ТИПЫ АДРЕСОВ СТЕКА TCP/IP

Стек протоколов TCP/IP предназначен для соединения отдельных подсетей, построенных по разным технологиям канального и физического уровней (Ethernet, Token Ring, FDDI, ATM, X.25 и т. д.) в единую составную сеть. Каждая из технологий нижнего уровня предполагает свою схему адресации. Поэтому на межсетевом уровне требуется единый способ адресации, позволяющий уникально идентифицировать каждый узел, входящий в составную сеть. Таким способом в TCP/IP-сетях является *IP-адресация*. Узел составной сети, имеющий IP-адрес, называется *хост* (host).

В стеке TCP/IP используются три типа адресов:

– локальные (другое название – аппаратные);

– IP-адреса (сетевые адреса);

– символьные доменные имена.

Локальный адрес – это адрес, присвоенный узлу в соответствии с технологией подсети, входящей в составную сеть. Если подсетью является локальная сеть Ethernet, Token Ring или FDDI, то локальный адрес – это ***MAC-адрес*** (MAC address – Media Access Control address). MAC-адреса назначаются сетевым адаптерам и портам маршрутизаторов производителями оборудования и являются уникальными, так как распределяются централизованно. MAC-адрес имеет размер 6 байт и записывается в шестнадцатеричном виде, например, 00-08-A0-12-5F-72.

IP-адреса *(IP address)* представляют собой основной тип адресов, на основании которых сетевой уровень передает сообщения, называемые IP-пакетами. Эти адреса состоят из 4 байт, записанных в десятичном виде и разделенных точками, например, 117.52.9.44. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Internet. Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых адаптеров. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьные доменные имена *(domain name)* служат для удобства представления IP-адресов. Символьные имена в IP-сетях называются доменными и строятся по иерархическому признаку. Составляющие полного символьного имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу: RU - Россия, UK - Великобритания, US - США). Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба ***Domain Name System (DNS)***, устанавливающая соответствие между IP-адресами и символьными доменными именами, например, base2.sales.zil.ru. Поэтому доменные имена называют также DNS-именам.

Формат и классы IP-адресов

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых *октетами*.

Наиболее распространенной формой представления IP-адреса является запись в виде четырех чисел, представляющих значения каждого байта в *десятичной форме* и разделенных точками, например: 128.10.2.30

Этот же адрес может быть представлен в *двоичном формате*: 10000000 00001010 00000010 00011110.

А также в *шестнадцатеричном формате*: 80.0A.02.1D

Следует заметить, что максимальное значение октета равно 11111111 (двоичная система счисления), что соответствует в десятичной системе 255.

Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона.

IP-адрес состоит из двух логических частей – ***номера подсети (ID подсети)*** и ***номера узла (ID хоста)*** в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом:

ID подсети: 172.16.0.0.

ID хоста: 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно 2N – 2. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно 216 – 2 = 65534 узла.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа:

1) с помощью классов
2) с помощью масок.

Общее правило: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Признаком, на основании которого IP-адрес относят к тому или иному классу, являются значения нескольких первых битов адреса.

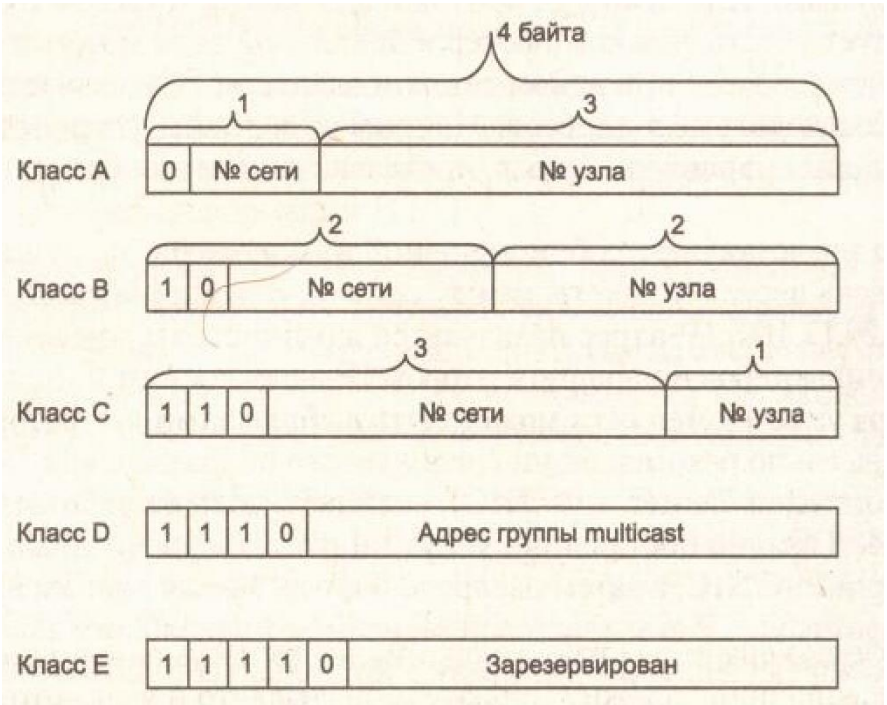

Таблица - Классы IP-адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.1.0	223.255.255.0	2097152	$2^{8} - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Адреса ***класса A*** предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов.

Адреса ***класса B*** используются в сетях среднего размера, например, сетях университетов и крупных компаний.

Адреса класса C используются в сетях с небольшим числом компьютеров.

Адреса класса D используются при обращениях к группам машин.

Адреса класса E зарезервированы на будущее.

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей:

- Если все биты IP-адреса равны нулю, адрес обозначает узел- отправитель и используется в некоторых сообщениях ICMP.
- Если все биты ID сети равны 1, адрес называется *ограниченным широковещательным (limited broadcast)*, пакеты, направленные по такому адресу, рассылаются всем узлам той подсети, в которой находится отправитель пакета.
- Если все биты ID хоста равны 1, адрес называется *широковещательным (broadcast)*, пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
- Если все биты ID хоста равны 0, адрес считается идентификатором подсети (subnet ID).

Особый смысл имеет IP-адрес, первый октет которого равен 127. Этот адрес является *внутренним адресом стека протоколов* компьютера (или маршрутизатора). Он используется для тестирования программ, а также для организации работы клиентской и серверной частей приложения, установленных на одном компьютере. Обе программные части данного приложения спроектированы в расчете на то, что они будут обмениваться сообщениями по сети. В IP-сети запрещается присваивать сетевым интерфейсам IP-адреса, начинающиеся со значения 127. Когда программа посылает данные по IP-адресу 127.x.x.x, то данные не передаются в сеть, а возвращаются модулям верхнего уровня того же компьютера, как только что принятые. Маршрут перемещения данных образует «петлю», поэтому этот адрес называется *адресом обратной петли* (loopback).

Форма *группового IP-адреса - multicast* - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Групповой адрес не делится на номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение групповых адресов распространение информации по схеме «один ко многим». Основное назначение multicast-адресов - распространение информации по схеме “один-ко-многим”. Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Manageme Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, подключенных к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам и те передают эту информацию хосту, инициатору создания новой группы. Групповая адресация предназначена для экономичного распространения в Internet или

большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей.

Новый протокол Ipv6 использует 128-разрядные адреса для идентификации устройств и применяет другую схему адресации. В новой схеме адресации Ipv6 появилась концепция общего адреса, которая позволяет присваивать один и тот же адрес разным устройствам. Посланный по общему адресу пакет доставляется единственному устройству, которое является ближайшим по определению маршрутизатора устройством среди всех имеющих данный адрес.

Использование масок в IP-адресации

Маска - число, которое служит для выделения частей IP-адреса, чтобы TCP/IP мог отличать номер сети от номера хоста. Используя маску подсети, TCP/IP-хосты могут связаться и определить, где находится хост назначения: в локальной или удаленной сети. Пример маски подсети: 255.255.255.0.

Биты IP-адреса, определяющие номер IP-сети, в маске подсети должны быть равны 1, а биты, определяющие номер узла, в маске подсети должны быть равны 0. Для стандартных классов сетей маски имеют следующие значения:

-класс A - 11111111. 00000000. 00000000. 00000000 (255.0.0.0);

-класс B - 11111111.11111111. 00000000. 00000000 (255.255.0.0);

-класс C-11111111.11111111.11111111. 00000000 (255.255.255.0).

Маски подсетей могут использоваться для маскирования тех частей адреса, которые согласно структуре класса, определяются как адреса сети. На практике разделение на подсети применяется в случае, когда конкретное сетевое адресное пространство разбивается дальше на отдельные подсети.

Подсети являются удобным средством структуризации сетей в рамках одной организации, когда все адресное пространство сети internet может быть разделено на непересекающиеся подпространства - "*подсети*", с каждой из которых можно работать как с обычной сетью TCP/IP. Таким образом единая IP-сеть организации может строиться как объединение подсетей. При этом организация должна получить один сетевой номер.

Механизм масок широко распространен в IP-маршрутизации, причем маски могут использоваться для самых разных целей. С их помощью администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей. На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых "префиксов" с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов.

Отображение IP-адресов на локальные адреса

Для определения локального адреса по IP-адресу используется *протокол разрешения адреса (Address Resolution Protocol, ARP)*. Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети или же протокол глобальной сети (X.25, frame relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется *реверсивным ARP* (Reverse Address Resolution Protocol, RARP) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например, драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения.

Работа протокола ARP начинается с просмотра так называемой ARP-таблицы. Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Для каждой сети, подключенной к сетевому адаптеру компьютера или к порту маршрутизатора, строится отдельная ARP-таблица.

В ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых операциях. Поскольку такой способ хранения информации называют *кэшированием*, ARP-таблицы иногда называют ARP-кэш.

После того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно.

Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес, а затем отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Ответ присылает узел, опознавший свой IP-адрес. Если в сети нет машины с искомым IP-адресом, то ARP-ответа не будет. Протокол IP уничтожает IP-пакеты, направляемые по этому адресу. Некоторые реализации IP и ARP не ставят IP-пакеты в очередь на время ожидания ARP-ответов. Вместо этого IP-пакет просто уничтожается, а его восстановление возлагается на модуль TCP или прикладной процесс, работающий через UDP. Такое восстановление выполняется с помощью тайм-аутов и повторных передач. Повторная передача сообщения проходит успешно, так как первая попытка уже вызвало заполнение ARP-таблицы.

Система доменных имен DNS

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы.

DNS (Domain Name System - система доменных имен) - это централизованная служба, основанная на распределенной базе отображений «доменное имя — IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS использует текстовые файлы почти такого формата, как и файл hosts, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов hosts. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер. Этот сервер может хранить отображения «доменное имя — IP-адрес» для всего домена, включая все его поддомены. Однако при этом решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности. Чаще сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. (Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети.

Процедура поиска адреса файла по символьному имени заключается в последовательном просмотре каталогов, начиная с корневого. При этом предварительно проверяется кэш и текущий каталог. Для определения IP-адреса по доменному имени также необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным же отличием является то, что файловая система расположена на одном компьютере, а служба DNSпо своей природе является распределенной.

Существуют две основные схемы разрешения DNS-имен. В первом варианте работу по поиску IP-адреса координирует DNS-клиент:

• DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;

• DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;

• DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к NS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает ответ клиенту.

Такая схема взаимодействия называется нерекурсивной или итеративной, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

Во втором варианте реализуется рекурсивная процедура:

• DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;

• если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;

• если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему серверу, поэтому схема называется косвенной или рекурсивной. Практически все DNS-клиенты используют

рекурсивную процедуру.

Для ускорения поиска IP-адресов DNS-серверы широко применяют процедуру кэширования проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на определенное время обычно от нескольких часов до нескольких дней.