1. Основные понятия и определения компьютерных систем.

**Компьютерная сеть** - это совокупность компьютеров и телекоммуникационного оборудования, обеспечивающая обмен данными между компьютерами. **Основное их назначение** - обеспечение совместного доступа к информационным и аппаратным ресурсам. **Узел сети** - устройство, соединенное с другими устройствами, как часть компьютерной сети, имеющее уникальный сетевой адрес. **Коммутация** - это технология организации передачи данных по сети. Скорость передачи данных измеряется количеством единиц информации, передаваемых за секунду.

Объем информации, передаваемой через сеть за определенный период времени, называют **сетевым трафиком**. Может изменяться в количестве пакетов или битами, байтами и т.д.

**Трафик классифицируется:**

1. Входящий

2. Исходящий

3. Внутренний

4. Внешний

**Канал связи** - система технических средств и среда распространения сигналов для передачи данных от источника к приемнику. **Сетевой коммутатор** - устройства для соединения нескольких узлов компьютерной сети в пределах одного или нескольких ее сегментов. **Маршрутизатор** - специализированное устройство для соединения различных сегментов сети или разнородных сетей на основе сетевого уровня. **Сетевой концентратор** - устройство для объединения компьютеров с применением кабельной инфраструктуры. **Сервер** - это компьютер, который предоставляет другим узлам сети доступ к своим ресурсам и услуги по из использования. **Клиент** - компьютер, обращающийся к серверу за ресурсами или услугами.

2. Классификация компьютерных систем.

**По технологии передачи данных сети можно разделить на 2 типа:**

1. Один ко многим или широковещательная.

2. Соединение "точка-точка".

**По принципу организации обмена данными различают сети, основные на коммутации каналов, коммутации сообщений и коммутации пакетов.**

**Сеть с коммутацией каналов** - каждой паре абонентов на весь сеанс связи предоставляется физическое соединение недоступное на это время другим абонентам.

**В сети с коммутацией сообщений** осуществляется физическое соединение только на время передачи одного логически завершенного сообщения.

**При коммутации пакетов** данные разбиваются на отдельные блоки небольших размеров. Эти блоки могут пересылаться между узлами сети последовательно по различным маршрутам с промежуточным их хранением в узлах коммутации.

**По территориальному признаку различают локальные, промежуточные и глобальные.**

**Локальные** связывают сетевые узлы на небольшой географической площади, чаще всего в одной организации. Чаще всего при их монтаже используются специально положение линии связи.

**Промежуточные** объединяют узлы на территории района, города или большой корпорации. При построении могут использовать как специальные, так и уже имеющиеся линии связи.

**Глобальные** объединяют узлы без привязки к географии. Используют любые доступные линии связи.

**По принципу организации взаимозависимости узлов компьютерные сети разделяют на 2 класса:**

**1. Одноранговые (одноуровневые).** Состоит из равноправных узлов, каждый из которых имеет уникальное имя и пароль для входа. Роль сервера в такой сети определяется каждой конкретной задачей.

**2. Иерархические (многоуровневые).** Содержит один или несколько разноуровневых серверов. Узлы, не являющиеся серверами, называются рабочими станциями или клиентами.

**Различают 2 архитектуры использования серверов:**

**1. Файл-сервер.** Данные и программы хранятся на сервере, а обработка данных и выполнение программ происходит на клиентах.

**2. Клиент-сервер.** На сервере помимо хранения данных и программ выполняется работа серверного ПО, выполняются прикладные программы, обрабатываются данные и т.д.

**По типу среды передачи данных компьютерные сети разделяются на проводные и беспроводные.**

3. Топология компьютерных систем.

Под **топологией сети** понимается конфигурация физических связей между компонентами сети. От выбора топологии зависят большинство характеристик сети: возможность балансировать загрузку каналов, расширяемость, минимизация затрат…

**Принято выделять 3 базовых топологии:**

**1. Общая шина.** Все узлы подключаются к одной линии связи (чаще всего коаксиальный кабель). Для подключения каждой станции используется «Т»- коннектор. Свободные концы кабеля закрываются терминаторами, один из которых заземляется. Сигнал проходит по сети через все компьютеры и отражается от терминаторов.

**2. Кольцо.** Компьютеры подключаются поочередно друг к другу, образуя замкнутое кольцо. При этом, данные передаются последовательно от одного компьютера к другому пока не достигнут адреса назначения.

**3. Звезда.** Подразумевает наличие объединяющего устройства (концентратора или коммутатора), к которому отдельными линиями связи подключаются все узлы.

Реальные сети чаще всего состоят из нескольких сегментов, возможно различных топологий. Сети со структурой типа «дерево» чаще всего объединяют сегменты, начальный из которых имеет топологию «общая шина».

4. Кабельные линии связи.

Строятся на основе проводников, заключённых в несколько слоев изоляции, и характеризуются следующими параметрами:

1. Полоса пропускания.

2. Степень защищённости от помех.

3. Затухание сигнала.

В современных компьютерных сетях могут использоваться коаксиальный кабель, витая пара, оптоволоконный кабель.

**Коаксиальный кабель** – медный проводник, заключённый в слой диэлектрика, на поверхности которого находится металлическая экранирующая пленка, поверх которой ещё один слой диэлектрика. Данные передаются по центральной жиле. Экранирующая пленка защищает от внешних электромагнитных полей. Используется тонкий и толстый кабель. Тонкий кабель имеет сопротивление 50 Ом, диаметр центральной жилы 0,85 мм, внешний около 5 мм. Толстый кабель – такое же сопротивление, диаметр центральной жилы 2.17 мм внешний диаметр около 10 мм.

**Витая пара** представляет собой от 1 до 4 пар изолированных проводников, скрученных между собой и помещенных в общий изолирующий слой. Кабель может быть экранирован и тогда он называется STP или не экранирован UTP. Экранированная витая пара превосходит не экранированную по помехозащищённости, но уступает по скорости передачи данных и удобству прокладки. Существует несколько категорий витой пары различающиеся частотой полосы пропускания. По сравнению с коаксиальным кабелем витая пара имеет следующие преимущества:

1) Возможность работы в дуплексном режиме.

2) Низкая стоимость.

3) Более высокая надёжность.

4) Удобство прокладки.

5) Большая помехоустойчивость в экранированной варианте.

**Оптоволоконный кабель** по структуре похож на коаксиальный кабель, но вместо центральной жилы используется стекловолокно диаметром от 1 до 10 микрон, а вместо внутренней изоляции специальная оболочка с большим внутренним отражением. Бывают бронированные варианты, когда 1 или несколько кабелей заключаются в металлическую оболочку для защиты от внешней среды. В зависимости от характера распространения света определяют следующие виды оптоволоконных кабелей:

1) Одномодовое волокно.

2) Многомодовое волокно со ступенчатым изменением показателя преломления.

Одномодовый кабель самый дорогой но его характеристики существенно выше остальных.

В многомодовых кабелях толщина волокна в десятки раз больше чем в одномодовых, из-за этого чем длиннее кабель, тем сильнее искажается сигнал, поэтому многомодовые кабели используют на расстоянии до 2х км на скорости не более 1 гигабита в секунду.

5. Физическая передача данных.

**Среда передачи данных** – это каналы связи, через которые происходит обмен информацией. Передача осуществляется с помощью сигнала соответствующего природе канала. Поэтому перед передачей информацию необходимо преобразовать в соответствующий вид сигнала, т.е. закодировать. Использование различных методов кодирования может существенно влиять на достоверность и скорость передачи данных. Кроме того линии связи значительно отличаются от информационных шин внутри компьютера, поэтому кодировку сигналов внутри компьютера не всегда можно использовать между компьютерами. Поэтому в компьютерных сетях кроме кодирования применяют модуляцию.

Второй проблемой передачи сигнала является взаимная синхронизация передатчика и приемника.

Существует несколько характеристик, связанных с передачей трафика через физические каналы:

1. Первой такой характеристикой называется **заявленная нагрузка** – это поток данных, поступающих от пользователя на вход сети, измеряемые в битах в секунду.

2. **Скорость передачи данных** - это фактическая скорость передачи данных, прошедших через сеть. Реально она может быть меньше, чем скорость заявленной нагрузки, потому что в процессе передачи данные могут искажаться или теряться.

3. **Ёмкость канала связи (пропускная способность)** – это максимально возможная скорость передачи информации по каналу. Она зависит не только от параметра физической среды передачи, но и от выбранного способа передачи. Передача коммуникационного устройства должна работать со скоростью равной пропускной способности канала (битовая скорость передатчика).

4. Полоса пропускания используется в 2х разных значениях:

1) Это ширина пропускания частот, которую линия передает без существенных искажений.

2) Этот термин часто использует как синоним ёмкости канала связи.

В зависимости от направления различают дуплексные каналы связи (передачи в обоих направлениях одновременно), полудуплексный каналы связи (передачи в обоих направлениях по очереди) и симплексный (передача только в одном направлении).

6.Задачи сетевого взаимодействия.

В процессе передачи данные проходят несколько этапов обработки. Прежде всего, информация разбивается на сетевые пакеты, каждый из которых кодируется в соответствии с используемой средой передачи и снабжается управляющей информацией. Пакеты передаются с помощью электрических или оптических сигналов в соответствии с выбранным методом доступа. На принимающей рабочей станции пакеты проходят обратную обработку и принимают первоначальный вид. При передаче сообщений оба участника сетевого обмена должны принять множество соглашений: уровни передаваемых сигналов их форм, способ определения длины, методы контроля достоверности…

Так как в сети определяется разное оборудование, то одной из наиболее острых проблем является проблема его совместимости. Без соблюдения всеми производителями общепринятых правил разработки оборудования решить её не возможно, поэтому любая новая технология сначала проходит стандартизацию и, лишь затем, внедряется.

**Открытая система** - это некая вычислительная черта, состоящая из аппаратных и программных продуктов и технологий, которые разработаны в соответствии с общедоступными и общепринятыми международными стандартами. Основой стандартизации компьютерных сетей является многоуровневый подход разработки средств сетевого взаимодействия. На основе этого подхода была создана стандартная модель взаимодействия открытых систем. Она была создана для стандартизации всех выполняемых процедур, разделяя их на уровни и подуровни. Оба участника информационного обмена должны принять множество соглашений. Одним из видов таких соглашений являются **протоколы** – формализованные правила, определяющие порядок и формат сообщений, которыми обмениваются сетевые компоненты, представляющие один уровень, но находящиеся в разных узлах сети.

Кроме того, такие же правила для обмена сообщениями соседних уровней, находящихся на одном уровне, принято называть интерфейсом.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеклом коммуникационных протоколов. Эти протоколы могут быть реализованы как программно, так и аппаратно, кроме того, они могут реализовываться не только компьютерами, но и другими сетевыми устройствами.

7. Сетевая модель OSI.

В 1970-х годах международная организация по стандартизации ISO предложила стандарт, который является эталонной моделью обмена информации открытых систем OSI. Эта модель развивает все процессы взаимодействия и передачи данных по сети на 7 уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный, физический. Любой протокол в этой модели должен взаимодействовать либо с протоколами своего уровня на взаимодействующем процессе, либо с верхним, либо с нижним уровнем своего процесса. Взаимодействие с протоколами своего уровня называются горизонтальными или виртуальными, а с уровнями выше или ниже вертикальными. Каждому уровню условно соответствует свой элемент данных. Например, на физическом уровне - бит, на канальном - кадр, на сетевом - пакет. OSI взаимодействует только с системными соглашениями, не касаясь пользовательских соглашений. Приложения организуют свои протоколы взаимодействия.

8.Физический уровень управления OSI.

Определяет метод передачи данных от одного метода передачи данных к другому. Выбор метода зависит от вида среды передачи данных. К нему относятся такие характеристики сред передачи данных как:… . На этом же уровне определяются характеристики сигналов переносящих информацию. К функциям физического уровня относятся: передача битов по физическим каналам, формирование несущих сигналов, кодирование информации, синхронизация, модуляция. Физический уровень реализуется аппаратным. Его функции выполняются на всех устройствах подключенных к сети. На этом уровне работают концентраторы (хаб), репитеры (повторители), на компьютерах эти функции реализуют сетевые карты или последовательные порты. На нем реализуются физические, электрические и механические интерфейсы, между двумя системами.

9. Канальный уровень модели OSI.

Канальный уровень предназначен для обеспечения взаимодействия сетей по физическому уровню и контролю над ними. Одной из задач канального уровня является проверка задач среды задач. Другой задачей является поиск и исправление ошибок. Для этого передаваемые биты группируются в наборы (кадр). Канальный уровень обеспечивает корректность передачи одного кадра. В начало и конец каждого кадра помещается специальная последовательность битов. Вычисляется контрольная сумма и добавляет её сумму к каждой. Получатель кадра снова вычисляет контрольную сумму полученных данных и сравнивает их с полученным результатом. Если они совпадают, кадр принимается. Если не совпадает, то фиксируется ошибка и сообщение о ней отправляется источнику. Канальный уровень источника повторяет передачу этого кадра. Хотя функция коррекции ошибок в некоторых протоколах канального уровня отсутствует. Разделяется на 2 подуровня: логической передачи данных (LLC) и управлением доступом к среде(MAC). LLC реализует функции, интерфейсы с прилегающим к нему сетевым уровнем, а mac обеспечивает корректное совместное использование общей среды.

Функции канального уровня:

1. Управление доступом к передающей среде.

2. Выделение границ кадра.

3. Аппаратная адресации.

4. Обеспечение достоверности принимаемых данных.

5. Адресация протокола верхнего уровня.

10. Сетевой уровень модели OSI.

Предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, за определение кротчайших маршрутов, коммутации и маршрутизации, отслеживании неполадок и заторов в сети. Ещё он должен обеспечивать обработку ошибок, мультиплексирование и управление потоками данных.

Протокол канального уровня сетей, жёстко призванных конкретной типовой топологией - это жесткое ограничение, не позволяющее строить сеть с развитой структурой. Для того чтоб преодолеть это ограничение и сохранить простоту передачи данных для типовых топологий на сетевом уровне под сетью понимается совокупность компьютеров, соединённых между собой одной из типовых топологий и использующий для передачи данных один из протоколов канального уровня предназначенной для этой топологии. Таким образом, внутри сети доставку данных регулируют канальные уровни, а между сетями – сетевой уровень. Основная задача сетевого уровня - маршрутизация данных. И её решение является главной задачей сетевого ввода.

Так же сетевой уровень решает задачи согласования, разных технологий упрощение адресации в крупных сетях и создание надёжных барьеров на пути нежелательного трафика между сетями.

Сообщение сетевого уровня называют пакетами, адрес получателя состоит из номера сети и номера узла в этой сети. На сетевом уровне определяются 2 вида протоколов:

1. Сетевые протоколы, реализующие движение пакетов через сеть.

2. Протоколы обмена маршрутной информацией. С их помощью маршрутизаторы собирают информацию о топологии межсетевых соединений.

Сетевые протоколы реализуются программными средствами операционной системы, а протоколы системы аппаратным.

11. Транспортный уровень модели OSI.

Является связующим звеном между вышележащими уровнями, которые в основном зависят от приложений, и нижележащими, которые больше привязаны к аппаратуре. Он обеспечивает надежную передачу данных от отправителя к получателю. Для этого он выполняет следующие задачи:

1. Разбивка сообщений сеансового уровня на пакеты и их нумерация.

2. Буферизация принимаемых пакетов.

3 Упорядочивание прибывающих пакетов.

4. Адресация прикладных процессов.

5. Управление потоком.

Все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами сетевых ОС. Примеры транспортных протоколов: TCP, UDP, SPX. Протоколы четырех нижних уровней называют транспортной подсистемой или сетевым транспортом, т.к. они полностью решают задачу транспортировки сообщений с заданным уровнем качества.

12. Сеансовый уровень и уровень представления модели OSI.

Сеансовый уровень отвечает за поддержку сеанса связи, чем обеспечивает координацию связи между двумя рабочими станциями сети. Он организует сеанс обмена данными, управляет созданием и завершением сеанса, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений. Синхронизация передачи обеспечивается помещением в поток данных контрольных точек, чтобы можно было откатиться к ним.

Уровень представления обеспечивает то, что информация, передаваемая прикладным уровнем, будет понятна прикладному уровню на другой машине. Уровень представления выполняет преобразование форматов данных в некоторый общий формат представления, а на приеме выполняет обратное преобразование. На этом уровне могут выполняться шифрование и дешифрование данных, обеспечивая секретность сразу для всех прикладных сервисов.

13. Прикладной уровень модели OSI.

Обеспечивает взаимодействие сети и пользователя, дает приложениям доступ к сетевым службам, отвечает за передачу служебной информации, предоставляет приложениям информацию об ошибках и формирует запросы к уровню представления, с помощью которых пользователи получают доступ к разделяемым ресурсам и организуют свою совместную работу. Единица данных прикладного уровня – сообщение.

Три нижних уровня являются зависимыми от конкретной реализации сети. Три верхних уровня ориентированы на приложения и мало зависят от технических особенностей сети. На их протоколы не влияют никакие изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным. Он скрывает детали работы нижних уровней от верхних. Это позволяет разрабатывать приложения, независящие от технических средств транспортировки сообщений.

14. Общие характеристики протоколов.

**Сетевой протокол** - это набор правил и соглашений, в соответствии с которыми происходит обмен сообщениями в определённых форматах. Иерархически организованная совокупность протоколов различных уровней достаточных для организации взаимодействия узлов в КС называют стэком протокола. В отличие от сетевой модели **стек протокола** - это набор конкретных спецификаций, позволяющих реализовать сетевое взаимодействие.

От используемого стека протокола во многом зависят характеристики сети в небольших локальных сетях, обычно достаточно одного стека в больших корпоративных параллельно используются несколько стеков. В сетевом оборудование реализуются протоколы нижнего уровня, которые в большей степени стандартизованы чем протоколы верхних уровней, это позволяет совместно работать с оборудованием различных производителей. Перечень протоколов поддерживаемых конкретным сетевым устройством является одной из важнейших характеристик устройства.

Протоколы для обмена в локальных сетях делиться по функциональности на 3 вида: прикладные, транспортные и сетевые.

Прикладные протоколы выполняют 3 функции. Они обеспечивают взаимодействие приложений и обмен данными между ними

Транспортные протоколы реализуют функции транспортного и сеансового уровня OSI они инициализируют и поддерживают сеансы связи между узлами и обеспечивают требуемый уровень надёжности в передачи данных

Сетевые протоколы выполняют функции трёх нижних уровней OSI, они управляют адресацией, маршрутизацией, проверкой ошибок и повторной передачи кадров.

В 1980 г. в ИЕЕЕ был организован комитет. В результате его работы было принято ИЕЕЕ.2.x его стандарты охватывают только два нижних уровня семиуровневой модели OSI физический и кто найдет слово тот умница.

15. Стек протоколов OSI.

Это международный независимый от производителей стандарт. Эти протоколы требуют больших затрат вычислительной мощности процессорного блока, поэтому они более подходят большим ЭВМ, чем персональным компьютерам. Стек протоколов OSI содержит спецификации всех семи уровней модели OSI.

На физическом и канальных уровнях стек поддерживает протоколы Ethernet, TokenRing, FDDI, LLC, X.25, SDN. Протоколы сетевого, транспортного и сеансового уровней также имеются, но они мало распространены, причем на сетевом уровне реализованы протоколы как с установлением соединения, так и без установления. Протоколы прикладного уровня включают передачу данных, эмуляцию терминала, службу каталогов и почту. Из них наиболее перспективными являются служба каталогов x.550, электронная почта x.400, протокол виртуального терминала VT, протокол передачи доступа и управления файлами FTAM, протокол пересылки и управления работами JTM.

Разработка и внедрение стека OSI предполагали отказ от существующих протоколов и переход на новые на всех уровнях стека. Это послужило причиной для отказа от него многих компаний, сделавших значительные инвестиции в разработку других сетевых технологий.

16. Стек протоколов TCPIP.

Это набор сетевых протоколов передачи данных, используемый в сетях включая интернет. Является одним из наиболее популярных и перспективных стеков. Большой вклад в развитие стека внёс калифорнийский университет Berkly. Стек имеет четырехуровневую структуру, которая не полностью соответствует модели OSI.

Нижний уровень четвертый - уровень межсетевых интерфейсов соответствует физическому и канальному уровням OSI. Поддерживает все популярные стандарты физического и канального уровней. Третий уровень - уровень межсетевого взаимодействия занимается передачей дэйтаграмм с использованием всех доступных линий связи. Основным протоколом является IP. Он предназначен для передачи пакетов в составных сетях со сложной топологией. На этом же уровне работают протоколы, связанные с составлением и модификацией таблиц маршрутизации. Это протоколы сбора маршрутной информации RIP и OSPF, а также протокол для организации обратной связи и CMP.

Второй уровень называется основным и обеспечивает транспортировку информации по сети. Здесь функционирует протокол управления передачей TCP - обеспечивает логическое соединение между прикладными процессами и обеспечивает повторную передачу ошибочных пакетов. Ещё один протокол UDP обеспечивает передачу прикладных пакетов дэйтаграммным методом, т.е. без установления логического соединения.

К первому уровню - прикладному относятся: протокол копирования файлов FTP, протокол эмуляции терминала TelNet, почтовый протокол SMTP, гипертекстовые сервисы доступа к удаленной информации...

17. Стек протоколов IPX/SPX.

Стек протоколов IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) является разработкой и собственностью компании Novell. Он был разработан для нужд операционной системы Novell NetWare, которая еще до недавнего времени занимала одну из лидирующих позиций среди серверных операционных систем.

Протоколы IPX и SPX работают на сетевом и транспортном уровнях модели ISO/ OSI соответственно, поэтому отлично дополняют друг друга. Протокол IPX может передавать данные с помощью датаграмм, используя для этого информацию о маршрутизации в сети. Однако для того, чтобы передать данные по найденному маршруту, необходимо сначала установить соединение между отправителем и получателем. Этим и занимается протокол SPX или любой другой транспортный протокол, работающий в паре с IPX.

К сожалению, стек протоколов IPX/SPX изначально ориентирован на обслуживание сетей небольшого размера, поэтому в больших сетях его использование малоэффективно: излишнее использование широковещательного вещания на низкоскоростных линиях связи недопустимо.

Для IPX/SPX доступны следующие протоколы:

1. RIP.

2. EIGRP (разработан компанией «Cisco Systems»).

3. NLSP (Netware Link Services Protocol) — адаптированная для IPX версия сетевого протокола IS-IS.

18. Общее представление о адресации в сетях.

19. Физическая адресация.

Физический адрес - локальный адрес узла определяемый технологией построения сети. Эти адреса назначаются производителями оборудования и являются уникальными так как управляются централизованно их называют MAC-адресом (Media Access Control). Они формируют основу сетей на канальном уровне OSI. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы. В сетях IPv4 это протоколы ARP и RARP. В сетях IPv6 это протокол NDP.

MAC-адрес обычно используется аппаратурой, поэтому его делают по возможности компактным и записывают в виде двоичного или шестнадцатеричного числа. В двоичном формате он имеет длину 48 бит. В шестнадцатеричном в виде 12 цифр по 2 в группе при этом первые 6 цифр указывают на производителя, а остальные идентифицируют само устройство. На основе MAC-адреса можно управлять доступом к сетевым ресурсам. Существую специально зарезервированные мак адреса. Например, 48 двоичных единиц это широковещательный адрес.

22. Протоколы обратного разрешения адресов.

Для определения локального адреса по IP адресу используется протокол разрешения адреса ARP. Он работает различными способами в зависимости от того какой протокол на канальном уровне работает в сети. В локальных сетях ARP использует рассылку широковещательных запросов. Он формирует запрос, указывая в нем сетевой адрес, для которого нужно определить соответствующий физический адрес, инкапсулирует этот запрос в кадр протокола канального уровня и производит широковещательную рассылку этого кадра.

Каждый узел, получивший этот запрос, сравнивает указанный в нем адрес со своим адресом, если адреса совпали, то узел формирует ответ, содержащий оба своих адреса (физический и сетевой), и отправляет его отправителю ARP запроса. Если искомого IP адреса нет в этой сети и она не соединена шлюзом, то разрешить запрос не получится. Такие пакеты уничтожаются по превышению лимита времени на разрешение запроса. Пакеты, содержащие ARP запрос и ответ, имеют одинаковый формат.

Для определения IP адреса по известному физическому адресу используется протокол обратного разрешения адресов RARP. Необходимость его использования обычно объясняется использованием бездисковых рабочих станций, которые загружаются с единого сервера.

23. Система доменных имен.

Для идентификации компьютеров в сети аппаратное и программное обеспечение использует IP адреса, но для пользователей это неудобно, поэтому кроме числовых адресов применяется их символьное представление, значит в сетях TCPip должен существовать механизм для установления соответствия между символьными именами и IP адресами. При нынешнем развитии сетей наиболее эффективно использование иерархической системы адресации. В стеке TCPip применяется доменная система имен, имеющая древовидную структуру и допускающая составление имени из произвольного количества составных частей.

DNS – система позволяющая преобразовывать символьные имена доменов в IP адреса и наоборот в сетях TCPip. Домен – определенная зона в DNS интернета, выделенная какой-либо стране или организации.

Доменное имя может состоять из нескольких частей, отделенных друг от друга точками. Каждая из таких частей тоже называется доменом. В домене слева записывается имя узла, входящего в домен, имеющий самый низкий уровень в иерархии, а справа домен самого высокого уровня в иерархии.

Имена доменов первого уровня назначаются централизованно в соответствии с международным стандартом. Они могут обозначать страны или типы организации. Имя домена второго уровня, обычно это псевдоним организации, которой принадлежит соответствующая корпоративная сеть или хост компьютера. Домены остальных уровней обычно оставляют некоторые подсети или дочерний хост, которые продаются другим организациям или физическим лицам. Разделение имени на части позволяет разделить административную ответственность за назначение уникальных имён в пределах своего уровня иерархии.

24. Доменное пространство имён.

Является распределенной базой данных, имеющей структуру дерево. Она называется доменным пространством имён. Имя домена идентифицирует его в БД по отношению к родительскому домену. Корневое имя имеет нулевую метку. Каждый узел дерева - это раздел БД или домена. Каждый домен может делится на поддомены. С помощью сервиса DNS централизованно осуществляется установление соответствия доменных имён адресам. Часть пространства доменных имён контролируемых DNS сервером называется зоной. Принцип работы сервисов DNS основывается на архитектуре клиент-сервер. DNS сервер - это программное обеспечение, которое хранить информацию о пространстве доменных имён. DNS клиенты обращаются к серверам с запросами о отображении доменного имени в IP адрес. Любой узел может получить сведения об искомом IP адресе любого узла сети.

DNS является базой данных с децентрализованой схемой. Это достигается делегированием полномочий организациям, приобретающим поддомен.

Один IP адрес может иметь несколько доменных имён, что позволяет поддерживать виртуальных хостинг. Одному доменному имени может соответствовать несколько IP адресов, что позволяет создавать балансировку нагрузки. Для повышения устойчивости системы используется множество серверов, содержащих одинаковую информацию, а в протоколе есть средства позволяющие её поддерживать.

25. Основные характеристики DNS.

Их можно определить следующим образом:

1. Распределенность хранения информации - каждый узел в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности и адреса корневых DNS сервера.

2. Иерархическая структура, в которой каждый узел может или самостоятельно определять работу ниже стоящих узлов или передавать их другим узлам

3. Безопасность и резервирование - за хранение и обслуживание своих зон отвечают несколько серверов. Они разделены как физически, так и логически, это обеспечивает сохранность данных и продолжение работы в случае сбоя одного из них.

Все программные решения DNS должны быть защищены, потому что, если злоумышленник взимает DNS сервер, то пользователь этого не заметит. Это несёт следующие угрозы:

1. В результате DNS атак, пользователь рискует не попасть на нужную страницу.

2. При переходе пользователя на ложный IP адрес злоумышленник получает данные…

3. DDoS атака – приводит к не работоспособности сервера, соответственно все IP адреса этого сервера перестают быть доступными.

Регистрация домена заключается в создании записей, указывающих на администратора домена в базе данных DNS, порядок регистрации и требования зависят от доменной зоны.

26. URL универсальный идентификатор ресурсов.

URL - это стандартизованный способ записи адреса ресурса в сети Интернет. Изначально URL предназначался для обозначения мест расположения файлов во всемирной паутине. Сейчас применяется для обозначения адресов почти всех ресурсов интернета и является частью более общей системы идентификации ресурсов URL. Стандарт URL регулируется организацией IETF.

Традиционная форма записи URL имеет вид:

<схема>://<логин><пароль>&<хост><порт>/<URL-путь>?<параметры>//<якорь>

Схема - чаще всего сетевой протокол.

Логин - это имя пользователя используемое для доступа к ресурсу.

Пароль- пароль этого пользователя.

Хост – это полное имя Хоста в системе DNS или его IP адрес в формате десятичных чисел.

Порт – порт Хоста для подключения.

URL путь – это уточняющая информация о месте нахождения.

ресурса, зависит от протокола.

Параметры- это строка запроса с передаваемыми на сервер параметрами.

& - разделитель параметра.

Якорь – это идентификатор «якоря» ссылающегося на некоторую часть открываемого документа. Страница в зависимости от указанного якоря может выглядеть по-разному.

Общее принятые схемы URL включают:

Http – протокол передачи

Https – тоже что и http, но с использование шифратора

Ftp – протокол передачи файлов

Rtmp – проприетарный протокол потоковой передачи данных

Rtsp – потоковый протокол реального времени

Mailto – адрес электронной почт

News – новости eather net

Telnet – файл

В схеме http в качестве адреса машины можно использовать IP адрес.

27. Сети Token Ring.

Под технологией локальных сетей подразумевается технология доступа сетевых узлов к среде передам данных. Обычно выделяют три базовых технологий.

Token Ring предложена фирмой IBM в 80-х годах. Цель-объединение в цепь всех объединениях IBM компьютеров. Утверждено стандартом ИЕЕЕ802.5. Метод управления доступом к передающей среде- маркерное кольцо. Любой User подключившийся первым запускает в сеть 3 байтовый маркер, которой обходит все узлы сети. Время владения маркером двери право узлу передать информацию. Для этого узел прокалывает к маркеру свое сообщение. Если отправлять нечего, то узел просто переправляет маркер дальше. Получив маркер узел проверяет адреса прикрепленных сообщений, если находит свой адрес, то снимает сообщение с маркера. Каждая станция может иметь определенный приоритет, влияющий на частоту посещения маркером и время владения маркером. Скорость передачи данных 4 или 16 Мб/с. Основными достоинствами являются надёжность, предсказуемость, устойчивость. Основных недостатков 2: высокая цена оборудования и ограниченная скорость передачи.

Технология ArcNet очень похожа на Token Ring с той лишь разницей, что в ней нет возможности присваивать сетевым углам приоритет. Эти две технологии являются без конфликтными.

28. Оптоволоконный интерфейс FDDI.

Технология fiber distribute data interface была разработана в 1980г. комитетом ANSI. Была первой технологией локальных сетей, использовавшей в качестве среды оптоволоконный кабель. Причинами, вызвавшими его разработку, были возрастающие требования к пропускной способности и надёжности сетей. Это стандарт передачи данных в локальной сети, протянутой на большее расстояния (до 200км), основных на протоколе Token Ring, кроме того, сеть FDDI способна поддерживать несколько тысяч пользователей.

В качестве среды передачи данных в FDDI чаще используется волоконно-оптический кабель, однако можно использовать и медный.

За основу стандарта FFDI был взят метод маркерного доступа, предусмотренный международными стандартом IEEE 802.5 Token Ring. Небольшие отличия от этого стандарта определяются необходимостью обеспечить высокую скорость передачи информации на большие расстояния.

Топология сетей FDDI – это кольцо, причем применяться два разнонаправленных оптоволоконных кабеля что позволяет в принципе использовать полнодуплексную передачу информации с удвоенной эффективной скоростью 200 Мбит/с.

Применяется и звёздно-кольцевая топология с концентраторами, включенными в кольцо. Данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передается информация в обычном состоянии, второе- вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Это позволяет FDDI достичь практически полной заявленной пропускной способности. В процессе нормального функционирования первичное кольцо простаивает. Таким образом, кольца образуют основной и резервный пути передачи данных между узлами сети. Наличие двух колец это способ повысить отказоустойчивости в сети FDDI, и узлы, которые хотят воспользоваться этим повышенным потенциалом надёжности, должны быть подключены к обоим кольцам. Сеть FDDI может полностью восстанавливать свою работоспособность в случае отказов одного из её элементов. Если отказов множество, то есть распадается на несколько не связных сетей. Технология FDDI дополняет множество механизмов обнаружения отказов технологии Token Ring механизмами реконфигурации пути передачи данных в сети, основными на наличии резервных связей, обеспечиваемых вторым кольцом.

Кольца в сетях FDDI рассматриваются как общая разделяемая среда передачи данных, поэтому для нее определен специальный метод доступа. Этот метод очень близок к методу доступа сетей Token Ring и также называется методом маркерного кольца. Отличия метода доступа заключается в том, что время удержания маркера в сети FDDI не является постоянной величиной, как в сети Token Ring. Это время зависит от загрузки кольца – при небольшой загрузке оно увеличивается, а при больших перегрузках может уменьшится до нуля.

В настоящее время большинство сетевых технологий поддерживают оптоволоконные кабели в качестве одного из вариантов физического уровня, и стандарты FDDI прошлом проверку временем и устоялись, так что оборудование различных производителей показывает хорошую совместимость.

29. Технология Ethernet.

Это технология пакетной передачи данных с разрешением коллизий.

Перед началом передачи, рабочая станция опрашивает сеть на возможность передачи. Если сеть свободна, то станция начинает передачу, если сеть занята, то передача откладывается на некоторый промежуток времени.

Если две станции одновременно начали передачу данных, то возникает ситуация конфликта, то передача прерывается и откладывается у каждой станции на разные промежутки времени.

Разрабатывалась эта технология для топологии общая шина. Сейчас является универсальный и самой распространенной для локальных сетей. Оборудование для подключения:

Сетевая карта (Ethernet), обычно имеет 2 разъема (rg45, bnc) или под оптический кабель. В первой версии обеспечивала скорость в 10 Мбит/с, основным недостатком является наличие коллизий, т.к. при количестве рабочих станций от 70 и более в одном сегменте локальных сетей, скорость заметно падает. Она претерпела много изменений: 10 база 5(для толстого кабеля), 10 база 2, 100 база s (100 Мбит/с Ethernet) 1000 база x (1гбит/с), 10г база-lx (10 Гбит/с), 40г базе-sr4, 100г base-sr10.