.25, IDP. Мультипротокольные маршрутизаторы (более сложные и дорогие) поддерживают несколько протоколов одновременно для гетерогенных сетей. Brouter (Bridging router) - комбинация моста и маршрутизатора, оперирует как на сетевом, так и на канальном уровне.

Основные характеристики маршрутизатора:

- тип: одно- или многопротокольный, LAN или wAN, Brouter;
- поддерживаемые протоколы;
- пропускная способность;
- типы подключаемых сетей;
- поддерживаемые интерфейсы (LAN и wAN);
- количество портов;
- возможность управления и мониторинга сети.

Шлюз (Gateway) - средство соединения существенно разнородных сетей. В отличие от повторителей, мостов и маршрутизаторов, прозрачных для пользователя, присутствие шлюза заметно. Шлюз выполняет преобразование форматов и размеров пакетов, преобразование протоколов, преобразование данных, мультиплексирование. Обычно реализуется на основе компьютера с большим объемом памяти.
Примеры шлюзов:
Fax: обеспечивает доступ к удаленному факсу, преобразуя данные в факс-формат;
E-mail: обеспечивает почтовую связь между локальными сетями. Шлюз обычно связывает MHS, специфичный для сетевой операционной системы с почтовым сервисом по X.400;
Internet: обеспечивает доступ к глобальной сети Internet.

Организация доменов и доменных имен. Домены на кириллице. Определение имен узлов.

Доменные имена

Собственно имя компьютера или домена состоит из:

- латинских букв;
- цифр;
- знака тире (–).

В имени должна быть хотя бы одна буква. Регистр букв значения не имеет (строчные и заглавные буквы можно употреблять на равных). Имена вида "195.19" недопустимы, их можно спутать с IP-адресами.

Полное доменное имя начинается с имени компьютера,
за которым следует имя домена, к которому принадлежит компьютер,
за которым следует имя домена, к которому принадлежит тот домен, к которому принадлежит компьютер
и так далее, пока не будут перечислены все домены.

Примеры:
comphys.phys.spbu.ru
ftp.microsoft.com

Доменные имена верхнего уровня

Такие домены, которые не вложены ни в какие другие домены, называются доменами верхнего

уровня.

Географические домены верхнего уровня соответствуют странам. Имена географических доменов верхнего уровня состоят из двух букв.

Примеры:

- ru – Россия;
- ua – Украина;
- au – Австралия;
- at – Австрия.

Тематические домены верхнего уровня

Имена тематических доменов верхнего уровня состоят из трех или более букв.

Примеры:

- mil – организации Министерства обороны США;
- gov – правительственные учреждения США;
- edu – учреждения образования (в основном, США, но встречаются и домены в других
- странах);
- com – коммерческие организации;
- org – некоммерческие организации;
- int – международные организации;
- net – все остальные организации и даже частные лица, имеющие отношение к сетевой
- деятельности.
- unesco.org – международная организация ЮНЕСКО;
- microsoft.com – коммерческая фирма Microsoft;
- hp.com – коммерческая фирма Hewlett-Packard.

Служба доменных имен

Служба доменных имен – отвечает за преобразование доменных имен в IP-адреса и обратно (DNS – Domain Name Server). Состоит из компьютеров, программ, баз данных и людей, которые сопровождают базы данных, программы и компьютеры, на которых эти программы работают. Эти люди – администраторы DNS – вручную заносят в базы данных DNS информацию о соответствии между доменными адресами и IP-номерами. 4

Программа, работающая с Интернетом, получив от пользователя доменное имя, в первую очередь обращается к тому компьютеру, на котором работает программа DNS с запросом о преобразовании этого имени в IP-номер. Только получив от DNS IP-номер, эта программа начинает связываться с соответствующим сетевым интерфейсом.

DNS жизненно необходима для работы в Интернете. В сетевых настройках компьютера должен быть указан IP-номер того компьютера, на котором работает программа DNS.

Для каждого сервера имен определен "вышестоящий" сервер имен, к которому он обращается, если не в состоянии преобразовать имя в IP-номер или выполнить обратное преобразование. На самом верхнем уровне иерархии расположены 10 дублирующих друг друга компьютеров, в базах данных которых содержится информация об IP-номерах серверов имен доменов верхнего уровня – эти компьютеры "знают", какой именно из "подчиненных" компьютеров ведет заданный домен.

Если вы обратились к какому-то компьютеру, то велика вероятность, что вы обратитесь к нему еще раз:

- прочитав каталог ftp-сервера, вы либо смените каталог, либо захотите скачать файл;
- получив HTML-страницу, вы, щелкнув по ссылке, можете перейти на другую страницу того же сайта;
- получив электронную почту, вы захотите отправить ответ и т. д.

поэтому серверы имен, получив однажды с другого сервера имен информацию о соответствии доменного имени и IP-номера, хранят такую информацию неделю.

Протоколы: основные понятия и принципы взаимодействия.

Главная цель, которая преследуется при соединении компьютеров в сеть - это возможность использования ресурсов каждого компьютера всеми пользователями сети. Для того, чтобы реализовать эту возможность, компьютеры, подсоединенные к сети, должны иметь необходимые для этого средства взаимодействия с другими компьютерами сети. Задача разделения сетевых ресурсов является сложной, она включает в себя решение множества проблем - выбор способа адресации компьютеров и согласование электрических сигналов при установление электрической связи, обеспечение надежной передачи данных и обработка сообщений об ошибках, формирование отправляемых и интерпретация полученных сообщений, а также много других не менее важных задач.

Обычным подходом при решении сложной проблемы является ее декомпозиция на несколько частных проблем - подзадач. Для решения каждой подзадачи назначается некоторый модуль. При этом четко определяются функции каждого модуля и правила их взаимодействия.

Частным случаем декомпозиции задачи является многоуровневое представление, при котором все множество модулей, решающих подзадачи, разбивается на иерархически упорядоченные группы - уровни. Для каждого уровня определяется набор функций-запросов, с которыми к модулям данного уровня могут обращаться модули выше лежащего уровня для решения своих задач. Такой формально определенный набор функций, выполняемых данным уровнем для выше лежащего уровня, а также форматы сообщений, которыми обмениваются два соседних уровня в ходе своего взаимодействия, называется *интерфейсом*.

Интерфейс определяет совокупный сервис, предоставляемый данным уровнем выше лежащему уровню.

При организации взаимодействия компьютеров в сети каждый уровень ведет "переговоры" с соответствующим уровнем другого компьютера. При передаче

сообщений оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности и т.п. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого уровня передачи битов, до самого высокого уровня, детализирующего, как информация должна быть интерпретирована.

Правила взаимодействия двух машин могут быть описаны в виде набора процедур для каждого из уровней. Такие формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются *протоколами*.

Из приведенных определений можно заметить, что понятия "интерфейс" и "протокол", в сущности, обозначают одно и то же, а именно - формализовано заданные процедуры взаимодействия компонент, решающих задачу связи компьютеров в сети. Однако довольно часто в использовании этих терминов имеется некоторый нюанс: понятие "протокол" чаще применяют при описании правил взаимодействия компонент одного уровня, расположенных на разных узлах сети, а "интерфейс" - при описании правил взаимодействия компонентов соседних уровней, расположенных в пределах одного узла.

Согласованный набор протоколов разных уровней, достаточный для организации межсетевого взаимодействия, называется *стеком протоколов*.

Программные средства, реализующие некоторый протокол, также называют протоколом. При этом соотношение между протоколом - формально определенной процедурой взаимодействия, и протоколом - средством, реализующим эту процедуру, аналогично соотношению между алгоритмом решения некоторой задачи и программой, решающей эту задачу. Понятно, что один и тот же алгоритм может быть запрограммирован с разной степенью эффективности. Точно также и протокол может иметь несколько программных реализаций, например, протокол IPX, реализованный компанией Microsoft для Windows NT в виде программного продукта NWLink, имеет характеристики, отличающиеся от реализации этого же протокола компанией Novell. Именно поэтому, при сравнении протоколов следует учитывать не только логику их работы, но и качество программных решений. Более того, на эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, то есть, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними.

Протоколы реализуются не только программно-аппаратными средствами компьютеров, но и коммуникационными устройствами. Действительно, в общем случае связь компьютеров в сети осуществляется не напрямую - "компьютер-компьютер", а через различные коммуникационные устройства такие, например, как концентраторы, коммутаторы или маршрутизаторы. В зависимости от типа устройства, в нем должны быть встроены средства, реализующие некоторый набор сетевых протоколов.

При организации взаимодействия могут быть использованы два основных типа протоколов. В протоколах *с установлением соединения* (connection-oriented network service, CONS) перед обменом данными отправитель и получатель должны сначала установить логическое соединение, то есть договориться о параметрах процедуры обмена, которые будут действовать только в рамках данного соединения. После завершения диалога они должны разорвать это соединение. Когда устанавливается новое соединение, переговорная процедура выполняется заново. Телефон - это пример взаимодействия, основанного на установлении соединения.

Вторая группа протоколов - протоколы *без предварительного установления* соединения (connectionless network service, CLNS). Такие протоколы называются также *дейтаграммными*протоколами. Отправитель просто передает сообщение, когда оно готово. Опускание письма в почтовый ящик - это пример связи без установления соединения.

Виды адресации в компьютерных сетях.

Виды адресации в компьютерных сетях

Для того, чтобы компьютеры могли идентифицировать друг друга в информационно-вычислительной сети, им присваиваются явные адреса. Основными типами адресов являются следующие:

- MAC-адрес;
- IP-адрес;
- доменный адрес;
- URL.

Физические адреса

MAC-адрес, который также называют ***физическим адресом***, ***Ethernet-адресом***, присваивается каждому сетевому адаптеру при его производстве. Его размер - 6 байт.

Этот сетевой адрес является уникальным, - фирмам-производителям выделены списки адресов, в рамках которых они обязаны выпускать карты. Адрес записывается в виде шести групп шестнадцатеричных цифр по две в каждой (шестнадцатеричная запись байта). Первые три байта называются префиксом (что определяет 2^{24} различных комбинаций или почти 17 млн адресов), и именно они закреплены за производителем.

Адаптер "слушает" сеть, принимает адресованные ему кадры и широковещательные кадры с адресом FF:FF:FF:FF:FF:FF и отправляет кадры в сеть, причем в каждый момент времени в сегменте узла сети находится только один кадр.

Собственно, MAC-адрес соответствует не компьютеру, а его сетевому интерфейсу. Таким образом, если компьютер имеет несколько интерфейсов, то это означает, что каждому интерфейсу будет назначен свой физический адрес. Каждой сетевой карте соответствует собственный MAC-адрес и IP-адрес, уникальный в рамках глобальной сети.

MAC-адреса используются на физическом и канальном уровнях, т.е. в "однородной" среде. Для того, чтобы могли связываться друг с другом компьютеры, входящие в большие составные сети, используется другой вид адресов - IP-адреса.

IP-адресация

IP-адрес является основным видом адресации в Internet. Он обозначает не только компьютер, но и сегмент сети, в котором находится данный компьютер. Например, адрес 192.123.004.010 соответствует узлу номер 10 в сети 192.123.004. У другого узла в этом же

сегменте может быть номер 20 и т.д. Сети и узлы в них - это отдельные объекты с отдельными номерами.

IP-адрес -

представляет собой 32-разрядное двоичное число (например, 11000000 01111011 00001010). Для удобства оно разбивается на четыре восьмиразрядных поля, называемых*октетами*. TCP/IP представляет эти двоичные октеты их десятичными эквивалентами (в данном примере это 192.123.004.010), что облегчает использование IP-адресов для человека.

Классы IP-сетей

Эти четыре октета в разных сетях обозначают разные вещи. В некоторых организациях создается одна большая сеть, но с миллионами узлов. Здесь первый октет адреса используется для обозначения сети, а остальные три октета - для обозначения отдельных рабочих станций. Такой адрес называют адресом класса А. Самые частые потребители адресов класса А - поставщики сетевых услуг (провайдеры), которые обслуживают очень большие сети с тысячами конечных пунктов.

В некоторых организациях могут быть тысячи узлов, включенных в состав нескольких сетей. В таких случаях используются адреса класса В, в которых первые два октета (16 битов) используются для обозначения сети, а последние два - для обозначения отдельных узлов. Наиболее известные потребители адресов класса В - университеты и крупные учреждения.

Наконец, наиболее часто используется адрес класса С, в котором первые три октета (или 24 бита) служат для обозначения сегмента, а последний октет - для обозначения рабочих станций. Такие адреса лучше всего подходят для случая, когда имеется множество отдельных сетей, в состав каждой из которых входит всего несколько десятков узлов. Адреса такого типа чаще всего встречаются в локальных сетевых средах, где в одном сетевом сегменте в среднем бывает около 40 узлов.

При соединении сети класса А с сетью класса В маршрутизатору необходимо сообщить, как он должен отличать одну сеть от другой. В противном случае он подумает, что трафик, исходящий из сети класса С и предназначенный для узла класса, можно идентифицировать по последнему октету. На самом же деле узел класса А обозначается последними тремя октетами - а это большая разница. Не зная этого, маршрутизатор попытается найти трехоктетную сеть, к которой подключен однооктетный хост. На самом же деле ему нужно послать данные в однооктетную сеть, в которой находится трехоктетный хост.

Стек протоколов TCP/IP использует первые три бита первого октета для идентификации класса сети, позволяя устройствам автоматически распознавать соответствующие типы адресов. У адресов класса А первый бит установлен в 0, а остальные семь битов служат для идентификации сетевой часть адреса (как вы полмните, в адресах класса А первый октет служит для обозначения сети, а остальные три - для обозначения узлов). Поскольку можно использовать только семь битов, максимально возможное количество сетей - 128. Номера сетей 000 и 127 зарезервированы для использования программным обеспечением, поэтому это число уменьшается до 126 (001 - 126). Для обозначения узлов можно использовать 24 бита, поэтому для каждой из этих сетей максимальное число узлов составляет 16 777 216.

У адресов класса B первый бит всегда устанавливается в 1, а второй в 0. Поскольку для обозначения сетей здесь используются два октета, то для каждого сетевого сегмента остается, таким образом, 14 битов. Следовательно, максимально возможное число адресов этого класса - 16 384, в диапазоне от 128.001 до 191.254 (номера 000 и 255 зарезервированы).

В адресах класса C первые два бита всегда равны 1, а третий установлен в 0. В этих адресах для обозначения сетей используются первые три октета, следовательно, остается 21 бит. Диапазон возможных номеров сетей - от 192.001.001 до 223.254.254, или 2 097 152 сегмента. При этом, однако, для обозначения узлов остается только один октет, поэтому в каждом сегменте может быть всего 254 устройства.

В таблице 1 приведены характеристики адресов сетей различных классов. Адреса класса D предназначены для широковещательной рассылки пакетов сразу группе машин. Адреса класса E пока не используются. Предполагается, что со временем они будут задействованы с целью расширения стандарта.

Таблица 1. Характеристика классов IP-адресов

Класс сети	**Байт 1**	**Байт 2**	**Байт 3**	**Байт 4**
A	0	Номер сети	Номер хоста	
B	10	Номер сети	Номер хоста	
C	110	Номер сети		Номер хоста
D	1110			
E	11110			

Среди IP-адресов несколько зарезервировано под специальные случаи использования (табл. 2). Так, значение первого октета 127 зарезервировано для служебных целей, в основном, для тестирования сетевого оборудования, поскольку IP-пакеты, направленные на такой адрес, не передаются в сеть, а ретранслируются обратно управляющей надстройке сетевого программного обеспечения как только что принятые.

Таблица 2. Значение выделенных IP-адресов

IP-адрес	**Значение**
0.0.0.0	Данный компьютер
Номер сети.0	Данная IP-сеть
0.0.0.Номер узла	Узел в данной локальной сети
255.255.255.255	Все узлы в данной локальной сети
Номер сети.255	Все узлы указанной IP-сети

Централизованным распределением IP-адресов занимаются государственные организации. В США - Стенфордский международный научно-исследовательский институт (Stanford Research Institute), расположенный в г. Мэнло-Парк, штат Калифорния. Услуга по присвоению новой локальной сети IP-адресов бесплатная, и занимает она приблизительно неделю.

В небольших локальных сетях, использующих стек TCP/IP, можно назначать IP-адреса компьютерам произвольно - в том случае, если данные компьютеры не имеют непосредственного (прямого) выхода в Internet

Протокол динамической конфигурации узла (DHCP).

DHCP (Dynamic Host Configuration Protocol) - протокол динамической конфигурации хоста.

DHCP является расширением и дополнением протокола BOOTP, который предназначен для выдачи IP-адресов бездисковым машинам.

Используется транспортный протокол **UDP**.

DHCP построен по схеме клиент-сервер.

Сервер должен отвечать на пакеты с IP-адресом 255.255.255.255, т.к. клиент может не знать где находится (какая IP-сеть, какой IP-адрес у DHCP).

Порт сервера по умолчанию 67.

Порт клиента по умолчанию 68.

Механизмы выделения IP-адресов сервером DHCP:

- Динамическое присвоение - присваивает клиенту IP-адрес на ограниченное время.
- Ручное выделение - IP-адрес клиента привязывается к адресу канального уровня (MAC-адрес для Ethrnet) клиента в базе DHCP, сетевым администратором.

Основные компоненты службы:

- DHCP клиент
- DHCP сервер
- **Relay Agent** (агент пересылки) BOOTP - хост (маршрутизатор), который осуществляет связь между клиентом и сервером DHCP. В 2001г принят стандарт DHCP Relay Agent - RFC3046, и в следующей версии, наверное, будет DHCP Relay Agent вместо Relay Agent BOOTP. В старой версии (RFC0951) Relay Agent назывался **BOOTP forwarding agents**.
- **Binding** (сопряжение) - совокупность конфигурационных параметров, включая, как минимум, IP-адрес, присваиваемый DHCP-клиенту.

Протокол TCP/IP: назначение и общая характеристика.

В 1972 году группа разработчиков под руководством Винтона Серфа, которого сейчас называют “отцом Интернета”, создала семейство (стек) протоколов**TCP/IP – Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Интернета**), ставшее основой сети Интернет.

Семейство протоколов TCP/IP разделяют на четыре уровня. Каждый уровень выполняет свою задачу.

Структура семейства протоколов TCP/IP

Прикладной уровень	HTTP, FTP, Telnet, SMTP, POP3
Транспортный уровень	TCP
Сетевой уровень	IP
Канальный уровень	сетевая карта и ее драйвер

Работая в сети, мы имеем дело с протоколами прикладного уровня:

Протокол HTTP (Hypertext Transfer Protocol – Протокол передачи гипертекста) является протоколом самого верхнего уровня - уровня приложения. Он был разработан для эффективной передачи по Интернету Web-страниц, т.е. является основой системы Word Wide Web.

Протокол FTP (File Transfer Protocol – Протокол передачи файлов) определяет правила передачи файлов с одного компьютера на другой и предоставляет возможность абоненту обмениваться двоичными и текстовыми файлами с любым компьютером сети.

Telnet – с помощью этого протокола можно подключиться к удаленному компьютеру (если знать имя пользователя и пароль) и производить действия над его файлами и приложениями точно так же, как на своем собственном компьютере.

WAP (Wireless Application Protocol) был разработан в 1997 году группой компаний Ericsson, Motorola, Nokia и Phone.com для того, чтобы предоставить доступ к службам Интернета пользователям беспроводных устройств – таких как мобильные телефоны, пейджеры, электронные органайзеры и других, использующих различные стандарты связи.

SMTP, POP3, IMAP - протоколы, по которым работает e-mail.

Протоколы верхнего уровня используют TCP.

Телефонная линия - коммутация каналов. (Когда звоним, занимаем линию)

Пакетная коммутация: - почтовое ведомство. Вся пересылаемая информация разбивается на так называемые пакеты (как письмо в конверте). Каждому пакету присваивается адрес получателя (как адрес на письме). Пакеты от разных отправителей последовательно друг за другом могут передаваться по одному каналу связи, достигая нужного адресата. Таким образом, несколько систем могут работать одновременно, используя один канал связи. (Если хотим отправить одно письмо, для этого не нужно специально арендовать самолет)

Протокол TCP отвечает за

- правильность разбиения сообщений на пакеты информации
- сборку пакетов в конечном пункте в соответствии с их номерами. Если какой-либо из пакетов утерян или поврежден (передан с ошибками), то его передачу повторяют.

Пример: Нужно отправить толстую книгу, а почта принимает только письма. Отправляем книжку по листочку, на каждом пишем адрес и номер страницы. Бросаем в почтовый ящик. Получатель должен собрать все страницы и склеить их обратно, при условии, что ни одна не пропала. Все эти задачи решает протокол TCP.

Протокол IP отвечает непосредственно за передачу данных по сети и адресацию, т.е. за правильность доставки сообщений по указанному адресу. Иногда пакеты одного сообщения могут доставляться разными путями.

Пример: почта – IP играет роль конверта.

В каждом IP-пакете указывается адрес отправителя и адрес получателя. Маршрутизатор автоматически определяет маршрут передачи пакета и передает

следующему маршрутизатору. Пакет передается маршрутизаторами от одного к другому, пока не достигнет сети, в которой расположен компьютер, которому адресован пакет. Маршрутизатор этой сети определяет, какой рабочей станции адресован пакет. Все пакеты доставляются на эту рабочую станцию и из них собирается сообщение

Принципы объединения сетей на основе протоколов сетевого уровня.

Для объединения нескольких сетей в единую систему, способную передавать данные между любыми узлами объединенной сети, служит сетевой уровень.

На сетевом уровне вычислительной сетью будем называть совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типов топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Компонентами составной сети могут являться как локальные, так и глобальные сети.

Основная идея введения сетевого уровня состоит в том, чтобы оставить технологии, используемые в объединяемых сетях в неизменном в виде, но добавить в кадры всех сетей дополнительную информацию - заголовок сетевого уровня, который позволил бы находить на основании этой информации адресата в сети любого типа. Заголовок пакета сетевого уровня имеет унифицированный формат, не зависящий от форматов кадров канального уровня тех сетей, которые могут входить в интерсеть.

Внутри сети доставка данных обеспечивается канальным уровнем, а доставкой данных между сетями занимается сетевой уровень. Он выбирает правильный маршрут передачи, чтобы данные достигли нужной сети. Сети соединяются между собой маршрутизаторами. Сообщения сетевого уровня называют пакетами.

В функции сетевого уровня входит:

- передача пакетов между конечными узлами в составных сетях;
- выбор маршрута передачи пакетов, наилучшего по некоторому критерию;
- согласование разных протоколов канального уровня, использующихся в смежных подсетях.

На сетевом уровне необходима собственная система адресации, не зависящая от способов адресации узлов в отдельных подсетях.

Сетевой адрес формируется как пара: номер сети (подсети) и номера узла.

Основным полем заголовка пакета на сетевом уровне является номер сети – адресата. Благодаря нумерации подсетей сетевой уровень может составлять точную карту межсетевых связей и выбирать рациональные маршруты.

Организация межсетевого взаимодействия. Протоколы маршрутизации.

Важнейшей задачей сетевого уровня является маршрутизация – организация доставки пакетов по назначению.

Рассмотрим принципы маршрутизации на примере составной сети, изображенной на рис.1.

Маршрутизаторы имеют по несколько портов (не менее двух), к которым присоединяются сети. Каждый порт маршрутизатора можно рассматривать как отдельный узел сети: он имеет собственный сетевой адрес и собственный локальный адрес в той подсети, которая к нему подключена. Например, маршрутизатор номер 1 имеет три порта:

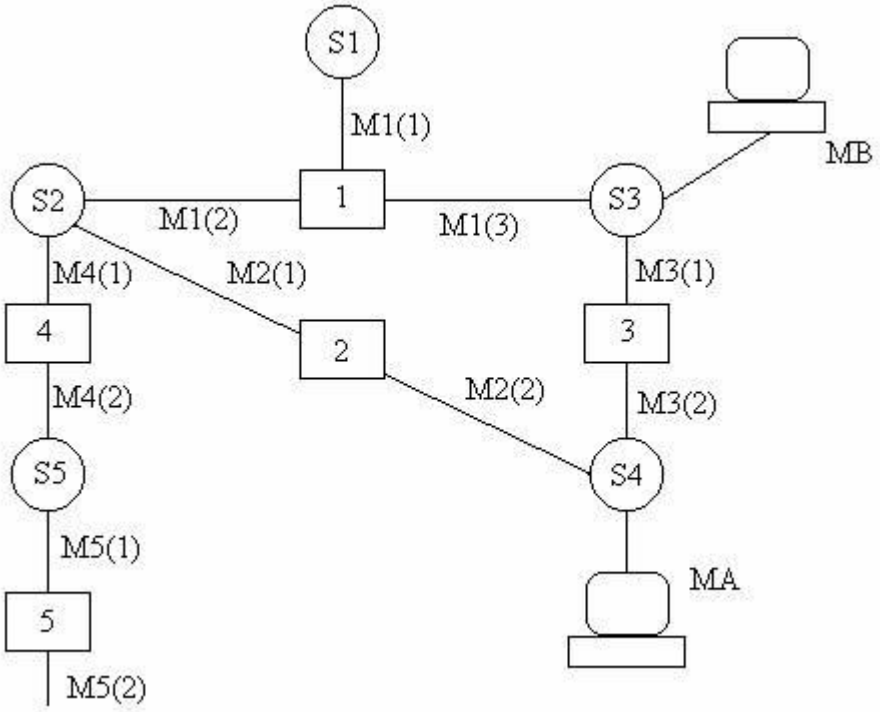
S1, S2, S3 – сети, подключенные к портам;

M1(1), M1(2), M1(3) – сетевые адреса этих портов;

Порт M1(1) имеет локальный адрес в сети S1;

Порт M1(2) имеет локальный адрес в сети S2;

Порт M1(3) имеет локальный адрес в сети S3;



S1, S2, … S5 – номера сетей, соединенных маршрутизаторами.

Рис. 1. Принцип маршрутизация в составной сети

Маршрутизатор можно рассматривать как совокупность нескольких узлов, каждый из которых входит в свою сеть. Как единое устройство маршрутизатор не имеет отдельного сетевого или локального адреса.

Маршрут – это последовательность марщрутизаторов, которые должен пройти пакет. В сложных сетях обычно существует несколько альтернативных маршрутов.

Каждый маршрутизатор выбирает маршрут дальнейшего следования пакета. Для этого он использует таблицу маршрутизации и указанный критерий выбора маршрута.

Табл.1 иллюстрирует пример таблицы маршрутизации для маршрутизатора 4.

Табл. 1. Таблица маршрутизации маршрутизатора 4.

Номер сети	Адрес следующего маршрутизатора	Адрес выходного порта	Расстояние до сети
S1	M1(2)	M4(1)	1
S2	-	M4(1)	0 (подс.)
S3	M1(2)	M4(1)	1
S4	M2(1)	M4(1)	1
S5	-	M4(2)	0 (подс.)
Умолчание	M5(1)	M4(2)	-

Описание таблицы маршрутизации по столбцам слева направо:

· номер сети назначения;

· сетевой адрес следующего маршрутизатора (то есть адрес соответствующего порта следующего маршрутизатора), на который следует направить пакет, чтобы тот передавался по направлению к сети с данным номером по рациональному маршруту;

· сетевой адрес выходного порта – на какой из собственных портов маршрутизатор должен направить пакет;

· расстояние до сети назначения – используется, если в таблице маршрутизации есть несколько строк, соответствующих некоторому адресу сети назначения.

Под расстоянием понимается значение, определенное при некоторой метрике и используемое в соответствии с заданным в сетевом пакете критерием. Этот критерий иногда называют классом сервиса. Расстояние может измеряться хопами (скачками), временем прохождения пакета по линиям связи, характеристикой надежности связи на данном маршруте и т. п.

Если марщрутизатор поддерживает несколько классов сервиса пакетов, то таблица маршрутов составляется и применяется отдельно для каждого вида сервиса (критерия).

Если таблица маршрутизации в случае кркпной сети имеет слишком большой объем, то для сокращения числа записей в таблице используют специальную запись «маршрутизатор по умолчанию» (default). Маршрутизаторы в этом случае хранят строки для соседних сетей. Обо всех остальных сетях в таблице делают одну запись, указывающую на маршрутизатор, через который пролегает путь ко всем остальным сетям. В нашем примере таким маршрутизатором для четвертого маршрутизатора является маршрутизатор 5 (порт М5(1)).То есть путь ко всем остальным сетям большой сети проходит через этот порт маршрутизатора.

Таблица маршрутизации строят также и для конечных узлов. Особенности таблиц маршрутизации на конечных узлах:

– они аналогичны по структуре таблицам, хранящимся в маршрутизаторах;

– используются для оределения того, направляется ли пакет в другую сеть или он адресован какому-либо узлу данной сети;

– эти таблицы маршрутизации чаще строятся вручную.

Табл. 2 содержит пример таблицы маршрутизации для узла А.

Табл2. Таблица маршрутизации конечного узла А.

Номер сети	Адрес следующего маршрутизатора	Адрес выходного порта	Расстояние до сети
S4	-	MA	0
S3	M3(2)	MA	1
Умолчание	M2(2)	MA	-

Протоколы и алгоритмы маршрутизации

Цель маршрутизации – доставка пакетов по назначению с максимизацией эффективности. Маршрут выбирается на основании имеющейся у маршрутизаторов информации о конфигурации (топологии) сети, длин очередей в узлах коммутации, интенсивности входных потоков и других факторов, а также на основании заданного критерия выбора маршрута.

Алгоритмы маршрутизации включают процедуры:

– измерение и оценивание параметров сети;

- принятие решения о рассылке служебной информации;
- построение таблиц маршрутизации;
- реализация принятых маршрутных решений.

Таблицы маршрутизации создаются в основном автоматически, но могут корректироваться и дополняться вручную. Для автоматического построения таблиц маршрутизаторы обмениваются информацией о связях в сети. При этом используются специальные служебные протоколы, называемые протоколами маршрутизации. Протоколы маршрутизации помещают свои служебные пакеты в поле данных пакетов сетевого или транспортного уровня, то есть используют соответствующие протоколы для транспортировки своих сообщений. Формально эти протоколы можно отнести к более высокому уровню, чем сетевой.

Объединение подсетей для создания более сложной (неоднородной) сети можно осуществлять и средствами канального уровня. Для этого могут быть использованы некоторые типы мостов и коммутаторов. Однако применение средств канального уровня для создания сложных сетей имеет существенные ограничения и недостатки. В табл. 3. проводится сравнение маршрутизаторов и коммутаторов (мостов) с точки зрения их применения для объединения подсетей.

Протокол Frame Relay: назначение и общая характеристика.

Frame Relay - это более современная концепция коммутации пакетов, разработанная для увеличения пропускной способности и сведения к минимуму коммуникационных расходов путем упрощения сетевой обработки. Frame Relay, в частности, подходит для приложений, в которых оборудование конечного пользователя является интеллектуальным (например, рабочие станции или мосты для взаимодействия локальных сетей), а линии передачи отличаются высоким качеством. Концепция сети Frame Relay сходна с X.25, но благодаря снижению протокольной обработки в каждом узле сети общая сквозная задержка уменьшается. Вся процедура детектирования ошибок и восстановления данных выполняются оборудованием конечного пользователя. Управление потоком данных также осуществляется в конечных точках (хотя сеть при необходимости и выдает сигналы о перегрузке). Упрощение работы сети в случае Frame Relay приводит к более эффективному использованию каналов связи и увеличению пропускной способности сети. Frame Relay использует только первых два уровня модели OSI. В рекомендации ITU I.122 1988 года был включен протокол Frame Relay, а затем аналогичный стандарт был выпущен и Американским национальным институтом стандартов ANSI.

Объединение компьютерных сетей: принципы, маршрутизация.

Принципы объединения сетей

Современные вычислительные сети часто строятся с использованием нескольких различных базовых технологий - Ethernet, Token Ring или FDDI. Такая неоднородность возникает либо при объединении уже существовавших ранее сетей, использующих в своих транспортных подсистемах различные протоколы канального уровня, либо при переходе к новым технологиям.

Когда две или более сетей организуют совместную транспортную службу, то такой режим взаимодействия обычно называют *межсетевым взаимодействием* (internetworking). Для обозначения составной сети в англоязычной литературе часто также используется термин *интерсеть* (internetwork или internet).

Для образования единой транспортной системы, объединяющей несколько сетей с различными принципами передачи информации между конечными узлами, служит

сетевой уровень. Сетевой уровень позволяет передавать данные между любыми, произвольно связанными узлами сети. Таким образом, объединение различных компьютерных сетей основано на использовании протоколов сетевого уровня.

Протоколы канального уровня не позволяют строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами. Сетевой уровень вводится для того, чтобы, с одной стороны, сохранить простоту процедур передачи пакетов для типовых топологий, а с другой стороны, допустить использования произвольных топологий.

Основная идея введения сетевого уровня состоит в том, чтобы оставить технологии, используемые в объединяемых сетях, в неизменном виде, но добавить в кадры канального уровня дополнительную информацию - заголовок сетевого уровня, на основании которого можно было бы находить адресата в сети с любой базовой технологией. Заголовок пакета сетевого уровня имеет унифицированный формат, не зависящий от форматов кадров канального уровня тех сетей, которые могут входить в объединенную сеть.

Заголовок сетевого уровня должен содержать адрес назначения и другую информацию, необходимую для успешного перехода пакета из одной сети в другую сеть (см. лекцию 16). К такой информации может относиться, например:

- номер фрагмента пакета, нужный для успешного проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами кадров канального уровня;
- время жизни пакета, указывающее, как долго от путешествует по интерсети, это время может использоваться для уничтожения "заблудившихся" пакетов;
- информация о наличии и о состоянии связей между сетями, помогающая узлам сети и маршрутизаторам рационально выбирать межсетевые маршруты;
- информация о загруженности сетей, также помогающая согласовать темп посылки пакетов в сеть конечными узлами с реальными возможностями линий связи на пути следования пакетов;
- качество сервиса - критерий выбора маршрута при межсетевых передачах - например, узел-отправитель может потребовать передать пакет с максимальной надежностью, возможно, в ущерб времени доставки.

В качестве адресов отправителя и получателя в составной сети используется не MAC-адрес, а IP-адрес, содержащий информацию о номере сети и номере компьютера в данной сети. В канальных протоколах поле "номер сети" отсутствует - предполагается, что все узлы принадлежат одной сети. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты при любой их топологии, используя альтернативные маршруты, если они имеются, что не умеют делать мосты.

Таким образом, внутри сети доставка сообщений регулируется канальным уровнем. А доставкой пакетов между сетями занимается сетевой уровень.

Маршрутизация

Основные понятия

Реализация протокола сетевого уровня подразумевает наличие в сети специального устройства - *маршрутизатора* (см. лекцию 10). Маршрутизаторы объединяют отдельные

сети в общую составную сеть. К каждому маршрутизатору могут быть присоединены несколько сетей (по крайней мере, две).

Уточним, что понимается под термином ***сеть*** в протоколах сетевого уровня:

Сеть -

совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи пакетов общую базовую сетевую технологию. Внутри сети сегменты не разделяются маршрутизаторами, иначе это была бы не одна сеть, а несколько сетей. Маршрутизатор соединяет несколько сетей в интерсеть (составную сеть).

В сложных составных сетях всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Задачу выбора маршрутов из нескольких возможных решают маршрутизаторы, а также конечные узлы.

Маршрут -

это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения.

Маршрутизатор выбирает маршрут на основании своего представления о текущей конфигурации сети и соответствующего критерия выбора маршрута. Обычно в качестве критерия выступает время прохождения маршрута, которое в локальных сетях совпадает с длиной маршрута, измеряемой в количестве пройденных узлов маршрутизации (в глобальных сетях принимается в расчет и время передачи пакета по каждой линии связи).

Процесс прохождения пакетов с данными от одного компьютера до другого можно пронаблюдать с помощью программы ***Traceroute***. Откройте во время подключения к Сети командную строку, наберите в командной строке tracert и через пробел нужный IP-адрес, нажмите Enter.

В результате вам будет выдан путь пакетов от вашего компьютера до того, IP-адрес которого вы указали в команде tracert, а также указано время (в миллисекундах), которое потребовалось пакетам для прохождения каждого отрезка пути. Практически все IP-адреса в списке пройденных пакетом узлов принадлежат встреченным на пути маршрутизаторам. Первый адрес списка принадлежит вашему компьютеру, а последний – Интернет-ресурсу, путь к которому вы решили отследить.

В служебной информации каждого пакета с данными есть параметр ***TTL*** (***Time to Live - время жизни пакета***, см. лекцию 16, протокол ICMP). Он показывает, сколько узлов сети Интернет этот пакет еще может пройти. На каждом из узлов, через которые следует пакет, этот параметр уменьшается на единицу, и при достижении им значения 0 пакет уничтожается. Это сделано для того, чтобы пакеты не циркулировали по замкнутым цепям. Однако, если это значение слишком мало, пакет может не успеть дойти до нужного маршрутизатора. Данный параметр можно изменить в реестре Windows.

Каждый маршрутизатор ведет свою *таблицу маршрутизации* , содержащей сведения о том, к каким маршрутизаторам из числа подключенных к данному маршрутизатору следует обращаться, чтобы отправить полученный пакет на тот или иной ресурс Сети с тем или иным IP-адресом, т.е. попросту говоря, на какой из подключенных к нему кабелей эти пакеты данных отправлять. Таким образом, маршрутизатор "знает", на какой порт отправить принятый пакет.

Таблица маршрутизации -

база данных, в которой указаны группы сетей и порты маршрутизатора, к которым они подключены.

Маршрутизатор распределяет приходящие к нему пакеты данных исключительно по своим подключениям: по тем кабелям и оптоволоконным линиям, которые подсоединены к нему самому. Т.к. в памяти остальных маршрутизаторов тоже есть соответствующие таблицы маршрутизации, т. они перенаправят данные дальше, на следующий маршрутизатор. Так будет до тех пор, пока они наконец не попадут на маршрутизатор, к которому подключен компьютер с нужным IP-адресом.

Как нетрудно понять, при подключении нового маршрутизатора с новым набором IP-адресов, ранее в Сети не присутствовавших, необходимо сообщить уже имеющимся ее участникам о появившейся новой части Интернета и показать им путь к ней. Новый маршрутизатор сообщает другим маршрутизаторам о том, к каким IP-адресам он имеет прямой доступ (*анонсирует* себя). Те, получив эту информацию, вносят ее в свои таблицы. При поступлении к ним пакета, адресованного на эти IP-адреса, они просто его пересылают на этот новый маршрутизатор. А потом процесс повторяется, остальные маршрутизаторы тоже узнают о новых IP-адресах и помещают информацию о них в свои таблицы маршрутизации, указывая в качестве направления отправки пакетов на них тот маршрутизатор, от которого они получили информацию.

Анонсирование -
сообщение маршрутизатором другим маршрутизаторам сведений о диапазоне IP-адресов сетей, которыми они "заведуют".

Так информация о новой части Сети постепенно расходится по маршрутизаторам. В настоящее время в сети Интернет для того, чтобы самые отдаленные ее уголки узнали о новоподключенных ресурсах, требуется 2-3 часа. В принципе, пока маршрутизатор отдельной сети, подключенной к Интернету, не получит данные о них (т.е. информацию о том, что эти ресурсы существуют, и о том, какие у них IP-адреса), с компьютеров этой сети доступ к новым ресурсам будет невозможен, несмотря на то, что физически соединение этих ресурсов с сетью Интернет уже будет реализовано.

Процесс анонсирования маршрутизаторов, т.е. оповещения своих «коллег» об IP-адресах, которыми они «заведуют», происходит не только при первом подключении маршрутизатора к Сети. Он совершается постоянно, ведь IP-адреса могут изыматься у одной сети и передаваться другой, меду маршрутизаторами может устанавливаться новое соединение для более быстрого обмена данными. Так что каждый маршрутизатор постоянно сообщает своему окружению о «подведомственной» ему «территории», а остальные отслеживают изменения этой информации.

Взаимодействие маршрутизаторов осуществляется по протоколам маршрутизации (см. лекцию 16) RIP (Routing Information Protocol) и OSPF (Open Shortest Path First).

Маршрутизаторы разных сетей соединены между собой мощными линиями связи, обычно оптоволоконными. Для того чтобы более эффективно выполнять распространение данных по Интернету, существуют «маршрутизаторы маршрутизаторов», т.е. маршрутизаторы, к которым подключаются другие маршрутизаторы, а не отдельные компьютеры (в отличие от обычных маршрутизаторов их принято именовать роутерами, несмотря на то, что слово router и означает «маршрутизатор»). Образуется как бы мегасеть из серверов-маршрутизаторов отдельных сетей университетов, фирм, предприятий и провайдеров с роутером во главе. Роутеры тоже соединены между собой кабелями, образу паутинообразную структуру соединений.

Поскольку Сеть благодаря соединениям меду маршрутизаторами имеет паутинообразную структуру, очень часты случаи, когда какой-нибудь маршрутизатор получает описанным выше способом информацию о нескольких возможных путях доступа к какому-либо IP-адресу. В таком случае маршрутизатор обменивается данными с ресурсами Интернета, располагающимися по этим IP-адресам, и высчитывает, какой из обнаруженных путей наиболее быстрый и надежный. Именно такой путь и используется. Подобная проверка проводится регулярно, тем самым в зависимости от состояния Сети оптимальный путь между двумя ее ресурсами может меняться.

Организация виртуальных каналов информационного обмена.

Сети X.25

Рекомендация ITU-T X.25 имеет название: Interface between DTE and DCE for terminals operating in the packet mode and connected to public data networks by dedicated circuit.

Принципы построения и компоненты сети X.25

Главной особенностью сети X.25 является использование аппарата **виртуальных каналов** для обеспечения информационного взаимодействия между компонентами сети. *Виртуальные каналы предназначены для организации вызова и непосредственной передачи данных между абонентами сети.* Информационный обмен в сети X.25 во многом похож на аналогичный процесс в сетях ISDN и состоит из трех обязательных фаз:

- Установление вызова (виртуального канала)
- Информационный обмен по виртуальному каналу
- Разрывание вызова (виртуального канала)

Информационное взаимодействие в сети X.25 осуществляется на физическом, канальном и сетевом уровнях. На физическом уровне могут быть использованы любые универсальные или специализированные интерфейсы. Компонентами сети являются устройства трех основных категорий:

- **Устройства DTE** (Data Terminal Equipment)
- **Устройства DCE** (Data Circuit-Terminating Equipment)
- **Устройства PSE** (Packet Switching Exchange)

Устройство PAD (packet assembler/ disassembler) является специфическим устройством сети X.25. PAD предназначен для обеспечения взаимодействия неспециализированных терминалов с сетью , для преобразования потока символов, который поступает от неспециализированного терминала в пакеты X.25 и выполнения обратного преобразования.

Взаимодействие на канальном уровне сети X.25

Протоколы канального уровня HDLC/SDLC, были разработаны для того, чтобы решать следующие задачи:

- Обеспечение передачи сообщений, которые могут содержать любое количество бит и любые возможные комбинации бит - требование кодовой прозрачности.
- При передаче потока бит должны выполняться процедуры, которые позволяют обнаружить ошибки на приемной стороне.

- Возникновение ошибки при передаче не должно приводить к потере или дублированию компонентов сообщения, т.е. к его искажению.
- Протокол канального уровня должен был обеспечивать работу как двухточечных, так и многоточечных физических цепей
- Протокол должен обеспечивать подключение дуплексных и полудуплексных линий
- Протокол должен обеспечивать информационный обмен при значительных вариациях времени распространения сигнала

Протоколы семейства HDLC

Протоколы осуществляют передачу данных в виде кадров переменной длины. Начало и конец кадра помечается специальной последовательностью битов, которая называется **флагом**. Для обеспечения дисциплины управления процессом передачи данных, одна из станций, которые обеспечивают информационный обмен, может быть обозначена, как **первичная**, а другая (или другие) станции могут быть обозначены, как **вторичные**. *Кадр, который посылает первичная станция, называется **командой** (command). Кадр, который формирует и передает вторичная станция, называется **ответ** (response).*

Режимы организации взаимодействия на канальном уровне

Вторичная станция сегмента может работать в двух режимах: режиме **нормального ответа** или в режиме **асинхронного ответа**. Вторичния станция, которая находится в режиме нормального ответа, начинает передачу данных только в том случае, если она получила разрешающую команду от первичной станции. Вторичная станция, которая находится в режиме асинхронного ответа, может по своей инициативе начать передачу кадра или группы кадров. Станции, которые сочетают в себе функции первичных и вторичных станций и называются**комбинированными**.Симметричный режим взаимодействия комбинированных станций называется **сбалансированным режимом.**

Процедура LAPB

Процедура **LAPB** (Link Access Procedure Balanced) используется в сетях X.25 в качестве протокола канального уровня.

Флаг

Протокол LAPB использует в качестве флага комбинацию из 8 бит, которая состоит из 6-ти единиц и двух нулей, которые обрамляют эту последовательность спереди и сзади (01111110). Процесс приема кадра завершается при получении следующего флага. В том случае, если к моменту получения завершающего флага приемник получил менее 32 бит, принятый кадр считается ошибочным и уничтожается. Для предотвращения появления флаговой комбинации в теле кадра используется специальная процедура.

Структура кадра LAPB

Рекомендация X.25 определяет два основных типа процедуры LAPB - **основной** тип (modulo 8, basic) и **расширенный** тип (modulo 128, extended). Эти режимы отличаются разрядностью счетчиков, которые используются для управления потоком кадров. Кадр протокола LAPB содержит 4 поля: **ADRESS, CONROL, Data, FCS**. Поле DATA в кадре LAPB может отсутствовать.

Поле ADRESS

Поле ADRESS занимает в кадре один байт. В этом поле располагается бит признака C/R (Command /Response) В поле ADDRESS кадра управляющей команды размещается физический адрес принимающей станции. В поле ADRESS кадра ответа на команду размещается физический адрес передающей станции.

Поле CONTROL

Содержимое этого поля поля определяет тип кадра.

- **Информационные кадры** (Information Frames, I-кадры). В битах поля CONTROL размещаются 3-х разрядный номер передаваемого кадра и 3-х разрядный номер кадра, который ожидается для приема для обеспечения управления потоком.
- **Управляющие кадры** (Supervisory Frames, S-кадры). В поле CONTROL размещается 3-х разрядный номер информационного кадра, который ожидается для приема и два бита, которые определяют тип передаваемого управляющего кадра.

Обозначение	Тип кадра	Бит №3	Бит №4
RR	Приемник готов (Receiver Ready)	0	0
RNR	Приемник не готов (Receiver Not Ready)	1	0
REJ	Отказ/переспрос (Reject)	0	1

- Наиболее часто в процессе информационного взаимодействия используются управляющие кадры типа **RR**. Кадры данного типа передает получатель данных для того, чтобы обозначить готовность к приему очередного кадра, в том случае, когда он сам не имеет информации для передачи. Кадры **RNR** используются устройствами DCE и DTE для того, чтобы сообщить абоненту о возникновении аварийной ситуации, в которой дальнейший прием информационных кадров невозможен. Кадры REJ используются устройствами DCE и DTE для того, чтобы сигнализировать абоненту о разрешении аварийной ситуации, в которой был невозможен прием информационных кадров. Кадр REJ передается после кадра RNR и подтверждает факт перехода линии в нормальный режим работы.
- **Ненумерованные кадры** (Unnumbered Frames, U - кадры). Предназначены для организации и разрывания логического соединения, согласования параметров линии и формирования сигналов о возникновении неустранимых ошибок в процессе передачи данных I-кадрами.

Обозначение	Тип	Признак
SABM(E)	Set Asynchronous Balanced Mode	Команда
DISC	Disconnect	Команда
DM	Disconnect Mode	Ответ
UA	Unnumbered Acknowledgement	Ответ
FRMR	Frame Reject	Ответ

- Кадр **FRMR** передается вторичной станцией для того, чтобы указать на возникновение аварийной ситуации, которая не может быть разрешена путем повторной передачи аварийного кадра.

Сетевой уровень X.25

Для передачи по сети пакеты X.25 инкапсулируются в кадры LAPB. Протокол LAPB обеспечивает надежную доставку этих пакетов по каналу, который связывает один компонент сети с другим. Один физический канал в сети X.25 может быть использован для того, чтобы передавать пакеты которые относятся к нескольким различным процессам сетевого уровня. В отличие от принципа статического временного разделения, который используется в сетях ISDN, в сети X.25 для распределения канальных ресурсов используется принцип динамического разделения.

Виртуальные каналы X.25

Процесс сетевого уровня получает в свое распоряжение часть полосы пропускания физического канала в виде виртуального канала. Полная полоса пропускания канала делится в равных пропорциях между виртуальными каналами, которые активны в текущий момент. В сети X.25 существует два типа виртуальных каналов: **коммутируемые** (SVC) и **постоянные** (PVC).

Формат пакета X.25

Пакет X.25 состоит как минимум из трех байтов, которые определяют заголовок пакета. Первый байт содержит 4 бит **идентификатора общего формата** и 4 бита **номера группы логического канала**. Второй байт содержит **номер логического канала**, а третий — **идентификатор типа пакета**. Пакеты в сети бывают двух типов — **управляющие пакеты и пакеты данных**. Тип пакета определяется значением младшего бита идентификатора типа пакета.

Идентификатор общего формата

Поле идентификатора общего формата содержит признак, который устанавливает тип процедуры управления потоком пакетов (modulo 8 или modulo 128).

Номер логического канала

Номер логического канала задается содержимым двух полей — номер группы логического канала от 0 до 15 и номер канала в группе от 0 до 255. Таким образом, максимальное число логических каналов может достигать значения 4095. Номер логического канала определяет виртуальный порт, с которым ассоциируется конкретный пользовательский процесс.

Идентификатор типа пакета

DCE ⇢ DTE	DTE ⇢ DCE	Код (16)
Incoming Call	Call Request	0B
Call Connected	Call Accepted	0F
Clear Indication	Clear Request	13
Clear Confirmation	Clear Confirmation	17

DCE ⇢ DTE	DTE ⇢ DCE	Код (16)
Interrupt	Interrupt	23
Interrupt Confirmation	Interrupt Confirmation	27
Receiver Ready (RR)	Receiver Ready (RR)	X1
Receiver Not Ready (RNR)	Receiver Not Ready (RNR)	X5
—	Reject (REJ)	X9

Сетевые адреса получателя и отправителя пакета размещаются в поле "данные", и предназначены для управления вызовами.

Формат сетевого адреса X.25

Сетевой адрес состоит из двух частей

- Data Network ID Code (DNIC)
- Network Terminal Number

Поле DNIC содержит 4 десятичных цифры и определяет код страны и номер провайдера. Содержимое поля Network Terminal Number содержит 10 или 11 десятичных цифр, которые определяет провайдер и предназначено для определения конкретного пользователя.

Управление потоком кадров

Для управления потоком пакетов на сетевом уровне X.25 используются такие же процедуры и механизмы, какие используются для управления потоком кадров на канальном уровне сети X.25.

Протоколы распределенных файловых систем (FTP, HTTP).

Протокол FTP

File Transfer Protocol - протокол передачи файлов, протокол высокого уровня (а именно, уровня приложений).
. Используется службой FTP для передачи файлов.

Первый стандарт - RFC114 (File Transfer Protocol A.K. Bhushan Apr-10-1971).

Последняя версия - RFC959 (File Transfer Protocol J. Postel, J.K. Reynolds Oct-01-1985).

FTP отличается от других приложений тем, что он использует два TCP соединения для передачи файла.

1. Управляющее соединение - соединение для посылки команд серверу и получение ответов от него. Для канала управления используется протокол Telnet.

2. Соединение данных - соединение для передачи файлов.

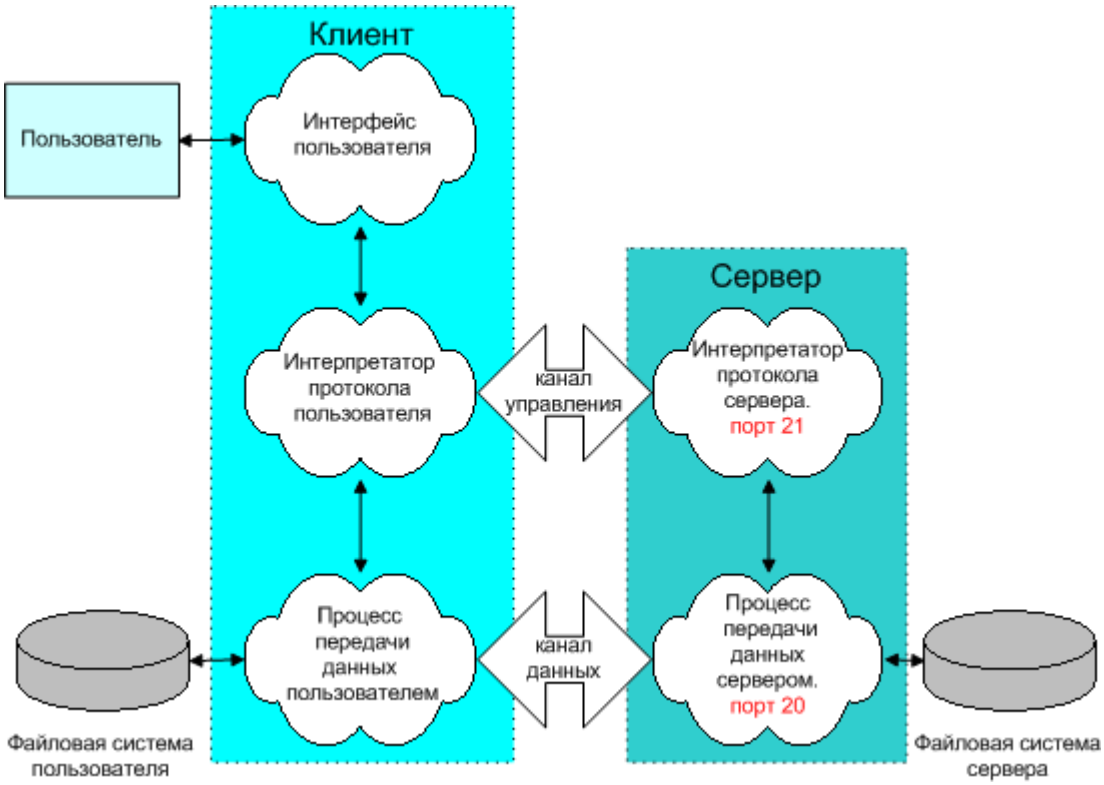


Схема двух каналов соединения по протоколу FTP

В старых версиях для передачи данных использовался только 20-й порт (**активный режим**), в современных версиях FTP-серверов порт для канала данных может назначаться сервером из нестандартных (N > 1024) портов (**пассивный режим**).

Протокол FTP определяет запрос-ответный способ взаимодействия между программой-клиентом и программой-сервером.

Работа FTP на пользовательском уровне содержит несколько этапов:

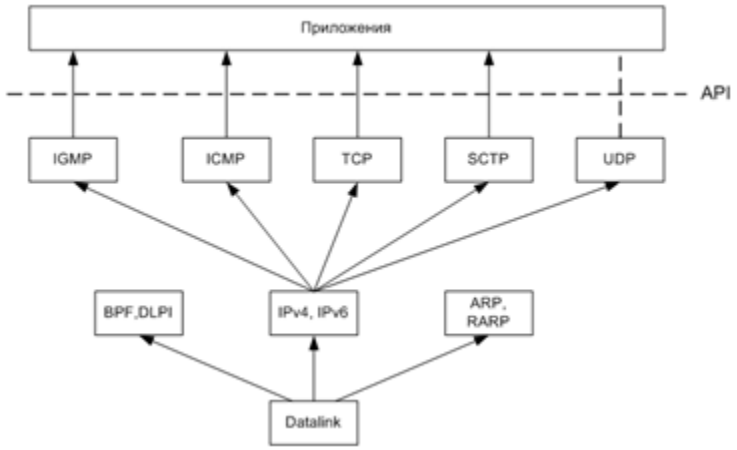
1. Идентификация (ввод имени и пароля).
2. Выбор каталога.
3. Определение режима обмена (поблочный, поточный, ascii или двоичный).
4. Выполнение команд обмена (get, mget, dir, mdel, mput или put).
5. Завершение процедуры (quit или close).

Протокол HTTP

Языки и средства создания Web-приложений.

Протокол HTTP (HyperText Transfer Protocol — протокол передачи гипертекста) был разработан как основа World Wide Web. Все нюансы протокола описаны в RFC (для версии 1.0 — RFC 1945). Работа по протоколу HTTP происходит следующим образом: программа-клиент устанавливает TCP-соединение с сервером (стандартный номер порта-80) и выдает ему HTTP-запрос. Сервер обрабатывает этот запрос и выдает HTTP-ответ клиенту. Структура HTTP-запроса. HTTP-запрос состоит из заголовка запроса и тела запроса, разделенных пустой строкой. Тело запроса может отсутствовать. Заголовок

запроса состоит из главной (первой) строки запроса и последующих строк, уточняющих запрос в главной строке. Последующие строки также могут отсутствовать. Запрос в главной строке состоит из трех частей, разделенных пробелами – метода запроса, строки запроса (части URL без имени сервера), и метки – версии протокола (например HTTP/1.0 или HTTP/1.1) Пример: GET /test/file.html HTTP/1.0



Метод (иначе говоря, команда HTTP): GET — запрос документа. Наиболее часто употребляемый метод. Параметры запроса передаются через URL. HEAD — запрос заголовка документа. Отличается от GET тем, что выдается только заголовок запроса с информацией о документе. Сам документ не выдается. POST — запрос документа. Также часто употребляемый метод. Параметры запроса передаются через тело запроса. Также существуют методы: PUT, DELETE, LINK, UNLINK, но практически не используются.

Протокол передачи гипертекста HTTP является протоколом прикладного уровня для распределенных информационных систем. Это объектно-ориентированный протокол, пригодный для решения многих задач, таких как создание серверов имен, распределенных объектно-ориентированных управляющих систем и др. Структура HTTP позволяет создавать системы, независящие от передаваемой информации.

Первые версии, такие как HTTP/0.9, представляли собой простые протоколы для передачи данных через Интернет. Версия HTTP/1.0, улучшила протокол, разрешив использование сообщений в формате MIME, содержащих метаинформацию о передаваемых данных, и модификаторы для запросов/откликов.

HTTP используется также в качестве базового протокола для коммуникации пользовательских агентов с прокси-серверами и другими системами Интернет, в том числе и использующие протоколы SMTP, NNTP, FTP, Gopher и Whois. Последнее обстоятельство способствует интегрированию различных служб Интернет. HTML (Hyper Text Mark-up Language) является общемировым языком для создания WWW-страниц (web-страниц). HTML-файл представляет собой текстовый файл, в котором записаны команды языка HTML. Команды, которые составляют язык, называются тэгами. Тэги заключаются в угловые скобки. Все, что находится вне угловых скобок, является текстом, подлежащим выводу в окно браузера с теми параметрами форматирования (размер шрифта, элемент таблицы, отступы, центровка и т.п.), которые были установлены тэгами. Существует международный стандарт, полностью описывающий все возможные тэги и их допустимые сочетания. Картинки и другие нетекстовые компоненты не вставляются в документ непосредственно и хранятся отдельно. Вместо этого в текст вставляется ссылка, указывающая имя файла, содержащего картинку.

Языки и средства создания Web-приложений. ASP – Active Server Pages – технология компании Microsoft для создания серверной части web-приложений. ASP.NET – новый шаг в технологиях Microsoft – логическое продолжение ASP при использовании платформы .NET (dotNet), которая является мощным конкурентом Java. Java — это технология и язык программирования сетевых приложений, разработаные фирмой Sun Microsystems для систем распределенных вычислений. Особенности языка Java: объектно-ориентированный, прототипом является C++, но более прост в использовании (так, например, убраны указатели); введены многопотоковость (например, оператор синхронизации), дополнительная защита от вирусов. Java приложения могут работать как на стороне сервера (например JSP – Java Server Pagers) так и на стороне клиента (java-applets). PHP — язык программирования на стороне сервера, предназначен для создания динамических web-сайтов. В последнее время он получил огромную популярность в виду своей простоты. Преимуществами языка являются: простота изучения, понятный синтаксис, большое количество встроенных функций, относительно высокая скорость работы, бесплатность. Как показывает практика – хорош для небольших web-приложении, на крупных проектах (тысячи человеко/часов) показывает свою ограниченность – тут больше подходят «серьезные» технологии вроде ASP.NET или Java. PERL — это мощный язык программирования, позволяющий вам эффективно обрабатывать большие документы, активно пользоваться ресурсами сервера и осуществлять связь сайта с базами данных. ColdFusion — системы быстрой разработки web-серверных приложений от Macromedia. В настоящее время доступны версии ColdFusion для всех распространенных ОС. Эта система идеально подходит для разработки баз данных, доступ к которым осуществляется в интерактивном режиме через web-браузер.

Существует еще множество серверных и клиентских технологий применяемых при построении web-приложений.

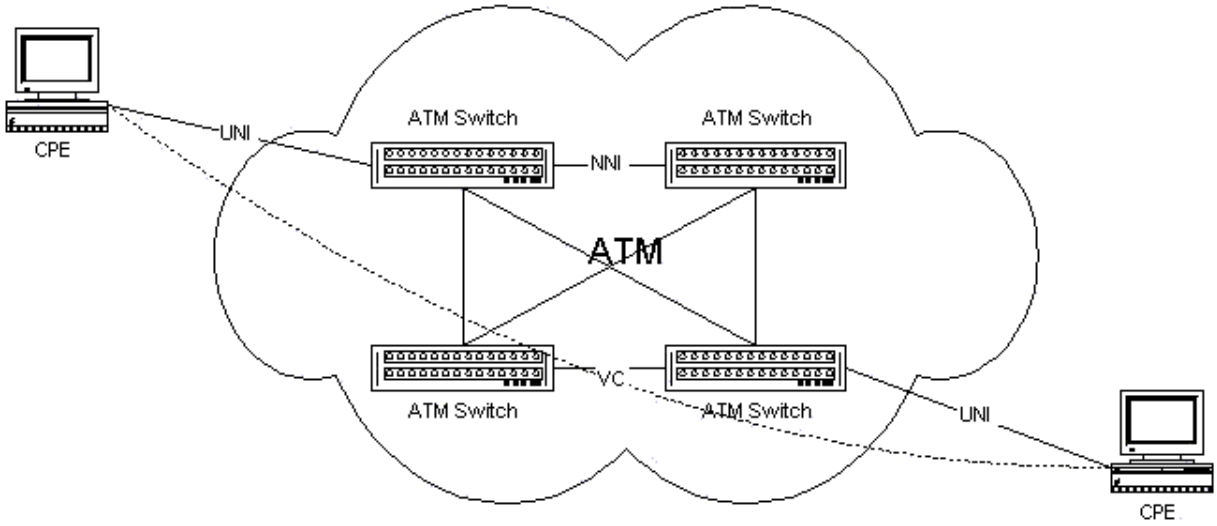
Технология ATM (Asynchronous Transfer Mode).

Технология ATM представляет собой дальнейшее развитие принципов, которые были положены в основу технологий ISDN и Frame Relay. Технологии N-ISDN, X.25 и Frame Relay не могли обеспечить возможность построения достаточно качественной и гибкой цифровой сети с интегрированными услугами Технология N-ISDN обеспечивала гарантированное качество обслуживания, однако, не обладала необходимой гибкостью и не обеспечивала высокие (более 2 Мбит/сек) скорости передачи данных. Технология Frame Relay обеспечивала большие, чем технология N-ISDN скорости передачи данных и достаточную эффективность использования ресурсов физического канала, однако, она не обеспечивала выделения гарантированной полосы пропускания для передачи трафика, который чувствителен к задержкам (оцифрованный голос), то есть необходимого качества обслуживания. Аббревиатура ATM означает Asynchronous Transfer Mode (в дословном переводе - технология асинхронной передачи). Термин "асинхронный" в названии технологии указывает на её отличие от синхронных технологий с фиксированным распределением пропускной способности канала между информационными потоками (TDM, ISDN). Существенные отличия технологии ATM от

ISDN и Frame Relay заключается в том, что блок данных ATM, **ячейка**, имеет фиксированную длину - 53 байта. Фиксированная длина ячейки ATM обеспечивает гарантированное постоянное время её обработки на коммутирующем оборудовании, и следовательно - возможность обеспечения гарантированного качества обслуживания информационных потоков пользователя.

Компоненты сетей ATM

Технология ATM обеспечивает информационное взаимодействие на двух уровнях, которые соответствуют канальному и физическому уровням модели OSI. ATM - коммутаторы представляют собой быстродействующие специализированные вычислительные устройства, которые аппаратно реализуют функцию коммутации ячеек ATM между несколькими своими портами. Устройства CPE (Customer Premises Equipment) обеспечивают адаптацию информационных потоков пользователя для передачи с использованием технологии ATM. Для передачи данных в сети ATM организуется виртуальное соединение - virtual circuit (VC).

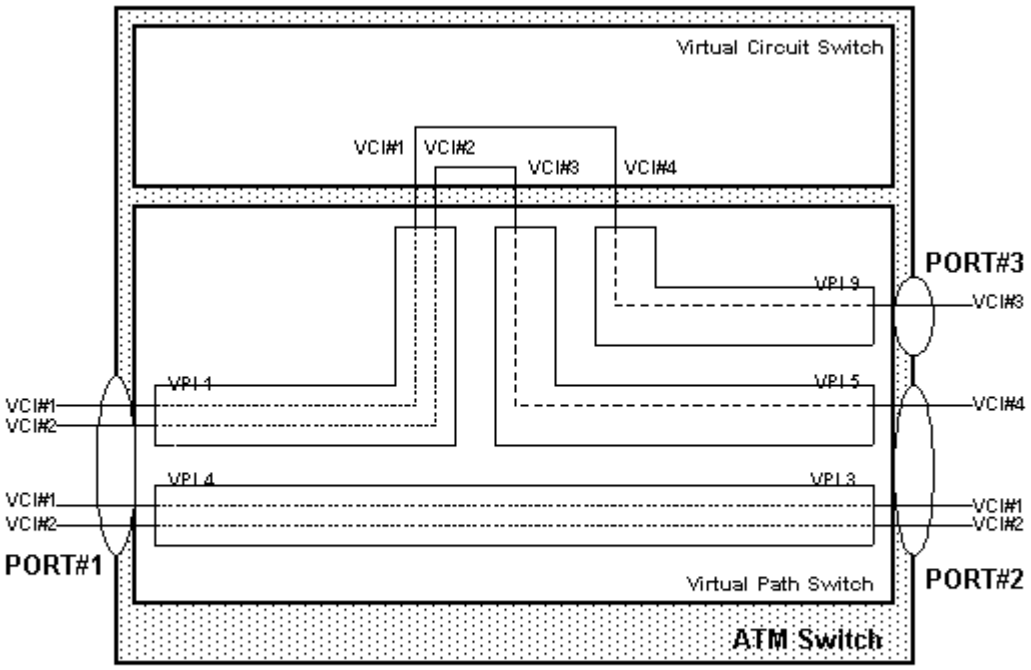


Идентификаторы виртуального соединения ATM

В пределах интерфейса NNI виртуальное соединение определяется уникальным сочетанием идентификатора виртуального пути (virtual path identifier) и идентификатора виртуального канала (virtual circuit identifier).

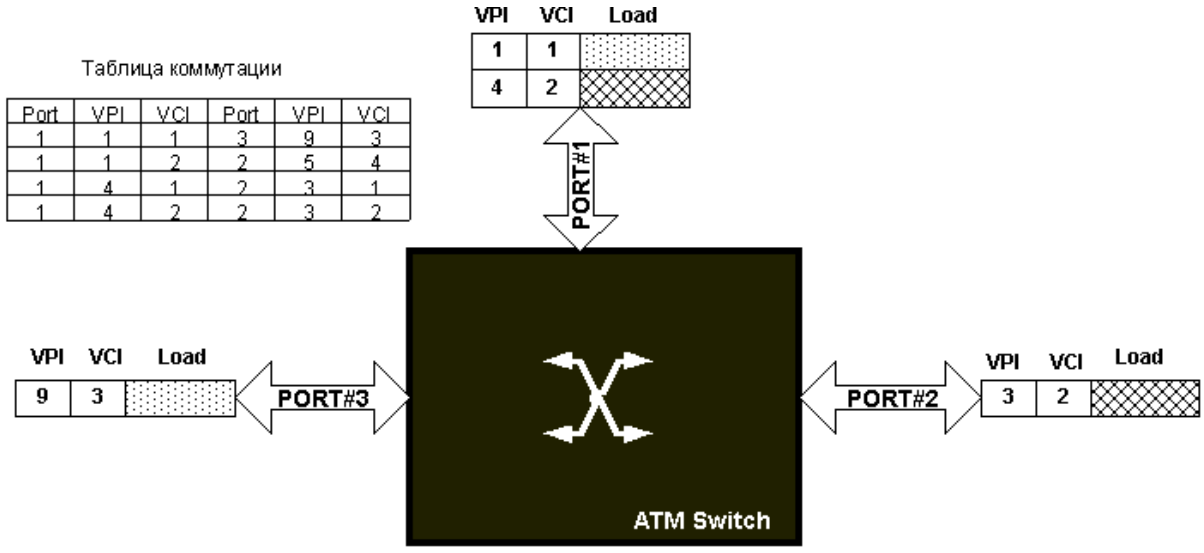
Виртуальный канал представляет собой фрагмент логического соединения, по которому производится передача данных одного пользовательского процесса.

Виртуальный путь представляет собой группу виртуальных каналов, которые в пределах данного интерфейса имеют одинаковое направление передачи данных.



Коммутатор ATM состоит из двух коммутаторов - коммутатора виртуальных путей и коммутатора виртуальных каналов. Эта особенность организации ATM обеспечивает дополнительное увеличение скорости обработки ячеек.

ATM коммутатор анализирует значения, которые имеют идентификаторы виртуального пути и виртуального канала у ячеек, которые поступают на его входной порт и направляет эти ячейки на один из выходных портов. Для определения номера выходного порта коммутатор использует динамически создаваемую таблицу коммутации.



Формат ячейки ATM

Ячейка состоит из двух частей: поле заголовка занимает 5 байт и ещё 48 байт занимает поле полезной нагрузки.

Поле заголовка

В заголовке ячейки содержатся следующие поля:

- Virtual Path Identifier (VPI)
- Virtual Ccircuit Identifier (VCI)
- Payload Type (PT)
- Congestion Loss Priority (CLP)
- Header Error Control (HEC)

Поля идентификаторов VPI и VCI

Идентификаторы VPI и VCI используются для обозначения виртуальных соединений ATM.

Поле типа нагрузки PT

В этом поле располагается информация, которая определяет тип даных, которые находятся в поле полезной нагрузки ячейки ATM.

Бит понижения приоритета CLP

Бит CLP в ячейке ATM имеет такое - же значение, как бит DE в кадре Frame Relay.

Поле контрольной суммы заголовка HEC

В поле HEC размещается проверочная контрольная сумма 4-х предыдущих байтов заголовка.

Поле Generic Flow Control (GFC)

Поле GFC содержат только ячейки ATM которые передаются через интерфейс UNI. Содержимое этого поля используется в тех случаях, когда один ATM UNI интерфейс обслуживает несколько станций одновременно.

Структуры заголовка ячейки ATM

Формат заголовка ячейки ATM UNI		
GFC	VPI	
VPI	VCI	
VCI		
VCI	PT	CLP
HEC		

Формат заголовка ячейки ATM NNI	
VPI	
VPI	VCI
VCI	

Формат заголовка ячейки ATM NNI		
VCI	PT	CLP
HEC		

Классы данных ATM

Спецификация ATM forum 4.0 определяет пять основных классов данных, которые используются в технологии ATM.

- Constant Bit Rate (CBR)
- Real Time Variable Bit Rate (RT-VBR)
- Non-Real Time Variable Bit Rate (NRT-VBR)
- Unspecified Bit Rate (UBR)
- Available Bit Rate (ABR

Уровни информационного взаимодействия ATM

Физический уровень взаимодействия ATM

На этом уровне определяются способы задания границ и правила упаковки ячеек ATM в кадры физического уровня.Физический уровень ATM функционально делится на два подуровня -

- Уровень физической среды (physical medium sub-layer)
- Уровень преобразования (transmission convergence sub-layer)

Канальный уровень взаимодействия ATM

Информационное взаимодействие на канальном уровне ATM осуществляется на двух подуровнях:

- Канальный уровень ATM (уровень ATM)
- Уровень адаптации ATM

Уровень ATM

На уровне ATM определяются процедуры и выполняются основные функции, которые обеспечивает технология ATM:

- Создание виртуальных соединений
- Управление виртуальными соединениями
- Обеспечение необходимого уровня обслуживания

Уровни адаптации ATM

Назначением данного уровня является определение процедур в соответствии с которыми выполняется преобразование блоков данных верхних уровней в поток ячеек ATM. Для того, чтобы преобразование в ячейки оптимальным образом соответствовало типу трафика пользователя, применяется несколько стандартных уровней адаптации ATM:

- ATM Adaptation Layer1 (AAL1)
- ATM Adaptation Layer3/4 (AAL3/4)
- ATM Adaptation Layer5 (AAL5)

Уровень AAL1

Уровень адаптации AAL1 предназначен для обеспечения передачи по сетям ATM трафика типа CBR (оцифрованный голос, видеоконференции).

Уровень AAL3/4

Уровень адаптации AAL3/4 предназначен для обеспечения передачи по сетям ATM блоков данных SMDS (Switched Multi megabit Data Service).

Уровень AAL5

Данный уровень адаптации наиболее часто используется для передачи по сетям ATM трафика локальных вычислительных сетей и имеет специальное название - SEAL (Simple and Efficient Adaptation Layer).

Сетевой шлюз. Брандмауэр.

Мосты и шлюзы: назначение и особенности работы.

В процессе передачи мост регенерирует сигналы пакета, что позволяет передавать данные вдоль сети на значительные расстояния. Мост просматривает любой пакет и решает, к какой из 2-х сетей он принадлежит (в отличие от повторителей, которые лишь «проталкивают» пакеты из одной ЛС в другую без просмотра и анализы передаваемых данных).

В процессе передачи какого-либо пакета мост отслеживает адреса приемника и передатчика информации. Если пакет передается из станции 1 локальной сети «А» на станцию 5 локальной сети «Б», то мост должен обработать и пропустить пакет именно сеть «Б». Если же пакет поступает из станции 1 сети «А» на станцию 3 той же сети «А», то мост никакого воздействия на прохождение пакета не оказывает.

Мосты распознают, какой сети принадлежит тот или иной пакет, благодаря просмотру информации уровня управления доступом к среде, которая содержится в любом пакете (это протоколы канального уровня). Они отвечают за предоставление компьютерам доступа к сетевому кабелю. На этом же уровне определяется, откуда пакет выходит и куда должен поступить.

Почему мосты?

Наиболее общей причиной применения мостов является повышение ??? сети за счет понижения трафика путем деления одной большой сети на 2 части. В любой из частей величина трафика уменьшается, однако при этом сохраняется возможность связи между рабочими станциями обеих частей.

Другая причина применения мостов заключается в сопряжении ??? средств с различными кабельными соединениями. Мосты позволяют также связать сети типа Ethernet или сети Token Ring с различными скоростями передачи данных.

Принцип работы мостов основан на использовании протоколов управления доступом к среде, которые относятся к канальному уровню протокольного стека модели OSI. Это значит, что они могут применяться в сетях, использующих различные протоколы, что определяет протоколонезависимость мостов. Например, один и тот же мост может обеспечивать связь сетей на базе таких протоколов транспортного уровня, как TCP/IP, IPX и XNS. Этот факт объясняется тем, что уровень управления доступом к среде находится ниже сетевого уровня, который содержит информацию о протоколе более высокого транспортного уровня.

Однако мосты не обеспечивают связь пользователей, говорящих на языке протокола TCP/IP с пользователями, говорящими на IPX.

Устройства, которые позволяют обеспечить связь между такими протоколами, называются **шлюзами**. Эти устройства обеспечивают трансляцию межсетевых протоколов, в то время как мосты обеспечивают передачу пакетов между сетями независимо от типа используемого протокола.

Мосты как бы предоставляют возможность любым двум пользователям, работающим в разных сетях, но «говорящим» на языке одного и того же протокола, взаимодействовать друг с другом.

Многие сети работают на базе нескольких протоколов. Мост, объединяющий такие сети, пропускает пакеты этих (2-3) протоколов. В действительности, мост может и не «знать», пакеты какого протокола передаются через него в данный момент. Главное условие — оба компьютера, между которыми устанавливается связь, должны пользоваться одинаковыми протоколами.

Обучение и фильтрация

Мост обычно работает с так называемой **адресной таблицей**. Когда мост подключен к сети, он начинает опрашивать все рабочие станции в локальном сегменте сети. После приема всех ответов от рабочих станций мост строит таблицу локальных адресов. Этот процесс называется **обучением**.

Большинство мостов относится к типу обучаемых, хотя существует 1-2 типа мостов, в которых задание всех локальных адресов должен выполнять администратор сети. Такие мосты называются **статическими**.

После того, как мост сформировал таблицу локальных адресов, он готов к работе. Когда мост получает пакет, производится проверка адреса получателя и, если этот адрес является локальным, мост игнорирует его. В противном случае мост копирует пакет во вторую сеть. Процесс просмотра адресов пакетов называется **фильтрацией**, а процесс копирования пакета в другую сеть — **продвижением** пакета.

Наиболее часто применяется тот тип фильтрации, при котором пакеты с локальными адресами сохраняются в локальном сегменте сети, а пересылаются лишь удаленные пакеты.

Существует также фильтрация с использованием специальных адресов источника и получателя пакета. Применение такого типа фильтрации позволяет, например, мосту «запретить» какой-либо рабочей станции выполнять передачу пакетов из локального сегмента сети в другие сети или, наоборот, запретить прием всех внешних пакетов.

Существуют также удаленные мосты, которые обеспечивают соединение двух сетей, находящихся на значительном расстоянии друг от друга. Такие мосты работают через телекоммуникационные каналы.

Помимо мостов и шлюзов существуют еще повторители и маршрутизаторы — в качестве устройств межсетевого взаимодействия.

Любой из типов устройств работает на своем уровне модели OSI:

1) Физический уровень — повторители (регенерация пакетов — позволяют удлинить сеть)

2) Канальный уровень — мосты (анализ данных, понижение трафика, связь сегментов сети)

3) Сетевой уровень — маршрутизаторы

4) На остальных четырех — шлюзы

Маршрутизаторы — связь логически не связанных сетей, использующих один и тот же протокол транспортного уровня. Являются протоколозависимым устройством, что отличает их от мостов, обладают более сложной логикой работы. Служат для определения оптимальных маршрутов передачи пакетов.

Шлюзы - устройства, обеспечивающие преобразование, трансляцию несовместимых между собой протоколов транспортного уровня. Наиболее часто используются для связи между локальными сетями.

В последнее время появились «гибриды» — мост-маршрутизатор, маршрутизирующий мост.

Межсетевой Экран (МЭ)

http://ru.wikipedia.org/wiki/Межсетевой_экран

устройство (программа), которое управляет доступом (выходом) в частную сеть или компьютер.

Другие названия:

Брандма́уэр (Brandmauer) – из немецкого, каменная стена между деревянными домами, препятствующая распространению огня.

Файрво́лл, **файрво́л**, **файерво́л**, **фаерво́л** (Firewall) - из английского, тоже самое.

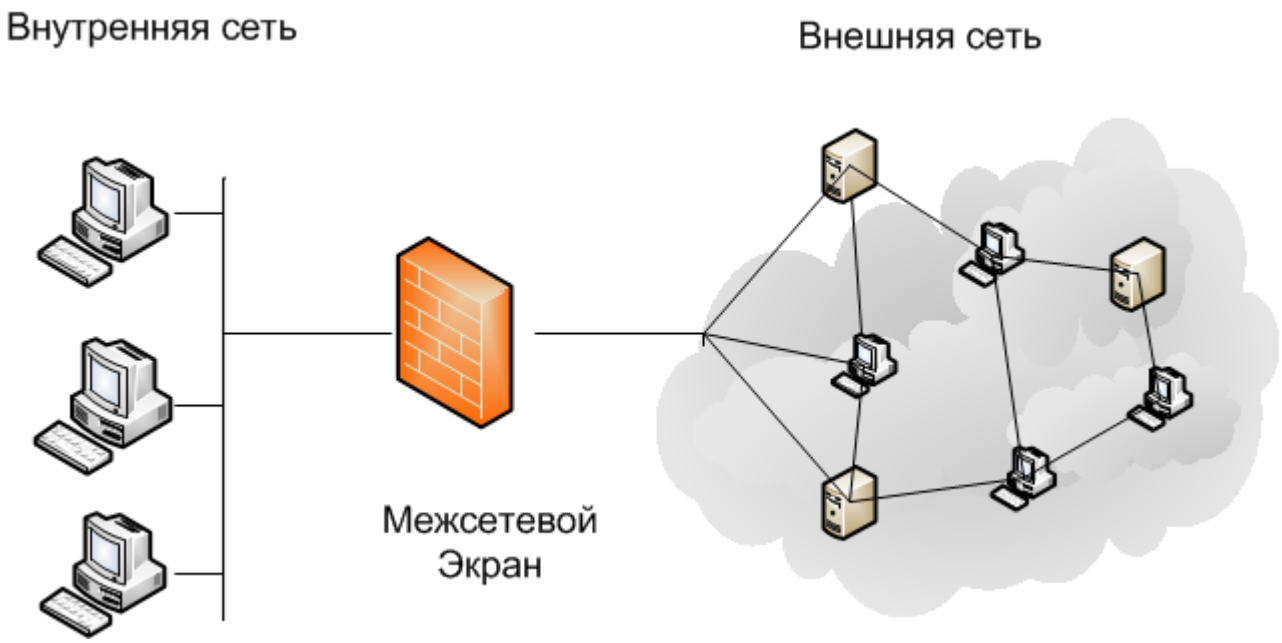


Рис. Межсетевой экран

Места применения МЭ:

- На персональном компьютере
- На маршрутизаторе между сегментами локальной сети
- На шлюзе из локальной сети во внешнею (глобальную) сеть
- На сервере удаленного доступа
- На сервер, МЭ уровня приложений (например: ModSecurity для фильтрации запросов (ответов) к HTTP-серверу)

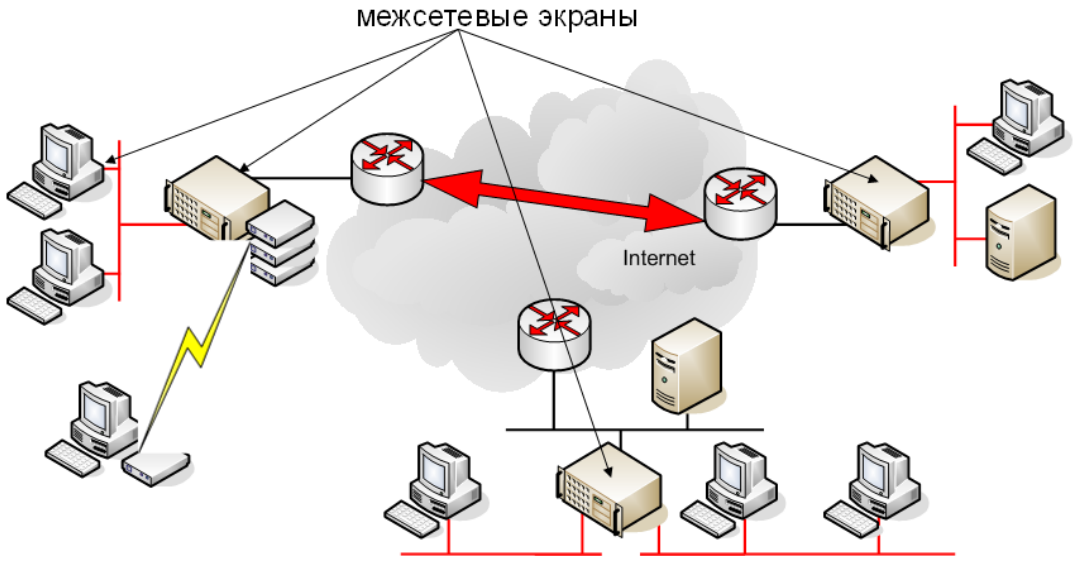


Рис. Схемы применения межсетевых экранов

Функции межсетевого экрана:

- **Фильтрация** - фильтры отсеивают нежелательные пакеты (запросы), на основе содержимого полей (адресов отправителя и получателя, номерам протоколов, номерам портов прикладных сервисов, флагов управления и т.д.) или запросов на прикладном уровне.

- **Трансляция сетевых адресов NAT (Network Address Translation)** – обеспечивает сокрытие внутренней структуры частной сети.
- **Туннелирование** (VPN - Virtual Private Network) - инкапсуляция IP-датаграмм в транспортные IP-датаграммы позволяет скрыть, с применением шифрования и аутентификации, IP-обмен между виртуальными частными сетями.
- **Proxy-сервер** - полная обработка прикладных данных (например: размер файлов, содержимое файлов).
- **Регистрация событий** - анализ и регистрация трафика и обнаружение фактов нарушения защиты.