IP-адресация, классы сетей, подсети, суперсети.

Ссылки

- RFC1180 – A TCP/IP Tutorial.
- RFC1918 – Address Allocation for Private Internets.

Registry	Area Covered
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

- При подключении к Internet необходимо получить идентификатор сети или у провайдера Internet, или в организации IANA (http://www.iana.org/numbers) у одного из пяти региональных операторов.
- Для нашего региона идентификаторы IPv4, IPv6 и ASN можно получить у RIPE NCC (https://www.ripe.net/).
- Вопросами распределения DNS имен для Латвии занимается Latnet (http://www.nic.lv/)

1. IP-адреса

Каждый узел TCP/IP идентифицируется логическим IP-адресом. Эти адреса уникальны для каждого из узлов, общающихся по протоколу TCP/IP. Каждый 32-битный IP-адрес идентифицирует местонахождение узла в сети точно так же, как обычный адрес обозначает дом на улице города.

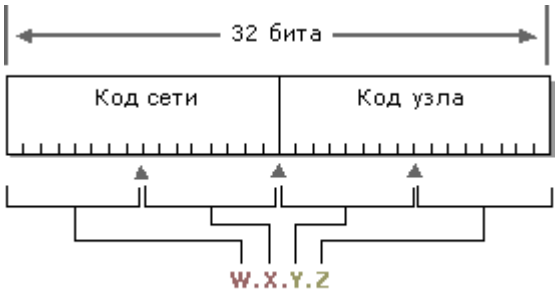
Аналогично обычному адресу, состоящему из двух основных частей (названия улицы и номера дома), IP-адрес также имеет **две части** – код (идентификатор) **сети** и код (идентификатор) **узла**.

- **Код сети**, также называемый адресом сети, обозначает один сетевой сегмент в более крупной объединенной сети (сети сетей), использующей протокол TCP/IP. IP-адреса всех систем, подключенных к одной сети, имеют один и тот же код сети. Этот код также используется для уникального обозначения каждой сети в более крупной объединенной сети.
- **Код узла**, также называемый адресом узла, идентифицирует узел TCP/IP (рабочую станцию, сервер, маршрутизатор или другое TCP/IP-устройство) в пределах одной сети. Код узла уникальным образом обозначает систему в том сегменте сети, к которой она подключена.

Вот пример 32-битного IP-адреса: 10000011 01101011 00010000 11001000

Для облегчения восприятия человеком IP-адреса записываются в точечно-десятичной нотации. 32-битный IP-адрес делится на четыре 8-битных октета. Октеты представляются в десятичной системе счисления (системе с основанием 10) и разделяются точками. Таким образом вышеприведенный IP-адрес в точечно-десятичной нотации выглядит так: 131.107.16.200.

На следующем рисунке показан пример IP-адреса (131.107.16.200), разделенного на код сети и код узла. Часть, соответствующая коду сети (131.107), в данном случае определяется первыми двумя октетами IP-адреса. Часть, задающая код узла (16.200), обозначается последними двумя октетами IP-адреса.

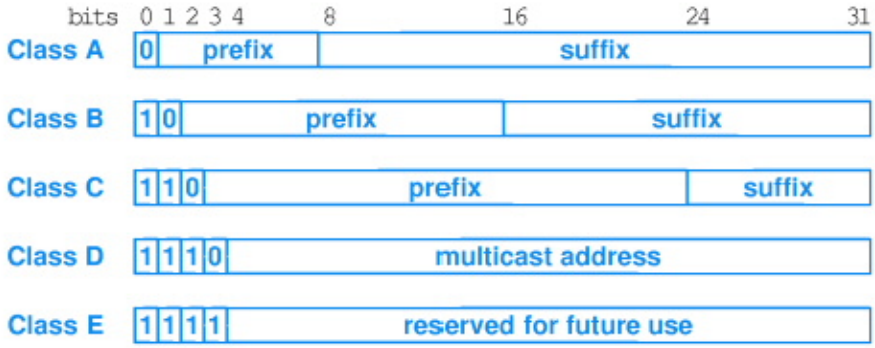


Пример: 131.107.16.200

- Поскольку IP-адреса служат для идентификации устройств в сети, каждому устройству в сети должен быть назначен **уникальный** IP-адрес.
- Многие компьютеры имеют только один сетевой адаптер, поэтому им требуется лишь один IP-адрес. Если же в компьютере установлено несколько сетевых адаптеров, то каждому из них должен быть назначен свой IP-адрес.
- Маршрутизаторы имеют не менее двух сетевых интерфейсов.

2. Классы IP-адресов (традиционные)

Сообщество Интернета определило пять классов IP-адресов — A, B, C, D и E. Адреса классов A, B и C могут назначаться узлам TCP/IP, а также существуют нераспределенные и специальные адреса. Дополнительно о распределении адресов см. на IANA IP Address Allocations http://www.iana.org/numbers.



Класс адреса задает число бит в адресе, которые отводятся под коды сети и узла. Тем самым, класс адреса определяет и то, сколько всего может быть сетей данного класса и узлов в каждой из этих сетей.

В следующей таблице символы *w.x.y.z* обозначают четыре октета IP-адреса. Эта таблица показывает:

- как значение первого октета (w) любого IP-адреса задает класс этого адреса;
- как октеты адреса данного класса делятся на код сети и код узла;
- число возможных сетей данного класса и число узлов в этих сетях.

Таблица 1. Классы IP-адресов

Класс сети	Значение w	Начало w	Код сети, диапазон	Код узла, диапазон	Число сетей [расчет]	Число узлов [расчет]
A	1–126	0	w. 1-126 (127 зарезервирован)	x.y.z 0.0.1-255.255.254	126 $[2^{(8-1)}-2]$	16 777 214 $(2^{24}-2)$
B	128–191	10	w.x. 128.1-191.255	y.z 0.1-255.254	16 382 $[2^{(16-2)}-2]$	65 534 $(2^{16}-2)$
C	192–223	110	w.x.y. 192.0.1-223.255.255	z 1-254	2 097 150 $[2^{(24-3)}-2]$	254 $(2^{8}-2)$
D	224–239	1110	w.x.y.z (multicasting group ID) 224.0.0.0-239.255.255.255	Неприменимо	268 435 456 $[2^{(32-4)}]$	Неприменимо
E	240–247	11110	240.0.0.0-247.255.255.255 Зарезервировано для экспериментальных целей	Неприменимо	Неприменимо	Неприменимо
	248-254	11111	Не распределено ни в один из классов	Неприменимо	Неприменимо	Неприменимо

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

3. Правила назначения IP-адресов.

Необходимо учитывать некоторые особые адреса, при выборе корректных идентификаторов для узлов и сетей, см. http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml :

Prefix	Suffix	Type Of Address	Purpose
all-0s	all-0s	this computer	used during bootstrap
network	all-0s	network	identifies a network
network	all-1s	directed broadcast	broadcast on specified net
all-1s	all-1s	limited broadcast	broadcast on local net
127	any	loopback	testing

- ***Идентификатор сети не может равняться 127*** (loopback), например, 127.0.0.1. Это значение зарезервировано для ***локальной заглушки*** и используется для диагностики стека TCP/IP с исключением из петли сетевой карты, а значит физического и канального уровней модели ISO-OSI.
- ***Все биты идентификатора сети и узла равняются нулю***, например, 0.0.0.0. Такой идентификатор называется неопределенным адресом и обозначает адрес того узла, который сгенерировал этот пакет. Адрес такого вида в особых случаях помещается в заголовок IP-пакета в поле адреса отправителя.
- ***Все биты идентификатора сети и узла равняются единице***, например, 255.255.255.255. Такой идентификатор означает ***все узлы в данной IP-сети*** (локальном сегменте).
- ***Все биты идентификатора узла равняются нулю***, например, 172.20.0.0. Такой идентификатор означает ***указанную IP-сеть*** (локальную или удаленную) и применяется для ссылок на всю IP-сеть в целом.
- ***Все биты идентификатора узла равняются единице*** (broadcast), например, 172.20.255.255. Такой идентификатор означает ***все узлы в указанной IP-сети*** (локальной или удаленной) и применяется для широковещательных сообщений в указанной IP-сети.
- ***Все биты идентификатора сети равняются нулю***, например, 0.0.0.130. Такой идентификатор означает ***конкретный узел в данной IP-сети*** (локальной).
- Адреса начинающиеся с ***248 – 254*** (***Unallocated IP Addresses***) считаются не распределенными ни в один из классов и не могут использоваться.
- Для взаимодействия друг с другом все узлы одной физической сети должны иметь одинаковый идентификатор сети (подсети);
- Если физическая сеть разделена маршрутизатором, то она разбита на подсети и для каждой нужен свой идентификатор сети (подсети);
- Каждый идентификатор узла должен быть уникален для соответствующего идентификатора сети (подсети).

4. Изолированные (частные) сети TCP/IP и адреса сетей для примеров.

4.1. Изолированные сети.

Для частных TCP/IP-сетей, которые ***не подключены к Интернету***, можно использовать любой допустимый диапазон IP-адресов классов A, B или C. Вы вольны использовать любые корректные IP-адреса, но, всё-таки рекомендуется использовать специально выделенные диапазоны адресов.

Для частных TCP/IP-сетей, которые ***подключены к Интернету не напрямую***, а с помощью преобразователя сетевых адресов (NAT) или шлюза уровня приложения, например прокси-сервера, **настоятельно** рекомендуется использовать частные IP-адреса.

Для любых узлов локальной сети, ***непосредственно подключаемых к Интернету***, необходимо получить у поставщика услуг Интернета зарегистрированные общие (не частные) IP-адреса.

По соображениям безопасности не рекомендуется подключать к Интернету большое количество систем TCP/IP из локальной сети напрямую, нужно использовать NAT.

Пространство IP-адресов, предназначенных для использования в изолированных сетях было определено в RFC1918 – Address Allocation for Private Internets, February 1996. Эти диапазоны адресов зарезервированы организацией ***IANA*** (Internet Assigned Numbers Authority — http://www.iana.org/) для частных TCP/IP-сетей и не используются в Интернете (одна сеть класса A, 16 сетей класса B и 256 сетей класса C).

Обновлённый (более обширный) список подсетей специального назначения определён в RFC 6890.

Таблица 2. Частные IP-адреса

ID изолированной сети		Маска подсети	Диапазон IP-адресов	Префиксная нотация
10.0.0.0	(CIDR)	255.0.0.0	10.0.0.1 – 10.255.255.254	10/8
100.64.0.0	(CG NAT)	255.192.0.0	100.64.0.1 – 100.127.255.254	100.64/10
172.16.0.0	(CIDR)	255.240.0.0	172.16.0.1 – 172.31.255.254	172.16/12
192.168.0.0	(CIDR)	255.255.0.0	192.168.0.1 – 192.168.255.254	192.168/16
169.254.0.0	(APIPA)	255.255.0.0	169.254.0.1 – 169.254.255.254	169.254/16
fc00::	(CIDR)	IPv6		fc00::/7

CGN – Carrier-Grade NAT. Подсеть рекомендована для использования в сетях сервис-провайдера в качестве адресов Shared Address Space согласно RFC 6598.

APIPA - Automatic Private IP Addressing. Автоматическая IP-адресация применяется если сетевой интерфейс настроен для автоматической IP-конфигурации по DHCP, но при этом в сети отсутствует сервер DHCP.

4.2. Диапазоны адресов для примеров в документах.

Назначение: даже если читатель бездумно введет адреса из примеров в конфигурацию живой сети, это не приведет к глобальному конфликту.

В IPv6 выделен один блок побольше, и авторы сами могут раскроить его по своему усмотрению:

- 2001:DB8::/32 [RFC 3849].

В IPv4 для примеров используют три блока [RFC 5735, RFC 5737]:

- 192.0.2.0/24,
- 198.51.100.0/24
- 203.0.113.0/24.

Несколько блоков понадобилось для удобства составления наглядных примеров взаимодействия разных сетей.

Блок 192.0.2.0/24 был назначен IANA.

Блоки 198.51.100.0/24, 203.0.113.0/24 и 2001:DB8::/32 выделены региональной регистратурой Азии и Океании APNIC.

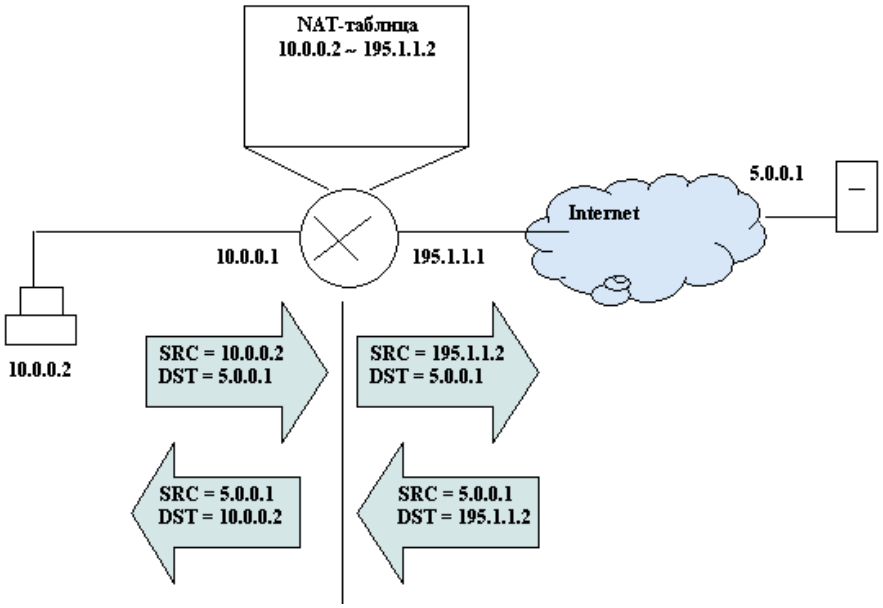
У IPv4 есть сводный документ, посвященный адресам особого назначения [RFC 5735].

Аналогичный документ есть и у IPv6 [RFC 5156].

4.3. Подключение частных сетей к Internet через NAT и прокси-сервера.

Пользователям, находящимся внутри частной сети, как правило, нужен доступ в Internet. Для обеспечения доступа в Internet могут использоваться маршрутизаторы с поддержкой NAT (Network Address Translation), а также прокси-сервера.

Трансляция сетевых адресов NAT основана на замене IP-адреса в заголовке пакета с приватного на реальный и наоборот. В памяти маршрутизатора содержится таблица преобразования адресов (Address translation table), в которой содержится соответствие между реальными и приватными адресами. При отправке пакета маршрутизатор осуществит замену IP-адреса отправителя с приватного адреса на реальный. При получении пакета маршрутизатор осуществит преобразование адреса получателя с реального на приватный, после чего отправит пакет в корпоративную сеть. Таким образом, маршрутизатор с поддержкой NAT прозрачно для конечного пользователя обеспечивает доступ к глобальной сети, см. рис.

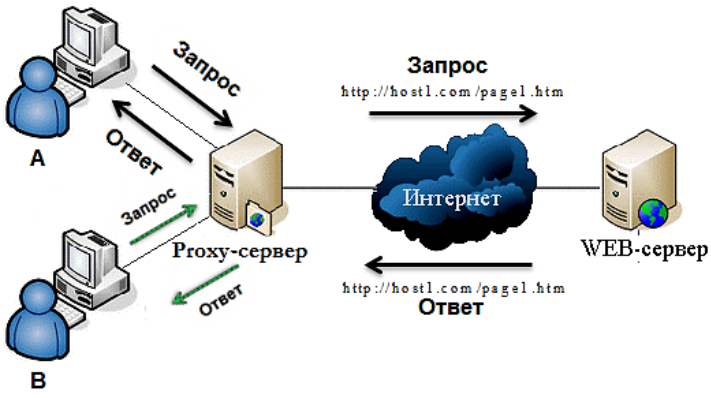


Существует динамический NAT и статический NAT.

В случае статического NAT соответствие между реальным и приватным адресом устанавливается на неограниченный срок. В случае динамического соответствие устанавливается на определённый промежуток времени, после чего этот же реальный адрес может быть поставлен в соответствие другому приватному адресу. Динамический NAT позволяет обеспечить большее количество пользователей для доступа в Internet.

Часто используются решения с PAT (**Port Address Translation**) и с NAPT (**Network Address Port Translation**). PAT позволяет обеспечить выход в Internet для нескольких тысяч пользователей с одного реального адреса.

Proxy-сервер (англ. proxy – посредник) – это компьютер, одновременно подключенный к корпоративной и глобальной сетям. Компьютер в корпоративной сети отправляет запрос прокси-серверу, а прокси-сервер со своего реального адреса отправляет этот запрос в глобальную сеть, принимает ответ, при необходимости запоминает (кэширует) результат и отправляет полученный ответ компьютеру в локальной сети. Таким образом, прокси-сервера позволяют предоставить компьютерам корпоративной сети выход в Internet, а также сократить внешний трафик за счёт кэширования.



5. Маски подсети, задаваемые по умолчанию

Коды сетей и коды узлов в IP-адресе можно различить с помощью маски подсети. Каждая маска подсети представляет собой 32-битное число, состоящее из последовательной группы единичных битов для выделения из IP-адреса кода сети, и последовательной группы нулевых битов для выделения кода узла.

Например, вот маска подсети, которая обычно используется с IP-адресом 131.107.16.200:

11111111 11111111 00000000 00000000

Эта маска подсети состоит из 16 единичных битов, за которыми следуют 16 нулевых битов, что означает, что части этого IP-адреса, соответствующие коду сети и коду узла, имеют одинаковую длину в 16 бит. В точечно-десятичной нотации эта маска будет иметь следующий вид: 255.255.0.0.

В следующей таблице показаны маски подсети для A, B и C классов адресов Интернета.

Таблица 3. Стандартные маски

Класс адреса	Биты маски подсети	Маска подсети	Префикс
Класс A	11111111 00000000 00000000 00000000	255.0.0.0	/8
Класс B	11111111 11111111 00000000 00000000	255.255.0.0	/16
Класс C	11111111 11111111 11111111 00000000	255.255.255.0	/24

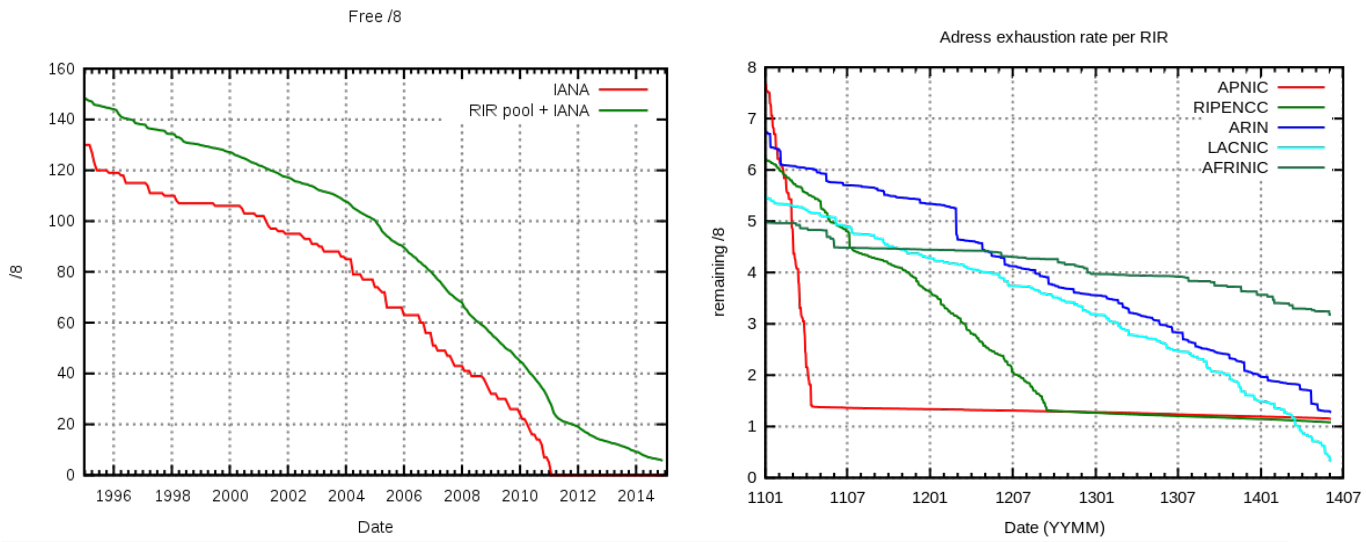
Обычно значения маски подсети по умолчанию используется для сетей в которых каждый сегмент IP-сети соответствует одной физической сети, но в некоторых случаях можно использовать специальные маски подсети для деления сети на IP-подсети.

Дополнительные сведения об использовании специальных масок содержатся в разделе ***Деление сети на подсети***.

Важно! В случае если два компьютера имеют IP-адреса с разными номерами сетей (даже если они принадлежат одной физической сети), то они не смогут общаться друг с другом напрямую: для их взаимодействия необходим маршрутизатор (см. раздел IP-маршрутизация), а также, во избежание неполадок с адресацией и маршрутизацией все компьютеры TCP/IP в одном сегменте сети должны использовать одну и ту же маску подсети.

6. Проблемы с адресами и продление жизни адресного пространства IPv4

Длина IP-адреса составляет 32 бита, что позволяет использовать до 2^{32}=4294967296 уникальных адресов для абстрактной бесклассовой совокупности узлов и сетей. Но из-за случайного распределения адресов без учета географического положения, из-за исчерпания адресов класса B и прекращения выдачи адресов класса A стала проявляться нехватка адресов. Выдача адресов класса C привела к экспоненциальному росту размеров таблиц маршрутизации, что приводило к перегрузкам глобальных маршрутизаторов и замедляло передачу пакетов по Internet.



Динамика количества свободных блоков /8 с 1995 года Исчерпание запаса IP-адресов у RIR в 2011-2014 г.
В 2011 г. компания Microsoft купила 666 624 адресов IPv4 на распродаже Nortel за 7,5 миллионов долларов.

Для решения возникших проблем было предпринято несколько попыток продлить жизнь IPv4 и разработан протокол IPv6. Часть решений по продлению жизни IPv4 уже описана выше (введение классов сетей, Private Addresses, NAT, PAT, Proxy), далее рассмотрены ещё несколько решений (VLSM, CIDR, Address Return).

- ***RFC 760*** первое описание протокола IP. Отсутствует концепция классов, адреса представляли собой 8-битовые идентификаторы сетей, за которыми следовали 24-битовые локальные адреса.
- ***RFC 791*** предложено разбиение адресов на классы. Классы A, B, C, D, E были описаны ранее.
- ***RFC 950*** предложено использование масок и подсетей, что обеспечивает эффективность использования классов адресов и эффективность маршрутизации.
- ***RFC 1338*** использование суперсетей, которые образуются при использовании маски меньших размеров, нежели стандартная маска сетевого IP-адреса класса A, B или C.
- ***RFC 1517-1520*** описывается внеклассовая межрегиональная маршрутизация CIDR (Classless Inter-Domain Routing). Со второй половины 1990-х CIDR маршрутизация вытеснила классовую.
- ***RFC 1819*** IPv5 работает на том же уровне что и IPv4, разработан для приложений реального времени, содержит средства обеспечения QoS (Quality of Service).
- ***RFC 1883, RFC 2460*** IPv6 развитие IPv4. На IPv6 происходит переход с IPv4.
- ***RFC 1475*** IPv7 или TP/IX.

7. Деление сети на подсети VLSM (subnetting)

VLSM - Variable Length Subnet Masks. В некоторых случаях можно использовать ***специальные маски подсети*** для деления сети на IP-подсети.

Деление сети на IP-подсети (RFC 950) позволяет разделить стандартную часть IP-адреса, соответствующую коду узла, на подсети, которые являются подразделами исходного кода сети, основанного на классе. **Это становится возможным за счет увеличения битов маски в сетевой части адреса.** Изменяя длину частей маски подсети, можно уменьшить число битов, используемых для кода узла и таким образом регулировать количество возможных подсетей и узлов в каждой из них.

При классической IP-адресации используется следующая схема разбиения IP-адреса на классы.

Биты	0 1 2 3 ...		... 30 31
Часть	Ключ класса сети	Номер сети	Номер устройства в сети

При использовании подсетей, имеется еще один уровень иерархии – номер подсети, который выделяется в адресной части номера устройства с помощью наложения маски подсети. Та часть IP-адреса в которой маска подсети имеет значение 1 является расширенным префиксом сети, а оставшаяся является номером устройства в этой подсети.

Биты	0 1 2 3 ...		... 30 31	
Часть	Ключ класса сети	Номер сети	Номер подсети	Номер устройства в подсети

Если распространить ограничения на назначения адресов узлам в сети на подсети (запрещены все 1 или 0), то можно сделать вывод, что в любой подсети минимум два последних бита должны выделяться под номер узла. Отсюда следуют описанные ниже ограничения на описание подсетей с помощью маски.

Сеть класса A с подсетями 10.X.Y.Z

0 0 0 0 1 0 1 0	**X X X X X X X X**	**Y Y Y Y Y Y Y Y**	**Z Z Z Z Z Z**	**z z**
Идентификатор сети 10	Идентификатор подсети может занять до 22 бит			Узел

Сеть класса B с подсетями 138.10.Y.Z

1 0 0 0 1 0 1 0	**0 0 0 0 1 0 1 0**	**Y Y Y Y Y Y Y Y**	**Z Z Z Z Z Z**	**z z**
Идентификатор сети 138.10		Идентификатор подсети до 14 бит		Узел

Сеть класса C с подсетями 202.10.10.Z

1 1 0 0 1 0 1 0	**0 0 0 0 1 0 1 0**	**0 0 0 0 1 0 1 0**	**Z Z Z Z Z Z**	**z z**
Идентификатор сети 202.10.10			Подсеть до 6 бит	Узел

8. Внеклассовая междоменная маршрутизация CIDR (supernetting)

CIDR - Classless Inter-Domain Routing используется в маршрутных таблицах глобальных маршрутизаторов (поддерживается для BGP, OSPF и не поддерживается для RIP и EGP). Вместо обычной классовой маршрутизации используется маршрутизация нескольких смежных сетей как единой сети. **Это становится возможным за счет уменьшения битов маски в сетевой части адреса.** На стороне вашей локальной сети продолжает использоваться классовая маршрутизация. Позволяет замедлить рост таблиц маршрутизации и уменьшить потребность в выделении новых номеров IP-сетей.

Префиксная нотация используется как для CIDR маршрутизации, так и для более компактной записи маски подсетей в VLSM. Формат IP-адреса заменяется на следующий: <IP-адрес, префикс>. Значение префикса любое от 0 до 32. Префикс означает количество битов, начиная слева, используемых для адреса сети.

Префикс не зависит от класса, ниже приводятся примеры префиксов для различных IP-адресов.

- Сети класса A имеют префикс /8.
- Сети класса B имеют префикс /16.
- Сети класса C имеют префикс /24.
- 198.1.192.0/20 – похоже на класс C, но у C префикс /24.
- 128.1.128.0/20 – похож на адрес B, но у B префикс /16.
- 15.1.192.0/20 – похож на адрес A, но у A префикс /8.

Таблица 4. Префиксная нотация масок

Префикс	Десятичное представление	Количество адресов	Количество адресов различных классов
/14	255.252.0.0	256Ki	4 класса B или 1024 класса C
/15	255.254.0.0	128Ki	2 класса B или 1024 класса C
/16	255.255.0.0	64Ki	1 класса B или 256 класса C
/17	255.255.128.0	32Ki	128 класса C
/18	255.255.192.0	16Ki	64 класса C
/19	255.255.224.0	8Ki	32 класса C
/20	255.255.240.0	4Ki	16 класса C
/21	255.255.248.0	2Ki	8 класса C
/22	255.255.252.0	1Ki	4 класса C
/23	255.255.254.0	512	2 класса C
/24	255.255.255.0	256	1 класса C
/25	255.255.255.128	128	1/2 класса C
/26	255.255.255.192	64	1/4 класса C
/27	255.255.255.224	32	1/8 класса C
/28	255.255.255.240	16	1/16 класса C
/29	255.255.255.248	8	1/32 класса C
/30	255.255.255.252	4	1/64 класса C
/31	255.255.255.254	2	1/128 класса C

9. Межсетевой протокол IPv6.

Важнейшие инновации IPv6 состоят в следующем:

- упрощен стандартный заголовок IP-пакета
- изменено представление необязательных полей заголовка
- **расширено адресное пространство**
- улучшена поддержка иерархической адресации, агрегирования
- маршрутов и автоматического конфигурирования адресов
- введены механизмы аутентификации и шифрования на уровне IP
- введены метки потоков данных IP-пакетов
- расширен QoS

При этом в IPv6 все изменения планировались таким образом, чтобы минимизировать изменения на других уровнях протокольного стека TCP/IP. IPv6 остался расширяемым протоколом, причём поля расширений (дополнительные заголовки) могут добавляться без снижения эффективности маршрутизации.

Предполагается широкое использование IPv6 в сетях мобильной связи 3-го и 4-го поколений.

Самое главное – в IPv6 увеличена длина адреса до 128 бит, что позволяет использовать до 2^{128} адресов.

Вот как выглядит это 128 битное число в сравнении с 32 битной версией IPv4:

340 282 366 920 938 463 463 374 607 431 768 211 456 в сравнении с **4 294 967 296**

IPv6 адрес записывается в 16-ой форме и состоит из 8 групп по четыре 16-ричные цифры:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX.

Адреса получаются очень громоздкие, поэтому очень важно использование более лаконичных имен DNS и сокращений в записи адреса.

Правила сокращения - отбросить можно только одну последовательность нулей и незначимые нули слева. Например:

1080:0000:0000:0000:0008:0800:200C:417A или 1080:0:0:0:800:200C:417A или 1080::800:200C:417A

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 - а этот адрес, сокращенно записать нельзя;

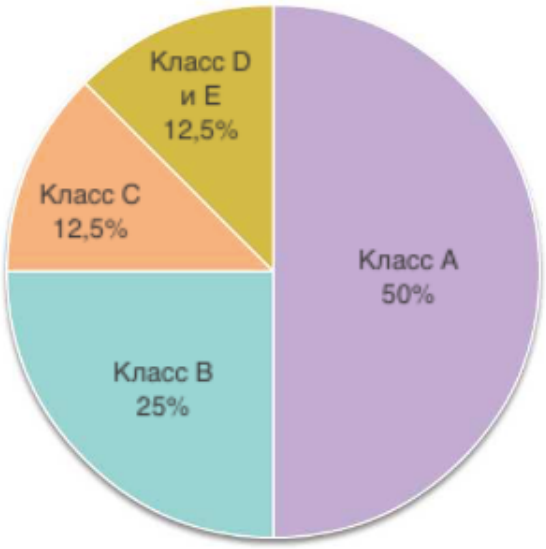
Нотация ::ffff:xx.xx.xx.xx описывает IPv4-адрес отображённый на IPv6. В процессе перехода на Ipv6 создается двойной стек TCP/IP и используется ***туннелирование*** протоколов в обе стороны.

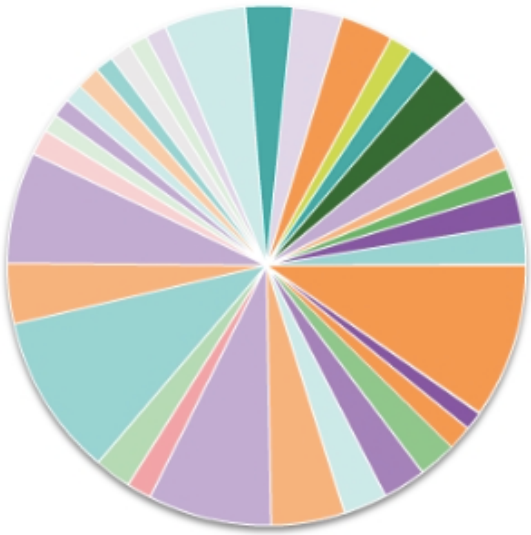
При использовании IPv6-адреса в URL необходимо заключать адрес в квадратные скобки, если необходимо указать порт, то он пишется после скобок:

http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]/ и http://[2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d]:8080/

10. Причины разделения сетей на подсети.

1. Сети класса A и B из-за своих размеров имеют очевидные проблемы с огромным трафиком через точку входа в сеть и сложность администрирования такими огромными сетями. Управлять каждой отдельной подсетью значительно проще.
2. В подсетях возможно использовать различные технологии организации сетей. Невозможно смешивать технологии Ethernet, Token Ring, FDDI, ATM и т.п. на одной физической сети - однако они могут быть связаны логически через маршрутизаторы!
3. Удалённое физическое размещение узлов имеет ограничения на длину кабеля, но, связь в организации можно обеспечить через множественные лигические сети используя единственный выданный блок адресов.
4. Разделение на подсети может быть продиктовано соображениями безопасности, т.к. трафик в общей сети может быть перехвачен. Организация подсетей обеспечивает способ, позволяющий предохранить отдел маркетинга от "сующих нос не в свои дела".
5. Сеть перегружена. Ее разбивают на подсети так, чтобы трафик был сосредоточен внутри подсетей, разгружая таким образом всю сеть, без необходимости увеличивать ее общую пропускную способность.

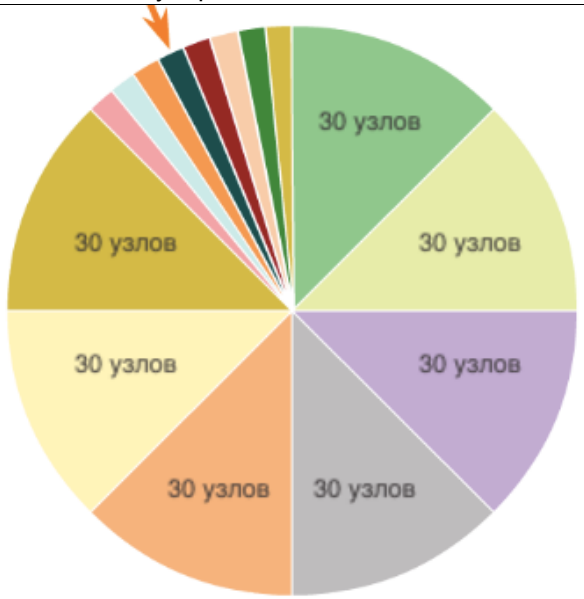




Классовая адресация – неэффективно. Избыточное выделение IP адресов.

CIDR – эффективно. Позволяет заказчикам получить пространство с учётом фактических потребностей.

FVLSM – Fixed. Сети равного размера



VLSM – с подсетями различного размера. Одна подсеть далее разделена на 8 подсетей по 4 узла.

11. Работа по организации подсетей.

Краткий обзор шагов, необходимых для организации подсетей:

1. Установите физическую связанность (сетевые соединения - типа маршрутизаторов).
2. Решите, какой (большой/маленькой) должна быть каждая подсеть, т.е. какое количество IP-адресов требуется для каждого сегмента.
3. Вычислите соответствующую сетевую маску и сетевые адреса.
4. Установите каждому интерфейсу на каждой сети его собственный IP адрес и соответствующую сетевую маску.
5. Установите направления связи на маршрутизаторах и соответствующих шлюзах, направления связи и/или заданные по умолчанию направления связи на сетевых устройствах.
6. Протестируйте систему, исправьте ошибки.

12. Примерное содержание заданий на экзамене по теме адресация IPv4.

1. Преобразовать двоичную запись IPv4-адреса в десятичную 4-октетную нотацию.

2. Определить класс сети для данного IPv4-адреса, заданного как nnn.nnn.nnn.nnn

3. Определить маску подсети, использующую n-разрядный префикс, для сети с заданным IP-адресом.

4. Определить адрес подсети с маской nnn.nnn.nnn.nnn по IP-адресу узла nnn.nnn.nnn.nnn.