**Сетевые протоколы**

**ip**

IP-адреса (IP address) представляют собой основной тип адресов, на основании которого передаются сообщения, называемые IP пакетами. Эти адреса состоят из 4 байт, записанных в десятичном виде и разделенных точками, например 117.52.9.44. Номер узла в протоколе IP обозначается в последних значениях адреса, а номер сети (в которую входит узел), обозначается в первых значениях адреса

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

00010001 11101111 00101111 01011110

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94.

Следует заметить, что максимальное значение октета равно 111111112 (двоичная система счисления), что соответствует в десятичной системе 255\*\*10.

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 (ID1 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 2\*\*N – 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.

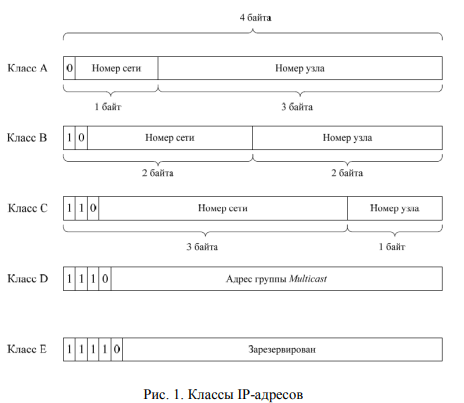
Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа: с помощью классов и с помощью масок.

**Классы IP-адресов**

Существует пять классов IP-адресов: A, B, C, D и E. За принадлежность к тому или иному классу отвечают первые биты IP-адреса.

Деление сетей на классы описано в RFC 791 (документ описания протокола IP).

Целью такого деления являлось создание малого числа больших сетей(класса А), умеренного числа средних сетей (класс В) и большого числа малых сетей (класс С).



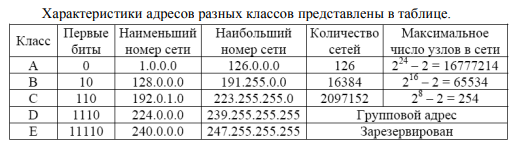
Если адрес начинается с 0, то сеть относят к классу А и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. Сетей класса А немного, зато количество узлов в них может достигать 2\*\*24 – 2, то есть 16 777 214 узлов.

Если первые два бита адреса равны 10, то сеть относится к классу В. В сетях класса В под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса В является сетью средних размеров с максимальным числом узлов 2\*\*16 – 2, что составляет 65 534 узлов.

Если адрес начинается с последовательности 110, то это сеть класса С. В этом случае под номер сети отводится 24 бита, а под номер узла – 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено 2\*\*8 – 2, то есть 254 узлами.

Адрес, начинающийся с 1110, обозначает особый, групповой адрес (multicast). Пакет с таким адресом направляется всем узлам, которым присвоен данный адрес.

Адреса класса Е в настоящее время не используются (зарезервированы для будущих применений).



Применение классов удовлетворительно решало задачу деления на подсети в начале развития Интернета. В 90-е годы с увеличением числа подсетей стал ощущаться дефицит IP-адресов. Это связано с неэффективностью распределения при классовой схеме адресации.

Например, если организации требуется тысяча IP-адресов, ей выделяется сеть класса В, при этом 64534 адреса не будут использоваться.

Существует два основных способа решения этой проблемы:

1) более эффективная схема деления на подсети с использованием масок (RFC 950);

2) применение протокола IP версии 6 (IPv6).

**DHCP**

Протокол DHCP был разработан как расширение по сравнению с *BOOTP*. Он сохранил лучшие аспекты своего предшественника, то есть сохранение и автоматическую доставку данных конфигурации TCP/IP, и при этом был расширен для получения лучшего решения.

DHCP может назначать IP-адреса своим клиентам, используя три различных способа.

* Ручное выделение. Это фактически эквивалент службы *BOOTP*; IP-адреса и другие настройки конфигурации вводятся по отдельности администратором, сохраняются на сервере и доставляются заранее определенным клиентам.
* Автоматическое выделение. Это подход, который мы называем использованием *статического пула*. При первой загрузке рабочей станции клиента DHCP в сети сервер DHCP назначает ему IP-адрес и другие настройки конфигурации из пула имеющихся адресов, которые были сконфигурированы администратором для использования этим сервером; они становятся постоянными настройками для данной машины. Этот метод называется *отображением резервирования*.
* Динамическое выделение. Это тот же метод, что и автоматическое выделение, за исключением того, что настройки TCP/IP не назначаются как постоянные; они лишь предоставляются в аренду на заданный период времени. Эта аренда должна периодически обновляться посредством (автоматического) согласования между клиентом DHCP и сервером.

Эти три метода можно использовать одновременно, обеспечивая все возможности, которые потребуются сетевым администраторам. Ручное выделение – необходимая часть, унаследованная от *BOOTP*, так как часто определенным компьютерам в сети требуется определенный постоянно назначенный IP-адрес, например, серверам World Wide Web и FTP. Преимуществом использования DHCP для таких компьютеров (вместо их ручного конфигурирования) является то, что всю информацию по IP-адресам для всей сети можно хранить в одном месте, и DHCP не позволит любому другому клиенту DHCP использовать адреса, которые были назначены вручную.

В сети, которая изменяется редко, можно использовать DHCP для автоматического выделения IP-адресов, создавая тем самым постоянную сетевую конфигурацию. Если какой-либо компьютер перемещается из одной подсети в другую, ему автоматически назначается новый IP-адрес для этой подсети; однако адрес, использовавшийся в старой подсети, останется занятым, пока администратор не удалит вручную эти назначения из таблицы DHCP.

Если компьютеру динамически выделяется IP-адрес, аренда этого адреса должна периодически обновляться, иначе истечет срок ее действия, что вызовет возврат данного адреса в пул свободных IP-адресов. Процесс обновления аренды выполняется автоматически и незаметен для пользователя (кроме случаев сбоя этого процесса). Если данный компьютер перемещается в другую подсеть, ему назначается подходящий IP-адрес для его новой подсети. Старый адрес возвращается в пул, когда истекает срок его аренды.

Таким образом, динамическое выделение позволило разрешить проблему "блуждающего пользователя", работающего на мобильном компьютере, с которого может выполняться вход в сеть из других офисов, других зданий или даже других городов.

Другие возможности DHCP.

Ясно, что управляемое выделение IP-адресов является наиболее важной функцией DHCP, но сам по себе IP-адрес является недостаточным для полного конфигурирования стека TCP/IP. DHCP может снабжать клиента настройками для более чем 50 связанных с TCP/IP параметров, многие из которых предназначены для использования только с компьютерами, которые не являются клиентами Microsoft.

Для DHCP-клиента Windows Server 2003 или предыдущих версий Windows могут задаваться некоторые или все следующие параметры конфигурации (это наиболее употребительные параметры, передаваемые клиентам).

* IP-адрес (IP address). 32-битный разбитый точками на 4 октета десятичный адрес, используемый для идентификации определенного хоста в сети IP.
* Маска подсети (*Subnet mask*). 32-битное разбитое точками на 4 октета десятичное значение, которое отделяет биты адреса сети в IP-адресе от битов адреса хоста.
* Маршрутизатор (Router). IP-адреса шлюза по умолчанию, который будет использоваться клиентом для доступа к удаленным сетям (доступ к этим адресам выполняется в порядке их следования в списке).
* Серверы DNS (DNS servers). IP-адреса серверов DNS, которые будут использоваться клиентом для разрешения (преобразования) имен хостов Интернет в IP-адреса (в порядке их следования в списке).
* Имя домена (Domain name). Имя домена данного клиента.
* Адреса WINS/N-NS (Windows Internet Naming System / NetBIOS Name Server – Система именования для Интернет в Windows / Сервер имен NetBIOS). IP-адреса серверов WINS, которые будут использоваться клиентом для служб регистрации и разрешения имен NetBIOS.
* Тип узла WINS/N-T (Windows Internet Naming System/NetBIOS over TCP/IP).Код, который используется, чтобы указать, какие методы разрешения имен и в каком порядке будут использоваться клиентом.
* Идентификатор области NetBIOS (NetBIOS scope ID). Символьная строка, используемая для идентификации группы машин NetBIOS, которые могут взаимодействовать только друг с другом. (Избегайте использования такой группы: она вызывает почти всегда слишком много проблем.)

Имеются также несколько других параметров, которые используются реже, чем приведенные выше параметры. Тем не менее, они могут быть полезны клиентам в зависимости от их окружения. Вот названия некоторых из них.

* Cookie-серверы
* LPR-серверы
* Impress-серверы
* Серверы местоположения ресурсов
* Хост-имя (Host name)

**DNS**

DNS (Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IPадреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Начиная с 2010 года, в систему DNS внедряются средства проверки целостности передаваемых данных, называемые DNS Security Extensions (DNSSEC). Передаваемые данные не шифруются, но их достоверность проверяется криптографическими способами. Внедряемый стандарт DANE обеспечивает передачу средствами DNS достоверной криптографической информации (сертификатов), используемых для установления безопасных и защищённых соединений транспортного и прикладного уровней.

Ключевые характеристики DNS:

* Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.
* Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.
* Кеширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
* Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.
* Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

Ключевыми понятиями DNS являются:

• Домеен (domain — область) — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вначале корневой домен (не имеющий идентификатора), ниже идут домены первого уровня (доменные зоны), затем — домены второго уровня, третьего и т.д.

• Поддомен (subdomain) — подчинённый домен. Теоретически деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. На практике больше трёх уровней встречается крайне редко.

• Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному Доменному имени, узлу в дереве имен), тип и поле данных, формат и содержание которого зависит от типа.

• Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен, а чаще — одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации (делегирование).

• Делегирование — операция передачи ответственности за часть дерева доменных имен другому лицу или организации. За счет делегирования в DNS обеспечивается распределенность администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону, и размещении этой зоны на DNS-сервере, управляемом этим лицом или организацией.

• DNS-сервер — специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется.

• DNS-клиент — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

• Авторитетность — признак размещения зоны на DNS-сервере. Ответы DNSсервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (англ. Non-authoritative), когда сервер обрабатывает запрос, и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).

• DNS-запрос (DNS query) — запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным.

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS (от англ. authoritative — авторитетный), на котором расположена информация о домене.

Корневой домен:

Корневой домен (нулевой домен, root domain) — домен самого верхнего уровня в любой системе доменных имён. Обслуживается корневыми серверами системы доменных имен, которые располагаются в различных странах мира. Обозначается пустым именем. При записи доменного имени, каждый домен отделяется точкой; в конце имени может присутствовать точка, которая отделяет пустое имя, соответствующее корневому домену. Если эта точка есть (например «www.example.com.»), то доменное имя считается полным (абсолютным). Если точки в конце имени нет («www.example» или «www.example.com»), то имя считается относительным. Каждое интернет-приложение должно правильно обрабатывать завершающую точку, однако большинство приложений позволяют вводить доменное имя без точки в конце; обработка зависит от реализации. В простейшем случае к адресу добавляется завершающая точка, и он трактуется как абсолютный. В ряде случаев для получения полного доменного имени локальное программное обеспечение (либо приложение, либо операционная система) может присоединить к относительному имени некоторый домен по умолчанию, который определяется по доменному имени компьютера или может быть задан в настройках. Иногда в настройках может быть задано несколько таких доменов, которые перебираются по очереди, до тех пор, пока не будет найдено существующее в DNS имя. Такой подход может приводить к неоднозначности, которая может быть разрешена с помощью задания полного имени.

Корневые серверы:

Корневые серверы DNS — DNS-серверы, содержащие информацию о доменах верхнего уровня, указывающую на DNS-серверы, поддерживающие работу каждого из этих доменов. Основные корневые серверы DNS размещены в домене root-servers.org и обозначаются латинскими буквами от A до М. Они управляются различными организациями, действующими по согласованию с ICANN1 . Количество серверов ограничено в связи с максимальным объёмом UDP-пакета (большее количество серверов потребовало бы перехода на TCP-протокол для получения ответа, что существенно бы увеличило нагрузку). У многих корневых серверов DNS существуют зеркала. В частности, российское зеркало сервера F расположено в РосНИИРОС в Москве, сервера K в Новосибирске, а сервера L в Ростове-на-Дону. Из-за существовавших в прошлом ограничений на размеры DNS-пакета (512 байт) в DNS ответ могло быть помещено всего 13 серверов (от A до M — тринадцатой буквы в алфавите), сейчас за этими 13 именами стоят более 200 серверов. Ближайший (к пользователю) адрес «зеркала» корневого сервера выбирается автоматически благодаря IP AnyCast2 . Так, при обращении к K.root-servers.net, пользователь из Новосибирска скорее всего обратится к новосибирскому серверу.