IP-адрес, маска подсети, классы IP-адресов

Все узлы в компьютерных сетях должны иметь IP-адреса. За выдачу IP-адресов отвечает Агентство по выделению имён и уникальных параметров протоколов Интернет (IANA). Обычно Интернет-провайдеры получают диапазоны IP-адресов у IANA, а затем перераспределяют их между своими абонентами.

IP-адрес имеет длину 4 байта (32 бита) и разделён на 4 секции, каждая из которых содержит 8 бит и называется *октетом*. Любой из байтов может принимать значение от 0 до 255 (2^8 вариантов).

IP-адрес может быть представлен в двоичном 10101100.00010100.00111111.11111110 и в десятичном 172.20.63.254 формате. Для обозначения октетов используются буквы – w.x.y.z.

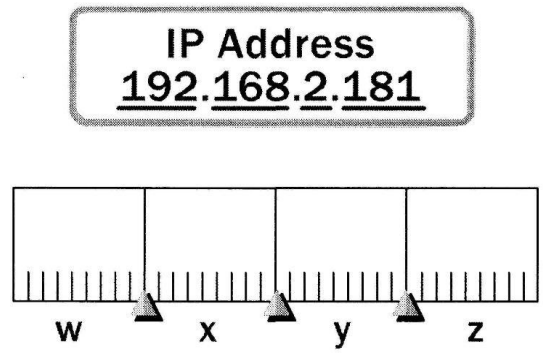

Рис. Формат IP-адреса

IP-адрес состоит из двух логических частей – идентификатора (или номера) сети (*Network ID*) и идентификатора (или номера) узла в сети (*Host ID*). Так же, как все квартиры в одном доме в своём адресе должны иметь одинаковый номер дома и уникальный для этого дома номер квартиры, так и каждый узел одной сети должен иметь одинаковый Network ID и уникальный Host ID.

Маршрутизаторы используют IP-адреса для пересылки сообщений от одной сети к другой. По мере того как пакет путешествует от маршрутизатора к маршрутизатору, он отрабатывает свой путь слева направо в IP-адресе, пока не поступит на маршрутизатор, находящийся в нужной сети.

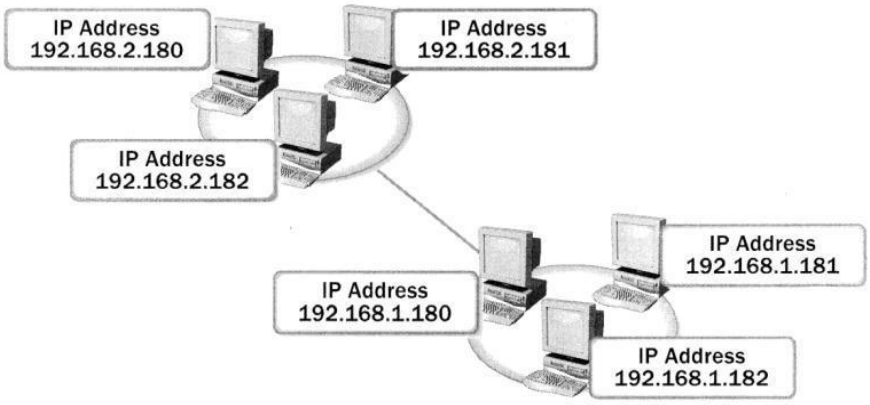

Рис. Пример IP-адресов двух сетей

В этом смысле IP-адреса аналогичны телефонным номерам, содержащим код города, номер АТС и последние цифры, посылающие телефонный вызов владельцу телефонной линии.

IP-адрес сети состоит из номера сети и нулей во всех разрядах, относящихся к номеру узла.

Если в поле номера узла, записанного в двоичной системе счисления, стоят только единицы (в десятичной СС это будет выглядеть как 255), то пакет, имеющий такой адрес, рассылается всем узлам в сети с заданным номером сети. Например, пакет с адресом 192.168.21.255 будет доставлен всем узлам сети 192.168.21.0. Такая рассылка называется *широковещательным сообщением (broadcast).*

Запись IP-адреса не предусматривает специального разграничительного знака между Network ID и Host ID. Каким образом маршрутизаторы выделяют из адреса назначения номер сети, чтобы по нему определить дальнейший маршрут?

Классы подсетей

Традиционный подход заключается в использовании классов. IETF – организация, следящая за Интернетом – делит все IP-адреса на три обобщающих класса – A, B, C.

Примечание. IETF выделяет ещё два класса адресов: D – групповой адрес (multicast) и E, адреса которого зарезервированы для будущих применений.

Каждый класс отличается способом назначения сетевых адресов по сравнению с хостами. Принадлежность IP-адреса к классу определяется значениями нескольких первых битов адреса.

Это разделение диапазонов называется правилом *первого октета*. Любой маршрутизатор сможет прочесть первый октет IP-адреса и интерпретировать биты, чтобы отличить сетевые адреса от адресов хостов.

Табл. Классы сетей

Класс	Первые биты	Первый октет	Число сетей	Число узлов в сети
A	0	1 – 127	126	16.777.214 (2^{24}-2)
B	10	128 – 191	16.384	65.534 (2^{16}-2)
C	110	192 – 223	2.097.152	254 (2^{8}-2)

Если адрес начинается с 0, то этот адрес относится к классу A, в котором под идентификатор сети отводится один байт, а остальные три байта интерпретируются как идентификатор узла в сети. Диапазон адресов класса A – от 0.0.0.0 до 127.0.0.0. Однако сеть не может состоять из одних нулей, а 127.0.0.0 зарезервирован. Остаётся 126 сетей.

Примечание. IP-адрес, первый октет которого равен 127, используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы петля. Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Этот адрес называется *loopback*.

Сетей класса A немного, зато количество узлов в них может достигать 2^{24}-2.

Примечание. Для выполнения расчёта количества хостов два зарезервированных адреса должны быть удалены из пула: 0 для адреса данной сети и 255 для широкого вещания.

Если первые два бита IP-адреса равны 10, то адрес относится к *классу B*. В нём под номер сети и под номер узла отводится по два байта.

Если адрес начинается с 110, то это IP-адрес *класса С*. В этом случае под номер сети отводится три байта, а под номер узла – один байт.

Только очень небольшое число организаций может иметь адреса класса А. Большинство пользователей для связи с Интернетом используют IP-адреса классов В и С.

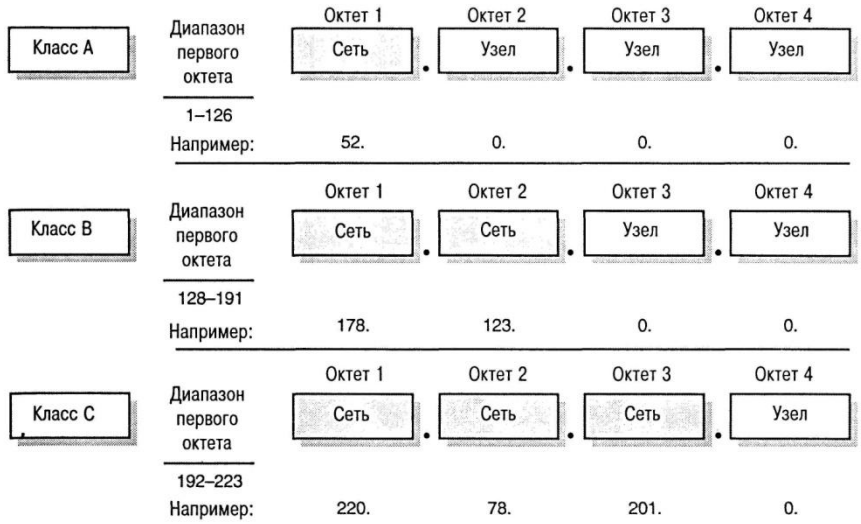

Рис. Форматы IP-адресов сетей различных классов

Второй подход основан на использовании *маски подсети*. Маска – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит непрерывную последовательность единиц в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети, переходящую в непрерывную последовательность нулей в разрядах, соответствующих номеру узла. Т.е. граница между последовательностью единиц и последовательностью нулей в маске соответствует границе между номером сети и номером узла в IP-адресе.

Чем больше битов используется для маски подсети, тем больше доступно подсетей, но меньше хостов на каждую подсеть. Использование большего количества битов, чем нужно, позволит увеличить количество подсетей, но ограничит количество хостов. Использование меньшего количества битов, позволит увеличить количество хостов, но ограничит количество подсетей.

Математическая операция сопоставления IP-адреса и маски подсети называется ANDing. Если побитно логически сложить IP-адрес узла и маску, то результатом будет IP-адрес сети.

Для стандартных классов сетей маски имеют следующие значения:

- класс А – 11111111.00000000.00000000.00000000 (255.0.0.0);
- класс В – 11111111.11111111.00000000.00000000 (255.255.0.0);
- класс С – 11111111.11111111.11111111.00000000 (255.255.255.0).

Однако, снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать систему адресации более гибкой. Например, если IP-адрес 135.10.11.5 ассоциировать с маской 255.255.255.0, то номером сети будет 135.10.11.0, а не 135.10.0.0, как это определено системой классов.

Использование масок при IP-адресации

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8.

Если границу единиц и нулей в маске сдвинуть на несколько разрядов, то эта операция называется *маскированием*. А такая маска будет называться *бесклассовой*.

В зависимости от преследуемых целей, граница маски может быть сдвинута вправо или влево.

Supernetting

Если требуется большее количество сетевых адресов, чем может быть предоставлено в соответствии с классом выделенной сети, то границу единиц и нулей маски перемещают *влево*.

Такая операция называется *supernetting*.

На основе этого механизма поставщики услуг могут объединять адресные пространства нескольких сетей с целью уменьшения таблиц маршрутизации и повышения за счёт этого производительности маршрутизаторов.

Например, предприятию нужно объединить в сеть 2 тысячи компьютеров. Если приобрести сеть класса C, то диапазона адресов для хостов не хватит. Если же приобретать сеть класса B, то это расход лишних средств и, что ещё более важно, неэффективный расход IP-адресов, потому что более 14 тысяч адресов окажутся «не у дел». Решить вопрос можно при помощи операции сабнеттинга.

Напомним, что количество узлов, которое может принадлежать сети, можно подсчитать при помощи формулы $2^n - 2$, где n – это количество нулей в маске.

Поэтому для подсчёта количества разрядов, в которых у новой маски будут стоять нули, можно использовать формулу:

$x = log_2 N,$

где N – требуемое количество узлов в сети. При необходимости x нужно округлить до целого в большую сторону.

Например, для двух тысяч адресов узлов необходимо 11 нулевых битов в маске, и маска будет выглядеть как 11111111.11111111.11111000.00000000 или 255.255.248.0.

Руководство для выбора маски при сабнеттинге

1. Выбор количества битов

Первый шаг сабнеттинга – это выбор количества битов, которые должны быть взяты из идентификатора узла (Host ID) и присвоены идентификатору подсети (Subnet ID). Количество битов определяется требуемым количеством подсетей и количеством хостов на каждую подсеть.

Формула 2n подсчитывает количество подсетей, которое может быть создано с помощью n битов. Например, с помощью 3-х битов можно выделить 23 = 8 подсетей.

Т.е. нужно определить, в какую степень нужно возвести двойку, чтобы получить нужное количество подсетей. Математически это записывается как $\log_2 N$, где N – требуемое количество подсетей. При необходимости x нужно округлить до целого в большую сторону.

В следующем примере сеть 172.20.0.0 делится на подсети с использованием трёх битов из Host ID. В таблице приведены IP-адреса подсетей.

Табл. IP-адреса подсетей

	Двоичный формат	Десятичный формат
Исходный IP-адрес сети	10101100.00010100.00000000.00000000	172.20.0.0
Исходная маска подсети	11111111.11111111.00000000.00000000	255.255.0.0
Новая маска подсети	11111111.11111111.**111**00000.00000000	255.255.224.0
IP-адрес подсети 1	10101100.00010100.**000**00000.00000000	172.20.0.0
IP-адрес подсети 2	10101100.00010100.**001**00000.00000000	172.20.32.0
IP-адрес подсети 3	10101100.00010100.**010**00000.00000000	172.20.64.0
IP-адрес подсети 4	10101100.00010100.**011**00000.00000000	172.20.96.0
IP-адрес подсети 5	10101100.00010100.**100**00000.00000000	172.20.128.0
IP-адрес подсети 6	10101100.00010100.**101**00000.00000000	172.20.160.0
IP-адрес подсети 7	10101100.00010100.**110**00000.00000000	172.20.192.0
IP-адрес подсети 8	10101100.00010100.**111**00000.00000000	172.20.224.0

2. Определение IP-адресов подсетей

Если в маске подсети много битов, то перебор двоичных чисел, как в табл. 5.2, будет трудоёмким. Для определения IP-адресов подсетей можно использовать следующий метод:

1. Пропишите новую маску путём добавления к ней слева направо единичных битов, количеством, равным количеству битов Subnet ID. Например, если это три бита, то маска подсети будет равна 11100000.
2. Конвертируйте бит с наименьшим значением в десятичный формат. Это приращение, которое используется для определения следующего IP-адреса подсети. Например, если у вас три бита – наименьшее значение -32.
3. Начните с нуля, прибавляя полученное в п.2 приращение для каждой последующей подсети, пока вы не пронумеруете максимальное количество подсетей.

3. Определение диапазона IP-адресов узлов

Чтобы быстро подсчитать количество хостов, доступных в подсети, вы можете использовать формулу $2^n - 2$, где n – количество битов, оставшихся для Host ID.

В пределах подсети не все комбинации битов могут быть использованы для хостов. Когда все биты для хостов равны нулю, то это означает адрес подсети. Когда все биты для хоста равны единицы, комбинация представляет Broadcast (широковещательную рассылку) для этой подсети. Когда формула $2^n - 2$ используется для подсчёта количества хостов в подсети, «минус два» представляет собой удаление адреса подсети и адреса Broadcast.

Следующая таблица представляет несколько подсетей, первый хост в каждой подсети, последний хост в каждой подсети и адрес Broadcast. Выделенные биты – это биты подсети.

Табл. Диапазон IP-адресов узлов и Broadcast

	Двоичный формат	Десятичный формат
Исходный IP-адрес сети	10101100.00010100.00000000.00000000	172.20.0.0

Исходная маска подсети	11111111.11111111.00000000.00000000	255.255.0.0
Новая маска подсети	11111111.11111111.**111**00000.00000000	255.255.224.0
Подсеть 1	10101100.00010100.**000**00000.00000000	172.20.0.0
Первый хост подсети 1	10101100.00010100.**000**00000.00000001	172.20.0.1
Последний хост подсети 1	10101100.00010100.**000**11111.11111110	172.20.31.254
Broadcast подсети 1	10101100.00010100.**000**11111.11111111	172.20.31.255
Подсеть 2	10101100.00010100.**001**00000.00000000	172.20.32.0
Первый хост подсети 2	10101100.00010100.**001**00000.00000001	172.20.32.1
Последний хост подсети 2	10101100.00010100.**001**11111.11111110	172.20.63.254
Broadcast подсети 2	10101100.00010100.**001**11111.11111111	172.20.63.255

IP-адреса общего пользования и частные адреса

Все IP-адреса можно разделить на две группы - адреса общего пользования и частные.

Адреса общего пользования (public) – это те адреса, по которым любой компьютер, соединённый с Интернетом, может получить доступ к веб-сайту.

IANA назначает диапазоны IP-адресов общего пользования для организаций, чтобы те впоследствии могли присваивать эти адреса индивидуальным компьютерам. Это предохраняет организации от использования одних и тех же IP-адресов общего пользования.

Частные (private) адреса используются только в рамках локальной сети. Их использование позволяет различным локальным сетям использовать одни и те же IP-адреса.

Это возможно, потому что IANA резервирует для частного использования три блока IP-адресов:

- С 10.0.0.0 по 10.255.255.255. Блок 10 – это один сетевой номер класса A.
- С 172.16.0.0 по 172.31.255.255. Блок 172 – это 16 сетевых номеров класса B.
- С 192.168.0.0 по 192.168.255.255. Блок 192 – это 256 сетевых номеров класса C.

Не существует официальных правил, когда использовать один из перечисленных блоков частных сетевых IP-адресов. Обычно используют тот, который больше подходит по размеру.

Адреса, входящие в эти диапазоны, вычеркнуты из таблиц глобальной маршрутизации Интернета. Если кто-то, находящийся за пределами локальной сети, запросит или передаст информацию на адрес, например, 192.168.0.4, то ему будет отказано: этот адрес не является глобально маршрутизируемым.

Для того чтобы узлы с частными адресами могли через Интернет связываться между собой или с узлами, имеющими глобальные адреса, необходимо использовать технологию *трансляции сетевых адресов (Network Address Translation, NAT)*.

Это осуществляется через так называемые NAT-маршрутизаторы, которые, получая пакеты от узлов обслуживаемой сети, заменяют указанный адрес на уникальный IP-адрес и транслируют дальше пакеты. Уникальность компьютеров во внутренней сети обеспечивается за счёт номеров портов, идентифицирующих соединение. В NAT-маршрутизаторе ведётся специальная таблица, предназначенная для преобразования сетевых адресов.

Одной из наиболее популярных причин использования технологии NAT является дефицит IP-адресов. Если по каким-либо причинам предприятию, у которого имеется потребность

подключения к Интернету, не удаётся получить у поставщика услуг необходимого количества глобальных IP-адресов, то оно может прибегнуть к технологии NAT.

Потребность в трансляции IP-адресов возникает и тогда, когда предприятие из соображений безопасности желает скрыть адреса узлов своей сети, чтобы не дать возможности злоумышленникам составить представление о структуре и масштабах своей сети, а также о структуре и интенсивности исходящего и входящего трафиков.