GeekBrains

Компьютерные сети

Сетевой уровень. Часть 2. Бесклассовая адресация

Бесклассовая адресация. Маски переменной длины. IP-калькулятор. IPX. Введение в IPv6

Введение

OSI/ISO	TCP/IP (DOD)
7. Прикладной уровень	4. Уровень приложений
6. Уровень представления	
5. Сеансовый уровень	
4. Транспортный уровень	3. Транспортный уровень
3. Сетевой уровень	2. Сетевой уровень
2. Канальный уровень	1. Уровень сетевых интерфейсов
1. Физический уровень	

Продолжаем изучать сетевой уровень.

На этом занятии мы разберем бесклассовую адресацию и маски переменной длины, а также альтернативные сетевые протоколы, такие как IPX и IPv6.

Бесклассовая адресация

В классовой адресации для определения, какая часть IP-адреса является идентификатором сети, а какая — идентификатором хоста, служил сам класс сети, который определялся (и определяется при необходимости сейчас) из первых битов адреса (от 1 до 4). Позже способ разделения идентификатора сети и идентификатора хоста был сформулирован с помощью масок. Для того, чтобы выделить адрес сети из хоста, то есть определить, какой сети хост принадлежит, используется маска сети, которая сопоставлена с сетью (или сначала с классом сети).

Маска сети, как и IP-адрес, состоит из 4 октетов, и, как мы знаем, маска для классовых сетей состоит из двух частей. Левая часть содержит от 1 до 3 октетов, имеющих значения 255. Правая часть состоит из от 3 до 1 октетов, имеющих значение 0. Например, 255.0.0.0 — стандарная маска для сетей класса A.

Произведя двоичное умножение маски сети на IP-адрес побитово, мы получим адрес сети.

Для сетей класса B — маска 255.255.0.0.

Для сетей класса C — маска 255.255.255.0.

Позже стало понятно, что такое выделение сетей нерационально. Можно заметить, что фактически маска состоит из двух половин, одна из которых содержит единицы, другая нули. Мы, мысля в

десятичной системе счисления и работая только с масками 255 и 0, можем считать, что если в октете маски 255, то соответствующий октет IP-адреса сохраняется в адресе сети, если же 0, то соответствующий октет адреса сети тоже будет иметь значение 0.

Для классовых масок накладывается органическое ограничение следующим правилом: число бит должно было быть кратно байту (то есть 8, 16, 24). Соответственно, есть еще и префиксная запись, когда число бит указывается как маска.

Например:

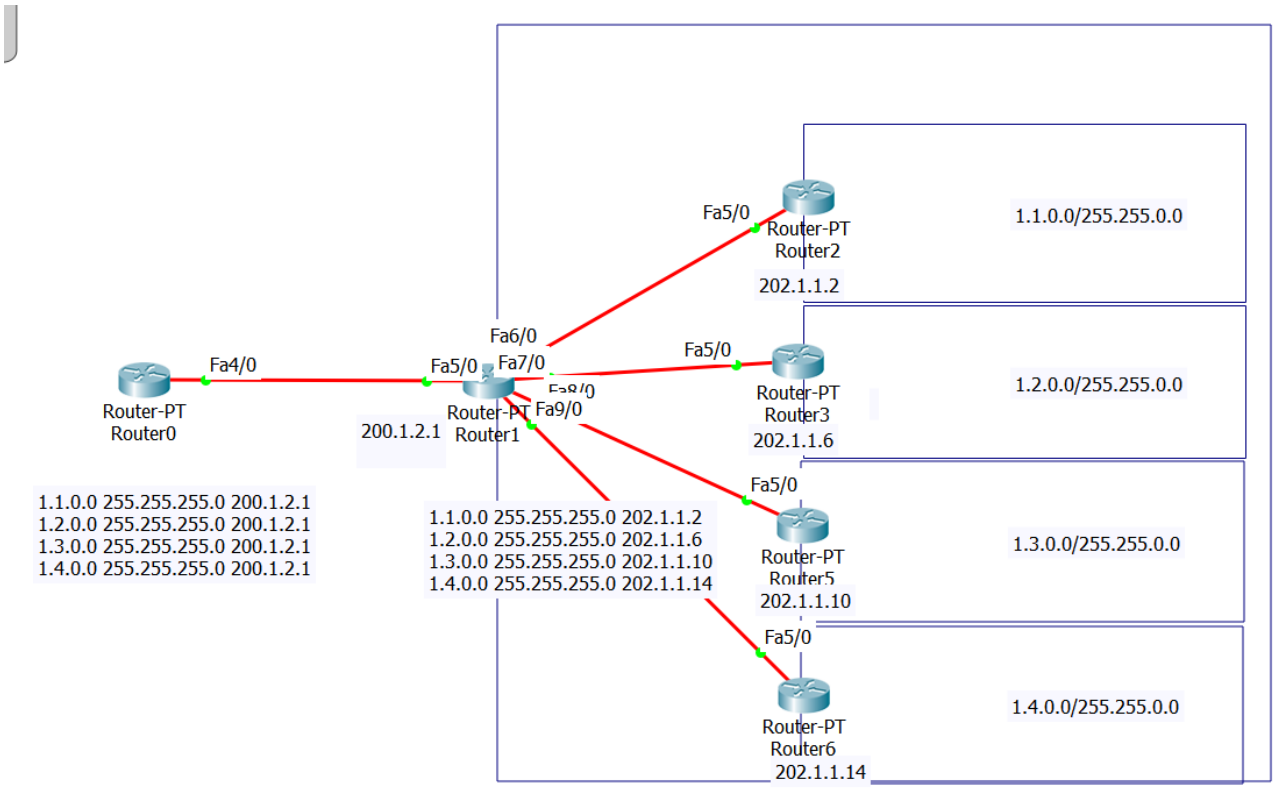
- 255.0.0.0=/8;
- 255.255.0.0=/16;
- 255.255.255.0=/24.

Класс	Число возможных адресов сетей	Число возможных адресов хостов	Маска подсети	Начальный адрес	Конечный адрес
A	128	16 777 214	255.0.0.0	0.0.0.0	127.255.255.255
B	16 384	65 534	255.255.0.0	128.0.0.0	191.255.255.255
C	2 097 152	254	255.255.255.0	192.0.0.0	223.255.255.255
D	Групповой адрес			224.0.0.0	239.255.255.255
E	Зарезервировано			240.0.0.0	255.255.255.255

Разбиение сетей на подсети. Бесклассовая адресация

Если мы возьмем сеть 1.0.0.0/8, или, что тоже самое, 1.0.0.0 с маской 255.0.0.0, или, что тоже самое, 1.0.0.0/255.0.0.0, в такой сети может быть 16 777 214 хостов (компьютеров). Это невозможно с точки зрения организации канального уровня — сколько коммутаторов должно быть, как будут рассылаться ARP-запросы. С концентраторами такое даже в принципе нельзя представить.

Поэтому такие сети нужно разбивать на подсети и связывать между собой с помощью маршрутизации. То есть вместо одной сети 1.0.0.0/8 с 16 777 214 хостами мы можем получить 256 сетей по 65 534 хоста (каждую из которых в свою очередь тоже можно поделить на сети по 254 хоста).

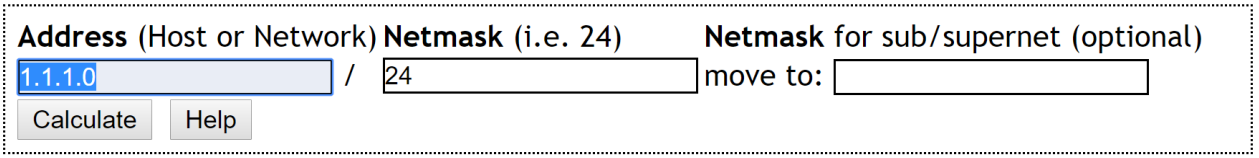


Обратите внимание, что сеть 1.1.0.0/255.255.0.0 не является сетью класса B, а сеть 1.1.1.0/255.255.255.0 не является сетью класса C, несмотря на ту же самую маску. Не маска

определяет класс сети — напротив, класс сети определяет маску. Даже с вышеуказанными масками приведенные сети все равно относятся к классу A.

Класс сети определяется первыми битами адреса.

Онлайн-калькулятор http://jodies.de/ipcalc?host=1.1.1.0&mask1=24&mask2= подтверждает:

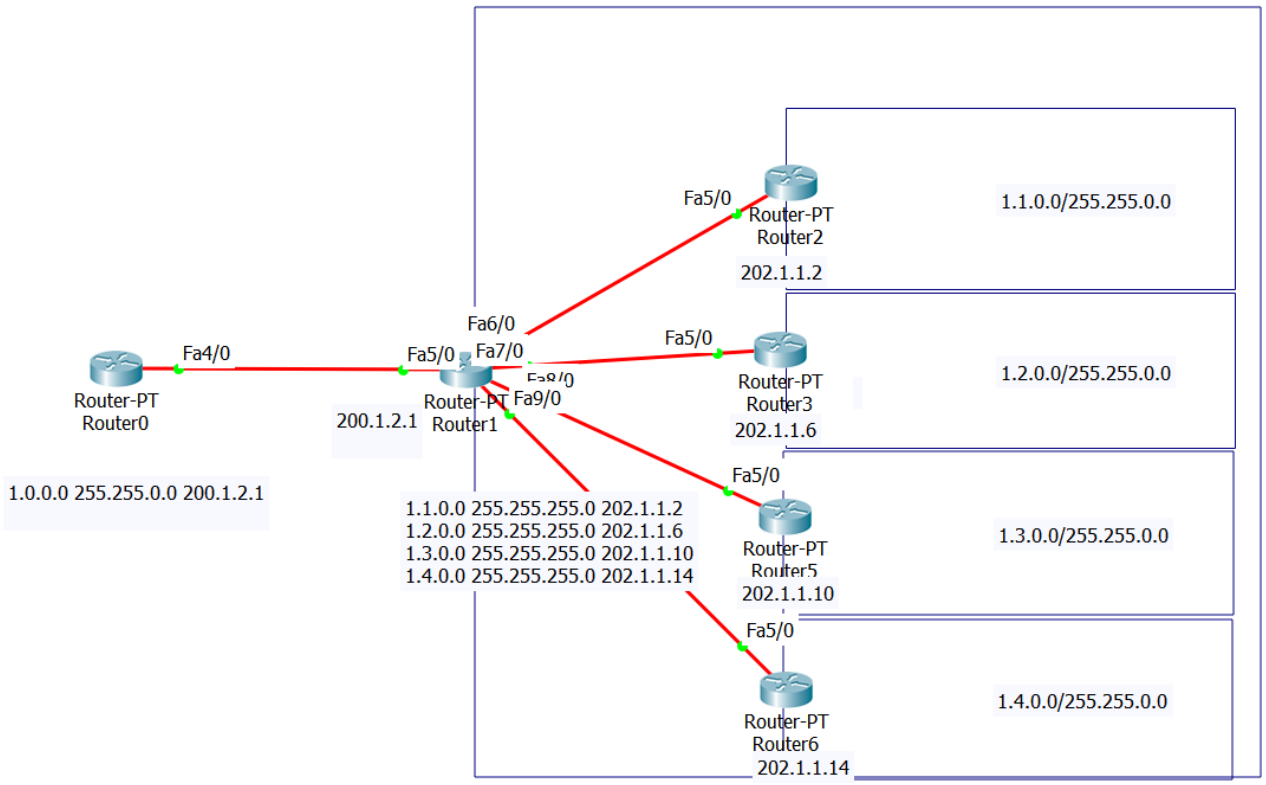



```
Address:   1.1.1.0              00000001.00000001.00000001 .00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111 .00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000 .11111111
=>
Network:   1.1.1.0/24           00000001.00000001.00000001 .00000000 (Class A)
Broadcast: 1.1.1.255            00000001.00000001.00000001 .11111111
HostMin:   1.1.1.1              00000001.00000001.00000001 .00000001
HostMax:   1.1.1.254            00000001.00000001.00000001 .11111110
Hosts/Net: 254
```

Такая адресация называется бесклассовой, или CIDR-адресацией (Classless Interdomain Routing).

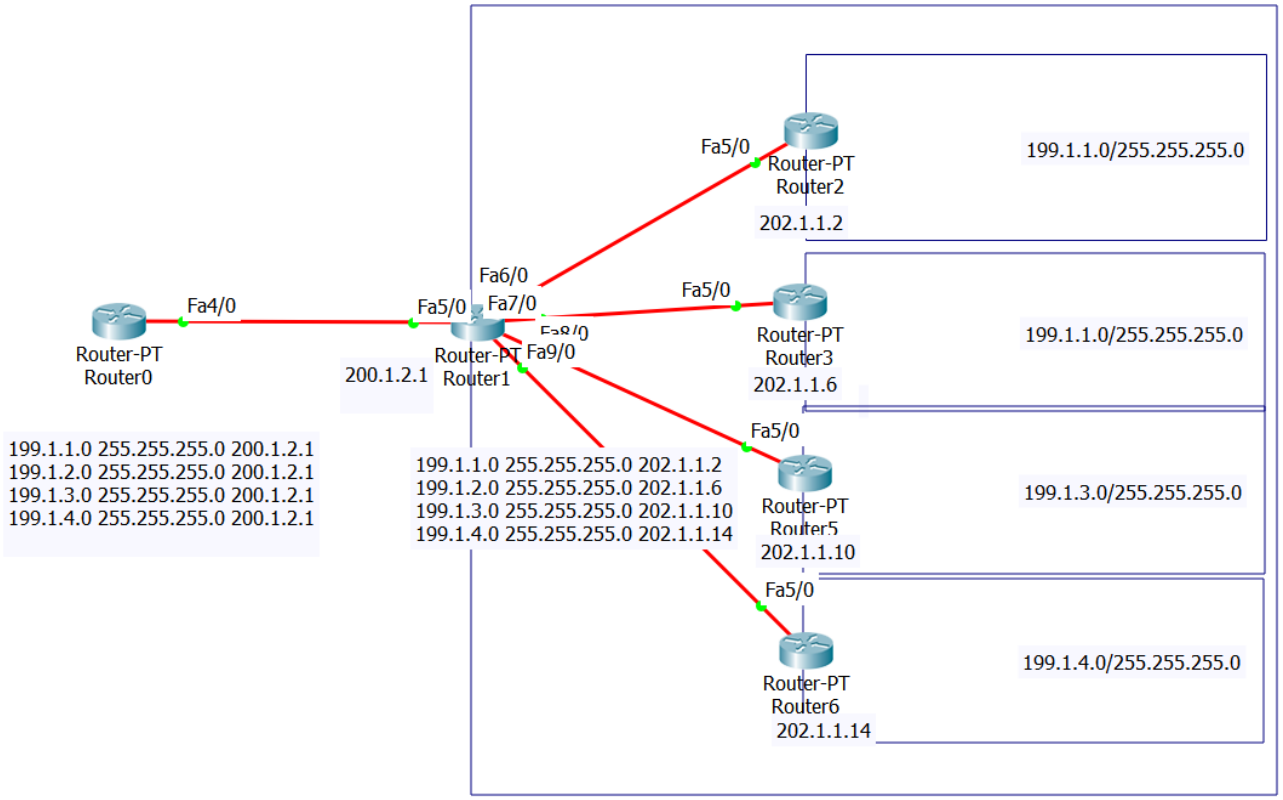
Суммаризация маршрутов

Если мы будем разбивать сеть класса A на подсети с маской 255.255.0.0 то у нас получится 65 536 маршрутов. Но если все эти сети доступны через один маршрутизатор, то можно выполнить суммаризацию маршрута. Мы указываем маршрут в сеть с маской 255.0.0.0 на маршрутизатор, на котором уже присутствуют нужные маршруты.



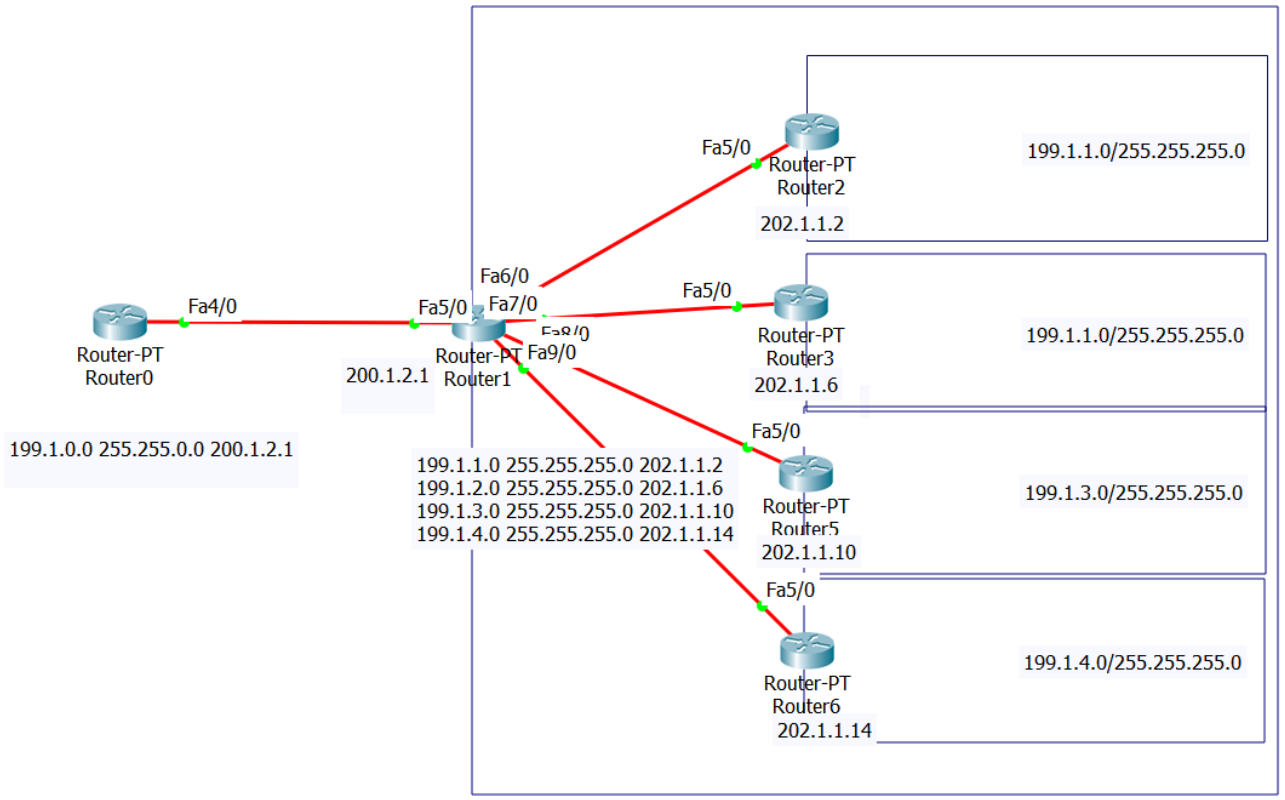
Рассмотрим обратную ситуацию. Здесь сеть, разбитая на подсети, действительно «снаружи» выглядит как одна сеть с маской 255.0.0.0.

Но если мы берем несколько сетей класса C и, соответственно, с маской 255.255.255.0, то и маршруты должны быть отдельными.



Но и наоборот, мы можем объединить сети (например, класса C), в одну сеть с маской 255.255.0.0. При этом адреса не перестанут принадлежать классу C.

И здесь мы можем суммаризировать маршрут, объединив сети.



Рассмотренные нами случаи — это примеры бесклассовой адресацией. Она позволяет более гибко работать с адресным пространством. Но и этого недостаточно.

Маски переменной длины

До сих пор мы рассматривали сети, в которых было минимум 254 адреса хостов. А что, если нам нужно меньше адресов — допустим, 126?

Например, мы можем выделить под адрес не 24 бита (как в сетях класса С), а 25 — тогда мы получим не 255 сетей, а в два раза больше. И наоборот, имея в распоряжении одну сеть класса С и выделив еще один бит, мы сможем разбить ее уже на 2 сети, но не по 244 адреса (256—2), а по 126 (256/2—2). Такую маску также можно записать и в десятичном виде. В последнем случае октет будет иметь двоичное значение 10000000, а десятичное — 128.

Сравним:

255.255.255.0 = 1111 1111. 1111 1111. 1111 1111. 0000 0000

255.255.255.128 = 1111 1111. 1111 1111. 1111 1111. 1000 0000

Число бит также принято указывать через косую черту после адреса (префикс)

255.255.255.0 = 1111 1111. 1111 1111. 1111 1111. 0000 0000 = /24

255.255.255.128 = 1111 1111. 1111 1111. 1111 1111. 1000 0000 = /25

Записи:

10.0.0.0/255.255.255.0 = 10.0.0.0/24

10.0.0.0/255.255.255.128 = 10.0.0.0/25

10.0.0.128/255.255.255.128 = 10.0.0.128/25

Подробнее для этого примера: http://jodies.de/ipcalc?host=10.0.0.0&mask1=24&mask2=25.

Это VLSM (Variable Length Subnet Mask) — маски переменной длины. Термины «бесклассовая адресация» и «маски переменной длины» очень часто употребляют вместе (CIDR/VLSM).

С бесклассовой адресацией и масками переменной длины можно по-другому взглянуть на частные адреса. Можно просуммировать частные диапазоны, получив всего три сети: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16.

Чтобы освоить их более полно, настоятельно рекомендуем потренироваться в IP-калькуляторе: http://jodies.de/ipcalc. Он позволяет посчитать маски, бродкасты для указанных сетей, выводит полезную информацию (о типе сети — например, частная). Также он позволяет делить сети на подсети.

IPX-адреса

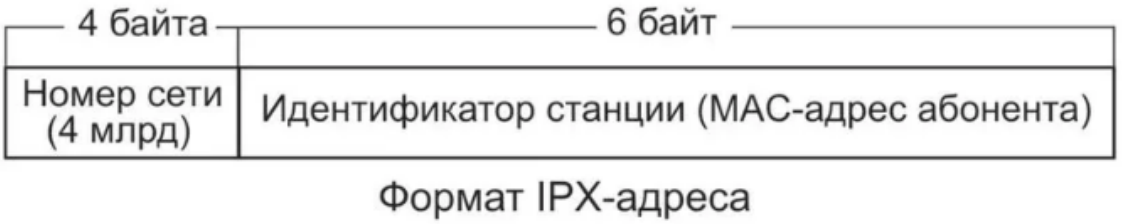
IPX (англ. Internetwork Packet Exchange — межсетевой обмен пакетами) — протокол сетевого уровня модели OSI в стеке протоколов IPX/SPX. Он использовался для передачи датаграмм. Для передачи данных установка соединения не требуется (так же, как и для IP и NetBIOS). Протокол обеспечивал связь между серверами с сетевой операционной системы NetWare и конечными станциями.

Стек IPX/SPX был весьма популярен до распространения TCP/IP. На канальном уровне использовался протокол Ethernet. При этом в кадры Ethernet инкапсулировались IPX-дейтаграммы. Они обеспечивали негарантированную доставку (как IP+UDP). Если же нужна была гарантированная доставка, то в IPX-дейтаграммы (IPX-пакеты) инкапсулировались SPX-пакеты (транспортного уровня). Это совсем не похоже на стек TCP/IP с параллельным использованием адресных пространств TCP и UDP.

Стек протоколов IPX/SPX был разработан компанией Novell для ее проприетарной сетевой ОС NetWare. За основу IPX был взят протокол IDP из стека протоколов Xerox Network Services.

С конца 1980-х и до середины 1990-х годов сети на основе IPX были широко распространены из-за большой популярности сетевой ОС NetWare. Однако в дальнейшем с развитием Интернета и стека TCP/IP оригинальный транспортный протокол SPX от Novell не способствовал успеху IPX-сетей.

В качестве адреса хоста IPX использует идентификатор, образованный из четырехбайтного номера сети (назначаемого маршрутизаторами) и MAC-адреса сетевого адаптера.



Формат IPX-адреса

Формат IP-адреса

Сравнение формата IPX- и IP-адреса

Большое преимущество протокола IPX в том, что конфигурация почти не нужна. В те времена, когда протоколов для динамической конфигурации хоста не существовало и протокол BOOTP для централизованного назначения адресов не был распространен, сеть IPX можно было настраивать почти автоматически. Клиентский компьютер использует MAC-адрес своей сетевой карты в качестве адреса узла и узнаёт, что ему нужно знать о топологии сети, от серверов или маршрутизаторов: маршруты распространяются по RIP (Routing Information Protocol), а сервисы — по Service Advertising Protocol.

Логическим сетям присваивается уникальный 32-разрядный адрес в диапазоне 0x1 — 0xFFFFFFFE.

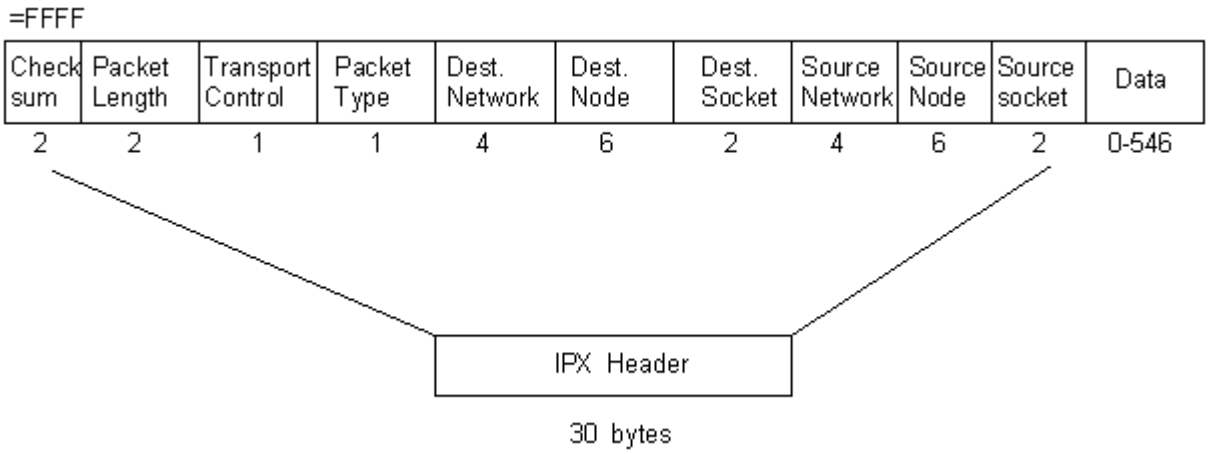
Хосты имеют 48-разрядный адрес узла, являющийся MAC-адресом сетевого адаптера. Адрес узла добавляется к адресу сети для создания уникального идентификатора хоста в сети.

Номер сети 00:00:00:00 означает текущую сеть. Широковещательный адрес — FF:FF:FF:FF.

IPX-адрес имеет следующую структуру:

Номер сети				Номер узла (MAC-адрес)						Номер сокета	

Каждый IPX-пакет начинается с заголовка, имеющего следующую структуру:



Типы пакетов:

Значение	Протокол
0	Неизвестный
1	RIP
2	Echo Packet
3	Error Packet
4	PEP
5	SPX
17	NCP

Номер сети

Благодаря номеру сети можно было связывать узлы узлы IPX, которые не принадлежат к одной и той же сети или «кабельной системе». Чтобы связь между различными сетями была возможна, они должны быть связаны с IPX-маршрутизатором. Набор взаимосвязанных сетей называется internetwork.

Номер сети IPX концептуально идентичен сетевой части IP-адреса (части с netmask-битами, установленными в 1). Номер узла имеет то же значение, что и биты IP-адреса сетевой маски, установленные в 0. Разница в том, что граница между сетевой и узловой частью адреса в IP переменная, а в IPX — фиксированная. Поскольку адрес узла, как правило, идентичен MAC-адресу сетевого адаптера, протокол Address Resolution Protocol не нужен в IPX.

Для маршрутизации записи в IPX таблицы маршрутизации аналогичны таковым в IP. Маршрутизация осуществляется по сетевому адресу, и для каждого сетевого адреса узел маршрутизатора указывается аналогично (в таблицах IP-маршрутизации указывается IP-адрес / сетевая маска).

В ранних сетях IPX Routing Information Protocol (RIP) был единственным доступным протоколом для обмена информацией о маршрутизации. В отличие от протокола RIP для IP, версия для IPX использует время задержки в качестве основного показателя, сохраняя счетчик переходов как вторичный показатель.

Номер узла

Номер узла используется для адресации отдельного компьютера (точнее, сетевого интерфейса) в сети. Клиентские станции используют в качестве номера узла MAC-адрес своей сетевой карты.

Значение FF:FF:FF:FF:FF:FF может использоваться как номер узла в адресе для широковещательного пакета «всем узлам в текущей сети».

Номер сокета

Номер сокета служит для выбора процесса или приложения в узле назначения. Наличие номера сокета в IPX-адресе позволяет IPX выступать в качестве протокола транспортного уровня, сопоставимого с протоколом UDP в IPS.

Номер сокета	Протокол
0x0001-0x0BB8	Зарезервирован Xerox
0x0001	Routing Information Packet
0x0002	Echo Protocol Packet
0x0003	Error Handling Packet
0x0020-0x003F	Экспериментальный
0x0BB9-0xFFFF	Динамически присвоенный
0x0451	NCP — используется серверами Novell Netware
0x0452	SAP
0x0453	RIP
0x0455	NetBIOS
0x0456	Diagnostic Packet
0x0457	Serialization Packet
0x4000-0x4FFF	Динамически присвоенные номера сокетов

0x4003	Используется Novell Netware Client
0x8000-0xFFFF	Статически присвоенные номера сокетов
0x8060	IPX
0x9091	TCP через IPXF
0x9092	UDP через IPXF
0x9093	IPXF

IPv6-адреса

В связи с исчерпанием диапазона IPv4-адресов предполагается, что в дальнейшем будут использоваться IPv6-адреса. Пространство IPv6-адресов на многие порядки больше, чем в четвертой версии протокола, поэтому предполагается, что их хватит всем.

Почему v6 а не v5? Версия IPv5 была экспериментальной: она оперировала IPv4-адресами, но отличалась заголовками пакета (хотя первый байт также обозначал версию протокола). IPv5 известен тем, что в дальнейшем его влияние испытали протоколы ST, ST-II и MPLS, и тем, что следующая версия IP после четвертой — шестая, а не пятая.

IPv6-адреса 128-битные, причем распределяются большими блоками, т. е. зачастую с 64-битной маской. Можно проследить влияние протокола IPX: достаточно большая часть адреса отводится под сеть — больше, чем в IP (3 байта для сети класса C) и в IPX (4 байта), т.е. целых 8 байт. Оставшуюся часть под хост можно было получить из MAC-адреса (как в IPX), но 6-байтовый (48-битный) адрес нужно было преобразовать в 8-байтный (64-битный), приведя его к стандарту EUI-64 (EUI-64, EUI-48, MAC — в целом, родственные стандарты физической адресации). В дальнейшем стало понятно, что такая система небезопасна (возможность идентифицировать узел, используемое оборудование — возникает угроза слежки), поэтому стали использоваться случайные последовательности. Кроме того, есть механизмы инкапсуляции IPv4-адресов в IPv6 (например, 6to4) для работы IPv6-сетей через IPv4-сети.

Несмотря на встречающиеся сомнения по поводу IPv6 и на медленную скорость его внедрения, это определенно, технология будущего. Адресное пространство IPv4 практически исчерпано, а количество техники, подключающейся к сети (смартфоны, планшеты, IPTV, устройства «умного дома», Интернет вещей, квадрокоптеры и прочие интересные игрушки), растет все быстрее. IPv6 разработан уже в расчете на такое использование. Организации, поддерживающие глобальную структуру сети Интернет, оказались дальновидными: IPv4 был разработан в 1979 году, а о IPv6 стали задумываться в 1992 году и стандартизировали его в 1995. На данный момент все корневые сервера поддерживают AAAA ресурсные записи (для IPv6). Почтовые службы Yandex и Google обмениваются IPv6-трафиком.

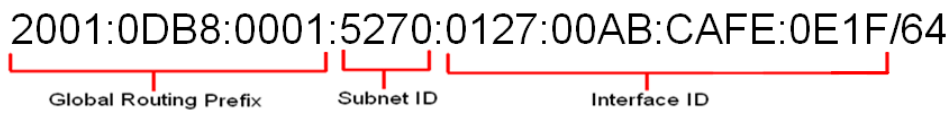
IPv6 во многом перенял черты как IPv4 так и IPX. Если мы возьмем IPv4-маску вида 255.255.0.0 то у нас окажется всего 2 байта на сеть и 2 на хост. Сейчас, применяя NAT, мы уже фактически используем пары IP-адресов — «белый» и «серый». Потому при разработке IPv6 логично было бы выделить 4 разряда под хост и 4 разряда под сеть.

Но есть еще протоколы ICMP, ARP и их стандартные уязвимости. Почему бы не взять идею из IPX и использовать в качестве адреса хоста MAC-адрес, хотя бы для локальных адресов? Но есть одна проблема: 6-байтный адрес не помещается в 4 разряда. Потому приняли решение использовать не октеты, а хекстеты — двубайтные идентификаторы.

Таким образом IPv6-адрес состоит из 8 двубайтных разрядов: 4 под сеть и 4 под хост (впрочем можно использовать и другое распределение). Маски используются так же, и стандартный префикс для IPv6 — 64-битный адрес.

Так как адреса в хекстетах слишком объемны, а сам адрес 128-битный, запись ведется в шестнадцатеричном формате (0–9, A–F). Шестнадцатеричные числа разделяются двоеточиями (:). Каждая четверка шестнадцатеричных цифр эквивалентна 16 битам (двум байтам). Каждый хекстет состоит из восьми четверок, каждая из которых эквивалентна 16 битам. Адрес IPv6 имеет такой вид: 2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F/64. 2001 в шестнадцатеричном виде — это 0010 0000 0000 0001 в двоичном.

Структура адресов IPv6



Префикс сайта, или префикс глобальной маршрутизации — это первые три четверки (или 48 бит) адреса. Он назначается интернет-провайдером.

ID подсети — это 4-я четверка адреса.

ID интерфейса — это последние 4 четверки (64 бита) адреса. Он может вручную или динамически назначаться с помощью механизма EUI-64 (Extended Unique Identifier).

Первые 3 бита фиксированы: 001 (двоич), что дает 200::/12 (IANA Global Routing Number).

Биты 16–24 идентифицируют регионального регистратора:

- 2001:0000::/23 — IANA,
- 2001:0200::/23 — APNIC (Азиатско-Тихоокеанский регион),
- 2001:0400::/23 — ARIN (Североамериканский регион),
- 2001:0600::/23 — RIPE (Европа, Ближний Восток, Россия и СНГ).

Оставшиеся 8 бит до 32-го идентифицируют ISP.

3-я четверка представляет идентификатор сайта/компании.

4-я четверка представляет идентификатор подсети:

- позволяет адресовать 65 536 подсетей с 18 446 744 073 709 551 616 (18 квинтиллионов) адресов в каждой подсети;
- не является частью хостового поля адреса.

Идентификатор интерфейса **—** это оставшиеся 64 бита адреса. Может быть сконфигурирован вручную или динамически с использованием EUI-64 (Extended Unique Identifier). Механизм EUI-64 использует 48-битный MAC-адрес устройства и конвертирует его в 64-битный путем вставки значения FF:FE в середину адреса.

Первый (сетевой) и последний (широковещательный) адреса могут быть назначены интерфейсам. Интерфейсу можно назначить более одного IPv6-адреса. Широковещательных адресов в принципе нет, вместо этого используется мультикастинг.

IPv6 использует тот же метод разделения на подсети, что и IPv4:

- /127 дает 2 адреса;
- /124 дает 16 адресов;
- /120 дает 256 адресов.

Первый адрес в подсети полностью состоит из 0, последний — полностью из F.

Для простоты и единства структуры рекомендуется везде использовать /64. Использование чего-либо меньшего, чем /64, может потенциально привести к сбою некоторых функций IPv6 и неоправданному усложнению структуры адресации.

Нули в старших разрядах любой 16-битной секции могут быть опущены.

Адрес до упрощения:

2001:0DB8:0001:5270:0127:00AB:CAFE:0E1F/64

Адрес после упрощения:

2001:DB8:1:5270:127:AB:CAFE:E1F/64

Это правило применимо только к нулям в старших разрядах. Если опустить нули в младших разрядах, адрес будет неверен.

Link-Local-адреса предназначены для использования только в локальном канале. Адреса Link-Local автоматически конфигурируются на всех интерфейсах. Префикс, используемый Link-Local адресами

— FE80::X/10. Маршрутизаторы не перенаправляют пакеты с Link-local адресом источника или назначения.

Адрес Loopback — функция схожа с IPv4-адресом 127.0.0.1. Адрес Loopback 0:0:0:0:0:0:0:1 может быть сокращен до ::1. Используется устройством для посылки пакета себе самому.

Структура IPv6-пакета

Структура IPv6-пакета проще, чем структура IPv4-пакета.

Вместо неиспользуемого типа обслуживания используются приоритеты и метки потоков. Следующий заголовок — указание на наличие дополнительного заголовка (фрагментация, либо AH/ESP для IPSEC, либо TCP/UDP).

Сравнение IPv4 и IPv6

Ниже приведены ключевые отличия версий протоколов.

IPv6:

- 128-битный адрес, состоящий из префикса глобальной маршрутизации, ID подсети и ID интерфейса;
- используется шестнадцатеричная запись (0–9, A–F), разделитель — двоеточие;
- минимальный размер максимального пакета — 1280 байт;
- сетевой и широковещательный адреса могут быть назначены интерфейсам конечных устройств;
- встроенное шифрование IPsec.

IPv4:

- 32-битный адрес, состоящий из сетевой и хостовой части;

- используется десятичная запись, разделитель — точка;
- минимальный размер максимального пакета — 576 байт;
- сетевой и широковещательный адреса нельзя назначать интерфейсам конечных устройств;
- для шифрования IPv4-пакетов нужно применять технологии VPN.

Практическое задание

Сегодня нам Cisco Packet Tracer не понадобится. Это задание на расчет сетей. Можно пользоваться калькулятором http://jodies.de/ipcalc (но он не сможет полностью решить задачу за вас).

1. Разбить сеть 192.168.1.0 на 2, 4 и 8 подсетей.
2. Сколько хостов будет в сети 172.16.1.0/25? А в сети 10.0.0.0/26?
3. Каков будет бродкаст-адрес в сети 10.0.0.0/3? А в сети 10.255.255.124/30?
4. Какими будут адрес и маска первой и последней сетей, если разбить 192.168.0.0/24 на 16 сетей? А если разбить сеть 100.64.0.0/25 на 8 сетей?

Ответы принимаются в текстовом виде в файле docx/pdf или в комментарии к домашнему заданию. Просьба не прикреплять их в формате txt (так может не распознаться кодировка), либо дублируйте текст в комментарии. Пожалуйста, не присылайте скриншоты калькулятора! Нужны исключительно ответы на поставленные вопросы.

Дополнительные материалы

1. https://version6.ru/.
2. http://xgu.ru/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%B2_Linux.

Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:

1. https://ru.bmstu.wiki/IPX_(Internetwork_Packet_Exchange).
2. https://ppt-online.org/186394.
3. http://what-when-how.com/networking/internetwork-packet-exchange-networking/.
4. http://www.rhyshaden.com/ipx.htm.