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

Компьютерная сеть – это множество компьютеров, соединенных линиями связи и работающих под управлением специального программного обеспечения.

Линия связи - совокупность технических устройств, и физической среды, обеспечивающих передачу сигналов от передатчика к приемнику. В реальной жизни примерами линий связи могут служить участки кабеля и усилители, обеспечивающие передачу сигналов между коммутаторами телефонной сети. На основе линий связи строятся каналы связи.

Канал связи - система технических устройств и линий связи, обеспечивающую передачу информации между абонентами. Канал связи может включать в себя несколько разнородных линий связи, а одна линия связи может использоваться несколькими каналами

Интерфейс - формально определенная логическая и (или) физическая граница между взаимодействующими независимыми объектами. Он задает параметры, процедуры и характеристики взаимодействия объектов.

Сетевой адаптер выступает в качестве интерфейса между ПК и сетевым кабелем в сети с жёсткой логикой соединений, он вставляется в слот материнской платы.

Важной характеристикой любой компьютерной сети является широта территории, которую она охватывает. Широта охвата определятся взаимной удаленностью компьютеров, составляющих сеть и, следовательно, влияет на технологические решения, выбираемые при построении сети. Классически выделяют два типа сетей: **локальные сети** и **глобальные сети**.

К **локальным сетям** относят сети, компьютеры которых сосредоточены на относительно небольших территориях (как правило, в радиусе до 1-2 км). Классическим примером локальных сетей является сеть одного предприятия, расположенного в одном или нескольких стоящих рядом зданиях.

**Глобальные сети** – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга

Исторически главной целью объединения компьютеров в сеть являлось совместное использование ресурсов.

Цели создания КС:

* Создание и использование информационных систем общего пользования(веб-сайты, БД, информационно-коммуникационные сервисы, облачные хранилища данных и т.д.)
* Совместное использование устройств и каналов связи (принтеры, факсы, веб-камеры, различные датчики, смартфоны, Интернет, масса других беспроводных устройств)
* Передача данных между устройствами(компьютеры, серверы, телеметрические системы и др.)
* Организация параллельных вычислений, в т.ч. Территориально распределённых.

**2. Сетевые интерфейсы.**

Для связи устройств в сети, прежде всего, должны быть предусмотрены внешние интерфейсы. Разделяют физический и логический интерфейсы.

Физический интерфейс (называется также портом) - определяется набором электрических связей и характеристиками сигналов. Обычно он представляет собой разъём с набором контактов. Пара разъёмов соединяется кабелем, состоящим из набора проводов, каждый из которых соединяет соответствующе контакты. Так создается линия связи между двумя устройствами.

Логический интерфейс (называется также протоколом) - это набор информационных сообщений определённого формата, которыми обмениваются два устройства или две программы. Также это набор правил, определяющих логику обмена между этими сообщениями.

Средство взаимодействия между логическими интерфейсами называется канал связи.

Интерфейс компьютер — компьютер позволяет двум компьютерам обмениваться информацией. С каждой стороны он реализуется парой:

• аппаратным модулем, называемым сетевым адаптером, или сетевой интерфейсной картой (Network Interface Card, NIC);

•драйвером сетевой интерфейсной карты — специальной программой, управляющей работой сетевой интерфейсной карты.

Сетевой адаптер (или карта) обеспечивает комп-у связь с физической средой. Т.е., сетевые адаптеры обеспечивают через канал связи физическое соединения компьютера с сетью.

 У сетевой карты есть трансивер, который направляет данные из параллельного канала в последовательный и наоборот.

**3. Компоненты компьютерных сетей.**

Компьютерная сеть данных - это совокупность узлов, связываемых посредством сетевых устройств.

Узел - это любое устройство, отправляющее и принимающее информацию по сети.

Периферийные устройства - устройства, подключаемые к узлам.

Некоторые устройства могут выступать как в роли узлов, так и в роли периферийных устройств. Например, принтер подключенный к сетевому портативному ПК, является периферийным устройством. Если принтер подключен непосредственно к сетевому устройству, такому как концентратор, коммутатор или маршрутизатор, то он выступает в роли узла.

КС - совокупность каналов связи, устройств приёма и передачи информации (hardware), коммуникационного оборудования и сетевого ПО для объединения комп-ов и обеспечения данных между ними (software).

Основными компонентами КС являются:

* Конечные устройства  (end Devices): сервера, комп-ы, телефоны, веб-камеры и т.д.
* Промежуточные устройства (intermediary devices): маршрутизаторы, коммутаторы, беспроводные точки доступа,  модемы

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 - сетвеое устройство или программное средства для сопряжения разнородных сетей.

* Среды передачи данных (media): металл, стекло, пластик, радио волны и излучения

Физические средства связи: эфир (воздушное пространство), коаксиальный кабель, волоконно-оптический кабель, витая пара, разновидности плоских кабелей.

* Программные средства (Services: веб-сервер, mail-сервер, ftp- сервер, telnet. Processes - специальные сетевые процессы, которые работают на сетевом оборудовании)

 Сервер - компьютер или программа, предоставляющая некоторые услуги.

Клиент - компьютер или программа, запрашивающая услуги: толстый клиент,, тонкий клиент, сверхтонкий клиент.

Выделенный сервер - компьютер, служащий только для обслуживания клиентских машин.

**4. Проблемы связи нескольких компьютеров. Топология. Выбор физической топологии.**

Объединяя в сеть несколько (больше двух) компьютеров, необходимо решить, каким образом соединить их друг с другом, другими словами, выбрать конфигурацию физических связей, или топологию.

**Физическая топология** описывает компоновку проводов и устройств, а также каналы, использующиеся при передаче данных.

**Логическая топология** – это путь, который проходят сигналы при перемещении из одной точки в другую. Существует шинная, звездообразная, кольцевая и ячеистая топологии.

**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, и их связь между ними.

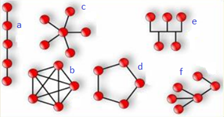
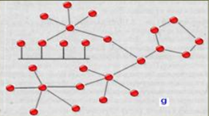
Базовые топологии:

Линейная шина (общая шина - Bus);

Звезда (Star);

Кольцо (Ring).

По физической топологии связей различают:

1. «Точка-точка»;
2. Полносвязная топология;
3. «Звезда»;
4. «Кольцо»;
5. «Общая шина»;
6. «Дерево»;
7. Сети со смешанной топологией.

Физическая топология, как правило, не совпадает с логической.

Физические топологии LAN

* Шина (Bus)
  + Все ПК подключаются к одному незамкнутому кабелю – шине.
  + Каждый ПК может взаимодействовать с любым другим ПК,
  + Все ПК независимы.
  + Надежность, т.к. при выходе из строя одного ПК сеть продолжает работать.
* Кольцо (Ring)
  + Все ПК подключены к одному кабелю, замкнутому в кольцо, т.е. связаны по кругу.
  + При выходе из строя одного ПК не работает вся сеть.
  + Каждый ПК ретранслирует (усиливает, восстанавливает) приходящий к нему сигнал.
  + Данная топология имеет высокую скорость передачи данных, широко применяется.
  + Размеры сетей достигают десятков километров (кольцо в этом отношении существенно превосходит любые другие топологии).
  + Максимально возможное число абонентов велико (>1000).
* Звезда (Star)
  + Каждый кабель подключен отдельным кабелем к спец. центральному устройству – концентратору.
  + Обмен информацией – через центральный узел, на который ложится большая нагрузка.
  + Выход из строя периферийного ПК не нарушает функционирования всей сети, но отказ центрального компьютера делает сеть неработоспособной.
  + Позволяет создавать сложные разветвленные сети.
  + Все точки подключения собраны в одном месте: удобство с точки зрения контроля работы сети, ограничения доступа посторонних лиц.
  + Недостаток – большой расход кабеля.

Наиболее распространенными типами логических топологий являются широковещательная рассылка и маркерная передача данных.

В топологии широковещательной рассылки

* Каждый узел адресует данные либо определенному узлу, либо всем узлам, подключенным к сети.
* Специального порядка, которому должны следовать узлы при использовании сети, не существует – при передаче данных в сети действует правило «первым пришел, первым обслужен».

При маркерной передаче данных

* Управление сетевым доступом осуществляется путем передачи электронного маркера последовательно каждому узлу.
* Когда узел получает маркер, он может передавать данные по сети. Если у узла нет данных для передачи, он передает маркер следующему узлу, и процесс повторяется.

Архитектуры LAN

|  |  |  |
| --- | --- | --- |
| Архитектура | Физическая топология | Логическая топология |
| Ethernet | Шина  Звезда  Расширенная звезда | Шина |
| Token Ring (кольцевая сеть с маркерным доступом) | Звезда | Кольцо |
| Fiber-Distributed Data Interface – интерфейс для передачи распределенных данных по волоконно-оптическим каналам (FDDI) | Двойное кольцо | Кольцо |

**5. Проблемы связи нескольких компьютеров. Адресация сетевых интерфейсов.**

Еще одной новой проблемой, которую нужно учитывать при объединении трех и более компьютеров, является проблема их адресации, точнее адресации их сетевых интерфейсов.

Один сетевой узел может иметь несколько сетевых интерфейсов.

Например, для создания полносвязной структуры из N компьютеров необходимо, чтобы у каждого из них имелся N-1 интерфейс.

**Адреса интерфейсов можно классифицировать следующим образом:**

* Уникальный адрес (unicast) используется для идентификации отдельных интерфейсов;
* Групповой адрес (multicast) идентифицирует сразу несколько интерфейсов, входящих в группу, поэтому данные, помеченные групповым адресом, доставляются каждому из узлов, входящих в группу;
* Широковещательный адрес (broadcast) идентифицирует адреса всех сетевых интерфейсов;
* Адрес произвольной рассылки (anycast), определенный в новой версии протокола IPv6, так же, как и групповой адрес, задает группу адресов, однако данные, посланные по этому адресу, должны быть доставлены не всем адресам данной группы, а любому из них.

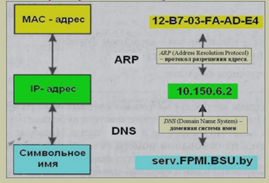
**Типы адресов (схемы адресации):**

* Числовые и символьные (Пример: 192.168.1.1 и fpmi.bsu.by).
* Аппаратные обычно встроены в устройство (Пример: MAC-адрес – 11-F1-00-E5-24-DC) и сетевые (IP-адрес 10.150.1.3, номер сети, номер узла в сети).
* Плоские и иерархические (Пример: MAC-адрес, IP-адрес, символьный).

Для установления соответствия между адресами различных типов в сетевых технологиях применяют специальные вспомогательные процедуры, которые называют протоколами разрешения адресов (служба разрешения адресов).

Множество всех адресов, которые являются допустимыми в рамках некоторой схемы адресации, называется адресным пространством.

**Преобразование адресов:**



**6. Проблемы связи нескольких компьютеров. Коммутация (Определение потоков, определение маршрутов, коммутация в транзитном узле, мультиплексирование и демультиплексирование)**

Пусть компьютеры физически связаны между собой в соответствии с некоторой топологией и выбрана система адресации. Но остается нерешенной проблема: каким способом передавать данные между конечными узлами?

Особую сложность приобретает эта задача для неполносвязной топологии сети, когда обмен данными между произвольной парой конечных узлов (пользователей) должен идти в общем случае через транзитные узлы.

Транзитные узлы, предназначенные только для коммутации, образуют коммутационную сеть.

Соединение отправителя и получателя через сеть транзитных узлов называют коммутацией.

Последовательность узлов, лежащих на пути от отправителя к получателю, образует маршрут.

Для выполнения коммутации должны быть выполнены следующие основные задачи:

* Определение потоков данных;
* Определение маршрутов;
* Продвижение данных в каждом транзитном узле;
* Мультиплексирование и демультиплексирование потоков.

**Основные определения:**

**Информационным потоком** (data flow, data stream) 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 весь 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.

**Определить маршрут** – это значит выбрать последовательность транзитных узлов (коммутаторов) и их интерфейсов, через которые надо передавать данные, чтобы доставить их адресату.

**Примеры критериев выбора маршрута:**

* Номинальная пропускная способность;
* Загруженность каналов связи;
* Задержки, вносимые каналами;
* Количество промежуточных транзитных узлов;
* Надежность каналов и транзитных узлов.

Гибкое решение задачи определения маршрута предполагает постоянный анализ состояния сети и обновление маршрутов. С этой целью в узлах используется структура данных – **таблица коммутации.**

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, то есть выполнить коммутацию интерфейсов.
* Устройство, функциональным назначением которого является коммутации, называется коммутатором. Коммутатор может быть как специализированное устройство, так и компьютер со встроенным программным механизмом коммутации. В этом случае имеем программный коммутатор.

Основные задачи коммутации:

* Задача мультиплексирования (multiplexing) – образование из нескольких отдельных потоков общего агрегированного потока, который можно передать по одному физическому каналу связи.
* Задача демультиплексирования (demultiplexing) – разделение суммарного агрегированного потока, поступающего на один интерфейс, на несколько составляющих потоков.

На каждом интерфейсе могут одновременно выполняться обе функции – мультиплексирование и демультиплексирование.

**Основные типы мультиплексирования:**

* Частотное мультиплексирование – FDM (Ком. каналов и пакетов)
* Волновое мультиплексирование – WDM (Ком. каналов)
* Временное мультиплексирование – TDM (Ком. каналов)

Принцип временного мультиплексирования (TDM) состоит в выделении каналу каждого соединения определенного кванта времени на использование линии связи.

**Временное уплотнение**

* 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.

Частный случай коммутатора, у которого все входящие информационные потоки коммутируются на один выходной интерфейс, где они мультиплексируются в один агрегированный поток, называется мультиплексором.

Коммутатор, который имеет один входной интерфейс и несколько выходных, называется демультиплексором.

**Частотное уплотнение**

* Полоса частот системы разбита на неперекрывающиеся частотные поддиапазоны и каждой паре взаимодействующих узлов выделяется один из них.
* Нет необходимости ограничивать 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.

**7. Коммутация каналов**

**На практике утвердилось два основных способа коммутации**

* коммутация каналов;
* коммутация пакетов.

Исторически коммутация каналов появилась намного раньше коммутации пакетов. Коммутация каналов ведет свое происхождение от первых телефонных сетей.

Этот способ был разработан телефонистами.

**Коммутация каналов** - это образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами.

Каналы соединяются между собой коммутаторами. Таким образом, по аналогии, 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

**Временные диаграммы:**

* Установление составного канала
* Передача данных.



**Задержка соединения** - установление соединения.

**Задержка распространения** - определяется скоростью распространения электромагнитных волн в конкретной физической среде.

**Достоинства и недостатки сетей с коммутацией каналов**

Достоинства коммутации каналов:

1. Постоянная и известная скорость передачи данных по установленному между конечными узлами каналу.
2. Низкий и постоянный уровень задержки передачи

данных через сеть.

Недостатки коммутации каналов:

1. Отказ сети в обслуживании запроса на установление соединения.
2. Нерациональное использование пропускной способности физических каналов.
3. Обязательная задержка перед передачей данных из-за фазы установления соединения.

Примером реализации способа коммутации каналов может служить классическая

телефонная сеть, в качестве адреса выступает здесь телефонный номер.

**При коммутации каналов всегда можно четко выделить три фазы информационного обмена:**

• Установление соединения;

• Передача информации;

• Разрушение соединения.

Для организации соединения и обслуживания соединения необходимо выделить монопольно ресурсы: каналы связи, управляющее коммуникационное оборудование и т. д. и освободить ресурсы при разрушении соединения.

**8. Коммутация пакетов**

Принцип коммутации пакетов был изобретен разработчиками компьютерных сетей.

При коммутации пакетов учитываются особенности компьютерного трафика, поэтому данный способ коммутации является более эффективным для компьютерных сетей по сравнению с традиционным методом коммутации каналов, применяющимся в телефонных сетях.

Сети с коммутацией пакетов, так же как и сети с коммутацией каналов, состоят из коммутаторов, связанных физическими линиями связи.

Однако передача данных в этих сетях происходит совершенно по-другому.

Образно говоря, по сравнению с сетью с коммутацией каналов сеть с коммутацией пакетов ведет себя менее «ответственно».

Например, она может принять данные для передачи, не заботясь о резервировании линий связи на пути следования этих данных и не гарантируя требуемую пропускную способность.

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.

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. информацию: нумерацию 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.

! Главное отличие пакетных коммутаторов - наличие внутренней буферной памяти для временного хранения пакетов.

Пакетный коммутатор может работать на основании одного из **трех** методов продвижения пакетов:

1. Дейтаграммный способ передачи данных

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.

То есть каждый отдельный пакет 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.

1. Передача с установлением логического соединения

Следующий рассматриваемый способ продвижения пакетов основывается на знании устройствами сети «истории» обмена данными, например, на запоминании узлом-отправителем числа отправленных, а узлом-получателем - числа полученных пакетов.

Такого рода информация фиксируется в рамках логического соединения.

Процедура согласования двумя конечными узлами сети некоторых параметров процесса обмена пакетами, называется установлением логического соединения.

Когда отправитель и получатель фиксируют начало нового соединения, они, прежде всего, «договариваются» о начальных значениях параметров процедуры обмена и только после этого начинают передачу собственно данных.

Передача с установлением соединения более надежна, но требует больше времени для передачи данных и вычислительных затрат от конечных узлов.

Процедура установления логического соединения состоит обычно из трех шагов:

1. Узел-инициатор соединения отправляет узлу-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. Это могут быть, например, идентификатор соединения, количество кадров, которые можно отправить без получения подтверждения и т. п.
3. Узел-инициатор соединения может закончить процесс установления соединения отправкой третьего служебного пакета, в котором сообщит, что предложенные параметры ему подходят.

3) 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 (virtual circuit или virtual channel).

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 VC (virtual channel) (динамическому или постоянному).

Пример - глобальные сети X.25, Frame Relay, ATM

Достоинства и недостатки сетей с коммутацией пакетов

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.

**7-8. Общая таблица**



**9. Многоуровневый подход. Протокол. Межуровневый интерфейс. Стек**

Организация взаимодействия между компонентами компьютерной сети является очень сложной задачей.

Для решения сложных задач используется известный универсальный прием - **декомпозиция**, то есть разбиение одной сложной задачи на несколько

более простых задач-модулей.

Декомпозиция состоит:

в четком определении функций каждого модуля, а также порядка их взаимодействия (то есть межмодульных интерфейсов).

Еще более эффективной концепцией, развивающей идею декомпозиции, является **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 к нему соседние вышележащий и нижележащий уровни.

Многоуровневое представление средсетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют, по меньшей мере, две стороны, то есть 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 уровни и форму электрических сигналов, способ определения размера сообщений, 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.

Термины:

**Межуровневый интерфейс** - называемый также интерфейсом услуг, определяет набор функций (услуг), которые нижележащий уровень предоставляет вышележащему.

**Протокол** - это формализованные правила, определяющие последовательность

и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на ОДНОМ уровне, но в разных узлах.

**Стек протоколов** - это иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов сети.

Передача:

1. Компьютер-источник - передает исходные данные в блок протокола
2. Блок протокола - отвечает за логику передачи данных в сети; организует

данные в пакет передачи, содержащий запрос к обслуживающим устройствам информацию по обработке запроса и исходные данные для передачи

1. Передатчик - преобразовывает данные в сетевой сигнал
2. Физическая кабельная сеть
3. Приемник - перекодирует сигнал в данные
4. Блок протокола - проверяет данные на сбойность, передает квитанцию о

приеме пакета источнику, переформировывает пакеты и передает их в компьютер-адресат

1. Компьютер-адресат

**10. Модель взаимодействия открытых систем (модель OSI), ее назначение и функции каждого уровня (кратко).**

Модель OSI- модель взаимодействия открытых систем.

Модель OSI разрабатывалась в качестве своего рода универсального языка сетевых специалистов. Назначение модели OSI состоит в обобщенном представлении средств сетевого взаимодействия

Модель OSI 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 модели OSI средства взаимодействия делятся на семь уровней: прикладной, представления, сеансовый, транспортный, сетевой, канальный и физический.

Функции уровней:

**Прикладной** – представляет набор интерфейсов, позволяющий получить доступ к сетевым службам

**Представления** – преобразует данные в общий формат

**Сеансовый** – поддержка взаимодействия(сеанса) между удаленными процессами

**Транспортный** – управляет передачей данных по сети, обеспечивает подтверждение передачи.

**Сетевой** – маршрутизация , управление потоками данных, адресацией сообщений для доставки, преобразование логических сетевых адресов и имен в соответствующие им физические.

**Канальный** – управляет формированием кадров(LLC) и доступом к среде (MAC)

**Физический**– битовые протоколы передачи данных.

**11 Сетезависимые и сетенезависимые уровни. Соответствие функций различным типам коммуникационного оборудования и уровням модели OSI.Физический**

Физический , канальный и сетевой уровни – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Прикладной, представительный и сеансовый уровни – являются сетенезависимыми. 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.





**12.Стандартные стеки коммуникационных протоколов.**

Следует четко различать модель OSI и стек OSI.

Модель OSI является концептуальной схемой взаимодействия открытых систем

Стек OSI представляет собой набор вполне конкретных спецификаций протоколов



В отличие от других стеков протоколов стек OSI полностью соответствует модели OSI, он включает спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели.

В тоже время заметим , что протоколы стека OSI отличает сложность и неоднозначность спецификаций.

Эти свойства явились результатом общей политики разработчиков стека, стремившихся учесть в своих протоколах все многообразие уже существующих и новых появляющихся сетевых технологий.

Наиболее популярны следующие стеки:

TCP/IP

IPX SPX

NetBIOS SMB

DECnet

SNA

OSI

Все стеки, перечисленные выше, кроме SNA, на нижних уровнях физическом и канальной – используют одни и те же хорошо стандартизированные протоколы Ethernet, Token Ring, FDDI. Зато на верхних уровнях все стеки работают по своим протоколам

Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

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

Сетевой уровень служит для образования единой транспортной системы, которая объединяет несколько сетей (может быть разного типа). Такая сеть называется составной.



Сетевой уровень решает задачи:

• Определение маршрута от узла отправителя до узла получателя

• Организация продвижения данных по этому маршруту

• Согласование технологий при передаче данных, так как подсети составной сети могут быть построены на основе разных технологий

• Управление параметрами процесса передачи данных (временные задержки, загрузки линий связи)

• Создание барьеров на пути нежелательного трафика между сетями

Технология межсетевого взаимодействия – технология, которая позволяет соединять в единую сеть множество сетей, в общем случае построенных на основе разных технологий. Дополнительные средства, необходимые для связывания между собой этой сет, как раз-таки предоставляются сетевым уровнем. ТМВ предусматривает использование между соединяемыми сетями специального пограничного устройства – маршрутизатора.

Подсеть – целостное адресное пространство (в терминах IP-адресов).

IP-адрес – уникальное число, приписываемое сетевому интерфейсу.

Маршрутизатор – устройство с сетевыми интерфейсами, «смотрящими» в разные подсети.

Путь:

1. Чтобы связать сети, необходимо соединить их маршрутизаторами и установить соответствующее ПО межсетевого взаимодействия

2. Чтобы узлы могли обмениваться данными в пределах составной сети, они должны иметь сетевой адрес

3. В пакете, передаваемом через составную сеть, должен быть указан адрес назначения

4. Маршрут в составной сети описывается последовательностью подсетей (или маршрутизаторов), через которые должен пройти пакет

5. Маршрутизатор собирает информацию о топологии связей и строит таблицу маршрутизации

6. Так, путь пакета разбит на участки от одного маршрутизатора до другого, где каждый участок – путь через отдельную сеть

7. Маршрутизатор-отправитель должен упаковать передаваемый пакет в поле данных пакета, имеющего формат, принятый в данной транзитной сети

8. В качестве адреса назначения в заголовке пакета указывается не сетевой адрес, а локальный адрес интерфейса следующего маршрутизатора. Так доставка пакета между двумя маршрутизаторами может быть выполнена средствами промежуточной сети.

9. Когда пакет доставят на следующий маршрутизатор, он распакует его, извлечёт исходный пакет, а затем выполнит все прошлые процедуры, чтобы воспользоваться транспортными возможностями следующей промежуточной сети по маршруту передачи пакета.

Типы адресов стека TCP/IP

1. Локальные (аппаратные) – определяется технологией, с помощью которой построена отдельная сеть, в которую входит данный узел (MAC-адреса). Он действует только в пределах подсети. Для узла – входящего в локальные сети – это MAC-адрес сетевого адаптера или маршрутизатора. Назначается производителем устройства. Некоторые глобальные сети (X.25, ATM, Frame relay) имеют свою систему адресации.

Физический (локальный) адрес узла определяется технологией, с помощью которой построена сеть, в которую входит узел. В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов (столько сетевых адаптеров никогда не будет выпущено).



2. Сетевые (IP-адреса) – основной тип адреса, которые используются на сетевом уровне для передачи пакетов между сетями. Чтобы технология TCP/IP могла решать свою задачу объединения сетей, ей необходима собственная глобальная система адресации, не зависящая от способов адресации узлов в отдельных сетях. Эта система должна позволять универсальным и однозначным способом идентифицировать любой интерфейс составной сети. Решение – нумерация всех сетей составной сети, а затем нумерация всех узлов в пределах каждой из этих сетей.

Сетевой адрес – пара, состоящая из номера сети и номера узла.

IP-адрес является основным типом адреса, который используется на сетевом уровне для передачи пакетов между сетями. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов (статически) или протоколом DHCP (динамически – на время аренды адреса, то есть временно).

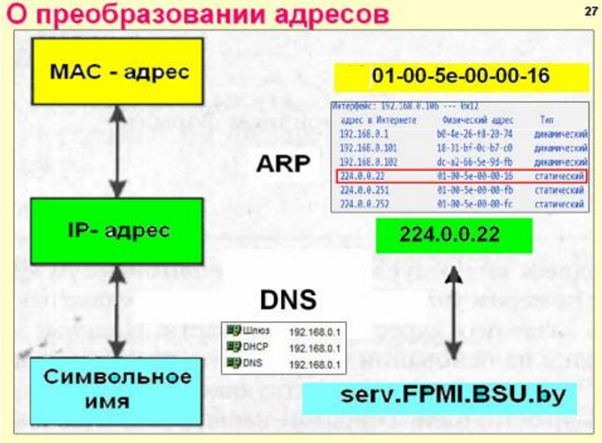
MAC-адрес – номер паспорта, IP-адрес – адрес с почтовым индексом.

3. Символьные (доменные) имена (DNS-имена, NetBIOS-имена) – более удобное символьное имя компьютера, нежели IP-адрес. Символьные идентификаторы сетевых интерфейсов строятся по иерархическому принципу в пределах составной сети. Составляющие имени разделяются точкой и перечисляются в порядке от имени хоста до имени домена самого высокого уровня (между ними – имена групп хостов)

serv604.FPMI.BSU.BY

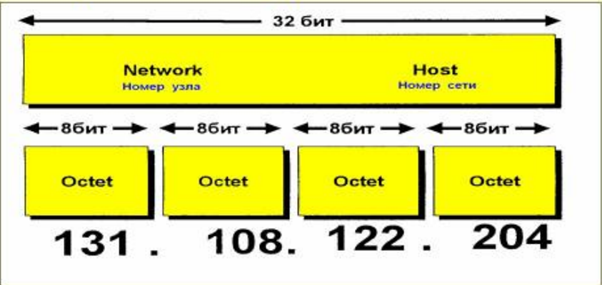
Между доменным именем и IP-адресом нет никакой функциональной зависимости, поэтому соответствие можно установить только с помощью таблицы. В сетях TCP/IP используется специальная система доменных имён (Domain Name System, DNS), которая устанавливает это соответствие на основании создаваемых администратором сети таблиц соответствия. Поэтому их называют DNS-именами.

В общем случае сетевой интерфейс может иметь несколько локальных адресов, сетвых адресов и доменных имен.



**14. Адресация в IP сетях. Классы IP-адресов. Распределение IP –адресов.**

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



Запись адреса не предусматривает специального разграничительного знака между номером сети и номером узла. Вместе с этим при передаче пакета по сети часто возникает необходимость разделить адрес на эти две части. Маршрутизация, как правило, осуществляется на основании номера сети, поэтому каждый маршрутизатор, получая пакет, должен прочитать из соответствующего поля заголовка адрес назначения и выделить из него номер сети.

Как маршрутизатор определяет, какая часть относится к номеру сети, а какая – к номеру узла?

1. Может быть использована фиксированная граница. Так, всё 32-битное поле адреса делится на две части фиксированной (не обязательно равно) длины, в одной из которых всегда будет размещаться номер сети, а в другой – номер узла.

2. Может быть использована маска, которая максимально гибко устанавливает границу между номером сети и номером узла. Тогда можно создавать множество сетей разного размера.

3. Использование классов адресов. Это – компромисс между 1. и 2. Размеры сетей не могут быть произвольным, но и не должны быть одинаковыми. Вводится пять классов: A,B,C,D,E. A,B и С используются для адресации сетей, а оставшиеся два имеют специальное назначение. Для каждого класса установлено своё собственное положение границы между номером сети и номером узла.

Классы IP-адресов – в вопросе 16.

Четыре варианта распределения IP-адресов:

1. Если сеть работает автономно, то назначение IP-адресов произвольно. То есть, администратор может выбирать адреса произвольным образом.

2. Диапазоны адресов в стандартах Internet, рекомендуемых для локального применения (частные, или серые номера):

• В классе A – сеть 10.0.0.0; диапазон адресов: 10.0.0.1 – 10.255.255.254

• В классе B – 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 C – диапазон из 256 сетей: 192.168.0.0 – 192.168.255.0; диапазон адресов: 192.168.0.1 – 192.168.255.254

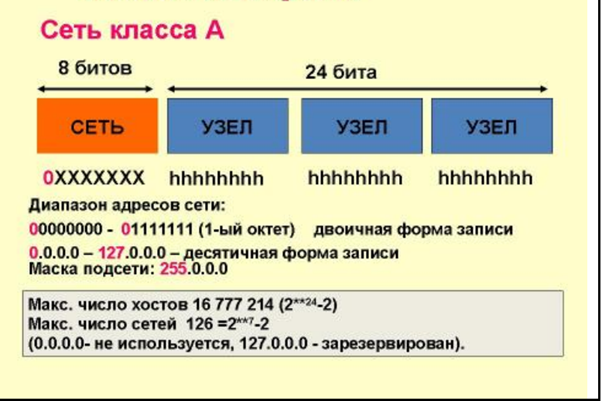
Любая организация может использовать IP-адреса из этих блоков без согласования с ICANN или Internet-регистраторами. В результате эти адреса используются во множестве организаций. Уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов.

3. Централизованное распределение используется в случае, если сеть является частью глобальной сети Internet. Главным органом регистрации глобальных адресов Интернет с 1998 г. является ICANN (Internet Corporation for Assigned Names and Numbers). Проблема этого вида распределения – дефицит адресов, обусловленный не только ростом сетей, но и нерациональным расходованием 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 B. 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.

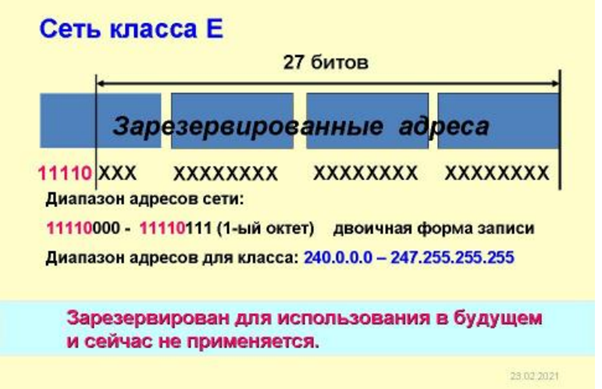
**15. Классы IP-адресов. Особые IP –адреса (Соглашения о специальных адресах).**

Классы IP-адресов.





Группой адрес идентифицирует группу сетевых интерфейсов, которые в общем случае могут принадлежать разным сетям. Интерфейс, входящий в группу, получается наряду с обычным индивидуальным IP-адресом ещё один группой адрес. Если при отправке пакета в качестве адреса назначения указан адрес класса D, то такой пакет должен быть доставлен всем узлам из группы. Групповые адреса используются для служебных пакетов протоколов TCP/IP. Один и тот же узел может входить в несколько групп. В общем случае члены группы могут распределиться по различным сетям, находящимся на произвольно большом расстоянии друг от друга. Многоадресный MAC-адрес – особое значение, которое в шестнадцатеричной форме начинается с 01-00-5E.



Недостатки деления адресов на классы:

• Имеем только 3 вида компьютерных сетей: крупные (A), средние (B) и малые (C).

• Дефицит IP-адресов. Решение – IP-адресация шестой версии – IPv6.

• Если выделена сеть A-C, то вся сеть будет едина, администратор не сможет поделить её на внутренние подсети. Очень трудно организовать права доступа на различные ресурсы сети.

• Возникла задача более гибкой адресации. Решена путём разработки технологии маски переменной длины – VLSM.

Особы IP-адреса

В TCP/IP существуют ограничения при назначении IP-адресов, а именно номера сетей и номера узлов не могут состоять из одних двоичных 0 и 1.

Некоторые IP-адреса интерпретируются особым образом:

1. Адрес только из 0 – неопределённый адрес, обозначающий адрес того узла, который сгенерировал этот пакет. Это хост. Помещается в заголовок пакета в поле адреса отправителя.

2. Если в поле номера сети 0 (0.0.X.Y) – узел принадлежит той же самой сети, что и узел, который отправил пакет. Такой адрес может быть использован только в качестве адреса отправителя.

3. Адрес только из 1 (255.255.255.255) – пакет должен рассылаться всем узлам, находящимся в той же сети, что и источник пакета. Такой адрес называется ограниченным (пакет не выйдет за границы данной сети) широковещательным.

4. Если в поле номера узла 0 (X.Y.Z.255) – пакет рассылается всем узлам сети, номер которого указан в адресе назначения. (Пакет с адресом 192.190.21.255 будет направлен всем узлам сети 192.190.21.0). Такой тип адреса называется широковещательным.

5. Первый октет равен 127 (127.X.Y.Z) – этот адрес является внутренним адресом стека протоколов компьютера (или маршрутизатора). Используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. Когда программа посылает данные по такому адресу, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера, как только что принятые. Адрес 127.0.0.0 зарезервирован для тестирования сетевого ПО узла методом обратной передачи без реальной отправки пакета по сети. Маршрут перемещения образует петлю, поэтому этот адрес называется адресом обратной петли. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127.

**16. Структуризация сети масками одинаковой длины.**

Допустим, администратор получил в свое распоряжение сеть класса В: 129.44.0.0. Он может организовать сеть с большим числом узлов, номера которых доступны ему из диапазона 0.0.0.1-0.0.255.254. Всего в его распоряжении имеется (216 - 2) адреса. Вычитание двойки связано с учетом того, что адреса из одних нулей и одних единиц имеют специальное назначение и не годятся для адресации узлов. Однако ему не нужна одна большая неструктурированная сеть. Производственная необходимость диктует администратору другое решение, в соответствии с которым сеть должна быть разделена на три 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 большой сети с помощью масок имеет еще одно преимущество — оно позволяет скрыть внутреннюю структуру сети предприятия от внешнего наблюдения и тем самым повысить ее безопасность.)

На рис. 1 показано разделение всего полученного администратором адресного диапазона на 4 равные части — каждая по 214 адресов. При этом число разрядов, доступное для нумерации узлов, уменьшилось на два бита, а префикс (номер) каждой из четырех сетей стал длиннее на два бита. Следовательно, каждый из четырех диапазонов можно записать в виде IP-адреса с маской, состоящей из 18 единиц, или в десятичной нотации - 255.255.192.0.

129.44.0.0/18 (10000001 00101100 00000000 00000000)

129.44.64.0/18 (10000001 00101100 01000000 00000000)

129.44.128.0/18 (10000001 00101100 10000000 00000000)

129.44.192.0/18 (10000001 00101100 11000000 00000000)

Из приведенных записей видно, что администратор получает возможность использовать для нумерации подсетей два дополнительных бита (выделенных жирным шрифтом). Именно это позволяет ему сделать из одной централизованно выделенной сети четыре, в данном примере это 129.44.0.0/18,129.44.64.0/18,129.44.128.0/18,129.44.192.0/18.мл

Пример сети, построенной путем деления на 4 сети равного размера, показан на рис. 2. Весь трафик во внутреннюю сеть 129.44.0.0, направляемый из внешней сети, поступает через маршрутизатор R1. В целях структуризации информационных потоков во внутренней сети установлен дополнительный маршрутизатор R2. Каждая из вновь образованных сетей 129.44.0.0/18, 129.44.64.0/18,129.44.128.0/18 и 129.44.192.0/18 подключена к соответственно сконфигурированным портам внутреннего маршрутизатора R2.

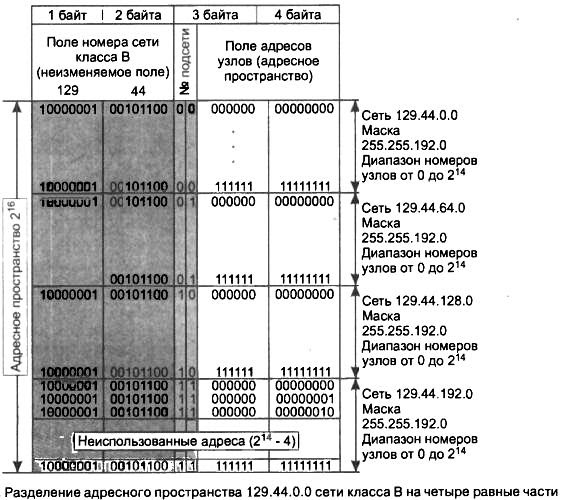


Рис. 1. Разделение адресного пространства 129.44.0.0 сети класса В на четыре равные части

Извне сеть по-прежнему выглядит, как единая сеть класса В. Однако поступающий в сеть общий трафик разделяется локальным маршрутизатором R2 между четырьмя сетями. В условиях, когда механизм классов не действует, маршрутизатор должен иметь другое средство, которое позволило бы ему определять, какая часть 32-разрядного числа, помещенного в поле адреса назначения, является номером сети. Именно этой цели служит дополнительное поле маски, включенное в таблицу маршрутизации (табл. 1).

Первые четыре записи в таблице соответствуют внутренним подсетям, непосредственно подключенным к портам маршрутизатора R2.

Запись 0.0.0.0 с маской 0.0.0.0 соответствует маршруту по умолчанию.

Последняя запись определяет специфический маршрут к узлу 129.44.128.15. В тех строках таблицы, в которых в качестве адреса назначения указан полный IP-адрес узла, маска имеет значение 255.255.255.255. В отличие от всех других узлов сети 129.44.128.0, к которым пакеты поступают с интерфейса 129.44.128.5 маршрутизатора R2, к данному узлу они должны приходить через маршрутизатор R3.

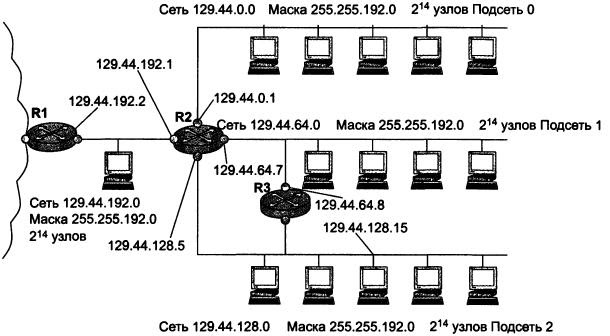


Рис. 2. Маршрутизация с использованием масок одинаковой длины

Таблица 1 Таблица маршрутизатора R2 в сети с масками одинаковой длины

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Адрес назначения | Маска | Адрес следующего маршрутизатора | Адрес порта | Расстояние |
| 129.44.0.0 | 255.255.192.0 | 129.44.0.1 | 129.44.0.1 | Подключена |
| 129.44.64.0 | 255.255.192.0 | 129.44.64.7 | 129.44.64.7 | Подключена |
| 129.44.128.0 | 255.255.192.0 | 129.44.128.5 | 129.44.128.5 | Подключена |
| 129.44.192.0 | 255.255.192.0 | 129.44.192.1 | 129.44.192.1 | Подключена |
| 0.0.0.0 | 0.0.0.0 | 129.44.192.2 | 129.44.192.1 | - |
| 129.44.128.15 | 255.255.255.255 | 129.44.64.8 | 129.44.64.7 |  |

**17    Классы IP-адресов. Маски подсети переменной длинны. (Реализовать следующий пример разбиения сети на подсети: 192.168.2.0/24, разбить на три подсети по 100, 50 и 10 узлов).**

IP-адреса делятся на 5 классов (A, B, C, D, E). A, B и C — это классы коммерческой адресации. D – для многоадресных рассылок, а класс E – для экспериментов.

Класс А: 1.0.0.0 — 126.0.0.0, маска 255.0.0.0

Класс В: 128.0.0.0 — 191.255.0.0, маска 255.255.0.0

Класс С: 192.0.0.0 — 223.255.255.0, маска 255.255.255.0

Класс D: 224.0.0.0 — 239.255.255.255, маска 255.255.255.255

Класс Е: 240.0.0.0 — 247.255.255.255, маска 255.255.255.255

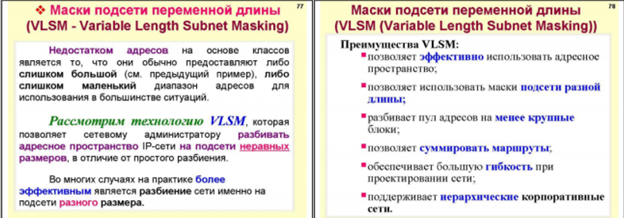
Больше см п.15.

VLSM (variable length subnet masks) — сетевые маски переменной длины. Используются в бесклассовой маршрутизации для задания масок сетей. Например 4 сети класса C (4 \* 255 адресов, маска 255.255.255.0 или /24) могут быть объединены в одну сеть /22. Кроме того сети можно разбивать на более мелкие подсети.

По сравнению с обычной (классовой) системой адресации, VLSM разрешает использование подсетей, с номерами, состоящими из всех нулей или единиц (в двоичной форме)

Возможно применение различных масок подсетей к различным подсетям

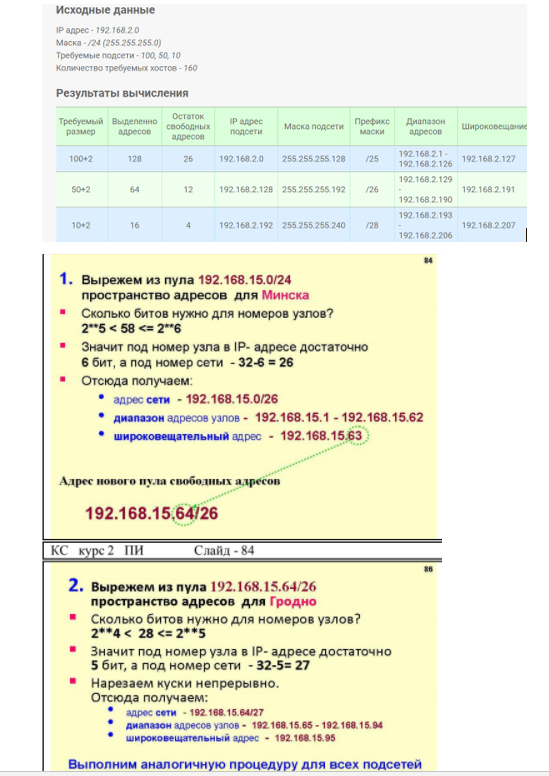
Появляется возможность использования подподсетей (подсетей в подсетях)



Алгоритм выполнения для задания:

При использовании VLSM (Variable Length Subnet Mask) сначала убедитесь, что вы начинаете разделение с самой большой подсети иначе у вас будет перекрывающееся адресное пространство.

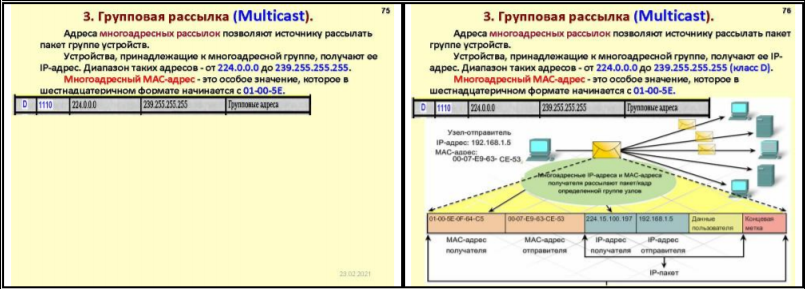
ПРОДОЛЖЕНИЕ (КАРТИНКИ) НА СЛЕД СТРАНИЦЕ



**18 Категории IP-адресов. Одноадресные, широковещательные и многоадресные рассылки.**







**19. Способы назначения IP-адресов. Протокол DHCP. Алгоритм протокола DHCP.**

IP-адреса могут назначаться хостам либо вручную(администратором сети при выполнении конфигурирования), либо динамически(с помощью протокола DHCP(Dynamic Host Configuration Protocol)).

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 при их обращении к DHCP.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес из пула наличных IP-адресов без вмешательства оператора. Границы пула задает администратор. Между идентификатором клиента  и его IP по прежнему существует постоянное соответствие, которое устанавливается в момент первичного назначения DHCP-сервером IP-адреса.

При динамическом назначении адресов DHCP выдает клиенту IP на определенное время - срок аренды, что дает возможность впоследствии использовать этот же адрес другими хостами. Это позволяет строить сети, количество узлов которой намного больше количества имеющихся в распоряжении IP-адресов.

DHCP(Dynamic Host Configuration Protocol) автоматизирует процесс конфигурирования сетевых интерфейсов, обеспечивая отсутствие дублирования адресов за счет централизованного управления их распределением.

3 режима работы (ручной, автоматический статический и автоматический динамический). В начале каждого администратор сообщает один или несколько диапазонов IP-адресов.

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных происходит с помощью протокола UPD, при этом сервер принимает сообщения на порт 67, а отправляет на порт 68.

DHCP сервер:

1. имеет статический адрес
2. находится в одной подсети с клиентами
3. определен пул адресов и срок аренды

Использование DHCP несет в себе некоторые проблемы:

1. Необходимость согласования информационной базы в службах DHCP и DNS
2. Нестабильность IP-адресов (динамических) усложняет процесс управления сетью. Возникают проблемы при конфигурации фильтров маршрутизаторов, которые оперируют с IP-адресами.
3. Есть протоколы, которые были разработаны с учетом статичности IP.
4. Снижение надежности системы при отказе DHCP-сервера. Тогда клиенты не могут получить IP и другие параметры конфигурации.

**20. Отображение IP-адресов на локальные адреса. Протокол ARP**

На каждом маршрутизаторе протокол IP определяет, какому следующему маршрутизатору в этой сети необходимо отправить пакет.

В результате решения этой задачи протоколу IP становится известен IP-адрес следующего маршрутизатора или конечного узла.

Чтобы локальная технология сети смогла доставить пакет на следующий маршрутизатор, необходимо:

1. упаковать пакет в кадр необходимого формата для данной сети
2. снабдить данный кадр локальным адресом интерфейса следующего маршрутизатора.

Как уже было сказано, никакой прямой зависимости между локальным и IP адресом нет, поэтому единственный способ установления соответствия - таблицы.

В результате конфигурирования сети каждый интерфейс знает свой IP и локальный адрес, что можно рассматривать как таблицу из одной строки.

Проблема состоит в том, как организовать обмен информацией между узлами сети.

Для определения локального адреса по IP-адресу используется протокол разрешения адресов (Address Resolution Protocol, ARP).

Он 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.

Работа ARP в широковещательных сетях:

Прежде чем упаковать пакет в кадр Ethernet и направить его маршрутизатору, необходимо определить MAC-адрес. Для этого протокол IP обращается к протоколу ARP.

Протокол ARP поддерживает на каждом интерфейсе сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе конфигурирования сети накапливается информация о соответствии между IP и MAC адресами других интерфейсов данной сети. Первоначально все таблицы пусты.

Процедура отображения IP-адресов в локальных сетях:

1. Передача от IP к ARP сообщения “Какой MAC-адрес имеет интерфейс с адресом IP?”
2. Протокол просматривает собственную таблицу.
3. В случае отсутствия необходимого адреса исходящий IP-пакет запоминается в буфере, а протокол ARP формирует ARP-запрос и широковещательно рассылает.
4. Все интерфейсы сети получают запрос и направляют собственному протоколу ARP.
5. ARP сравнивает указанный в запросе адрес IP с IP-адресом интерфейса, на который поступил запрос.
6. В случае совпадения формируется ARP-ответ. В нем указывается MAC-адрес данного интерфейса.
7. Широковещательный ответ в данном случае не требуется, так как мы знаем, кому отвечать.
8. Заметим, что зона распространения запросов ограничивается локальной сетью, так как на пути широковещательных кадров барьером стоит маршрутизатор.
9. Чтобы уменьшить число запросов, найденное соответствие сохраняется в таблице маршрутизатора.

**21. Протокол IP(структура заголовка)**

Протокол IP(Internet Protocol, протокол межсетевого взаимодействия) составляет основу транспортного стека протоколов TCP/IP. Он относится к протоколам без установления соединения(дейтаграммный протокол).

К основным функциям протокола отнесем:

1. Обеспечивает передачу IP-пакетов от отправителя к получателям через объединенную систему компьютерных сетей.
2. Не устанавливает соединение.
3. Не дает гарантии доставки и сохранения порядка доставки.
4. Обрабатывает каждый пакет как независимую единицу, не связанную с другими пакетами.
5. Способен выполнять динамическую фрагментацию пакетов при передаче их между сетями с различным максимальным размером кадра.

IP-пакет состоит из полей заголовка и данных. Имеется прямая связь между количеством полей заголовка пакета и функциональной сложностью протокола, который работает с этим заголовком. Чем проще заголовок, тем проще протокол, и наоборот. Большая часть действий протокола связана с обработкой той служебной инфы, которая хранится в заголовке.

Изучая назначение каждого поля заголовка пакета, мы получаем не только формальные знания о структуре пакета, но и знакомимся с основными функциями IP-протокола.

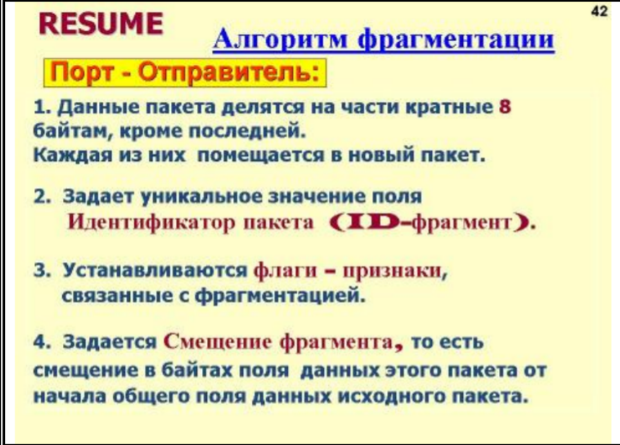
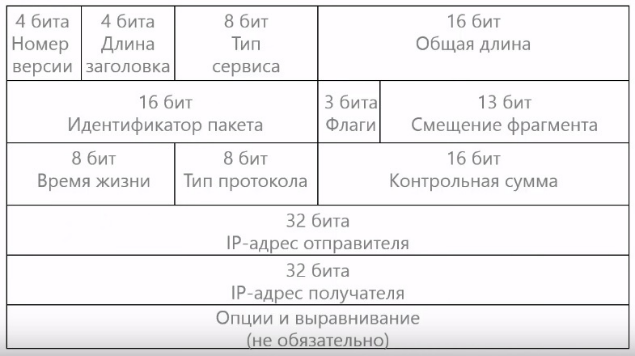
Структура заголовка IP-пакета.

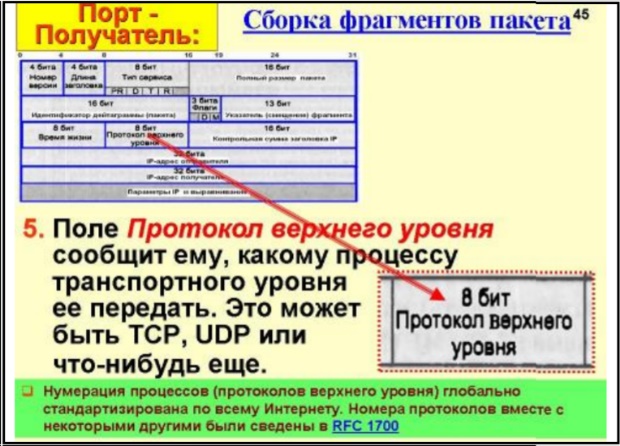
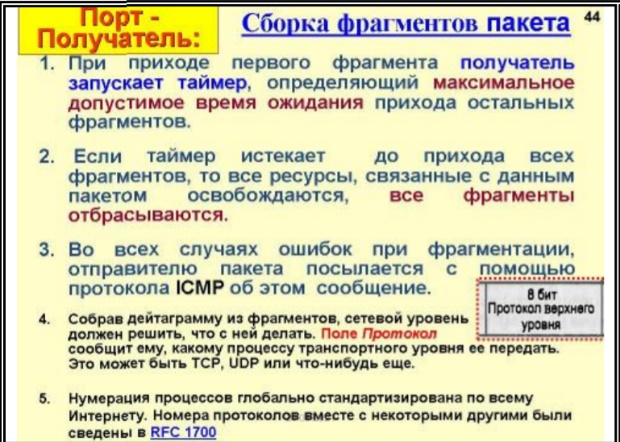


**22. Фрагментация IP-пакетов. Алгоритм фрагментации.**

Длина IP пакета может достигать 64 Кбайтов, что может превышать размер фрейма (MTU) протокола нижнего уровня, в который инкапсулируется IP. Поскольку IP может передаваться по средам с разными значениями MTU, в него был встроен механизм фрагментации. Задача принимающей стороны обратно собрать фрагменты в оригинальный IP пакет.

При IP фрагментации IP пакет делится на несколько кусочков (фрагментов), оформленных таким образом, чтобы у принимающей машины была возможность их собрать в оригинальный IP пакет. Для ее работы в заголовке IP пакета используются сл. поля: адрес источника и получателя, идентификационный номер, размер пакета, смещение фрагмента и флаги: «не фрагментировать» (DF) и «у пакета еще есть фрагменты»(MF).





**23.Маршрутизация. Таблицы маршрутизации (основные компоненты, источники записей в ТМ).**

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

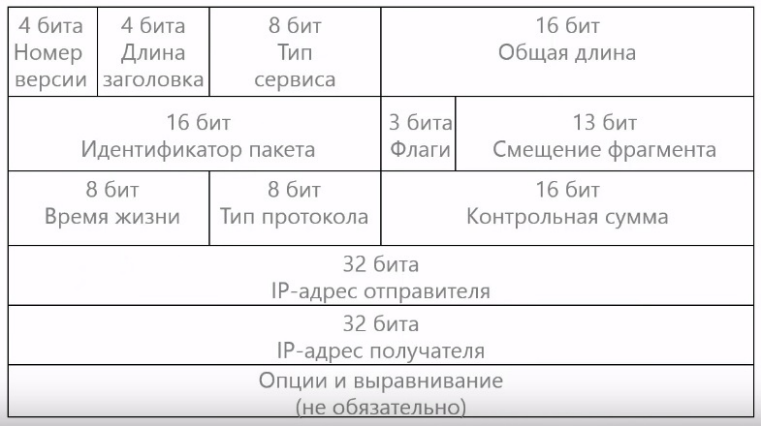
Во-вторых, программное обеспечение автоматически заносит в таблицу маршрутизации записи об адресах особого назначения.

Вторым источником появления записи в таблице является администратор, непосредственно формирующий запись 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.

**24. Маршрутизация. Маршрутизация без масок на основе классов.**



Пусть на порт маршрутизатора поступает пакет. Протокол IP извлекает из заголовка пакета адрес назначения(адрес получателя).

1. **Первая фаза просмотра** - поиск конкретного маршрута к узлу
2. IP-адрес (целиком) из заголовка пакета  последовательно строка за строкой сравниваются с содержимым поля адреса назначения таблицы маршрутизации
3. Если произошло совпадение, то из соответствующей строки извлекается адрес следующего маршрутизатора  и идентификатор входного интерфейса. На этом просмотр таблицы заканчивается.
4. Предположим теперь, что в таблице совпадения не произошло

В этом случае протокол IР переходит ко второй фазе просмотра -» поиску маршрута к сети назначения.

2. **Вторая Фаза просмотра.**

1. Из  IР адреса выделяется номер сети и, ТМ снова просматривается на предмет совпадения номера сети в какой-либо строке с номером сети из пакета
2. При совпадении из соответствующей строки таблицы и твлскаются адрес следующею маршрутизатора и идентификатор выходного интерфейса.
3. наконец. предположим, что адрес назначения в пакете был таков, что совпадения не произошло ни в первой, ни во второй фазах просмотра.

3. **Третья фаза.**

  В таком случае средствами протокола IР либо выбирается маршрут по умолчанию (и пакет направляется по адресу), либо если маршрут по умолчанию отсутствует, пакет отбрасывается.

**25.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 М2 с внешним маршрутизатором М1.

Преимущества VLSM:

* позволяет эффективно использовать адресное пространство;
* позволяет 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.

В IP-адресе такой вырожденной сети для поля номера узла как минимум должны быть отведены два двоичных разряда. Из четырех возможных комбинаций номеров узлов: 00, 01, 10 и 11 два номера имеют специальное назначение и не могут быть присвоены узлам, но оставшиеся два 10 и 01 позволяет адресовать порты для маршрутизаторов. В приведенном примере сеть была выбрана с определенным запасом – на 8 узлов. Поле номера узла в таком случае имеет три двоичных разряда, маска в десятичной нотации имеет вид 255.255.255.248, а номер сети – 129.44.192.0. Если эта сеть является локальной, то на ней могут быть расположены четыре узла помимо двух портов маршрутизаторов.

Оставшееся адресное пространство администратор может «нарезать» на разное количество сетей разного объема в зависимости от своих потребностей. Таким образом, с помощью масок переменного размера администратор всегда имеет возможность гораздо рациональнее использовать все имеющиеся у него адреса.

На рис. 8 показана схема сети, структурированной с помощью масок переменной длины.

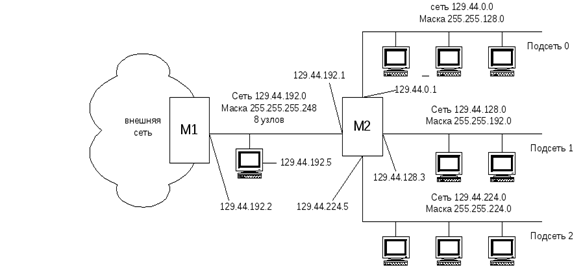


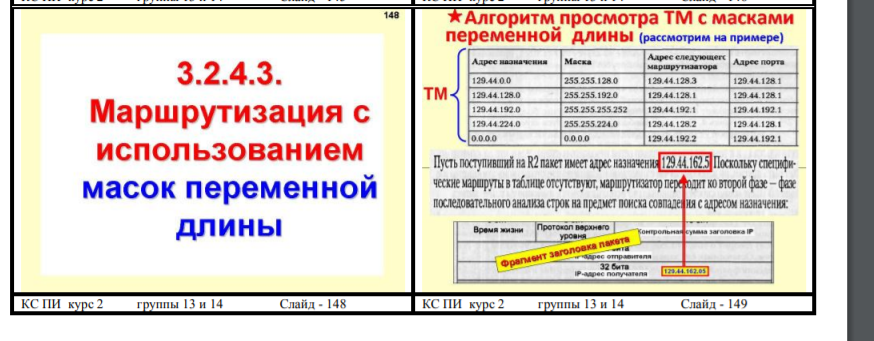
Рис. 8. Сеть, структурированная с использование масок переменной длины

Таблица маршрутизации М2, соответствующая структуре сети, показанной на рис. 2, содержит записи о четырех непосредственно подключенных сетях и запись о маршрутизаторе по умолчанию (табл. 2). Процедура поиска маршрута при использовании масок переменной длины ничем не отличается от подобной процедуры, описанной ранее для масок одинаковой длины.

Таблица 2 Таблица маршрутизатора М2 в сети с масками переменной длины

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер сети | Маска | Адрес следующего маршрутизатора | Адрес порта | Расстояние |
| 129.44.0.0 | 255.255.128.0 | 129.44.0.1 | 129.44.0.1 | Подключена | |
| 129.44.128.0 | 255.255.192.0 | 129.44.128.3 | 129.44.128.3 | Подключена | |
| 129.44.192.0 | 255.255.255.248 | 129.44.192.1 | 129.44.191.1 | Подключена | |
| 129.44.224.0 | 255.255.224.0 | 129.44.224.5 | 129.44.224.5 | Подключена | |
| 0.0.0.0 | 0.0.0.0 | 129.44.192.2 | 129.44.192.1 | --- | |

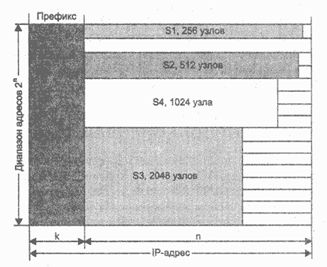
Некоторые особенности масок переменной длины проявляются при наличии так называемых «перекрытий». Под перекрытием понимается наличие нескольких маршрутов к одной и той же сети или одному и тому же узлу. В этом случае адрес сети в пришедшем пакете может совпадать с адресами подсетей, содержащихся сразу в нескольких записях таблицы маршрутизации.





**26. Технология CIDR и маршрутизация.**

 Бесклассовая адресация (англ. Classless Inter-Domain Routing, CIDR - бесклассовая междоменная маршрутизация) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.



Суть технологии CIDR заключается в следующем. Каждому поставщику услуг Internet должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого поставщика услуг имеют общую старшую часть - префикс, поэтому маршрутизация на магистралях Internet может осуществляться на основе префиксов, а не полных адресов сетей. Агрегирование адресов позволит уменьшить объем таблиц в маршрутизаторах всех уровней, а следовательно, ускорить работу маршрутизаторов и повысить пропускную способность Internet.

Деление IP-адреса на номер сети и номер узла в технологии CIDR происходит не на основе нескольких старших бит, определяющих класс сети (А, В или С), а на основе маски переменной длины, назначаемой поставщиком услуг. На рис. показан пример некоторого пространства IP-адресов, которое имеется в распоряжении гипотетического поставщика услуг. Все адреса имеют общую часть в k старших разрядах - префикс. Оставшиеся n разрядов используются для дополнения неизменяемого префикса переменной частью адреса. Диапазон имеющихся адресов в таком случае составляет 2n. Когда потребитель услуг обращается к поставщику услуг с просьбой о выделении ему некоторого количества адресов, то в имеющемся пуле адресов "вырезается" непрерывная область S1, S2, S3 или S4 соответствующего размера. Причем границы этой области выбираются такими, чтобы для нумерации требуемого числа узлов хватило некоторого числа младших разрядов, а значения всех оставшихся (старших) разрядов было одинаковым у всех адресов данного диапазона. Таким условиям могут удовлетворять только области, размер которых кратен степени двойки. А границы выделяемого участка должны быть кратны требуемому размеру.

*Предпосылки (соглы презентации):*

* Из-за несовершенства протоколов маршрутизации служебный трафик протоколов приводил к сбоям на магистральных маршрутизаторах из-за нехватки ресурсов на обработку этой служебной информации.
* Например, уже в 1994 году таблицы маршрутизации магистральных маршрутизаторов Интернета содержали до 70 000 маршрутов.
* Внедрение CIDR сократило число записей в несколько раз.
* Еще одной предпосылкой для внедрения CIDR явилась:
* -нехватка адресного пространства при дальнейшем расширении Интернета и
* -нерациональное использование адресов.

Технология CIDR успешно решает две основные задачи:

* О это экономное расходование адресов благодаря отходу от традиционной концепции разделения адресов на классы (вспомним VLSM). (Не надо забывать и о технологии NAT. Об этом позже)
* Эффективная реализация маршрутизации. Это объединение (агрегирование) маршрутов, когда одна запись в ТМ могла представлять СОТНИ маршрутов.

Повторяю. Основная идея:

* Отказ от классовой адресации, и деление IP-адреса на номера сети и узла в технологии CIDR происходит на основе маски переменной длины, назначаемой поставщиком услуг.
* Непременным условием применимости CIDR является наличие у организации, распоряжающейся адресами (например, провайдера), непрерывных диапазонов адресов.
* При таком подходе адреса всех сетей каждого провайдера имеют общую старшую часть префикс (посмотрите лаб. №5).

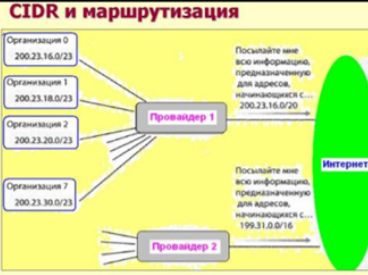
Другими словами и кратко в три предложения:

* Структуризация сети на основе масок называется разделением на подсети (subnetting).
* Вместе с тем при разделении ости на подсети помощью масок проявлялся и обратный эффект  - объединение подсетей
* Чтобы направить весь суммарный трафик адресованный из внешнего окружения в корпоративную 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.

*CIDR и маршрутизация*

Необходимым условием эффективного использования технологии CIDR является локализация адресов, то есть назначение адресов, имеющих совпадающие префиксы, сетям, располагающимся территориально по соседству.

Только в таком случае трафик реально (а не формально!) может быть агрегирован.



*CIDR. RESUME.*

Итак, внедрение технологии CIDR позволяет решить две основные задачи.

Более экономное расходование адресного пространства Благодаря технологии CIDR поставщики услуг получают возможность «нарезать» блоки из выделенного им адресного пространства в точном соответствии с требованиями каждого клиента, при этом у клиента остается пространство для маневра на случай будущего роста

Уменьшение числа записей в таблицах маршрутизации за счет объединения маршрутов - одна запись в таблице маршрутизации может представлять большое количество сетей. Если все поставщики услуг Интернета начнут придерживаться стратеги и CIDR, то особенно заметный выигрыш будет достигаться в магистральных маршрутизаторах.

Необходимым условием эффективного использования технологии CIDR является локализация адресов, то есть назначение адресов имеющих совпадающие префиксы, сетям, располагающимся территориально по соседству. Только в таком случае трафик может быть агрегирован.

Замечание

*Суть технологии CIDR заключается в следующем:*

* Каждому поставщику услуг Интернета назначается непрерывный диапазон IP-адресов.
* При таком подходе все адреса каждого поставщика услуг имеют общую старшую часть - префикс, поэтому маршрутизация на магистралях Интернета может осуществляться на основе префиксов, а не полных адресов сетей.
* А это значит, что вместо множества записей по числу сетей будет достаточно поместить одну запись сразу для всех сетей, имеющих общий префикс.
* Такое агрегирование адресов позволит уменьшить объем таблиц в маршрутизаторах всех уровней, а следовательно, ускорить работу маршрутизаторов и повысить пропускную способность Интернета.



**27. Трансляция сетевых адресов. (Технологии NAT, NAPT).**

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 получателя.

* 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.
* Одна из причин популярности технологии NAT это дефицит IP-адресов.
* Если сеть фирмы автономна, то в ней могут быть использованы любые IP-адреса, лишь бы правильно были записаны.
* Совпадение адресов в не связанных между собой сетях не вызовет проблем.
* Однако, если сети подключены к Интернет, то необходимы глобальные IP-адреса. Их уникальность гарантирована ICANN.

Одна из причин популярности технология NAT это дефицит IP-адресов. Если сеть фирмы автонсима, то в ней могут быть использованы IP-адреса, лишь бы правильно были записаны. Совпадение адресов в не связанных между собой сетях не вызовет проблем

Однако, если сети подключены к Интернет, то необходимы глобальные IP-адреса. Их уникальность гарантирована ICANN

Если фирме не удается получить у провайдера нужного числа глобальных IP-адресов, то можно прибегнуть к технологии NAT.

В этом случае для адресации внутренних адресов зарезервированы частные адреса:

10.0.0.0 - 10.255.255.255

172. 16.0.0 - 172. 31.255.255

192. 168. 0.0 - 192. 168. 255. 255

Пакеты с такими адресами будут проигнорированы маршрутизаторами на магистралях Internet. Как быть ?

Для того, чтобы узлы с частными адресами могли связываться через Интернет необходимо использовать технологию NAT.

* Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством маршрутизатором, сервером доступа, межсетевым экраном (говорят NAT-устройство).
* Суть механизма состоит в замене адреса источника (source) при прохождении пакета в одну сторону и обратной замене адреса назначения (destination) в ответном пакете.
* Наряду с адресами source/destination могут также заменяться номера портов source/destination.

*NAT выполняет две важных функции:*

1. Позволяет сэкономить IP-адреса, транслируя несколько внутренних IP- адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних).
2. \* Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, но оставляя возможность обращения изнутри наружу.

