

Лекция 2

Методы адресации узлов сети

Вопросы:

1. Виды адресации узлов сети
2. Протоколы разрешения адресов. Протокол ARP
3. Локальные адреса
4. IPv4-адреса. Классы. Маски
5. Диапазоны IPv4-адресов. Назначение IP-адресов
6. IPv6-адреса. Форма записи
7. Типы IPv6-адресов
8. Символьные адреса

[вопрос 1]

Требования к адресам узлов сети:

1. Адрес должен уникально идентифицировать компьютер в сети любого масштаба.
2. Схема назначения адресов должна быть удобной
3. Адрес должен иметь иерархическую структуру, удобную для построения больших сетей.
4. Адрес должен быть удобен для пользователей сети, т.е. должен иметь символьное представление.
5. Адрес должен иметь компактное представление, чтобы не перегружать память коммуникационной аппаратуры, маршрутизаторов и т.п.

Для доступа в сеть, компьютерам надо назначать адреса. Делают это или сисадмин или DHCP. Администратор должен удобно работать с назначением адресов, поэтому схема назначения должна быть удобной.

Адрес должен иметь иерархическую структуру. Если сеть большая, то пользователи могут начать называть свои компьютеры одинаково (Михайл-PC 😊), для того чтобы этого не случилось, используется иерархия. Вспоминаем наши реальные адреса: страна, город, дом и т.д. Это иерархическая система. Иногда улицы называются одинаково, но располагаются в разных городах. Тем не менее адрес остается уникальным благодаря этой иерархии. Также и в компьютерных сетях. Если мы разделим адреса на уровни, администратору будет удобно работать с настройкой всей сети.

Адреса должны быть удобны и пользователю. К примеру www.microsoft.com.

Адреса не должны занимать много памяти. И наконец адреса постоянно передаются. Когда мы передаем пакет вместе с ним передается адрес получателя и адрес отправителя (как в письмах). Если адрес будет использовать много памяти, это негативно скажется на скорости КС.

Адресное пространство – это множество всех адресов, допустимых в рамках некоторой схемы адресации

Всего существует 2^{32} адресов (если IPv4), так как адрес занимает 32 бита. Адресное пространство может быть плоское, если нет иерархии. А если иерархия есть, то это иерархическое адресное пространство.

Каждый современный ПК можно подключить в несколько сетей. Компьютер один, но он имеет несколько сетевых интерфейсов. Например интерфейс для неэкранированной витой пары(Ethernet), интерфейс Wi-Fi, Bluetooth-интерфейс. По количеству адресуемых сетевых интерфейсов можно классифицировать адреса.

Например:

1. Уникальный адрес (Unicast) – используется для идентификации одного интерфейса конечного узла или маршрутизатора. Позволяет пересыпалть сообщения в одну точку (на один интерфейс)
2. Групповой адрес (Multicast) задает группу интерфейсов. Данные доставляются каждому адресу. Позволяет отсылать что-либо целой группе компьютеров.
3. Широковещательный адрес (Broadcast). Обычно такой адрес состоит из всех двоичных единиц. Например 255.255.255.255 (255 это 11111111). Если с компьютера в локальной сети отправить такой пакет, то его получат все узлы сети. Это и есть широковещательный адрес.
4. Адрес произвольной рассылки (anycast) – похожи на Multicast, но информация доставляется не всем членам группы, а одному, обычно ближайшему. То есть это как группа anycast, но информация доходит только к одному узлу.

[вопрос 2]

Протоколы разрешения адресов – специальные протоколы, используемые для преобразования из одного типа в другой.

Используются два подхода к разрешению адресов:

- Централизованный
- Распределенный

Централизованные протоколы

Используются в крупных сетях.

В сети выделяется компьютер-сервер, на котором хранится база соответствия адресов, все клиенты обращаются к серверу по мере необходимости.

Например, протокол **DNS (Domain Name System)** – преобразует доменное имя в IP-адрес. Используется в Интернете.

Распределенные протоколы

Используются в небольших сетях.

Каждый узел сам решает задачу установления соответствия между адресами. Для этого применяются широковещательные запросы.

Например, протокол разрешения адреса **ARP**.

Почему их называют распределенным протоколом? Они не относятся к серверу

Что это значит? Это значит, что сервера нету и нужно опрашивать все узлы. Узел, которому нужно узнать адрес, будет опрашивать все узлы в сети. В интернете, к примеру, можно всех спросить? Конечно нельзя. Поэтому такой подход нельзя использовать в крупных сетях, только в локальных. В качестве примера таких протоколов рассмотрим ARP.

Протокол ARP

ARP (Address Resolution Protocol) – используется стеком TCP/IP для преобразования IP-адреса в аппаратный адрес.

Необходимость обращения к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet.

Это протокол, предназначенный для преобразования IP-адреса в MAC-адрес. То есть каждый раз, когда узлу приходит пакет, или маршрутизатору приходит пакет и его надо передать в локальной сети, узел начинает решать эту проблему с помощью ARP протокола.

Работа ARP протокола начинается с таблички, которую можно получить при помощи команды

➤ `arp -a`

Статические строчки хранятся в таблице постоянно, а динамические постоянно изменяются. То есть вид таблицы зависит от активности в сети. Табличка ARP еще называют ARP-кэш

Если мы просмотрим ARP-кэш и там есть нужный IP-адрес, то мы можем туда передать пакет. Но если его там нет? Тогда выполняются широковещательные запросы всем узлам подсети.

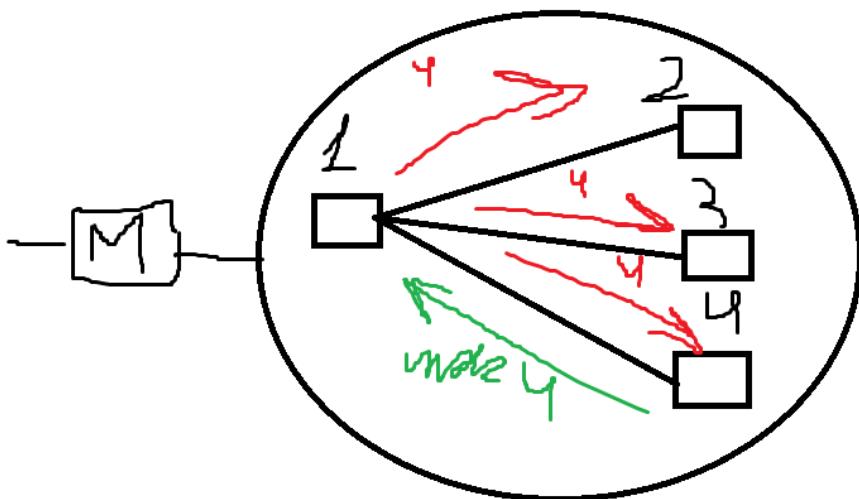
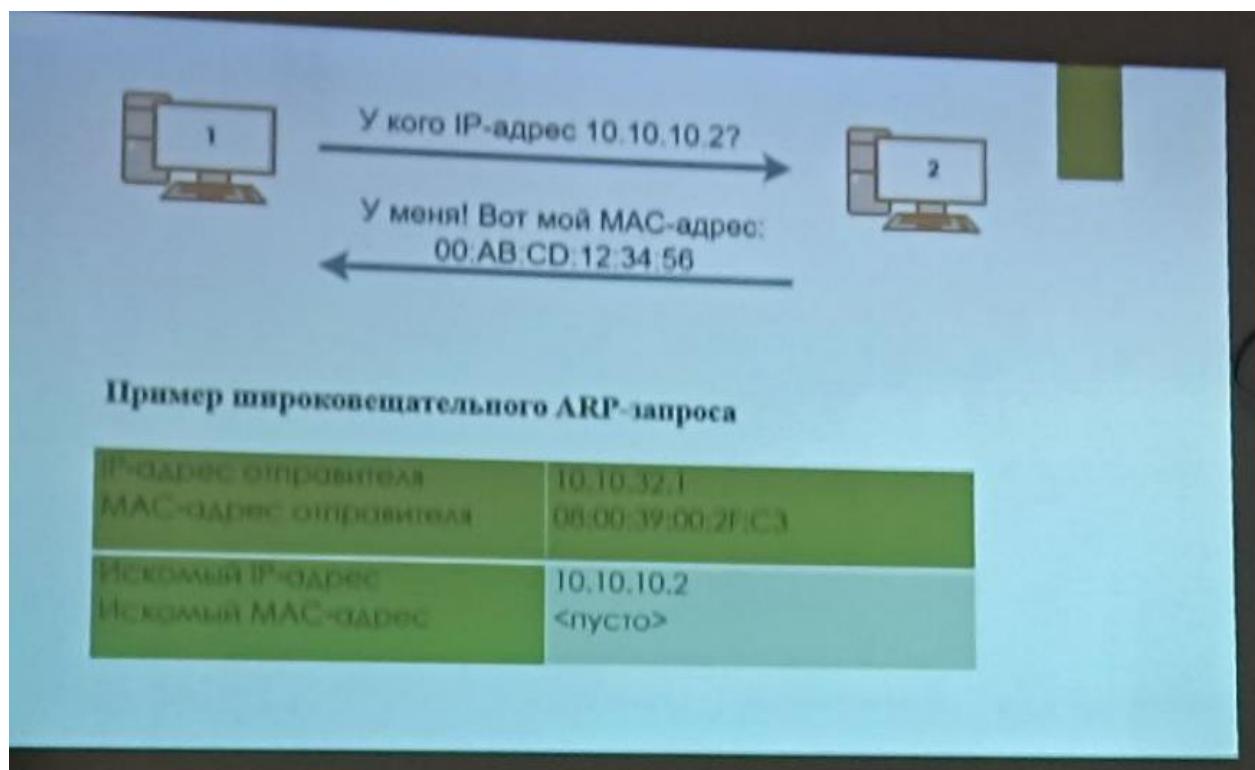


Рисунок 1 – Работа широковещательного запроса

1-ый отправляет широковещательный запрос всем узлам и если одна из машин узнает свой IP-адрес в запросе, то отправит свой MAC в ответ на машину 1.



[вопрос 3]

У любого компьютера в сети есть эти адреса:

- Локальные адреса
- Числовые составные адреса
- Символьные адреса или имена

Начнем мы с вами с локальных адресов. Их еще называют mac-адреса или физическими адресами. Эти адреса имеют плоское адресное пространство

А локальные сегменты у нас строятся на одной сетевой технологии. Мы можем сказать, что локальный адрес, это такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети.

Локальный адрес – такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной сети.

Подсеть – совокупность хостов, которые взаимодействуют друг с другом не прибегая к маршрутизации. Подсети объединяются в сеть с помощью маршрутизаторов

В разных подсетях допустимы различные сетевые технологии. Поэтому существуют разные типы локальных адресов.

Для ЛВС локальный адрес – это **MAC-адрес (Media Access Control)** сетевого адаптера Ethernet. Его записывают в ПЗУ платы сетевого адаптера на заводе изготовителе. При замене сетевого адаптера изменяется аппаратный адрес.

Например: **11-A0-17-3D-BC-01**

У одного узла может быть несколько сетевых интерфейсов и, следовательно, несколько аппаратных адресов.

[вопрос 4]

Числовые адреса

Следующий тип адресов, это числовые адреса (IPv4)

Физические адреса у нас только внутри подсети, а через маршрутизатор нужны IPv4, например в другую подсеть. Числовых адресов много, но в данный момент доминирующая технология – TCP/IP. Поэтому мы рассматриваем IPv4.

IP их называют, потому что они используются для передачи пакетов между подсетями и для доступа в интернет (Ip = internet protocol). Они назначаются конечным узлам и маршрутизаторам. IP адресов у узла может быть столько, сколько существует сетевых подключений. И у маршрутизатора может быть много сетевых интерфейсов, поэтому сколько у него интерфейсов, столько может быть IP-адресов. IP протокол мы позже будем подробно изучать, пока только адреса. IP протокол используется в двух версиях – IPv4 и IPv6. Начинаем с более старого, IPv4. Это 32-битный адрес или 4-байтный. Такие адреса записываются в точечно-десятичной нотации. Записываются 4 числа записанные через точку. Но поскольку это 1 байт, то есть ограничение доступных чисел 0-255. Каждое число в IPv4 адресе может быть от 0 до 255.

Например: 145.10.34.3. Когда мы смотрим на такой адрес, мы видим 4 части, но на самом деле там не 4 части, просто 4 числа. Такой адрес состоит из 2 логических частей – Номер сети и Номер узла.

Номер сети есть ID узла, но вот номер сети также называют сетевым префиксом.

Сетевой префикс идентифицирует сетевой интерфейс данного устройства.

[вопрос 5]

Разработчики придумали делить адреса на **классы**: А, В, С, D, Е. По классу можно определять какая часть адреса относится к номеру сети, а какая к номеру узла.

Сам класс определяется по первым видам адреса. Если адрес записать в двоичном виде, то тогда по началу адреса можно понять, что это за класс.

Еще один термин — это **пул адресов**. Если у нас, например адрес узла 172.16.0.1, то пул адресов таков:

172.16.0.1 – 172.16.255.254

Почему в конце не 255, потому что если будет 255, то это уже называется широковещательный адрес.



Если мы записали первое число в двоичном виде и увидели, что в первом бите **0**, то адрес относится к классу **A**. Это будет означать, что первый байт — это номер сети, а остальные 3 байта — это номер узла. Следовательно, номеров для сети мало, а для узлов много.

Если адрес начинается на **10**, то это адрес класса **B** и тогда он делится по полам. Два байта на номер сети и два байта номер узла. Но из номера сетей исключаются 2 первых бита. Из-за этого

у нас получается не 2^{16} возможный номеров сетей, а только 2^{14} . А номеров узлов в классе В 2^{16} адресов.

В классе **C** начинается адрес с **110**. В такой сети 3 байта на номера сети и 1 байт на номера узлов.

Если у нас **1110**, то адрес относится к классу **D**, то такой адрес вообще не делится на номер сети и номер узла. Это **групповой multicast** адрес.

Ну и наконец класс **E** это **1111** зарезервирован для специальных целей и не используется пользователями.

Максимальное количество сетей класса A: $2^7 - 2 = 126$

Максимальное число узлов в сети класса A: $2^{24} - 2 = 16\ 777\ 214$

Например 102.56.187.5

Максимальное количество сетей класса B: $2^{14} - 2 = 16382$

Максимальное число узлов в сети класса B: $2^{16} - 2 = 65534$

Например 129.16.87.52

Максимальное количество сетей класса C: $2^{21} - 2 = 2\ 097\ 152$

Например 197.116.73.1

Класс **D** не делится на номер сети и номер узла и идентифицирует группу узлов, которые могут принадлежать подсетям.

Также, например, нету адреса **127.0.0.0**, то бишь адреса класса A, ибо это есть **локальный адрес** для узла.

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

Деление по классу, это устаревшее деление, которое практически уже не используется. Поэтому мы используем уже **Маску**. **Маска** нужна для определения, где в адресе номер сети, а где номер узла. Поэтому маска — это число, которое используется в паре с IP адресом и содержит двоичные единицы в тех байтах, которые в IP адресе интерпретируются как номер сети. Где единички, там номер сети. Где ноль, там номер узлов.

Если мы просто запишем адрес и маску в паре, мы увидим, где номер сети, а где номер узлов.

IP адрес AND маска = Номер сети

(AND – логическое умножение)

Пример: IP адрес 129.64.134.5, маска 255.255.128.0

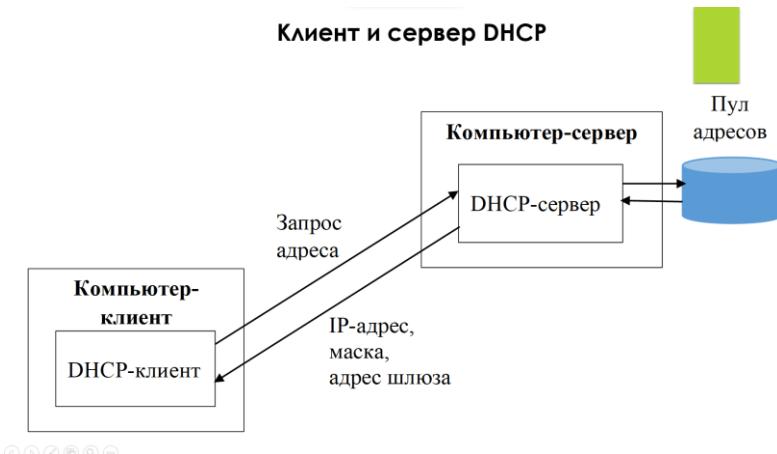
В двоичном виде:

IP адрес: 10000001.01000000.10000110.00000101

Маска: 11111111.11111111.10000000.00000000

Номер сети: 129.64.128.0 Номер узла: 0.0.6.5

Как можно назначить адрес компьютеру? Можно просто подключить в сеть и получить адрес от DHCP – автоматически



Можно и вручную назначить через специальное окно, но тогда адрес будет статический и будет сохраняться в сети постоянно.

Но это не всегда удобно, например когда мы подключаемся к сети временно. Тогда есть способ назначить IP-адрес автоматически. Такой адрес будет динамический и будет сохраняться до отсоединения узла от сети. Следующий раз подключитесь, вам может быть выдан другой IP-адрес. Чтобы это сделать есть специальный протокол DHCP.

Индивидуальные Адреса IPv4 (Unicast) делятся на:

1. Частные адреса
2. Публичные адреса
3. Специальные адреса

Частные адреса

Может быть ситуация, когда DHCP недоступен. Вышел из строя или сетевое подключение нарушено. И ваш компьютер, настроенный на автоматическую конфигурацию, не может получить IP.

Тогда есть адреса **APIPA (Automatic Private IP Addressing)**

Такие адреса по умолчанию назначаются всем сетевым подключениям в случае недоступности DHCP-сервера.

Частные адреса APIPA расположены в диапазоне от 169.254.0.1 до 169.254.255.254. Маска подсети 255.255.0.0.

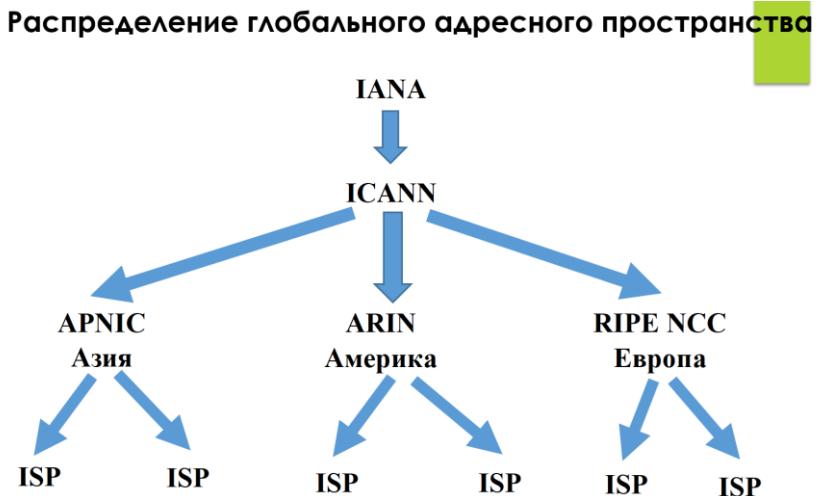
Помимо адресов для доступа в интернет, если и частные адреса, которые не обрабатываются маршрутизатором для доступа в интернет. **Такие адреса называются частные.**

Публичные адреса

Каждый публичный адрес должен быть уникален. Если у нас в сети интернет будут отличаться адреса, то невозможно будет передавать данные между компьютерами в сети интернет. Кто-то должен контролировать эту уникальность.

Распределение адресов в интернет курирует **IANA (Internet Assigned Numbers Authority)**.

А главный орган регистрации глобальных адресов называется ICANN. Но она сама не занимается этим. Она отдает некоторый пул каждому региону: APNIC, ARIN, RIPE NCC. Они тоже не занимаются этим, они делят этот пул между провайдерами, и провайдеры уже делят их между узлами.



Частные адреса, это те адреса которые IANA исключила из публичного пула адресов. Это такие адреса

Диапазоны частных адресов:

Класс	Начальный адрес	Конечный адрес
A	10.0.0.0/8	10.255.255.254
B	172.16.0.0/16	172.31.255.254 (16 номеров сетей)
C	192.168.0.0/24	192.168.255.254 (255 сетей)

Специальные адреса

Есть адреса, которые не АРIPA, не частные и не публичные. Они выделены для специальных нужд.

Первый адрес – **0.0.0.0**. Такой адрес означает все сетевые интерфейсы сетевого узла. Ну или **основной шлюз**. В IPv6 – “::”

Когда такой адрес можно использовать? Вот вы будете разрабатывать СОМ-приложение. Сервер у вас будет слушать клиент по определенному адресу. Но вы постоянно переподключаетесь. Тогда какой адрес должен сервер слушать? Вот как раз этот адрес. Тогда сервер будет слушать все адреса, поступающие к нему. Так делать не безопасно, но для нашего учебного материала этого будет достаточно.

Если номер сети равен нулю, то считается что узел назначения принадлежит к той же самой сети, что и узел-отправитель.

Следующий адрес **255.255.255.255** это, наоборот, адрес, целиком состоящий из единиц. Такой адрес называют **ограниченным широковещательным сообщением**. Если мы передаем пакет с таким адресом узла-назначения, то его получат все узлы сети. Но маршрутизатор его не передаст. Поэтому это и ограниченный широковещательный запрос.

Еще один адрес - направленное широковещательное сообщение.

В поле “номер узла назначения” все двоичные единицы

Например: 192.168.21.255 с маской 255.255.255.0

Это значит, что запрос найдет сеть 192.168.21.*^{***} и туда всем узлам отправит широковещательный запрос.

Если поле номера узла содержит все нули, это пул адресов

Например: 129.36.0.0/16

Адреса, значение первого байта которых превышает 223 **не могут использоваться качестве номера узла**

[Вопрос 6]

IPv6-адреса. Форма записи

Если мы изначально рационально использовали адреса IPv4, то до сих пор мы пользовались как раз четвертой версией. Но в 90-ые годы произошла интернет-революция, то есть интернет начал быстро расти.

В течении буквально нескольких лет объем узлов в интернете значительно вырос и IPv4 стало не хватать, тогда-то начали работать над шестой версией

Для этих адресов решили сразу взять 16 байтов адресного пространства или же 128 бит. Решили закрыть вопрос с достатком адресов навсегда.

Давайте сравним их адресное пространство:

- Размер IPv6-адреса 128-бит (16 байт)
- Адресное пространство IPv4 – 2^{32} (4,3 млрд возможных адресов).
- Адресное пространство IPv6 – 2^{128}

$340\ 282\ 366\ 920\ 938\ 463\ 463\ 374\ 607\ 431\ 768\ 211\ 456$ ($3,4 \times 10^{38}$)

10^7 степени IP-адресов на $1m^2$ земной площади

Давайте разберём как они записываются:

IPv6 адрес записывается в шестнадцатеричном виде.

- 8 групп по 4 16-ричных цифры. Для разделения групп используется двоеточие

Например: 2001:D0B8:000:000:000:4567:89AB:CDEF

- Если одна или более групп подряд равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::). Такой пропуск должен быть единственным в адресе.

Например: 2001:D0B8::4567:89AB:CDEF

Адрес 0000:0000:0000:0000:0000:0000:AE21:0D12 можно сократить до ::AE21:0D12

- Можно опускать незначащие нули в начале каждой группы.

Например: вместо 00B8 записать B8

Поговорим про назначение

IPv6 адреса конечных узлов всегда по умолчанию имеют:

- 64 бита – номер сети
- 64 бита – номер узла

Маска для IPv6-адреса записывается в представлении с косой чертой

Например: 2001:DB8:3FA9::/48

Версия IPv6 не использует широковещание в сети. Вместо этого применяется групповая передача

IPv6-адреса обычно конфигурируются автоматически. Компьютеры могут получать IPv6-адреса от соседних маршрутизаторов или от DHCPv6-серверов.

Кроме того, компьютеры сами автоматически назначают себе IPv6 адрес для использования исключительно в локальной подсети.

[Вопрос 7]

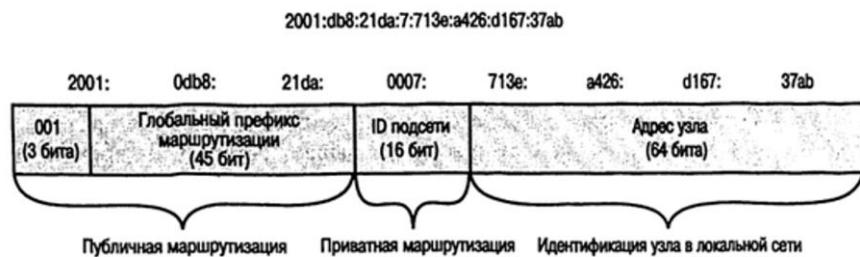
IPv6-адреса делятся на:

- 1) Глобальные адреса
- 2) Канальные адреса
- 3) Уникальные локальные адреса

Глобальные адреса

Глобальные адреса применяются в IPv6 интернете (В интернете есть IPv4 участки и IPv6). Чтобы эти адреса определить используется префикс 001 или маска 3 -> 001::/3

Если мы будем записывать в шестнадцатеричном виде то получим адреса от 2000 до 3FFF



Как видно, ip делится вроде как пополам: 64 бита номер сети и 64 бита узла. Вот он префикс – 001 или же 3 бита. Дальше может идти глобальный префикс маршрутизации 45 бит, потом ID подсети 16 бит и потом адрес узла 64 бита.

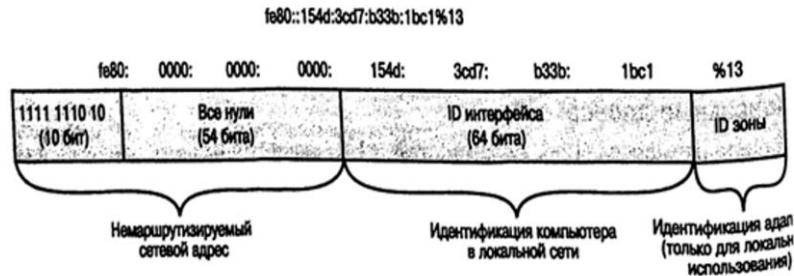
Канальные адреса IPv6.

Они аналогичны адресам APIPA, только тут они называются LLA. Они используются только внутри локальной сети. Причем такой адрес конфигурируется автоматически и назначается интерфейсу даже если интерфейсу вписывается адрес вручную. На всякий случай, чтобы узлы себя видели в локальной сети

Как его узнать? Он всегда начинается с **fe80**.

И еще один момент. У него в конце стоит "% 13" в данном случае. Это так называемый идентификатор зоны. Он не относится к 128 битам адреса. Почему он появляется? Потому что номер сети у всех этих адресов одинаковый (fe80). То есть они в одной сети. Но локальная сеть может иметь более сложную структуру, и мы получается не можем обращаться в конкретные подсети. Поэтому независимо от нас сеть делится на некие зоны и присваивается этот идентификатор зоны. Единственное, где может понадобится этот идентификатор зоны, это только

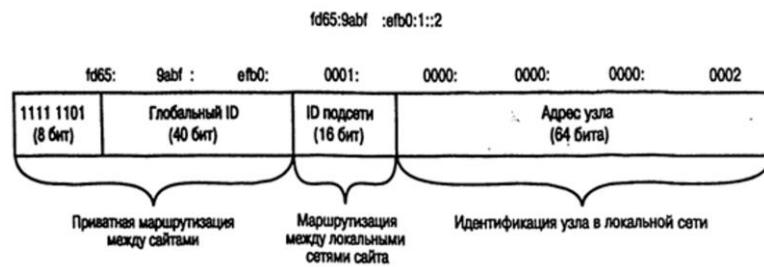
в том случае если мы пингуем соседний компьютер по адресу с идентификатором зоны, то мы указываем идентификатор зоны своего компьютера.



У него вот 10 бит это fe80 в начале. Потому 54 бита нулей ибо в такой сети нету маршрутизации. А потом номер узла 64 бита и в конце ID зоны не входящий в адрес.

Уникальные локальные адреса (ULA)

Это адреса аналогичные частным адресам IPv4. Эти адреса только внутри частной сети могут использоваться и в интернете не обрабатываются. Но частная сеть может быть крупной и в нём могут быть свои маршрутизаторы. Так вот эти адреса внутри частной сети позволяют выполнять маршрутизацию внутри. Узнать их можно по началу "fd". Но номер сети у них есть, поэтому могут быть fd65, fd22 и так далее.



Видите? Вот начало 8 бит – fd, а дальше идет глобальный ID – 40 бит, ID подсети – 16 бит и адрес узла – 54 бита.

Вот собственно вся информация, которую мы изучаем по адресам. Остались у нас только символьные адреса. Про это мы еще будем говорить подробно. Пока только некая вводная информация

[Вопрос 8]

Во-первых, символьные адреса могут использоваться в любых сетях. Символьные адреса предназначены только для удобства пользователя. Поэтому они желательно несут смысловую нагрузку, чтобы человек мог их запомнить. Эти адреса тоже имеют иерархическую структуру.

Примеры таких адресов:

1. UNC адреса: \\pv1-server\ДП2019\Правила_оформления.doc
2. DNS адреса: 219-3.povt.fitr.bntu.by
3. URI адреса: <ftp://ftp.ncsa.uiuc.edu/Mac/Mosaic>