1. **Основные понятия КС. Преимущества работы в сети.**

Компьютерная сеть - группа компьютеров, объединенная друг с другом каналами связи.

Основным преимуществом работы в локальной сети является использование в многопользовательском режиме общих ресурсов сети: дисков, принтеров, модемов, программ и данных, хранящихся на общедоступных дисках, а также возможность передавать информацию с одного компьютера на другой.

1. **Способы организации и передачи данных** (дополнить).

Передача информации необходима для того или иного ее распространения. Общая схема передачи такова: источник информации - канал связи - приемник (получатель) информации

Для передачи информации с помощью технических средств используются кодирующее устройство, предназначенное для преобразования исходного сообщения источника информации к виду, удобному для передачи, и декодирующее устройство, необходимое для преобразования кодированного сообщения в исходное.

При передаче информации необходимо учитывать тот факт, что информация при этом может теряться или искажаться, т.е. присутствуют помехи. Для нейтрализации помех при передаче информации зачастую используют помехоустойчивый избыточный код, который позволяет восстановить исходную информацию даже в случае некоторого искажения.

Основными устройствами для быстрой передачи информации на большие расстояния в настоящее время являются телеграф, радио, телефон, телевизионный передатчик, телекоммуникационные сети на базе вычислительных систем.

1. **Сетевые пакеты**.

Из-за того что большие блоки замедляют работу сети, их разбивают на пакеты.

Структура пакета:

* Header
  + Сигнал говорящий о том, что пакет передается
  + Адрес источника
  + Адрес получателя
* Data
  + Передаваемые данные (в зависимости от типа сети варьируются от 0,5 до 4 кбайт)
* Footer (trailer)
  + Содержимое зависит от протокола связи. Чаще всего содержит инфу для проверки ошибок при передаче.

1. **Переключения соединений**

Коммутация, или переключение соединения позволяет аппаратным средствам использовать один и тот же физический канал для соединения со множеством устройств. Этот принцип лежит в основе телефонной сети общего пользования (ТФОП). При отсутствии механизма коммутации, вам необходимо иметь тысячу соединительных линий чтобы позвонить тысяче абонентов. Используя механизм коммутации можно обойтись одной единственной линией. По этой же причине коммутация используется в компьютерных сетях.

Существует два вида коммутации:

* 1. коммутация цепей
  2. коммутация пакетов

Переключение цепей создает единое непрерывное соединение между двумя сетевыми устройствами. Пока эти устройства взаимодействуют, другие не могут воспользоваться этим соединением. Т.е. устройства делят между собой физический канал связи и вынуждены ждать, пока он не освободится. В телефонной сети используют именно этот способ коммутации.

Переключение пакетов позволяет не поддерживать постоянный физический канал между двумя устройствами. Информация при этом способе коммутации делится на части, называющиеся пакетами, и каждый пакет передается отдельно, по свободным в данный момент каналом связи. При этом каждый пакет может проходить по своему маршруту.

1. **Архитектуры сетей**

Обычно это:

* 1. Одноранговая архитектура

Одноранговая архитектура (peer-to-peer architecture) – это концепция информационной сети, в которой ее ресурсы рассредоточены по всем системам. Данная архитектура характеризуется тем, что в ней все системы равноправны.

К одноранговым сетям относятся малые сети, где любая рабочая станция может выполнять одновременно функции файлового сервера и рабочей станции. В одноранговых ЛВС дисковое пространство и файлы на любом компьютере могут быть общими. Чтобы ресурс стал общим, его необходимо отдать в общее пользование, используя службы удаленного доступа сетевых одноранговых операционных систем. В зависимости от того, как будет установлена защита данных, другие пользователи смогут пользоваться файлами сразу же после их создания. Одноранговые ЛВС достаточно хороши только для небольших рабочих групп.

Одноранговые сети имеют следующие преимущества:

* они легки в установке и настройке;
* отдельные ПК не зависят от выделенного сервера;
* пользователи в состоянии контролировать свои ресурсы;
* малая стоимость и легкая эксплуатация;
* минимум оборудования и программного обеспечения;
* нет необходимости в администраторе;
* хорошо подходят для сетей с количеством пользователей, не превышающим десяти.

Говоря понятным языком, приведу в пример torrent, через прогу ты просто берешь и шаришь файлы, всем у кого есть ссылка на него, т.е. доступ скачать его. Здесь нет централизованного сервака, вырубив 1 комп из 100 – ничего с сетью не случится, разве что не будет доступа к файлам отключенного компа.

* 1. Клиент-серверная

Архитектура клиент-сервер (client-server architecture) – это концепция информационной сети, в которой основная часть ее ресурсов сосредоточена в серверах, обслуживающих своих клиентов (рис. 1.8). Рассматриваемая архитектура определяет два типа компонентов: серверы и клиенты.

Сервер – это объект, предоставляющий сервис другим объектам сети по их запросам. Сервис – это процесс обслуживания клиентов.

Сервер работает по заданиям клиентов и управляет выполнением их заданий. После выполнения каждого задания сервер посылает полученные результаты клиенту, пославшему это задание.

Сервисная функция в архитектуре клиент-сервер описывается комплексом прикладных программ, в соответствии с которым выполняются разнообразные прикладные процессы.

Процесс, который вызывает сервисную функцию с помощью определенных операций, называется клиентом. Им может быть программа или пользователь. На рис. 1.9 приведен перечень сервисов в архитектуре клиент-сервер.

Клиенты – это рабочие станции, которые используют ресурсы сервера и предоставляют удобные интерфейсы пользователя. Интерфейсы пользователя (рис. 1.9) это процедуры взаимодействия пользователя с системой или сетью.

Круг задач, которые выполняют серверы в иерархических сетях, многообразен и сложен.

1. Файл-серверы и принт-серверы.
2. Серверы приложений (в том числе сервер баз данных (БД), WEB-сервер)
3. Почтовые серверы
4. Факс-серверы
5. Коммуникационные серверы
6. Сервер служб каталогов предназначен для поиска, хранения и защиты информации в сети.

Клиент является инициатором и использует электронную почту или другие сервисы сервера. В этом процессе клиент запрашивает вид обслуживания, устанавливает сеанс, получает нужные ему результаты и сообщает об окончании работы.

Сети на базе серверов имеют лучшие характеристики и повышенную надежность. Сервер владеет главными ресурсами сети, к которым обращаются остальные рабочие станции.

Сети клиент-серверной архитектуры имеют следующие преимущества:

* позволяют организовывать сети с большим количеством рабочих станций;
* обеспечивают централизованное управление учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;
* эффективный доступ к сетевым ресурсам;
* пользователю нужен один пароль для входа в сеть и для получения доступа ко всем ресурсам, на которые распространяются права пользователя.

Наряду с преимуществами сети клиент-серверной архитектуры имеют и ряд недостатков:

* неисправность сервера может сделать сеть неработоспособной;
* требуют квалифицированного персонала для администрирования;
* имеют более высокую стоимость сетей и сетевого оборудования.

1. **Файловые серверы**

FTP (File Transfer Protocol - Протокол передачи файлов) позволяет передавать файлы между двумя компьютерами, соединенными средствами Internet. Для доступа к FTP вам нужна программа-клиент для соединения с машиной, содержащей файлы (сервером) Если в вашей системе есть FTP-клиент и вы соединены с Internet, вы можете получить доступ к очень большому количеству файлов, доступных на FTP-серверах.

Файл-сервер — это выделенный сервер, предназначенный для выполнения файловых операций ввода-вывода и хранящий файлы любого типа. Как правило, обладает большим объемом дискового пространства, реализованном в форме RAID-массива для обеспечения бесперебойной работы и повышенной скорости записи и чтения данных.

Протокол обмена при такой схеме представляет собой набор вызовов, обеспечивающих приложению доступ к файловой системе на файл-сервере.

К недостаткам данной технологии относится низкий сетевой трафик (передача множества файлов, необходимых приложению), небольшое количество операций манипуляции с данными (файлами), отсутствие адекватных средств безопасности доступа к данным (защита только на уровне файловой системы) и т. д.

1. **Сетевые приложения** (дополнить).

Компьютер, подключенный к сети, может выполнять следующие типы приложений:

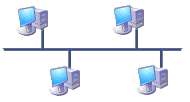
Локальное приложение целиком выполняется на данном компьютере и использует только локальные ресурсы. Для такого приложения не требуется никаких сетевых средств, оно может быть выполнено на автономно работающем компьютере.

Централизованное сетевое приложение целиком выполняется на данном компьютере, но обращается в процессе своего выполнения к ресурсам других компьютеров сети. В примере приложение, которое выполняется на клиентском компьютере, обрабатывает данные из файла, хранящегося на файл-сервере, а затем распечатывает результаты на принтере, подключенном к серверу печати. Очевидно, что работа такого типа приложений невозможна без участия сетевых служб и средств транспортировки сообщений.

Распределенное (сетевое) приложение состоит из нескольких взаимодействующих частей, каждая из которых выполняет какую-то определенную законченную работу по решению прикладной задачи, причем каждая часть может выполняться и, как правило, выполняется на отдельном компьютере сети. Части распределенного приложения взаимодействуют друг с другом, используя сетевые службы и транспортные средства ОС. Распределенное приложение в общем случае имеет доступ ко всем ресурсам компьютерной сети.

1. **Базовые топологии сетей. Топология шина. Принцип построения. Достоинства и недостатки.**

Топология шина (или, как ее еще часто называют общая шина или магистраль) предполагает использование одного кабеля, к которому подсоединены все рабочие станции.



Общий кабель используется всеми станциями по очереди. Все сообщения, посылаемые отдельными рабочими станциями, принимаются и прослушиваются всеми остальными компьютерами, подключенными к сети. Из этого потока каждая рабочая станция отбирает адресованные только ей сообщения.

Достоинства:

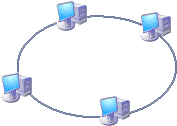
* простота настройки;
* относительная простота монтажа и дешевизна, если все рабочие станции расположены рядом;
* выход из строя одной или нескольких рабочих станций никак не отражается на работе всей сети.

Недостатки:

* неполадки шины в любом месте (обрыв кабеля, выход из строя сетевого коннектора) приводят к неработоспособности сети;
* сложность поиска неисправностей;
* низкая производительность – в каждый момент времени только один компьютер может передавать данные в сеть, с увеличением числа рабочих станций производительность сети падает;
* плохая масштабируемость – для добавления новых рабочих станций необходимо заменять участки существующей шины.

1. **Базовые топологии сетей. Топология кольцо. Принцип построения. Достоинства и недостатки.**

Кольцо – это топология локальной сети, в которой рабочие станции подключены последовательно друг к другу, образуя замкнутое кольцо. Данные передаются от одной рабочей станции к другой в одном направлении (по кругу). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК, т.е. данные передаются от одного компьютера к другому как бы по эстафете.



Если компьютер получает данные, предназначенные для другого компьютера – он передает их дальше по кольцу, в ином случае они дальше не передаются.

Достоинства:

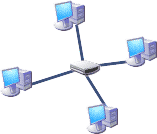
* простота установки;
* практически полное отсутствие дополнительного оборудования;
* возможность устойчивой работы без существенного падения скорости передачи данных при интенсивной загрузке сети.

Недостатки:

* каждая рабочая станция должна активно участвовать в пересылке информации; в случае выхода из строя хотя бы одной из них или обрыва кабеля – работа всей сети останавливается;
* подключение новой рабочей станции требует краткосрочного выключения сети, поскольку во время установки нового ПК кольцо должно быть разомкнуто;
* сложность конфигурирования и настройки;
* сложность поиска неисправностей;
* Кольцевая топология сети используется довольно редко. Основное применение она нашла в оптоволоконных сетях стандарта Token Ring.

1. **Базовые топологии сетей. Топология звезда. Принцип построения. Достоинства и недостатки.**

Звезда – это топология локальной сети, где каждая рабочая станция присоединена к центральному устройству (коммутатору или маршрутизатору). Центральное устройство управляет движением пакетов в сети. Каждый компьютер через сетевую карту подключается к коммутатору отдельным кабелем.



При необходимости можно объединить вместе несколько сетей с топологией “звезда” – в результате вы получите конфигурацию сети с древовидной топологией. Древовидная топология распространена в крупных компаниях. Мы не будем ее подробно рассматривать в данной статье.

Топология “звезда” на сегодняшний день стала основной при построении локальных сетей. Это произошло благодаря ее многочисленным *достоинствам*:

* выход из строя одной рабочей станции или повреждение ее кабеля не отражается на работе всей сети в целом;
* отличная масштабируемость: для подключения новой рабочей станции достаточно проложить от коммутатора отдельный кабель;
* легкий поиск и устранение неисправностей и обрывов в сети;
* высокая производительность;
* простота настройки и администрирования;
* в сеть легко встраивается дополнительное оборудование.

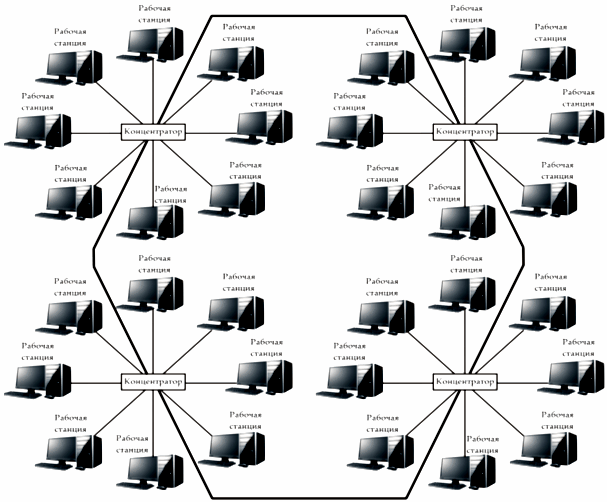
Недостатки:

* выход из строя центрального коммутатора обернется неработоспособностью всей сети;
* дополнительные затраты на сетевое оборудование – устройство, к которому будут подключены все компьютеры сети (коммутатор);
* число рабочих станций ограничено количеством портов в центральном коммутаторе.

Звезда – самая распространенная топология для проводных и беспроводных сетей. Примером звездообразной топологии является сеть с кабелем типа витая пара, и коммутатором в качестве центрального устройства. Именно такие сети встречаются в большинстве организаций.

1. **Комбинированные топологии сетей. Топология звезда-кольцо. Принцип построения. Достоинства и недостатки.**

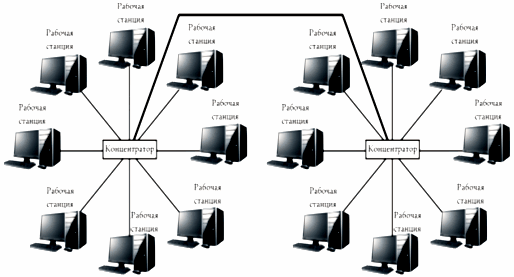
Звезда-шина (star-bus) - это комбинация топологий «шина» и «звезда». Чаще всего это выглядит так: несколько сетей с топологией ``звезда'' объединяются при помощи магистральной линейной шины. В этом случае выход из строя одного компьютера не оказывает никакого влияния на сеть - остальные компьютеры по-прежнему взаимодействуют друг с другом. А выход из строя концентратора повлечет за собой остановку подключенных к нему компьютеров и концентраторов.



1. **Комбинированные топологии сетей. Топология звезда-шина. Принцип построения. Достоинства и недостатки.**

Смешанная топология соединяет в себе две или более топологии, образуя тем самым завершенную сетевую структуру. На данный момент такая сеть является самой распространенной; наиболее часто объединяют звездообразную и шинную топологии.

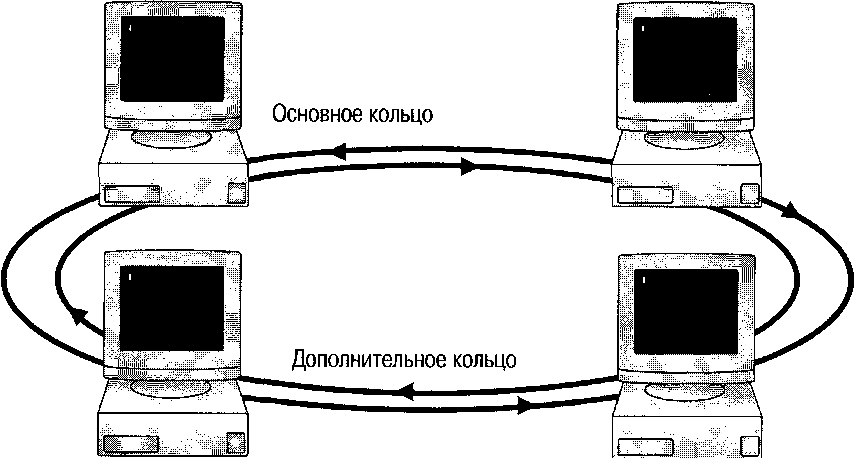
При использовании топологии «звезда-шина» несколько сетей, имеющих звездообразную топологию, подключены к одной шине.



В данной топологии сбой на одном из компьютеров совершенно не отразится на работе сети в целом. Если же произойдет ошибка центрального компонента (концентратора), к которому подключаются компьютеры «звезды», то все они не смогут больше поддерживать связь.

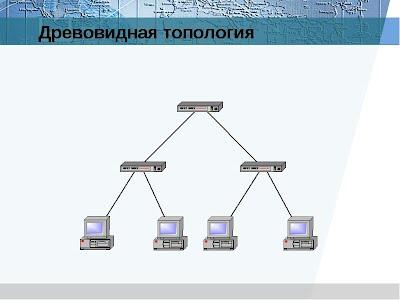
1. **Комбинированные топологии сетей. Топология двойное-кольцо. Принцип построения. Достоинства и недостатки.**

Двойное кольцо — это топология, построенная на двух кольцах. Первое кольцо — основной путь для передачи данных. Второе — резервный путь, дублирующий основной. При нормальном функционировании первого кольца, данные передаются только по нему. При его выходе из строя оно объединяется со вторым и сеть продолжает функционировать. Данные при этом по первому кольцу передаются в одном направлении, а по второму в обратном. Примером может послужить сеть FDDI.



1. **Комбинированные топологии сетей. Древовидная топология. Принцип построения. Достоинства и недостатки.**

По структуре похож на расширенную звезду, но ее центральным элементом является не центральный узел, а так называемый магистральный кабель. Как правило, он применяется в случае необходимости доступа многих узлов к одному, в жестко выраженном клиент-серверной среде.



1. **13**
2. **Комбинированные топологии сетей. Ячеистая топология. Принцип построения.**

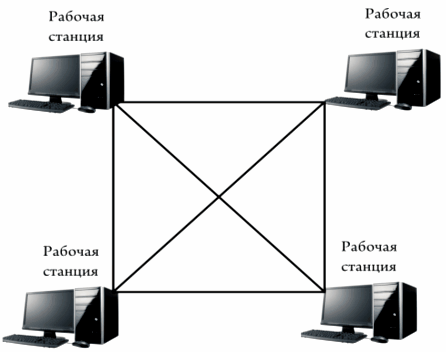
Данная топология подразумевает подключение каждого компьютера через отдельный кабель ко всем остальным компьютерам, находящимся в сети. Применение этого метода позволяет использовать дополнительные пути транспортировки данных. В случае обрыва какого-либо кабеля поток данных пойдет по другому пути, а сеть сможет нормально функционировать далее. Такая топология характерна для глобальных сетей и объединения нескольких удаленных сетей с применением оптоволоконных, выделенных или спутниковых каналов связи. Для локальных сетей данная топология не используется, так как требует присутствия одновременно нескольких сетевых интерфейсов на одной машине и больших объемов кабеля.

\_

В сети с ячеистой топологией непосредственно связываются только те компьютеры, между которыми происходит интенсивный обмен данными, а для обмена данными между компьютерами, не соединенными прямыми связями, используются транзитные передачи через промежуточные узлы. Ячеистая топология допускает соединение большого количества компьютеров и характерна, как правило, для глобальных сетей. Достоинства данной топологии в ее устойчивости к отказам и перегрузкам, т.к. имеется несколько способов обойти отдельные узлы.

\_

К преимуществам ячеистой топологии относят эффективную работу с большими потоками данных, высокий уровень стабильности сети из-за использования дополнительных каналов связи, высокий уровень безопасности; поток информации идет от компьютера-отправителя к получателю напрямую, что теоретически исключает перехват данных.



К недостаткам - потребность в наличии нескольких сетевых интерфейсов на компьютерах, входящих в сеть, большая стоимость организации сети.

1. **Комбинированные топологии сетей. Иерархическая топология. Принцип построения. Достоинства и недостатки.**

Иерархическая топология (hierarchical topology) похожа на расширенную звездообразную топологию. Только в такой сети нет центрального узла. Вместо этого используется магистральный узел (trunk node), от которого отходят ветви (branches) к другим узлам. Существуют два типа иерархической топологии: бинарное дерево - от каждого узла отходят два соединения; и магистральное дерево - магистральный узел имеет узлы-ветви, от которых отходят каналы к рабочим станциям.



1. **Модель OSI. 1-2 уровни.**
   1. Физический.
   2. Канальный.
   3. Сетевой.
   4. Транспортный.
   5. Сеансовый.
   6. Представления.
   7. Прикладной.

Физический уровень обеспечивает виртуальную линию связи для передачи данных между узлами сети. На этом уровне выполняется преобразование данных, поступающих от следующего, более высокого уровня (уровень управления передачей данных), в сигналы, передающиеся по кабелю.

Канальный обеспечивает виртуальную линию связи более высокого уровня, способную безошибочно передавать данные в асинхронном режиме. При этом данные обычно передаются блоками, содержащими дополнительную управляющую информацию. Такие блоки называют кадрами.

1. **Модель OSI. 2-3 уровни.**

Сетевой уровень предполагает, что с каждым узлом сети связан некий процесс. Процессы, работающие на узлах сети, взаимодействуют друг с другом и обеспечивают выбор маршрута передачи данных в сети (маршрутизацию), а также управление потоком данных в сети. В частности, на этом уровне должна выполняться буферизация данных.

1. **Модель OSI. 3-4 уровни.**

Транспортный - может выполнять разделение передаваемых сообщений на пакеты на передающем конце и сборку на приемном конце. На этом уровне может выполняться согласование сетевых уровней различных несовместимых между собой сетей через специальные шлюзы. Например, такое согласование потребуется для объединения локальных сетей в глобальные.

1. **Модель OSI. 4-5 уровни.**

Сеансовый - обеспечивает интерфейс с транспортным уровнем. На этом уровне выполняется управление взаимодействием между рабочими станциями, которые участвуют в сеансе связи. В частности, на этом уровне выполняется управление доступом на основе прав доступа.

1. **Модель OSI. 5-6 уровни.**

Представления - описывает шифрование данных, их сжатие и кодовое преобразование. Например, если в состав сети входят рабочие станции с разным внутренним представлением данных (ASCII для IBM PC и EBCDIC для IBM-370), необходимо выполнить преобразование.

1. **Модель OSI. 6-7 уровни.**

Прикладной - отвечает за поддержку прикладного программного обеспечения конечного пользователя.

1. **Модель OSI. Поиск и устранение неисправностей сети по модели OSI.**

хз

1. **Методы доступа к средам передачи данных. CSMA/CD**

Множественный доступ с контролем несущей и обнаружением коллизий

Данный метод доступа устанавливает следующий порядок

Компьютер отправитель сначала посылает запрос на проверку свободен канал или нет, в процессе передачи станция продолжает прослушивать канал для обнаружения коллизий, если был обнаружен конфликт соединение останавливается до тех пор, пока канал не освободится.

На всякий Множественный доступ с прослушивание несущей и избеганием коллизий

Отличается от предыдущего тем, что коллизии подвержены не пакеты, а сигналы

Или так:

1.

* Передающий проверяет сеть
* Если несущая отсутствует
* Можно передавать

2.

* Передающий комп проверяет сетку
* Несущая обнаружена
* Передавать нельзя – ожидание

После обнаружения коллизии передающий комп уходит в таймаут, а потом пытается передать инфу снова.

1. **Методы доступа к средам передачи данных. TPMA**

Множественный доступ с передачей полномочий

Метод доступа, в котором от ПК к ПК передается маркер, дающий разрешение на передачу. ПК может получать информацию только в том случае, если он получил маркер.

1. **Методы доступа к средам передачи данных. TDMA**

Множественный доступ с разделением по времени

Основан на распределении времени работы сигнала. В данном методе используется тактовый генератор, который делит время канал на повторяющиеся циклы. Каждый интервал называют «ячейками».

1. **Методы доступа к средам передачи данных. FDMA**

Множественный доступ с разделением по частоте

Основан на разделении полосы пропускания на группу полос частот, который называется логическим каналом. По каждому из них передается информация.

1. **Методы доступа к средам передачи данных. WDMA**

Множественный доступ с разделение волны

Широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. Размеры узких полос могут быть различными. При использовании FDMA, именуемого также множественным доступом с разделением волны WDMA, широкая полоса пропускания канала делится на ряд узких полос, разделенных защитными полосами. В каждой узкой полосе создается логический канал. Размеры узких полос могут быть различными. Передаваемые по логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Вместе с этим, иногда, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать шум в соседнем логическом канале.

1. **Спецификация стандартов 802. Технология 802.3. Ethernet**

Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле Ethernet - это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. Метод доступа был опробован еще раньше: во второй половине 60-х годов в радиосети Гавайского университета использовались различные варианты случайного доступа к общей радиосреде, получившие общее название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля, который стал последней версией фирменного стандарта Ethernet. Поэтому фирменную версию стандарта Ethernet называют стандартом Ethernet DIX или Ethernet II.

Когда говорят Ethernet, то под этим обычно понимают любой из вариантов этой технологии. В более узком смысле Ethernet - это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. Метод доступа был опробован еще раньше: во второй половине 60-х годов в радиосети Гавайского университета использовались различные варианты случайного доступа к общей радиосреде, получившие общее название Aloha. В 1980 году фирмы DEC, Intel и Xerox совместно разработали и опубликовали стандарт Ethernet версии II для сети, построенной на основе коаксиального кабеля, который стал последней версией фирменного стандарта Ethernet. Поэтому фирменную версию стандарта Ethernet называют стандартом Ethernet DIX или Ethernet II.

В зависимости от типа физической среды стандарт IEEE 802.3 имеет различные модификации - l0Base-5, l0Base-2, l0Base-T, l0Base-FL, l0Base-FB.

1. **Спецификация стандартов 802. Технология 802.3. Fast Ethernet**

Технология Fast Ethernet является эволюционным развитием классической технологии Ethernet. Ее основными достоинствами являются:

* увеличение пропускной способности сегментов сети до 100 Мб/c;
* сохранение метода случайного доступа Ethernet;
* сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных - витой пары и оптоволоконного кабеля.

Указанные свойства позволяют осуществлять постепенный переход от сетей 10Base-T - наиболее популярного на сегодняшний день варианта Ethernet - к скоростным сетям, сохраняющим значительную преемственность с хорошо знакомой технологией: Fast Ethernet не требует коренного переобучения персонала и замены оборудования во всех узлах сети. Официальный стандарт 100Base-T (802.3u) установил три различных спецификации для физического уровня (в терминах семиуровневой модели OSI) для поддержки следующих типов кабельных систем:

* 100Base-TX для двухпарного кабеля на неэкранированной витой паре UTP Category 5, или экранированной витой паре STP Type 1;
* 100Base-T4 для четырехпарного кабеля на неэкранированной витой паре UTP Category 3, 4 или 5;
* 100Base-FX для многомодового оптоволоконного кабеля.

1. **Спецификация стандартов 802. Технология 802.3. Gigabit Ethernet**

Гигабитный Ethernet также известен как "гигабит по меди" или 1000BaseT. Он представляет собой обычную версию Ethernet, работающую на скоростях до 1.000 мегабит в секунду, то есть в десять раз быстрее 100BaseT.

Основой гигабитного Ethernet является стандарт IEEE 802.3z, который был утвержден в 1998 году. Однако в июне 1999 года к нему вышло дополнение - стандарт гигабитного Ethernet по медной витой паре 1000BaseT. Именно этот стандарт смог вывести гигабитный Ethernet из серверных комнат и магистральных каналов, обеспечив его применение в тех же условиях, что и 10/100 Ethernet.

До появления 1000BaseT для гигабитного Ethernet необходимо было использовать волоконно-оптический или экранированный медный кабели, которые вряд ли можно назвать удобными для прокладки обычных локальных сетей. Данные кабели (1000BaseSX, 1000BaseLX и 1000BaseCX) и сегодня используются в специальных областях применения, поэтому мы не будем их рассматривать.

Группа гигабитного Ethernet 802.3z прекрасно справилась со своей работой - она выпустила универсальный стандарт, в десять раз превышающий скорость 100BaseT. 1000BaseT также является обратно совместимым с 10/100 оборудованием, он использует CAT-5 кабель (или более высокую категорию). Кстати, сегодня типичная сеть построена именно на базе кабеля пятой категории.

1. **Спецификация стандартов 802. Технология 802.4.**

Маркерная шина (IEEE 802.4)

Стандарт IEEE 802.4 описывает свойства сетей, известных под названием маркерная шина. С точки зрения правил предоставления доступа этот стандарт схож с token ring. В качестве физической среды используется 75-омный кабель. При необходимости построения сети типа дерева, а также для увеличения длины сети используются повторители. Сеть способна обеспечить пропускную способность до 10 Мбит/с при полосе пропускания кабеля 12 МГц.

Для доступа к сетевой среде станция должна получить пакет-маркер. Получив маркер, сетевое устройство может начать передачу данных, а завершив эту процедуру, устройство должно переслать маркер следующей сетевой станции. Передача маркера происходит до тех пор, пока он не достигнет младшей станции, после чего он возвращается первой станции

1. **Спецификация стандартов 802. Технология 802.5.**

Сети Token Ring были разработаны фирмой IBM в 1970-х годах и рассчитана на скорость обмена 4.16 Мбит/c при числе сегментов до 250. По своей популярности она уступает лишь Ethernet/IEEE 802.3. Спецификация IEEE 802.5 практически идентична ей и полностью совместима. Сеть Token Ring имеет топологию звезды, все оконечные станции которой подключаются к общему устройству (MSAU - MultiStation Access Unit). В IEEE 802.5 топология не оговаривается, не регламентирована здесь и сетевая среда. В Token Ring сеть базируется на скрученных парах. Обе эти разновидности сети используют схему передачи маркера (небольшой пакет - token).

В отличие от сетей с csma/cd доступом (например, Ethernet) в IEEE 802.5 гарантируется стабильность пропускной способности (нет столкновений). Сети Token Ring имеют встроенные средства диагностики, они более приспособлены для решения задач реального времени, но в то же время более дороги.

Сети Token Ring имеют несколько механизмов для обнаружения и предотвращения влияния сетевых сбоев и ошибок. Например, пусть одна из станций выбрана в качестве активного монитора. Эта станция работает как центральный источник синхронизации для других станций сети и выполняет ряд других функций. Одной из таких функция является удаление из кольца бесконечно циркулирующих кадров (маркеров). Если отправитель ошибся, установив, например ошибочный адрес места назначения, это может привести к зацикливанию кадра. Ведь кадр может быть поврежден в пути и отправитель его уже не узнает. А это в свою очередь блокирует работу остальных станций. Активный монитор должен обнаруживать такие кадры, удалять их и генерировать новый маркер. Функции активного монитора часто выполняют MSAU. Попутно msau может контролировать, какая из станций является источником таких дефектных кадров, и вывести ее из кольца. Если станция обнаружила серьезную неполадку в сети (например, обрыв кабеля), она посылает сигнальный кадр (beacon). Такой кадр несет в себе идентификатор отправителя и имя соседа-предшественника (NAUN - nearest active upstream neighbour). Такой кадр инициализирует процедуру автореконфигурации, при которой узлы в районе аварии пытаются реконфигурировать сеть так, чтобы ликвидировать влияние поломки.

1. **Спецификация стандартов 802. Технология 802.8.**

Спецификация группы IEEE 802.8 называется «Распределенный интерфейс передачи данных по волоконно-оптическому кабелю» (Fiber Distributed Data Interface - FDDI, часто произносится как «фидди»). Вопреки распространенному мнению будто данный стандарт является просто высокоскоростной сетью архитектуры Token Ring, FDDI принципиально отличается топологией, управлением и даже структурой маркера и кадра.

Во-первых, в отличие от сети Token Ring, которая использует метод доступа путем резервации/приоритета (priority/reservation access method), FDDI использует для управления доступом к среде протокол упорядоченной рассылки маркеров (timed-token protocol). В итоге более детерминистическая локальная сеть позволяет отказаться от использования в кадре поля управления доступом к среде.

Сеть FDDI стандарта IEEE 802.5 использует этот маркер для управления доступом к среде передачи данных. Кадр маркера состоит из преамбулы, начального ограничителя, поля управления кадром и конечного ограничителя.

Несущий данные кадр сети FDDI состоит из следующих полей:

* Поля преамбулы длиной в восемь октетов, обозначающей начало кадров.
* Начального ограничителя (Start-of-Frame) длиной в один октет, обозначающего начало содержимого кадра.
* Поля управления кадром, определяющего тип кадра, например маркер, MAC или LLC, кадр приоритета и т.п.
* МАС-адреса предполагаемого получателя длиной шесть октетов.
* МАС-адреса отправителя длиной шесть октетов.
* Поля данных переменной длины (максимальный размер ограничен 4478 октетами).
* Контрольной последовательности кадра длиной в четыре октета, используемой для проверки целостности кадра.
* Конечного ограничителя длиной в пол-октета (четыре бита).
* Поля статуса кадра длиной в три октета, которое, в свою очередь, состоит из трех подполей по одному октету: Error (ошибка), Address-match (соответствие адресу) и Copied (копия). Каждое поле может принимать значение «S» (Set - истина) или «R» (Reset - ложь).

Длина кадра IEEE 802.8 FDDI ограничена 4500 октетами, включая данные и все служебные компоненты.

1. **Спецификация стандартов 802. Технология 802.11. 802.11a**

IEEE 802.11a — перспективный стандарт беспроводной сети, который рассчитан на работу в двух радиодиапазонах — 2,4 и 5 ГГц. Метод OFDM, который использется, позволяет достичь максимальной скорости передачи данных 54 Мбит/с.

Кроме этой скорости, спецификациями предусмотрены и другие:

* обязательные — 6, 12 и 24 Мбит/с;
* необязательные — 9, 18, 36, 48 и 54 Mбит/с.
* Этот стандарт также имеет свои преимущества и недостатки. Из преимуществ
* можно отметить:
* высокая скорость передачи;
* использование параллельной передачи данных;
* возможность подключения большого количества компьютеров.

Недостатки стандарта IEEE 802.11a такие:

меньший радиус сети при использовании диапазона 5 ГГц (около 100 м);

большая потребляемая мощность радиопередатчиков;

более высокая стоимость оборудования по сравнению с оборудованием других стандартов;

для использования диапазона 5 ГГц требуется наличие специального разрешения.

1. **Спецификация стандартов 802. Технология 802.11. 802.11b**

Работа над стандартом IEEE 802.11b (др. назв. — IEEE 802.11 High rate, высокая пропускная способность) была закончена в 1999 году, и именно с ним связано название Wi Fi (Wireless Fidelity, беспроводная точность). Работа стандарта основана на методе прямого расширения спектра (DSSS) с использованием восьмиразрядных последовательностей Уолша. При этом каждый бит данных кодируется с помощью последовательности дополнительных кодов (CCK). Это позволяет достичь скорости передачи данных 11 Мбит/с. Как и базовый стандарт, IEEE 802.11b работает с частотой 2,4 ГГц, используя не более трех неперекрывающихся каналов. Радиус действия сети при этом составляет около 300 м. Этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Отличительной особенностью этого стандарта является то, что при необходимости скорость передачи данных может уменьшаться вплоть до 1 Мбит/с. Напротив, обнаружив, что качество сигнала улучшилось, сетевое оборудование автоматически повышает скорость передачи до максимальной.

1. **Спецификация стандартов 802. Технология 802.11. 802.11g**

Стандарт IEEE 802.11g унаследовал самые лучшие свойства стандартов IEEE 802.11a и IEEE 802.11b и обладает многими собственными полезными качествами. Целью создания данного стандарта было достижение скорости передачи данных 54 Мбит/с. Как и IEEE 802.11b, стандарт IEEE 802.11g разработан для работы в частотном диапазоне 2,4 ГГц. IEEE 802.11g предписывает обязательные и возможные скорости передачи данных:

обязательные — 1, 2, 5.5, 6, 11, 12, 24 Мбит/с;

возможные — 33, 36, 48 и 54 Мбит/с.

Для достижения таких показателей используется кодирование с помощью последовательности дополнительных кодов (CCK), метод ортогонального частотного мультиплексирования (OFDM), метод гибридного кодирования (CCK-OFDM) и метод двоичного пакетного сверточного кодирования (PBCC). Стоит отметить, что одной и той же скорости можно достичь разными методами, однако обязательные скорости передачи данных достигаются только с помощью методов CCK и OFDM, а возможные скорости — с помощью методов CCK-OFDM и PBCC.

Преимуществом оборудования стандарта IEEE 802.11g является обратная совместимость с оборудованием IEEE 802.11b.

1. **Спецификация стандартов 802. Технология 802.11. 802.11n**

Этот стандарт был утверждён 11 сентября 2009.[1][2]

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a;

смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n;

«чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n).

Черновую версию стандарта 802.11n (DRAFT 2.0) поддерживают многие современные сетевые устройства. Итоговая версия стандарта (DRAFT 11.0), которая была принята 11 сентября 2009 года, обеспечивает скорость до 300 Мбит/с,

1. **Спецификация стандартов 802. Технология 802.12**

В качестве альтернативы технологии Fast Ethernet, фирмы AT&T и HP выдвинули проект новой технологии со скоростью передачи данных 100 Мб/с — 100Base-VG. В этом проекте было предложено усовершенствовать метод доступа с учётом потребности мультимедийных приложений, при этом сохранить совместимость формата пакета с форматом пакета сетей 802.3. В сентябре 1993 года по инициативе фирм IBM и HP был образован комитет IEEE 802.12, который занялся стандартизацией новой технологии. Проект был расширен за счёт поддержки в одной сети кадров не только формата Ethernet, но и формата Token Ring. В результате новая технология получила название 100VG-AnyLAN, то есть технология для любых сетей (Any LAN — любые сети), имея в виду, что в локальных сетях технологии Ethernet и Token Ring используются в подавляющем количестве узлов.

Летом 1995 года технология 100VG-AnyLAN получила статус стандарта IEEE 802.12.

1. **Спецификация стандартов 802. Технология 802.15**

Bluetooth …

1. **Спецификация стандартов 802. Технология 802.16**

WMAN — беспроводные сети масштаба города. Предоставляют широкополосный доступ к сети через радиоканал.

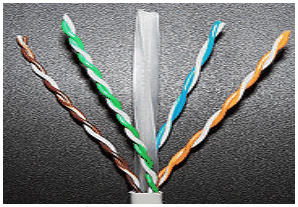
Стандарт IEEE 802.16, опубликованный в апреле 2002 года, описывает wireless MAN Air Interface. 802.16 — это так называемая технология «последней мили», которая использует диапазон частот от 10 до 66 GHz. Так как это сантиметровый и миллиметровый диапазон, то необходимо условие «прямой видимости». Стандарт поддерживает топологию point-to-multipoint, технологии frequency-division duplex (FDD) и time-division duplex (TDD), с поддержкой quality of service (QoS). Возможна передача звука и видео. Стандарт определяет пропускную способность 120 Мбит/с на каждый канал в 25 MHz.

1. **Кабельные среды передачи данных. Коаксиальный кабель.**



Коаксиальный кабель состоит из медного провода, покрытого изоляцией, экранирующей металлической оплеткой и внешней оболочкой. По центральному проводу кабеля передаются сигналы, в которые предварительно были преобразованы данные. Такой провод может быть как цельным, так и многожильным. Для организации локальной сети применяются два типа коаксиального кабеля: ThinNet. (тонкий, 10Base2) и ThickNet (толстый, 10Base5). В данный момент локальные сети на основе коаксиального кабеля практически не встречаются. Скорость передачи информации в такой сети не превышает 10 Мбит/с.

1. **Кабельные среды передачи данных. Витая пара. Категории и спецификации.**



Для построения локальных сетей сейчас наиболее широко используется витая пара. Внутри такой кабель состоит из двух или четырех пар медного провода, перекрученных между собой. Витая пара также имеет свои разновидности: UTP ( неэкранированная витая пара) и STP ( экранированная витая пара). Эти разновидности кабеля способны передавать сигналы на расстояние порядка 100 м. Как правило, в локальных сетях используется именно UTP. STP имеет плетеную оболочку из медной нити, которая имеет более высокий уровень защиты и качества, чем оболочка кабеля UTP. В кабеле STP каждая пара проводов дополнительно экранирована (она обернута слоем фольги), что защищает данные, которые передаются, от внешних помех. Такое решение позволяет поддерживать высокие скорости передачи на более значительные расстояния, чем в случае использования кабеля UTP. Витая пара подключается к компьютеру с помощью разъема RJ-45, который очень напоминает телефонный разъем RJ-11.

Существует семь категорий кабеля витая пара, которые нумеруются от CAT1 до CAT7. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины. Категории неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях).

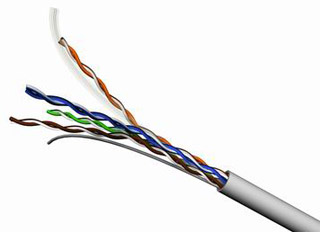
**CAT1** (частота 0,1 МГц) - однопарный телефонный кабель (кабель без скруток, в народе именуемый как «лапша»). Использовались там, где требования к скорости передачи данных были минимальны. Активно использовались в телефонии, так как скорость ограничивалась до 20 Кбит/с.



**CAT2** (частота 1 МГц) - 2 пары проводников поддерживают передачу данных со скоростью до 4 Мбит/с. Иногда встречается в телефонных сетях. Более качественный кабель, используемый в линиях ISDN.



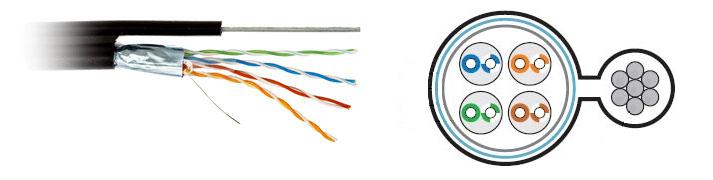
**CAT3** (частота 16 МГц) - четырехпарный кабель, использовался при построении локальных сетей Token Ring, поддерживает скорость передачи данных до 10 Мбит/с или 100 Мбит/с. Также до сих пор встречается в телефонных сетях. Может использоваться как для передачи голоса, так и данных. Достаточно распространен в постройках до 1996 года.   
  
  
  
  **CAT4** (частота 20 МГц) - кабель состоит из 4 скрученных пар, использовался в сетях Token Ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре, на данный момент не используется. Улучшенный вариант третьей категории.   
  
  
  **САТ5** (частота 100 МГц) - четырехпарный кабель, использовался при построении локальных сетей 100BASE-TXи, для прокладки телефонных линий, поддерживает скорость передачи данных до 100 Мбит/с при использовании 2 пар. Он пришел на замену третьей категории. Сегодня является самым распространенным видом кабеля так, как имеет низкую цену.



**САТ5e** (частота 125 МГц) - четырехпарный экранированный кабель, усовершенствованная категория 5. Скорость передач данных до 1000 Мбит/с при использовании четырех пар. Кабель подходит для прокладки вне помещений.



**CAT5 (5e)** (частота 125 МГц) - четырехпарный экранированный кабель. Для горизонтальной прокладки вне помещений, поддерживающий скорость передачи данных до 1000 Мбит/с при использовании 2 пар. Крепкая внешняя оболочка и поддерживающий металлический трос гарантируют долгосрочную и бесперебойную связь.



**СAT6** (частота 250 МГц) - четырехпарный кабель, способен передавать данные на скорости до 1000 Мбит/с. Создан для поддержки работы высокоскоростных протоколов на отрезках большей длины, чем при использовании кабеля пятой категории.  
  
  
  **CAT6A** (частота 500 МГц) - четырехпарный кабель, способен передавать данные на скорости до 10 Гигабит/с.  
  
  
  **CAT7** — спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных до 100 Гигабит/с, частоты пропускаемого сигнала до 600—700 МГц. Экранизированный кабель не только имеет защиту всех проводников, но и каждую пару в отдельности. Седьмая категория именуется как S/FTP (Screened Fully shielded Twisted Pair). Создан для тех же целей, что и кабель шестой категории. Является более дорогостоящим.



1. **Кабельные среды передачи данных. Витая пара. Стандарты обжима кабеля.**

2 стандарта обжима

* **568А**

1. бело-зеленый

2. зеленый

3. бело-оранжевый

4. синий

5. бело-синий

6. оранжевый

7. бело-коричневый

8. коричневый

* **568В**

1. бело-оранжевый

2. оранжевый

3. бело-зеленый

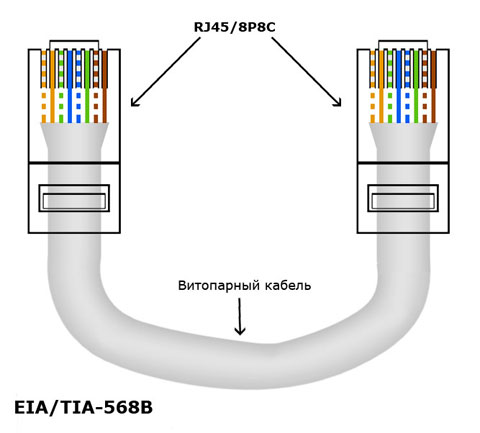
4. синий

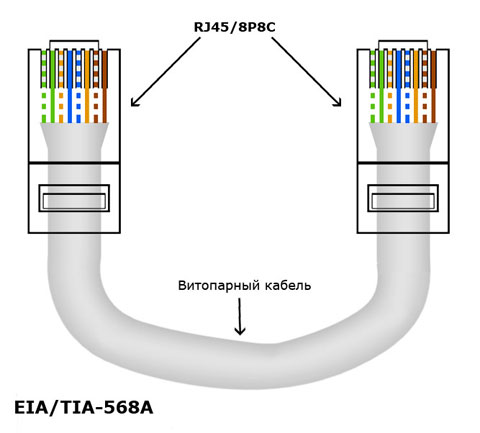
5. бело-синий

6. зеленый

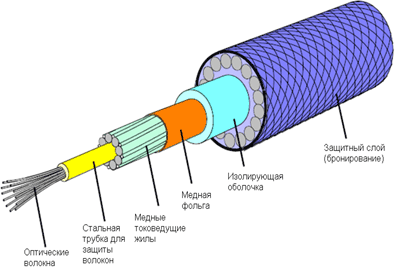
7. бело-коричневый

8. коричневый





1. **Кабельные среды передачи данных. Оптоволоконный кабель.**



В основе оптоволоконного кабеля находятся оптические волокна (световоды), данные по которым передаются в виде импульсов света. Электрические сигналы по оптоволоконному кабелю не передаются, поэтому сигнал нельзя перехватить, что практически исключает несанкционированный доступ к данным. Оптоволоконный кабель используют для транспортировки больших объемов информации на максимально доступных скоростях. Главным недостатком такого кабеля является его хрупкость: его легко повредить, а монтировать и соединять можно только с помощью специального оборудования.

1. **Беспроводные среды передачи данных** (дополнить).
   1. Радиоволны
   2. Микроволны
   3. Инфракрасные
2. **Устройства расширения сети и межсетевого взаимодействия. Повторители и концентраторы.**

Повторитель (рипитер) – это устройство служит для повторения сигналов, поступающее на его вход, также улучшает характеристики электрических сигналов и их синхронность

Концентратор (хабы) –многопортовый повторитель. Повторитель и концентратор работают на физическом уровне модели ОСИ. Суммарная пропускная способность входных каналов всегда выше чем у выходных каналов. Ядром концентратора является процессор. Для объединения входной информации чаще всего используется множественный доступ с разделением по времени. Образуют из отдельных отрезков кабеля общих сред передачи данных, которую называют Логический сегмент (Domen Collision)

1. **Устройства расширения сети и межсетевого взаимодействия. Коммутаторы.**

Коммутатор (свич) – это устройство, осуществляющее выбор оного из возможных вариантов направления передачи. Невозможно хранить данные. При использовании свича скорость передачи данных должна быть одинаковой.

* 1. Обеспечение сквозной коммутации
  2. Наличие средств маршрутизации
  3. Поддержка простого протокола управления сетью, организация виртуальных сетей и ретрансляция блоков данных

1. **Устройства расширения сети и межсетевого взаимодействия. Маршрутизаторы**

Маршрутизатор (роутер) – работает на сетевом уровне модели ОСИ. Маршрутизатор понимает куда передает информацию. Могут фильтровать данные. Также могут объединять сети, имеющие различную архитектуру

1. **Устройства расширения сети и межсетевого взаимодействия. Мультиплексоры**

Мультиплексор – электронный коммутатор, который позволяет передавать по одной линии сразу несколько потоков данных – мультиплексирование.

* 1. Частотное – множественный доступ по частоте
  2. Разделение по времени (всех)
  3. Статическое разделение по времени (тех, кто передает)

1. **Устройства расширения сети и межсетевого взаимодействия. Ретрансляторы.**

Ретранслятор – беспроводные повторители

1. **Устройства расширения сети и межсетевого взаимодействия. Модемы**

Модем – устройство, позволяющее соединяться с аналоговыми линиями связи. Процесс преобразования аналогового сигнала в цифровой называют демодуляцией, обратно – модуляцией.

1. **Устройства расширения сети и межсетевого взаимодействия. Мосты**

Мост (Бридж) – ретрансляционная система, соединяющая каналы передачи данных. Работает на канальном уровне модели ОСИ. Делит общую среду передачи данных на логические сегменты. Во время передачи информации могут использоваться только два порта

1. **Технология xDSL.**

Технологии широкополосного доступа к сетевым услугам по существующей медной абонентской телефонной линии - xDSL - появились, по меркам информационных технологий, достаточно давно. В этом семействе объединены как симметричные, то есть имеющие одинаковую скорость приема и передачи, так и ассиметричные технологии, у которых скорость от абонента существенно ниже потока данных, поступающего к абоненту.

**Асимметричные технологии**

**ADSL** (Asymmetric Digital Subscriber Line -- асимметричная цифровая абонентская линия) предполагает доступ в Интернет с сохранением у пользователя телефонного номера и обеспечивает скорость "нисходящего" потока данных в пределах от 1,5 до 8 Мбит/с и скорость "восходящего" потока -- от 640 Кбит/с до 1,5 Мбит/с (в зависимости от реализации) на расстояние до 5,5 км по одной витой паре проводов диаметром 0,5 мм.

**VDSL** (Very High Bit-Rate Digital Subscriber Line -- сверхвысокоскоростная цифровая абонентская линия) - еще одна асимметричная технология, которая, впрочем, может работать и в симметричном режиме. В асимметричном режиме скорость "нисходящего" потока находится в пределах от 13 до 52 Мбит/с и "восходящего" -- от 1,5 до 2,3 Мбит/с по одной медной паре телефонных проводов; в симметричном режиме -- до 26 Мбит/с. Однако максимальное расстояние передачи данных для этой технологии -- 1300 м

**Симметричные технологии**

**HDSL** (High Bit-Rate Digital Subscriber Line -- высокоскоростная цифровая абонентская линия) со скоростями передачи данных до 2,048 Мбит/с по 4-проводной линии на расстояние порядка 3,5-4,5 км;

**HDSL2** - результат развития технологии HDSL, обеспечивает аналогичные HDSL характеристики, но по двум проводам.

**SDSL** - передает поток данных по двум проводам со скоростью до 2,048 Мбит/с на расстояние до 3 км.

**SHDSL** - симметричная технология, обеспечивающая скорость передачи данных до 2,312 Мбит/с по двум проводам и вдвое большую скорость по четырем. Причем дальность передачи данных может быть достаточно большой (до 10 км).

1. **Стеки протоколов. Стек TCP/IP.**

|  |  |
| --- | --- |
| 7 уровней модели ОСИ | TCP/IP |
| Прикладной | Прикладной  TFTP,FTP,HTTP,Сокеты,POP3,SMTP |
| Представительский |
| Сеансовый |
| Транспортный | Транспортный (TCP,UTP) |
| Сетевой | Межсетевой (IP,rarp,arp,icmp,igmp) |
| Канальный | Межсетевой интерфейс (Сетевые платы, IEEE, среда передачи данных) |

IP – это протокол, который обеспечивает обмен дейтаграммами (хранятся адреса) между узлами сети. Для определения локального адреса по IP адресу используется протокол ARP. Это протокол с возможностью широковещательного доступа одновременно ко всем узлам сети. Для определения IP по локальному адресу используется протокол RARP.

ICMP – Протокол управления сообщениями интернета – используется IP протоколами для формирования отчетов о переданной информации.

IGMP – протокол управления группами интернета, формирует информацию о группах, содержащихся на маршрутизаторе в локальной сети.

TCP – отвечает за надежную передачу данных от одного компьютера к другому. Создает сеанс установления соединения.

Сетевой порт – условное число, которое указывает, какому приложению предназначен пакет.

UDP – предназначен для отправки небольших объемов данных без установления соединения. Также используется приложениями, которые не требует подтверждения адресатом. Не гарантирует, что пакеты будут доставлены в правильном порядке.

1. **Стеки протоколов. Стек IPX/SPX.**

|  |  |
| --- | --- |
| 7 уровней модели ОСИ | IPX/SPX |
| Прикладной | SAP, NSP |
| Представительский |
| Сеансовый |
| Транспортный | SPX |
| Сетевой | IPX |
| Канальный |  |
| Физический |

IPX/SPX – разработала стек программа Novell, которая разработала ОС Netware. На физическом и канальном уровне – Ethernet, TokenRing, WIFI…

IPX – межсетевой обмен пакетами, применяется модулями перенаправления файлов

Выполняет функцию адресации, маршрутизации и переключения пакетов в процессе передачи данных. В 95% данные доставляются без ошибок

SPX – последовательный обмен пакетами, предназначен для установления диалога в течение сеанса. Гарантирует безошибочную доставку пакетов. Также используется для доступа к внутренним функциям управления сети

NSP – является протоколом взаимодействия сервера и рабочей станции. Реализует только архитектуру клиент-сервер.

SAP – позволяет корректировать данные о том, какие сервисные услуги имеются сейчас

NETBIOS/SMB – совместная разработка IBM и Microsoft. Состоит из трех уровней

1. **Стеки протоколов. Стек NETBIOS/SMB**

|  |  |
| --- | --- |
| 7 уровней модели ОСИ | NETBIOS/SMB |
| Прикладной | SMB |
| Представительский |
| Сеансовый | NetBios |
| Транспортный |
| Сетевой |
| Канальный |  |
| Физический |

Протокол NetBIOS – позволяет обеспечить сервис, не обладает способностью маршрутизации. Позволяет обмениваться дейтаграммами и устанавливать соединение

Протокол SMB – реализует сервис сообщений, сервис печати, файловый доступ, управление сессиями.

1. **Стеки протоколов. Стек OSI.**

Ой да тут дохуя …

1. **Иерархия сети Интернет. ISP классификация.**

ЩИТО!!!?????

1. **Адресация сетей. Обзор IPv4, IPv6**

IPv4 — четвёртая версия IP-протокола, первая широко используемая версия. Протокол описан в RFC 791.

IPv4 использует 32-битные (четырёхбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами.

Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, 192.168.0.1. (или 128.10.2.30 — традиционная десятичная форма представления адреса)

10.0.0.0/8 Для использования в частных сетях.

127.0.0.0/8 Подсеть для коммуникаций внутри хоста (см.: localhost)

192.168.0.0/16 Для использования в частных сетях.

Уже в 1980-е годы стало очевидно, что распределение адресного пространства происходит значительно более быстрыми темпами, чем было заложено в архитектуру IPv4. Это привело сначала к появлению классовой адресации, позднее бесклассовой адресации, и в конечном итоге к разработке нового протокола IPv6.

В феврале 2011 года IANA выделила 5 последних блоков адресов RIRам. Блоки свободных IP-адресов начали заканчиваться у региональных регистраторов с 2011 года.

Короче он заканчивается и мы переходим на IPv6.

**IPv6**

IPv6 — новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в интернете, за счёт использования длины адреса 128 бит вместо 32.

Иногда утверждается, что новый протокол может обеспечить по 5·1028 адресов на каждого жителя Земли. Однако такое огромное адресное пространство IPv6 было введено ради иерархичности адресов (это упрощает маршрутизацию) и бо́льшая его часть в принципе не будет задействована никогда. Тем не менее, увеличенное пространство адресов сделает NAT необязательным.

Из IPv6 убраны функции, усложняющие работу маршрутизаторов:

* Маршрутизаторы больше не разбивают пакет на части (возможно разбиение пакета с передающей стороны). Соответственно, оптимальный MTU придётся искать через Path MTU discovery. Для лучшей работы протоколов, требовательных к потерям, минимальный MTU поднят до 1280 байт. Информация о разбиении пакетов вынесена из основного заголовка в расширенные.
* Исчезла контрольная сумма. С учётом того, что канальные (Ethernet) и транспортные (TCP и UDP) протоколы тоже проверяют корректность пакета, контрольная сумма на уровне IP воспринимается как излишняя. Тем более каждый маршрутизатор уменьшает hop limit на единицу, что в IPv4 приводило к пересчёту суммы.

Несмотря на огромный размер адреса IPv6, благодаря этим улучшениям заголовок пакета удлинился всего лишь вдвое: с 20 до 40 байт.

Улучшения IPv6 по сравнению с IPv4:

* В сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) — до 4 гигабайт;
* Time to Live переименовано в Hop Limit;
* Появились метки потоков и классы трафика;
* Появилось многоадресное вещание;

1. **Адресация сетей. Типы адресов.**
2. **Адресация сетей. Классовая адресация сетей.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 0 | 8 | 16 | 24 | 32 |
| A | 0 | Сеть | Узел |  |  |
| B | 10 | Сеть | | Узел |  |
| C | 110 | Сеть | | | Узел |
| D | 1110 | Групповая среда | | | |
| E | Резерв | | | | |

A 0

B 10

C 110

D 1110

E 11110

|  |  |  |  |
| --- | --- | --- | --- |
|  | Диапазон | Кол-во сетей | Кол-во узлов |
| A | 1-126 | 126 | 16777214 |
| B | 128-191 | 16382 | 65534 |
| C | 192-223 | 2097150 | 255 |
| D | 224-239 | - | 2….28 |
| E | 240-247 | - | 2….27 |

1. **Адресация сетей. Бесклассовая адресация сетей (CIDR)**

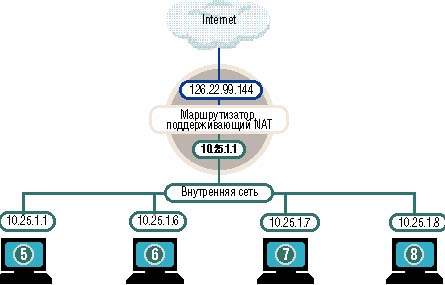
Метод адресации, который позволяет рационально управлять пространством IP-адресов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **P/маска** | **До последнего IP**  **в подсети** | **Маска** | **Количество адресов** | **Класс** |
| a.b.c.d**/32** | +0.0.0.0 | 255.255.255.255 | 1 | 1/256 C |
| a.b.c.d**/31** | +0.0.0.1 | 255.255.255.254 | 2 | 1/128 C |
| a.b.c.d**/30** | +0.0.0.3 | 255.255.255.252 | 4 | 1/64 C |
| a.b.c.d**/29** | +0.0.0.7 | 255.255.255.248 | 8 | 1/32 C |
| a.b.c.d**/28** | +0.0.0.15 | 255.255.255.240 | 16 | 1/16 C |
| a.b.c.d**/27** | +0.0.0.31 | 255.255.255.224 | 32 | 1/8 C |
| a.b.c.d**/26** | +0.0.0.63 | 255.255.255.192 | 64 | 1/4 C |
| a.b.c.d**/25** | +0.0.0.127 | 255.255.255.128 | 128 | 1/2 C |
| a.b.c.0**/24** | +0.0.0.255 | 255.255.255.000 | 256 | 1 C |
| a.b.c.0**/23** | +0.0.1.255 | 255.255.254.000 | 512 | 2 C |
| a.b.c.0**/22** | +0.0.3.255 | 255.255.252.000 | 1024 | 4 C |
| a.b.c.0**/21** | +0.0.7.255 | 255.255.248.000 | 2048 | 8 C |
| a.b.c.0**/20** | +0.0.15.255 | 255.255.240.000 | 4096 | 16 C |
| a.b.c.0**/19** | +0.0.31.255 | 255.255.224.000 | 8192 | 32 C |
| a.b.c.0**/18** | +0.0.63.255 | 255.255.192.000 | 16 384 | 64 C |
| a.b.c.0**/17** | +0.0.127.255 | 255.255.128.000 | 32 768 | 128 C |
| a.b.0.0**/16** | +0.0.255.255 | 255.255.000.000 | 65 536 | 256 C = 1 B |
| a.b.0.0**/15** | +0.1.255.255 | 255.254.000.000 | 131 072 | 2 B |
| a.b.0.0**/14** | +0.3.255.255 | 255.252.000.000 | 262 144 | 4 B |
| a.b.0.0**/13** | +0.7.255.255 | 255.248.000.000 | 524 288 | 8 B |
| a.b.0.0**/12** | +0.15.255.255 | 255.240.000.000 | 1 048 576 | 16 B |
| a.b.0.0**/11** | +0.31.255.255 | 255.224.000.000 | 2 097 152 | 32 B |
| a.b.0.0**/10** | +0.63.255.255 | 255.192.000.000 | 4 194 304 | 64 B |
| a.b.0.0**/9** | +0.127.255.255 | 255.128.000.000 | 8 388 608 | 128 B |
| a.0.0.0**/8** | +0.255.255.255 | 255.000.000.000 | 16 777 216 | 256 B = 1 A |
| a.0.0.0**/7** | +1.255.255.255 | 254.000.000.000 | 33 554 432 | 2 A |
| a.0.0.0**/6** | +3.255.255.255 | 252.000.000.000 | 67 108 864 | 4 A |
| a.0.0.0**/5** | +7.255.255.255 | 248.000.000.000 | 134 217 728 | 8 A |
| a.0.0.0**/4** | +15.255.255.255 | 240.000.000.000 | 268 435 456 | 16 A |
| a.0.0.0**/3** | +31.255.255.255 | 224.000.000.000 | 536 870 912 | 32 A |
| a.0.0.0**/2** | +63.255.255.255 | 192.000.000.000 | 1 073 741 824 | 64 A |
| a.0.0.0**/1** | +127.255.255.255 | 128.000.000.000 | 2 147 483 648 | 128 A |
| 0.0.0.0**/0** | +255.255.255.255 | 000.000.000.000 | 4 294 967 296 | 256 A |

1. **Адресация сетей. Преобразование сетевых адресов (NAT)**

Преобразование сетевых адресов (Network Address Translation - NAT) - это метод определения соответствия IP-адресов между разными адресными пространствами (например, между частной сетью intranet и общедоступной Internet).

В условиях продолжающего экспоненциально расширяться Internet присваивание "хороших", то есть уникальных в глобальном смысле сетевых адресов частным сетям стало считаться непроизводительной тратой ценных виртуальных ресурсов. В соответствии со стандартом Network Address Translation определенные IP-адреса выделены для параллельного использования в частных сетях и в общедоступной сети.

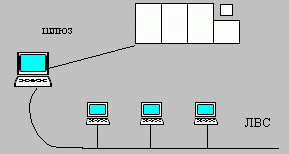


1. **Физическая адресация. Mac – адрес, MAC – адрес широковещательной рассылки** (дополнить).

Физический (MAC) - представляется в 16-ой системе, состоит из 6 байт. Первые 3 числа – идентификатор производителя, остальные 3 числа – идентификатор устройства

1. **Назначения шлюза**

Шлюзы - это устройства, которые обеспечивают связь между различными архитектурами и средами. Главное их назначение - осуществить связь между ПК и средой мини-компьютеров или мейнфреймов (рис. ниже).



Обычно роль шлюзов в ЛВС выполняют выделенные сервера, а все остальные рабочие станции ЛВС работают с мейнфреймом также просто, как со своими ресурсами. Шлюз связывает две системы, которые используют разные:

* коммуникационные протоколы;
* структуры и форматы данных;
* языки и архитектуры.

1. **DHCP серверы**
2. **Служба доменных имен DNS** (дополнить).

DNS-имя – символьное имя.

Виды адресов:

1. Индивидуальный – назначается одному сетевому интерфейсу (устройству), расположенному в одной подсети. Подключение точка-точка.

2. Групповой – назначается одному или нескольким сетевым интерфейсам в различных подсетях. Тип подключения точки-многие-точки

3. Широковещательный – назначается всем сетевым интерфейсам (устройствам), расположенным в подсети. Тип подключения точки-все точки подсети

1. **Типы беспроводных сетей. WPAN, WLAN, WWAN.**
2. **Межсетевые экраны.**
3. **Диагностические утилиты TCP/IP. Ping. Tracert. Netstat. Nslookup**

**Ping** — утилита для проверки соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса.

Пример: ping ya.ru

**Tracert** (кроме windows — traceroute) — утилита для определения маршрутов следования данных в сетях TCP/IP.

Traceroute может использовать разные протоколы передачи данных в зависимости от операционной системы устройства. Такими протоколами могут быть UDP, TCP, ICMP или GRE. Компьютеры, с установленной операционной системой Windows используют ICMP протокол, при этом маршрутизаторы Cisco — протокол UDP.

**Netstat** — утилита для отображения статистики протокола и текущих подключений TCP/IP.

Отображает активные подключения TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6).

**Nslookup** — интерактивная утилита для обращения к DNS-серверам.

Позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера.

1. **Протокол Telnet.**

TELNET — сетевой протокол для реализации текстового интерфейса по сети (в современной форме — при помощи транспорта TCP).

Выполняет функции протокола прикладного уровня модели OSI.

Назначение протокола TELNET в предоставлении достаточно общего, двунаправленного, восьмибитного байт-ориентированного средства связи. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

1. **Типы глобальных сетей. Х.25.**

Сети Х.25 являются на сегодняшний день "старейшиной" применяемых пакетных сетей, хотя популярность их быстро падает. Стандарт Х.25 был разработан комитетом CCITT в 1974 году. Стандарт наилучшим образом подходит для передачи трафика низкой интенсивности, характерного для терминалов, и в меньшей степени соответствует более высоким требованиям трафика локальных сетей.

Сеть Х.25 состоит из коммутаторов (Switches, S), расположенных в различных географических точках и соединенных высокоскоростными выделенными каналами.

Стандарты сетей Х.25 описывают три уровня протоколов.

* На физическом уровне определены синхронные интерфейсы Х.21 и Х.21 bis к оборудованию передачи данных - либо DSU/CSU, если выделенный канал является цифровым, либо к синхронному модему, если канал аналоговый.
* На канальном уровне используется подмножество протокола HDLC, обеспечивающих возможность автоматической передачи в случае возникновения ошибок в линии.
* На сетевом уровне определен протокол Х.25/3 обмен пакетами между оконечным оборудованием и сетью передачи данных.

1. **Типы глобальных сетей. Frame Relay.**

Сети frame relay - сравнительно новые сети, которые гораздо лучше подходят для передачи пульсирующего трафика локальных сетей по сравнению с сетями Х.25. Преимущество сетей frame relay заключается в их низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежную передачу кадров технология frame relay не обеспечивает. Сети frame relay специально разрабатывались как общественные сети для соединения частных локальных сетей. Они обеспечивают скорость передачи данных до 2 Мбит/с.

Услуги frame relay обычно предоставляются теми же операторами, которые эксплуатируют сети Х.25. Большая часть производителей выпускают сейчас коммутаторы, которые могут работать как по протоколам Х.25, так и по протоколам frame relay. Технология frame relay начинает занимать в территориальных сетях с коммутацией пакетов ту же нишу, которая заняла в локальных сетях технология Ethernet. Надо отметить, что полезная пропускная способность прикладных протоколов при работе через сети frame relay будет зависеть от качества каналов и методов восстановления пакетов на уровне стека, расположенного над протоколом frame relay.

Сети frame relay следует применять только при наличии на магистральных каналах волоконно-оптических кабелей высокого качества.