Адресация в IP-сетях

- Один компьютер может иметь несколько сетевых интерфейсов. Например, для создания полносвязной структуры из N компьютеров необходимо, чтобы у каждого из них имелся N - 1 интерфейс.
- По количеству адресуемых интерфейсов адреса можно классифицировать следующим образом:

• **уникальный адрес (unicast**) используется для идентификации отдельных интерфейсов;

• **групповой адрес** (**multicast**) идентифицирует сразу несколько интерфейсов, поэтому данные, помеченные групповым адресом, доставляются каждому из узлов, входящих в группу;

• данные, направленные по **широковещательному адресу** (**broadcast**), должны быть доставлены всем узлам сети;

• адрес **произвольной рассылки** (**anycast**), определенный в новой версии протокола IPv6, так же, как и групповой адрес, задает группу адресов, однако данные, посланные по этому адресу, должны быть доставлены не всем адресам данной группы, а любому из них.

- Адреса могут быть **числовыми** (например, 129.26.255.255 или 81.la.ff.fF) и **символьными** (site.domen.ru, willi-winki).
- Множество всех адресов, которые являются допустимыми в рамках некоторой схемы адресации, называется **адресным пространством.**

Адресация в IP-сетях

- Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: **физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).**
- ***Физический, или локальный адрес узла,*** определяемый технологией, с помощью которой построена сеть, в которую входит узел.

Для узлов, входящих в локальные сети - это **MAC–адрес** сетевого адаптера или **порта** маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано.

- Для всех существующих технологий локальных сетей **MAC – адрес** имеет формат **6 байтов**: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Сетевой (IP-адрес)

- ***Сетевой, или IP-адрес***, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне.

Он 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 (Network Information Center, NIC), если сеть должна работать как составная часть Internet.

Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами. Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться произвольно. Узел может входить в несколько IP-сетей. В этом случае узел должен иметь несколько IP-адресов, по числу сетевых связей. IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьный адрес

- **Символьный адрес, или DNS-имя**, например, SERV1.IBM.COM.
- Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или telnet.
- Все IP-адреса протокола IPv4 делятся на **публичные/глобальные/внешние** (их называют "белые") — они используются в сети Интернет, и **частные/локальные/внутренние** (их называют "серые") — используются в локальной сети.

Каждый узел в объединенной сети, как указывалось выше, должен иметь свой уникальный IP-адрес, состоящий из двух частей — номера сети и номера узла. Какая часть адреса относится к номеру

Рис.1 Классы адресов в сети Интернет

сети, а какая к номеру узла, определяется значениями первых битов адреса.

класс A — 0. 0. 0. 0 ... 127. 255. 255. 255;
класс B — 128. 0. 0. 0 ... 191. 255. 255. 255;
класс C — 192. 0. 0. 0 ... 223. 255. 255. 255;
класс D — 224. 0. 0. 0 ... 239. 255. 255. 255;
класс E — 240. 0. 0. 0 ... 247. 255. 255. 255.

С помощью специального механизма маскирования любая сеть, в свою очередь, может быть представлена набором более мелких сетей.

Определение номеров сети по первым байтам адреса — не вполне гибкий механизм для адресации. В настоящее время получили широкое распространение маски. Маска — это тоже 32-разрядное число, она имеет такой же вид, как и IP-адрес. Маска используется в паре с IP-адресом, но не совпадает с ним.

Принцип определения номера сети и номера узла в IP-адресе с использованием маски состоит в следующем. Двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны представляться как номер сети, и нули в тех разрядах, которые представляются как номер хоста. Кроме того, поскольку номер сети является целой частью адреса, единицы в маске должны представлять непрерывную последовательность.

Каждый класс IP-адресов (A, B, C) имеет свою маску, используемую по умолчанию:

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).

Адресация в IP-сетях

- Если адрес начинается с 0, то сеть относят к ***классу A*** 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. (Номер 0 не используется, а номер 127 зарезервирован для специальных целей). Сетей класса А немного, зато количество узлов в них может достигать 2^{24}, то есть **16 777 216 узлов**.
- Если первые два бита адреса равны 10, то сеть относится к ***классу B***.
- 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}, что составляет **65 536 узлов**.

Адресация в IP-сетях

- 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 28, то есть **256 узлами**.
- Если адрес начинается с последовательности **1110**, то он является адресом ***класса D*** *и* обозначает особый, **групповой адрес - multicas**t. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым присвоен данный адрес.
- Если адрес начинается с последовательности **11110**, то это значит, что данный адрес относится к ***классу Е.*** Адреса этого класса зарезервированы для будущих применений.

Публичные "белые" IP-адреса

В сети Интернет используются именно публичные глобальные адреса. Публичным IP-адресом называется IP-адрес, который используется для выхода в Интернет. Публичные (глобальные) IP-адреса маршрутизируются в Интернете, в отличие от частных адресов.

Наличие публичного IP-адреса на вашем роутере или компьютере позволит организовать собственный сервер (VPN, FTP, WEB и др.), удаленный доступ к компьютеру, камерам видеонаблюдения, и получить к ним доступ из любой точки глобальной сети. С "белым" IP-адресом можно организовать любой собственный домашний сервер для публикации его в сети Интернет: веб (HTTP), VPN (PPTP/IPSec/OpenVPN), медиа (аудио/видео), FTP, сетевой накопитель NAS, игровой сервер и т.д.

Примечание: Все публичные серверы и сайты в сети Интернет используют "белые" IP-адреса (например, сайт google.com — 172.217.22.14, DNS-сервер Google — 8.8.8.8, сайт yandex.ru — 213.180.204.11, DNS-сервер Яндекс.DNS — 77.88.8.8). Все публичные IP-адреса в сети Интернет уникальны и не могут повторяться.

Частные "серые" IP-адреса

Частные внутренние адреса не маршрутизируются в Интернете и на них нельзя отправить трафик из Интернета, они работают только в пределах локальной сети.
К частным "серым" адресам относятся IP-адреса из следующих подсетей:

- От **10.0.0.0 до 10.255.255.255** с маской 255.0.0.0 или /8
- От **172.16.0.0 до 172.31.255.255** с маской 255.240.0.0 или /12
- От **192.168.0.0 до 192.168.255.255** с маской 255.255.0.0 или /16
- От **100.64.0.0 до 100.127.255.255** с маской подсети 255.192.0.0 или /10; данная подсеть рекомендована согласно rfc6598 для использования в качестве адресов для CGN (Carrier-Grade NAT)

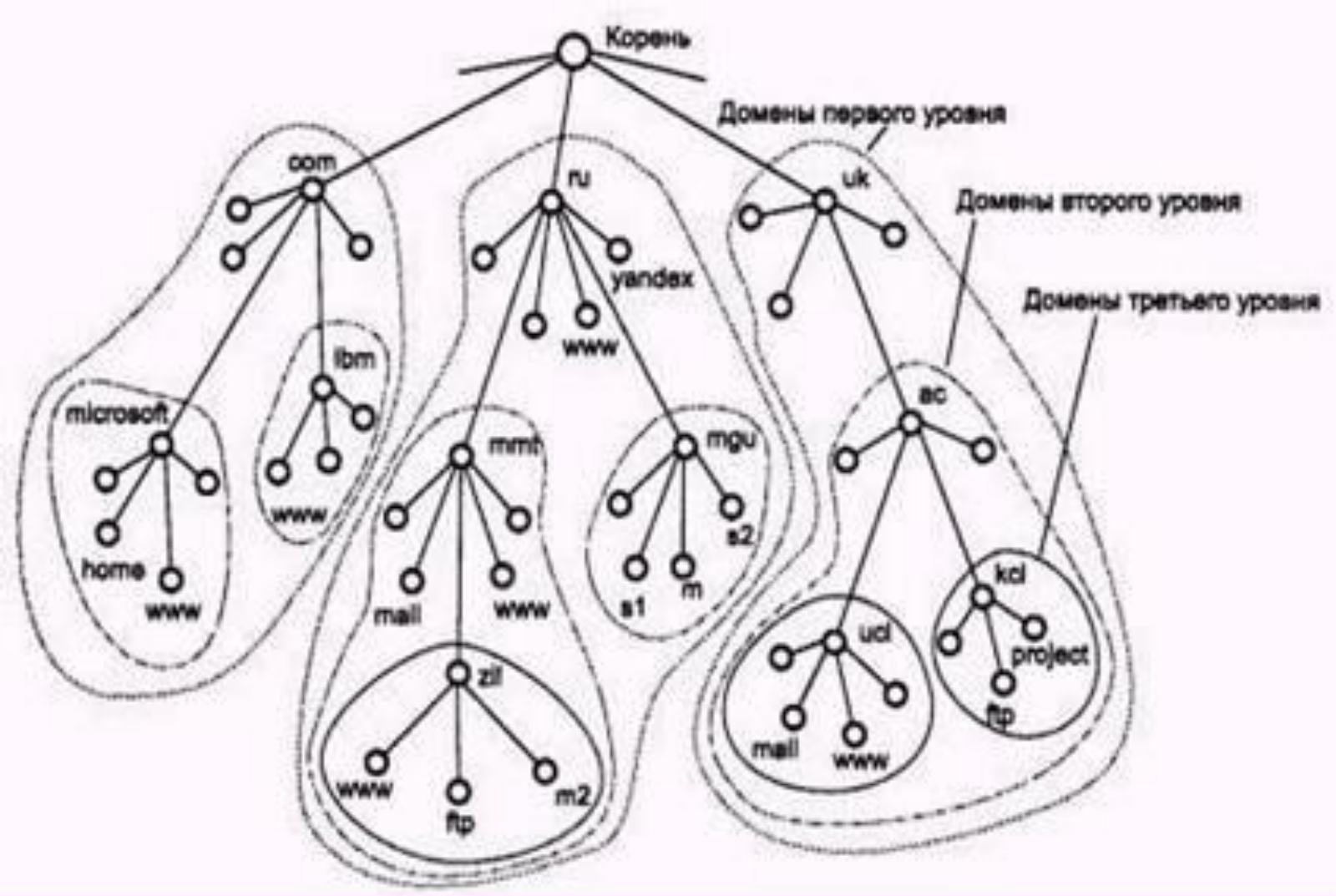
Это зарезервированные IP-адреса. Такие адреса предназначены для применения в закрытых локальных сетях, распределение таких адресов никем не контролируется. Напрямую доступ к сети Интернет, используя частный IP-адрес, невозможен. В этом случае связь с Интернетом осуществляется через NAT (трансляция сетевых адресов заменяет частный IP-адрес на публичный). Частные IP-адреса в пределах одной локальной сети должны быть уникальны и не могут повторяться.

Построение доменных имен

- ***Система доменных имен (Domain Name System, DNS).***
- **DNS** - 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.
- Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов.

Пространство доменных имен

Запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей.



Технология CIDR

- Современные маршрутизаторы используют форму IP адресации называемую **безклассовой междоменной маршрутизацией (Classless Interdomain Routing (CIDR)**), которая игнорирует классы.

В системах, использующих классы, маршрутизатор определяет класс адреса и затем разделяет адрес на октеты сети и октеты хоста, базируясь на этом классе. В CIDR маршрутизатор использует биты маски для определения в адресе сетевой части и номера хоста. Граница разделения адреса может проходить посреди октета.

- CIDR позволяет маршрутизаторам агрегировать или суммировать информацию о маршрутах. Они делают это путём использования маски вместо классов адресов для определения сетевой части IP адреса. Это сокращает размеры таблиц маршрутов, так как используется лишь один адрес и маска для представления маршрутов ко многим подсетям.
- Пример записи *IP*-адреса с применением бесклассовой адресации: **10.1.2.33/27**.
- По-другому такая *запись* называется *запись IP*-адреса не в классическом виде и стиле Cisco. При этом подходе маску подсети записывают вместе с *IP*-адресом в формате *IP-адрес*/количество единичных *бит* в маске.
- Число после слэша означает количество единичных разрядов в маске подсети.

Маски переменной длины VLSM

- **Маска подсети** является необходимым дополнением к IP адресу. Маска переменной длины (Variable-Length Subnet Mask (VLSM)) позволяет организации использовать более одной маски подсети внутри одного и того же сетевого адресного пространства. Реализацию VLSM часто называют «подсети на подсети».
- Если бит в IP адресе соответствует единичному биту в маске, то этот бит в IP адресе представляет номер сети, а если бит в IP адресе соответствует нулевому биту в маске, то этот бит в IP адресе представляет номер хоста.
- Так для маски 255.255.0.0 и адреса 172.24.100.45 номер сети будет 172.24.0.0, а для маски 255.255.255.0 номер сети будет 172.24.100.0.
- Другая форма записи маски - /N, **где N – число единиц в маске.** Эта форма используется только в сочетании с IP адресом. Например, для маски 255.255.0.0 и адреса 172.24.100.45 пишут 172.24.100.45/16.
- Все адреса класса **A** имеют маску **255.0.0.0**,
- адреса класса **B** имеют маску **255.255.0.0**, а
- адреса класса **C** имеют маску **255. 255. 255.0**.

Протоколы сопоставления адреса ARP и RARP

- Для определения локального адреса по IP-адресу используется протокол разрешения адреса ***Address Resolution Protocol (ARP)***. **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 реверсивный ARP – ***RARP (Reverse Address Resolution Protocol)*** и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.
- В локальных сетях ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.
- Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует **ARP-запрос**, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос **широковещательно**. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным адресом. В случае их совпадения узел формирует **ARP-ответ**, в котором указывает свой IP-адрес и свой локальный адрес и 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.