



<p>1. Основные понятия компьютерных сетей. Цели создания компьютерных сетей. Интерфейсы. Компьютерная сеть - это совокупность: каналов связи; устройств приема и передачи данных; коммуникационного оборудования и сетевого программного обеспечения для объединения компьютеров и обеспечения передачи данных между ними.Цель объединения компьютеров в сеть - совместное использование ресурсов: *периферийных устройств; *данных,хранящихся в оперативной памяти или на внешних запоминающих устройствах; *вычислительной мощности. Цели создания КС: *создание и использование информационных систем общего пользования (веб-сайты, базы данных, информационно-коммуникационные сервисы, облачные хранилища данных, ...); *совместное использование устройств и каналов связи (принтеры, факсы, Web-камеры, различные датчики, смартфоны, Интернет, масса других беспроводных устройств,...); *передача данных между устройствами (компьютеры, серверы, телеметрические системы и др.); *организация параллельных и облачных вычислений, в т. ч. территориально распределенных. <i>Физический интерфейс</i> определяется набором электрических характеристик сигналов и технических параметров кабеля, разъемов. <i>Линия связи</i> – участок кабеля с разъемами. <i>Логический интерфейс</i> (протокол) — это набор информационных сообщений определенного формата, которыми обмениваются 2 устройства/программы, а также набор правил, определяющих логику обмена этими сообщениями. <i>Канал связи</i> - система технических средств для передачи сообщений от источника к получателю. Функции передачи данных по линиям связи выполняются сетевыми интерфейсными картами (сетевыми адаптерами) и их драйверами.</p>	<p>2. Компоненты компьютерной сети Компьютерная сеть - это совокупность * каналов связи; * устройств приема и передачи данных; * коммуникационного оборудования и сетевого программного обеспечения для объединения компьютеров и обеспечения передачи данных между ними. <i>Основные компоненты сети(по группам):</i> 1. конечные устройства (сервера, компьютеры, телефоны, веб-камеры); 2. промежуточные устройства (маршрутизаторы, коммутаторы, беспроводные точки доступа,некоторые модемы). В современном исполнении это специализированные компьютеры. Сетевой коммутатор (switch) - устройство для соединения нескольких входных каналов связи к одному выходному без изменения скорости передач. Сетевой концентратор (hub) - сетевое устройство для переключения потока данных из канала на другой. Основные характеристики: количество портов, скорость передачи данных, типа сетевого носителя. Маршрутизатор - сетевое устройство на основании информации о топологии сети и определённых правил, принимающее решения о пересылке пакетов сетевого уровня между различными сегментами сети. Мост - сетевое оборудование для объединения сегментов локальной сети. Шлюз - сетевое устройство или программное средства для сопряжения разнородных сетей. 3. среды передачи данных (металл, стекло, пластик, радиоволны и излучения). Физические среды связи: -эфир(электромагнитные волны, ультракоротковолновый канал, спутниковая система связи, ИК-излучение); -витая пара; -волоконно-оптические линии связи; -коаксиальный кабель; -разновидности плоских кабелей; -волны оптического диапазона (распространение в атмосфере излучения спец.лазеров, передача информации осуществляется в пределах прямой видимости; распространение в световоде); программные средства. 4.Сервисы (веб-сервер, mail-сервер, telnet) сервер-компьютер или программа, предоставляющая некоторые услуги; клиент-компьютер или программа, запрашивающая услуги. 5.Процессы специальные служебные сетевые процессы, работающие на сетевом оборудовании. Не только ПК, но и например, на маршрутизаторах.</p>	<p>3. Сетевые интерфейсы. Физический интерфейс. Логический интерфейс. В КС разделяют физический и логический интерфейсы. <i>Физический интерфейс</i> (аппаратный порт) определяется набором электрических связей и характеристиками сигналов. Обычно он представляет собой разъем с набором контактов. пара разъемов соединяется кабелем, состоящим из набора проводов, каждый из которых соединяет соответствующие контакты. Так создается линия связи между двумя устройствами. <i>Логический интерфейс</i> - это: *это набор информационных сообщений определенного формата, которыми обмениваются два устройства или две программы, * а также набор правил, процедур определяющих логику обмена этими сообщениями. <i>Канал связи</i> - это система технических средств для передачи сообщений от источника к получателю (от сетевого интерфейса отправителя до сетевого интерфейса получателя). У компьютеров функции передачи данных по линиям связи выполняются сетевыми интерфейсными картами, называемыми также сетевыми адаптерами и их драйверами. Чтобы приложения могли "понимать" получаемую друг от друга информацию необходимо определить протокол взаимодействия приложений. Сетевой протокол -это совокупность правил, методов, стандартов, алгоритмов, процедур и реализующих их аппаратных и программных средств, совместно обеспечивающих взаимодействие компьютеров в КС. *Упомянутая совокупность включает чрезвычайно широкий спектр правил, стандартов и пр. и не может быть реализована в аппаратуре и программном обеспечении без специальной структуризации этой совокупности. *Естественным способом структуризации сетевых протоколов является их уроневая организация при котором все множество сетевых протоколов разбивается на совокупность иерархически упорядоченных уровней, каждый из которых минимально зависит от других уровней и может развиваться практически независимо от других.</p>	<p>4.Основные проблемы связи нескольких компьютеров. Топология. Структурированная кабельная система. Адресация. Коммутация. Основные проблемы,возникающие при объединении компьютеров в сеть 1.Выбор топологии сети Топология сети описывает расположение или взаимосвязь сетевых устройств,а также соединения между ними.Объединяя в сеть несколько компьютеров нужно выбрать конфигурацию физических связей или топологию.Физическая топология-это физическая компоновка компонентов сети.Следует различать физическую и логическую топологии сети: -<i>физическая топология</i> представляет собой наиболее общую структуру сети и отображает схему соединения сетевых элементов линиями связи,термин относится к физическим соединениям и определяет,каким образом соединяются друг с другом оконечные устройства и устройства сетевой инфраструктуры (промежуточные устройства), такие как маршрутизаторы, коммутаторы и беспроводные точки доступа и другие сетевые устройства. («Точка-точка», Полносвязная топология; «Звезда»; «Кольцо»; «Общая шина»; «Дерево»; Сети со смешанной топологией. -<i>логическая топология</i> показывает как по сети передаются определенные единицы информации(потоки данных)(термин,используемый для описания путей передачи кадров между узлами,структура логической топологии состоит из виртуальных соединений между узлами сети) (точка-точка, множественного доступа, широковетвистая, маркерная) 2.Организация совместного использования линий связи структурированная кабельная система(ОКС) представляет собой набор коммуникационных элементов-кабелей, разъемов, коннекторов, кроссовых панелей и шкафов,которые удовлетворяют стандартам и позволяют создавать регулярные,легко расширяемые структуры связей. Кабельные системы первых сетей существенно различались как по типу кабеля,так и по топологии. типичная иерархическая структура СКС включает: 1.горизонтальные подсистемы, соответствующие этажам здания, 2. вертикальные подсистемы, соединяющие кроссовые шкафы каждого этажа с центральной аппаратной здания. 3. подсистема кампуса, объединяющая несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы обычно называют магистралью.</p> 	<p>5. Проблемы связи нескольких компьютеров. Коммутация. Основные задачи коммутации. (Определение потоков, определение маршрутов, коммутация в транзитном узле, мультиплексирование и демультиплексирование). <i>Коммутация</i> - это соединение отправителя и получателя через сеть транзитных узлов. Последовательность узлов, лежащих на пути от отправителя к получателю, образует <i>маршрут</i>. Для выполнения коммутации должны быть решены следующие основные задачи: 1. определение потоков данных; 2. определение маршрутов; 3. продвижение данных в каждом транзитном узле; 4. мультиплексирование и демультиплексирование потоков. Определение потоков данных. Информационным потоком называют непрерывную последовательность данных, объединенных набором общих признаков, который выделяет эти данные из общего сетевого трафика. Очевидно, что при коммутации в качестве обязательного признака выступает адрес назначения данных. На основании этого признака вес поток входящих в транзитный узел данных разделяется на подпотоки, каждый из которых передается на интерфейс, соответствующий маршруту продвижения данных. Данные, образующие поток, могут быть представлены в виде различных информационных единиц: данных - сегментов, пакетов, кадров или ячеек. Определение маршрутов. <i>Определить маршрут</i> - это значит выбрать посл-сть транзитных узлов (коммутаторов) и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату. При выборе маршрута надо учитывать: *номинальная пропускная способность; *загруженность каналов связи; *задержки, вносимые каналами; *кол-во промежуточных транзитных узлов; *надежность каналов и транзитных узлов; *и др. (цена, политика, ...). Продвижение данных в каждом транзитном узле. Транзитные узлы должны соответствующим образом в зависимости от выбранного маршрута выполнить переключение потока данных с одного своего интерфейса на другой, т е выполнить коммутацию интерфейсов. <i>Продвижение данных</i> - это распознавание потоков и локальная коммутация на каждом транзитном узле. Транзитные узлы, предназначенные только для коммутации образуют коммутационную сеть. Мультиплексирование и демультиплексирование потоков. Задача мультиплексирования - образование из нескольких отдельных потоков общего агрегированного потока, который можно передавать по одному физическому каналу связи. Задача демультиплексирования - разделение суммарного агрегированного потока, поступающего на один интерфейс, а несколько составляющих потоков. Частный случай коммутатора, у которого все входящие информационные потоки коммутируются на один выходной интерфейс - мультиплексор. Коммутатор, который имеет один входной интерфейс и несколько выходных - демультиплексор. Основные типы мультиплексирования: *частотное - FDM; *волновое - WDM; *временное - TDM.</p>
--	---	---	--	--


<p>6. Классификация компьютерных сетей. Признаки классификации:1. Территориальный; 2. тип среды передачи; 3. функциональное взаимодействие; 4. сетевая топология; 5. масштаб производственного разделения; 6. сетевые ОСи; 7. режим доступа пользователей. Территориальный. локальная — группа взаимосвязанных сетей под одним административным управлением. Пример: персональная сеть, сеть кампуса. используют один вид протоколов. глобальная — сети географически расположенные в разных местах без общего управления. Пример: интернет. используются разные протоколы. городская — сочетает признаки локальной и глобальной. пример: сеть кабельного тв. По типу среды передачи: проводные сети для передачи данных используют электрические кабели (коаксиальные, витая пара) или волоконно-оптические кабели, беспроводные, в которых передача данных осуществляется с использованием электромагнитных волн в определенном частотном диапазоне. Отдельно: сенсорные (применение сенсорных — удаленные датчики,обнаружение аварий, телемедицина, мониторинг местности). По масштабу -сети отделов — используются группами сотрудников до 100-150 человек. -сети кампусов — студгородки и подобное. -корпоративные — объединяют большое число кмпов на всех территориях одного предприятия. Свойства: масштабность, повышенный уровень гетерогенности, использование глобальных связей. По типу взаимодействия Одноранговые — все компьютеры равноправны. Достоинства: *простота настройки; *низкая стоимость развертывания и поддержки; *независимость компьютеров и их ресурсов друг от друга; *отсутствие необходимости в дополнительном программном обеспечении; *отсутствии необходимости в постоянном присутствии системного администратора. Недостатки: *отсутствие возможности централизованного управления сетью; *может отсутствовать централизованное хранилище данных. Необходимо постоянно выполнять отдельное резервное копирование данных. Эта ответственность ложится на плечи отдельных пользователей. Клиент-серверные: выделяется один или несколько компьютеров, называемых серверами, задача которых состоит в быстрой и эффективной обработке большого числа запросов других компьютеров - клиентов. Достоинства: *высокая масштабируемость; *высокая производительность; *возможность централизованного управления сетью. Недостатки: *высокая стоимость сопровождения; *сложность в развертывании и поддержке; *наличие единой точки отказа. По режиму доступа Открытые (public) — подключиться может любой (например, интернет)Частные (private) — только те, у кого есть доступ (домашняя сеть, корпоративная и т.п) По способу коммутации: пакетов и каналов.</p>	<p>7. Классификация провайдеров Интернета по видам оказываемых услуг. Провайдер, или поставщик услуг, Интернета обычно относят к компаниям, которые выполняют для конечных пользователей лишь транспортную функцию - обеспечивают передачу их трафика в сети других поставщиков. Поставщиком интернет-контента называют такого провайдера, который имеет собственные информационно-справочные ресурсы, предоставляя их содержание - контент - в виде веб-сайтов. Многие поставщики услуг Интернета являюся одновременно поставщиками интернет-контента. Поставщики услуг хостинга - это компания, которая предоставляет свое помещение, свои каналы связи и серверы для размещения контента, созданного другими предприятиями. Поставщики услуг по доставке контента - это предприятия, которые не создают информационного наполнения, а занимаются доставкой контента в многочисленные точки доступа, максимально приближенные к пользователям, что позволяет повысить скорость доступа. Поставщики услуг по поддержке приложений предоставляют клиентам доступ к крупным универсальным программным продуктам, которые самим пользователям сложно поддерживать. Поставщики биллинговых услуг обеспечивают оплату счетов по Интернету.</p>	<p>8.Коммутация. Основные задачи коммутации. Соединение отправителя и получателя через сеть транзитных узлов называют коммутацией. Для выполнения коммутации должны быть решены следующие основные задачи:1) определение потоков данных (информационным потоком называют непрерывную последовательность данных, объединенных набором общих признаков, который выделяет эти данные из общего сетевого трафика, при коммутации в качестве обязательного признака выступает адрес назначения данных. На основании этого признака весь поток входящих данных разделяется на подпотоки, каждый из которых передается интерфейсу, соответствующий маршруту продвижения данных. Данные, образующие поток, могут быть представлены в виде различных информационных единиц данных-сегментов, пакетов, кадров или ячеек 2) определение маршрутов (значит выбрать последовательность транзитных узлов(коммутаторов) и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату. 3) продвижение данных в каждом транзитном узле 4) мультитиплексирование и демультитиплексирование потоков</p>	<p>9. Коммутация пакетов и каналов. В жизни используются два способа коммутации: *коммутация каналов;*коммутация пакетов. При коммутации пакетов учитываются особенности компьютерного трафика, поэтому данных способ коммутации является более эффективным для КС по сравнению с традиционным методом коммутации каналов. применяющимся в телефонных сетях. Коммутация каналов - образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Каналы соединяются между собой - коммутаторами. Глобальным признаком потока является пара адресов абонентов. связывающихся между собой. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал (создается временно на период сеанса). И только после этого можно начинать передавать данные. Достоинства коммутации каналов: *постоянная и известная скорость передачи данных по установленному между конечными узлами каналу. *низкий и постоянных уровень задержки передачи данных через сеть. Недостатки коммутации каналов: *отказ сети в обслуживании запроса на установление соединения. *нерациональное использование пропускной способности физических каналов. *обязательная задержка перед передачей данных из-за фазы установления соединения. Коммутация пакетов - это способ коммутации абонентов для передачи компьютерного трафика, при котором происходит: *разбиение сообщения пользователя на пакеты; *включение в пакет заголовка, содержащего адрес узла назначения и доп. информацию: нумерация пакета, длина поля данных, концевик с контрольной суммой и т. д. *передача пакетов по сети как независимых информационных единиц (блоков передачи); *формирование очередей пакетов на коммутаторах пакетной сети для сглаживания пульсации трафика на каналах связи. Сети с коммутацией пакетов состоят из коммутаторов, связанных физическими линиями связи. Главное отличие пакетных коммутаторов - наличие внутренней буферной памяти для временного хранения пакетов. Сеть с коммутацией пакетов не создает заранее для своих абонентов отдельных, выделенных исключительно для них каналов связи. Данные могут задерживаться и даже теряться по пути следования. Разделение данных на пакеты позволяет передавать неравномерный компьютерный трафик более эффективно, чем в сетях с коммутацией каналов. Достоинства коммутации пакетов: *Высокая общая пропускная способность сети при передаче пульсирующего трафика. *Динамическое перераспределение пропускной способности физических каналов связи. Недостатки коммутации пакетов: *Неопределенная скорость передачи данных между абонентами сети. *Переменная величина задержки пакетов данных. *Возможные потери данных из-за переполнения буферов.</p>	<p>10.Коммутация пакетов, основные методы продвижения пакетов. Сети с коммутацией пакетов, так же как и сети с коммутацией каналов, состоят из коммутаторов, связанных физическими линиями связи. Важнейшим принципом функционирования сетей с коммутацией пакетов является представление информации передаваемой по сети, в виде структурно отделенных друг от друга порций данных,называемых пакетами. Коммутация пакетов - это способ коммутации абонентов для передачи компьютерного трафика, при котором происходит: -разбиение сообщения пользователя на пакеты, -включение в пакет заголовка, содержащего адрес узла назначения и доп информации (нумерацию пакета, длина поля данных, концевик с контрольной суммой), -передача пакетов по сети как независимых информационных единиц (блоков передачи), -формирование очередей пакетов на коммутаторах пакетной сети для сглаживания пульсации трафика на каналах связи. Главное отличие пакетных коммутаторов - наличие внутренней буферной памяти для временного хранения пакетов. Три метода продвижения пакетов на пакетном коммутаторе: -дейтаграммная передача(основан на том, что все пакеты продвигаются, то есть передаются от одного узла сети другому) независимо друг от друга на основании одних и тех же правил, никакая информация об уже переданных пакетах сетью не хранится и в ходе обработки очередного пакета во внимание не принимается, то есть каждый отдельный пакет рассматривается сетью как совершенно независимая единица передачи - дейтаграмма, этот метод работает быстро, трудно проверить факт доставки пакета получателю, метод не гарантирует доставку пакета); -передача с установлением логического соединения (это процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами, процедура установление логического соединения состоит обычно из трех шагов 1)узел-инициатор соединения отправляет получателю первый служебный пакет с предложением установить соединение; 2)если узел-получатель согласен с этим, то он посылает в ответ другой служебный пакет, подтверждающий установление соединения и предлагающий некоторые параметры, которые будут использоваться в рамках данного логического соединения 3)узел-инициатор соединения может закончить процесс установления соединения отправкой третьего служебного пакета, в котором сообщит, что предложенные параметры ему подходят, эта передача более надежная чем дейтаграмма, однако этот способ более медленный); -передача с установлением виртуального канала (основан на частном случае логического соединения, в число параметров которого входит жестко определенный для всех пакетов маршрут, то есть все пакеты передаваемые в рамках данного соединения, должны проходить по одному и тому же закрепленному за этим соединением пути,единственный заранее проложенный фиксированный маршрут.соединяющий конечные узлы в сети с коммутацией пакетов.называют виртуальным каналом. виртуальные каналы прокладываются для устойчивых информационных потоков,с целью выделения потока данных из ощего трафика каждый пакет этого потока помечается специальным видом признака-меткой. Достоинства коммутации пакетов:1)высокая общая пропускная способность сети при передаче пульсирующего трафика 2)динамическое перераспределение пропускной способности физических каналов связи. Недостатки коммутации пакетов:1)неопределенная скорость передачи данных между абонентами сети 2)переменная величина задержки пакетов данных 3)возможные потери данных из-за переполнения буферов.</p>
<p>11. Мультитиплексирование/демультитиплексирование и коммутация в линиях связи. Коммутация - это соединение отправителя и получателя через сеть транзитных узлов. Последовательность узлов, лежащих на пути от отправителя к получателю, образует маршрут. Мультитиплексирование и демультитиплексирование потоков. Задача мультитиплексирования - образование из нескольких отдельных потоков общего агрегированного потока, который можно</p>	<p>12.Три режима передачи данных в КС. (Симплексный, полудуплексный или полнодуплексный) Симплексной, которую также называют односторонней,является одиночная,односторонняя передача.Пример:сигнал,который передается с радиостанции на ваш радиоприемник. Полудуплексная (одновременно, но только в одном направлении) называется передача, при котором данные одновременно движутся только в одном направлении. При</p>	<p>13. Дейтаграммный способ передачи пакетов. Дейтаграммный способ передачи данных основан на том, что все пакеты продвигаются (передаются от одного узла сети другому) независимо друг от друга на основании одних и тех же правил. *Никакая информация об уже переданных пакетах сетью не хранится и в ходе обработки очередного пакета во внимание не принимается. Т е каждый отдельный пакет</p>	<p>14.Передача с установлением логического соединения. -передача с установлением логического соединения(это процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами,процедура установление логического соединения состоит обычно из трех шагов 1) узел-инициатор соединения отправляет получателю первый служебный пакет с предложением установить соединение; 2) если узел-получатель согласен с этим, то он посылает в ответ другой служебный пакет ,подтверждающий</p>	<p>15. Передача с установлением виртуального канала. Данный метод основан на частном случае логического соединения, в число параметров которого входит жестко определенный для всех пакетов маршрут. Т е все пакеты, передаваемые в рамках данного соединения, должны проходить по одному и тому же закрепленному за эти соединением пути. Единственным заранее проложенный</p>

<p>передавать по одному физическому каналу связи. Задача демультиплексирования – разделение суммарного агрегированного потока, поступающего на один интерфейс, а несколько составляющих потоков. Частный случай коммутатора, у которого все входящие информационные потоки коммутируются на один выходной интерфейс – мультиплексор. Коммутатор, который имеет один входной интерфейс и несколько выходных – демультиплексор. Основные типы мультиплексирования: •частотное – FDM; •волновое – WDM; •временное – TDM. <i>Принцип временного TDM</i> состоит в выделении канала каждому соединению определенного кванта времени на использование линии связи. <i>Временное уплотнение.</i> • В любой момент времени передачу данных через сеть ведет одно устройство, занимая всю полосу частот системы. •Очень высокая скорость передачи. •Чтобы в сети могли общаться все абоненты, длительность каждой передачи ограничивается заданным интервалом времени. •К каждому блоку данных присоединяется адрес узла-адресата. Каждый узел постоянно контролирует адреса на шине и выделяет "свои" блоки. <i>Частотное уплотнение.</i> "Полоса частот системы разбита на непрерывающиеся частотные поддиапазоны и каждой паре взаимодействующих узлов выделяется один из них. •Нет необходимости ограничить длительность передачи и указывать адрес перед блоком данных. •В любой момент времени обращаться к сети может много абонентов. •Число одновременно взаимодействующих пар ограничено количеством поддиапазонов.</p>	<p>полудуплексной передаче канал связи позволяет изменять передачу в двух направлениях,но не в обоих одновременно. В основе работы приемно-передающих установок, таких как подвижные радиостанции милиции или аварийных служб, лежит принцип полудуплексной передачи Когда нажимаешь на кнопку на микрофоне для передачи,мы не сможем услышать человека на другом конце. Если люди на обоих каналах связи пытаются говорить одновременно, передача не будет осуществляться ни в одну сторону. Полнодуплексная (одновременная в обоих направлениях) называется передача, при которой данные одновременно передаются в обоих направлениях. Примером является разговор по телефону. Оба человека одновременно могут говорить и слышать. Полудуплексная сетевая технология увеличивает быстроедействие сети, потому что данные можно отправлять и передавать одновременно.</p>	<p>рассматривается сетью как совершенно независимая единица передачи - дейтаграмма. •Дейтаграммный метод работает быстро. •При этом методе трудно проверить факт доставки пакета получателю. • Метод не гарантирует доставку пакета, доставка происходит с максимальными усилиями (best effort). Пример. В технологии Ethernet используется дейтаграммная коммутация пакетов.</p>	<p>установление соединения и предлагающий некоторые параметры, которые будут использоваться в рамках данного логического соединения 3) узел-инициатор соединения может закончить процесс установления соединения отправкой третьего служебного пакета, в котором сообщит, что предложенные параметры ему подходят. Заметим, что логическое соединение может быть рассчитано на передачу данных как в одном направлении- от инициатора соединения, так и в обоих направлениях,после передачи законченного набора данных, например, определенного файла, узел-отправитель инициирует разрыв данного логического соединения, посылая соответствующий служебный кадр. В плане надежности и безопасности обмена данными такая передача более надежна, чем дейтаграммная, однако этот способ более медленный, так как он подразумевает дополнительные вычислительные затраты на установление и поддержание логического соединения.</p>	<p>фиксированный маршрут, соединяющий конечные узлы в сети с коммутацией пакетов,называют виртуальным каналом. •Виртуальные каналы прокладываются для устойчивых информационных потоков. •С целью выделения потока данных из общего трафика каждый пакет этого потока помечается специальным видом признака - меткой. •Коммутатор реализует передачу пакетов по предварительно построенному виртуальному каналу (динамическому или постоянному). Передаются отдельные пакеты, а не потоки данных с постоянной скоростью.</p>
<p>16.Сравнение сетей с коммутацией каналов и пакетов. <i>Коммутация каналов</i> 1)необходимо предварительно устанавливать соединение 2)адрес требуется только на этапе установки соединения 3)сеть может отказать абоненту в установлении соединения 4)гарантированная пропускная способность(полоса пропускания)для взаимодействующих абонентов 5)трафик реального времени передается без задержек 6)высокая надежность передачи 7)нерациональное использование пропускной способности каналов,снижающее общую эффективность сети. <i>Коммутация пакетов</i> 1)отсутствует этап установления соединения(дейтаграммный способ) 2)адрес и другая служебная информация передается с каждым пакетом 3)сеть всегда готова принять данные от абонента 4)пропускная способность сети для абонентов неизвестна,задержки передачи носят случайный характер 5)ресурсы сети используются эффективно при передаче пульсирующего трафика 6)возможные потери данных из-за переполнения буферов. 7)автоматическое динамическое распределение пропускной способности физических каналов в соответствии с фактической интенсивностью трафика абонентов. <i>По долгосрочным прогнозам многих специалистов будущее принадлежит технике коммутации пакетов,как более гибкой и универсальной.</i></p>	<p>17. Сетевые модели и протоколы. Многоуровневый подход. Протокол. Межуровневый интерфейс. Стек протоколов. Организация взаимодействия между устройствами различных технических систем явл. сложной задачей. Для решения сложных систем используется известный универсальный прием - декомпозиция, т.е разбивание одной сложной задачи на несколько более простых задач-модулей. Декомпозиция состоит: «в четком определении функций каждого модуля, «а также порядка их взаимодействия (т.е. межмодульных интерфейсов). <i>Многоуровневый подход при декомпозиции любой задачи.</i> •Декомпозиция задачи - очень эффективный способ облегчить себе жизнь и уменьшить объем работы. •Есть еще более эффективный способ разбиения больших задач на маленькие, который заключается в том, чтобы разбивать задачу не только на модули, но и на уровни. •Для этой задача сначала разбивается на модули, а затем эти модули делятся на уровни, которые образуют иерархическую модель. •Архитектура сети подразумевает представление сети в виде системы элементов, каждый из которых выполняет определенную частную функцию, при этом все элементы вместе согласованно решают общую задачу взаимодействия компьютеров. •Другими словами, архитектура сети отражает декомпозицию общей задачи взаимодействия компонентов сети на отдельные подзадачи, которые должны решаться отдельными элементами сети. •Еще более эффективной концепцией, развивающую идею декомпозиции, явл. многоуровневый подход. •После представления исходной задачи в виде множества модулей эти модули группируют и упорядочивают по уровням, образующим иерархию. •В соответствии с принципом иерархии для каждого промежуточного уровня можно указать непосредственно примыкающие соседние вышележащий и нижележащий уровни. •<i>Межуровневый интерфейс</i>, называемый также интерфейсом услуг, определяет набор функций, которые нижележащий уровень предоставляет вышележащему. •С другой стороны, результаты работы каждого из модулей, отнесенных к некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. •Чтобы такая иерархическая декомпозиция задачи работала предполагается четкое определение функций и интерфейсов не только отдельных модулей, но и каждого уровня. Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют, по меньшей мере, две стороны, т.е. в данном случае необходимо организовать согласованную работу двух иерархий аппаратных и программных средств на разных компьютерах. •Оба участника сетевого обмена должны принять множество соглашений. Например. они должны согласовать: 1. уровни и форму электрических сигналов; 2. способ определения размера сообщений; 3. договориться о методах контроля достоверности и т.п. Другими словами, соглашения должны быть приняты на всех уровнях, начиная от самого низкого - уровня передачи битов, и заканчивая самым высоким, реализующим обслуживание пользователей сети. <i>Протокол</i> - это формализованные правила, определяющие посл-сть и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.</p>	<p>18.Сетевые модели и протоколы. Модель взаимодействия открытых систем (модель OSI), ее назначение и функции каждого уровня. Модель OSI разрабатывалась в качестве своего рода универсального языка сетевых специалистов, именно поэтому называется справочной. Назначение данной модели состоит в обобщенном представлении средств сетевого взаимодействия. Модель взаимодействия открытых систем-модель OSI (под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами по стандартным правилам, определяющим формат, содержание и значение принимаемых и отправляемых сообщений). Данная модель определяет 1)уровни взаимодействия систем в сетях с коммутацией пакетов 2)стандартные названия уровней 3)функции, которые должен выполнять каждый уровень (модель OSI не содержит описаний конкретных протоколов и их реализаций. В данной модели средства взаимодействия делятся на уровни: <i>прикладной</i> (представляет набор интерфейсов, позволяющий получить доступ к сетевым службам, пользовательское управление данными, единица данных, которой оперирует прикладной уровень обычно называется сообщением, к протоколам прикладного уровня относится, в частности, протокол HTTP, с помощью которого браузер взаимодействует с веб-сервером), <i>представления</i> (преобразует данные в общий формат, интерпретация данных, не меняя содержания, отвечает за преобразование форматов данных, кодирование/декодирование, примеры преобразования данных это форматирование, сжатие, перевод, кодирование, шифрование), <i>сеансовый</i> (поддержка взаимодействия между удаленными процессами, управляет диалогами между двумя процессами, на практике немногие приложения используют данный уровень, и он редко используется в виде отдельных протоколов, функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе), <i>транспортный</i> (управляет передачей данных по сети, обеспечивает подтверждение передачи, осуществляет надежную доставку данных от отправителя к получателю в ненадежной КС, основные функции это принять данные сеансового уровня, разбить их при необходимости на небольшие части, передать их сетевому уровню и гарантировать что эти части в правильном виде придут по назначению и там будут собраны), <i>сетевой</i> (маршрутизация, управление потоками данных, адресацией сообщений для доставки преобразования логических сетевых адресов и имен соответствующие в физические, задача этого уровня заключается в том, чтобы обеспечить связь и выбор оптимального пути между двумя узлами компьютерной сети, этот уровень решает две важные задачи 1)решается задача логической адресации узлов 2)проеисходит выбор оптимального пути для доставки данных (пакеты данных). Маршрутизация)), <i>канальный</i> (управляет формированием кадров LLC и доступом к среде MAC, передает кадры между двумя узлами сети непосредственно связанными между собой, функции этого уровня -управление доступом к среде; -надежная доставка и обнаружение и возможность исправления ошибок-управление потоком), <i>физический</i> (битовые протоколы передачи данных, со</p>	<p>19. Распределение функций между сетевым оборудованием по уровням модели OSI. Прикладной уровень (уровень 7). Обеспечивает взаимодействие сети и пользователя. Прикладной уровень содержит набор популярных протоколов, необходимых пользователям. Протоколы этого уровня определяют совместно используемые сетевые службы, например: www; электронная почта; сетевая печать; пересылка файлов через сеть. Адресация приложений: номер порта. Протоколы: HTTP, SMTP, POP3, IMAP, FTP. Единица данных,которой оперирует прикладной уровень, обычно называется сообщением. <i>Уровень представления (уровень 6).</i> Уровень представления обеспечивает представление передаваемой по сети информации, не меняя при этом ее содержания. Уровень отвечает за: преобразование форматов данных; кодирование/декодирование.Примеры преобразования данных: форматирование; сжатие; перевод; кодирование; шифрование. <i>Сеансовый уровень.</i> Позволяет двум сторонам поддерживать длительное взаимодействие по сети, называемое сеансом. Функции сеансового уровня: установление сеанса; поддержка/управление сеансов; разрыв сеанса; синхронизация передачи данных (можно помещать контрольные точки в поток данных и возвращаться назад к определенной точке). Примеры протоколов: N248; SSH. На практике немногие приложения используют сеансовый уровень и он редко реализуется в виде отдельных протоколов. Более того в реальных стеках протоколов функции рассмотренных трех уровней (прикладной, представления, сеансовый) часто объединяют с функциями прикладного уровня и реализуют в одном протоколе. <i>Транспортный уровень.</i> Основная функция транспортного уровня: принять данные от сеансового уровня; разбить их при необходимости на небольшие части; передать их сетевому уровню и гарантировать, что эти части в правильном виде придут по назначению, и там будут собраны. Все протоколы, начиная с транспортного уровня и выше (4,5,6,7), реализуются программными средствами конечных узлов сети - компонентами их сетевых операционных систем. пример транспортных протоколов: протокол TCP и UDP стека TCP/IP и протокол SPX стека Novell. <i>Сетевой уровень.</i> Сетевой уровень решает следующие задачи: определение маршрута от узла отправителя до узла получателя; организация продвижения данных по этому маршруту; согласование технологий при передаче данных, т.к. подсети составной сети могут быть построены на основе разных технологий; управление параметрами процесса передачи данных (временные задержки, загрузки линий связи); создание барьеров (экраны) на пути нежелательного трафика между сетями. Таким образом, сетевой уровень отвечает за передачу датаграмм между удаленными компьютерами. Функции сетевого уровня: адресация компьютеров во всей глобальной сети (IP-адреса); выбор маршрута доставки сообщений; не обеспечивает надежность доставки (искажения, потери, изменение порядка следования). Протоколы: IP, ARP, RARP, ICMP, DHCP. <i>Канальный уровень (уровень 2).</i> Передает кадры-наборы битов - между двумя узлами (ПК и сетевые устройства) сети, непосредственно связанными между собой (в пределах подсети). Функции канального уровня: управления доступом к среде (подуровень MAC); надежная доставка и обнаружение возможность исправления ошибок (контрольная сумма, спец. кодирование); управление потоком. Идентификация компьютеров: MAC-адреса в Ethernet. Адреса, с которыми работает канальный уровень, используются для доставки кадров только в пределах подсети. технологии: Ethernet (802.3), WiFi (802.11), Token Ring (802.5), SONET/SDH. <i>Физический уровень (уровень 1).</i> Физический уровень в первом приближении имеет дело с передачей потока битов по физическим каналам связи, например, таким как: коаксиальный кабель; витая пара; оптоволоконный кабель или цифровой территориальный канал. Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером.</p>	<p>20.Сетезависимые и независимые уровни модели OSI Физический,канальный и сетевой являются сетезависимыми,то есть протоколы этих уровней тесно связаны с технической реализацией сети и используются коммуникационным оборудованием. Прикладной,представительный и сеансовый -являются сетезависимыми.Ориентированы на приложения и мало зависят от технических особенностей построения сети. Именно на протоколы этих уровней не влияют какие бы то ни было изменения,например, в топологии сети замена оборудования или переход на другую сетевую технологию. Транспортный уровень является промежуточным,он скрывает все детали функционирования нижних уровней от верхних.Это позволяет разрабатывать приложения,не зависящие от технических средств транспортировки сообщений</p> 

<p>единицы(1). Это означает, что пакет получат и обработают все узлы в локальной сети.Групповая рассылка(Multicast)</p> <p>Адреса многоадресных рассылок позволяют источнику рассылать пакет группе устройств. Устройства, принадлежащие к многоадресной группе, получают ее IP-адрес. Диапазон таких адресов - от 224.0.0.0 до 239.255.255.255(класс D). Многоадресный MAC-адрес - это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E.</p>	<p>В – диапазон из 16 номеров сетей: 172.16.0.0 – 172.31.0.0; диапазон адресов: 172.16.0.1 – 172.31.255.254 •В классе С – диапазон из 256 сетей: 192.168.0.0 – 192.168.255.0; диапазон адресов: 192.168.0.1 – 192.168.255.254. Любая организация может использовать IP-адреса из этих блоков без согласования с ICANN или Internet-регистраторами. В результате эти адреса используются во множестве организаций. Уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. 3. Централизованное распределение используется в случае, если сеть является частью глобальной сети Internet. Главным органом регистрации глобальных адресов Проблема этого вида распределения – дефицит адресов, обусловленный не только ростом сетей, но и нерациональным расходом адресного пространства. ICANN занимается распределением диапазонов адресов между крупными организациями-поставщиками услуг по доступу к сети Интернет (Internet Service Provider). В Европе, например, это RIPE (Reseaux IP Europeens). 4. Специальный пул адресов класса В. Адреса 169.254.0.1 по 169.254.255.254 зарезервированы для динамического назначения адресов в отсутствие DHCP-сервера. Такая система адресации называется автоматической частной IP-адресацией (Automatic Private IP Addressing, APIPA). Адреса из этого диапазона получают рабочие станции, настроенные как DHCP-клиенты если DHCP-сервер не доступен.</p>	<p>равные отдельных подсети, при этом трафик в каждой подсети должен быть надежно локализован. Это позволит легче диагностировать сеть и проводить в каждой из подсетей особую политику безопасности. Заметим, что разделение большей сети с помощью масок имеет еще одно преимущество - оно позволяет скрыть внутреннюю структуру КС предприятия от внешнего наблюдения и тем самым повысить ее безопасность. Выполним разделение пула адресов на две равные части каждая по 128. При этом число разрядов, доступное для нумерации узлов, уменьшилось на один бит (было 8- стало 7), а префикс (номер сети) каждой из двух сетей стал длиннее на один бит (было 24 - стало 25). Следовательно, каждый из двух диапазонов можно записать в виде IP-адреса с маской, состоящей не из 24, а из 25 единиц. Итак с помощью масок администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей.</p>	<p>эффективно использовать адресное пространство; •позволяет использовать маски подсети разной длины; •разбивает блок адресов на менее крупные блоки; •позволяет суммировать маршруты; •обеспечивает большую гибкость при конструировании сети; •поддерживает иерархические корпоративные сети. Пример: Пусть сеть имеет номер 129.44.0.0 (00000001 00101100 00000000 00000000), относящийся классу В. Зададим маску равную 255.255.192.0 (11111111 11111111 11000000 00000000). После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 до 18, то есть получили возможность использовать вместо одного, централизованно заданного номера сети, четыре.</p>	<div><div>Отображение IP-адресов на локальные адреса</div><div><div><div>MAC - адрес</div><div>12-B7-03-FA-AD-E4</div></div><div><div>IP-адрес</div><div>10.150.6.2</div></div><div>ARP</div></div></div> <p>Протокол разрешения адресов реализуется различным образом в зависимости от того, работает ли в данной сети протокол локальной сети с возможностью широковещания или же какой-либо из протоколов глобальной сети, которые как правило не поддерживают широковещательный доступ. Протокол ARP поддерживает на каждом интерфейсу сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе функционирования сети накапливается информация о соответствии между IP-адресами и MAC-адресами других интерфейсов данной сети. Первоначально, при включении компьютера или маршрутизатора в сеть его ARP-таблицы пусты.Посмотреть арп-таблицу можем с помощью утилиты арп -а.Процедура отображения 1)на первом шаге происходит передача от протокола IP протоколу ARP 2) Работа протокола ARP начинается с просмотра собственной ARP-таблицы.Предположим, что среди содержащихся в ней записей отсутствует запрашиваемый IP 3) В этом случае исходящий IP пакет, для которого оказалось невозможным определить локальный адрес из ARP-таблицы, запоминается в буфере,а протокол ARP формирует ARP-запрос,вкладывает его в кадр протокола Ethernet и широковещательно рассылает 4)Все интерфейсы сети Ethernet получают ARP-запрос и направляют его "своему" протоколу ARP. 5)ARP сравнивает указанный в запросе адрес IP с IP-адресом интерфейса, на который поступил этот ARP-запрос 6)протокол ARP который констатировал совпадение,формирует ARP-ответ 7)В ARP-ответе узел(хост,маршрутизатор)указывает локальный адрес MAC своего интерфейса и отправляет его запрашивающему узлу,используя его локальный адрес, взятый из запроса 8)Широковещательный ответ в этом случае не требуется,так как формат ARP-запроса предусматривает поля локального и сетевого адресов отправителя 9)Заметим,что зона распространения ARP-запросов ограничивается локальной сетью,так как на пути широковещательных кадров барьером стоит маршрутизатор 10)чтобы уменьшить число ARP-обращений в сети,найденное соответствие IP-адрес и MAC-адрес запоминается в ARP-таблице инициатора запроса 11)теперь если вдруг вновь возникает необходимость послать пакет по тому же адресу,то протокол IP прежде,чем отсылать широковещательный запрос,проверит,нет ли уже такого адреса в ARP-таблице 12)Таким образом ARP-таблица пополняется не только за счет поступающих на данный интерфейс ARP-ответов,но и также в результате извлечения полезной информации из широковещательных ARP-запросов</p>																																
<p>31. Способы назначения IP-адресов. Протокол DHCP. IP-адреса могут назначаться узлам сети: •вручную администратором сети; •динамически. <i>Протокол DHCP (Dynamic Host Configuration Protocol).</i> Способы назначения адресов: 1. 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. 2. При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и 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 некоторое время (продолжительность аренды). <i>Описание протокола.</i> Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68. Шаг 1. Обнаружение DHCP. При старте компьютер-клиент, находящийся в состоянии инициализация, посылает ограниченное широковещательное сообщение - discover (исследовать), которое распространяется по локальной сети и передается всем DHCP-серверам. Шаг 2. Предложение</p>	<p>32. Алгоритм протокола DHCP. 1) Обнаружение DHCP. При старте компьютер-клиент, находящийся в состоянии инициализация, посылает ограниченное широковещательное сообщение - discover (исследовать), которое распространяется по локальной сети и передается всем узлам данной сети и DHCP-серверам. 2) Предложение DHCP. Каждый DHCP-сервер (их может быть несколько), получивший это сообщение, отвечает на него сообщением DHCP OFFER (предложение), которое содержит IP-адрес и конфигурационную информацию. Но это только предложение! 3) Запрос DHCP. Компьютер-клиент собирает конфигурационные предложения от DHCP-серверов и переходит в состояние выбор. Клиент выбирает один из предложенных адресов и посылает широковещательно DHCPREQUEST, которое должно содержать параметр Server Identifier, чтобы указать, какой сервер им выбран. 4) Подтверждение DHCP. Все серверы получают DHCP-запрос, и только один выбранный DHCP-сервер посылает сообщение DHCP-acknowledgment (подтверждение → квитанцию), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации. Все оставшиеся серверы аннулируют свои предложения.</p>	<p>33. Специальный пул адресов класса В. Адреса 169.254.0.1 по 169.254.255.254. Это специальный пул адресов класса В, зарезервированных для динамического назначения адресов в отсутствие DHCP-сервера. Такая система адресации называется автоматической частной IP-адресацией (Automatic Private IP Addressing, APIPA). Адреса из этого диапазона получают рабочие станции, настроенные как DHCP-клиенты, если DHCP-сервер не доступен.</p>	<p>34. Протокол межсетевого взаимодействия. Протокол IP составляет основу транспортных средств стека протоколов TCP/IP. Он относится к протоколам без установления соединения (дейтаграммный протокол). Основные свойства и функции протокола: 1) Обеспечивает передачу IP-дейтаграмм (IP- пакетов) от отправителя к получателям через объединенную систему компьютерных сетей (между сетями). 2) Не устанавливает соединение (дейтаграммный протокол). 3) Не дает гарантии доставки и сохранения порядка доставки. Если произошла ошибка то протокол ничего не делает для исправления ошибки. 4) Обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. 5) Способен выполнять динамическую фрагментацию пакетов при передаче их между сетями с различным максимальным размером кадра (путевой параметр MTU).</p>	<p>35. Формат IP-пакета. IP-пакет состоит из полей заголовка и данных. Имеется прямая связь между кол-вом полей заголовка пакета и функциональной сложностью протокола, который работает с этим заголовком. Чем проще заголовок - тем проще соответствующий протокол. Большая часть действий протокола связана с обработкой той служебной информации, которая переносится в полях заголовка пакета. Изучая назначение каждого поля заголовка IP-пакета, мы получаем не только формальные знания о структуре пакета, но и знакомимся с основными функциями IP-протокола.</p> <table><tr><td>4 бита Номер версии</td><td>4 бита Длина заголовка</td><td>8 бит Тип сервиса</td><td>16 бит Полный размер пакета</td></tr><tr><td colspan="2">PR</td><td colspan="2">D T T R</td></tr><tr><td colspan="2">16 бит Идентификатор дейтаграммы (пакета)</td><td>3 бита Отклик</td><td>13 бит Указатель (сигнатура) фрагмента</td></tr><tr><td colspan="2">D M</td><td colspan="2"></td></tr><tr><td>8 бит Время жизни</td><td>8 бит Протокол верхнего уровня</td><td colspan="2">16 бит Контрольная сумма заголовка</td></tr><tr><td colspan="4">32 бита IP-адрес отправителя</td></tr><tr><td colspan="4">32 бита IP-адрес получателя</td></tr><tr><td colspan="4">Параметры IP и выравнивания</td></tr></table> <p>Поле Версия содержит версию протокола, к которому принадлежит дейтаграмма. Включение версии в каждую</p>	4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Полный размер пакета	PR		D T T R		16 бит Идентификатор дейтаграммы (пакета)		3 бита Отклик	13 бит Указатель (сигнатура) фрагмента	D M				8 бит Время жизни	8 бит Протокол верхнего уровня	16 бит Контрольная сумма заголовка		32 бита IP-адрес отправителя				32 бита IP-адрес получателя				Параметры IP и выравнивания			
4 бита Номер версии	4 бита Длина заголовка	8 бит Тип сервиса	16 бит Полный размер пакета																																	
PR		D T T R																																		
16 бит Идентификатор дейтаграммы (пакета)		3 бита Отклик	13 бит Указатель (сигнатура) фрагмента																																	
D M																																				
8 бит Время жизни	8 бит Протокол верхнего уровня	16 бит Контрольная сумма заголовка																																		
32 бита IP-адрес отправителя																																				
32 бита IP-адрес получателя																																				
Параметры IP и выравнивания																																				

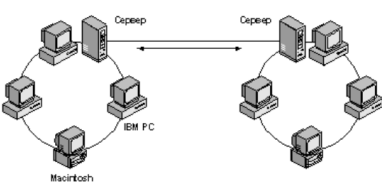
<p>DHCP. Каждый DHCP-сервер, получивший это сообщение, отвечает на него сообщением DHCPOFFER (предложение), которое содержит IP-адрес и конфигурационную информацию. Но это только предложение. Шаг 3. Запрос DHCP. Компьютер-клиент переходит в состояние выбора и собирает конфигурационные предложения от DHCP-серверов. Клиент выбирает один из предложенных адресов и посылает широковещательно DHCPREQUEST, которое должно содержать параметр ServerIdentifier, чтобы указать, какой сервер им выбран. Шаг 4. Подтверждение DHCP. Выбранный DHCP-сервер посылает сообщение DHCP-acknowledgment (подтверждение), содержащее тот же IP-адрес, который уже был послан ранее на стадии исследования, а также параметр аренды для этого адреса. Кроме того, DHCP-сервер посылает параметры сетевой конфигурации.</p> <p>DHCP-сервер может назначить клиенту не только его IP-адрес, но и другие параметры стека, необходимые для эффективной работы: маску, IP-адрес маршрутизатора по умолчанию, IP-адрес сервера DNS, доменное имя компьютера и др.</p>				<p>дейтаграмму позволяет использовать разные версии протокола на разных сетевых устройствах (ПК, router,...). Поле Тип сервиса используется для управления приоритетом (качеством сервиса) отведено 8 бит. - PR, приоритет: *111 - управление сетью; *110 - межсетевое управление; *100 - более чем мгновенно; * 011 - мгновенно; * 010 - немедленно; * 001 - срочно; * 000 - обычно.</p> <p>Флаги D, T, R определяют желаемый тип маршрутизации: D - выбор маршрута с минимальной задержкой; T - выбор маршрута с максимальной пропускной способностью; R - выбор маршрута с максимальной надежностью.</p>														
<p>36. О фрагментации IP-пакетов. Идентификатор (16 бит) пакета используется для распознавания пакетов, образовавшихся путем деления на части (фрагментации) исходного пакета. Все части (фрагменты) одного пакета должны иметь одинаковое значение этого поля. Поле Сместение фрагмента указывает положение фрагмента в исходной дейтаграмме. Длина всех фрагментов в байтах, кроме длины последнего фрагмента, должна быть кратна 8. Так как на это поле выделено 13 бит, максимальное количество фрагментов в дейтаграмме равно 8192, что дает максимальную длину дейтаграммы 65 536 байт. Флаги занимают 3 бита и содержат признаки, связанные с фрагментацией: 1й бит – резерв, всегда 0. 2й бит – DF, 1- DonotFragment – запрещает фрагментацию, бит MF – MoreFragments – 0 для нефрагментированного или последнего пакета в серии, 1 – в противном случае. Алгоритм фрагментации. Отправитель: 1. Данные пакета делятся на кратные 8 байтам части, кроме последней. Каждая из них помещается в новый пакет. 2. Задаёт уникальное значение поля Идентификатор пакета. 3. Устанавливаются флаги - признаки, связанные с фрагментацией: 4. Сместение фрагмента (13 бит) - смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета. Получатель: 1. При приеме первого фрагмента получатель запускает таймер, определяющий максимальное допустимое время ожидания прихода остальных фрагментов – максимальное из двух значений: а) начальное установочное время; б) TTL, указанное в фрагменте. 2. Если таймер истекает до прихода всех фрагментов, то все ресурсы, связанные с данным пакетом, освобождаются, все фрагменты отбрасываются. 3. Во всех случаях ошибок при фрагментации отправителю пакета посылается сообщение с помощью протокола ICMP.</p>	<p>37. Характеристика MTU.(Path Maximum Transmission Unit). MTU - это максимальный размер пакета данных, который может быть передан по сетевому интерфейсу без фрагментации. Значения MTU зависят как от протокола, так и от настройки сетевых интерфейсов. При фрагментации в узле-отправителе протоколы верхнего уровня анализируют технологию нижнего уровня и определяют ее MTU. При фрагментации сообщений в транзитных узлах передача пакета из сети с большим в сеть с меньшим MTU.</p> <p>Значения MTU некоторых технологий</p> <table><tr><th>Технология</th><th>MTU, байт</th></tr><tr><td>Ethernet DIX</td><td>1500</td></tr><tr><td>Ethernet 802.3</td><td>1492</td></tr><tr><td>Token Ring (IBM, 16 Мбит/с)</td><td>17914</td></tr><tr><td>Token Ring (802.5, 4 Мбит/с)</td><td>4464</td></tr><tr><td>FDDI</td><td>4352</td></tr><tr><td>X.25</td><td>576</td></tr></table> <p>Фрагментация: *Если размер пакета превышает MTU, он будет разбит (фрагментирован) на несколько меньших пакетов. *Фрагментация происходит на сетевом уровне (IP-уровне) и требует дополнительных накладных расходов. *При приеме фрагментированные пакеты должны быть собраны обратно в исходный пакет. Производительность: *Большее значение MTU обычно улучшает производительность за счет снижения накладных расходов на обработку заголовков. *Однако слишком большой MTU может привести к потере пакетов на перегруженных или ненадежных линиях связи. Настройка: *MTU можно настраивать на сетевых интерфейсах, маршрутизаторах и других сетевых устройствах. *Правильная настройка MTU важна для оптимизации производительности сети.</p>	Технология	MTU, байт	Ethernet DIX	1500	Ethernet 802.3	1492	Token Ring (IBM, 16 Мбит/с)	17914	Token Ring (802.5, 4 Мбит/с)	4464	FDDI	4352	X.25	576	<p>38. ICMP-протокол межсетевых управляющих сообщений. Является вспомогательным сетевым протоколом, включенным в стек протоколов TCP/IP. - дополняет протокол IP -выполняет вспомогательные функции мониторинга и диагностики. Протокол IP не содержит достаточных средств для организации надежной доставки сообщения. В частности, пакеты IP теряются в случае, если пакет не прошел проверку контрольной суммы, не найден маршрут к заданному узлу назначения (параметр TTL равен нулю) и т.д. Все это сводится к тому, что протокол IP передает сообщения «по возможности» или другими словами, не прилагает никаких мер для гарантированной доставки сообщений. Компенсируют недостаточную надежность протокола IP механизмы уменьшения ненадежной передачи сообщений протоколом IP – протокол ICMP. Принцип работы ICMP заключается в том, что данный протокол срабатывает для передачи сообщений об ошибках при передаче или исключительных ситуациях, то есть, когда маршрутизатор не работает или требуемая услуга недоступна. По сути, протокол ICMP не может запросить послать потерянный пакет повторно, а просто оповещает о несчастных случаях. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают. Также на ICMP возлагаются некоторые сервисные функции. Когда протокол IP определяет, что дальнейшая передача пакета невозможно, перед тем как уничтожить пакет, должен отослать узлу-источнику диагностическое ICMP-сообщение. Если при передаче самого ICMP-сообщения возникла ситуация препятствующая его передаче, то протокол ICMP не будет отправлять об этом диагностическое сообщения, для избегания «штормов» в сетях. При передаче по сети, сообщения ICMP инкапсулируются в поле данных IP-пакетов.</p>	<p>39. Маршрутизирующие протоколы и протоколы маршрутизации. На уровне межсетевого взаимодействия располагаются два вида протоколов: 1. Маршрутизирующие протоколы, которые обеспечивают продвижение пакетов из одной подсети в другую (например, IPv4, IPv6 реализуют транзит на базе TM); 2. Протоколы маршрутизации, которые обеспечивают автоматическое заполнение маршрутных таблиц (TM). Маршрутизирующие протоколы. К таким протоколам относятся интернет-протоколы IP четвертой и шестой версии. Для их правильного функционирования в памяти маршрутизатора должны храниться TM. Конкретный вид TM зависит кроме того от модели устройства-маршрутизатор, ОС и протоколов маршрутизации. Задачу выбора маршрута решают устройства маршрутизаторы. а также конечные узлы. На основе TM. TM заполняют протоколы маршрутизации.</p>	
Технология	MTU, байт																	
Ethernet DIX	1500																	
Ethernet 802.3	1492																	
Token Ring (IBM, 16 Мбит/с)	17914																	
Token Ring (802.5, 4 Мбит/с)	4464																	
FDDI	4352																	
X.25	576																	
<p>41. Таблица маршрутизации (TM). Таблица маршрутизации - электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации. Каждая запись в таблице маршрутизации состоит, как правило, из таких полей: адрес сети назначения (destination); маска сети назначения (netmask, genmask); адрес шлюза (gateway), за исключением тех случаев, когда описывается в маршрут непосредственно доступную (directly connected) сеть, в этом случае вместо адреса шлюза обычно указывается 0.0.0.0; метрика маршрута (не всегда). Первым источником является программное обеспечение стека TCP/IP. При инициализации маршрутизатора это программное обеспечение автоматически заносит в таблицу несколько записей, в результате чего создается так называемая минимальная таблица маршрутизации. Это, во-первых, записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию, информация о которых появляется в стеке при ручном конфигурировании интерфейсов компьютера или маршрутизатора. Во-вторых, программное обеспечение автоматически заносит в таблицу маршрутизации записи об адресах особого назначения. Вторым источником появления записи в таблице является администратор, непосредственно формирующий запись с помощью некоторой системной утилиты</p> <p>В аппаратных маршрутизаторах также всегда имеется команда для ручного задания записей таблицы маршрутизации. Заданные вручную записи всегда являются статическими, то есть не имеют срока истечения жизни. Эти записи могут быть</p>	<p>42. Источники и типы записей в TM. Практически для всех маршрутизаторов существуют три основных источника формирования записей в таблице маршрутизации:</p> <p>1) Программное обеспечение стека TCP/IP (протокол ICMP), создающее минимальную TM, содержащую записи: о непосредственно подключенных сетях, маршрутизаторах по умолчанию. адресах особого назначения, специфические адреса.</p> <p>2) Администратор КС, непосредственно формирующий записи, например, с помощью системных утилит (route) или при конфигурировании устройства. Заданные вручную записи являются статическими и не имеют срока истечения жизни</p> <p>3) Протоколы маршрутизации, работающие на основе адаптивных алгоритмов (RIP , OSPF). Такие записи всегда являются динамическими, т.е. имеют ограниченный срок жизни</p>	<p>43. Маршрутизация в IP-сетях. Маршрутизация без масок на основе классов. Пусть на порт маршрутизатора поступает пакет. Протокол IP извлекает из заголовка пакета адрес назначения. 1. Первая фаза просмотра - поиск конкретного маршрута к узлу. IP-адрес (целиком) из заголовка пакета последовательно строка за строкой сравнивается с содержимым поля адреса назначения TM. Если произошло совпадение, то из соответствующей строки извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса текущего маршрутизатора. На этом просмотр таблицы заканчивается. Предположим теперь, что в таблице совпадения не произошло. В этом случае протокол IP переходит ко второй фазе просмотра -> поиску маршрута к сети назначения. 2. Вторая фаза просмотра. Из IP-адреса (заголовков пакета) выделяется номер строки (класс адреса известен) и, TM снова просматривается на предмет совпадения номера сети в какой-либо строке с номером сети из пакета. При совпадении из соответствующей строки таблицы извлекаются адрес следующего маршрутизатора и идентификатор выходного интерфейса. Наконец, предположим, что адрес назначения в пакете был таков, что совпадения не произошло ни в первой, ни во второй фазе просмотра. 3. Третья фаза. В таком случае средствами протокола IP а) либо выбирается маршрут по умолчанию (и пакет направляется по адресу), б) либо если маршрут по умолчанию отсутствует, пакет отбрасывается.</p>	<p>44. Маршрутизация в IP-сетях. Маршрутизация с использованием масок постоянной длины. Алгоритм просмотра таблиц маршрутизации, содержащих маски, имеет много общего с описанным алгоритмом просмотра таблиц, не содержащих маски. Однако в нем имеются и существенные изменения. Поиск следующего маршрутизатора для вновь поступившего IP-пакета протокол начинает с того, что извлекает из заголовка пакета адрес назначения. Затем протокол IP приступает к процедуре просмотра таблицы маршрутизации, также состоящей из двух фаз, как и процедура просмотра таблицы, в которой столбцы маски отсутствуют. Первая фаза состоит в поиске специфического маршрута для адреса. С этой целью из каждой записи таблицы, в которой маска имеет значение 255.255.255.255, извлекается адрес назначения и сравнивается с адресом из пакета. Если в какой-либо строке совпадение произошло, то адрес следующего маршрутизатора для данного пакета берется из данной строки. Вторая фаза выполняется только в том случае, если во время первой фазы не произошло совпадения адресов. Она состоит в поиске специфического маршрута, общего для группы узлов, к которой относится и пакет с адресом IP. Для этого заново просматривается таблица маршрутизации, причем с каждой записью производится следующие действия: 1. маска, содержащаяся в данной записи (строке TM), "накладывается" на IP-адрес узла назначения, извлеченного из заголовка пакета. 2. полученное в результате число сравнивается со значением, которое помещено в поле адреса назначения той же записи TM; 3. если происходит совпадение, протокол IP соответствующим образом отмечает эту строку; 4. если просмотрены не все строки, то протокол IP аналогичным образом просматривает следующую строку, если все (включая строку о маршруте по умолчанию), то просмотр записей заканчивается, и происходит переход к следующему шагу. После просмотра всей таблицы маршрутизатор выполняет одно из трех действий: а) если не</p>															
				<p>45. Маршрутизация в IP-сетях. Маршрутизация с использованием масок переменной длины. Маски подсети переменной длины (VLSM - Variable Length Subnet Masking). Недостатком адресов на основе классов является то, что они обычно предоставляют либо слишком большой (см. предыдущий пример), либо слишком маленький диапазон адресов для использования в большинстве ситуаций. Технология VLSM, которая позволяет сетевому администратору разбивать адресное пространство IP-сети на подсети неравных размеров, в отличие от простого разбиения. Во многих случаях на практике более эффективным является разбиение сети именно на подсети разного размера. Администратор может более рационально распределить имеющееся в его распоряжении пространство с помощью масок переменной длины. Если использовать маски переменной длины, то можно организовать более рациональное распределение адресного пространства, при котором избыточность имеющегося множества IP-адресов может быть сведена к минимуму. Половина из имеющихся адресов, НАПРИМЕР, отводится для создания сети с адресом 129.44.0.0 и маской 255.255.128.0. Следующая порция адресов, составляющая четверть всего адресного пространства назначается для сети 129.44.128.0 с маской 255.255.192.0. Далее в пространстве адресов «вырезается» небольшой фрагмент для создания сети, предназначенной для связывания внутреннего маршрутизатора M2 с внешним маршрутизатором M1. Преимущества VLSM: *позволяет эффективно использовать адресное пространство; *позволяет</p>														

<p>как постоянными, то есть сохраняющимися при перезагрузке маршрутизатора, так и временными, хранящимися в таблице только до выключения устройства. Часто администратор вручную заносит запись default о маршрутизаторе по умолчанию. И наконец, третьим источником записей могут быть протоколы маршрутизации, такие как RIP или OSPF. Такие записи всегда являются динамическими, то есть имеют ограниченный срок жизни.</p>			<p>произошло ни одного совпадения и маршрут по умолчанию отсутствует, то пакет отбрасывается; б) если произошло только одно совпадение, то пакет отправляется по маршруту, указанному в строке с совпавшим адресом; в) если произошло несколько совпадений, то все помеченные строки сравниваются и выбирается маршрут из той строки, в которой кол-во совпавших двоичных разрядов в старшей части IP-адреса в заголовке пакета наибольшее. Другими словами, в ситуации, когда адрес назначения пакета принадлежит сразу нескольким подсетям, маршрутизатор использует наиболее специфический маршрут.</p>	<p>использовать маски подсети разной длины; *разбивает пул адресов на менее крупные блоки; *позволяет суммировать маршруты; *обеспечивает большую гибкость при проектировании сети; *поддерживает иерархические корпоративные сети.</p>
<p>46. Технология бесклассовой междоменой маршрутизации CIDR. Технология бесклассовой междоменой маршрутизации CIDR. Недостатки в организации распределения адресного пространства: • Нехватка IP. Размеры существующих классов сетей перестали отражать требования средних организаций. Количество компьютеров в сети организации часто оказывалось больше, чем количество адресов в сети класса C, но гораздо меньше, чем в сети класса B. • Замедление обработки таблиц маршрутизации. Рост размеров таблиц маршрутизации в Internet-маршрутизаторах привел к тому, что их стало сложно администрировать. Основная идея – каждому провайдеру услуг Internet должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого провайдера имеют общий префикс. Пусть имеется некоторое пр-во IP с общим префиксом в к старших разрядах. Оставшиеся n разрядов, составляющие переменную часть адреса, позволяют иметь диапазон в 2ⁿ адресов. Когда потребитель услуг обращается к поставщику с просьбой о выделении некот. кол-ва адресов, то в имеющемся пуле вырезается непрерывная область соответствующего размера. Такому условию удовлетворяют только области, размер которых кратен 2, а границы выделяемого участка должны быть кратны требуемому размеру. Для обобщенного представления пула адресов в виде IP/n справедливо: *Значением префикса (номера сети) являются в старших двоичных разрядах IP-адреса. *Поле для адреса состоит из (32-n) младших двоичных разрядов IP. *Первый по порядку адрес должен состоять только из нулей. *Количество адресов в пуле равно 2(32-n) . Структуризация сети на основе масок называется разделением на подсети. Вместе с тем при разделении сети на подсети с помощью масок проявлялся и обратный эффект — объединение подсетей. Чтобы направить весь суммарный трафик, адресованный из внешн. окруж. в корпорат. сеть, разделенную на подсети, достаточно, чтобы в таблицах маршрутизации всех внешних маршрутизаторов имелась только одна строка — необходимо провести операцию агрегирования нескольких сетей в одну более крупную сеть. Неохот. усл. эффективного использования CIDR – локализация адресов, то есть назначение адресов, имеющих совпадающие префиксы, сетям, расположенным территориально по соседству. Только в таком случае трафик может быть агрегирован.</p>	<p>47. Трансляция сетевых адресов Network Address Translation (NAT). Маршрутизация в составной сети осуществляется на основе тех адресов назначения, которые помещены в заголовки пакетов. Как правило, эти адреса остаются неизменными с момента их формирования отправителем до момента поступления на узел получения. Однако из этого правила есть исключения. Например, в широко применяемой сегодня технологии трансляции сетевых адресов (Network Address Translation, NAT) предполагается продвижение пакета во внешней сети (в Интернете) на основании адресов, отличающихся от тех, которые используются для маршрутизации пакета во внутренней (корпоративной) сети. Основная причина использования NAT — дефицит IP. Традиционная технология NAT позволяет улаزم из частной сети прозрачным для пользователей образом получать доступ к улазм внешних сетей. Традиционная технология NAT подразделяется на технологии. Базовой трансляции сетевых адресов (Basic NAT) Трансляции сетевых адресов и портов (Network Address Port Translation, NATP). Basic NAT- для отображения используются только IP-адреса. Статические преобразования гарантируют, что частный IP-адрес отдельного улаза будет всегда преобразовываться в один и тот же зарегистрированный глобальный адрес. Кроме того, благодаря этому адрес никогда не получит другой локальный узел. Динамическое преобразование NAT происходит в том случае, если маршрутизатор присваивает IP-адреса из доступного пула внешних глобальных адресов. При настройке NAT для внешнего доступа следует использовать динамический вариант NAT. Если устройство из внутренней сети должно быть доступно извне, используйте статич. вариант NAT. Ответный трафик адресуется на преобразованный IP-адрес и номер порта улаза. В таблице маршрутизатора находится список внутренних IP-адресов и номеров портов, которые преобразуются во внешние адреса. Ответный трафик направляется на соответствующий внутренний адрес и номер порта.</p>	<p>48. Трансляция адресов и номеров портов (Network Address Port Translation - NATP). Если зарегистрированный пул IP-адресов организации очень небольшой или если у нее есть всего один IP-адрес, к общедоступной сети все равно могут одновременно подключаться несколько пользователей, с использованием механизма, который называется технологией NATP. В режиме NATP шлюз преобразует адрес локального источника и номер порта из пакета в один глобальный IP-адрес и уникальный номер порта выше 1024. Ответный трафик адресуется на преобразованный IP-адрес и номер порта улаза. В таблице маршрутизатора находится список внутренних IP-адресов и номеров портов, которые преобразуются во внешние адреса. Ответный трафик направляется на соответствующий внутренний адрес и номер порта. NATP позволяет всем улазм внутренней сети одновременно взаимодействовать с внешними сетями, используя единственный зарегистрированный IP-адрес. Для однозначной идентификации улаза отправителя привлекается дополнительная информация. Если в IPv-пакете находятся данные протокола UDP или TCP, то в качестве такой информации выступают номер UDP- или TCP-порта соответственно. Но и это не вносит полной ясности, поскольку из внутренней сети может исходить несколько запросов с совпадающими номерами портов отправителя, а значит, опять возникает вопрос об однозначности отображения единственного глобального адреса на набор внутренних адресов. Решение состоит в том, что при прохождении пакета из внутренней во внешнюю сеть каждой паре [внутренний частный адрес; номер TCP- или UDP-порта отправителя] ставится в соответствие пара [глобальный IP-адрес внешнего интерфейса; назначенный номер TCP- или UDP-порта]. Назначенный номер порта выбирается произвольно, однако должен быть выполнено условие его уникальности в пределах всех узлов.</p>	<p>49. Основные понятия маршрутизации. Основная функция устройства-маршрутизатор - чтение заголовков пакетов сетевых протоколов, принимаемых из буферизованных по каждому порту (например, IPX, IP, AppleTalk или DECnet); и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номера сети и улаза. Будет представлять себе маршрутизатор как устройство, в котором функционируют два процесса. Один из них обрабатывает приходящие пакеты и выбирает для них по ТМ исходящий путь, т.е. маршрут. Такой процесс назовем пересылкой. Второй процесс отвечает за пополнение и обновление ТМ. Именно здесь реализован алгоритм маршрутизации. Основные функции сетевого устройства - маршрутизатор могут быть разбиты на три группы (три уровня) в соответствии с уровнями модели OSI. Будем понимать устройство-маршрутизатор как специализированный компьютер с множеством "сетевых карт", заточенный на обеспечение функционирования КС. 1. Уровень интерфейсов. Основная задача - прием и распределение кадров по портам. 2. Уровень сетевого протокола. а) проверка контрольной суммы пакета, удаление поврежденных пакетов; б) проверка времени жизни пакета TTL пакета, удаление пакетов с превышенной допустимой величиной TTL; в) модификация заголовка, если пакет прошел проверки 1,2; наращивание TTL, пересчет контрольной суммы. г) Фильтрация трафика - задавать и обрабатывать сложные правила фильтрации; производить разбор и анализ отдельных полей пакета; д) введение очереди пакетов с различной дисциплиной обслуживания, в том числе и приоритетной (FIFO или случайное раннее обнаружение RED); е) определение маршрута пакета - основная функция маршрутизатора; ж) преобразование сетевого адреса следующего маршрутизатора в локальный адрес той технологии, которая используется в сети, содержащей следующий маршрутизатор; з) передача пакета на канальный уровень. 3. Уровень протоколов маршрутизации. Создание и ведение ТМ. Решение этой задачи возлагается на протоколы маршрутизации.</p>	<p>50. Классификация маршрутизаторов по областям применения. По областям применения маршрутизаторы делятся на несколько классов: 1.Магистральные маршрутизаторы, предназначенные для построения магистральной сети оператора связи или крупной корпорации. Работает внутри сети и не взаимодействует с внешним миром(не выполняет пограничные функции, требующие фильтрации и профилирования). Оперируют агрегированными информационными потоками, преобразуя данные большого кол-ва пользователей в соединения. Обладают высокой производительностью и надежностью! Каждый порт(группа портов) олицетворяет собственным микропроцессором, который самостоятельно выполняет продвижение пакетов на основе локальной копии ТМ.2.Пограничные маршрутизаторы (маршрутизаторы доступа), например, соединяют магистральную сеть с периферийными сетями. образуют основную слой, который выполняет функции приема трафика от внешних по отношению магистрали сетей. Часто находится под автономным административным управлением. На первый план выступают его способности к максимальной гибкости при фильтрации и профилировании трафика. 3.Маршрутизаторы локальных сетей предназначены для разделения крупных локальных сетей на подсети. Как правило, не имеют интерфейсов глобальных сетей. Многие маршрутизаторы этого типа ведут свое происхождение от коммутаторов локальных сетей (мосты), что и дало им второе название - коммутаторы 3-го уровня. К.Зур. выполняют все функции маршрутизаторов, но, могут работать как обычные коммутаторы локальных сетей, т.е. как К.Зур. Режим работы (маршрутизатор или коммутатор) зависит от конфигурационных параметров. К.Зур. поддерживает технику VLAN, являясь основным типом устройств для соединения отдельных виртуальных сетей в составную IP-сеть. 4.Маршрутизаторы удаленных офисов соединяют единственную локальную сеть удаленного офиса с магистральной сетью или сетью, регионального отделения по глобальной связи. Может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала. 5.Маршрутизаторы домашних сетей</p>
<p>51. Алгоритмы маршрутизации. Классификация алгоритмов маршрутизации. В общем случае под алгоритмом маршрутизации понимается набор правил, регламентирующих процедуры обмена служебной информацией между маршрутизаторами с целью заполнения из таблиц (ТМ).</p> <p>Классификация алгоритмов маршрутизации</p> <p>Алгоритмы простой маршрутизации. Существуют и такие способы продвижения пакетов в составных сетях вообще не требуют наличия таблиц маршрутизации на маршрутизаторах. Примеры: *Лавинная маршрутизация, когда каждый маршрутизатор передает пакет всем своим непосредственным соседям, исключая тот, от которого его получил (недостатки очевидны). *Случайная маршрутизация. Для передачи пакета выбирается, случайно выбранное направление. Пакет блуждает по сети и когда-либо достигнет адресата. Очень просто, но не эффективно. *Маршрутизация от источника (source routing). В этом случае отправитель помещает в пакет информацию о том, какие промежуточные маршрутизаторы должны участвовать в передаче пакета к сети назначения.</p>	<p>52. Статическая маршрутизация. При небольшом количестве подсетей, как правило, используется статическая маршрутизация, информация для которой выбирается при конфигурировании сетевого устройства. При конфигурировании необходимо: *задать адресацию подсетей; *Портам маршрутизаторов назначить сетевые адреса из диапазона адресного подпространства выше определенных подсетей; *компьютерам подсетей также необходимо задать соответствующие сетевые настройки; *этот процесс можно автоматизировать с применением протокола DHCP; *На практике обычно настраивается еще ряд параметров, например, протоколы DHCP и NAT. Замечание. Конфигурирование маршрутизаторов зависит от его модели. Статические алгоритмы маршрута называют также неадаптивные алгоритмы. Неадаптивные алгоритмы не учитывают при выборе маршрута топологию и текущее состояние сети, не измеряют трафик на линиях (не учитывается изменение нагрузки). *Несмотря этого выбор маршрута для каждой пары станций производится заранее, в автономном режиме, и список маршрутов загружается в маршрутизаторы во время загрузки сети. *Такая процедура иногда называется статической маршрутизацией. Поскольку статическая маршрутизация не реагирует на свои, она, как правило, используется в тех случаях, когда выбор маршрута очевиден и количество подсетей не много.</p>	<p>53. Динамические алгоритмы маршрутизации. Алгоритмы адаптивной маршрутизации изменяют решение о выборе маршрутов при изменении топологии и также иногда в зависимости от состояния каналов связи. Это динамические алгоритмы маршрутизации (dynamic routing algorithms), которые отличаются источниками получения информации. Такими источниками могут быть, например, *локальными, если это соседние маршрутизаторы, *либо глобальными, если это вообще все маршрутизаторы сети, *моментами изменения маршрутов. Например, при изменении топологии или через определенные равные интервалы времени при изменении нагрузки, и данными, используемыми для оптимизации (расстояние, количество транзитных участков или ожидаемое время пересылки). Основные динамические алгоритмы маршрутизации включают: 1. Алгоритм Беллмана-Форда: *Используется в протоколах маршрутизации, таких как RIP; *Основан на минимизации количества переходов (hop count); *Очень прост, но может быть медленным при сходимости. 2. Алгоритм Дейкстры: *Используется в протоколах, таких как OSPF и IS-IS; *Находит кратчайшие пути от одного улаза до всех остальных; *Более сложный, но эффективный и быстрый в скорости. 3. Алгоритм DUAL (Diffusing Update Algorithm); *Используется в протоколе EIGRP; *Обеспечивает быструю сходимости и предотвращает петли; *Учитывает несколько метрик (пропускная способность, задержка, надежность). 4. Алгоритм BGP (Border Gateway Protocol); *Используется для междоменой маршрутизации в Интернете; *Основан на политиках, а не только на оптимизации метрик; *Учитывает путь через автономные системы (AS path). Все эти алгоритмы позволяют маршрутизаторам динамически реагировать на изменения в сетевой топологии, избегать петель и предоставлять оптимальные маршруты для передачи трафика. Выбор конкретного алгоритма зависит от требований сети, масштабируемости и производительности.</p>	<p>54. Источники записей в таблице маршрутизации. Таблица маршрутизации — электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации. Каждая запись в таблице маршрутизации состоит, как правило, из таких полей: *адрес сети назначения (destination); *маска сети назначения (netmask, genmask); *адрес шлюза (gateway), за исключением тех случаев, когда описывается в маршрут непосредственно доступную (directly connected) сеть, в этом случае вместо адреса шлюза обычно указываются 0.0.0.0; *метрика маршрута (не всегда). Первым источником является программное обеспечение стека TCP/IP. При инициализации маршрутизатора это программное обеспечение автоматически заносит в таблицу несколько записей, в результате чего создается так называемая минимальная таблица маршрутизации. Это, во-первых, записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию, информация о которых появляется в стеке при ручном конфигурировании интерфейсов компьютера или маршрутизатора. Во-вторых, программное обеспечение автоматически заносит в таблицу маршрутизации записи об адресах особого назначения. Вторым источником появления записи в таблице является администратор, непосредственно формирующий записи с помощью некоторой системной утилиты. В аппаратных маршрутизаторах также всегда имеется команда для ручного задания записей таблицы маршрутизации. Заданные вручную записи всегда являются статическими, то есть не имеют срока истечения жизни. Эти записи могут быть как постоянными, то есть сохраняющимися при перезагрузке маршрутизатора, так и временными, хранящимися в таблице только до выключения устройства. Часто администратор вручную заносит запись default о маршрутизаторе по умолчанию. И наконец, третьим источником записей могут быть протоколы маршрутизации, такие как RIP или OSPF. Такие записи всегда являются динамическими, то есть имеют ограниченный срок жизни.</p>	<p>55. Дистанционно-векторные алгоритмы (DVA) и протоколы маршрутизации. 1. В DVA алгоритмах каждый маршрутизатор периодически и широкоовещательно рассылает по сети вектор расстояний от самого себя до известных ему подсетей. В качестве метрики обычно используется количество промежуточных маршрутизаторов (хопов), через которые должен пройти пакет, чтобы достигнуть подсети назначения. Маршрут с минимальной метрикой считается оптимальным. 2. Получая такой вектор от соседа-маршрутизатора, каждый маршрутизатор корректирует свою ТМ - добавляет свои сведения обо всех известных ему подсетях, и снова рассылает обновленный вектор по сети. При передаче пакета маршрутизатор (точнее IP протокол) выбирает из нескольких альтернативных маршрутов тот маршрут, который имеет наименьшую метрику. 3. Таким образом, в результате такого обмена векторами, каждый маршрутизатор в конце концов получит информацию обо всех подсетях, входящих в составную сеть, а также о расстояниях (метрике) до них. Протоколы маршрутизации: 1.RIP (Routing Information Protocol); *Простой протокол, использующий алгоритм Беллмана-Форда; *Метрика - количество переходов; *Ограничен до 15 переходов, медленная сходимости.2. OSPF (Open Shortest Path First); *Протокол с состоянием канала; *Использует алгоритм Дейкстры для нахождения кратчайшего пути; *Метрика - пропускная способность, задержка, надежность; *Масштабируется лучше, чем RIP. 3. EIGRP (Enhanced Interior Gateway Routing Protocol); *Гибридный протокол, использующий алгоритм DUAL; *Метрика учитывает несколько факторов (пропускная способность, задержка, надежность, загрузка); *Быстрая сходимости, эффективен в больших сетях. 4. IS-IS (Intermediate System to Intermediate System); *Протокол с состоянием канала, похож на OSPF; *Использует алгоритм Дейкстры; *Метрика - произвольные числовые</p>

				значения; •Широко используется в магистральных сетях провайдеров. 5. BGP (Border Gateway Protocol); •Протокол междоменной маршрутизации; •Использует политики маршрутизации; •Метрика - путь AS (Autonomous System); •Основа маршрутизации в Интернете.
<p>56. Алгоритмы состояния связей (LSA). 1. Алгоритм LSA обеспечивает каждый маршрутизатор информацией, достаточной для построения точного графа связей составной сети. Можно сказать так: карта сети. 2ю Все маршрутизаторы работают на основании одного и того же графа. 3. Итак точнее: Для формулирования алгоритмов маршрутизации сеть рассматривается как граф. При этом маршрутизаторы являются узлами, а физические линии между маршрутизаторами - ребрами соответствующего графа. Каждому ребру графа присваивается определенное число - стоимость, зависящая от физической длины линии, скорости передачи данных по линии или стоимости и др. характеристик. 4. Широковещательная рассылка используется здесь только при изменениях состояния связей. 5. А так в обычном режиме маршрутизаторы обмениваются короткими пакетами со своими ближайшими соседями. 6. Т е служебный трафик LSA менее интенсивен, чем трафик - DVA.</p>	<p>57. Архитектура маршрутизации Интернет. Архитектурно задача динамической маршрутизации в Интернет делится на два уровня: 1. маршрутизация между автономными системами; 2. маршрутизация внутри автономных систем. <i>Тилы автономных систем:</i> •Многоинтерфейсная AS - это AS, которая имеет соединения с более чем одной AS (и не является транзитной) (на рис. С). •Ограниченная AS - это AS, имеющая единственный выход во внешний мир (на рис. D). •Транзитная AS - это AS, которая имеет несколько соединений с внешним миром и если административная политика AS позволяет передавать через свои сети транзитный трафик других AS, подключенных к ней. (на рис. А, В). </p>	<p>58. Внутренняя и внешняя маршрутизация. Протоколы маршрутизации. Протоколы маршрутизации, осуществляющие маршрутизацию между автономными системами называются внешними. Протоколы маршрутизации, осуществляющие маршрутизацию внутри автономных систем называются внутренними. Протоколы внутренней маршрутизации используются для определения маршрутов внутри автономной системы. Эти протоколы также называют внутренними или внутришлюзовыми протоколами. <i>Протоколы внутренней маршрутизации.</i> •RIP - прост (минимизирует путь только по числу хопов), ограничен (максимальная длина пути - 16 хопов), получил широкое распространение в малых сетях. •IGRP - определяет путь с учетом скорости линий и суммарной задержки; развитие - EIGRP, более эффективен, и 6 используется для маршрутизации не только IP (IPX, AppleTalk). •OSPF - развитой междоменный иерархический (делит AC на магистраль и подсети) протокол, разработанный взамен RIP; гибок, эффективен, поддерживает маски сетей переменной длины. •IS-IS - междоменный иерархический протокол маршрутизации, похож на OSPF; работает через мн-во LAN- и WAN-подсетей, двухточечные соединения, поддерживает протоколы OSI. Протоколы внешней маршрутизации. •EGP - обеспечивает динамическую маршрутизацию, очень прост, ограничен, исходит из предположения, что автономные системы подключены к древовидной топологии, не использует метрик. •BGP - работает в произвольных топологиях, исключает циклы, использует метрики, высоко масштабируем.</p>	<p>59. Протокол маршрутной информации RIP. Достоинства и недостатки. Существует две версии RIP - RIPv1 и RIPv2. • первая использует маршрутизацию на основе классов (т е без масок подсетей), • вторая версия (доработана) RIPv2 использует бесклассовую маршрутизацию (позволяет работать с масками подсетей), поэтому он в большей степени соответствует требованиям сегодняшнего дня.</p> <p>Кроме того, в дополнение к широковещательному режиму поддерживает мультикастинг (Multicast - специальная форма широковещания, при которой копии пакетов направляются определённому подмножеству адресатов). •Протокол RIP не является универсальным протоколом маршрутизации и не может быть использован в IP-сети любого размера и сложности. В частности. протокол накладывает ограничения на максимальный диаметр сети. •Для протоколов RIP обеих версий максимальный диаметр сети составляет 15 маршрутизаторов. Поэтому маршрут с метрикой 16 считается недоступным (бесконечным). Отсюда RIP для больших сетей не годится.</p> <p>Для сравнения двух маршрутов к одной и той же подсети используется только метрика (кол-во хопов) и не учитываются такие параметры: скорость передачи, надежность, доступная полоса пропускания.</p> <p>•В больших сетях чаще возникает проблема цикла. Хотя в RIP предусмотрен механизм распознавания петель, но в больших сетях соответствующие алгоритмы не рациональны (по времени), увеличивают трафик сети. • Каждому маршруту в TM ставится в соответствие таймер. Тайм-аут-таймер сбрасывается каждый раз, когда маршрут инициируется или корректируется. •RIP требует много времени для восстановления связи после сбоя в маршрутизаторе (минуты). •Протокол не в состоянии отличить различные типы адресов - нет маски.</p>	<p>60. Протокол RIP. Процесс построения таблиц маршрутизации на примере составной сети. Этап 1 - создание минимальной таблицы. •В исходном состоянии на каждом маршрутизаторе обеспечение стека TCP/IP автоматически создаст минимальную таблицу маршрутизации, в которой учитывается только непосредственно подсоединенные подсети. Этап 2 - рассылка минимальной таблицы соседям. •После инициализации каждый маршрутизатор начинает пересылать из всех своих портов сообщения протокола RIP, в которых содержится его минимальная таблица. Этап 3 - получение RIP-сообщений и обработка полученной информации. •После получения аналогичных сообщений от R2 и R3 маршрутизатор R1: запоминает свой порт на который пришло данное сообщение, а также адрес порта маршрутизатора передавшего сообщение. (формирование доп. строк). Затем маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице. Этап 4 - рассылка новой таблицы соседям. После рассмотренные выше процедуры повторяются, только соседям рассылаются уже не минимальные таблицы, а таблицы с данными, полученными от других маршрутизаторов. Этап 5 - получение RIP-сообщений от соседей и обработка полученной информации. Пятый этап повторяет этап 3. Происходит следующая итерация: Маршрутизаторы принимают RIP-сообщения, обрабатывают полученную информацию и на ее основании корректируют свои TM. Правила обработки полученной информации и внесения новых данных в таблицу остаются прежним - запись о новом маршруте к уже известной сети производится в том случае, если метрика нового маршрута меньше метрики имеющегося маршрута. <i>О времени сходимости.</i> Если маршрутизаторы периодически повторяют этапы рассылки и обработки RIP-сообщений, то за конечное время в сети установится корректный режим маршрутизации. Под корректным режимом маршрутизации понимается такое состояние таблицы, когда все подсети достижимы из любой подсети с помощью некоторого маршрута. Если бы маршрутизаторы, их интерфейсы, их линии связи оставались работоспособными, то выше описанный процесс можно делать достаточно редко, например, один раз в день, а не 30 сек как в реальных условиях. Поэтому данное ограничение не позволяет его использовать в крупных сетях. TM передаются в полном объеме независимо от состояния сети.</p>
<p>61. Основные RIP проблемы и их разрешение. RIP-проблемы: •Медленная сходимость. Изменения, произошедшие на одном из участков сети, распространяются очень медленно через остальные сети. Один из методов сокращения этого недостатка - сетчик участков до 15. •Циклические маршруты. В протоколе нет механизмов выявления замкнутых маршрутов (петель). Особенно когда петля затрагивает несколько маршрутизаторов. <i>О разрешении подобных ситуаций:</i> 1. Split horizon (разделение горизонта) - это механизм, препятствующий посылке информации тому маршрутизатору, от которого эта информация получена. Имеет два варианта реализации: а) Информация не посылается тому маршрутизатору от которого она получена; б) Информация посылается тому маршрутизатору, от которого она была получена, но в качестве метрики используется -16; в) Выбор реализации - это право администратора сети. 2. Triggered update (принудительные обновления). Если маршрутизатор получает информацию о изменении конфигурации сети (перестал работать собственный порт, пришло сообщение из-за которого пришлось изменить TM), а то он не ожидает очередного срока пересылки и обновлений, а посылает update через некоторое небольшое случайное время; б) Случайное время выбирается. Чтобы избежать одновременных штормов update-ов в пределах сети, в) Несмотря на то, что задержка посылки крайне мала, возможна ситуация, когда маршрутизатор пересылает уже устаревшую информацию; г) Однако через некоторое время все станет на свое место (TM получает реальную информацию). 3. Замораживание изменений. а) Он связан с введением тайм-аута на принятие новых данных о сети, которая только что стала недоступной. б) Этот тайм-аут предотвращает принятие устаревших сведений о некотором маршруте от тех маршрутизаторов, которые находятся на некотором расстоянии от отказавшей связи и передают устаревшие сведения о ее работоспособности. в) Предполагается, что в течении тайм-аута эти маршрутизаторы вычернут из своих таблиц данный маршрут, т к не получают о нем новых записей и не будут распространять устаревшие</p>	<p>62. Протоколы состояния связей. Основные характеристики и особенности протокола OSPF. При работе протоколов состояния связей каждый маршрутизатор контролирует состояние своих связей с соседями и при изменении состояния (например, при обрыве связи) рассылает сообщение, после получения которого все остальные маршрутизаторы корректируют свои базы данных и пересчитывают маршруты. •В отличие от дистанционно- векторных протоколов протоколы состояния связей создают на каждом маршрутизаторе базу данных, описывающую полный граф сети и позволяющую локально и, следовательно, быстро производить расчёт маршрутов. •Распространенный протокол такого типа, OSPF, базируется на алгоритме SPF (Shortest Path First) поиска кратчайшего пути в графе, предложенном Дейкстрой (E.W.Dijkstra). Протоколы состояния связи существенно сложнее дистанционно-векторных, но обеспечивают более быстрое, оптимальное и корректное вычисление маршрутов. Данные OSPF передаются непосредственно в IP-детаграммах со значением протокола 89. <i>Протокол OSPF</i> (Open Shortest Path First) - это открытый стандарт протоколов маршрутизации, разработанный рабочей группой Internet Engineering Task Force (IETF) для поддержки IP-трафика. (RFC 2328). Протокол состояния канала связи (link-state): другим маршрутизаторам той же иерархии каждые 30 мин. рассылаются объявления о состоянии канала связи (Links State Advertisement – LSA), которые описывают состояние всех своих интерфейсов, метрики и другие параметры. Маршрутизаторы накапливают эту информацию и используют алгоритм Дейкстры (Dijkstra) для расчета кратчайшего пути до каждого узла. Особенности: 1.отсутствие ограничений на размер сети, иерархическая структура сети; 2.несколько маршрутов в сторону одного узла → балансировка трафика; 3.аутентификация; 4.поддержка бесклассовых сетей (VLSM) и агрегации маршрутов; 5.передача обновлений маршрутов с использованием групповых адресов (multicast 224.0.0.5 и 224.0.0.6); 6.работа поверх IP (не UDP/TCP); 7.поддержка маршрутизации с учетом TOS (type-of-service). По сравнению с протоколами на базе векторов</p>	<p>63. Сравнительная характеристика OSPF и RIP. Быстрый рост и расширение современных сетей привели к тому, что протокол RIP достиг пределов своих возможностей. Протокол RIP имеет определенные ограничения, которые могут привести к возникновению проблем в крупных сетях: 1. RIP поддерживает макс 15 переходов. Сеть с более 15 маршрутизаторами рассматривается, как недоступная. 2. RIP не может обрабатывать маски подсети переменной длины (VLSM). 3. Периодически (30 сек.) широковещательные рассылки потребляют значительную долю трафика. Это основная проблема для RIP в крупных сетях. 4. Обмен происходит целыми таблицами, поэтому протокол целыми таблицами, поэтому протокол RIP не применяется в крупных сетях. 5. Конвергенция (согласование всех таблиц маршрутизации) протокола RIP происходит медленно, чем OSPF. В RIP отсутствуют характеристики задержки и стоимости канала. Так в RIP путь с наименьшим числом переходов до места назначения всегда более предпочтителен, даже если более длинный путь обладает меньшими задержками и большей пропускной способностью. RIP-сети должны быть однородными. Понятие областей или границ отсутствует. Нет суммирования маршрутов, а также бесклассовой маршрутизации. В OSPF все вышеперечисленное присутствует.</p>	<p>64. Протокол OSPF. Зоны (области) OSPF. Метрика. Структуризация AS: •Протокол OSPF позволяет разделить AS на пронумерованные области - на сети или множества смежных сетей. Области не должны перекрываться, но не обязаны быть исчерпывающими (некоторые маршрутизаторы могут не принадлежать ни одной области). За пределами области ее топология и детали не видны. •У каждой AS есть магистральная область, называемая областью 0. Все области соединены с магистралью, что позволяет по магистрали попасть из любой области AS в ее любую другую область. Топология магистралей за ее пределами не видна. •У всех маршрутизаторов, принадлежащих к одной области, одинаковая база данных состояний линий и алгоритм выбора кратчайшего пути. Работа маршрутизаторов заключается в расчете кратчайшего пути от себя до всех остальных маршрутизаторов этой области, включая маршрутизатор, соединенный с магистралью, который обязательно должен иметься в области, хотя бы один. Маршрутизатор, соединенный с двумя областями, должен иметь базы данных для каждой области. Кратчайший путь для каждой области вычисляется отдельно. Протокол OSPF обновляет метрику стоимости для отдельного канала на его пропускной способности или скорости. стоимость = 100 000 000 / пропускная способность канала в бит/с. Метрикой для конкретной сети назначения является сумма стоимости всех каналов пути. Если существует несколько путей к сети, предпочтительным является путь с наименьшей стоимостью, и он заносится в таблицу маршрутизации. <i>OSPF : принцип работы:</i> 1. Обнаружение соседних маршрутизаторов; 2.Обмен базами LSDB; 3.Алгоритм поиска первого кратчайшего маршрута (алгоритм Дейкстры). OSPF : обнаружение соседних маршрутизаторов. <i>Проверка базовых настроек, должны совпадать:</i> 1.Маска подсети, адрес подсети; 2.Hello Interval &Dead Interval; 3. Идентификатор зоны 4. Параметры аутентификации. OSPF : обмен базами LSDB. LSDB (Link-State Database) – база данных состояния каналов, используется маршрутизаторами для расчета оптимального маршрута к известной подсети. Эта база данных формируется на основе анонсов состояния каналов (LSA), которыми обмениваются маршрутизаторы.</p>	<p>65. Типы маршрутизаторов OSPF. Типы маршрутизаторов OSPF: •DR (Designated router) – выделенный маршрутизатор; •BDR (Backup Designated router) – резервный выделенный маршрутизатор; •DOthers – все остальные. Наличие в сети DR снижает OSPF-трафик, маршрутизаторы обмениваются анонсами через него. Происходит поддержание LSDB за счет hello- и dead-сообщений. Если происходит изменение топологии, то соседние маршрутизаторы получают анонсы с этими изменениями и синхронизируют свои LSDB. Для построения таблиц маршрутизации запускается алгоритм Дейкстры, на вход подается топологическая таблица, далее выбирается оптимальный маршрут к каждой подсети исходя из общей стоимости к нему, он и устанавливается в таблицу маршрутизации. <i>Состояния маршрутизатора OSPF:</i> •Down – начальное состояние процесса обнаружения соседей. Это состояние указывает на то, что от соседей не была получена своя информация. •Init – состояние, в котором находится маршрутизатор, отправивший своему соседу hello и ожидающий от него ответного hello. •Two-way – при получении ответных hello маршрутизатор должен увидеть в них свой Router ID в списке соседей. Если это так, то он устанавливает отношения и переходит в состояние two-way. •Exstart – маршрутизаторы определяют Master/Slave отношения на основании Router ID. Маршрутизатор с высшим RID становится Master-маршрутизатором, который определяет DD Sequence number, а также первым начинает обмен DD-пакетами. •Exchange – маршрутизаторы посылают друг другу database description пакеты (DD) с информацией о сетях, содержащихся в их собственной LSDB. •Loading – Если маршрутизатор видит, что части маршрутов нет в его базе данных состояния каналов , он посылает сообщение LSR с перечислением тех сетей, по которым он хочет получить дополнительную информацию. Пока маршрутизатор находится в</p>

<p>сведения по сети.</p> <p>Для предотвращения заклинивания пакетов по составным петлям при отказах связей применяют два приема: прием триггерных обновлений и замораживание изменений. Заметим, что проблема с петлей, образующейся между соседями-маршрутизаторами решается с помощью метода расщепления горизонта. <i>Борьба с ложными маршрутами в RIP</i>. RIP не в состоянии полностью справиться с переходными процессами в сети, когда некоторые маршрутизаторы пользуются устаревшей информацией о уже несуществующих маршрутах, в этом случае имеется несколько методов борьбы с этим явлением. Одним из них метод расщепления горизонта. Однако этот метод не работает в тех случаях, когда петли образуются не двумя, а большим числом маршрутизаторов.</p>	<p>расстояния, для протоколов маршрутизации по состоянию канала требуется следующее: 1.более сложный процесс планирования и конфигурации сети; 2.увеличенные ресурсы маршрутизатора; 3.большой объем памяти для хранения большого количества таблиц; 4.более высокая мощность процессора и вычислительная мощность для сложных расчетов маршрутизации.5.Маршрутизаторы, на которых выполняются протоколы OSPF, создают полную карту сети со своей точки обзора. Данная карта позволяет им быстро определять беспетлевые альтернативные маршруты в случае отказа какого-либо сетевого канала. 6.Для определения стоимости канала используется пропускная способность. Канал с более высокой пропускной способностью обеспечивает более низкую стоимость. Конвергенция протокола OSPF. 1.В пределах одной области маршрутизаторы OSPF сообщают информацию о состоянии своих соединений соседним маршрутизаторам (пакет LSA); 2. После получения объявлений LSA с описанием всех каналов в пределах соответствующей области маршрутизатор OSPF использует алгоритм SPF для создания топологической древовидной схемы. 3.Каждый маршрутизатор определяет себя в качестве корневого элемента своего собственного дерева SPF. 4.Начиная от корневого элемента, дерево SPF определяет кратчайший путь к каждому месту назначения и общую стоимость каждого пути; 5.Информация о дереве SPF хранится в базе данных топологии. Маршрутизатор заносит кратчайший путь к каждой сети в таблицу маршрутизации. Работа OSPF основана на обмене между маршрутизаторами следующими типами сообщений: 1.Hello – используется для создания и поддержки таблицы соседних устройств; 2.Пакет описания базы данных DBD – описывает содержимое базы данных состояния каналов; 3.Запрос информации о состоянии каналов (LSR)- запрашивает отдельные фрагменты базы данных состояния каналов маршрутизатора; 4.Обновление состояния каналов (LSU) – передает объявления о состоянии каналов (LSA) соседним маршрутизаторам. 5.Подтверждение получения объявления о состоянии каналов (LSACK) – подтверждает получение LSA от соседнего устройства.</p>			<p>ожидании ответа в виде LSU сообщений, он пребывает в состоянии Loading. *Full — Когда маршрутизатор получил всю информацию и LSDB на обоих маршрутизаторах синхронизирована, оба маршрутизатора переходят в состояние fully adjacent (FULL).</p>
<p>66. Повышение эффективности протокола OSPF. Назначенные Маршрутизаторы (DR и другие). Среди всех маршрутизаторов данной сети выбирается один выделенный маршрутизатор DR (designated router), с которым все остальные маршрутизаторы устанавливают отношения смежности. Соседние маршрутизаторы, не являющиеся смежными, не обмениваются информацией друг с другом. На случай выхода из строя основного DR всегда поддерживается в готовом состоянии запасной назначенный маршрутизатор BDR (Backup designated router). Выбор DR и BDR На роль DR выбирается маршрутизатор с наивысшим приоритетом из всех, объявлявших себя в качестве DR. В случае равных приоритетов выбирается маршрутизатор с большим идентификатором. На роль BDR выбирается маршрутизатор с наивысшим приоритетом из всех, объявлявших себя в качестве BDR, при этом маршрутизаторы, объявлявшие себя в качестве BDR, не рассматриваются. Если никто не объявил себя в качестве BDR, выбирается маршрутизатор с высшим приоритетом из тех, кто не объявил себя в качестве DR. В случае равных приоритетов выбирается маршрутизатор с большим идентификатором.</p>	<p>67. Три механизма выбора DR и BDR. На роль DR выбирается маршрутизатор с наивысшим приоритетом из всех, объявлявших себя в качестве DR. В случае равных приоритетов выбирается маршрутизатор с большим идентификатором. На роль BDR выбирается маршрутизатор с наивысшим приоритетом из всех, объявлявших себя в качестве BDR, при этом маршрутизаторы, объявлявшие себя в качестве BDR, не рассматриваются. Если никто не объявил себя в качестве BDR, выбирается маршрутизатор с высшим приоритетом из тех, кто не объявил себя в качестве DR. В случае равных приоритетов выбирается маршрутизатор с большим идентификатором.</p> <p>В широковещательных сетях множественного доступа, таких как Ethernet, может появиться большое число отношений соседства, поэтому требуется назначать маршрутизатор DR. В сетях типа точка-точка установление отношений полной смежности не представляет сложности, поскольку, по определению, в этих сетях на канале находится только два маршрутизатора. Назначение маршрутизатора DR не является обязательным и не выполняется.</p> <p>В нешироковещательной сети множественного доступа рекомендуется, чтобы администратор выбирал маршрутизатор DR или BDR путем настройки приоритета маршрутизатора. Это обеспечивает наличие у маршрутизатора DR или BDR возможности полной передачи данных на все соседние маршрутизаторы.</p>	<p>68. Протоколы динамической маршрутизации. Внутренние и внешние шлюзовые протоколы. Динамическая маршрутизация - это процесс использования протокола для поиска и обновления таблиц маршрутизации в устройствах. Сетевой шлюз — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы. Автономная система — это совокупность сетей под одним административным управлением, обеспечивающих общую для всех входящих в автономную систему маршрутизаторов политику маршрутизации. Автономные системы соединяются внешними шлюзами (маршрутизаторами). Протоколы маршрутизации, осуществляющие маршрутизацию между автономными системами называют внешними; маршрутизацию внутри автономных систем осуществляют внутренними. Протоколы внутренней маршрутизации используются для определения маршрутов внутри автономной системы. Эти протоколы также называют внутренними или внутри шлюзовыми протоколами. Внутренние шлюзовые протоколы отвечают за маршрут внутри автономной системы. В случае транзитной автономной системы эти протоколы указывают точную последовательность маршрутизаторов от точки входа в автономную систему до точки выхода из нее. Между внешними шлюзами разрешается использовать только один протокол маршрутизации, причем не произвольный, а тот, который в данное время признается сообществом Интернета в качестве стандартного для внешних шлюзов. Такой протокол маршрутизации называется внешним шлюзовым протоколом (EGP, Exterior Gateway Protocol) и в настоящее время им является протокол BGP версии 4 (BGPv4). Все остальные протоколы (RIP, OSPF, IS-IS) являются внутренними шлюзовыми протоколами (IGP, Interior Gateway Protocol). Внешний шлюзовый протокол отвечает за выбор маршрута между автономными системами. В качестве адреса следующего маршрутизатора указывается адрес точки входа в соседнюю автономную систему.</p>	<p>69. Протокол пограничной маршрутизации BGP. BGP - это протокол маршрутизации между автономными системами. Наиболее существенным достижением BGP4 является использование им механизма внутридоменной бесплассовой маршрутизации (CIDR). Он основан на методах маршрутизации, называемых "маршрутизация вектором пути". Путь обычно определяется как упорядоченный список автономных систем, который должен пройти пакет для достижения пункта назначения. Каждый вход в таблицу маршрутизации содержит сетевое назначение, следующий маршрутизатор и путь до пункта назначения, следующий маршрутизатор и путь до пункта назначения. BGP - протокол динамической маршрутизации, в котором описана возможность существования правил (policy), ограничивающих распространение некоторых адресов в объявлениях. Общая схема работы BGP: *BGP-маршрутизаторы соседних AS устанавливают между собой соединения по протоколу TCP (порт 179) и становятся BGP-соседями; *BGP использует подход под названием path vector, являющийся развитием дистанционно-векторного подхода; *BGP-соседи анонсируют друг другу path vectors, которые содержат адрес сети и список атрибутов, описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть. <i>Наиболее важные атрибуты маршрута:</i> AS_PATH — список номеров AS, через кот. должен пройти IP-пакет на пути в указанную сеть. Анонсируя какой-либо маршрут, BGP-маршрутизатор добавляет в AS_PATH номер своей AS. Атрибут AS_PATH можно использовать также для: *нахождения циклов, если номер одной AS встречается в AS_PATH дважды; *вычисления метрики маршрута - метрикой в данном случае является число AS, которые нужно пересечь; *применения маршрутной политики - если AS_PATH содержит номера политически неприемлемых AS, то данный маршрут исключается из рассмотрения. ORIGIN - указывает надежный источник информации о маршруте. NEXT_HOP - указывает адрес следующего BGP-маршрутизатора на пути в заявленную сеть. LOCAL_PREF - используется BGP-маршрутизатором, чтобы сообщить своим BGP-партнерам в своей собственной AS степень предпочтения объявленного маршрута.</p>	<p>70. Протокол BGP (внешний и внутренний). BGP - это протокол маршрутизации между автономными системами. Наиболее существенным достижением BGP4 является использование им механизма внутридоменной бесплассовой маршрутизации (CIDR). Он основан на методах маршрутизации, называемых "маршрутизация вектором пути". Путь обычно определяется как упорядоченный список автономных систем, который должен пройти пакет для достижения пункта назначения. Каждый вход в таблицу маршрутизации содержит сетевое назначение, следующий маршрутизатор и путь до пункта назначения, следующий маршрутизатор и путь до пункта назначения. BGP - протокол динамической маршрутизации, в котором описана возможность существования правил (policy), ограничивающих распространение некоторых адресов в объявлениях. Общая схема работы BGP. BGP-маршрутизаторы соседних AS устанавливают между собой соединения по протоколу TCP (порт 179) и становятся BGP-соседями. BGP использует подход под названием path vector, являющийся развитием дистанционно-векторного подхода. BGP-соседи анонсируют друг другу path vectors, которые содержат адрес сети и список атрибутов, описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть. Протокол BGR может быть внутренним и внешним. Внутренний IBGP — с его помощью информация, полученная сервисом AC распространяется внутри нее. Не является обязательным. Однако система получается более чистой и удобной в управлении.</p>
<p>71. Протоколы транспортного уровня TCP и UDP. Порты и сокет. <i>Протокол TCP (Transmission Control Protocol)</i> потоковый транспортный сервис с надежной доставкой. <i>Протокол UDP (User Datagram Protocol)</i> сервис негарантированной доставки единичных сообщений. * Транспортный уровень принимает из сети пакеты для множества приложений, возникает проблема разобраться, где чьи данные; *Сетевые приложения идентифицируются 16-разрядным числом – портом; одно приложение может использовать несколько портов; * сетевое соединение (между приложениями) однозначно определяется набором параметров: протокол транспортного уровня, порт-ист, ip-ист., порт-назн., ip-назн. Протоколы TCP и UDP ведут для каждого приложения две системные очереди: поступающих и отправляемых данных. <i>Порты (port) и сокеты (socket)</i> Данные, поступающие на транспортный уровень, организованы ОС в виде множества</p>	<p>72. Протоколы транспортного уровня TCP и UDP. Протокол UDP. UserDatagramProtocol, UDP (RFC 768) обеспечивает обмен единичными сообщениями между приложениями. UDP очень прост, это прямая ретрансляция сервиса протокола IP приложениям. UDP - дейтаграммный протокол, не гарантирующий доставку и не сохраняющий порядка следования сообщений. Сообщение протокола UDP называют пользовательской дейтаграммой. <i>Структура заголовка UDP:</i></p>	<p>73. Протоколы транспортного уровня TCP и UDP. Протокол TCP. Протокол TCP предназначен для передачи данных между приложениями. Этот протокол основан на логическом соединении, что позволяет ему обеспечивать гарантированную доставку данных, используя в качестве инструмента ненадежный дейтаграммный сервис протокола IP. Все соединения TCP дуплексные и двучастные. Широковещательная и групповая рассылка протоколом TCP не поддерживается. * Протокол управления передачей данных TCP появляется в начальный период создания КС, когда глобальные сети не отличались своей надежностью. *Самой сильной его стороной явл. именно надежность. *Он диагностирует ошибки, при необходимости посылает данные повторно и сообщает об ошибке на другие уровни, если не может их исправить самостоятельно. <i>Основные функции протокола TCP:</i> 1. Базовая передача данных. TCP</p>	<p>74. Установление логического соединения в протоколе TCP. Основным отличием TCP от UDP является то, что на протокол TCP возложена дополнительная задача - обеспечить надежную доставку сообщений, используя в качестве основы ненадежный дейтаграммный протокол IP. Для решения этой задачи TCP использует метод продвижения данных с установлением логического соединения. TCP является протоколом ориентированным на установление соединения. Это означает, что перед передачей данных должно быть установлено логическое соединение между клиентом и сервером. Логическое соединение дает возможность участникам обмена следить за тем, чтобы данные: не были потеряны; искажены или продублированы; а также чтобы они пришли к получателю (не интерфейсу, а процессу) в том порядке, в котором они были отправлены. Протокол TCP устанавливает логические соединения между прикладными процессами, причем в каждом соединении участвуют только два процесса. Логическое TCP-соединение однозначно идентифицируется</p>	<p>75. Протокол TCP. Окноное управление потоком. Есть 2 метода организации процесса обмена квитанциями:1) Метод с простыми 2) метод скользящего окна. Метод с простыми (Idle Source) требует, чтобы источник, пославший кадр, ожидал получения квитанции (положительной или отрицательной) от приемника и только после этого посылал следующий кадр (или повторял искаженный). Если же квитанция не приходит в течение тайм-аута, то кадр (или квитанция) считается утерянным и его передача повторяется. На рис. 35, а видно, что в этом случае производительность обмена данными существенно снижается, — хотя передатчик и мог бы послать следующий кадр сразу же после отправки предыдущего, он обязан ждать прихода квитанции. Снижение производительности этого метода коррекции особенно заметно на низкоскоростных каналах связи, то</p>

<p>череды в точках входов прикладных процессов – портов. Номера портов разделены на три диапазона: стандартные, зарегистрированные и динамические или частные. Стандартные порты или назначенные (хорошо известные) — это порты в диапазоне от 0 до 1023. Зарегистрированные порты — это порты в диапазоне от 1024 до 49151. Динамические/частные порты — порты в диапазоне от 49152 до 65535. <i>Прикладной интерфейс socket.</i> Наиболее распространенным прикладным интерфейсом для передачи данных по сети является интерфейс socket • socket описывает сетевое соединение как файл ввода-вывода •Номер порта в совокупности с адресом конечного узла однозначно определяют прикладной процесс в сети, который имеет название socket. Socket = {IP-адреса хоста, номер порта}</p>	<div><div><div><div>48</div><div>8</div><div>16</div><div>32 бита</div></div><table><tr><td>Порт отправителя</td><td>Порт получателя</td></tr><tr><td>Длина дейтаграммы</td><td>Контрольная сумма</td></tr><tr><td colspan="2">Данные</td></tr></table><p>Псевдозаголовок UDP. Добавляется к UDP-пакету перед вычислением контрольной суммы. Нужен для проверки корректности доставки. Получателю не пересылается.</p><div><div>Пространство расчета контрольной суммы</div><div><div>Псевдо-заголовок</div><div>заголовок</div><div>сегмент данных</div></div><div><div>IP-адрес отправителя</div><div>IP-адрес получателя</div><div>00000000 00010001</div><div>Длина UDP-пакета</div></div><div><div>Тип протокола</div><div>Без учета псевдозаголовка</div></div></div><p>UDP используется следующими важными протоколами прикладного уровня:•Система доменных имен (DNS); •протокол динамической настройки узла (DHCP); •протокол маршрутной информации (RIP); •упрощенный протокол передачи файлов (TFTP); •онлайн-игры.</p></div></div>	Порт отправителя	Порт получателя	Длина дейтаграммы	Контрольная сумма	Данные		<p>рассматривает информацию, поступающую к нему от прикладных процессов, как неструктурированный поток пронумерованных байтов. Поступающие данные буферизуются средствами TCP. Для передачи на сетевой уровень из буфера “вырезается” некоторая непрерывная часть данных, которая называется сегментом и снабжается заголовком. 2. Обеспечение достоверности. TCP обеспечивает защиту от повреждения,потери, дублирования и нарушения очередности получения данных. Для выполнения этих задач все океты в потоке данных сквозным образом пронумерованы в возрастающем порядке. Для каждого сегмента вычисляется контрольная сумма, позволяющая обнаружить повреждение. нумерация используется для упорядочения и обнаружения дубликатов. 3. Разделение каналов. Протокол TCP обеспечивает работу одновременно нескольких соединений. •Каждый прикладной процесс идентифицируется номером порта. •Заголовок TCP-сегмента содержит номера портов процесса отправителя и процесса-получателя. •Socket уникально идентифицирует прикладной процесс в Интернет. 4. Управление соединением. Соединение - это совокупность информации о состоянии потока данных, включающая socket, номера посланных, принятых и подтвержденных окетов, размеры окон. 5. На протокол TCP - вложена сложная и очень важная задача: обеспечение надежной передачи данных через ненадежную сеть.</p>	<p>парой socketов. Один socket может участвовать в нескольких соединениях. Установление соединения в TCP: 1.Клиент обращается к протоколу TCP, который в ответ на это обращение посылает сегмент-запрос на установление соединения протоколу TCP, работающему на стороне сервера. В числе прочего в запросе содержится флаг SYN, установленный в единице. 2.Получив запрос, модуль TCP на стороне сервера пытается создать “инфраструктуру” для обслуживания нового клиента. Если все было получено и создано, то модуль TCP посылает клиенту сегмент с флагами ACK и SYN. 3. В ответ клиент посылает ACK и переходит в состояние логического соединения ESTABLISHED. Когда сервер получит ACK он также переходит в состояние ESTABLISHED.</p>	<p>есть в территориальных сетях. Второй метод называется методом скользящего окна (sliding window). В этом методе для повышения коэффициента использования линии источнику разрешается передать некоторое количество кадров в непрерывном режиме, то есть в максимально возможном для источника темпе, без получения на эти кадры положительных ответных квитаций. Количество кадров, которые разрешается передавать таким образом, называется размером окна. При отправке пакетов устанавливается тайм-аут ожидания квитации. Метод с простыми является частным случаем метода скользящего окна, когда размер окна равен единице.</p>
Порт отправителя	Порт получателя									
Длина дейтаграммы	Контрольная сумма									
Данные										
<p>76. Прикладной уровень в стеке TCP/IP. На прикладном уровне располагаются программные средства двух видов - приложения и службы. Приложения организуют интерфейс между пользователем и сетью. Службы готовят данные для дальнейшей передачи по сети. Все нижележащие уровни в стеке TCP/IP обеспечивают доставку информации по сети, но никак не связаны с прикладными программами и программированием. Прикладной уровень не занимается доставкой. Он описывает протоколы взаимодействия программ (структуру передаваемой информации и правила ее обработки получателем) и возможную реализацию процедур общения к примитивам TCP. Прикладное ПО (сервера WWW, FTP, электронной почты и соответствующие клиенты), реализованы с учетом протоколов прикладного уровня, т е общающиеся между собой с использованием соответствующих протоколов (HTTP, FTP и т.д.). Примеры протоколов: DNS, HTTP, FTP, SMTP, Telnet. Прикладной уровень объединяет все службы, предоставляемые системой пользовательским приложением. Прикладной уровень реализуется программными системами, построенными в архитектуре клиент-сервер, базирующейся на протоколах нижних уровней. Протоколы прикладного уровня в стеке TCP/IP занимаются деталями конкретного приложения и “не интересуются” способами передачи данных по сети. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам, сравнительно новых служб. Знаковый пример, протокол передачи гипертекстовой информации HTTP (сервера www).</p>	<p>77. Система доменных имен DNS. Основные подходы к разрешению доменных имен. DNS - это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet. На прикладном уровне применяется символическая система адресации. Пространство символической адресации независимо от IP-адресации - проблема разрешения имен – преобразование символического имени в IP-адрес и обратно. Служба DNS предназначена для автоматического поиска IP-адреса по известному символическому имени узла. Для именования компьютеров в больших сетях применяется: •Доменная система имен; •Служба WINS, которая поддерживает систему NetBIOS-имен. <i>Схемы разрешения DNS-имен:</i> 1. Рекурсивная процедура. Клиент обращается с запросом разрешения имени к одному из локальных DNS-серверов. Если искомый домен входит в его сферу ответственности, то он сразу же возвращает клиенту авторитетную запись ресурса. Авторитетной называют запись, получаемую от официального источника. Записи, попадая на сервер имен, кшируются. Авторитетная запись всегда считается верной. Если же домен является удаленным, то локальный DNS-сервер посылает запрос серверу домена верхнего уровня. Ответы также поэтапно передаются обратно. 2. Итеративная процедура. Работу по поиску IP-адреса координирует DNS-клиент. Если после обращения к локальному серверу разрешение не найдено, то он сразу же информирует об этом клиента, сообщая при этом имя следующего сервера, которого можно спросить. Все пространство имен доменов распределено на непересекающиеся зоны. Зона содержит часть общего дерева доменов и обслуживается основным сервером имен, хранящего информацию о ресурсах этой зоны. Для обеспечения надежности в зоне может быть несколько дополнительных серверов имен, которые синхронизируются с основным сервером. Файл зоны содержит стандартные записи ресурсов базы данных DNS для преобразования доменных имен хостов в данной зоне в IP-адреса, определения авторитетных DNS-серверов данной зоны, определения хостов-обработчиков почты для доменных имен в данной зоне и др. Файлы баз данных DNS состоят из стандартных записей ресурсов. <i>Службы имен – DNS. Типы записей.</i> А (адрес) - Содержит отношение имя-адрес. Применяется для прямых зон. Добавляется в случае отсутствия возможности динамического добавления записей. NS (сервер имен) - Определяет список серверов имен, ответственных за данную зону. CNAME (подстановочное имя) - Позволяет добавлять синонимы имен, определенных записями типа А. MX (обработчик почты) - Определяет адрес сервера, на котором установлено приложение доставки почты для данной зоны. SOA (начало зоны) - Определяет начало зоны и важные параметры ее функционирования. PTR (указатель) - Используется в обратных зонах для указания соответствия адреса и имени. SRV (сервис) - Добавляются сервисами для упрощения поиска клиентскими компьютерами. Поддерживаются только динамическим обновлением.</p>	<p>78. Электронная почта. Протоколы электронной почты. Сетевая почтовая служба (электронная почта) – это распределенное приложение, главной функцией которого является предоставление пользователям сети возможности обмениваться электронными сообщениями. Почтовый клиент - программа, помогающая составлять и посылать электронные сообщения, получать и отображать письма на компьютере пользователя. Почтовый сервер программа, пересылающая сообщения из почтовых ящиков на другие серверы или на компьютер пользователя по запросу его почтового клиента. В системе электронной почты на устройствах пользователей установлены клиентские почтовые программы, а на одном или нескольких серверах электронной почты – серверные почтовые программы. •Клиенты считают электронную почту с почтового сервера с помощью одного из двух протоколов: 1.протокол POP. 2. протокол IMAP •Клиенты отправляют электронную почту на почтовый сервер, а почтовые серверы пересылают почту друг другу с помощью простотого протокола пересылки почты (SMTP). <i>Сервер электронной почты.</i> Сервер электронной почты — это компьютер, который может отправлять и принимать электронную почту от имени почтовых клиентов. Примеры распространенных у нас, являются следующие серверы электронной почты: Microsoft Exchange, Sendmail, Eudora Internet Mail Server (EIMS). <i>Протокол SMTP (Simple Mail Transfer Protocol- простой протокол передачи почты).</i> Протокол SMTP обеспечивает как передачу сообщений в адрес одного получателя, так и тиражирование нескольких копий сообщений для передачи в разные адреса. Программы, использующие этот протокол: Outlook Express, Microsoft Mail, Lotus и т.д. По умолчанию TCP- протокол подключен к протоколу SMTP через порт 25. <i>Логика работы протокола SMTP (простейший случай).</i> •После того как, пользователь щелкает на значке, инициирующем отправку сообщения, SMTP-клиент посылает запрос на установление TCP-соединения на порт 25 (это назначенный порт SMTP-сервера). •Если сервер готов, то он посылает свои идентифицирующие данные, в частности свое DNS-имя. •Затем клиент передает серверу адреса (имена) отправителя и получателя. •Если имя получателя соответствует ожидаемому, то после получения адресов сервер дает согласие на установление TCP-соединения, и в рамках этого надежного логического канала происходит передача сообщения. •Используя одно TCP-соединение, клиент может передать несколько сообщений, передавая каждое из них указанием адресов отправителя и получателя. •После завершения передачи TCP- и SMTP-соединения разрываются. POP3 – это простейший протокол для работы пользователя со своим почтовым ящиком. Он позволяет только забрать почту из почтового ящика (на сервере) на компьютер клиента и удалить ее из почтового ящика на сервере. POP3- сервер не отвечает за отправку почты, он работает только как универсальный почтовый ящик для группы пользователей. POP3- протокол подключается к транспортному уровню TCP через 110-й протокол. Протокол IMAP4 (Internet Message Access Protocol, Version4) позволяет клиентам получать доступ и манипулировать сообщениями электронной почты на сервере. Существенным отличием протокола IMAP4 от протокола POP3 является то, что IMAP4 поддерживает работу с системой каталогов (или папок) сообщений. IMAP4 позволяет клиенту создавать, удалять и переименовывать почтовые ящики, проверять наличие новых сообщений и удалять старые. При работе с протоколом TCP, IMAP4 использует 143-й порт.</p>	<p>79. Идентификации сетевых ресурсов. URL, URI, URN. URI (Universal Resource Identifier) – универсальный идентификатор ресурса. (включает имя ресурса, его местоположение и используемый для доступа к ресурсу протокол). URN (Uniform Resource Name) реализует механизмы оптимального поиска документа (ближайшей копии ресурса на узле либо его зеркале). URL (Uniform Resource Locator, местонахождение ресурса) предназначен для идентификации типов, методов и компьютеров, на которых находятся определенные ресурсы, доступные через Интернет. В URL-адресе можно выделить три части. •Тип протокола доступа. Помимо HTTP здесь могут быть указаны и другие протоколы, такие как FTP, telnet... •DNS-имя сервера. Имя сервера, на котором хранится нужная страница. •Путь к объекту. Обычно это составное имя файла (объекта) относительно главного каталога веб-сервера, предлагаемого по умолчанию. Веб-клиент, называемый также браузером, или агентом пользователя веб-службы, представляет собой приложение, которое устанавливается на компьютере конечного пользователя и одной из важных функций которого является поддержание графического пользовательского интерфейса. Веб-сервер — программа, хранящая объекты локально в каталогах компьютера, на кот. она запущена, и обеспечивающая доступ к объектам по URL-адресам. Пример: Apache и Microsoft Internet Information Server. HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста) обеспечивает высокопроизводительный механизм передачи мультимедийной информации независимо от типа представленных данных.</p>	<p>80. WEB-служба. Web-служба - отдельные независимые приложения многократного использования, которые представляют свои функции через Web-интерфейс. Для связи с внешним миром, вместо протокола удаленного вызова процедур, используют протокол HTTP. Web-службы позволяют приложениям или другим Web-службам совместно использовать данные и функции таким способом, при котором не имеет значения, как именно эти приложения выполняются, какую платформу, операционную систему или устройство они используют. •Web-страницы или гипертекстовые документы (html-документы) - это текстовые файлы, размеченные тегами (tags) с помощью языка HTML (HyperText Markup Language). •Язык разметки HTML позволяет форматировать текст веб-страницы, размещать на ней графические объекты, рисунки, вставлять звукозаписи и различные мультимедийные элементы, а также скрипты (JavaScript, VBScript), создавая гипертекстовые ссылки. Особый тип тега, который имеет вид <a href=»...» ... называется гиперссылкой. •Веб-клиент, называемый также браузером, или агентом пользователя веб-службы, представляет собой приложение, которое устанавливается на компьютере конечного пользователя и одной из важных функций которого является поддержание графического пользовательского интерфейса. •Веб-сервер — это программа, хранящая объекты локально в каталогах компьютера, на котором она запущена, и обеспечивающая доступ к этим объектам по URL-адресам. Пример: Apache и Microsoft Internet Information Server. URL (Uniform Resource Locator, местонахождение ресурса) – предназначен для идентификации типов, методов и компьютеров, на которых находятся определенные ресурсы, доступные через Интернет. URI (Universal Resource Identifier) – универсальный идентификатор ресурса. (включает имя ресурса, его местоположение и используемый для доступа к ресурсу протокол). URN (Uniform Resource Name) реализует механизмы оптимального поиска документа (ближайшей копии ресурса на узле), HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста) обеспечивает высокопроизводительный механизм передачи мультимедийной информации независимо от типа представленных данных. Программа-клиент (браузер) устанавливает TCP-соединение с портом 80 сервера, затем посылает запрос. После ответа клиент или сервер закрывают соединение. <i>Статусная линия HTTP-ответа</i> Поясняющие коды: •1xx: Информационные; •2xx: Успешно - Действие/запрос был успешно получен, понят и выполнен; •3xx: Перенаправление - Указывает, какое действие должно быть выполнено, чтобы выполнить запрос; •4xx: Ошибка клиента - Запрос содержит неправильный синтаксис или не может быть выполнен; •5xx: Ошибка сервера - Сервер не может выполнить правильный запрос. Причина, как правило, в авторизации доступа к ресурсу. Status-Code= "200" ; OK "201" ; Created "202" ; Accepted "204" ; No Content "301" ; Moved Permanently "302" ; Moved Temporarily "304" ; Not Modified "400" ; Bad Request "401" ; Unauthorized "403" ; Forbidden "404" ; Not Found "500" ; Internal Server Error "501" ; Not Implemented "502" ; Bad Gateway "503" ; Service Unavailable</p>						

<p>81. Канальный уровень. Подуровни канального уровня. Канальный уровень управляет процедурами, которые обеспечивают установу и поддержание связи между беспроводными устройствами в сети. Канальный уровень разделен на два подуровня: 1. Подуровень MAC-управления доступом к среде. Основные функции подуровня уровня MAC: •Управление доступом к разделяемой среде; •Обеспечение мобильности узлов при наличии нескольких базовых станций; •Обеспечение безопасности, не уступающей безопасности в проводных сетях; •Передача кадров между конечными узлами посредством функций и устройств физического уровня. Подуровень MAC поддерживает два режима коллективного доступа к разделяемой среде: Распределенный режим - DCF (Distributed Coordination Function) является базовым для протоколов 802.11 и может функционировать в беспроводных сетях как в произвольном режиме там и в архитектурном. Централизованный режим - PCF (Point Coordination Function) может применяться в том случае, когда в BSS сети есть станция, выполняющая функции точки доступа. 2. Подуровень управления логическим соединением (LLC). Если уровень MAC специфичен для каждой технологии и отражает различия в методах доступа к разделяемой среде, то Уровень LLC представляет собой обобщение функций разных технологий по обеспечению передачи кадров с различными требованиями надежности и передает данные пользователя и служебные данные между MAC и сетевым уровнем. По стандарту определено три вида услуг: •Услуга LLC1 - без установления соединения и без подтверждения получения данных. Обычно эта процедура используется, когда восстановление данных после ошибок и упорядочивание выполняется протоколами вышележащих уровней, поэтому нет смысла дублировать их на уровне LLC. •Услуга LLC2 - установить логическое соединение перед началом передачи любого блока, если надо выполнить процедуру восстановления после ошибок и упорядочивание потока блоков. •Услуга LLC3 - без установления соединения, но с подтверждением получения данных. Актуален в системах управления промышленности объектами в реальном времени - на лету. Это своего рода компромисс между LLC1 и LLC2. Еще одна функция подуровня LLC - передача пользовательских и служебных данных между MAC и сетевым уровнем.</p>	<p>82. Задачи подуровня LLC в локальных сетях. Подуровень управления логическим соединением (LLC). Если уровень MAC специфичен для каждой технологии и отражает различия в методах доступа к разделяемой среде, то Уровень LLC представляет собой обобщение функций разных технологий по обеспечению передачи кадров с различными требованиями надежности и передает данные пользователя и служебные данные между MAC и сетевым уровнем. По стандарту определено три вида услуг: •Услуга LLC1 - без установления соединения и без подтверждения получения данных. Обычно эта процедура используется, когда восстановление данных после ошибок и упорядочивание выполняется протоколами вышележащих уровней, поэтому нет смысла дублировать их на уровне LLC. •Услуга LLC2 - установить логическое соединение перед началом передачи любого блока, если надо выполнить процедуру восстановления после ошибок и упорядочивание потока блоков. •Услуга LLC3 - без установления соединения, но с подтверждением получения данных. Актуален в системах управления промышленности объектами в реальном времени - на лету. Это своего рода компромисс между LLC1 и LLC2. Еще одна функция подуровня LLC - передача пользовательских и служебных данных между MAC и сетевым уровнем.</p>	<p>83. Методы доступа к разделяемой среде в технологии Ethernet. Цель - нахождение простого и дешевого решения объединения в вычислительную сеть нескольких десятков компьютеров, находящихся в пределах одного здания. Для упрощения и удешевления аппаратных и программных решений разработчики остановились на совместном использовании общей среды передачи данных. Радиоканал определенного диапазона частот естественным образом является общей средой для всех передатчиков, использующих частоты этого диапазона для кодирования данных (т.е. это был беспроводной вариант). Сеть ALOHA работала по методу случайного доступа - когда любой узел мог начать передачу пакета в любой момент времени. Немного позже эта идея разделяемой общей среды была перенесена на проводной вариант технологии LAN. Все ПК присоединялись к сегменту кабеля (коаксиального) по схеме монтажного ИЛИ, поэтому при передаче сигналов одним из передатчиков все приемники получали один и тот же сигнал, как и при использовании радиоволн. А в корпорации IBM разрабатывалась кольцевая технология Token Ring. Физ. топология этих сетей - кольцо, каждый узел соединяется кабелем с двумя соседними узлами, но эти отрезки (сегменты) также являются разделяемыми, т.к. в каждый момент времени только 1 пк может задействовать кольцо для передачи своих пакетов. Технология Ethernet. Ethernet - самый распространенный сегодня стандарт локальных сетей. Это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. Ethernet использует: 1. физические топологии «шина», «звезда» или «звезда-шина»; 2. логическую топологию «шина»; 3. метод случайного доступа к общей среде. Высокоскоростные стандарты: 1. Fast Ethernet (100 мбит/с). 2. Gigabit Ethernet (1 гбит/с). 3. 10g ethernet (10 гбит/с). 4. 40 и 100g ethernet. Дополнительная спецификация среды: 1. 10base5 - толстый коаксиальный кабель. 2. 10 base-t - кабель витая пара. 3. 10base-fl - оптоволокно.</p>	<p>84. Методы доступа к разделяемой среде в кольцевых технологиях локальных сетей. Цель - нахождение простого и дешевого решения объединения в вычислительную сеть нескольких десятков компьютеров, находящихся в пределах одного здания. Для упрощения и удешевления аппаратных и программных решений разработчики остановились на совместном использовании общей среды передачи данных. Радиоканал определенного диапазона частот естественным образом является общей средой для всех передатчиков, использующих частоты этого диапазона для кодирования данных (т.е. это был беспроводной вариант). Сеть ALOHA работала по методу случайного доступа - когда любой узел мог начать передачу пакета в любой момент времени. Немного позже эта идея разделяемой общей среды была перенесена на проводной вариант технологии LAN. Все ПК присоединялись к сегменту кабеля (коаксиального) по схеме монтажного ИЛИ, поэтому при передаче сигналов одним из передатчиков все приемники получали один и тот же сигнал, как и при использовании радиоволн. А в корпорации IBM разрабатывалась кольцевая технология Token Ring. Физ. топология этих сетей - кольцо, каждый узел соединяется кабелем с двумя соседними узлами, но эти отрезки (сегменты) также являются разделяемыми, т.к. в каждый момент времени только 1 пк может задействовать кольцо для передачи своих пакетов.</p>	<p>85. Базовые технологии локальных сетей. Технология Ethernet и ее основные особенности. Сетевые технологии называют базовыми, так как на их основе строится базис любой сети. Сетевая архитектура - это комбинация стандартов, топологий и протоколов, необходимых для создания работоспособной сети. К базовым сетевым технологиям относят: Ethernet, Token Ring, FDDI. Метод доступа - это способ «захвата» передающей среды, способ определения того, какая из рабочих станций сети может следующей использовать ресурсы сети. Каждый метод доступа определяется алгоритмом, используемым сетевым оборудованием для того, чтобы направлять поток сообщений через сеть. Разделяют два типа методов доступа к среде передачи данных: случайный и маркерный. Технология Ethernet. Ethernet - самый распространенный сегодня стандарт локальных сетей. Это сетевой стандарт, основанный на экспериментальной сети Ethernet Network, которую фирма Xerox разработала и реализовала в 1975 году. Ethernet использует: 1. физическую топологию «шина», «звезда» или «звезда-шина»; 2. логическую топологию «шина»; 3. метод случайного доступа к общей среде. Высокоскоростные стандарты: 1. Fast Ethernet (100 мбит/с). 2. Gigabit Ethernet (1 гбит/с). 3. 10g ethernet (10 гбит/с). 4. 40 и 100g ethernet. Дополнительная спецификация среды: 1. 10base5 - толстый коаксиальный кабель. 2. 10 base-t - кабель витая пара. 3. 10base-fl - оптоволокно.</p>						
<p>86. Базовые технологии локальных сетей. Технология Token Ring и ее основные особенности. История развития: •1984 год - первая реализация компанией IBM. •1985 год - стандарт IEEE 802.5. Разрабатывалась как надежная альтернатива Ethernet. Основные положения: «Физическая топология «звезда», логическая топология - «кольцо»; «скорость передачи» 4 и 16 Мбит/с; «соединение неэкранированной и экранированной витой пары»; метод доступа - маркерное кольцо. Маркерный метод доступа к среде: «Станция, имеющая кадры для передачи, при получении свободного маркера удаляет его из кольца. «Если кадр проходит через станцию назначения, то, расписав свой адрес, станция копирует кадр в буфер (устанавливается признак распознавания адреса и копирования). «Кадр отправляется отправителю (подтверждение получения данных). «Передача в кольцо нового маркера. Время владения разделяемой средой в сети Token Ring ограничивается временем удержания маркера THT (token holding time), после истечения которого станция обязана прекратить передачу и передать маркер далее по кольцу. Время удержания маркера 10 мс. В Token Ring существует три различных формата кадров: маркер - специальный кадр, который определяет право доступа станций к общему разделяемому ресурсу; кадр данных - собственно сами данные; прерывающая последовательность - последовательность, которая прерывает всякую передачу в кольце, как маркера, так и кадра.</p> <p>Формат маркера</p> <table><tr><th>SD</th><th>AC</th><th>ED</th></tr><tr><td>J K O K O O O</td><td>P P P T M R R R</td><td>J K I K I U E</td></tr></table> <p>Первое поле - начальный ограничитель (Start Delimiter, SD) Поле SD представляет собой последовательность уникальную последовательность символов магистрального кода: J K O K O O O.</p> <p>Поле AC - управление доступом (Access Control) PPP - биты приоритета. T - бит маркера, M - бит монитора RRR - резервные биты приоритета.</p> <p>Поле - конечный ограничитель (End Delimeter, ED) ED - последнее поле маркера.</p> <p>Управление кольцом используются: активный монитор AM (Active Monitor); резервные мониторы SM (Standby Monitor). Функции AM может выполнять любая станция кольца. Обычно это самая первая станция, включающаяся в кольцо. В любой момент времени в кольце должен быть только один AM. Основа кольцевой сети - концентратор MAU (Multistation Access Unit) или MSAU (Multi-Station Access Unit). Для каждого абонента в составе концентратора применяется специальный блок подключения к магистральной (TCU-Trunk Coupling Unit). Обеспечение отказоустойчивости Token Ring. При обрыве кабеля или отключении концентратора выполняется процедура сворачивания кольца (wrap) - все оставшиеся узлы сохраняют работоспособность, при этом сохраняется даже порядок обхода станций. В случае нарушения кольца в двух или более местах,</p>	SD	AC	ED	J K O K O O O	P P P T M R R R	J K I K I U E	<p>87. Принципы построения локальных сетей на основе технологии FDDI. Технология FDDI - первая технология, использующая в качестве среды передачи данных локальных сетей оптоволоконный кабель. Стандарт FDDI был выпущен ANSI (American National Standards Institute) в 1984 году. В 1986-1988 появились начальные версии стандарта FDDI и первое оборудование - сетевые адаптеры, концентраторы, мосты и маршрутизаторы, поддерживающие этот стандарт. Технология FDDI - Fiber Distributed Data Interface. Технология FDDI во многом основывается на технологии Token Ring, развивая и совершенствуя ее основные идеи. Цели: «Повысить битовую скорость передачи данных до 100 Мб/с. «Повысить отказоустойчивость сети. «Максимально эффективно использовать потенциальную пропускную способность сети. Цель - построение высокоскоростных магистральных каналов связи (backbone) предназначенных для объединения нескольких сегментов локальной сети.</p>  <p>Сеть FDDI строится на основе двух оптоволоконных колец, которые образуют основную и резервную пути передачи данных между узлами сети. В нормальном режиме работы сети данные проходят через все узлы и все участки кабеля только первичного (Primary) кольца. Этот режим назван режимом Thru-«связным» или «транзитным». Вторичное кольцо (Secondary) в этом режиме не используется. В случае какого-либо вида отказа, когда часть первичного кольца не может передавать данные (например, обрыв кабеля или отказ узла), первичное кольцо объединяется со вторичным, вновь образуя единое кольцо. Этот режим работы сети называется Wrap, то есть «свертывание» или «сворачивание» колец. Стандарт FDDI для достижения высокой гибкости сети предусматривает включение в кольцо абонентов двух типов: Абоненты (станции) класса А (абоненты двойного подключения, DAS - Dual-Attachment Stations) подключаются к обоим (внутреннему и внешнему) кольцам сети. Абоненты (станции) класса В (абоненты одностороннего подключения, SAS - Single-Attachment Stations) подключаются только к одному (внешнему) кольцу сети.</p> <p>Варианты связей в случае обрыва волокон.</p>	<p>88. Виртуальные локальные сети (VLAN). Виртуальной локальной сетью (Virtual LAN, VLAN) называется группа узлов, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. VLAN позволяет администратору объединять станции по логической функции, проектной группе или приложению независимо от физического положения пользователей. Виртуальная сеть образует доминион широковещательного трафика, поскольку широковещательный трафик не выходит за пределы соответствующей группы узлов; Объединение устройств в группы (устройства, расположенные в одной VLAN, невидимы для устройств, расположенных в другой VLAN). Передача кадров между разными виртуальными сетями на основании адреса канального уровня невозможна независимо от типа адреса (уникального, группового, широковещательного). Сети VLAN могут быть определены по: «Порту (наиболее частое применение внедрения VLAN, построенной на портах, когда рабочие станции используют протокол DHCP). «MAC-адресу (VLAN, базирующиеся на MAC-адресах, позволяют пользователям находиться в той же VLAN, даже если пользователь перемещается с одного места на другое). «Сетевому адресу (Этот метод может быть очень полезным в ситуации, когда важна безопасность и когда доступ контролируется списками доступа в маршрутизаторах). Характеристики VLAN: «Каждая VLAN функционирует как отдельная локальная сеть. «VLAN может охватывать один или несколько коммутаторов, что позволяет узлам работать так, как если бы они находились в одном сегменте. «Для передачи трафика между VLAN необходимо устройство 3-го уровня. «По умолчанию в качестве VLAN управления применяется VLAN1. «Администраторы используют IP-адрес VLAN управления для удаленной настройки коммутатора. «При создании сети VLAN назначается номер и имя. Номер VLAN - это любое число из диапазона, доступного коммутатору, кроме VLAN1. Именование VLAN считается рекомендуемым методом управления сетью. Идентификация VLAN: «Устройства, подключенные к VLAN, взаимодействуют только с другими устройствами в этой VLAN, при этом устройства могут быть подключены как к одному, так и к разным коммутаторам. «Коммутатор связывает каждый порт с определенным номером VLAN. При приеме кадра на порте коммутатор добавляет идентификатор VLAN (VLAN ID - VID) в кадр Ethernet. «Добавление идентификатора VLAN в кадр Ethernet называется маркировкой кадра. «Самый распространенный стандарт маркировки кадра - IEEE 802.1q. Стандарт 802.1Q, который иногда сокращается до dot1q, подразумевает вставку 4-байтного поля метки в кадр Ethernet. «Размер маркированного кадра Ethernet может достигать 1522 байта. Роли портов коммутатора. Для портов коммутатора можно задать две разные роли. Порт может быть определен как порт доступа или как магистральный порт. Порт доступа. Принадлежит только одной VLAN. Как правило, отдельные</p>	<p>89. Алгоритмы приема и передачи кадра сетевым адаптером (сетевой картой). Прием кадра адаптером (алгоритм): 1) Адаптер принимает из кабеля сигналы. 2) Выделение сигналов на фоне шума. 3) Если данные перед отправкой в кабель подвергались логич. кодир., то в адаптере восстанавливается исходный код. 4) Проверка контрольной суммы кадра. Если она неверна, то кадр отбрасывается. Если верна, то из МАК кадра извлекается кадр ИС и передается протоколу. 5) Кадр ИС помещается в буфер ол-ной памяти. Передача кадра из адаптера в кабель 1) Прием кадра данных LLC через межууровневый интерфейс вместе с адресной информацией мак-уровня. 2) Формирование кадра данных мак-ур, в кот. инкапсул. кадр ИС и заполнение адреса назначения, источника, вычисление контрольной суммы. 3) Выдача адаптером сигналов в кабель.</p>	<p>90. Физический уровень. Физический уровень отвечает за аппаратное обеспечение; определяет физические, механические, электрические характеристики линий связи (тип кабеля, количество разъемов коннектора, назначение каждого разъема и т.д.); описывает топологию сети и определяет метод передачи данных по кабелю (электрический, оптический). В основе всех беспроводных протоколов семейства 802.11 лежит технология улучшения спектра - SS (Spread Spectrum). Эта технология, в первую очередь, позволяет повысить помехоустойчивость кода для сигналов малой мощности. Основная идея этой технологии состоит в том, что для кодирования информационного сигнала при передаче используется более широкий частотный диапазон. Используются две основные технологии улучшения спектра - Прямое последовательное расширение спектра (DSSS, Direct Sequence Spread Spectrum) и Частотное многоканальное расширение спектра (FHSS, Frequency Hopping Spread Spectrum). В DSSS каждый бит данных умножается на псевдослучайную шумоподобную последовательность, называемую чип-последовательностью. Это увеличивает ширину полосы сигнала и делает его менее подверженным воздействию помех и интерференций. Частотное многоканальное расширение спектра (FHSS) передает данные, быстро переключаясь между разными частотами в пределах радиочастотного диапазона. Это делается в соответствии с определенным псевдослучайным порядком, известным как устройство передачи и приема. FHSS помогает уменьшить риск помех и прослушивания, так как сигнал трудно перехватить или нарушить из-за непредсказуемого изменения частоты.</p>
SD	AC	ED								
J K O K O O O	P P P T M R R R	J K I K I U E								

то оно распадается на два или более не связанных между собой работоспособных сегментов. <i>Passtime Token Ring...</i> •High Speed Token-Ring, HSTR - скорость 100 Мбит/с; •Gigabit Token-Ring - скорость 1000 Мбит/с. •Компании, поддерживающие Token-Ring (среди которых IBM, Ollicom, Madge), не намерены отказываться от своей сети, рассматривая ее как достойного конкурента Ethernet. •По сравнению с аппаратурой Ethernet аппарата Token Ring заметно дороже, так как используется более сложный метод управления обменом, поэтому сеть Token Ring не получила столь широкого распространения.	Концентраторы также бывают двойного подключения (DAC – Dual-Attachment Concentrator) и одинарного подключения (SAC – Single-Attachment Concentrator).	устройства, такие как компьютеры и серверы, подключаются к портам такого типа. Магистральный порт. Магистральный порт — это канал типа "точка-точка" между коммутатором и другим сетевым устройством.		
--	---	--	--	--