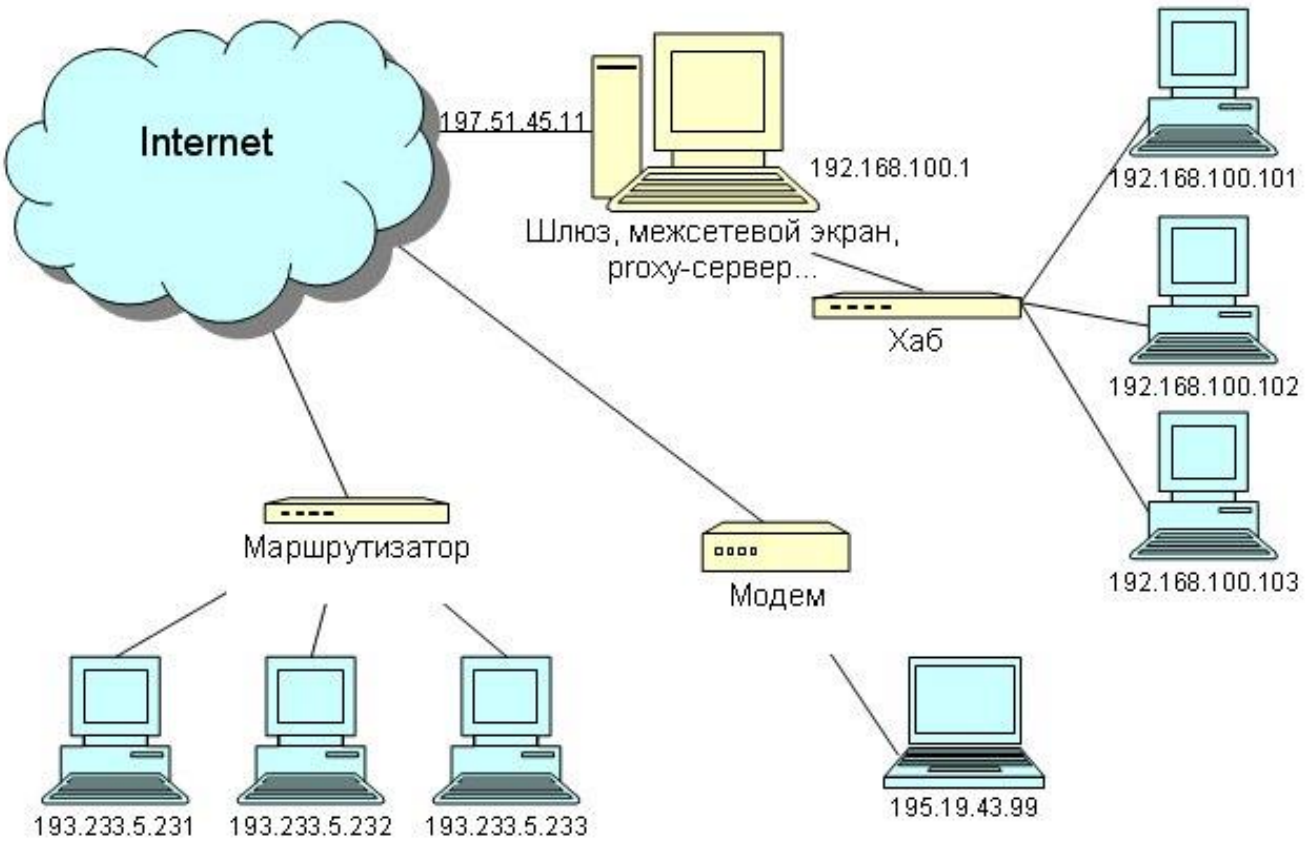
1. Определения компьютерной сети. Обобщенная схема функционирования сети.

Компьютерная сеть – структура объединяющая компьютеры между собой.



На этом рисунке 3 подсети.

В одной ПК подключены к маршрутизатору, во второй к модему, в третьей к хабу, который подключен к шлюзу. Все 3 подсети имеют доступ в интернет

2. Компьютерная сеть (определение, назначение, цель использование, виды). Предпосылки и причины появления сетей.

Определение:
Компьютерная сеть – структура объединяющая компьютеры между собой.

Назначения:
Совместное использование ресурсов.

Виды:
по территории:
1. LAN – локальные
2. WAN – глобальные
3. MAN – городские (региональные)

по архитектуре:
1. клиент-сервер
2. одноранговые

по скорости передачи данных:
1. низкоскоростные (до 10 Мбит/с)
2. среднескоростные (до 100 Мбит/с)
3. высокоскоростные (выше 100 Мбит/с)

по топологии:
общая шина, кольцо, звезда, смешанная, полносвязная, древовидная.

Предпосылки появления КС:
В 50х-60х годах появились терминалов, имеющих полноценные устройства ввода-вывода и работающие напрямую с одним общим компьютером. Именно тогда стали появляться первые сети, чей принцип работы заключался лишь в физическом удалении терминалов на определенные расстояния.
Как только начали появляться более компактные компьютеры – это произошло в 70-х годах, позволить себе их установку могли все больше предприятий, поэтому необходимость использования какого-либо средства связи возрастала и тогда возникли первые приближенные к современным способы объединения компьютеров в сеть и потребность в монтаже компьютерных сетей.
В 1969 году минобороны США приняло решение об объединении всех основных компьютерных узлов в общую сеть. Передача данных осуществлялась между ними по коммутируемому кабелю, а для ее осуществления были созданы специальные операционные системы и огромное количество сложных сопутствующих протоколов.
Краткая история развития компьютерных сетей:
1950-1960 годы – первые попытки объединения мейнфрейма с терминалами.
1969 – появление APRANET и использование телефонных сетей для передчи данных.
1970-1974 – возникновение мини-компьютеров и создание вручную настраиваемых локальных сетей.
1974 появление первой стандартизованной сетевой архитектуры IBM SNA, а также стандартизация X.25
1980-1985 возникновение персональных компьютеров, появление Интернета в близком к современности виде. Использование стека TCP/IP на всех узлах. Возникновение стандартных технологий локальных сетевых протоколов Ethernet, FDDI, Token Ring.
1986-1987 – старт коммерческого использования Интернета.
1991 появление протокола Web и первых интернет-сайтов.
1995-2000 развитие Web и массовая популяризация компьютеров.
2000-2010 – использование беспроводных сетей, снижение стоимости передачи единицы информации сразу в несколько тысяч раз.

3. Требования, предъявляемые к современным вычислительным сетям. Проблемные ситуации, возникающие в различных типах сетей, методы и средства их решения.

4. Производительность, надежность и безопасность компьютерных сетей. Расширяемость и масштабируемость компьютерных сетей. Управляемость и совместимость компьютерных сетей.

Совпали.

Требования:

производительность
надежность
безопасность
маштабируемость
управляемость
совместимость

Производительность:
Время реакции – время между возникновение запроса и получением ответа.
Пропускная способность – кол-во информации переданной через сеть в ед. времени. Определяется в битах в секунду.

Надежность:
Доля потерянных пакетов
Доступность – доля времени, в течении которого сеть работала.
Отказоустойчивость – отказ какого-то элемента не приводит к полному отказу сети.

Безопасность – способность сети обеспечить защиту информации от несанкционированного доступа.

Маштабируемость – возможность расширения сети без существенного снижения производительности.
Расширяемость – просто возможность добавить в сеть новых абонентов (ПК)

Управляемость:
Возможность управлять сетью с любого эл. сети.
Возможность определения проблем в работе сети.

Совместимость:
сеть способна включать в себя самое разнообразное ПО и обородувание (различные ОС, поддерживающие разные стеки протоколов)

5. Классификация, характеристики компьютерных сетей. Локальные, корпоративные, региональные и глобальные компьютерные сети.

Классификация компьютерных сетей:

1. по территории:

1.1. LAN – локальные – объед. абонентов, расположенных в пределах небольшой территории. Обычно не более 300 м.

1.2. WAN – глобальные – объед. абонентов, расположенных в различных странах, на различных континентах.

1.3. MAN – городские (региональные) – объед. абонентов, расположенных на значительном расстоянии друг от друга, например в большом городе. Обычно расстояние десятки-сотни км.

При этом локальная сеть может быть частью региональное, региональная – частью глобальной, а глобальные также могут образовывать друг с другом сложные структуры.

2. по топологии:
общая шина, кольцо, звезда, смешанная, полносвязная, древовидная.

Корпоративные сети (ККС) – сети масштаба предприятия, корпорации.

6. Особенности построения и функционирования компьютерных сетей. Конвергенция компьютерных сетей.

В общем случае КС представляет собой совокупность вложенных друг в друга подсистем:
сеть рабочих станций
сеть серверов
базовая сеть передачи данных

Рабочая станция – компьютер, за которым работает абонент сети.
Сервер – компьютер, выполняющий общие задачи сети и предоставляющий услуги рабочим станциям.
Базовая сеть передачи данных – совокупность средств передачи данных между серверами. Состоит из каналов и узлов связи.

Конвергенция КС:
В конце 80х годов отличия между LAN и WAN были весьма отчетливы:
протяженность и качество линий связи
LAN имели небольшую протяженность между узлами сети, поэтому использовались более качественные линии связи.
Сложность методов передачи данных
В WAN требовались более сложные методы передачи данных.
Скорость обмена данными
LAN: 10-100 Мбит/с
WAN: 2 Кбит/с – 2 Мбит/с
Разнообразие услуг
LAN: использование файлов, хранящихся на других компьютерах, совместное использование принтеров, модемов, факсов…
WAN: почтовые и файловые услуги в их простейшем виде.

Постепенно различия между ними стали сглаживаться. LANs начали объединяться друг с другом, в качестве связующей среды использовали WANs.

Большой вклад в сближение внесло доминирование протокола IP. Сегодня этот протокол работает поверх любых технологий LANs и WANs, объединяя различные подсети в совместную сеть.

Начиная с 90х годов WANs значительно расширили спектр услуг и догнали LANs.
1991 г. – появление Web (www)

Также еще один признак сближения это появление городских сетей (MANs)

И, наконец, появляются новые технологии предназначенные и для LANs, и для WANs.
Пример: семейство технологий Ethernet.

7. Понятие протокола и применение сетевых протоколов для взаимодействия объектов сети.

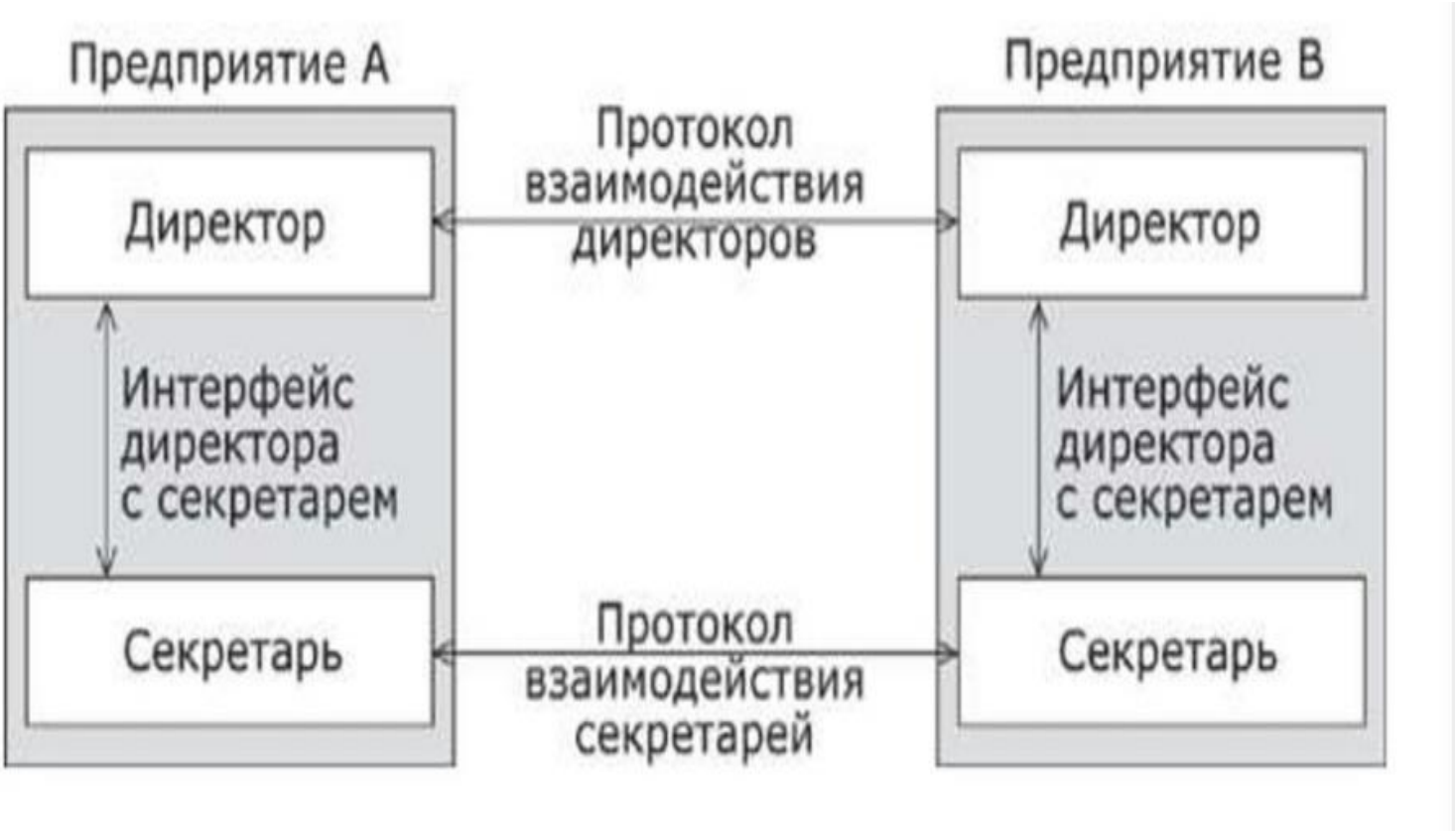
Сетевой протокол – набор правил, позволяющий осуществлять соединения и обмен данными между двумя и более включенными в сеть устройствами.

Протокол – правило, определяющее состав пакета и последовательность действий на соответствующем уровне.

Стек протоколов – совокупность протоколов нескольких уровней.

Интерфейс – способ передачи данных с уровня на уровень.

Наглядный пример:



8. Основные принципы построения сети. Многоуровневый подход к решению задачи обмена сообщениями между компьютерами.

Организация взаимодействия между устройствами сети является сложной задачей. Для её решения используется декомпозиция, т.е. разбиение одной задачи на несколько задач-модулей.

Декомпозиция состоит в четком определении функций каждого модуля.

Многоуровневый подход:

всё множество модулей разбиваются на группы и упорядочиваются по уровням, образующим иерархию.
для каждого промежуточного уровня можно указать примыкающие к нему верхний и нижний уровни.
группа модулей на каждом уровне для выполнения своих задач обращаются с запросами только к модулям соседнего нижележащего уровня.
результаты работы всех модулей на уровне могут быть переданы только модулям соседнего вышележащего уровня.

9. Основные понятия о протоколе. Стек протоколов. Модель OSI.
Протокол – правило, определяющее состав пакета и последовательность действий на соответсвующем уровне.
Стек протоколов – совокупность протоколов нескольких уровней.
Интерфейс – способ передачи данных с уровня на уровень.
Модель OSI – модель взаимодействия открытых систем.
Является стандартом передачи данных, позволяющий системам различных производителей устанавливать сетевые соединения.

Состоит из 7 уровней.
Каждый уровень существует как независимый модуль, можно заменить один протокол на другой на любом уровне без какого-либо влиянию на работу других уровней.
Уровни.
7. Прикладной
6. Представления
5. Сеансовый
4. Транспортный
3. Сетевой
2. Канальный
1. Физический

Физический уровень
Передача битов по каналам связи.

Канальный
Передача кадров между узлами, находящимися в том же сегменте сети.
Кадр выглядит так: MAC-адрес первого ПК, MAC-адрес второго ПК, данные.
Получение доступа к разделяемой среде.
Проверка целостности данных.

Сетевой
Маршрутизация
Таблица маршрутизации указывает: сеть назначения, след. узел, метрика(стоимость)
Адресация
Опред. кратчайшего пути
Проверка целостности данных

Транспортный
Обеспечивает надежную передачу данных от отправителя к получателю.
Сеансовый
Поддержка сеансов связи.
Передача сообщений.

Представления
Трансляция символов между стандартами кодировки.
Конвертирование данных.
Сжатие данных.
Шифрование данных.

Прикладной
Обеспечивает взаимодействие пользовательских приложений с сетью.

10. Классификация локальных вычислительных сетей, разделяемая среда передачи данных.

Классификация ЛВС:

. по управлению
. сети рабочих групп
. сети отделов
исп. небольшой группой сотрудников, работающих в одном отделе.
сети кампусов
их назначение объединять несколько мелких сетей в одну, т.е. обеспечить взаимодействие между сетями отделов.
. корпоративные сети
сети масштаба всего предприятия

. по назначению
. вычислительные (выполняют расчёты)
. информационно-вычислительные (расчёты и облуж. пользователей)
информационные (обслуж. пользователей: создание док-ов)
. информационно-поисковые (поиск инфы в сетевых хранилищах)
. информационно-советующие (дают советы, исходя из статистики)
информационно-управляющие

Разделяемая среда.
Разделение – совместное использование.

Существует 2 подхода:
1 подход: централизованный – доступом управляет спец. устройство (звезда)
2 подход: децентрализованный (общая шина)

11. Сети с централизированным управлением, иерархические сети: одноранговые и с выделенным сервером (сравнительный анализ, области применения).

Сети с централизированным управлением (с выделенным сервером)

В сети с централизованным управлением выделяются одна или несколько машин, управляющих обменом данными по сети. Диски выделенных машин, которые называются файл-серверами, доступны всем остальным компьютерам сети.

Остальные компьютеры называются рабочими станциями. Рабочие станции имеют доступ к дискам файл-сервера и совместно используемым принтерам, но и только. С одной рабочей станции вы не сможете работать с дисками других рабочих станций.

С одной стороны, это хорошо, так как пользователи изолированы друг от друга и не могут случайно повредить чужие данные.

С другой стороны, для обмена данными пользователи вынуждены использовать диски файл-сервера, создавая для него дополнительную нагрузку.

Однако, специальные программы, работающие в сети с централизованным управлением и позволяющие передавать данные непосредственно от одной рабочей станции к другой минуя файл-сервер.

Одноранговые сети (децентраливонные)

Часто в такой сети отсутствуют выделенные серверы, а каждый узел является как клиентом, так и выполняет функции сервера. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов.

Сравнительный анализ

Одноранговая сеть позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов, но при этом производительность на порядок меньше.

В сетях же с выделенными серверами при выходе сервера из строя вся сеть останется нерабочей.

Преимущество сети с выделенным сервером заключается в применении более мощных серверных аппаратных средств, за счет чего повышается эффективность доступа к ресурсам сети.

Лучшим образом проявляет себя сеть с выделенным сервером в плане масштабируемости.

12. Понятие топологии при построении компьютерных сетей. Логическая и физическая топологии сети.

Топология - это физическая конфигурация сети в совокупности с ее логическими характеристиками.

Топология - это стандартный термин, который используется при описании основной компоновки сети. Если понять, как используются различные топологии, то можно будет определить, какими возможностями обладают различные типы сетей.
Существует два основных типа топологий:
физическая
логическая

Логическая топология описывает правила взаимодействия сетевых станций при передаче данных.
Физическая топология определяет способ соединения носителей данных.
Термин "топология сети" характеризует физическое расположение компьютеров, кабелей и других компонентов сети. Топология сети обуславливает ее характеристики.

Виды топологий

Существуют основные топологии:

общая шина
кольцо
звезда

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля. Общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети.
В случае топологии Общая шина кабель используется всеми станциями по очереди.
Кольцо – это топология ЛВС, в которой каждая станция соединена с двумя другими станциями, образуя кольцо. Данные передаются от одной рабочей станции к другой в одном направлении (по кольцу). Каждый ПК работает как повторитель, ретранслируя сообщения к следующему ПК, т.е. данные, передаются от одного компьютера к другому как бы по эстафете.

Звезда – это топология ЛВС, в которой все рабочие станции присоединены к центральному узлу (например, к хабу), который устанавливает, поддерживает и разрывает связи между рабочими станциями. Преимуществом такой топологии является возможность простого исключения неисправного узла. Однако, если неисправен центральный узел, вся сеть выходит из строя.

13. Коммутация, мультиплексирование и демультиплексирование.

Коммутация - "переброска" данных с одного своего порта на другой.

В самом общем виде задача **коммутации** — задача соединения конечных узлов через сеть транзитных узлов.

Прежде чем выполнить переброску данных на определенные для них интерфейсы, коммутатор должен понять, к какому потоку они относятся. Эта задача должна решаться независимо от того, поступает ли на вход коммутатора только один поток в "чистом" виде, или "смешанный" поток, который объединяет в себе несколько потоков. В последнем случае к задаче распознавания добавляется задача демультиплексирования.

Задача мультиплексирования — образование из нескольких отдельных потоков общего потока, который можно передавать по одному физическому каналу связи — задача “смешивание”.

Задача демультиплексирования — разделение потока, поступающего на один интерфейс, на несколько составляющих потоков — задача “разделения”.

Существует множество способов мультиплексирования потоков в одном физическом канале, и важнейшим из них является разделение времени. При этом способе каждый поток время от времени (с фиксированным или случайным периодом) получает в свое распоряжение физический канал и передает по нему данные.

14. Топология шина, особенности реализации, коллизия, разделение передающей среды, надежность, безопасность, стоимость реализации.

Общая шина – это тип сетевой топологии, в которой рабочие станции расположены вдоль одного участка кабеля.

Особенности реализации:
Общая шина предполагает использование одного кабеля, к которому подключаются все компьютеры сети.
В случае топологии Общая шина кабель используется всеми станциями по очереди.

1. ПК-отправитель проверяет свободна ли сеть.
2. Если свободна, то начинает передачу данных.
3. Если занята, то ждет случайное время и переходит к шагу 1.
4. Данные, отправленные в сеть, получает все одновременно.
5. Только получатель отвечает на эти данные по такому же алгоритму.

Разделение передающей среды:
Технология TDM, т.е. выделяется каждому на определенный промежуток времени.

“Общая шина” получила огромное распространение из-за дешевизны.
Но КПД этой сети 30%.

В топологии «шина» отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность, т.к. если выйдет из строя 1 ПК, ничего не произойдет.

Для сетей, построенных на основе данной топологии, характерна низкая безопасность, так как информация на каждом компьютере может быть доступна с любого другого компьютера.

Коллизии – “столкновение пакетов”.
Такое происходит, когда неск. ПК одновременно проверяют, свободна ли сеть, если свободная, они оба начинают передавать данные. Коллизии распространяются лавинообразно. В итоге сеть будет не доступна.

15. Передающая среда для построения сети по топологии звезда, ограничения, стоимость и безопасность реализации сети.

При использовании топологии типа **звезда** информация между клиентами сети передается через единый центральный узел. В качестве центрального узла может выступать сервер или специальное устройство – **концентратор (хаб).**

Данные от передающей станции сети передаются через хаб по всем линиям связи всем ПК. Информация поступает на все рабочие станции, но принимается только теми станциями, которым она предназначается.

Преимущества сетей топологии звезда:
сеть устойчива к неисправностям отдельных ПК и к разрывам соединения отдельных ПК.
отсутствие коллизий

Недостатки сетей топологии звезда:
отказ хаба влияет приводит к отказу сети
большой расход кабеля. Высокая стоимость.
ограничение числа абонентов.
ограничение длины кабеля.

16. Особенности реализации топологии кольцо, стоимость и безопасность.

При топологии типа **кольцо** все компьютеры подключаются к линии, замкнутой в кольцо. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер.

Передача информации в такой сети происходит следующим образом:

Маркер (специальный сигнал) последовательно, от одного компьютера к другому, передается до тех пор, пока его не получит тот, которому требуется передать данные. Получив маркер, компьютер создает так называемый "пакет", в который помещает адрес получателя и данные, а затем отправляет этот пакет по кольцу. Данные проходят через каждый компьютер, пока не окажутся у того, чей адрес совпадает с адресом получателя.

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

Преимущества топологии типа кольцо состоят в следующем:

1. Не требует серьёзных расходов на кабель. Сетевой шнур нужен лишь для прокладки от одного компьютера к другому. Не высокая стоимость.
2. Протяженность сети может быть значительной. Т.е. компьютеры могут подключаться к друг к другу на значительных расстояниях, без использования специальных усилителей сигнала.

К недостаткам данной топологии относятся:

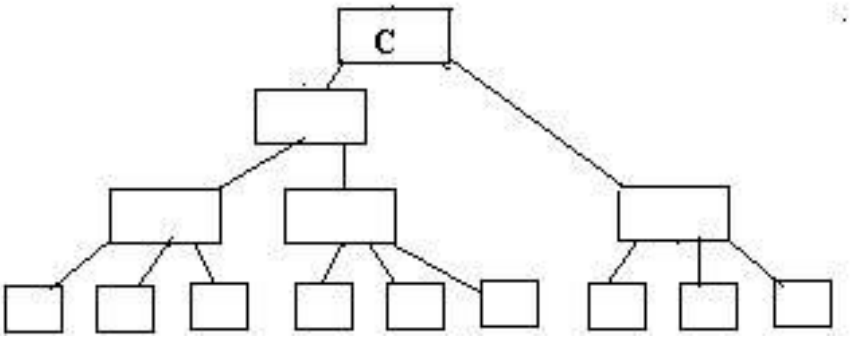
1. Низкая надежность сети, так как отказ любого компьютера влечет за собой отказ всей системы.
2. Для подключения нового клиента необходимо отключить работу сети.
3. При большом количестве клиентов скорость работы в сети замедляется, так как вся информация проходит через каждый компьютер, а их возможности ограничены.
4. Общая производительность сети определяется производительностью самого медленного компьютера.

17. Сотовая, полносвязная, древовидная и петлевая топологии, как производные топологии, основанные на трех базовых.

Сотовая топология – топология компьютерной сети, в которой каждая рабочая станция сети соединяется со всеми другими или многими рабочими станциями этой же сети.
Высокая надежность. Высокая стоимость(избыточное количество кабеля).

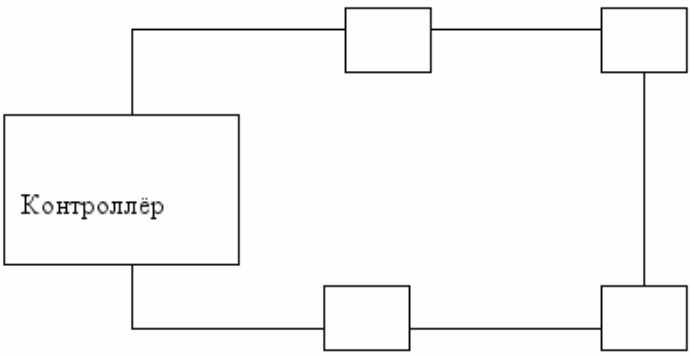
Полносвязная топология – топология компьютерной сети, в которой каждая рабочая станция сети соединяется со всеми другими или многими рабочими станциями этой же сети.
Высокая надежность. Высокая стоимость(избыточное количество кабеля).

Древовидная топология:



Дерево — это топология сетей, в которой каждый узел более высокого уровня связан с узлами более низкого уровня звездообразной связью, образуя комбинацию звезд. Также дерево называют иерархической звездой.

Отказ одного компьютера приводит к отказу одной ветви.
Также деревья могут быть как активными, так и пассивными. В активных деревьях в качестве узлов используют компьютеры, в пассивных — коммутаторы.
Петлевая топология. Все узлы соединены друг с другом в кольцо, но один из них управляет остальными и определяет, какой из узлов должен использовать канал связи (Рис 4).



18. Многоуровневая модель OSI, модель и взаимодействие протоколов. Стеки протоколов. Примеры протоколов.

Модель OSI

Обмен информацией между компьютерами, объединенными в сеть, очень сложная задача. Это связано с тем, что существует много производителей аппаратных и программных средств вычислительных систем. Единственный выход — унифицировать средства сопряжения систем. В 1984г. Международная Организация по Стандартизации (ISO) представила индустриальный стандарт — *модель взаимодействия открытых систем* (Open System Interconnection Reference Model — OSI/RM), чтобы помочь поставщикам создавать совместимые сетевые аппаратные и программные средства. В соответствии с этой моделью выделяются следующие уровни: физический, канальный, сетевой, транспортный, сеансовый, представительский, прикладной. В соответствии с эталонной моделью OSI эти уровни взаимодействуют друг с другом. Таким образом, сложная задача обмена информацией между компьютерами в сети разбивается на ряд относительно независимых и менее сложных подзадач *взаимодействия между смежными уровнями*. Два самых низших уровня — физический и канальный — реализуются аппаратными и программными средствами, остальные пять более высоких уровней реализуются, как правило, программными средствами.

Физический уровень

Этот уровень определяет механические, электрические, процедурные и функциональные характеристики установления, поддержания и размыкания физического соединения между конечными системами. Физический уровень определяет такие характеристики соединения, как уровни напряжений, синхронизацию и физическую скорость передачи данных и т.д.

Канальный уровень

Канальный уровень (уровень звена данных, информационно-канальный уровень) отвечает за надежную передачу данных через физический канал, а именно: обеспечивает физическую адресацию; обеспечивает обнаружение ошибок в передаче и восстановление данных; отслеживает топологию сети и обеспечивает дисциплину использования сетевого канала конечной системой; обеспечивает уведомление о неисправностях; обеспечивает упорядоченную доставку блоков данных и управление потоком информации.

Сетевой уровень

Этот уровень обеспечивает возможность соединения и выбор маршрута между двумя конечными системами, подключенными к разным подсетям, которые могут быть разделены множеством подсетей и могут находиться в разных географических пунктах. Протоколы маршрутизации позволяют сети из маршрутизаторов выбирать оптимальные маршруты через связанные между собой подсети.

Транспортный уровень

Транспортный уровень обеспечивает высшим уровням услуги по транспортировке данных, а именно: обеспечивает надежную транспортировку данных через объединенную сеть; обеспечивает механизмы для установки, поддержания и упорядоченного завершения действия виртуальных каналов; обеспечивает обнаружение и устранение неисправностей транспортировки; следит за тем, чтобы конечная система не была перегружена слишком большим количеством данных.

Сеансовый уровень

Сеансовый уровень реализует установление, поддержку и завершение сеанса взаимодействия между прикладными процессами абонентов. Сеансовый уровень синхронизирует диалог между объектами представительного уровня , определяет точки синхронизации для промежуточного контроля и восстановления при передаче файлов

Представительный уровень

Представительный уровень определяет синтаксис, форматы и структуры представления передаваемых данных. Для того, чтобы информация, посылаемая из прикладного уровня одной системы, была читаемой на прикладном уровне другой системы.

Прикладной уровень

В отличие от других уровней прикладной уровень — самый близкий к пользователю уровень OSI — не предоставляет услуги другим уровням OSI, однако он обеспечивает прикладные процессы, лежащие за пределами масштаба модели OSI.

Модель OSI не является реализацией, она лишь предлагает порядок организации взаимодействия между компонентами системы. Реализациями этих правил являются ***стеки протоколов***.

Стек протоколов — это иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия узлов в сети. Протоколы работают в сети одновременно, значит работа протоколов должна быть организована так, чтобы не возникало конфликтов или незавершённых операций. Поэтому стек протоколов разбивается на иерархически построенные уровни, каждый из которых выполняет конкретную задачу — подготовку, приём, передачу данных и последующие действия с ними.

Стек протоколов TCP/IP.

*Протокол TCP/IP (*протокол контроля передачи данных / протокол передачи данных между сетями, Internet) является основным протоколом, применяющимся в Internet. В состав стека протоколов TCP/IP входят протоколы: IP и ICMP – сетевой уровень, TCP и UDP – транспортный уровень.

Протокол IP отвечает за адресацию в сети и доставку пакетов между компьютерами сети, без установления соединения и гарантий доставки пакета. При использовании протокола IP, каждый компьютер в рамках сети должен иметь уникальный IP – адрес, представляющий собой 32-битное число. Для удобства чтения, IP адрес разбивают на четыре 8 битовых числа, называемых октетами, например 192.168.0.1. В локальной сети, которая не подключена к Internet или другим сетям можно назначать IP-адреса произвольно (главное, чтобы они не совпадали). Однако в Internet, IP-адреса выделяются централизовано в целом на локальную сеть. При доставке пакета по протоколу IP используется протокол ARP позволяющий преобразовывать IP-адреса (сетевой уровень) в 6 байтные MAC-адреса сетевых карт Ethernet (канальный уровень).

Протокол ICMP используется для передачи сообщений в случае возникновения ошибки доставки пакета. Кроме того, протокол ICMP позволяет посылать короткие служебные пакеты, предоставляющие возможность протестировать работоспособность сети.

Протокол TCP – протокол транспортного уровня - позволяет устанавливать виртуальный канал передачи данных между компьютерами.

Протокол UDP более быстр, чем протокол TCP, однако менее надежен. Данные передаются без установления виртуального канала, в предположении, что принимающая сторона ждет данные. Программа должна сама позаботиться о разбитии передаваемых данных на пакеты, протокол не содержит средств подтверждения факта доставки сообщения и средств коррекции ошибок - все эти задачи должна решать программа

Стек протоколов IPX/SPX.

Данный стек протоколов был разработан фирмой Novell для сетевой операционной системы NetWare и оптимизирован для использования в небольших локальных сетях, однако не удобен для глобальных сетей. Включает в себя протоколы IPX, SPX, SAP, NCP.

Протокол IPX– протокол сетевого уровня, поддерживает обмен пакетами без установления канала связи и гарантии доставки пакета.

Протокол IPX также отвечает за адресацию в сетях NetWare. Адрес имеет формат: номер сети, адрес сетевой карты номер сокета.

Протокол IPX самый быстрый и экономит память, однако не дает гарантии доставки сообщения. За восстановлением утерянных или испорченных пакетов должен следить сам программист. Использование протокола SPX избавляет программиста от этой необходимости.

Протокол SPX – протокол транспортного уровня, поддерживает установление логического канала связи между компьютерами для обмена данными, коррекцию ошибок и, при необходимости, повторную передачу пакетов.

Прикладной уровень стека IPX/SPX составляют два протокола: NCP и SAP.

Протокол NCP поддерживает все основные службы операционной системы Novell NetWare: файловую службу, службу печати и т. д.

Протокол SAP–выполняет вспомогательную роль. С помощью протокола SAP каждый компьютер, который готов предоставить какую-либо службу для клиентов сети, объявляет об этом широковещательно по сети, указывая в SAP-пакетах тип службы (например, файловая), а также свой сетевой адрес.

Протоколы RIP и NLSP отвечают за управление маршрутизацией (выбор маршрута доставки) пакетов

19. Протоколы HTTP, FTP

FTP — стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). FTP часто используется для загрузки сетевых страниц и других документов с частного устройства разработки на открытые сервера хостинга. Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. Пользователи FTP могут пройти аутентификацию, передавая логин и пароль открытым текстом, или же, если это разрешено на сервере, они могут подключиться анонимно.

HTTP — протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов в формате HTML, в настоящий момент используется для передачи произвольных данных). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP используется также в качестве «транспорта» для других протоколов прикладного уровня, таких как SOAP, XML-RPC, WebDAV. DNS нужен для разбора URL. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т. Д. Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

20 Расчёт корректности конфигурации локальной сети Ethernet и Fast Ethernet

Соблюдение многочисленных ограничений, установленных для различных стандартов физического уровня сетей Ethernet, гарантирует корректную работу сети (естественно, при исправном состоянии всех элементов физического уровня). Чтобы сеть Ethernet, состоящая из сегментов различной физической природы, работала корректно, необходимо выполнение четырех основных условий: количество станций в сети не более 1024, максимальная длина каждого физического сегмента не более величины, определенной в соответствующем стандарте физического уровня, время двойного оборота сигнала (Path Delay Value, PDV) между двумя самыми удаленными друг от друга станциями сети не более 575 битовых интервала, сокращение межкадрового интервала IPG (Path Variability Value, PVV) при прохождении последовательности кадров через все повторители должно быть не больше, чем 49 битовых интервала. Соблюдение этих требований обеспечивает корректность работы сети даже в случаях, когда нарушаются простые правила конфигурирования, определяющие максимальное количество повторителей и общую длину сети в 2500 м.

Расчет PDV и PVV смотреть в вопросе 23

Тем не менее комитет 802.3 говорит, что и 4 дополнительных битовых интервала создают достаточный запас надежности.

FAST ETHERNET

Как и все некоаксиальные варианты Ethernet технология Fast Ethernet рассчитана на использование повторителей (концентраторов) для образования древовидной иерархической топологии. Повторители Fast Ethernet делятся на два класса:

- повторители 1-го класса (поддерживают все типы логического кодирования - 4B/5B и 8B/6T); - повторители 2-го класса (поддерживают только один тип логического кодирования).

Параметры сети на основе повторителей 1-го класса

Тип кабеля	диаметр сети,м	длина сегмента,м	оллизий (см. ри
итая пара (100Base-T	200	100	---
птоволокно (100base-	272	136	---
сегментов на витой п ин на оптоволокне	260	100(TX) 160(FX)	1
сегментов на витой п олько на оптоволокне	272	100(TX) 136(FX)	3

При определении корректности конфигурации сети можно не руководствоваться вышеизложенными общими правилами, а рассчитывать время двойного оборота (PDV), как это делалось в Ethetnet-сетях_на 10Мбит/с. Для этого комитет IEEE 802.3

приводит данные об удвоенных задержках, вносимых кабельными сегментами, сетевыми адаптерами и повторителями Fast Ethernet. По сравнению с аналогичными данными для Ethernet-сетей методика расчета несколько изменилась - сегменты теперь не делятся на левый, правый и промежуточные; кроме того, вносимые сетевыми адаптерами задержки учитывают теперь преамбулы кадров, поэтому рассчитанное значение PDV нужно сравнивать не с 575bt, а с 512bt, т.е. временем передачи кадра минимальной длины без преамбулы. В соответствии с рекомендациями IEEE достаточным является запас в 4-6 битовых интервалов.

Задержки, вносимые кабелем

Тип кабеля	ржка, bt на 1м
UTP cat.3	1,14
UTP cat.4	1,14
UTP cat.5	1,112
STP	1,112
Оптоволокно	1,0

Задержки, вносимые адаптером

адаптеров	держка, bt
даптера TX/FX	100
адаптера T4	138
X/FX и один T4	127

Удвоенные задержки повторителей

овторителей	ржка, bt
класса 1	140
асса 2(T4)	67
са 2(TX/FX)	92

Сеть из одного повторителя первого класса и двух оптоволоконных сегментов 100Base-FX длиной по 130 метров каждый. Задержки сегментов: 2*1.0bt*130м=260bt. Задержка пары сетевых адаптеров 100Base-FX: 100bt. Удвоенная задержка повторителя первого класса: 140bt. Итого суммарная задержка в домене коллизий: 260+100+140=500bt, что не превышает допустимого значения в 512 битовых интервалов. Запас прочности 12bt, что очень и очень неплохо.

21 Базовые технологии локальных сетей. Принципы функционирования ЛВС. Стандарты локальных сетей.

Архитектуры или технологии локальных сетей можно разделить на два поколения. К первому поколению относятся архитектуры, обеспечивающие низкую и среднюю скорость передачи информации: Ethernet 10 Мбит/с), Token Ring (16 Мбит/с) и ARC net (2,5 Мбит/с). Для передачи данных эти технологии используют кабели с медной жилой. Ко второму поколению технологий относятся современные высокоскоростные архитектуры: FDDI (100 Мбит/с), ATM (155 Мбит/с) и модернизированные версии архитектур первого поколения (Ethernet): Fast Ethernet (100 Мбит/с) и Gigabit Ethernet (1000 Мбит/с). Усовершенствованные варианты архитектур первого поколения рассчитаны как на применение кабелей с медными жилами, так и на волоконно-оптические линии передачи данных. Новые технологии (FDDI и ATM) ориентированы на применение волоконно-оптических линий передачи данных и могут использоваться для одновременной передачи информации различных типов (видеоизображения, голоса и данных). Сетевая технология – это минимальный набор стандартных протоколов и реализующих их программно-аппаратных средств, достаточный для построения вычислительной сети. Сетевые технологии называют базовыми технологиями. В настоящее время насчитывается огромное количество сетей, имеющих различные уровни стандартизации, но широкое распространение получили такие известные технологии, как Ethernet, Token-Ring, Arcnet, FDDI.

Методы доступа к сети

Ethernet является методом множественного доступа с прослушиванием несущей и разрешением коллизий (конфликтов). Перед началом передачи каждая рабочая станция определяет, свободен канал или занят. Если канал свободен, станция начинает передачу данных. Реально конфликты приводят к снижению быстродействия сети только в том случае, когда работают 80–100 станций. Метод доступа Arcnet. Этот метод доступа получил широкое распространение в основном благодаря тому, что оборудование Arcnet дешевле, чем оборудование Ethernet или Token -Ring. Arcnet используется в локальных сетях с топологией «звезда». Один из компьютеров создает специальный маркер (специальное сообщение), который последовательно передается от одного компьютера к другому. Если станция должна передать сообщение, она, получив маркер, формирует пакет, дополненный адресами отправителя и назначения. Когда пакет доходит до станции назначения, сообщение «отцепляется» от маркера и передается станции.

Метод доступа Token Ring. Этот метод разработан фирмой IBM; он рассчитан па кольцевую топологию сети. Данный метод напоминает Arcnet, так как тоже использует маркер, передаваемый от одной станции к другой. В отличие от Arcnet при методе доступа Token Ring предусмотрена возможность назначать разные приоритеты разным рабочим станциям.

Базовые технологии ЛВС

Технология Ethernet сейчас наиболее популярна в мире. В классической сети Ethernet применяется стандартный коаксиальный кабель двух видов (толстый и тонкий). Однако все большее распространение получила версия Ethernet, использующая в качестве среды передачи витые пары, так как монтаж и обслуживание их гораздо проще. Применяются топологии типа “шина” и типа “пассивная звезда”.

Стандарт определяет четыре основных типа среды передачи:
10BASE5 (толстый коаксиальный кабель);
10BASE2 (тонкий коаксиальный кабель);
10BASE-T (витая пара);
10BASE-F (оптоволоконный кабель).
Fast Ethernet – высокоскоростная разновидность сети Ethernet, обеспечивающая скорость передачи 100 Мбит/с. Сети Fast Ethernet совместимы с сетями, выполненными по стандарту Ethernet. Основная топология сети Fast Ethernet - пассивная звезда. Стандарт определяет три типа среды передачи для Fast Ethernet:
100BASE-T4 (счетверенная витая пара);
100BASE-TX (сдвоенная витая пара);
100BASE-FX (оптоволоконный кабель).
Gigabit Ethernet – высокоскоростная разновидность сети Ethernet, обеспечивающая скорость передачи 1000 Мбит/с.
Стандарт сети Gigabit Ethernet в настоящее время включает в себя следующие типы среды передачи:
1000BASE-SX – сегмент на мультимодовом оптоволоконном кабеле с длиной волны светового сигнала 850 нм.
1000BASE-LX – сегмент на мультимодовом и одномодовом оптоволоконном кабеле с длиной волны светового сигнала 1300 нм.
1000BASE-CX – сегмент на электрическом кабеле (экранированная витая пара).
1000BASE-T – сегмент на электрическом кабеле (счетверенная неэкранированная витая пара).
В связи с тем, что сети совместимы, легко и просто соединять сегменты Ethernet, Fast Ethernet и Gigabit Ethernet в единую сеть.
Сеть Token-Ring предложена фирмой IBM. Token-Ring предназначалась для объединение в сеть всех типов компьютеров, выпускаемых IBM (от персональных до больших). Сеть Token-Ring имеет звездно-кольцевую топологию.
Сеть Arcnet - это одна из старейших сетей. В качестве топологии сеть Arcnet использует “шину” и “пассивную звезду”. Сеть Arcnet пользовалась большой популярностью. Среди основных достоинств сети Arcnet можно назвать высокую надежность, низкую стоимость адаптеров и гибкость. Основным недостаткам сети является низкая скорость передачи информации (2,5 Мбит/с).
FDDI (Fiber Distributed Data Interface) – стандартизованная спецификация для сетевой архитектуры высокоскоростной передачи данных по оптоволоконным линиям. Скорость передачи – 100 Мбит/с.
Основные технические характеристики сети FDDI следующие:
Максимальное количество абонентов сети – 1000.
Максимальная протяженность кольца сети – 20 км.
Максимальное расстояние между абонентами сети – 2 км.
Среда передачи – оптоволоконный кабель.
Метод доступа – маркерный.
Скорость передачи информации – 100 Мбит/с.

22 История появления и характеристика сетей Ethernet. Ограничения и правила построения сетей Ethernet.

Локальная сеть — семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространённой технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Token Ring, FDDI и ARCNET. Название «Ethernet» отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сети.

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года, когда Роберт Меткалф (*Robert Metcalfe*) составил докладную записку для главы PARC о потенциале технологии Ethernet. Но законное право на технологию Меткалф получил через несколько лет.

Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных вычислительных сетей (ЛВС). Ему удалось убедить DEC, Intel и Xerox работать совместно и разработать стандарт Ethernet (DIX). Впервые этот стандарт был опубликован 30 сентября 1980 года. Он начал соперничество с двумя крупными запатентованными технологиями: token ring и ARCNET, — которые вскоре были раздавлены под накатывающимися волнами продукции Ethernet. В процессе борьбы 3Com стала основной компанией в этой отрасли.

10 Мбит/с Ethernet (Thick ethernet)	Стандарт	Год выхода стандарта	Тип	Скорость передачи (Mbps)	Максимальная длина сегмента в метрах	Тип кабеля
	IEEE 802.3	1983	10Base5	10	500 м	коаксиальный
	IEEE 802.3a	1985	10Base2	10	185 м	
	IEEE 802.3b	1985	10Broad36	10	3600 м	
	IEEE 802.3e	1987	1Base5	1	250 м	UTP
	IEEE 802.3e	1987	StarLan 10	10	250 м	UTP
	IEEE 802.3d	1987	FOIRL	10	1000	оптоволоконный
	IEEE 802.3i	1990	10Base-T	10	100 м	UTP cat 3,5
	IEEE 802.3j	1993	10Base-F	10	2км	оптоволоконный

23 Расчет времени оборачиваемости сигнала (PDV) и сокращение межкадрового расстояния.

Расчет PDV

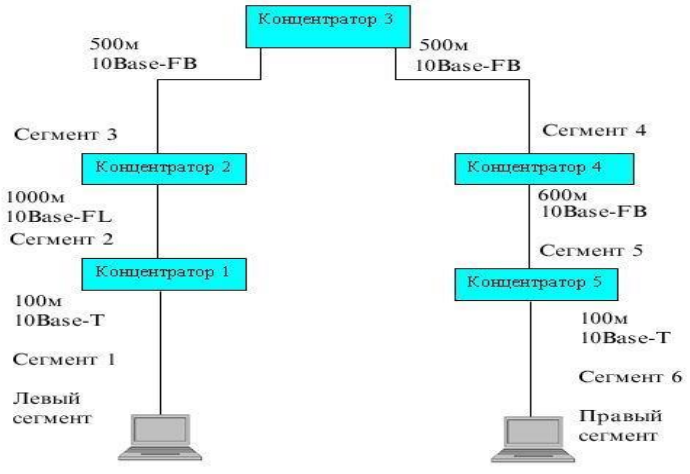
Для упрощения расчетов обычно используются справочные данные IEEE, содержащие значения задержек распространения сигналов в повторителях, приемопередатчиках и различных физических средах. В табл. 10.1 приведены данные, необходимые для расчета значения PDV для всех физических стандартов сетей Ethernet. Битовый интервал обозначен как bt.

Комитет 802.3 старался максимально упростить выполнение расчетов, поэтому данные, приведенные в таблице, включают сразу несколько этапов прохождения сигнала. Например, задержки, вносимые повторителем, состоят из задержки входного трансивера, задержки блока повторения и задержки выходного трансивера. Тем не менее, в таблице все эти задержки представлены одной величиной, названной базой сегмента. Чтобы не нужно было два раза складывать задержки, вносимые кабелем, в таблице даются удвоенные величины задержек для каждого типа кабеля.

Тип сегмента	**База левого сегмента, bt**	**База промежуточного сегмента, bt**	**База правого сегмента, bt**	**Задержка среды на 1 м, bt**	**Максимальная длина сегмента, м**
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	—	24,0	—	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI (> 2 м)	0	0	0	0,1026	2+48

В таблице используются также такие понятия, как левый сегмент, правый сегмент и промежуточный сегмент. Поясним эти термины на примере сети, приведенной на рис. 10.8. Левым сегментом называется сегмент, в котором начинается путь сигнала от выхода передатчика конечного узла. На примере это сегмент 1. Затем сигнал проходит через промежуточные сегменты 2-5 и доходит до приемника наиболее удаленного узла наиболее удаленного сегмента 6, который называется правым. Именно здесь в худшем случае происходит столкновение кадров и возникает коллизия, что и подразумевается в таблице.

С каждым сегментом связана постоянная задержка, названная базой, которая зависит только от типа сегмента и от положения сегмента на пути сигнала (левый, промежуточный или правый). База правого сегмента, в котором возникает коллизия, намного превышает базу левого и промежуточных сегментов.



Кроме этого, с каждым сегментом связана задержка распространения сигнала вдоль кабеля сегмента, которая зависит от длины сегмента и вычисляется путем умножения времени распространения сигнала по одному метру кабеля (в битовых интервалах) на длину кабеля в метрах.

Расчет заключается в вычислении задержек, вносимых каждым отрезком кабеля (приведенная в таблице задержка сигнала на 1 м кабеля умножается на длину сегмента), а затем суммировании этих задержек с базами левого, промежуточных и правого сегментов. Общее значение PDV не должно превышать 575.

Так как левый и правый сегменты имеют различные величины базовой задержки, то в случае различных типов сегментов на удаленных краях сети необходимо выполнить расчеты дважды: один раз принять в качестве левого сегмента сегмент одного типа, а во второй — сегмент другого типа. Результатом можно считать максимальное значение PDV. В нашем примере крайние сегменты сети принадлежат к одному типу — стандарту 10Base-T, поэтому двойной расчет не требуется, но если бы они были, сегментами разного типа, то в первом случае нужно было бы принять в качестве левого сегмент между станцией и концентратором 1, а во втором считать левым сегмент между станцией и концентратором 5.
Приведенная на рисунке сеть в соответствии с правилом 4-х хабов не является корректной — в сети между узлами сегментов 1 и 6 имеется 5 хабов, хотя не все сегменты являются сегментами 10Base-FB. Кроме того, общая длина сети равна 2800 м, что нарушает правило 2500 м. Рассчитаем значение PDV для нашего примера.
Левый сегмент 1: 15,3 (база) + 100 x 0,113 - 26,6.
Промежуточный сегмент 2*:* 33,5 + 1000 x 0,1 = 133,5.
Промежуточный сегмент 3*:* 24 + 500 x 0,1 = 74,0.
Промежуточный сегмент 4*:* 24 + 500 x 0,1 = 74,0.
Промежуточный сегмент 5: 24 + 600 x 0,1 = 84,0.
Правый сегмент 6*:* 165 + 100 x 0,113 = 176,3.
Сумма всех составляющих дает значение PDV, равное 568,4.
Так как значение PDV меньше максимально допустимой величины 575, то эта сеть проходит по критерию времени двойного оборота сигнала несмотря на то, что ее общая длина составляет больше 2500 м, а количество повторителей — больше 4-х.
PVV
Чтобы признать конфигурацию сети корректной, нужно рассчитать также уменьшение межкадрового интервала повторителями, то есть величину PVV.
Для расчета PVV также можно воспользоваться значениями максимальных величин уменьшения межкадрового интервала при прохождении повторителей различных физических сред, рекомендованными IEEE и приведенными в табл. 10.2.
Таблица 10.2. Сокращение межкадрового интервала повторителями

Тип сегмента	**Передающий сегмент, bt**	**Промежуточный сегмент, bt**
10Base-5 или 10Base-2	16	11
10Base-FB	—	2
10Base-FL	10,5	8
10Base-T	10,5	8

В соответствии с этими данными рассчитаем значение PVV для нашего примера.
Левый сегмент 1: 10Base-T: сокращение в 10,5 bt.
Промежуточный сегмент 2: 10Base-FL: 8.
Промежуточный сегмент 3: 10Base-FB: 2.
Промежуточный сегмент 4: 10Base-FB: 2.
Промежуточный сегмент 5: 10Base-FB: 2.
Сумма этих величин дает значение PVV, равное 24,5, что меньше предельного значения в 49 битовых интервала.
В результате приведенная в примере сеть соответствует стандартам Ethernet по всем параметрам, связанным и с длинами сегментов, и с количеством повторителей.

24. Расчет коэффициента загрузки сегмента сети.

Пример: Условие задания:

Объединить компьютеры двух подразделений предприятия в общую локальную сеть, если известно, что между подразделениями будет происходить обмен данными с трафиком 4 Mbit, а расстояние между подразделениями составляет порядка 20м; средний трафик между компьютерами 1 и 2 подразделения – 3 Mbit; предполагаемое количество компьютеров 1 подразделения – 9, 2 – 8. Компьютеры всех подразделений должны иметь выход в Интернет по общему коммутируемому каналу.

Решение: Решение задачи будем осуществлять в несколько этапов. 1. При проектировании сети на первом этапе необходимо провести сбор предварительной информации. Обозначим компьютеры первого подразделения ПК1 – ПК9, а второго подразделения ПК10 - ПК17 (ПК – персональный компьютер). Т.к. расстояние между компьютерами внутри подразделений не указаны, то будем считать, что они находятся в одной комнате, т.е. расстояние будет порядка 15м.

Всю информацию о проектируемой сети сведѐм в таблицу 2. 2. Анализ финансового обеспечения проекта проводить не нужно 3. Анализируя таблицу 2, видим, что максимальное расстояние между компьютерами двух подразделений может быть: 15+15+20=50м, а общее количество компьютеров предприятия равно 17, то нет необходимости сеть разбивать на 2 сегмента. В случае необходимости, можно будет выделить подсети на логическом уровне, путѐм задания адресов компьютеров. 4. Внутри общей сети трафик не будет превышать 4 Mbit/c, а количество компьютеров равно 17, поэтому можно использовать сетевое оборудование стандартов 10base-5, 10base-2, 10base-T, 10base-F, 100base-T4, 100base-TX, 100base-FX т.к. для всех стандартов выполняются ограничения на максимальный трафик, количество компьютеров и длину кабелей. Однако, для стандартов 10base-F и 100base-FX необходимо использовать дорогостоящий оптоволоконный кабель, поэтому ограничимся стандартами 10base-5, 10base-2, 10base-T, 100base-T4, 100base-TX. Стандарты 10base-5, 10base-2, 10base-T используют протокол Ethernet, а стандарты 100base-T4, 100base-TX используют протокол Fast Ethernet.

Рассчитаем коэффициент загрузки сети. Длина кадра для стандарта Ethernet составляет 72 байта = 72*8 = 576 бит. Скорость передачи 1 бита будет равна 0,1 мкс. Т.о. для передачи 1 кадра минимальной длины необходимо 0,1*576= 57,6 мкс. Между кадровый интервал в стандартом Ethernet устанавливается равным 9,6 мкс. Т.о. период следования кадров минимальной длины будет равен 57,6 + 9,6=67,1 мкс. Откуда следует, что максимальная пропускная способность сети Ethernet будет составлять 14880 кадров/с. По условию задано, что все компьютеры будут

передавать одинаковые объѐмы информации и с трафиком 4 Mbit/c. Предположим, что данная информация будет передаваться кадрами минимальной длины, что значительно понижает пропускную способность сети. Для того, чтобы передать 4 Mbit информации потребуется 7812 кадров, что меньше максимальной пропускной способности примерно в 2 раза.

$$S = \frac{\sum_{i=1}^{n} m_i}{f}$$ где mi— количество кадров в секунду, отправляемых в сеть ім узлом, f — максимально возможная пропускная способность сегмента, n - количество узлов.

$$S = \frac{\sum_{i=1}^{17} 7812}{14880} = 8{,}925 \geq 0{,}3$$ Т.о. использовать стандарты 10base-5, 10base-2, 10base-T нельзя. Для протокола Fast Ethernet формат кадра такой же, как и для стандарта Ethernet, но скорость передачи в 10 раз больше. Т.о. максимальная пропускная способность сети для кадров минимальной длины равна 148800 кадров/с, отсюда загрузка сегмента будет равна:

$$S = \frac{\sum_{i=1}^{17} 7812}{148800} = 0{,}8925 \geq 0{,}3$$ Отсюда следует, что применить простой концентратор нельзя, поэтому воспользуемся коммутируемым концентратором, тогда загрузка сегмента будет равна:

$$S = \frac{\sum_{i=1}^{2} 7812}{148800} = 0{,}105 \leq 0{,}3$$ Т.о. для объединения компьютеров воспользуемся стандартами 100baseT4 или 100base-TX, а для соединения будем применять кабель «витую пару». При этом все ограничения на максимальную длину кабеля (100м) и количество компьютеров (1024) выполняются. В качестве дополнительного оборудования будем использовать коммутируемый концентратор, имеющий 24 порта для подключения компьютеров. Будем использовать топологию типа «звезда».

25 Коммутируемые сети Ethernet. Скоростные версии Ethernet.

Скоростные версии Ethernet

Скорость 10 Мбит/с первой стандартной версии Ethernet долгое время удовлетворяла потребности пользователей локальных сетей. Однако в начале 90-х годов начала ощущаться недостаточная пропускная способность Ethernet, так как скорость обмена с сетью стала существенно меньше скорости внутренней шины компьютера. Кроме того, начали появляться новые мультимедийные приложения, гораздо более требовательные к скорости сети, чем их текстовые предшественники. В поисках решения проблемы ведущие производители сетевого оборудования начали интенсивные работы по повышению скорости Ethernet при сохранении главного достоинства этой технологии — простоты и низкой стоимости оборудования.

Результатом стало появление новых скоростных стандартов Ethernet: Fast Ethernet (скорость 100 Мбит/с), Gigabit Ethernet (1000 Мбит/с, или 1 Гбит/с) и 10G Ethernet (10 Гбит/с). На время написания этой книги два новых стандарта — 40G Ethernet и 100G Ethernet — находились в стадии разработки, обещая следующее десятикратное превышение верхней границы производительности Ethernet.

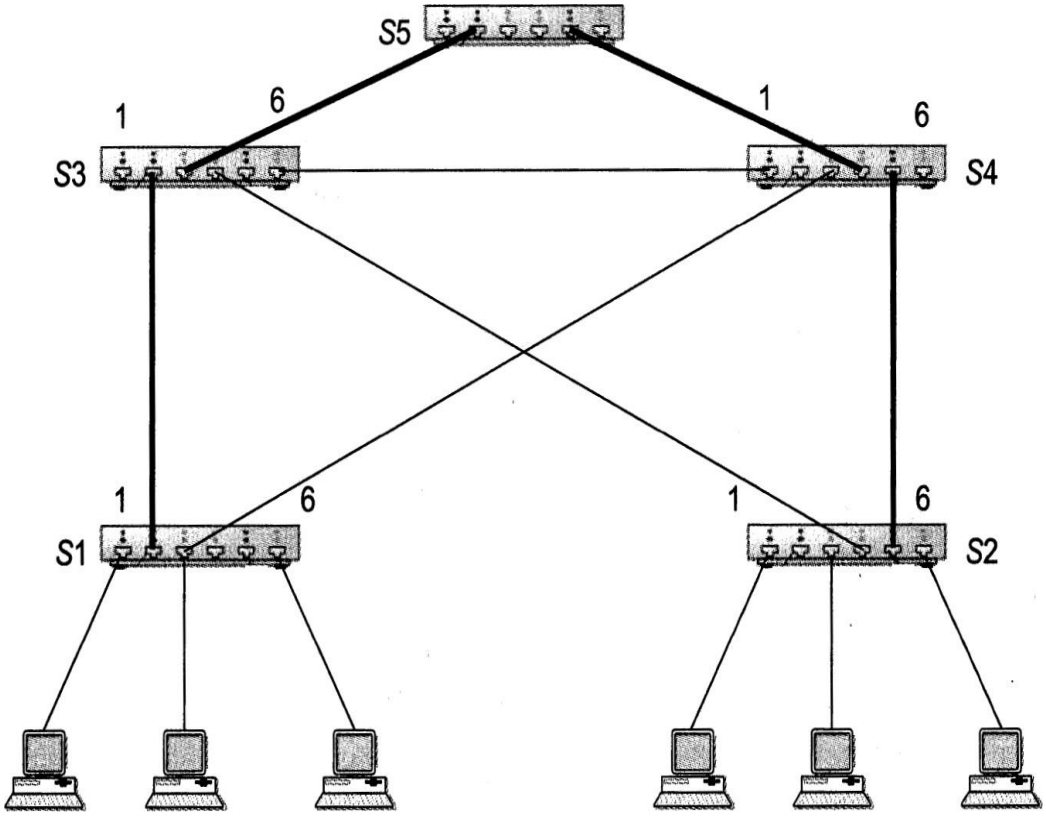
Коммутируемые сети Ethernet

Проблемы, возникающие из-за наличия единой разделяемой среды, были распознаны разработчиками и пользователями локальных сетей достаточно быстро, и ответом стало появление устройства под названием «мост». Мост локальной сети - выполняет логическую структуризацию сети, разделяя единую разделяемую среду на несколько сегментов. Мост передает кадры с одного своего порта на другой, анализируя MAC-адреса назначения, помещенные в эти кадры. Передача происходит только в том случае, когда действительно необходимо передать кадр из одного сегмента в другой. В том же случае, когда источник и приемник находятся в одном сегменте, мост игнорирует кадр.

Как видно из этого краткого описания, применение моста приводит к снижению нагрузки на разделяемую среду, так как каждый сегмент сети передает только свой внутрисегментный трафик плюс межсегментный, который поступает из другого сегмента или направляется в другой сегмент.

Мосты были медленными и дорогими. Ситуация изменилась в начале 90-х годов, когда появились так называемые коммутаторы локальных сетей. Коммутатор локально сети функционально подобен мосту – он работает по тому же алгоритму. Коммутаторы отличаются от традиционных мостов потребительскими характеристиками: большим количеством портов, высокой скоростью передачи кадров с порта на порт, низкой стоимостью. Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу только одного потока кадров и только между двумя портами, а коммутатор способен одновременно передавать несколько потоков данных между любыми своими портами.

Протокол покрывающего дерева предназначен для повышения надежности локальной сети на коммутаторах за счет использования произвольной топологии, обеспечивающей альтернативные пути между узлами сети.



Альтернативные пути можно использовать в разных целях, например, для повышения производительности сети, когда трафик к определенному узлу назначения распараллеливается между такими путями, а также для повышения надежности сети. В последнем случае некоторые линии связи между коммутаторами переводятся в резервное состояние, то есть такое, в котором они не применяются для передачи трафика, но могут быть оперативно переведены в рабочее состояние при выходе из строя какого-либо элемента сети — коммутатора, одного из портов или линии связи между портами. Резервные линии связи называют также избыточными.

26 Сетевые технологии локальных сетей: 100VG AnyLan, ArcNet.

100VG-AnyLan

Главными достоинствами ее являются большая скорость обмена, вдвое большую длину кабеля UTP категории 5 (до 200 метров), сравнительно невысокая стоимость аппаратуры (примерно вдвое дороже оборудования наиболее популярной сети Ethernet 10BASE-T), централизованный метод управления обменом без конфликтов, а также совместимость на уровне форматов пакетов с сетями Ethernet и Token-Ring.

Основные технические характеристики сети 100VG-AnyLAN:

Скорость передачи – 100 Мбит/с.

Топология – звезда с возможностью наращивания (дерево). Количество уровней каскадирования концентраторов (хабов) – до 5.

Метод доступа – централизованный, бесконфликтный (Demand Priority – с запросом приоритета).

Среда передачи – счетверенная неэкранированная витая пара (кабели UTP категории 3, 4 или 5), сдвоенная витая пара (кабель UTP категории 5), сдвоенная экранированная витая пара (STP), а также оптоволоконный кабель. Сейчас в основном распространена счетверенная витая пара.

Максимальная длина кабеля между концентратором и абонентом и между концентраторами – 100 метров (для UTP кабеля категории 3), 200 метров (для UTP кабеля категории 5 и экранированного кабеля), 2 километра (для оптоволоконного кабеля). Максимально возможный размер сети – 2 километра (определяется допустимыми задержками).

Максимальное количество абонентов – 1024, рекомендуемое – до 250.

Сеть 100VG-AnyLAN состоит из центрального (корневого) концентратора, и соединенных с ним конечных узлов и других концентраторов. Концентратор циклически выполняет опрос портов, к которым подключены компьютеры. Если к порту подключен другой концентратор, то опрос приостанавливается до завершения опроса концентратором нижнего уровня. Компьютер, желающий передать пакет, посылает специальный низкочастотный сигнал концентратору, запрашивая передачу кадра и указывая его приоритет: низкий (для обычных данных) или высокий (для данных, которые чувствительны к задержкам, например видеоизображение). Компьютер с низким уровнем приоритета, долго не имевший доступа к сети, получает высокий приоритет. Если сеть свободна, то концентратор разрешает передачу пакета. Анализируется адрес назначения в пакете, и он передается на тот порт, к которому подключен соответствующий компьютер. Если сеть занята, концентратор ставит полученный запрос в очередь. В очередь ставятся именно не сами кадры данных, а лишь запросы на их передачу. Запросы удовлетворяются в соответствии с порядком их поступления и с учетом приоритетов. Допускаются три уровня каскадирования.

ArcNet

Среди основных достоинств сети Arcnet по сравнению с Ethernet можно назвать ограниченную величину времени доступа, высокую надежность связи, простоту диагностики, а также сравнительно низкую стоимость адаптеров. К наиболее существенным недостаткам сети относятся низкая скорость передачи информации (2,5 Мбит/с), система адресации и формат пакета. В качестве среды передачи в сети используется коаксиальный кабель. В качестве топологии сеть Arcnet использует классическую шину (Arcnet-BUS), а также пассивную звезду (Arcnet-STAR). В звезде применяются концентраторы (хабы). количество сегментов,

соединенных последовательной цепочкой с помощью концентраторов, не должно превышать трех.
Концентраторы бывают двух видов:
Активные концентраторы (восстанавливают форму приходящих сигналов и усиливают их). Количество портов – от 4 до 64. Активные концентраторы могут соединяться между собой (каскадироваться). Шинные сегменты могут подключаться только к активным концентраторам.
Пассивные концентраторы (просто смешивают приходящие сигналы без усиления). Количество портов – 4. Пассивные концентраторы не могут соединяться между собой. Они могут связывать только активные концентраторы и/или сетевые адаптеры
В сети Arcnet используется маркерный метод доступа (метод передачи права).Последовательность действий абонентов при данном методе следующая:
Абонент, желающий передавать, ждет прихода маркера.
Получив маркер, он посылает запрос на передачу приемнику информации (то есть спрашивает, готов ли приемник принять его пакет).
Приемник, получив запрос, посылает ответ (то есть подтверждает свою готовность).
Получив подтверждение готовности, передатчик посылает свой пакет.
Получив пакет, приемник посылает подтверждение приема пакета.
Передатчик, получив подтверждение приема пакета, посылает маркер следующему абоненту.
Так же, как и в случае Token-Ring, конфликты в Arcnet полностью исключены. Как и любая маркерная сеть, Arcnet хорошо держит нагрузку . Основные технические характеристики сети Arcnet следующие.

1. Среда передачи – коаксиальный кабель, витая пара.
2. Максимальная длина сети – 6 километров.
3. Максимальная длина кабеля от абонента до пассивного концентратора – 30 метров.
4. Максимальная длина кабеля от абонента до активного концентратора – 600 метров.
5. Максимальная длина кабеля между активным и пассивным концентраторами – 30 метров.
6. Максимальная длина кабеля между активными концентраторами – 600 метров.
7. Максимальное количество абонентов в сети – 255.
8. Максимальное количество абонентов на шинном сегменте – 8.
9. Минимальное расстояние между абонентами в шине – 1 метр.
10. Максимальная длина шинного сегмента – 300 метров.
11. Скорость передачи данных – 2,5 Мбит/с.

27.Сетевые технологии локальных сетей: Token Ring, FDDI.

Протокол Token Ring (High Speed Token Ring).

Сеть Token Ring представляет собой кольцо: каждый компьютер соединен кабелем только с предыдущим и последующим компьютером в кольце. Физически это реализуется при помощи специальных концентраторов, которые обеспечивают целостность кольца даже при выключении или отказе одного из компьютеров, за счет обхода порта выключенного компьютера.

Принцип доступа к разделяемой среде – доступ с передачей маркера (token). Компьютер может начать передавать данные в сеть, только если получит от предыдущего компьютера в кольце «маркер» – специальный короткий пакет, свидетельствующий о том, что сеть свободна. Если компьютеру нечего передавать в сеть, то он передает маркер следующему компьютеру в кольце. Если компьютеру есть что передавать, то он уничтожает маркер и передает свой пакет в сеть. Пакет по битам ретранслируется по кольцу от компьютера к компьютеру, адресат получает пакет, устанавливает в пакете биты, подтверждающие, что пакет достиг адресата и передает пакет дальше по кольцу. Наконец, пакет возвращается к отправителю, который уничтожает его и передает в сеть новый маркер.

В процессе работы сети, из-за сбоев, возможна потеря маркера. За наличие в сети маркера, причем единственной его копии, отвечает один из компьютеров- активный монитор. Если активный монитор не получает маркер в течение длительного времени, то он порождает новый маркер. Активный монитор выбирается во время инициализации кольца, как станция с максимальным значением MAC-адреса сетевой карты.

Протокол FDDI

Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец необходимо для повышения отказоустойчивости сети FDDI. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля только первичного (Primary) кольца. Данные по первичному кольцу всегда передаются в одном направлении, а по вторичному — в обратном. Передача пакетов в сетях FDDI аналогична, как и в сетях Token Ring.

28 Ограничения и правила построения кольцевых сетей

Token Ring является главными примерами сетей с передачей маркера. Сети с передачей маркера перемещают по сети небольшой блок данных, называемый маркером. Владение этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки, он просто переправляет маркер к следующей конечной станции. Каждая станция может удерживать маркер в течение определённого максимального времени (по умолчанию — 10 мс).

Данная технология предлагает вариант решения проблемы коллизий, которая возникает при работе локальной сети. В технологии Ethernet такие коллизии возникают при одновременной передаче информации несколькими рабочими станциями, находящимися в пределах одного сегмента, то есть использующих общий физический канал данных.

Если у станции, владеющей маркером, имеется информация для передачи, она захватывает маркер, изменяет у него один бит (в результате чего маркер превращается в последовательность «начало блока данных»), дополняет информацией, которую он хочет передать, и отсылает эту информацию к следующей станции кольцевой сети. Когда информационный блок циркулирует по кольцу, маркер в сети, поэтому другие станции, желающие передать информацию, вынуждены ожидать. Следовательно, в сетях Token Ring не может быть коллизий. Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он окончательно удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения. Существуют 2 модификации по скоростям передачи: 4 Мбит/с и 16 Мбит/с. В Token Ring 16 Мбит/с используется технология раннего освобождения маркера. Суть этой технологии заключается в том, что станция, «захватившая» маркер, по окончании передачи данных генерирует свободный маркер и запускает его в сеть.

29 Основные принципы организации и передачи данных. Методы доступа к среде передачи.

30 Пропускная способность сетей с различной коммутацией

Коммутация каналов

При коммутации каналов коммутационная сеть образует между конечными узлами непрерывный составной физический канал из последовательно соединенных коммутаторами промежуточных канальных участков. Условием того, что несколько физических каналов при последовательном соединении образуют единый физический канал, является равенство скоростей передачи данных в каждом из составляющих физических каналов. Равенство скоростей означает, что коммутаторы такой сети не должны буферизовать передаваемые данные.

В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал. И только после этого можно начинать передавать данные. Например, если сеть, изображенная на рис. 1, работает по технологии коммутации каналов, то узел 1, чтобы передать данные узлу 7, сначала должен передать специальный запрос на установление соединения коммутатору A, указав адрес назначения 7. Коммутатор A должен выбрать маршрут образования составного канала, а затем передать запрос следующему коммутатору, в данном случае E. Затем коммутатор E передает запрос коммутатору F, а тот, в свою очередь, передает запрос узлу 7. Если узел 7 принимает запрос на установление соединения, он направляет по уже установленному каналу ответ исходному узлу, после чего составной канал считается скоммутированным, и узлы 1 и 7 могут обмениваться по нему данными.

Коммутация пакетов

Эта техника коммутации была специально разработана для эффективной передачи компьютерного трафика. Первые шаги на пути создания компьютерных сетей на основе техники коммутации каналов показали, что этот вид коммутации не позволяет достичь высокой общей пропускной способности сети. Типичные сетевые приложения генерируют трафик очень неравномерно, с высоким уровнем пульсации скорости передачи данных. Например, при обращении к удаленному файловому серверу пользователь сначала просматривает содержимое каталога этого сервера, что порождает передачу небольшого объема данных. Затем он открывает требуемый файл в текстовом редакторе, и эта операция может создать достаточно интенсивный обмен данными, особенно если файл содержит объемные графические включения. После отображения нескольких страниц файла пользователь некоторое время работает с ними локально, что вообще не требует

передачи данных по сети, а затем возвращает модифицированные копии страниц на сервер — и это снова порождает интенсивную передачу данных по сети. Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может достигать 1:50 или даже 1:100. Если для описанной сессии организовать коммутацию канала между компьютером пользователя и сервером, то большую часть времени канал будет простаивать. В то же время коммутационные возможности сети будут закреплены за данной парой абонентов и будут недоступны другим пользователям сети.

При коммутации пакетов все передаваемые пользователем сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Напомним, что сообщением называется логически завершенная порция данных — запрос на передачу файла, ответ на этот запрос, содержащий весь файл и т.д. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета на узел назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения (рис. 3). Пакеты транспортируются по сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге — узлу назначения.

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета (рис. 3). В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсацию трафика на магистральных связях между коммутаторами и тем самым наиболее эффективно использовать их для повышения пропускной способности сети в целом.

31 Метод доступа CSMA/CD, CSMA/CA

CSMA/CD — технология множественного доступа к общей передающей среде в локальной компьютерной сети с контролем коллизий Он используется как в обычных сетях типа Ethernet, так и в высокоскоростных сетях (Fast Ethernet, Gigabit Ethernet). Методы обнаружения коллизий зависят от используемого оборудования, но на электрических шинах, таких как Ethernet, коллизии могут быть обнаружены сравнением передаваемой и получаемой информации. Если она различается, то другая передача накладывается на текущую (возникла коллизия) и передача прерывается немедленно. Посылается сигнал преднамеренной помехи, что вызывает задержку передачи всех передатчиков на произвольный интервал времени, снижая вероятность коллизии во время повторной попытки.

Ethernet является классическим примером протокола CSMA/CD.

CSMA/CA, «множественный доступ с контролем несущей и избеганием коллизий» или «многостанционный доступ с контролем несущей и предотвращением конфликтов»— это сетевой протокол, в котором:

используется схема прослушивания несущей волны

станция, которая собирается начать передачу, посылает jam signal (сигнал затора)

после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу фрейма

если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку

CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы. Отсюда и название «Collision Avoidance» — предотвращение коллизий (именно пакетов данных).

Избегание коллизий используется для того, чтобы улучшить производительность CSMA, отдав сеть единственному передающему устройству. Эта функция возлагается на «jamming signal» в CSMA/CA. Улучшение производительности достигается за счёт снижения вероятности коллизий и повторных попыток передачи. Но ожидание jam signal создаёт дополнительные задержки, поэтому другие методики позволяют достичь лучших результатов. Избегание коллизий полезно на практике в тех ситуациях, когда своевременное обнаружение коллизии невозможно — например, при использовании радиопередатчиков.

32 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.

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.

33 Инкапсуляция пакетов.

При продвижении пакета данных по уровням сверху вниз каждый новый уровень добавляет к пакету свою служебную информацию в виде заголовка и, возможно, трейлера (информации, помещаемой в конец сообщения). Эта операция называется инкапсуляцией данных верхнего уровня в пакете нижнего уровня. Служебная информация предназначается для объекта того же уровня на удаленном компьютере, ее формат и интерпретация определяются протоколом данного уровня.

Разумеется, данные, приходящие с верхнего уровня, могут на самом деле представлять собой пакеты с уже инкапсулированными данными еще более верхнего уровня.

С другой стороны, при получении пакета от нижнего уровня он разделяется на заголовок (трейлер) и данные. Служебная информация из заголовка (трейлера) анализируется и в соответствии с ней данные, возможно, направляются одному из объектов верхнего уровня. Тот в свою очередь рассматривает эти данные как пакет со своей служебной информацией и данными для еще более верхнего уровня, и процедура повторяется, пока пользовательские данные, очищенные от всей служебной информации, не достигнут прикладного процесса.

Возможно, что пакет данных не будет доведен до самого верхнего уровня, например, в случае, если данный компьютер представляет собой промежуточную станцию на пути между отправителем и получателем. В этом случае объект соответствующего уровня при анализе служебной информации заметит, что пакет на этом уровне адресован не ему (хотя с точки зрения нижележащих уровней он был адресован именно этому компьютеру). Тогда объект выполнит необходимые действия для перенаправления пакета к месту назначения или возврата отправителю с сообщением об ошибке, но в любом случае не будет продвигать данные на верхний уровень.

34 Виртуальные каналы.

Виртуальное соединение, виртуальный канал— канал связи в сети коммутации пакетов, соединяющий двух и более абонентов, и состоящий из последовательных физических звеньев системы передачи между узлами связи (коммутаторами), а также из физических и логических звеньев внутри коммутаторов на пути между указанными абонентами. Логическое звено управляет физическим звеном и они оба одновременно организуются на этапе установления сквозного ВС между абонентами.

Логическое звено представляет собой запись в памяти коммутатора соответствия идентификатора входящего логического канала (ЛК), ожидаемого в заголовке пакета на данном входящем физическом порту, идентификатору исходящего ЛК и номеру исходящего физического порта.

Как только на данном входящем порту появляется пакет для передачи, логическое звено активируется и задействует соответствующее физическое звено, которое с помощью коммутационного поля передаёт пакет в исходящий порт. При этом входящий идентификатор ЛК (ИЛК) в заголовке пакета заменяется на исходящий ИЛК. Таким образом, помимо физической коммутации, осуществляется и логическая коммутация.

ВС обеспечивает передачу пакетов с сохранением их исходной последовательности[1] («строго друг за другом»). Каждый такой пакет содержит только идентификатор ближайшего логического канала в звене, и не несёт полную адресную информацию места назначения, в отличие от дейтаграмм. При разъединении ВС соответствующие ему записи в памяти коммутаторов стираются, и на их место могут быть записаны данные нового ВС.

35 Проводная и беспроводная среда передачи. Виды сигналов для передачи информации.

Физически сеть может быть проводной и беспроводной. У каждого из видов есть свои плюсы, минусы и особенности – как явные, так и скрытые.

Проводные сети - Основа всего: кабели. Во всех сетевых стандартах определены необходимые условия и характеристики используемого кабеля, такие как полоса пропускания, волновое сопротивление (импеданс), удельное затухание сигнала, помехозащищенность и другие.

Существуют два принципиально разных вида сетевых кабелей: медные и оптоволоконные.

Кабели на основе медных проводов, в свою очередь, делятся на коаксиальные и некоаксиальные. Обычно используемая витая пара

Коаксиальный кабель представляет собой центральный проводник, окруженный слоем диэлектрика (изолятора) и экраном из металлической оплетки, выполняющим также роль второго контакта в кабеле.

Витая пара представляет собой несколько (обычно 8) пар скрученных проводников. Скручивание применяется для уменьшения помех как самой пары, так и внешних, влияющих на нее. У скрученной определенным образом пары появляется такая характеристика, как волновое сопротивление.

Оптоволоконный кабель состоит из одного или нескольких волокон, заключенных в оболочки, и бывает двух типов: одномодовый и многомодовый. Их различие в том, как свет распространяется в волокне в одномодовом кабеле все лучи (посланные в один момент времени) проходят одинаковое расстояние и достигают приемника одновременно, а в многомодовом сигнал может размазаться.

Основное достоинство проводной сети – стабильность и надежность работы.

Высокая скорость и стабильность работы. Итак, возьмем распространенную конфигурацию сети со скоростью работы 1 Гбит/с. Эта скорость доступна для каждого клиента в сети и не делится между ними, плюс, это скорость в каждую сторону, т.е. суммарная пропускная способность может достигать 2000 Мбит/с

Оборудование. Гигабитный контроллер проводной сети сегодня интегрирован в любую продающуюся материнскую плату, т.е. по факту является бесплатным для пользователя. Кабели тоже относительно дешевы, плюс, их можно нарезать самостоятельно до нужной длины. Сетевое оборудование на рынке есть, что называется, на любой вкус и кошелек, всегда можно найти недорогие и при этом эффективные решения. Безопасность. Один из существенных плюсов проводной сети – безопасность. В первую очередь физическая, т.к. чтобы подключиться к сети, злоумышленнику нужен физический доступ в помещение, к розетке.

Беспроводные локальные сети становятся все более популярными среди пользователей. В течение нескольких лет они были усовершенствованы, была увеличена скорость, цены стали более доступными.

Существуют два варианта конфигурации устройств беспроводного доступа 802.11: BSS и IBSS.

Точки доступа представляют собой беспроводные сетевые устройства, позволяющие одному или большему количеству клиентов беспроводной сети использовать эти устройства в качестве центрального сетевого концентратора. При использовании точки доступа все клиенты работают через неё. Основной плюс беспроводной сети – свобода. В случае, если в офисе уже развернута беспроводная инфраструктура, то подключение дополнительного рабочего места не требует практически никаких дополнительных затрат – правда, пропускная способность точки доступа делится на всех клиентов, т.е. при большом обмене данных пропускная способность на клиента сильно упадет.

То же можно сказать и об устройствах – например, поставить новый принтер или МФУ с поддержкой Wi-Fi – дело пары минут. В результате, в некоторых случаях работа через Wi-Fi оказывается дешевле – особенно если количество сотрудников и устройств динамически меняется. Но нельзя забывать, что развертывание беспроводной инфраструктуры тоже стоит денег (и зачастую затраты больше, чем на проводную инфраструктуру), и провода тянуть (и делать коммутацию) все равно придется – хотя бы до точки доступа.

Однако в случае с Wi-Fi большинство плюсов сопровождается минусами – либо, на худой конец, увесистыми оговорками.

Скорость и стабильность. Формально скорость соединения – то, что пишут на коробках – даже превосходит скорость проводного соединения. Однако реальная скорость работы в этом случае всегда будет гораздо ниже. Основные ограничения беспроводных сетей Wi-Fi включают в себя:
заявленная производителем точки доступа скорость подключения делится между всеми клиентами, то есть при большом количестве клиентов реальная скорость будет значительно ниже заявленной;
Высокая скорость достигается только при применении нескольких антенн. Но даже если у роутера их 8, то у мобильного устройства вряд ли будет больше двух антенн, соответственно, скорость будет ниже.
Скорость беспроводного соединения зависит от многих факторов: помех, расстояния до точки доступа, количества стен и других преград между точкой доступа и клиентом и т.д. Для диапазона 5 ГГц влияние этих факторов выше (т.е. дальность устойчивой работы будет меньше, а скорость при увеличении расстояния или через препятствие падает быстрее).
Беспроводные сети при работе мешают друг другу. В местах, где одновременно работает несколько сетей на одинаковом или близком канале передачи, скорость обмена данными в каждой из них будет падать.
В соответствии со стандартом IEEE 802.11, работа идет в полудуплексном режиме – это значит, что передача данных может идти только в одном направлении в конкретный момент времени, а при активном обмене данными на вход и выход скорость можно делить пополам

Если рассматривать сигнал как функцию времени, то он может быть, либо аналоговым, либо цифровым. Аналоговым называется сигнал, интенсивность которого во времени изменяется постепенно. Другими словами, в сигнале не бывает пауз или разрывов.

Аналоговый сигнал — сигнал, область определения которого есть непрерывное пространство, то есть пространство, не являющееся дискретным.

Различают два пространства сигналов - пространство L (непрерывные сигналы), и пространство l (L малое) - пространство последовательностей. Пространство l (L малое) есть пространство коэффициентов Фурье (счетного набора чисел, определяющих непрерывную функцию на конечном интервале области определения), пространство L - есть пространство непрерывных по области определения (аналоговых) сигналов. При некоторых условиях, пространство L однозначно отображается в пространство l.

Аналоговые сигналы описываются непрерывными функциями времени, поэтому аналоговый сигнал иногда называют непрерывным сигналом. Аналоговым сигналам противопоставляются дискретные (квантованные, цифровые).

Дискретный сигнал - информационный сигнал, который представляется в виде отдельных отсчетов взятых по времени, но, в отличие от цифрового сигнала, не обязательно квантованных по уровню.

Под цифровым сигналом понимается дискретный сигнал, квантованный по амплитуде.

Сигналы представляют собой дискретные электрические или световые импульсы. При таком способе вся емкость коммуникационного канала используется для передачи одного сигнала. Цифровой сигнал использует всю полосу пропускания кабеля. Полоса пропускания – это разница между максимальной и минимальной частотой, которая может быть передана по кабелю. Каждое устройство в таких сетях посылает данные в обоих направлениях, а некоторые могут одновременно принимать и передавать. Узкополосные системы (baseband) передают данные в виде цифрового сигнала одной частоты.

Дискретный цифровой сигнал сложнее передавать на большие расстояния, чем аналоговый сигнал, поэтому его предварительно модулируют на стороне передатчика, и демодулируют на стороне приёмника информации. Использование в цифровых системах алгоритмов проверки и восстановления цифровой информации позволяет существенно увеличить надёжность передачи информации.

Следует иметь ввиду, что цифровой сигнал по своей физической природе является "аналоговым". Этот аналоговый сигнал (импульсный и дискретный) наделяется свойствами числа. В результате для его обработки становится возможным использование численных методов.

36. Коаксиальный кабель, витая пара, оптоволокно.

Витой парой называют скрученная пара проводов. Скручивание проводов снижает влияние внешних и взаимных помех на полезные сигналы. Кабели на основе витой пары-симметричные, т.е. состоят из двух одинаковых в конструктивном отношении проводников. Такие кабеля могут быть экранированными и неэкранированными.

Неэкранированная – используется для проводки внутри здания.

Экранированная – защищает передаваемые сигналы от внешних помех и меньше излучает электромагнитные колебания вовне.

Коаксиальный кабель состоит из несимметричных пар проводников. Они не считаются хорошим вариантом для построения кабельной системы здания. Типы: «Толстый» Коак. Кабель – для сетей Ethernet 10Base-5 с волновым сопротивлением 50 Ом и толстым внутренним проводником диаметром 2,17мм (хорошие механические и электрические характер. И плохо гнется), «Тонкий» коак кабель – для сетей Ethernet 10Base-2 с волновым сопротивлением 50 Ом и тонким внутренним проводником диаметром 0,89мм, Телевизионный кабель – имеет волновое сопративление 75 Ом широко применяется в кабельном телевидении.

Волоконно-оптический кабель состоит из тонких (5-60 микрон) гибких стеклянных волокон, по которым распространяются световые сигналы. Это наиболее качественный кабель (высокая скорость и хорошая защита от помех).

37. Радиоволны, микроволны, инфракрасное излучение. Методы доступа к среде в беспроводных сетях.

Радиово́лны — электромагнитные волны, частоты которых условно ограничены частотами ниже 3000 ГГц, распространяющиеся в пространстве без искусственного волновода. При этом способе сигналы передаются в некоторой в полосе частот, что позволяет избежать проблем связи, присущих одночастотной передаче. Скорость передачи в 250 Кбит/с (килобит в секунду) относит данный способ к разряду самых медленных.

Микроволны – электромагнитное излучение, включающее в себя дециметровый, сантиметровый и миллиметровый диапазоны радиоволн (длина волны от 1 м — частота 300 МГц до 1 мм — 300 ГГц). Передают сигналы между двумя направленными параболическими антеннами, которые имеют форму тарелки.

Инфракра́сное излуче́ние — электромагнитное излучение, занимающее спектральную область между красным концом видимого света (с длиной волны λ = 0,74 мкм и частотой 430 ТГц) и микроволновым радиоизлучением (λ ~ 1—2 мм, частота 300 ГГц). Этот способ позволяет передавать сигналы с большой скоростью, поскольку ин-фракрасный свет имеет широкий диапазон частот. Инфракрасные сети способны нормально функционировать на скорости 10 Мбит/с.

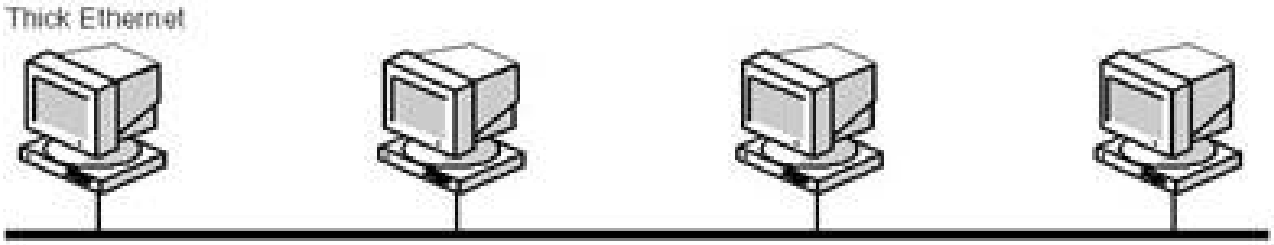
Георгафический д. позволяет использовать множество устройств на определенной территории, сама по себе приводит к неоправданному расточительству обычно скудных частотных ресурсов, поскольку требует выделения отдельной частоты для каждого беспроводного устройства.

TDM(уплотнение с временным разделением)-распределение каналов идет по времени, т. е. каждый передатчик транслирует сигнал на одной и той же частоте и в области, но в различные промежутки времени при строгих требованиях к синхронизации процесса передачи.

CDMA-все передатчики передают сигналы на одной и той же частоте,в области и во времи, но с разными кодами.

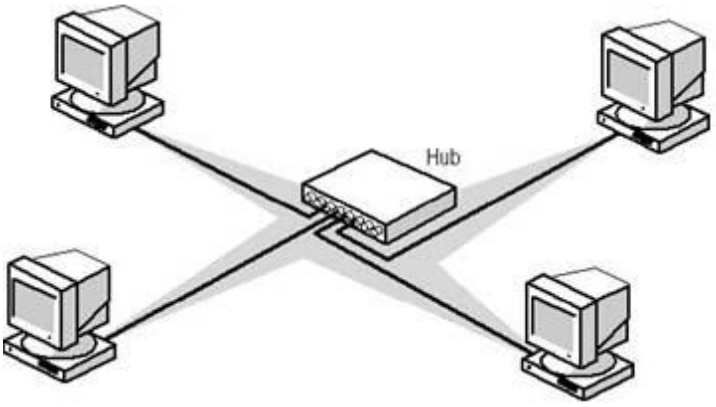
38. Коаксиальный кабель, как основная среда для реализации сети по топологии шина.

топология «шина»



В сетях типа «толстый» Ethernet компьютеры подключаются к общему коаксиальному кабелю с помощью кабелей меньшего размера, называемых кабелями AUI или трансиверами. В сети типа «тонкий» Ethernet компьютеры связаны друг с другом отдельными отрезками коаксиального кабеля меньшей толщины. Основной недостаток-дефект кабеля в любом месте его протяженности делит сеть на две части, не способные общаться между собой.

39. Витая пара, как основная среда для построения сети по топологии звезда.



топология «звезда» Основная часть портов концентратора предназначена для подключения кабелей специальных неэкранированных «витая пара». Т.к. она проста в монтаже, дешевая, помехоустойчивая, скорость 1000Мб/с.

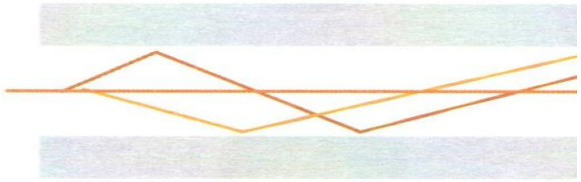
40. Принцип функционирования оптических сред передачи даных. Одномодовый и многомодовый (с линейным и градиентным коэффициентом преломления) кабель.

оптоволоконные кабеля уже полностью вытеснили медные (электрические) на магистральных каналах, и стремительно подбирается к конечному пользователю. Они состоят из тонких(5-60 микрон) гибких стеклянных волокон, по которым распространяются световые сигнал. Это наиболее качественный кабель (высокая скорость и хорошая защита от помех).

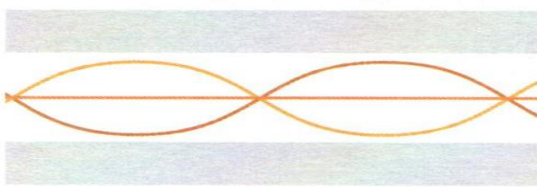
Одномодовый кабель(SMF) – диаметр центрального проводника 5-10мкм. Все лучи света распространяются вдоль оптической оси световода, не отражаясь от внешнего проводника.

Многомодовый (MMF) - диаметр центрального проводника 40-100мкм. Во внутреннем проводнике существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Режим отражения лучей в градиентовом мног.вол. имеет сложный характер.

Одномодовое волокно



Многомодовое волокно



Градиентное многомодовое волокно

41. Радиосети. Радиорелейные сети. Спутниковая связь.

Радиосеть - способ организации радиосвязи между тремя и более радиостанциями пунктов управления (командиров, штабов). В зависимости от назначения, связь в радиосети может обеспечиваться на одной частоте; на двух частотах; на частотах передатчиков; в комбинированной радиосети на частотах дежурного приема. При использовании радиостанций, оборудованных специальными устройствами, радиосвязь между ними может быть организована по абонентской радиосети.

Радиорелéйная свя́зь — один из видов наземной радиосвязи, основанный на многократной ретрансляции радиосигналов. Радиорелейная связь осуществляется, как правило, между стационарными объектами. Отличительной особенностью это связи от всех других видов наземной радиосвязи является использование узконаправленных антенн, а также дециметровых, сантиметровых или миллиметровых радиоволн.

Спутниковая связь используется для организации высокоскоростных микроволновых протяженных линий. Спутник отражает сигнал, чтобы можно было установить связь на большие расстояния.

42. Структура, классификация, протоколы систем мобильной связи.

Мобильная структура сети основана на принципе повторного использования частот – главном принципе мобильной сети. Элементами мобильной сети, кроме того, являются:– центр коммутации;– базовые станции;– подвижные станции, или абонентские радиотелефонные аппараты.

Классификация систем мобильной радиосвязи (СМРС):1.Наземные;1)системы персонального радиовызова;2)сотовые СМРС;3)системы с радиальной архитектурой;4)системы с радиально-зоновой архитектурой, транкинговая система мобильной радиосвязи;5)зоновые СМРС 2.Спутниковые;1)геостационарные (спутник находится на геостационарной орбите, высота около 36 тыс. км);2)среднеорбитальные;3)низкоорбитальные;4)высокоэллиптические

Протоколы: GSM - покрывает территорию, разбивая ее на ячейки - соты. (сотовая связь). CDMA –расщепление спектра(сигнал делится на множество потоков со значительно более узкой полосой спектра).

43. Основы кодирование сигналов: физическое, потенциальное и импульсное кодирование

Кодирование – Представление данных в виде электрических или оптических сигналов.

Физические код. - определяет число дискретных уровней сигнала (амплитуды напряжения, амплитуды тока, амплитуды яркости).

Потенциальный – Единице соответствует один уровень напряжения.

Импульсный – для представления цифр используют импульсы различной полярности.

44. Цифровое и логическое кодирование

Логическое кодирование подразумевает замену бит исходной информационной последовательности новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных или надежно поддерживать синхронизацию с поступающим сигналом.

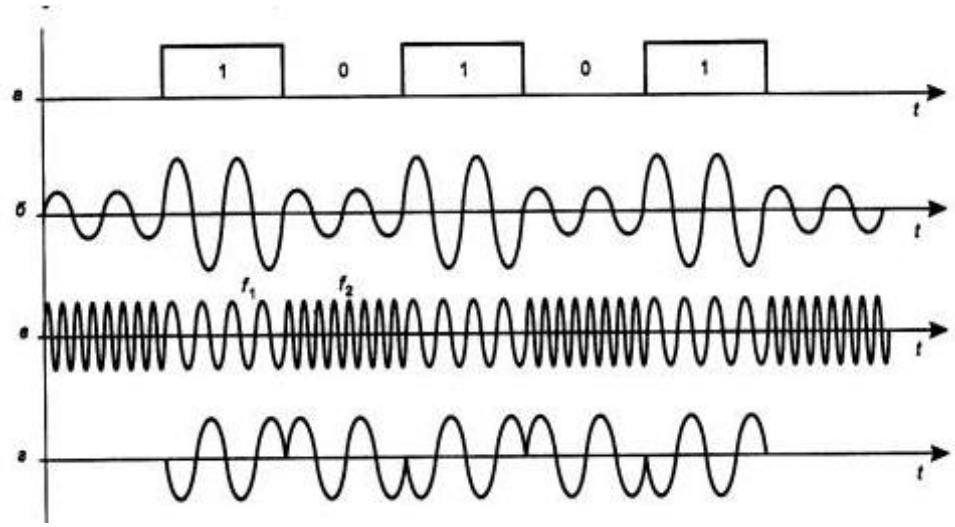
Цифровое кодирование – данные представляются в двоичный код, после чего кодируются(потенциальным или импульсным способ.) двоичные цифры.

45. Аналоговая модуляция применяется для передачи дискретных данных по каналам с узкой полосой частот, типичным

Аналоговая модуляция и методы аналоговой модуляции. Дискретная модуляция

аналоговых сигналов.

телефонных сетей. Аналоговая модуляция является таким способом физического кодирования, при котором информация кодируется изменением амплитуды, частоты или фазы синусоидального сигнала несущей частоты



а – исходные данные, б - амплитудная мод. В – частотная мод. Г - фазовая мод.

Дискретные способы модуляции основаны на дискретизации непрерывных процессов как по амплитуде, так и по времени.

46.Принципы межсетевого взаимодействия. Гетерогенность и проблемы межсетевого взаимодействия. Основные подходы к организация межсетевого взаимодействия.

межсетевое взаимодействие — это способ соединения компьютерной сети с другими сетями с помощью шлюзов, которые обеспечивают общепринятый порядок маршрутизации пакетов информации между сетями. Полученная система взаимосвязанных сетей называется составной сетью, или просто интерсетью. Наиболее ярким примером межсетевого взаимодействия является Интернет.

Сети неоднородные (гетерогенные), которые состоят из различных рабочих станций, операционных систем и приложений, а для реализации взаимодействия между компьютерами используют различные протоколы. Разнообразие всех компонентов, из которых строится сеть, порождает еще большее разнообразие структур сетей, получающихся из этих компонентов. Основные проблемы при организации взаимодействия различных сетей связаны с тем, что эти сети используют различные стеки коммуникационных протоколов. В каждом конкретном стеке протоколов средства, реализующие какой-либо уровень, обеспечивают интерфейс для вышележащего уровня своей системы и пользуются услугами интерфейсных функций нижележащего уровня.

Подходы: 1.трансляция - обеспечивает согласование стеков протоколов путем преобразования сообщений, поступающих от одной сети в формат сообщений другой сети.2.Мультиплексирование - в сетевое оборудование или в операционные системы серверов и рабочих станций встраиваются несколько стеков протоколов. 3.инкапсуляция - может быть использована, когда две сети с одной транспортной технологией необходимо соединить через транзитную сеть с другой транспортной технологией.

47. Мультиплексирование стеков протоколов

При мультиплексировании стеков протоколов на один из двух взаимодействующих компьютеров с различными стеками протоколов помещается коммуникационный стек другого компьютера. Для того, чтобы запрос от прикладного процесса был правильно обработан и направлен через соответствующий стек, в компьютер необходимо добавить специальный программный элемент - мультиплексор протоколов. Мультиплексор должен уметь определять, к какой сети направляется запрос клиента.

48. Особенности согласования сетей на транспортном уровне. Средства согласования физического уровня. Средства согласования на канальном уровне.

Согласование различных физических уровней одной и той же технологии выполняется концентраторами, имеющими порты с приемопередатчиками (трансиверами) различных типов. В стандартах новых технологий для работы с различными вариантами физической среды физический уровень обычно делится на две части: часть, зависящую от физической среды, и часть, не зависящую от физической среды.

Согласование протоколов канального уровня - для этого могут быть использованы некоторые типы мостов и коммутаторов. В частности, в объединяемых сетях должны совпадать максимальные размеры полей данных в кадрах, так как канальные протоколы, как правило, не поддерживают функции фрагментации пакетов.

49. Сетевые устройства: повторители, концентраторы, мосты, коммутаторы, маршрутизаторы.

Устройства, подключенные к какому-либо сегменту сети, называют сетевыми устройствами. Повторители (репитер) – функционирует на физическом уровне эталонной модели OSI. Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние(из слабого сигнала в сильный). Концентратор - принимает электронные сигналы одного порта и воспроизводит (или ретранслирует) то же сообщение для всех остальных портов. Мост – собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов. По этой причине они могут быстро пересылать данные любых протоколов сетевого уровня. Коммутаторы - соединяет несколько узлов с сетью. В отличие от концентратора, коммутатор в состоянии передать сообщение конкретному узлу. Когда узел отправляет сообщение другому узлу через коммутатор, тот принимает и декодирует кадры и считывает физический (MAC) адрес сообщения. Маршрутизатор - устройства объединенных сетей, которые пересылают пакеты между сетями на основе адресов третьего уровня. Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных.

50. Протоколы TCP и UDP.

Transfer Control Protocol – TCP. Надежность TCP заключается в том, что источник данных повторяет их посылку, если только не получит в определенный промежуток времени от адресата подтверждение об их успешном получении. В заголовке TCP существует поле контрольной суммы. Если при пересылке данные повреждены, то по контрольной сумме модуль может определить это. Поврежденный пакет уничтожается, а источнику ничего не посылается.

User Datagram Protocol – UDP. Один из двух протоколов транспортного уровня, которые используются в стеке протоколов TCP/IP. UDP позволяет прикладной программе передавать свои сообщения по сети с минимальными издержками, связанными с преобразованием протоколов уровня приложения в протокол IP. Однако при этом, прикладная программа сама должна заботиться о подтверждении того, что сообщение доставлено по месту назначения.

51. Основные принципы маршрутизации. Правила маршрутизации. Построение таблицмаршрутизации

Цель маршрутизации - доставка пакетов по назначению с максимизацией эффективности. Маршрутизация сводится к определению направлений движения пакетов в маршрутизаторах. Правила маршрутизации определяют куда и как должны посылаться пакеты для разных сетей и состоит из следующих компонентов:1. Начальный адрес подсети, порядок достижения которой описывает правило.2. Маска подсети, которую описывает правило.3. Шлюз показывает, на какой адрес будут посланы пакеты, идущие в сеть назначения.4. Интерфейс показывает через какой сетевой адаптер (его номер или IP адрес) должен посылаться пакет в заданную сеть.5. Метрика показывает время, за которое пакет может достигнуть сети получателя (величина условная и может быть изменена при маршрутизации). Если имеется несколько правил достижения одной сети, пакеты посылаются по правилу с наименьшей метрикой.

Таблица: 1.Сетевой адрес 2.Маска сети 3.Адрес шлюза 4.Интерфейс 5.Метрика

52. Сети TCP/IP. Принципы объединения сетей с помощью протоколов сетевого уровня.

Протоколы TCP/IP – разработаны специально для применения в сети с коммутацией пакетов, создававшейся Министерством обороны США. Тогда эта сеть называлась ARPANET, теперь же — Интернет. используется гибкая схема адресации, весьма удачная для маршрутизации даже в самых больших сетях. Пакеты данных можно коммутировать (перенаправлять в другую подсеть) в зависимости от адреса назначения, поддерживается практически во всех операционных системах и на всех платформах, является протоколом глобальной сети Internet. В любой системе, подключаемой к Internet, должен быть реализован протокол TCP/IP. TCP/IP присущи наименьшее быстродействие и наибольшая сложность конфигурирования.

Основная идея введения сетевого уровня состоит в следующем. Сеть в общем случае рассматривается как совокупность нескольких сетей и называется составной сетью или интерсетью. Сети, входящие в составную сеть, называются подсетями, составляющими сетями или просто сетями. Подсети соединяются между собой маршрутизаторами. Сетевой уровень выступает в качестве координатора, организующего работу всех подсетей, лежащих на пути продвижения пакета по составной сети. Для перемещения данных в пределах подсетей сетевой уровень обращается к используемым в этих подсетях технологиям.

53.Семейство протоколов TCP/IP. Протокол межсетевого взаимодействия IP, версии протокола.

TCP/IP – название семейства протоколов передачи данных в сети. Протокол – набор правил и команд (язык) с помощью которых происходит передача данных в сети. Протокол TCP/IP – сетевой протокол, обеспечивающий коммуникации по объединенным сетям, составленным из компьютеров с различной аппаратной архитектурой, работающих под управлением различных операционных систем. TCP/IP может использоваться для поддержки коммуникаций с системами Windows NT, с устройствами, использующими другие сетевые продукты Microsoft, а также с системами, отличными от Microsoft, например, UNIX-системами.
Семейство протоколов TCP/IP является стандартным набором сетевых протоколов или правил, управляющих способом передачи данных между компьютерами в сети. TCP/IP используется для соединения с Интернет, объединенной сетью в масштабах всего мира, охватывающей множество университетов, исследовательских лабораторий, организаций, корпораций, а также частные корпоративные сети, объединяющих несколько локальных сетей..

Семейство протоколов TCP/IP

В состав семейства входят протоколы UDP, ARP, ICMP, TELNET, FTP и многие другие. TCP/IP - это технология межсетевого взаимодействия, технология internet. Сеть, которая использует технологию internet, называется "internet. Для отображения IP-адресов в Ethernet адреса используется протокол ARP (Address Resolution Protocol - адресный протокол). Отображение выполняется только для отправляемых IP-пакетов, так как только в момент отправки создаются заголовки IP и Ethernet.

Протокол межсетевого взаимодействия (IP)

Протокол межсетевого взаимодействия (IP) — механизм передачи, используемый протоколами TCP/IP. Это ненадежная служба доставки дейтаграммы без установления соединения, но с "максимальными усилиями" (best-effort).Термин с "максимальными усилиями" означает, что делается все возможное (максимальные усилия), чтобы передать информацию к ее пункту назначения, но IP не обеспечивает никакой проверки ошибок или их отслеживания. IP предполагает ненадежность основных уровней, без гарантий требуемого уровня сервиса.

IP транспортирует данные в пакетах, называемые дейтаграммами, каждая из которых транспортируется отдельно. Дейтаграммы могут перемещаться по различным маршрутам и могут прибыть не в исходной последовательности или быть дублированы. IP не сохраняет копию маршрутов и не имеет никаких средств для того, чтобы переупорядочить дейтаграммы, как только они достигают пункта назначения.

Ограниченные функциональные возможности IP, однако, нельзя считать слабостью. IP обеспечивает "чистые" функции передачи, которые освобождены от пользовательских особенностей, и предполагает, что на других уровнях будут добавлены те средства, которые необходимы для данного приложения, и таким образом будет достигнута максимальная эффективность.

54.Адресация в IP-сетях. Использование масок и подсетей. IPv6 как развитие

стека TCP/I.

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:
· Локальный адрес узла
· Символьный идентификатор-имя
· IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме, и разделенных точками, например:
128.10.2.30 - традиционная десятичная форма представления адреса,
10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера узла в сети. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:
· Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса A имеют номера в диапазоне от 1 до 126. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже.) В сетях класса A количество узлов должно быть больше 216 , но не превышать 224.
· Если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 28 - 216. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта.
· Если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла - 8 битов.
Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
· Если адрес начинается с последовательности 11110, то это адрес класса E, он зарезервирован для будущих применений.

Использование масок и подсетей.
Важным элементом разбиения адресного пространства Internet являются подсети. Подсеть – это подмножество сети, не пересекающееся с другими подсетями. Это означает, что сеть организации может быть разбита на фрагменты, каждый из которых будет составлять подсеть. Реально, каждая подсеть соответствует физической локальной сети (например, сегменту Ethernet). Подсети используются для того, чтобы обойти ограничения физических сетей на число узлов в них и максимальную длину кабеля в сегменте сети. Например, сегмент тонкого Ethernet имеет максимальную длину 185 м и может включать до 32 узлов. Самая маленькая сеть класса C может состоять из 254 узлов. Для того чтобы достичь этого значения, необходимо объединить несколько физических сегментов сети. Сделать это можно либо с помощью физических устройств (например, повторителей), либо при помощи машин-шлюзов. В первом случае разбиение на подсети не требуется, так как логически сеть выглядит как одно целое. При использовании шлюза сеть разбивается на подсети.

Маска подсети – это четыре байта, которые накладываются на IP-адрес для получения номера подсети. Например, маска 255.255.255.0 позволяет разбить сеть класса B на 254 подсети по 254 узла в каждой. Подсети не только решают, но и создают ряд проблем. Например, происходит потеря адресов, но уже не по причине физических ограничений, а по причине принципа построения адресов подсети. Так, выделение трех битов на адрес подсети приводит к образованию не восьми, а только шести подсетей, так как номера 0 и 7 нельзя использовать в силу специального значения IP-адресов, состоящих из нулей или из единиц.

Для стандартных классов сетей маски имеют следующие значения:
класс A – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
класс B – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
класс C – 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой. Например, адрес 185.23.44.206 попадает в диапазон 128-191, то есть адрес относится к классу B.

Следовательно, номером сети являются первые два байта, дополненные двумя нулевыми байтами – 185.23.0.0, а номером узла – 0.0.44.206. Если этот адрес ас- 24 социировать с маской 255.255.255.0, то номером подсети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов.

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

IP-адрес 129.64.134.5 – 10000001.01000000.10000110.00000101
Маска 255.255.128.0 – 11111111.11111111.10000000.00000000
Если использовать для определения границы номера сети маску, то 17 последовательных единиц в маске, «наложенные» на IP-адрес, определяют в качестве номера сети в двоичном выражении число: 10000001. 01000000. 10000000. 00000000 или в десятичной форме записи номер сети 129.64.128.0, а номер узла 0.0.6.5.

. IPv6 как развитие стека TCP/I.

Новая (шестая) версия протокола IP (IPv6) внесла существенные изменения в систему адресации. Прежде всего, это коснулось увеличения разрядности адреса: вместо 4 байт IP-адреса в версии IPv4 в новой версии под адрес отведено16 байт. Это дает возможность пронумеровать огромное количество узлов:

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

Вместо прежних двух уровней иерархии адреса (номер сети и номер узла) в IPv6 имеется 4 уровня, из которых три уровня используются для идентификации сетей, а один —для идентификации узлов сети. В новой версии не поддерживаются классы адресов (A, B, C, D, E), но широко используется технология CIDR. Благодаря этому, а также усовершенствованной системе групповой адресации и введению адресов нового типа IPv6 позволяет снизишь затраты на маршрутизацию.

55.Типы протоколов обмена маршрутной информацией. Протоколы DHCP, OSPF, RIP,ARP, RARP

Протокол ARP (Протокол распознавания адреса) *предназначен для преобразования IP-адресов в MAC-адреса, часто называемые также физическими адресами*.

TCP/IP использует протоколы ARP (Address Resolution Protocol - протокол преобразования адресов) и RARP (Reverse Address Resolution Protocol - протокол обратного преобразования адресов) для инициализации использования адресов Internet в сетях Ethernet и сетях иных типов, использующих метод MAC (media access control) для управления доступом к среде передачи. Протокол ARP позволяет хостам обмениваться информацией с другими хостами в тех случаях, когда известен только IP-адрес ближайшего соседа. Перед тем, как использовать IP хост передает широковещательный запрос ARP, содержащий IP-адрес желаемой системы-получателя.

Протокол **(DHCP)** Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.
В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.
При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно другие параметры конфигурации клиента) из пула наличных IP-адресов без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.

Протокол RIP.Этот протокол маршрутизации предназначен для сравнительно небольших и относительно однородных сетей. Маршрут здесь характеризуется вектором расстояния до места назначения. Предполагается, что каждый маршрутизатор является отправной точкой нескольких маршрутов до сетей, с которыми он связан.

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

OSPF (Open Shortest Path First) – дословно переводится как «Сперва открытый короткий путь» - надежный протокол внутренней маршрутизации с учетом состояния каналов (Interior gateway protocol, IGP). Как правило, данный протокол маршрутизации начинает использоваться тогда, когда протокола RIP уже не хватает по причине усложнения сети и необходимости в её легком масштабировании. OSPF наиболее широко используемый протокол внутренней маршрутизации. Когда идёт речь о внутренней маршрутизации, то это означает, что связь между маршрутизаторами устанавливается в одном домене маршрутизации, или в одной автономной системе. Представьте компанию среднего масштаба с несколькими зданиями и различными департаментами, каждое из которых связано с другим с помощью канала связи, которые дублируются с целью увеличения надежности. Все здания являются частью одной автономной системы. Однако при использовании OSPF, появляется понятие «площадка», «зона» (Area), которое позволяет сильнее сегментировать сеть, к примеру, разделение по «зонам» для каждого отдельного департамента.

56 Сокеты. Передача данных по сети с использованием сокет.
Сокет(гнездо, разъем) – это программная абстракция, используемая для представления “терминалов” соединений между двумя машинами.

Каждый из сокетов определяется типом и ассоциированным с ним процессом. Реально для передачи организуются определенные дескрипторы TCP-соединения, т.н. гнезда (socket): гнездо сервера и гнездо клиента, которые в Internet домене включают в себя **IP-адреса сервера и клиента и номера портов**, через которые они взаимодействуют. Сервер, обычно, имеет закрепленный и постоянный во взаимодействии номер порта, а клиенту, обращающемуся по этому номеру для связи к серверу, назначается некоторый другой (эфемерный) номер порта после установления соединения с сервером на сеанс их взаимодействия и таким образом основной порт освобождается, для установления последующих связей (номер порта выбирается сервером из числа незанятых в диапазоне от **1024 до 65535**).

Сокеты для работы в сети можно создать 2-х типов:

1) Потоковые для TCP-соединения. TCP могут передавать даннные только между 2-мя приложениями, так как они предполагают наличие канала между этими приложениями.

2) Датаграммные. Для датаграмм не нужно создавать канал, данные посылаются приложению с использованием адреса, состоящего из сокета и номера порта. (В датаграммах не гарантируется доставка и корректность последовательности передачи пакетов) Для передачи датаграмм не нужны ни механизмы подтверждения связи, ни механизмы управления потоком данных.

57.Методы коммутации: коммутация каналов, коммутация пакетов, коммутация сообщений.

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

Коммутация сообщений – разбиение информации на сообщения, каждый из которых состоит из заголовка и информации. Это способ взаимодействия, при котором создается логический канал, путем последовательной передачи сообщений через узлы связи по адресу указанному в заголовке сообщения.При этом каждый узел принимает сообщение, записывает в память, обрабатывает заголовок, выбирает маршрут и выдает сообщение из памяти в следующий узел.

Коммутация пакетов - это особый способ коммутации узлов сети, который специально создавался для наилучшей передачи компьютерного трафика (пульсирующего трафика). Опыты по разработке самых первых компьютерных сетей, в основе которых лежала техника коммутации каналов, показали, что этот вид коммутации не предоставляет возможности получить высокую пропускную способность вычислительной сети. Причина крылась в пульсирующем характере трафика, который генерируют типичные сетевые приложения.

При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Необходимо уточнить, что сообщением называется логически завершенная порция данных - запрос на передачу файла, ответ на этот запрос, содержащий весь файл, и т. п. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт (EtherNet). Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения.

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета.

58 Мультиплексирование, виды мультиплексирования.

Мультиплексирование (англ. multiplexing, muxing)— это процесс уплотнение канала связи, другими словами, передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу связи, с использованием специального устройства, называемого мультиплексором.

Мультиплексор (MUX) — комбинационное устройство, обеспечивающее передачу в желаемом порядке цифровой информации, поступающей по нескольким входам на один выход. Может быть реализован как аппаратно так и программно.

Временное мультиплексирование (Time Division Multiplexing, TDM)
Частотное мультиплексирование (Frequency Division Multiplexing, FDM)
Волновое мультиплексирование (Wave Division Multiplexing, WDM)
Множественный доступ с кодовым разделением (CodeDivisionMultipleAccess, CDMA) - каждый канал имеет свой код наложение которого на групповой сигнал позволяет выделить информацию конкретного канала.

Временное мультиплексирование

Первой стали применять технологию TDM, которая широко используется в обычных системах электросвязи. Эта технология предусматривает объединение нескольких входных низкоскоростных каналов в один составной высокоскоростной канал.

Частотное мультиплексирование

Техника частотного мультиплексирования разрабатывалась для телефонных сетей. Основная идея состоит в выделении каждому соединению собственного диапазона частот в общей полосе пропускания линии связи. Мультиплексирование выполняется с помощь смесителя частот, а демультиплексирование – с помощью узкополосного фильтра, ширина которого равна ширине диапазона канала.

Частотное мультиплексирование

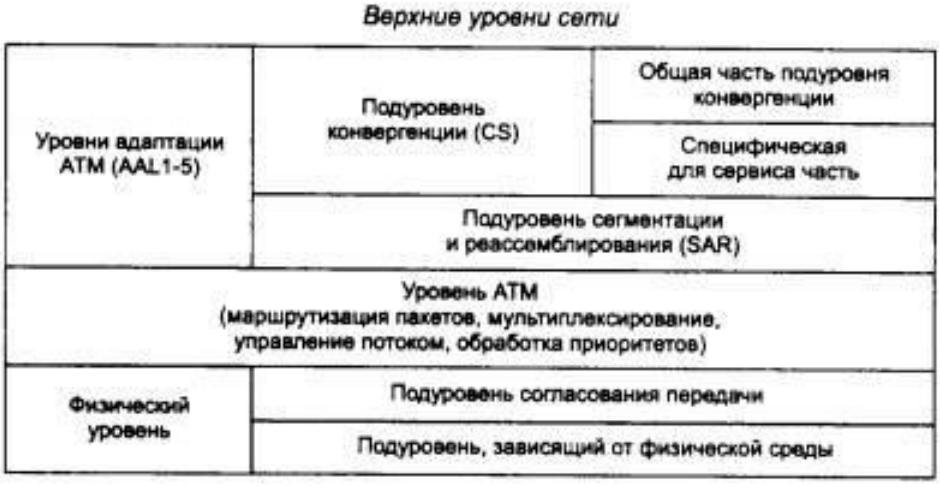
Техника частотного мультиплексирования разрабатывалась для телефонных сетей. Основная идея состоит в выделении каждому соединению собственного диапазона частот в общей полосе пропускания линии связи. Мультиплексирование выполняется с помощь смесителя частот, а демультиплексирование – с помощью узкополосного фильтра, ширина которого равна ширине диапазона канала.

59.Технология ATM, основные принципы технологии ATM, стек протоколов ATM, классы сервиса.

Технология ATM является наиболее перспективным решением задачи переноса разнородной информации в широкополосных цифровых сетях с интеграцией служб. Это - специфический, подобный пакетному, метод переноса информации, использующий принцип асинхронного временного мультиплексирования.

Метод ATM является ориентированным на соединения: любой передаче информации предшествует организация виртуального соединения (коммутируемого или постоянного) между отправителем и получателем данных, что впоследствии упрощает процедуры маршрутизации. Данные перед их передачей по каналам связи делятся на участки длиной 48 байт. К ним добавляется заголовок (5 байт). Образуются ячейки, которые передаются с использованием виртуальных каналов, т.е. имеющих идентификатор логических каналов, организуемых между двумя устройствами для установления связи. В одном физическом канале связи, как правило, передаются совместно ячейки, принадлежащие множеству различных виртуальных каналов. Ячейки, поступающие от различных комплектов оконечного оборудования данных, объединяются в канале связи, образуя групповой сигнал, и коммутируются в узлах сети.

Стек протоколов ATM показан на рис



Стек протоколов ATM соответствует нижним уровням семиуровневой модели ISO/OSI и включает уровень адаптации ATM, собственно уровень ATM и физический уровень. Прямого соответствия между уровнями протоколов технологии ATM и уровнями модели OSI нет.

Классы сервиса ATM содержат ряд параметров, которые определяют гарантии качества сервиса. В спецификациях форума ATM предусмотрено несколько классов

сервиса - CBR, VBR, UBR и др. Гарантии качества сервиса могут определять минимальный уровень доступной пропускной способности, предельное значение задержки ячейки и вероятность потери ячейки. В архитектуре ATM приложение заказывает у сети определенное качество обслуживания, и сеть динамически выделяет приложению необходимые ресурсы. В рассматриваемых нами DSL-линиях отсутствует сеть ATM в классическом понимании, и качество обслуживания сводится к статической настройке параметров передачи исходящих ячеек.

CBR (Constant Bit Rate) - постоянная битовая скорость, представляет собой наиболее простой класс сервиса ATM. Основной параметр - пиковая скорость передачи ячеек PCR (Peak Cell Rate) - максимальная скорость, которая может потребоваться каналу без риска потерять ячейку. Данные передаются по этому соединению с запрошенной скоростью - не быстрее и, во многих случаях, не медленнее. Трафик, передаваемый с большей скоростью, может теряться. CBR-соединения должны гарантировать пропускную способность с минимальной вероятностью потери ячейки и низкими изменениями задержки передачи ячейки. Сервис CBR предназначен специально для передачи голоса и видео в реальном времени.

UBR (Unspecified Bit Rate) - неопределенная битовая скорость, не определяет ни битовую скорость, ни параметры трафика, ни качество сервиса. Сервис UBR предлагает только доставку "по возможности", безо всяких гарантий. Сервис UBR представляет собой решение для эластичного трафика, не критичного к реальному времени и полосе пропускания. Этот класс сервиса обычно устанавливается по умолчанию.

VBR (Variable Bit Rate) - переменная битовая скоростью. По сравнению с сервисом CBR, VBR требует более сложной процедуры заказа соединения между сетью и приложением. В дополнение к пиковой скорости VBR определяет длительно поддерживаемую скорость (среднюю скорость ячеек в секунду) SCR (Sustained Cell Rate), которая представляет собой среднюю гарантированную скорость передачи данных. Канал может превышать скорость SCR вплоть до величины PCR, но только на определенное количество ячеек MBS (Maximum Burst Size), которое может быть передано со скоростью большей чем SCR, но меньшей чем PCR. VBR будет использовать среднее значение SCR для управления трафиком, снижая его интенсивность на соответствующие периоды времени. Как и в случае CBR, пользователи VBR получают гарантированное обслуживание в отношении потерь ячеек, изменения задержек передачи ячеек и доступной полосы пропускания до тех пор, пока трафик удовлетворяет определенным при соединении требованиям.

60.Принципы построения глобальной компьютерной сети Интернет

Интернет (англ.Internet, от*Inter*connected*Net*works — объединённые сети) — глобальная телекоммуникационная сеть информационных и вычислительных ресурсов. Служит физической основой для Всемирной паутины. Часто упоминается как Всемирная сеть, Глобальная сеть, либо просто Сеть.

Интернет состоит из многих тысяч корпоративных, научных, правительственных и домашних компьютерных сетей. Объединение сетей разной архитектуры и топологии стало возможно благодаря протоколу IP и принципу маршрутизации пакетов данных.

Что же такое протокол? Протокол — это правила передачи данных между узлами компьютерной сети. Для того, чтобы различные компьютеры сети могли взаимодействовать, они должны «разговаривать» на одном «языке», то есть использовать один и тот же протокол. Основными протоколами, используемыми в сети Интернет для передачи данных, являются TCP/IP («протокол управления передачей/межсетевой протокол»), HTTP («протокол передачи гипертекста»), FTP («протокол передачи файлов»).

Каждый компьютер, подключенный к Интернету, имеет уникальный адрес. Для записи адресов используются два равноценных формата - IP и DNS адреса.

IP-адрес состоит из четырех чисел со значениями от 0 до 255, разделенных точками (например, 195.27.38.172), и включает в себя две логические части - номер сети и номер узла в сети. Такая схема нумерации позволяет иметь в сети более четырех миллиардов компьютеров. Когда локальная сеть или отдельный компьютер впервые присоединяется к сети Интернет, специальная организация (провайдер) присваивает им IP-адрес, гарантируя его уникальность и правильность подключения.

Для удобства компьютерам в Интернете кроме цифровых адресов присваиваются собственные имена. При этом, как и в случае с IP-адресами, необходима уникальность этого имени. С этой целью была создана специальная система адресации - DNS («доменная система имен»). Доменные имена, в отличие от IP-адресов, необязательны, они

приобретаются дополнительно. DNS-адрес вместо цифр содержит буквы, разделяемые точками на отдельные уровни. Первым в DNS-адресе стоит имя реального компьютера с IP-адресом. Далее последовательно идут адреса доменов, в которые входит компьютер, вплоть до домена страны (для них принята двухбуквенная кодировка). Рассмотрим DNS-имя dit.isuct.ru. Здесь ru – национальный домен первого уровня, обозначающий Россию; isuct– доменное имя второго уровня, обозначающее организацию ИГХТУ; dit– доменное имя третьего уровня. По такому принципу иерархии строятся все DNS-имена.

Основными службами сети Интернет являются Всемирная паутина (WorldWideWeb), электронная почта (electronicmail), поисковые системы, веб-форумы, различные рассылки, файлообменные серверы и телеконференции (Usenet). Найти веб-страницу или файл в Интернете можно с помощью универсального указателя ресурсов –URL.

URL — это стандартизированный способ записи адреса ресурса в сети Интернет. Он включает в себя протокол доступа к документу, доменное имя сервера или его IP-адрес, а также полный путь к файлу на веб-сервере. Например, адрес статьи «Интернет» портала Википедия имеет вид

http://ru.wikipedia.org/wiki/Интернет,

где http:// - протокол доступа, ru.wikipedia.org – доменное имя сервера, /wiki/Интернет – путь к файлу.

Просмотр веб-страниц осуществляется с помощью специальных программ просмотра – браузеров. Браузер позволяет пользователю открывать и просматривать веб-страницы, а также перемещаться между документами в веб-пространстве. В настоящее время наиболее распространенными браузерами являются MozillaFirefox,OperaиInternetExplorer.

61.Сети ISDN.

ISDN(IntegratedServiceDigitalNetwork— цифровые сети с интегральными услугами) относятся к сетям, в которых основным режимом коммутации является режим коммутации каналов, а. данные обрабатываются в цифровой форме

Пользовательские интерфейсы ISDN. Одним из базовых принципов ISDN является предоставление пользователю стандартного интерфейса, с помощью которого пользователь может запрашивать у сети разнообразные услуги. Этот интерфейс образуется между двумя типами оборудования, устанавливаемого в помещении пользователя :терминальным оборудованием пользователя TE (компьютер с соответствующим адаптером, маршрутизатор, телефонный аппарат) и сетевым окончанием NT, которое представляет собой устройство, завершающее канал связи с ближайшим коммутатором ISDN. Пользовательский интерфейс основан на каналах трех типов: B — со скоростью передачи данных 64 кбит/с;D— со скоростью передачи данных 16 или 64 кбит/с, H — со скоростью передачи данных 384 кбит/с (H0), 1536 кбит/с (H 11) или 1920 кбит/с (H12).

Каналы типа B обеспечивают передачу пользовательских данных (оцифрованного голоса, компьютерных данных или смеси голоса и данных) и с более низкими скоростями, чем 64 кбит/с.
Канал типа D является каналом доступа к служебной сети с коммутацией пакетов, передающей сигнальную информацию. Передача адресной информации, на основе которой осуществляется коммутация каналов типа B в коммутаторах сети, является основной функцией канала D. другой его функцией является поддержание услуг низкоскоростной сети с коммутацией пакетов для пользовательских данных. Обычно эта услуга выполняется сетью в то время, когда каналы типа D свободны от выполнения основной функции.
Каналы типа H предоставляют пользователям возможности высокоскоростной передачи данных. На них могут работать службы высокоскоростной передачи факсов, видеоинформации, качественного воспроизведения звука.

Сеть ISDN поддерживает два типа пользовательского интерфейса — начальный (BasicRateInterface, BRI) и основной (PrimaryRateInterface, PRI).

Начальный интерфейс BRI предоставляет пользователю два канала по 64 кбит/с для передачи данных (каналы типа B) и один канал с пропускной способностью 16 кбит/с для передачи управляющей информации (канал типа D). Все каналы работают в полнодуплексном режиме.
Основной интерфейс PRI предназначен для пользователей с повышенными требованиями к пропускной способности сети. Интерфейс PRI поддерживает либо

схему 30B+D, либо схему 23B+D. В обеих схемах канал D обеспечивает скорость 64 кбит/с. Первый вариант предназначен для Европы, второй — для Северной Америки и Японии.

Адресация в сетях ISDN. Технология ISDN разрабатывалась как основа всемирной телекоммуникационной сети, позволяющей связывать как телефонных абонентов, так и абонентов других глобальных сетей — компьютерных, телексных. Основное назначение ISDN— передача телефонного трафика. Поэтому за основу адреса ISDN был взят формат международного телефонного плана номеров, описанный в стандарте ITU-T E.163. Однако этот формат был расширен для поддержки большего числа абонентов и для использования в нем адресов других сетей, например X.25. Стандарт адресации в сетях ISDN получил номер E.164.

Формат E.163 предусматривает до 12 десятичных цифр в номере, а формат адреса ISDNв стандарте E.164 расширен до 55 десятичных цифр. В сетях ISDN различают номер абонента и адрес абонента.

Использование служб ISDN для передачи данных. Несмотря на значительные отличия от аналоговых телефонных сетей, сети ISDN сегодня используются в основном так же, как аналоговые телефонные сети, то есть как сети с коммутацией каналов, но только более скоростные: интерфейс BRI дает возможность установить дуплексный режим обмена со скоростью 128 кбит/с (логическое объединение двух каналов типа B), а интерфейс PRI — 2,048 Мбит/с. Кроме того, качество цифровых каналов гораздо выше, чем аналоговых. Это значит, что процент искаженных кадров будет гораздо ниже, а полезная скорость обмена данными существенно выше. Обычно интерфейс BRI используется в коммуникационном оборудовании для подключения отдельных компьютеров или небольших локальных сетей, а интерфейс BRI— в маршрутизаторах, рассчитанных на сети средних размеров. Сети ISDN не рассматриваются разработчиками сетей передачи данных как хорошее средство для создания магистрали. Основная причина — отсутствие скоростной службы коммутации пакетов и невысокие скорости каналов, предоставляемых конечным пользователям. для целей же подключения мобильных и домашних пользователей, небольших филиалов и образования резервных каналов связи сети ISDN сейчас используются очень широко, естественно там, где они существуют.

62.Сети X.25, Frame Relay.

Сети **X.25**, работающие по одноименному стеку протоколов, предложенному международным телекоммуникационным союзом **ITU** (**International Telecommunication Union**), относятся к первому поколению сетей коммутации пакетов. Стандарт **X.25**относится к трем нижним уровням ЭМВОС, т. е. включает протоколы физического, канального и сетевого уровней. На сетевом уровне используется коммутация пакетов.

В сетях пакетной коммутации **Frame Relay** (**FR**) в отличие от сетей **X.25**обеспечивается большая скорость передачи данных (до **45 Мбит/с**) за счет исключения контроля ошибок в промежуточных узлах, так как контроль, адресация, инкапсуляция и восстановление выполняются в оконечных пунктах, т. е. на транспортном уровне. В промежуточных узлах ошибочные пакеты могут только отбрасываться, а запрос на повторную передачу происходит от конечного узла средствами уровня, выше сетевого. Но для реализации **FR** нужны помехо-устойчивые каналы передачи данных.

1.Архитектура и технологии построения сетей X.25

X.25 – это технология построения сети передачи данных с коммутацией пакетов. Архитектура X.25 включает описание процедур (протоколов) трех нижних уровней ЭМВОС: физического, звена данных и сетевого (а также частично транспортного). Сети X.25 отличаются способностью работать по каналам низкого качества с вероятностью ошибки в канале передачи до 0,01, но, как правило, с небольшой скоростью (единицы – десятки килобит в секунду). Основной недостаток – невозможность интерактивной работы в режиме реального времени (время доставки пакетов является случайным и относительно большим).

2. Архитектура и технологии построения сетей Frame Relay

Frame Relay – это технология построения сети передачи данных с ретрансляцией кадров, являющейся разновидностью быстрой коммутацией пакетов. Технология была создана для замены технологии X.25 путем ее упрощения с целью повышения эффективности передачи данных по высокоскоростным и надежным цифровым каналам. Стандарты FR описывают интерфейс доступа к сетям с быстрой коммутацией пакетов и включают процедуры (протоколы) двух нижних уровней ЭМВОС – физического и звена данных (не полностью, но с дополнительными функциями сетевого уровня). Как и X.25, технология обеспечивает образование и поддержку множества независимых виртуальных каналов в одном звене, но не имеет средств коррекции и восстановления кадров при возникновении ошибок. Вместо средств управления потоком в протоколе FR реализованы функции извещения о перегрузках в сети. Могут использоваться также более длинные кадры, чем в протоколе X.25/2.

FR позволяет эффективно передавать крайне неравномерно распределенный во времени трафик. Отличается малым временем задержки, скоростями до 2 Мбит/с, эффективным использованием пропускной способности каналов передачи. В отличие от сетей X.25 позволяет обеспечивать интерактивный обмен оцифрованными речевыми сообщениями. Недостаток – требует каналы высокого качества (с вероятностью ошибки 10–7 и лучше).

63.Сервисы сети Интернет. Протокол HTTP.

Сервесы:

- электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;
- телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями;
- сервис FTP – система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;
- сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме;
- World Wide Web (WWW, W3) – гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;
- сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;

Протокол HTTP (Hyper Text Transfer Protocol) обеспечивает передачу с удаленных серверов на локальный компьютер документов, содержащих код разметки гипертекста, написанный на языке HTML или XML, то есть веб-страниц. Данный прикладной протокол ориентирован прежде всего на предоставление информации программам просмотра веб-страниц, веб-браузерам, наиболее известными из которых являются такие приложения, как Microsoft Internet Explorer. Именно с использованием протокола HTTP организуется отправка запросов удаленным http-серверам сети Интернет и обработка их откликов; помимо этого HTTP позволяет использовать для вызова ресурсов Всемирной сети адреса стандарта доменной системы имен (DNS, Domain Name System), то есть обозначения, называемые URL (Uniform Resource Locator) вида http://www.domain.zone/page.

Основные понятия протокола HTTP

• **Сообщение**– основная единица обмена данными между клиентом и сервером. Сообщения обычно посылаются как часть процесса TCP-соединения. В качестве стандартного порта используется 80 порт.
• **Ресурс**– объект или служба, доступные на веб- сервере. Обычно html или xml-страница.
• **Запрос –**сообщение от клиента к серверу, которое запрашивает ресурс. В большинстве случает сообщение представляет GET-запрос.
• **Ответ –**сообщение от сервера к клиенту, которое возвращает информацию, указанную в сообщении запроса.

Основные понятия протокола HTTP

• **Метод – действие, которое следует выполнять на запрашиваемом ресурсе.**
• **Клиент**– любая программа, устанавливающее соединение с http-сервером для выдачи запроса.
• **Сервер**– процесс, принимающий http-запросы по соединениям от клиентских программ и предоставляющий ответные данные.
• **Кэш –**хранилище ответных сообщений прокси-клиента или сервера, используемые для сохранения кэшируемых ресурсов.

Основные понятия протокола HTTP

• **Туннель**– посредник транспортного уровня между программами клиента и сервера, который не принимает участия в процессе запроса/ответа, за исключением передачи данных.
• **Шлюз –**http-сервер, получающий запросы от имени другого сервера, часто отображается клиенту в виде запрашиваемого сервера.
• **Прокси**– программа, которая действует как клиент, и как сервер по http-соединению, получая сообщения от программы клиента, переоформляя запросы, как если бы прокси был клиентом, и возвращая ответы исходному заказчику.
• **URL –**унифицированный локатор ресурсов – стандартный способ обозначения ресурсов в интернет. *Протокол/имя_хоста:порт/имя_файла.*
• **Диапазон –**http-сообщения предоставляются в виде байтовых последовательностей (диапазонов). Если клиент запрашивает ресурс у http-сервера, ему необходимо знать общее число байт, поскольку объем ресурса может быть слишком велик для передачи за одну транзакцию.

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

В сетевой операционной системе отдельной машины можно выделить несколько частей
1.Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами в мультипроцессорных машинах, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.
2.Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.
3.Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.
4.Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т.п., то есть является средством транспортировки сообщений.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.
Сетевые операционные системы имеют разные свойства в зависимости от того, предназначены они для сетей масштаба рабочей группы (отдела), для сетей масштаба кампуса или для сетей масштаба предприятия.
Сети отделов - используются небольшой группой сотрудников, решающих общие задачи. Главной целью сети отдела является разделение локальных ресурсов, таких как приложения, данные, лазерные принтеры и модемы. Сети отделов обычно не разделяются на подсети.
Сети кампусов - соединяют несколько сетей отделов внутри отдельного здания или внутри одной территории предприятия. Эти сети являются все еще локальными сетями, хотя и могут покрывать территорию в несколько квадратных километров. Сервисы такой сети включают взаимодействие между сетями отделов, доступ к базам данных предприятия, доступ к факс-серверам, высокоскоростным модемам и высокоскоростным принтерам.
Сети предприятия (корпоративные сети) -объединяют все компьютеры всех территорий отдельного предприятия. Они могут покрывать город, регион или даже континент. В таких сетях пользователям предоставляется доступ к информации и приложениям, находящимся в других рабочих группах, других отделах, подразделениях и штаб-квартирах корпорации.

65.Команды ОС Windows конфигурирования и тестирования сетевых интерфейсов

Arp

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица. Запущенная без параметров, команда **arp** выводит справку.

Ipconfig

Служит для отображения всех текущих параметров сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды **ipconfig** без параметров выводится только IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Nbtstat

Служит для отображения статистики протокола NetBIOS over TCP/IP (NetBT), таблиц имен NetBIOS для локального и удаленного компьютеров, а также кэша имен NetBIOS. Команда **Nbtstat** позволяет обновить кэш имен NetBIOS и имена, зарегистрированные в службе имен Интернета Windows (WINS). Запущенная без параметров, команда **nbtstat** выводит справку.

Netstat

Отображение активных подключений 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). Запущенная без параметров, команда **nbtstat** отображает подключения TCP.

Nslookup

Предоставляет сведения, предназначенные для диагностики инфраструктуры DNS. Для использования этого средства необходимо быть знакомым с принципами работы системы DNS. Средство командной строки Nslookup доступно, только если установлен протокол TCP/IP.

Ping

С помощью отправки сообщений с эхо-запросом по протоколу ICMP проверяет соединение на уровне протокола IP с другим компьютером, поддерживающим TCP/IP. После каждой передачи выводится соответствующее сообщение с эхо-ответом. Ping - это основная TCP/IP-команда, используемая для устранения неполадки в соединении, проверки возможности доступа и разрешения имен. Команда **ping**, запущенная без параметров, выводит справку.

Route

Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации. Запущенная без параметров, команда **route** выводит справку.

Tracert

Определяет путь до точки назначения с помощью посылки в точку назначения эхосообщений протокола Control Message Protocol (ICMP) с постоянным увеличением значений срока жизни (Time to Live, TTL). Выведенный путь — это список ближайших интерфейсов маршрутизаторов, находящихся на пути между узлом источника и точкой назначения. Ближний интерфейс представляют собой интерфейс маршрутизатора, который является ближайшим к узлу отправителя на пути. Запущенная без параметров, команда **tracert** выводит справку.

Net session

Служит для управления подключениями к серверу. Команда **net session** без параметров выводит сведения обо всех сеансах локального компьютера.

Net share

Управление общими ресурсами. При вызове команды **net share** без параметров выводятся сведения обо всех общих ресурсах локального компьютера.

Net use

Подключение к общим сетевым ресурсам или вывод информации о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Вызванная без параметров, команда **net use** извлекает список сетевых подключений.

Net view

Выводит список доменов, компьютеров или общих ресурсов на данном компьютере. Вызванная без параметров, команда **net view** выводит список компьютеров в текущем домене.

66.Команды ОС Unix конфигурирования и тестирования сетевых интерфейсов

ifconfig

Команда используется для настройки сетевых интерфейсов

arp

Команда **arp** отображает ARP-таблицу данного хоста. С помощью параметра `-i` можно специфицировать сетевой интерфейс, информация о котором интересует.

route

Эта команда используется для просмотра и изменения таблицы маршрутизации хоста. Для этой команды также работает параметр `-n`, при использовании которого IP-адреса не будут заменяться символьными именами хостов.

traceroute

Команда **traceroute** служит для отладки сетевых соединений посредством построения маршрута следования пакетов к хосту назначения. Для этой команды также работает параметр `-n`, при использовании которого IP-адреса не будут заменяться символьными именами хостов.

host

Команда **host** служит для получения доменной информации о хосте: IP-адрес, MXзаписи и другой информации, связанной с данным символьным именем. Имя хоста указывается в качестве аргумента команды.

67.Сетевое управление в IP-сетях. Средства операционных систем для работы с компьютерными сетями

Одной из первых систем сетевого управления, получившей широкое распространение, был программный продукт SunNet Manager.

Система SunNet Manager была ориентирована на управление коммуникационным оборудованием и контроль трафика сети. Именно эти функции имеют чаще всего в виду, когда говорят о системе управления сетью (Network Management System, NMS).

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

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

Средства сетевых операционных систем

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

В сетевой операционной системе отдельной машины можно выделить несколько частей

- Средства управления локальными ресурсами компьютера: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами в мультипроцессорных машинах, управления периферийными устройствами и другие функции управления ресурсами локальных ОС.
- Средства предоставления собственных ресурсов и услуг в общее пользование - серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам.
- Средства запроса доступа к удаленным ресурсам и услугам и их использования - клиентская часть ОС (редиректор). Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.
- Коммуникационные средства ОС, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и т.п., то есть является средством транспортировки сообщений.

В зависимости от функций, возлагаемых на конкретный компьютер, в его операционной системе может отсутствовать либо клиентская, либо серверная части.

68.Электронная почта. Протоколы электронной почты, почтовые клиенты,безопасность.

Электронная почта - средство обмена информацией, подготовленной в электронном виде, между людьми, имеющими доступ к компьютерной сети.

Основными областями применения электронной почты являются ведение личной переписки и работа с некоторыми информационными ресурсами Интернета, такими как списки рассылки, off-line группы новостей и системы пересылки файлов по электронной почте.

Почтовый клиент (мейлер) - программа, помогающая составлять и посылать электронные сообщения, получать и отображать письма на компьютере пользователя.

Почтовая программа (почтовый клиент, клиент электронной почты, мейлер, мейл-клиент) – это ПО, которое инсталлируется на компьютер пользователя и предназначено для написания, получения, хранения, отправки электронной почты одного или нескольких пользователей (например, когда имеется несколько учетных записей на компьютере), или нескольких учетных записей пользователя.

Большие почтовые клиенты, например The Bat!, Mozilla Thunderbird, Microsoft Outlook, комбинируют в себе работу MRA, MSA и MDA. Более простые клиенты, например такие как Mutt, также являются почтовым ПО.

Почтовый клиент, в отличие от почтового сервера, обычно отправляет сообщение не прямо на сервер получателя, а на один и то же почтовый сервер, выступающий как релей. Часто это почтовый сервер провайдера, либо компании. Чаще всего отправка сообщений осуществляется с помощью протокола SMTP.

Почтовая программа принимает почту с одного или нескольких почтовых серверов. Зачастую это тот же сервер, который служит для отправки сообщений. Прием обычно осуществляется по протоколам IMAP или POP.

В функции клиента может входить хранение писем, их сортировка, поиск по архиву, фильтрация входящих сообщений по заданным критериям, ведение адресной книги, шифрование, конверсия форматов, организация интерфейсов с офисным ПО и т .д.

Самые популярные почтовые клиенты:

- Microsoft Outlook
- Mozilla Thunderbird
- Windows Mail
- The Bat!
- Opera Mail
- Lotus Notes

Работа с почтой может проводиться в режиме off-line. Это означает, что для получения и отправки почты в назначенный час вы устанавливаете соединение с провайдером. Затем вы

даете команду вашему почтовому клиенту, по которой он подключается к вашему почтовому серверу, отсылает подготовленные письма и забирает на локальный компьютер сообщения, пришедшие за истекший период на ваш почтовый ящик. Писать письма и читать полученные с сервера сообщения вы можете в автономном режиме, то есть, без подключения к Интернету.
SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты) - почтовый протокол, служащий для отправки сообщений с компьютера-клиента на почтовый сервер, а также для пересылки почты между серверами.
Для того чтобы получить доступ к вашему почтовому ящику на сервере и забрать свою почту, нужен другой протокол. В настоящее время самым используемым протоколом для передачи сообщения от сервера к клиенту является протокол POP3 (Post Ofice Protocol, протокол почтового офиса версия 3).
POP3 (Post Office Protocol, протокол почтового офиса версия 3) - почтовый протокол для получения доступа к почтовому ящику на сервере и пересылки сообщений на компьютер-клиент.
Этот протокол делает следующее:
Передает имя пользователя и пароль для доступа к почтовому ящику на почтовый сервер.
Определяет, есть ли очередная почта в этом почтовом ящике.
Загружает эту почту на ваш компьютер.
Уничтожает переданную почту на сервере.
Альтернативным протоколом для доставки почты на локальный компьютер является протокол IMAP (Internet Message Access Protocol, протокол доступа к сообщениям Интернета). Это более интеллектуальный протокол, позволяющий пользователю:

Создавать, стирать и переименовывать почтовые ящики
Производить проверку на наличие новых сообщений
Разыскивать и удалять сообщения на сервере
Выполнять выборочную доставку почты с сервера на локальный компьютер.
IMAP (Internet Message Access Protocol, протокол доступа к сообщениям Интернета) - протокол для доступа к почтовому ящику на сервере, позволяющий управлять корреспонденцией на сервере.

Безопасность:
С точки зрения безопасности, при работе с электронной почтой выделяют следующие угрозы и уязвимости:
• утечка конфиденциальной информации;
• отказ в обслуживании;
• заражение компьютерным вирусом;
• проникновение на компьютер активного содержимого.

Во избежание утечки конфиденциальной информации в почтовом обмене используют методы симметричной и несимметричной криптографии. При симметричной криптографии обе стороны используют одинаковое шифрующее и дешифрующее программное обеспечение. Зашифровав сообщение с помощью избранного ключа (пароля), отправитель сообщает этот ключ адресату, используя альтернативные средства связи, например телефон. При несимметричном шифровании отправитель шифрует сообщение с помощью сертификата (открытым ключом) получателя. Большинство современных почтовых клиентов делают эти операции автоматически, «прозрачно» (то есть незаметно) как для отправителя, так и для адресата.