1**. Основные понятия компьютерных сетей. Цели создания компьютерных сетей. Интерфейсы**.

Компьютерная сеть - это совокупность каналов связи, устройств приёма и передачи данных, коммуникационного оборудования, сетевого ПО для объединения компьютеров и обеспечения передачи данных между ними.

Компьютерная сеть включает

- Компьютеры или абонентские устройства на их основе;
- Коммуникационное оборудование;
- Линии и каналы передачи данных;
- Операционные системы; Сетевые приложения.

Цель объединения компьютеров в сеть – *совместное использование ресурсов*

•периферийных устройств;

•данных, хранящихся в оперативной памяти или на внешних запоминающих устройствах;

•вычислительной мощности.

Для чего нужно создавать компьютерные сети:

- создание, использование информационных систем общего пользования
- совместное использование устройств и каналов связи
- передача данных между устройствами
- организация параллельных вычислений, в т.ч. территориально распределённых.

ИНТЕРФЕЙС - совокупность средств, методов, правил взаимодействия между элементами системы. Бывает физическим и логическим.

Физический интерфейс определяется набором электрических характеристик сигналов и технических параметров кабеля, разъемов.

Линия связи – участок кабеля с разъёмами.

Логический интерфейс (протокол**)** — это набор информационных сообщений определенного формата, которыми обмениваются 2 устройства/программы, а также набор правил, определяющих логику обмена этими сообщениями.

Канал связи - 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.

2. **Проблемы связи нескольких компьютеров. Выбор физической топологии. Структурированная кабельная система**

Топология сети – это способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

Топология сети позволяет увидеть всю ее структуру, сетевые устройства, входящие в сеть, их связь между собой. Выделяют несколько видов топологий: физическую, логическую, информационную и т.д.

По физической топологии связей различают

A. Точка-точка
B. Полносвязную топологию
C. Звезда
D. Кольцо
E. Общая шина
F. Дерево

А также со смешанной топологией.

В основу любой полномасштабной структурированной кабельной системы (СКС) положена древовидная топология, которую иногда также называют структурой иерархической звезды.

(СКС) представляет собой набор коммуникационных элементов: кабелей, разъёмов, коннекторов, кроссовых панелей и шкафов, которые удовлетворяют стандартам и позволяют создавать регулярные, легко расширяемые структуры связей.

Горизонтальные подсистемы соответствуют этажам здания, они соединяют кроссовые шкафы этажа с розетками пользователей. Вертикальные подсистемы соединяют кроссовые шкафы каждого этажа с центральной аппаратной здания. Подсистема кампуса объединяет несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы обычно называется магистралями

Кабельная система должна иметь "прозрачную" и документировано оформленную структуру.

3. Классификации компьютерных сетей

По территориальному признаку:

- Локальные (LAN - Local Area Networks)
- Глобальные (WAN – Wide Area Networks)
- Региональные (городские) (MAN - Metropolitan Area Networks)

По масштабу производственного подразделения:

- Сети отделов (рабочих групп)
- Сети кампусов
- Корпоративные сети.

Одноранговая сеть

- Пользователи выступают сами в роли администраторов
- Для объединения компьютеров в сеть применяется простая кабельная система
- Вопросы защиты не критичны
- Потоки данных невелики
- Компьютер большую часть своих вычислительных ресурсов предоставляет пользователю, сидящему за компьютером.

Сети на основе серверов (serverbased)

Основа – выделенный сервер, аппаратно-ориентирован как сервер

Специализированные серверы:

Файл-серверы и принт-серверы

Серверы приложений

Почтовые серверы

Факс-серверы

Коммуникационные серверы (серверы удалённого доступа)

Локальные сети служат для объединения рабочих станций, периферии, терминалов и других устройств.

Характерными особенностями локальной сети являются

- ограниченные географические пределы;
- обеспечение многим пользователям доступа к среде с высокой пропускной способностью;
- постоянное подключение к локальным сервисам;
- физическое соединение рядом стоящих устройств.

Глобальные сети объединяют компьютеры, находящиеся на больших расстояниях друг от друга: в различных городах, разных странах и на разных континентах. Используют (или могут использовать) не слишком качественные каналы связи и сравнительно низкую скорость передачи.

Региональные или городские сети предназначены для обслуживания территории крупного города. Обладают качественными линиями связи и поддерживают высокие скорости обмена, обеспечивают доступ к глобальным сетям.
Глобальные сети (Internet)
Internet - это неформальное международное сотрудничество автономных взаимодействующих друг с другом сетей.
Это сотрудничество обеспечивает межмашинное взаимодействие на основе добровольного соблюдения открытых протоколов и процедур. (InternetStandards, RFC 1310,2)
По масштабу производственного подразделения различают
Сети отделов. Используются небольшой группой сотрудников (до 100-150), работающих в одном отделе предприятия.
Сети кампусов (Cumpus – студенческий городок)
Корпоративные сети (Enterprise-widenetworks) – сети масштаба предприятия. Объединяют большое число компьютеров на всех территориях отдельного предприятия.
Для корпоративной сети характерны

- масштабность — тысячи пользовательских компьютеров, сотни серверов, огромные объемы хранимых и передаваемых по линиям связи данных, множество разнообразных приложений;
- высокая степень гетерогенности — типы компьютеров, коммуникационного оборудования, операционных систем и приложений различны;
- использование глобальных связей — сети филиалов соединяются с помощью телекоммуникационных средств, в том числе телефонных каналов.

4. Коммутация пакетов и коммутация каналов

Коммутация каналов – образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами.
Каналы соединяются между собой коммутаторами.
В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал. И только после этого можно начинать передавать данные.
Задержка соединения – установление соединения.
Задержка распространения – скорость распространения электромагнитных волн в конкретной физической среде.
Достоинства коммутации каналов:

- Постоянная и известная скорость передачи данных по установленному между конечными узлами каналу.
- Низкий 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 – техника коммутации абонентов для передачи компьютерного трафика:

- Разбиение сообщения пользователя на пакеты.
- Включение в пакет заголовка, содержащего адрес узла назначения и некоторую нумерацию пакета.
- Передача пакетов по сети как независимых блоков.
- Формирование очередей пакетов на коммутаторах пакетной сети для сглаживания пульсации трафика на каналах связи.

Главное отличие пакетных коммутаторов от коммутаторов в сетях с коммутацией каналов состоит в том, что они имеют буферную память для временного хранения пакетов.
Режимы передачи пакетов:

- Дейтаграммная передача.

Коммутатор реализует независимую маршрутизацию каждого пакета; маршрут выбирается в зависимости от состояния сети. Пример – сеть Internet. Метод не гарантирует доставку пакета, доставка происходит с максимальными усилиями (besteffort).

- Передача с установлением логического соединения.

Согласование двумя конечными узлами сети некоторых параметров процесса обмена пакетами – установление логического соединения.

- Передача с установлением виртуального канала.

Основан на частном случае логического соединения, в число параметров которого входит жёстко определенный для всех пакетов маршрут. Коммутатор реализует передачу пакетов по предварительно построенному виртуальному каналу VC (virtualchannel) (динамическому или постоянному)
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.
2. Переменная величина задержки пакетов данных.
3. Возможные потери данных из-за переполнения буферов.

5. Дейтаграммный способ передачи пакетов

Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты продвигаются (передаются от одного узла сети другому) независимо друг от друга на основании одних и тех же правил.
Процедура обработки пакета определяется только значениями параметров, которые он несет в себе, и текущим состоянием сети (например, в зависимости от ее нагрузки пакет может стоять в очереди на обслуживание большее или меньшее время). Однако 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.
Решение о продвижении пакета принимается на основе таблицы коммутации, ставящей в соответствие адресам назначения пакетов информацию, однозначно определяющую следующий по маршруту транзитный (или конечный) узел. В качестве такой информации могут выступать идентификаторы интерфейсов данного коммутатора или адреса входных интерфейсов коммутаторов, следующих по маршруту.

6. Передача с установлением логического соединения

Коммутация пакетов. Это- техника коммутации абонентов для передачи компьютерного трафика: Разбиение сообщения пользователя на пакеты. Включение в пакет заголовка, содержащего адрес узла назначения и некоторую нумерацию пакета. Передача пакетов по сети как независимых информационных блоков. Формирование очередей пакетов на коммутаторах пакетной сети для сглаживания пульсации трафика на каналах связи. Главное отличие пакетных коммутаторов от коммутаторов в сетях с коммутацией каналов состоит в том, что они имеют буферную память для временного хранения пакетов.
Дейтаграммная передача. Коммутатор реализует независимую маршрутизацию каждого пакета; маршрут выбирается в зависимости от состояния сети. Пример – сеть Internet. Метод не гарантирует доставку пакета, доставка происходит с максимальными усилиями (best effort) Передача с установлением логического соединения. Процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами, называется установлением логического соединения

7. Передача с установлением виртуального канала.

Коммутация пакетов. Это- техника коммутации абонентов для передачи компьютерного трафика: Разбиение сообщения пользователя на пакеты.

Включение в пакет заголовка, содержащего адрес узла назначения и некоторую нумерацию пакета. Передача пакетов по сети как независимых информационных блоков. Формирование очередей пакетов на коммутаторах пакетной сети для сглаживания пульсации трафика на каналах связи. Главное отличие пакетных коммутаторов от коммутаторов в сетях с коммутацией каналов состоит в том, что они имеют буферную память для временного хранения пакетов.
Передача с установлением виртуального канала. Основан на частном случае логического соединения, в число параметров которого входит жестко определенный для всех пакетов маршрут. Коммутатор реализует передачу пакетов по предварительно построенному виртуальному каналу VC (virtual channel) (динамическому или постоянному)

8. Многоуровневый подход. Протокол. Межуровневый интерфейс. Стек протоколов.
В основе стандартизации комп. сетей – принцип декомпозиции, т.е. разделения сложных задач на отдельные подзадачи.
Многоуровневый подход: представление исходной задачи в виде множества модулей. Эти модули группируют и упорядочивают по уровням, образующим иерархию.
Протокол – это формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах.
Межуровневый интерфейс, называемый также интерфейсом услуг, определяет набор функций (услуг), которые нижележащий уровень предоставляет вышележащему.
Стек протоколов – иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети.

9. Модель взаимодействия открытых систем (модель OSI), ее назначение и функции каждого уровня.
Открытая система – сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами по стандартным правилам, определяющим формат, содержание и значение принимаемых и отправляемых сообщений.
Модель OSI определяет
•уровни взаимодействия систем в сетях с коммутацией пакетов;
•стандартные названия уровней;
•функции, которые должен выполнять каждый уровень.
Модель OSI не содержит описаний конкретных протоколов и их реализаций.
Уровни OSI (Единица данных):
Прикладной (сообщения), Представления данных (сообщения), Сеансовый (сообщения), Транспортный (сегменты), Сетевой (пакеты), Канальный (кадры), Физический (биты).
Каждый уровень модели OSI имеет свою систему адресации (адресное пространство).
Примеры адресных пространств:
MAC-адреса (канальный уровень);
IP-адреса (сетевой уровень);
номера портов (транспортный уровень).
7. Прикладной уровень – это набор протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры, гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты.
6. Представительный уровень выполняет преобразование данных между устройствами с различными форматами данных, не меняя при этом содержания.
имеет дело с формами представления данных
обеспечивает де- и шифрование данных. (коды ASCII и EBCDIC)
5. Сеансовый уровень – установка и проведение сеансов связи между передающим и принимающим компьютерами, проверка прав доступа взаимодействующих сторон, распознавание их логических имен, установка режима связи (дуплексный или полудуплексный).
4. Транспортный уровень предназначен для оптимизации передачи данных от отправителя к получателю с той степенью надёжности, которая требуется. Основная задача транспортного уровня – это обнаружение и исправление ошибок в сообщениях, пришедших с описанных выше уровней.
1. Переупаковывает информационные сообщения с передающей стороны: длинные -> несколько пакетов, короткие -> один.
2. С принимающей стороны собирает сообщения из пакетов.
3. Сетевой уровень отвечает за адресацию сообщений и преобразование логических адресов и имен в физические адреса канального уровня. Сетевой уровень определяет путь (маршрут) прохождения данных от передающего к принимающему компьютеру. Сообщения сетевого уровня принято называть пакетами (packet). Маршрутизация – главная задача уровня.
2. Канальный уровень упаковывает неструктурированные биты данных с физического уровня в структурированные пакеты (кадры данных). Уровень отвечает за обеспечение безошибочной передачи пакетов. Пакеты содержат исходный адрес и адрес назначения, что позволяет компьютеру извлекать предназначенные ему данные.
1 Физический уровень отвечает за аппаратное обеспечение; определяет физические, механические, электрические характеристики линий связи (тип кабеля, количество разъёмов коннектора, назначение каждого разъёма и т.д.); описывает топологию сети и определяет метод передачи данных по кабелю (электрический, оптический).
При передаче данных от приложения в сеть транспортный, сетевой и канальный уровень последовательно упаковывают (инкапсулируют) данные «внутрь» своего пакета.

10. Сетезависимые и независимые уровни модели OSI. На каких уровнях модели OSI работает сетевое оборудование (компьютеры, концентраторы, коммутаторы, маршрутизаторы).
Физический, канальный и сетевой — являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Прикладной, представительный и сеансовый — являются сетенезависимыми. Ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.
Шлюз (Шлюз приложений, Gateway) Шлюз - аппаратно-программный комплекс: - функционирующий на прикладном уровне модели OSI; - передающий данные между несовместимыми прикладными программами или между сетями, использующими различные протоколы. Маршрутизатор (Router) Маршрутизатор - устройство, обеспечивающее трафик между локальными сетями, имеющими разные сетевые адреса. Маршрутизатор: - функционирует на сетевом уровне модели OSI; - отвечает за выбор маршрута передачи пакетов между узлами. Коммутатор (Switch) - устройство либо программа, осуществляющая выбор одного из возможных вариантов направления передачи данных. Коммутаторы работают на канальном уровне контроля доступа к среде модели OSI. Повторитель (repeater) - повторение сигналов, поступающих на один из его портов, на другой порт. Концентратор(Concentrator); Хаб (Hub) – это многопортовый повторитель. Данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть.

11. Сетезависимые и независимые уровни модели OSI. Место и назначение транспортного уровня в модели OSI.
Физический, канальный и сетевой — являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Прикладной, представительный и сеансовый — являются сетенезависимыми. Ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения 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 непосредственной транспортировки сообщений.

12. Категории IP-адресов. Одноадресные, широковещательные и групповые

Unicast (адресует отдельный сетевой интерфейс)
Broadcast (адресует все интерфейсы заданной подсети)
Multicast (адресует группу интерфейсов, возможно принадлежащих разным подсетям)
Одноадресная рассылка (Unicast)
Адрес одноадресной рассылки чаще всего встречается в сети IP. Пакет с одноадресным получателем предназначен конкретному узлу. Пример: узел с IP-адресом 192.168.1.5 (источник) запрашивает веб-страницу с сервера с IP-адресом 192.168.1.200 (адресат).
Широковещательные адреса (Broadcast)
В пакете широковещательной рассылки содержится IP-адрес получателя, где в отведенной узлу части есть только единицы (1). То есть пакет получат и обработают все узлы локальной сети.
Групповая рассылка (Multicast).
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. Многоадресный MAC-адрес - это особое значение, которое в шестнадцатеричном формате начинается с 01-00-5E.

13. Сетевой уровень как средство построения больших сетей (понятие составной сети). Типы адресов стека TCP/IP.

Недостатки коммутируемой сети
Большое число узлов -> плоская сеть менее эффективна.
Одно из решений проблем больших плоских сетей - создание сетей VLAN
Большие корпоративные сети выигрывают от внедрения модели иерархической сети и соответствующей структуры адресов. Структура иерархической адресации логически делит сети на менее крупные подсети.
Сеть, образованная путём соединения нескольких подсетей разного типа, называется составной сетью.
Подсеть – целостное адресное пространство (в терминах IP-адресов)
IP-адрес – уникальное число, приписываемое сетевому интерфейсу; по IP-адресу находится получатель пакета
Маршрутизатор – устройство с сетевыми интерфейсами, «смотрящими» в разные подсети.
Адресация в IP-сетях
локальные - определяется технологией, с помощью которой построена отдельная сеть, в кот. входит данный узел (MAC-адреса)
сетевые IP-адреса - основной тип адреса, которые используются на сетевом уровне для передачи пакетов между сетями
символьные имена (DNS-имена, NetBIOSимена)
IP-адрес имеет длину 4 байта (32 бита) и состоит из двух логических частей – номера сети и номера узла.
Маска подсети
Сеть можно разделить на неск. частей, инструмент деления – маска
логические деление IP-адреса: адрес сети (подсети), адресное пространство хостов
маска подсети: битовое пространство адреса сети/подсети устанавливается в 1, а адресное пространство хостов – в 0
маска подсети администрируется и используется локально только в данной подсети
Маска подсети – это число, которое используется в паре с IP – адресом; двоичная запись маски содержит последовательность единиц в тех разрядах, которые должны в IP – адресе интерпретироваться как номер сети.
Операция ANDing выполняет побитовую операцию «и» над двумя двоичными числами: ip-адресом хоста и его маской подсети.
Понятие общих и частных IP-адресов
Существующие IP-адреса можно разделить на общие и частные.
Общие адреса, как правило, используются на компьютерах, которые напрямую подключены к сети Интернет.
Компьютеры, которые подключаются только к внутренней локальной сети, используют IP-адреса, которые называются частными или серыми.

14. Классовая адресация в IP-сетях

1. Сеть работает автономно -> назначение IP-адресов произвольно.
2. Диапазоны адресов в стандартах Internet, рекомендуемых для локального применения (частные или серые номера):
класс A – сеть 10.0.0.0; диапазон адресов: 10.0.0.1 -10.255.255.254
класс B – диапазон из 16 номеров сетей: 172.16.0.0 – 172.31.0.0 диапазон адресов:172.16.0.1 -172.31.255.254
класс C – диапазон из 256 сетей: 192.168.0.0 – 192.168.255.0 диапазон адресов:192.168.0.1 – 192.168.255.254
Если сеть является частью глобальной сети Internet, номера сетей назначаются централизованно. Главным органом регистрации глобальных адресов Интернет с 1998 г. является ICANN (Internet Corporation for Assigned Names and Numbers)
Адреса с 169.254.0.1 по 169.254.255.254. Диапазон адресов класса B, зарезервированных для динамического назначения адресов в отсутствие DHCP-сервера. Такая система адресации называется автоматической частной IP-адресацией (Automatic Private IP-Addressing, APIPA) .
Замечание. Адреса из этого диапазона получают рабочие станции, настроенные как DHCP-клиенты, если DHCP-сервер не доступен.

15. Адресация в IP-сетях. О распределение IP-адресов масками одинаковой длины. Привести пример.

Адресация в IP-сетях
1. локальные - определяется технологией, с помощью которой построена отдельная сеть, в кот. входит данный узел (MAC-адреса)
2. сетевые IP-адреса - основной тип адреса, которые используются на сетевом уровне для передачи пакетов между сетями
3. символьные имена (DNS-имена, NetBIOSимена)
IP-адрес имеет длину 4 байта (32 бита) и состоит из двух логических частей – номера сети и номера узла.
Маска подсети
Сеть можно разделить на неск. частей, инструмент деления – маска
логические деление IP-адреса: адрес сети (подсети), адресное пространство хостов
маска подсети: битовое пространство адреса сети/подсети устанавливается в 1, а адресное пространство хостов – в 0
маска подсети администрируется и используется локально только в данной подсети
Маска подсети – это число, которое используется в паре с IP – адресом; двоичная запись маски содержит последовательность единиц в тех разрядах, которые должны в IP – адресе интерпретироваться как номер сети.
Операция ANDing выполняет побитовую операцию «и» над двумя двоичными числами: ip-адресом хоста и его маской подсети.
Понятие общих и частных IP-адресов
Существующие IP-адреса можно разделить на общие и частные.
Общие адреса, как правило, используются на компьютерах, которые напрямую подключены к сети Интернет.
Компьютеры, которые подключаются только к внутренней локальной сети, используют IP-адреса, которые называются частными или серыми.

16. Адресация в IP-сетях. Маски подсети переменной длины. Технология VLSM. (Реализовать следующий пример разбиения сети на подсети: 192.168.2.0/24, разбить на три подсети по 10, 50 и 100 узлов).

Адресация в IP-сетях

1. локальные - определяется технологией, с помощью которой построена отдельная сеть, в кот. входит данный узел (MAC-адреса)
2. сетевые IP-адреса - основной тип адреса, которые используются на сетевом уровне для передачи пакетов между сетями
3. символьные имена (DNS-имена, NetBIOSимена)

IP-адрес имеет длину 4 байта (32 бита) и состоит из двух логических частей – номера сети и номера узла.

Маска подсети

Сеть можно разделить на неск. частей, инструмент деления – маска

логические деление IP-адреса: адрес сети (подсети), адресное пространство хостов

маска подсети: битовое пространство адреса сети/подсети устанавливается в 1, а адресное пространство хостов – в 0

маска подсети администрируется и используется локально только в данной подсети

Маска подсети – это число, которое используется в паре с IP – адресом; двоичная запись маски содержит последовательность единиц в тех разрядах, которые должны в IP – адресе интерпретироваться как номер сети.

Недостатком адресов на основе классов является то, что они обычно предоставляют либо слишком большой, либо слишком маленький диапазон адресов для использования в большинстве ситуаций.

VLSM - технология, которая позволяет сетевому администратору разбивать адресное пространство IP сети на подсети неравных размеров, в отличие от простого разбиения.

Преимущества VLSM:

позволяет 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 (10000001 00101100 00000000 00000000), относящийся классу B. 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

17. Отображение IP-адресов на локальные адреса.

Одной из главных задач, которая ставилась при создании протокола IP, являлось обеспечение совместной согласованной работы в сети, состоящей из подсетей, в общем случае использующих разные сетевые технологии. Непосредственно с решением этой задачи связан уровень межсетевых интерфейсов стека TCP/IP. На этом уровне определяются уже рассмотренные выше спецификации упаковки (инкапсуляции) IP-пакетов в кадры локальных технологий. Кроме этого, уровень межсетевых интерфейсов должен заниматься также крайне важной задачей отображения IP-адресов в локальные адреса.

Для определения локального адреса по IP-адресу используется протокол разрешения адреса (Address Resolution Protocol, ARP). Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети или же протокол глобальной сети (X.25, frame relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивным ARP (Reverse Address Resolution Protocol, RARP) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения.

Работа протокола ARP начинается с просмотра так называемой ARP-таблицы. Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Для каждой сети, подключенной к сетевому адаптеру компьютера или к порту маршрутизатора, строится отдельная ARP-таблица.

18. Способы назначения IP-адресов. Протокол динамического конфигурирования хостов (DHCP).

IP-адреса могут назначаться узлам сети

вручную администратором сети

динамически

Протокол DHCP (Dynamic Host Configuration Protocol)

Способы назначения адресов:

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и 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).

Описание протокола

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 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-acknowlegment (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.
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.

19. Протокол межсетевого взаимодействия (IP).
Протокол межсетевого взаимодействия (InternetProtocol, IP)
Обеспечивает передачу дейтаграмм от отправителя к получателям через объединенную систему компьютерных сетей (между сетями).
Не устанавливает соединение.
Не даёт гарантии доставки и сохранения порядка доставки.
Обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами.
Способен выполнять динамическую фрагментацию пакетов при передаче их между сетями с различным максимальным размером кадра.
структура:

20. Формат IP-пакета. Краткий обзор основных полей заголовка IP-пакета.

21. Фрагментация IP-пакетов. Характеристика MTU.
Важной особенностью протокола IP, отличающей его от других сетевых протоколов, является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными максимально допустимыми значениями длины поля данных кадров (Maximum Transmission Unit, MTU). Значения MTU зависят как от протокола, так и от настройки сетевых интерфейсов.
Фрагментация в узле-отправителе.
Деление сообщения на части внутри одного и того же стека внутри компьютера. Протоколы верхнего уровня анализируют технологию нижнего уровня и определяют её MTU.
Фрагментация сообщений в транзитных узлах.
Передача пакета из сети с большим в сеть с меньшим MTU. Эти функции выполняет протокол IP.
Идентификатор пакета используется для распознавания пакетов, образовавшихся при делении на части исходного пакета. Все части одного пакета должны иметь одинаковое значение этого поля.
Поле смещения фрагмента предоставляет получателю информацию о положении фрагмента относительно начала поля данных исходного нефрагментированного пакета. Так, например, первый фрагмент будет иметь в поле смещения нулевое значение. В пакете, не разбитом на фрагменты, поле смещения также имеет нулевое значение. Смещение задается в байтах и должно быть кратно 8 байт.
Флаги: 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. Задает уникальное значение поля Идентификатор пакета.
3. Устанавливаются флаги - признаки, связанные с фрагментацией:
D (DonotFragment) - запрет фрагментирования
M (MoreFragments) - данный пакет является промежуточным
4. Смещение фрагмента (13 бит) - смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета
Получатель:
1. При приходе первого фрагмента получатель запускает таймер, определяющий максимальное допустимое время ожидания прихода остальных фрагментов – максимальное из двух значений:
начальное установочное время
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.

22. ICMP-протокол межсетевых управляющих сообщений.
ICMP (Internet Control Message Protocol — протокол межсетевых управляющих сообщений) - этот протокол является вспомогательным сетевым протоколом, включенным в стек протоколов TCP/IP.
Как уже сообщалось ранее, 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 – протоколы верхних уровней, в частности протокол TCP (транспортный уровень) и DNS (прикладном уровне).
Помимо этого, существует еще один механизм уменьшения ненадежной передачи сообщений протоколом IP – это 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.

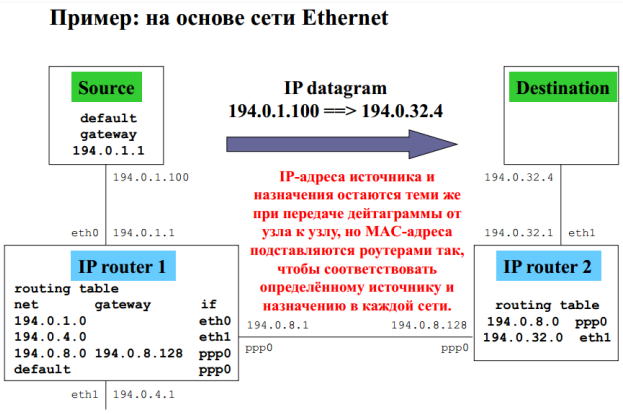
Когда протокол IP определяет, что дальнейшая передача пакета невозможно, перед тем как уничтожить пакет, должен отослать узлу-источнику диагностическое ICMP-сообщение. Если при передаче самого ICMP-сообщения возникла ситуация препятствующая его передачу, то протокол ICMP не будет отправлять об этом диагностическое сообщения, для избегания «штормов» в сетях.
При передаче по сети, сообщения ICMP инкапсулируются в поле данных IP-пакетов.

23. Маршрутизирующие протоколы и протоколы маршрутизации.

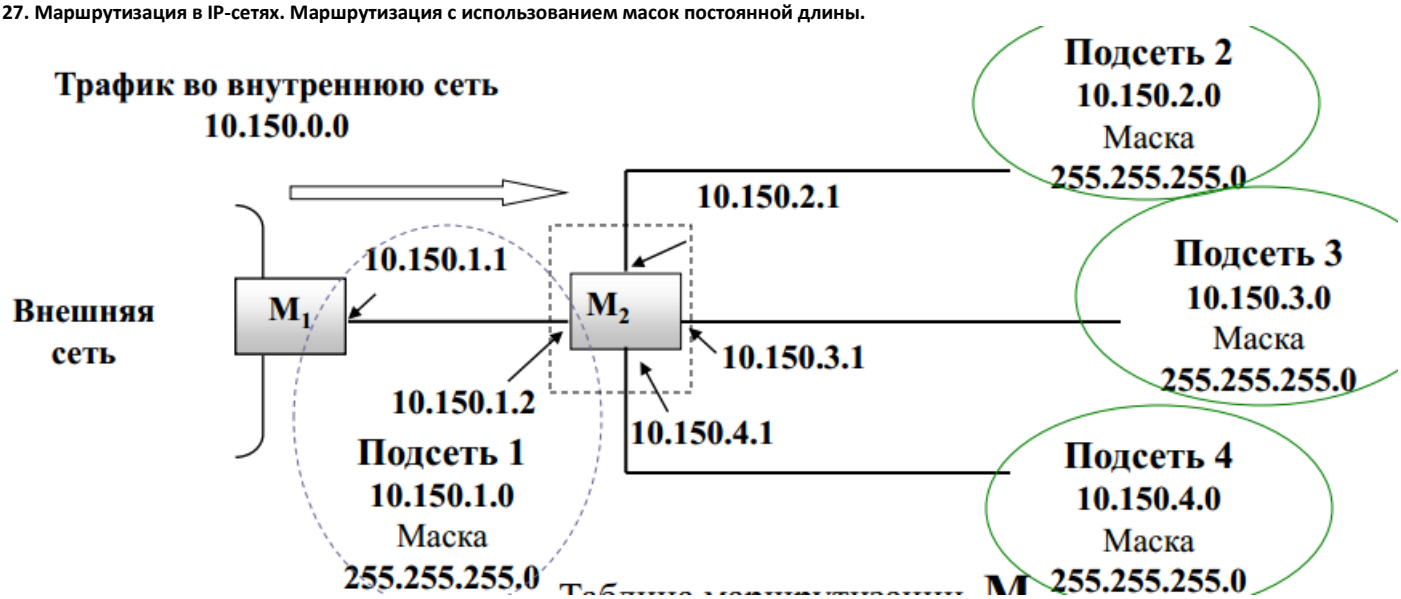
24. Принцип одношаговой маршрутизации.
Существует два подхода к выбору маршрута:
1)одношаговый подход;
2)маршрутизация от источника.
Согласно методу одношаговой маршрутизации каждый маршрутизатор и конечный узел принимает участие в выборе только одного шага передачи дейтаграммы. В каждой строке таблицы маршрутизации указывается не весь маршрут (в виде последовательности IP-адресов маршрутизаторов, через которые должна пройти дейтаграмма), а только один IP-адрес следующего маршрутизатора (маршрутизатора на том пути, по которому нужно передать дейтаграмму). Вместе с дейтаграммой этому маршрутизатору передается и ответственность за выбор следующего шага. Такой подход распределяет задачу выбора маршрута и снимает ограничение на максимальное количество маршрутизаторов в пути. Кроме того, за счет использования маршрутизатора по умолчанию (который обычно занимает в таблице маршрутизации последнюю строку) существенно сокращается объем таблицы. Все дейтаграммы, номера сетей которых отсутствуют в таблице маршрутизации, передаются маршрутизатору по умолчанию. Подразумевается, что маршрутизатор по умолчанию передает дейтаграмму в магистральную сеть, а маршрутизаторы, подключенные к магистральной сети, имеют полную информации о ее топологии.

25. Источники и типы записей в ТМ (таблица маршрутизации)
Обобщенная структура ТМ Номер Сети назначения , Сетевой адрес следующего маршрутизатора Сетевой адрес выходного порта маршрутизатора, Метрика маршрута – расстояние до сети назначения. Метрика: число участков маршрута; административные накладные расходы; полоса пропускания; скорость переда-чи; вероятность задержек; надежность. Расстояние для сетей, непосредственно подключенных к портам маршрутизатора, принимается равным 0, однако в некоторых реализациях отсчет расстояний начинается с 1.
1) программное обеспечение стека TCP/IP (протокол ICMP), создающее минимальную ТМ, содержащую записи о непосредственно подключенных сетях, маршрутизаторах по умолчанию, адресах особого назначения. В Windows запись, соответствующая маршрутизатору по умолчанию имеет значение Network Address = 0.0.0.0 и Netmask = 0.0.0.0, а в Linux – Destination = default. Примером записей об адресах особого назначения является записи 127.0.0.0 (loopback) и 224.0.0.0 (multicast)
2) администратор, непосредственно формирующий записи с помощью системных утилит (route). Заданные вручную записи являются статическими и не имеют срока истечения жизни
3) протоколы маршрутизации, работающие на основе адаптивных алгоритмов (RIP или OSPF). Такие записи всегда являются динамическими, т.е. имеют ограниченный срок жизни

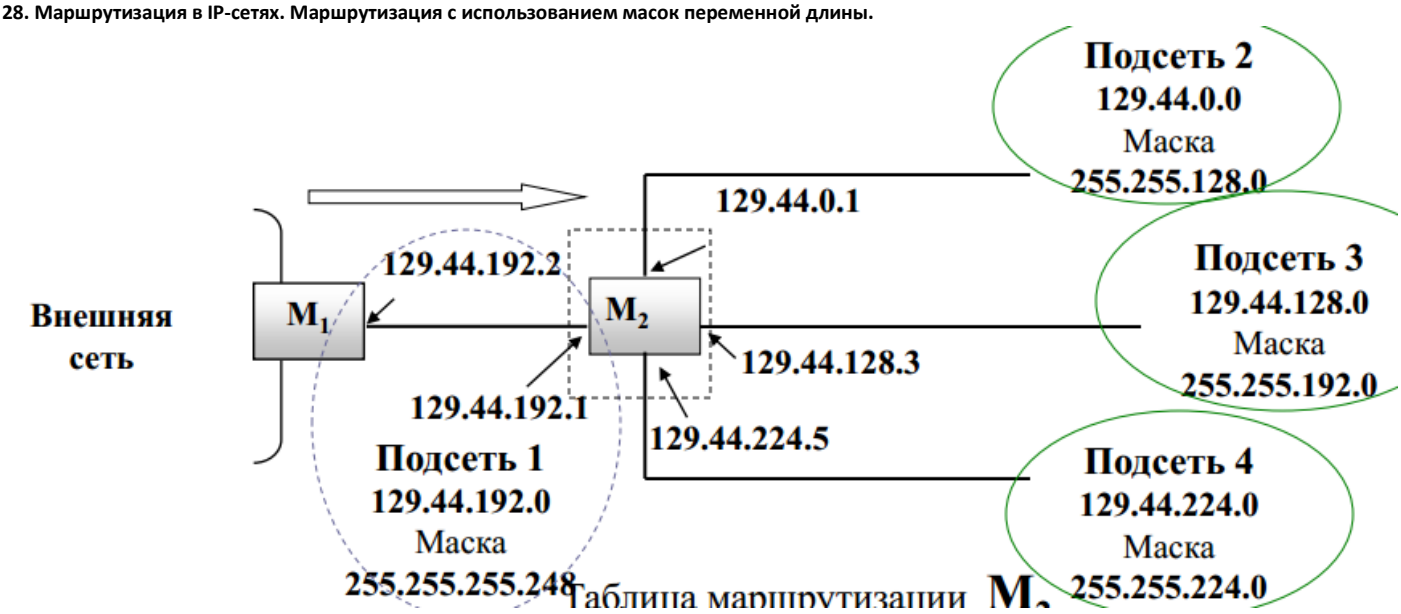
26. Маршрутизация в IP-сетях. Маршрутизация без масок на основе классов
Маршрутизация – выбор пути передачи пакетов между двумя конечными узлами в составной сети.
Задача маршрутизации состоит в выборе маршрута для передачи от отправителя к получателю.
Основные цели маршрутизации:
обеспечение минимальной задержки пакета при его передаче от отправителя к получателю;
обеспечение максимальной пропускной способности сети;
обеспечение максимальной защиты пакета от угроз безопасности содержащейся в нем информации;
обеспечение надежности доставки пакета адресату;
обеспечение min стоимости передачи пакета адресату.
Методы маршрутизации
Простая маршрутизация - маршрутизация, при которой выбор маршрута не зависит от изменения топологии сети, ее состояния (нагрузки).
Преимущества — простота реализации алгоритма маршрутизации и обеспечение устойчивой работы сети при выходе из строя отдельных ее элементов.
Фиксированная маршрутизация. Характеризуется тем, что при выборе маршрута учитывается изменение топологии сети и не учитывается изменение ее нагрузки.
Адаптивная маршрутизация отличается тем, что принятие решения о направлении передачи пакетов осуществляется с учетом изменения как топологии, так и нагрузки сети.
Задачу выбора маршрута решают маршрутизаторы, а также конечные узлы на основе таблицы маршрутизации



27. Маршрутизация в IP-сетях. Маршрутизация с использованием масок постоянной длины.



28. Маршрутизация в IP-сетях. Маршрутизация с использованием масок переменной длины.



29. Технология агрегирования адресов (CIDR).

Технология бесклассовой междоменной 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 привёл 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 n старших двоичных разрядов IP-адреса.

Поле для адресации 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.

Необх. усл. эффективного использования CIDR – локализация адресов, то есть назначение адресов, имеющих совпадающие префиксы, сетям, располагающимся территориально по соседству. Только в таком случае трафик может быть агрегирован.

30. Трансляция сетевых адресов Network Address Translation (NAT)

Основная причина использования NAT – дефицит IP.

Традиционная технология NAT позволяет узлам из частной сети прозрачным для пользователей образом получать доступ к узлам внешних сетей.

Традиционная технология NAT подразделяется на технологии

Базовой трансляции сетевых адресов (Basic NAT)

Трансляции сетевых адресов и портов (Network Address Port Translation, NAPT)
Basic NAT- для отображения используются только IP-адреса
Статические преобразования гарантируют, что частный IP-адрес отдельного узла 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 узла. 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.

31. Трансляция адресов и номеров портов. (Network Address Port Translation - NAPT).
NAPT (Network Address Port Translation) – привлекаются дополнительно транспортные идентификаторы (порты)
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 NAPT.
В режиме NAPT шлюз преобразует адрес локального источника и номер порта из пакета в один глобальный IP-адрес и уникальный номер порта выше 1024.

32. Классификация алгоритмов маршрутизации
Методы маршрутизации
Простая маршрутизация - маршрутизация, при которой выбор маршрута не зависит от изменения топологии сети, ее состояния (нагрузки).
Преимущества — простота реализации алгоритма маршрутизации и обеспечение устойчивой работы сети при выходе из строя отдельных ее элементов.
Фиксированная маршрутизация. Характеризуется тем, что при выборе маршрута учитывается изменение топологии сети и не учитывается изменение ее нагрузки.
Адаптивная маршрутизация отличается тем, что принятие решения о направлении передачи пакетов осуществляется с учетом изменения как топологии, так и нагрузки сети.
Задачу выбора маршрута решают маршрутизаторы, а также конечные узлы на основе таблицы маршрутизации

33. Статическая маршрутизация
Маршрутизатор – специализированный компьютер с множеством сетевых карт, заточенный на обеспечении функционирования компьютерной сети.
Стати́ческая маршрутиза́ция — вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.
При установке статического маршрута указывается:
Адрес сети (на которую маршрутизируется трафик), маска сети (адрес подсети)
Адрес шлюза (узла), который способствует дальнейшей маршрутизации (или подключен к маршрутизируемой сети напрямую)
(опционально) метрика (иногда именуется также «ценой») маршрута. При наличии нескольких маршрутов на одну и ту же сеть некоторые маршрутизаторы выбирают маршрут с минимальной метрикой
Процесс можно автоматизировать, применив протокол DHCP
Достоинства
Лёгкость отладки и конфигурирования в малых сетях.
Отсутствие дополнительных накладных расходов (из-за отсутствия протоколов маршрутизации)
Мгновенная готовность (не требуется интервал для конфигурирования/подстройки)
Низкая нагрузка на процессор маршрутизатора
Предсказуемость в каждый момент времени
Недостатки:
Очень плохое масштабирование (добавление (N+1)-ой сети потребует сделать 2*(N+1) записей о маршрутах, причём на большинстве маршрутизаторов таблица маршрутов будет различной, при N>3-4 процесс конфигурирования становится весьма трудоёмким).
Низкая устойчивость в ситуациях, когда обрыв происходит между устройствами второго уровня и порт маршрутизатора не получает статус down.
Отсутствие динамического балансирования нагрузки
Необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.
В реальных условиях статическая маршрутизация используется в условиях наличия шлюза по умолчанию (узла, обладающего связностью с остальными узлами) и 1-2 сетями. Помимо этого статическая маршрутизация используется для «выравнивания» работы маршрутизирующих протоколов в условиях наличия туннеля (для того, чтобы маршрутизация трафика, создаваемого туннелем, не производилась через сам туннель).

34. Алгоритмы маршрутизации. Динамические алгоритмы маршрутизации.
Алгоритм маршрутизации – набор правил, регламентирующих процедуры обмена служебной информацией между маршрутизаторами с целью заполнения их таблиц. Существует 3 вида: алгоритм фиксированной (статической) м-ии ,адаптивной (включает в себя дистанционно векторные алгоритмы и алгоритмы состояния связей) и простой (случайная м-я, лавинная и маршр-я по предыдущему опыту).
Алгоритмы адаптивной мар-ии == динамические алгоритмы м-ии. Они отличаются от статических источником получения информации. Такими источники могут быть локальными (соседние м-ры), глобальные (все м-ры сети), моментами изменения маршрутов (при изменении топологии или нагрузки) и данными, использующимися для оптимизации (расстояние, кол-во транзитных участков, время пересылки)

35. Дистанционно-векторные алгоритмы (DVA).
DVA алгоритм является адаптивным алгоритмом мар-ии. В DVA алгоритмах каждый маршрутизатор периодически и широковещательно рассылает по сети вектор расстояний (метрик) от самого себя до известных ему подсетей. В качестве метрики обычно исп-т количество промежуточных маршрутизаторов. Маршрут с минимальной метрикой считается оптимальным. Получив такой вектор от соседа-маршрутизатора каждый маршрутизатор добавляет свои сведения обо всех известных ему подсетях и снова рассылает обновлённый вектор. При передаче пакетов из альтернативных маршрутов выбирается маршрут с наименьшей метрикой. В конце концов каждый марш-р получит инф-ю обо всех подсетях, входящих в составную сеть, а также расстояния до них.
Этот алгоритм хорошо работает только в небольших сетях.

36. Алгоритмы состояния связей (LSA).
Алгоритмы состояния связей LSA являются адаптивными алгоритмами маршрутизации. LSA обеспечивает каждый марш-р информацией, достаточной для построения точного графа связей составленной сети. Все марш-ры работают на основании одного и того же графа. Т.е. сеть рассматривается как граф, при этом маршр-торы являются узлами, а физические линии между маршр-ми – рёбрами соответствующего графа. А каждому ребру

присваивается определённое число – стоимость зависящая от физ длины линии, скорости передачи данных или стоимости линии др. характеристик. В обычном режиме маршр-ры обмениваются короткими пакетами со своими близкими соседями.

37. Протокол маршрутной информации RIP

Протокол RIP работает по дистанционно-векторному алгоритму. Является одним из первых внутренних алгоритмов маршр-ии и относится к дистанционно-векторным протоколам. Существует 2 версии RIP. Первая использует маршр-р на основе классов (т.е. без масок подсетей), а вторая исп-т безклассовую маршрутизаци (позволяется работать с масками подсетей). Вторая версия в большей степени соответствует требований сегодняшнего дня.

Кроме того, в дополнение широковещательному режиму RIP поддерживает мультикастинг – специальная форма широковещания, при которой копии пакетов направляются определённому подмножеству адресатов.

Протокол РИП не может быть использован в IP-сети любого размера и сложности (есть ограничения на максимальный диаметр сети, равный 15 маршрутизаторов, ибо маршрут с метрикой 16 считается недостижимым).Т.е. РИП не подходит для больших сетей.

Характеристики RIP: дистанционно-векторный протокол внутренней марш-ии, использует число участков маршрута в качестве метрики для выбора маршрута, относит метрики выше 15 к недостижимым. Преимущество вычислительная простота, а недостатки – неоптимальность найденного маршр-та и увеличение трафика при рассылке широков-х пакетов.

38. Основные RIP проблемы и их разрешение.

1. Медленная скорость (изменения, которые произошли на одном из участков сети, распространяются очень медленно через остальные сети) 2. Циклические маршруты (в RIP нет механизмов выявления замкнутых маршрутов – петель, особенно, когда петля затрагивает несколько маршр-в).

Разрешение подобных ситуаций: Split horizon (разделение горизонта) – механизм, препятствующий посылке информации тому маршр-ру, от которого эта информация получена. Имеет 2 варианта реализации: инф-я не посылается тому маршр-ру, от которого получена, или инф-я посылается к этому маршруту с метрикой -16.

Triggered update (принудительные обновления): если маршрутизатор получает информацию о изменении конфигурации сети (к примеру, пришлось изменить ТМ), то он не ждёт пересылки обновлений, а посылает update через некоторое случайное время (но может случится ситуация, когда маршр-р перешлёт уже устаревшую инф-ю, хоть и задержка посылки крайне мала, но через некоторое время всё станет на свое место и ТМ получит реальную инфу).

Замораживание изменений – связан с введением тайм-аута, который предотвращает принятие устаревших сведений о некотором маршруте от тех маршрутизаторов, которые находятся на некотором расстоянии от октазавшей связи и передают устаревшие сведения о её работоспособности.

39. Особенности протокола OSPF

Протокол OSPF – внутренний шлюзовый протокол, предназначенный для расспространения данных маршрутизации внутри одной автономной системы (и не только). Может использоваться как протокол внешнего шлюза, но в таком случае он будет вычислять маршрут только до входных маршрутизаторов.

Основан на технологии отслеживания состояния канала, которая является отступлением от векторных алгоритмов (которые, к примеру, использовались в RIP).

Особенности: отсутствие ограничений на размер сети, иерархическая структура сети (3 тима маршрутизаторов: внутриобластные, межобластные и между AS), выравнивание нагрузки (когда несколько маршрутов направлены в сторону узла), аутентификация маршрутизации на основе паролей. Также он работает с бесклассовыми сетями. Не применим в классовых сетях.

40. 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 max 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 отсутствует 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.

41. Области (зоны) протокола OSPF. Типы маршрутизаторов.

Число маршрутизаторов автономной системы, использующих протокол OSPF для обмена маршрутной информацией может быть велико. Следствием этого является высокая загрузка каналов связи из-за большого объёма служебных сообщений OSPF. Для снижения объема передаваемой служебной информации, в протоколе OSPF предусмотрено деление автономной системы на области. Каждая из областей имеет 32-битный идентификатор. Принадлежность к области является характеристикой интерфейса, а не устройства. Таким образом, один маршрутизатор может быть подключен к нескольким областям. За областью с идентификатором 0.0.0.0 (область 0) зарезервирована специальная роль – такую область называют магистральной. Наличие магистральной области является обязательным условием для работы протокола OSPF. Каждая из областей должна быть непосредственно подключена к магистральной области, т.е. схема, в которой одна из областей подключена к другой, не имея соединения с магистральной, запрещена.

В зависимости от места маршрутизатора в схеме сети выделяют следующие типы устройств:

1) Внутренний маршрутизатор – маршрутизатор, все интерфейсы которого ассоциированы с одной областью.
2) Магистральный маршрутизатор – маршрутизатор, обладающий интерфейсом, подключенным к магистральной области.
3) Пограничный маршрутизатор области – маршрутизатор, интерфейсы которого ассоциированы с разными областями OSPF.
4) Пограничный маршрутизатор автономной системы – маршрутизатор, имеющий подключение к внешней сети.

42. Области (зоны) протокола OSPF. Область 0.

Число маршрутизаторов автономной системы, использующих протокол OSPF для обмена маршрутной информацией может быть велико. Следствием этого является высокая загрузка каналов связи из-за большого объёма служебных сообщений OSPF. Для снижения объема передаваемой служебной информации, в протоколе OSPF предусмотрено деление автономной системы на области. Каждая из областей имеет 32-битный идентификатор. Принадлежность к области является характеристикой интерфейса, а не устройства. Таким образом, один маршрутизатор может быть подключен к нескольким областям. За областью с идентификатором 0.0.0.0 (область 0) зарезервирована специальная роль – такую область называют магистральной. Наличие магистральной области является обязательным условием для работы протокола OSPF. Каждая из областей должна быть непосредственно подключена к магистральной области, т.е. схема, в которой одна из областей подключена к другой, не имея соединения с магистральной, запрещена.

OSPF имеет особые правила при использовании нескольких областей. Среди нескольких областей одна из них должна быть областью 0, которая называется область магистраль. Если в AS одна область, то это будет область 0. Магистраль (область магистраль) должна быть в центре других областей, то есть все другие области должны быть физически подключены к магистрали. Конфигурация типа звезда. Это означает, что OSPF ожидает от всех областей ввода маршрутной информации в магистраль, которая в свою очередь распространяет эту информацию в другие области.

43. Протокол OSPF. Установление соседства. HELLO-сообщения

Сосед/соседи – это два маршрутизатора, которые находятся в одной канальной среде. На интерфейсах этих маршрутизаторов, смотрящих друг на друга, должен быть включен и правильно настроен OSPF, то есть настройки должны быть консистентные с обеих сторон.

Отношение соседства – маршрутизаторы в OSPF должны постоянно синхронизировать свои базы данных, в которых хранится информации о сети, если два маршрутизатора нормально обмениваются такой информацией, то можно сказать, что они имеют соседские отношения.

Hello-протокол – для поиска соседей, установления соседства, а также для поддержки соседских отношений маршрутизаторы используют hello-пакеты.

Базы данных соседей – маршрутизатор должен знать всех своих соседей, чтобы в случае чего сделать запрос и, чтобы что-нибудь уточнить или что-нибудь сообщить своим соседям, например, если появилась новая сеть. Для этих целей у маршрутизаторов есть список соседей.

Задача HELLO-протокола – обнаружение соседей и установление с ними отношений смежности. Смежность - это продвинутая форма соседских отношений между маршрутизаторами, желающими обмениваться информацией о маршрутизации. При инициации маршрутизаторами отношения смежности с соседними маршрутизаторами начинается обмен обновлениями информации о состоянии каналов. Маршрутизаторы достигают состояния смежности FULL (полное), когда они имеют синхронизированные данные в своей базе данных состояний каналов. Соседями называются OSPF-маршрутизаторы, подключенные к одной сети (к одной линии связи) и обменивающиеся HELLO-сообщениями. Рассылка HELLO-сообщений осуществляется по групповому адресу 224.0.0.5, который присваивается всем маршрутизаторам OSPF-системы. С помощью получаемых ответов каждый маршрутизатор строит базу данных для хранения сведений о смежных маршрутизаторах AdB (Adjacency Data Base). Задача протокола HELLO - выборы DR и BDR маршрутизаторов на основании имеющихся у него данных о соседях, с которыми установлена двусторонняя связь и, приоритет которых не равен нулю.

44. Повышение эффективности протокола OSPF. Назначенные маршрутизаторы.

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, объявивших себя в качестве DR. В случае равных приоритетов выбирается маршрутизатор с большим идентификатором. На роль BDR выбирается маршрутизатор с наивысшим приоритетом из всех, объявивших себя в качестве BDR, при этом маршрутизаторы, объявившие себя в качестве DR, 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.

45. Маршрутизация в неоднородных сетях. Взаимодействие протоколов маршрутизации

Протокол пограничной маршрутизации (BGP — Border Gateway Protocol) BGP — это протокол маршрутизации между автономными системами. Наиболее существенным достижением протокола BGP4 является использование им механизма внутридоменной бесклассовой маршрутизации (Classless InterDomain Routing — CIDR) и поддержке IPv6. (BGP – протокол динамической маршрутизации, в котором описана возможность существования правил (policy), ограничивающих распространение некоторых адресов в объявлениях.) Особенности BGP: • Позволяет осуществлять настройку политики маршрутизации (различать пользователей). • Распространяет информацию о достижимости (расположенных внутри автономной системы получателях). • Относится одновременно к дистанционно-векторным протоколам и протоколам на основе состояния соединения. • Контролирует взаимодействие одноранговых маршрутизаторов для исключения рассылки противоречивой информации. BGP-маршрутизаторы соседних AS устанавливают между собой соединения по протоколу TCP (порт 179) и становятся BGP-партнерами (BGP-peers). BGP-партнеры анонсируют друг другу path vectors, которые содержат адрес сети и список атрибутов (path attributes), описывающих различные характеристики маршрута от маршрутизатора-отправителя в указанную сеть. (Решение о приемлемости или неприемлемости полученного маршрута маршрутизатор-получатель принимает на основании данных, содержащихся в атрибутах пути, проанализировав их с точки зрения политики своей AS) Наиболее важные атрибуты маршрута AS_PATH – определяет AS, через которые доставлена маршрутная информация. ORIGIN определяет происхождение информации о маршруте. NEXT_HOP– указывает IP-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.

46. Внутренние и внешние шлюзовые протоколы.

Сетевой шлюз — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы.

Автономная система – это совокупность сетей под единым административным управлением, обеспечивающим общую для всех входящих в автономную систему маршрутизаторов политику маршрутизации.

Автономные системы соединяются внешними шлюзами (маршрутизаторами). 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.

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.

47. Протокол пограничной маршрутизации BGP. Протокол BGP (внешний и внутренний)

BGP — это протокол маршрутизации между автономными системами.

Наиболее существенным достижением BGP4 является использование им механизма внутридоменной бесклассовой 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 сеть 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. Внуренний IBGP – с его помощью иформация, полученная сервисом AC распространяется внутри нее. Не ялвяется обязательным. Однако система получается более чистой и удобной в управлении.

48. Протоколы транспортного уровня стека протоколов TCP/IP. Их отличие.
Транспортный уровень сетевых моделей образует основную границу между поставщиком и пользователем.
К транспортному уровню TCP/IP относится: 1) протокол TCP – потоковый транспортный сервис надежной доставки. 2) Протокол UDP – сервис неориентированной доставки ед. сообщений. Не контролирует ничего кроме строения сообщения.
Протокол управления передачи TCP требует подтверждение о доставке. Основная разница между TCP и UPD в гарантии доставки сообщений. В отличие от UPD, который создает свои дейстраграммы на основе логически обособленных ед. данных-сообщений. протокол TCP режет поток данных на сегменты без учета структуры.

49. Понятие Сокета.
Сокеты (sockets) представляют собой высокоуровневый унифицированный интерфейс взаимодействия с телекоммуникационными протоколами. В технической литературе встречаются различные переводы этого слова - их называют и гнездами, и соединителями, и патронами, и патрубками, и т .д.
Сокет - это конечная точка сетевых коммуникаций. Он является чем-то вроде "портала", через которое можно отправлять байты во внешний мир. Приложение просто пишет данные в сокет; их дальнейшая буферизация, отправка и транспортировка осуществляется используемым стеком протоколов и сетевой аппаратурой. Чтение данных из сокета происходит аналогичным образом.
Концепция сокетов
Сетевой сокет (network socket) во многом напоминает электрическую розетку. В сети имеется множество сокетов, причем каждый из них выполняет стандартные функции. Все, что поддерживает стандартный протокол, можно «подключить» к сокету и использовать для коммуникаций. Для электрической розетки не имеет значения, что именно вы подключаете – лампу или тостер, поскольку оба прибора рассчитаны на напряжение 220 Вольт и частоту 50 Герц. Несмотря на то, что электричество свободно распространяется по сети, все розетки в доме имеют определенное место. Подобным образом работают и сетевые сокеты, за исключением того, что электроны и почтовые адреса заменены на пакеты TCP/IP и IP-адреса. Internet Protocol (IP) является низкоуровневым протоколом маршрутизации, который разбивает данные на небольшие пакеты и рассылает их по различным сетевым адресам, что не гарантирует доставку вышеупомянутого пакета адресату. Transmission Control Protocol (TCP) является протоколом более высокого уровня, собирающим пакеты в одну строку, сортирующим и перетранслирующим их по мере необходимости, поддерживая надежную рассылку данных. Третий протокол, UNIX Domain Protocol (UDP), используется вместе с TCP и может применяться для быстрой, но ненадежной передачи пакетов.

50. Дейтаграммный способ передачи пакетов. Протокол UDP на хостеотправителя и получателя.
Дейтаграммный способ передачи данных основан на том, что все передаваемые пакеты продвигаются (передаются от одного узла сети другому) независимо друг от друга на основании одних и тех же правил.
Процедура обработки пакета определяется только значениями параметров, которые он несет в себе, и текущим состоянием сети (например, в зависимости от ее нагрузки пакет может стоять в очереди на обслуживание большее или меньшее время). Однако 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.
Решение о продвижении пакета принимается на основе таблицы коммутации, ставящей в соответствие адресам назначения пакетов информацию, однозначно определяющую следующий по маршруту транзитный (или конечный) узел. В качестве такой информации могут выступать идентификаторы интерфейсов данного коммутатора или адреса входных интерфейсов коммутаторов, следующих по маршруту.
UDP обеспечивает передачу дейтаграмм между приложениями хостов Internet.
Так как отправитель не знает, какие процессы активны в настоящий момент, для отправки сообщений одному из приложений хоста **UDP** применяет целевой порт протокола (абстрактная точка для приема данных на хосте), представляющий собой положительное целое число. Полученные сообщения помещаются в очередь, связанную с портом протокола, пока приложение не сможет их обработать.
Для отправки дейтаграмм протокол **UDP** применяет протокол **IP**, поэтому **UDP** так же не устанавливает соединения, как и **IP**. Он не гарантирует доставку дейтаграммы и не обеспечивает защиту от дублирования данных. Однако **UDP** позволяет отправителю задать для сообщения исходный и целевой порты и обеспечивает проверку целостности данных и заголовка сообщения с помощью контрольной суммы. Это позволяет отправителю и получателю проверить правильность доставки сообщения.

51. Логическое соединение – основа надежности TCP.
На TCP возложена доп задача – обеспечить надежную доставку сообщений. Вне этого используется метод продвижения данных с установлением логического соединения. Оно позволяется участникам следить за тем, чтобы данные не были потеряны, искажены или пробублированы, а также чтобы был сохранен порядок.
TCP устанавливает логические соединения между процессами, в каждом соединении участвуют только 2 процесса. TCP-соединения являются дуплексными, т.е. каждый из участков может одновременно получать и отправлять данные.

52. Процедура установления соединения в TCP
Соединение устанавливается по инициативе клиентской части приложения.
1) Клиент обращается к TCP который посылает на это сообщение сегмент-запрос на установление соединения протоколу TCP, работая на сервере. Флаг SYN уст. в 1.
2) TCP на сервере пытается создать инфраструктуру для обслуживания клиента. ACK и SYN в 1.
Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK.
3) Клиент посылает ACK и переходит в состояние логического соединения STAB LISHED. Получения ASK сервер тоже переходит в STAB LISHED.
В случае неудачи сервер посылает клиенту сегмент с флагом RST.

53. Передача с установлением логического соединения.
После установления соединения между клиентом и сервером данные могут пересылаться независимо в обоих направлениях. При этом прием данных подтвергается квитанцией с использованием бита ACK и номера подтверждения.
Процедура установления соединения состоит обычно из трех шагов:
1. Узел-инициатор соединения посылает узлу-получателю служебный кадр с предложением установить соединение.

2. Если узел-получатель согласен с этим, то он посылает в ответ другой служебный кадр, подтверждающий установление соединения и предлагающий некоторые параметры, которые будут использоваться в рамках данного логического соединения. Это могут быть, например, идентификатор соединения, максимальное значение длины поля данных кадров, количество кадров, которые можно отправить без получения подтверждения, и т. п.
3. Узел-инициатор соединения может закончить процесс установления соединения отправкой третьего служебного кадра, в котором сообщит, что предложенные параметры ему подходят.
На этом логическое соединение считается установленным.
Логическое соединение может быть рассчитано на передачу данных как в одном направлении — от инициатора соединения, так и в обоих направлениях. После передачи некоторого законченного набора данных, например определенного файла, узел-отправитель инициирует разрыв данного логического соединения, посылая соответствующий служебный кадр.

54. Оконное управление потоком протоколом TCP
Есть 2 метода организации процесса обмена квитанциями:1) Метод с простоями 2) метод скользящего окна.
Метод с простоями (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 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 квитанций. Количество кадров, которые разрешается передавать таким образом, называется размером окна.
При отправке пакетов устанавливается тайм-аут ожидания квитанции.
Метод с простоями является частным случаем метода скользящего окна, когда размер окна равен единице.

55. Метод скользящего окна.
Есть 2 метода организации процесса обмена квитанциями:1) Метод с простоями 2) метод скользящего окна.
Метод с простоями (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 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 квитанций. Количество кадров, которые разрешается передавать таким образом, называется размером окна.
При отправке пакетов устанавливается тайм-аут ожидания квитанции.
Метод с простоями является частным случаем метода скользящего окна, когда размер окна равен единице.

56. Прикладной уровень стека TCP/IP
На прикладном уровне рассматриваются программные средства двух видов – приложения и службы. Приложения организуют интерфейс между пользователем и сетью, а службы готовят данные для передачи для сети. Различные протоколы прикладного уровня (HTTP, FTP, TellNet) формируют поток данных, поставляемый на нижележащий транспортный уровень.
Вне нижележащего уровни в стеке TCP/IP обеспечивают доставку инф-ии по сети, но не связывают с ПО.
Прикладной уровень не занимается доставкой: он описывает протоколы взаимодействия программы (структуру информации) и возможную реализацию процедур обращения к примитивной TCP. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам.
Прикладной уровень объединяет все службы, представленные системой пользовательским приложениями.

57. Система доменных имен DNS. Схемы разрешения имен DNS.
Домен – множество хостов, объединенных в некую логическую группу под одним именем группы. Совокупность имен, у которых несколько старших (справа) составных частей совпадают, образуют домен имен. DNS (Domain Name System) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов сети Internet. На прикладном уровне широко применяется символическая система адресации.
Проблема разрешения имен – преобразование символического имени в IP-адрес и обратно. Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла.
К примеров, доменные имена могут обозначать типы организаций (com – коммерческие, edu – образовательные и т.п.), или регионы (by – Беларусь, uk – Великобритания, ru - Россия).
Чаще домен-имен делится на поддомены, каждый из которых имеет свой DNS сервер. Используются 2 подхода к разрешению доменных имен: рекурсивная процедура (клиент обращается с запросом к DNS-серверу, а если домен ему подходит, то он сразу возвращает клиенту авторитетную запись ресурса, которые затем кэшируются, попадая на сервер) и итеративная процедура (работу по поиску IP-адреса координируе DNS-клиент: если после образения к лок серверу разрешение не найдено, то клиент сразу же информируется, что порождает недостаток – высокую загрузку клиента).

58. Электронная почта. Протоколы электронной почты. WEB-почта
Сетевая электронная почта – распеделенное приложение, главной функцией которого является предоставление пользователям сети возможности обмениваться электронными сообщениями. Как и все службы, электронная почта построена на архитектуре клиент-сервер. Почтовый клиент всегда располагается на ПК пользователя, а почт. сервер работает на выделенной ПК.
В качестве средств передачи сообщения почтовая служба использует стандартный разработанный специально для почтовых систем протокол SMTP (Simple Mail Transfer Protocol – простой протокол передачи почты). Он обеспечивает как передачу сообщений в адрес одного получателя, так и тиражирование нескольких копий сообщений для передачи в разные адреса.
Логика работы SMTP: после инициации отправки сообщения SMTP-клиент посылает запрос на установление TCP соединения на порт 25. Если сервер готов, то он посылает свои идентифицирующие данные (к примеру, своё DNS-имя). Затем клиент передает серверу адреса отправителя и получателя. Если имя получателя соответствует ожидаемому. то после получения адресов сервер дает согласие на установление TCP-соед. Используя одно TCP-соед. клиент может передать несколько сообщений, передоверяя каждое из них указанием адресов отправителя и получателя. После завершения передачи TCP и SMTP соединения разрываются.

Web-почта – один из примеров ПО, которые передают услуги, используя веб-технологии.

59. WEB-служба. Протокол HTTP.

WEB-служба – отдельные независимые приложения многократного использования, которые выполняют свои функции через веб-интерфейс. Для связи с внешним миром вместо протокола удаленного вызова процедур используют протакол HTTP. Веб-службы позволяют приложениям или другим Веб-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.

HTTP (HyperText Transfer Protocol – протокол передачи гипертекста) – это протокол прикладного уровня во многом аналогичный протоколам FTP и SMTP. Обмен сообщениями идёт по обычной схеме «запрос-ответ». Клиент и сервер обмениваются текстовыми сообщениями стандартного формата в кодировке ASCII. Для транспортировки HTTP-сообщений служит протокол TCP.

60. Понятие URL и URN

Браузер находит веб-страницы и отдельные объекты по адресам специального формата, называемым URL (Uniform Resource Locator – унифицированный указатель ресурса). Он предназначен для идентификации типов, методов и ПК, на которых находятся определённые ресурсы, доступные через интернет. В URL адресе можно выделить 3 части: тип протокола доступа (HTTP, FTP, telnet и т.п.), имя сервера (на котором хранится нужная страница и, как правило, это символическое имя) и путь к объекту (составное имя файла/объекта относительно главного каталога веб-сервера, предлагаемого по умолчанию).

URI – обобщение URL, созданы для решение проблемы того, что иногда имеет смысл ссылаться на страницу не указывая того, где эта страницы находится. Если URI указывают, как определить место нахождения ресурса – это URL. Другие URI указывают имя ресурса, но не его местонахождение. Они называются URN (Uniform Resource Name – унифицированное имя ресурса). Он реализует механизмы оптимального поиска документа (ближайшей копии ресурса на узле).

61. Понятие разделяемой среды. Методы доступа к разделяемой среде в технологиях с топологиями линейная шина и кольцо.

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 определённого 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 (коксиального) 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. топогия 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.

62. Базовые технологии локальных сетей. Технология Ethernet. Высоскоростные технологии

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.

Разделают два типа методов доступа к среде передачи данных: случайный и маркерный.

Технология Ethernet

Ethernet - самый распространённый 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 (100мбит/с). 2. Gigabit Ethernet (1гбит/с). 3. 10g ethernet (10 gbit/s). 4. 40 и 100g ethernet

Дополнительная спецификация среды: 1. 10 base5 – толстый коаксиальный кабель. 2. 10 base-t – кабель витая пара. 3. 10base-fl - оптоволокно

63. Принципы построения локальных сетей на основе технологии Token Ring

Характеристики TR:

логическая топология – кольцо, физическая топология – звезда, метод доступа – маркерное кольцо.

Маркер – кадр, определяющий право доступа к общему разрешённому ресурсу. Кадр данных – сами данные. Прерывающая последовательность -jam-последовательность, которая прерывает

Основные технические характеристики классического варианта сети Token Ring:

max количество концентраторов типа IBM 8228 MAU – 12;

максимальное количество абонентов в сети – 96;

max длина кабеля между абонентом и концентратором – 45 м;

максимальная длина кабеля между концентраторами – 45 м;

max длина кабеля, соединяющего все концентраторы – 120 м;

скорость передачи данных – 4 Мбит/с и 16 Мбит/с. (в случае использования неэкранированной витой пары)

64. Принципы построения локальных сетей на основе технологии FDDI

FDDI (Fiber Distribute Data Interface) – первая технология, используемая в качестве среды передачи оптоволоконный кабель. Оптоволокно может быть одномодовым (сигнал распространяется по одной прямой) и многомодовым (по синусоидам с разными шагами).

FDDI Во многом основан на Token Ring. Реализует передачу по двойному кольцу оптоволоконного кабеля со скоростью 100мбит/сек. Расстояние до 100км. Максимально число абонентов – 1000.

2 кольца оптоволокна: основной и резервный. В случае, когда первичное кольцо не может обеспечить передачу данных, оно объединяется со вторичным, вновь образуя единое кольцо. Это называется режим сети wrap.

65. VLAN - виртуальные локальные сети.

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 домен 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).
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 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.

66. Канальный уровень и его подуровни.
Канальный уровень – уровень, предназначенный для передачи данных узлам в пределах сегмента локальной сети. Есть 2 типа каналов:
Широковещательные каналы, несколько хостов, присоединённых к одному каналу связи. Для координации требуется протокол
Обычная двухточечная линия связи, соединяющая например 2 маршрутизатора или офисный ПК пользователя с Ethernet-коммутатором. Управление доступом к каналу является тривиальным. При помощи протокола двухточечной передачи (PPP) задаются разнообразные настройки: от коммутируемого доступа по телефонной линии до высокоскоростной двухточечной передачи кадров по оптоволоконным сетям.

67. Канальный уровень. Основные поля формата кадра
Уровень LLC представляет собой обобщение функционирований разных технологий по обеспечению передачи кадров с различными предпочтениями и требованиями. Формат кадра: [флаг|DSAP|SSAP|Control|Data|Флаг].
DSAP (destination service access point) – адрес точки входа службы назначения. SSAP (Source Service Access Point) – адрес точки входа службы источника. Control – поле управления, кот. используется для обозначения типа кадра данных – информационный, управляющий или ненумерованный.Data – поле данных кадра LLC, предназначено для передачи данных по сети пакетов протоколов верхних уровней или (в редких случаях) – прикладных протоколов.

68. Канальный уровень, MAC –адрес. Типы MAC- адресов
MAC-адрес назначается сетевым адаптером и сетевыми интерфейсами маршрутизаторов. Для всех существующих технологий локальных сетей MAC – адрес имеет формат 6 байт.
Типы:
1) Индивидуальный (Unicast). Когда осуществляется передача данных, то эти данные получит только 1 ПК
2) Групповой (multicast). Если осуществляется передача данных на групповой мак, то эти данные получат ПК, которые входят в группу. На них должен быть настроен прием данных по этому групповому маку. Начинается с 01.
3) Широковещательный (broadcost): адрес состоит из всех битовых единиц: FF-FF-FF-FF-FF-FF. Когда данные отправляются на такой адрес, их принимают все ПК в сети.
Маки должны быть учтены в пределах одного сегмента сети, иначе нельзя понять, к какому устройству нужно отправить данные.

69. Подуровень LLC. Подуровень MAC.
Канальный уровень делится на 2 подуровня: Logical Long Control (LLC) – уровень управления логическим каналом и Media Access Control (MAC) – уровень управления доступом к среде.
LLC реализуется программно на уровне ОС, а MAC – програмно-аппаратно, сетевым адаптером или его драйвером.
MAC обеспечивает корректное совместное использование разделяемой среды передачи данных в соответствии с определённым алгоритмом доступа (протоколом), который полностью определяет специфику сетевой локальной технологии. LLC отвечает за передачу кадров данных между узлами с различной степенью надёжности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем и MAC-подуровнем.
Вне реализации транспортных услуг LLC предусматривает 3 режима: LLC1 (процедура без установления соединения и без подтверждения), LLC2 (с уст. соед и с подтв), LLC3 (без уст. соед, но с подтв)

70. Алгоритмы функционирования сетевого адаптера при приеме и передачи в канале связи
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 исхожный 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 оп-ной памяти.
Передача кадра из адаптера в кабель
1) Прием кадра данных LLC через межуровневый 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.