Лекция 10-11. Адресация и маршрутизация в сетях. Физические и сетевые адреса

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

1. Физический адрес

Физический, или **локальный адрес узла** определяется технологией, с помощью которой построена сеть, в которую входит узел. Для узлов, входящих в локальные сети, это MAC-адрес сетевого адаптера или порта маршрутизатора.

В качестве стандартного выбран 48-битный формат адреса, что соответствует примерно 280 триллионам различных адресов. Понятно, что столько сетевых адаптеров никогда не будет выпущено.

С тем, чтобы распределить возможные диапазоны адресов между многочисленными изготовителями сетевых адаптеров, была предложена следующая структура адреса (рис. 1).

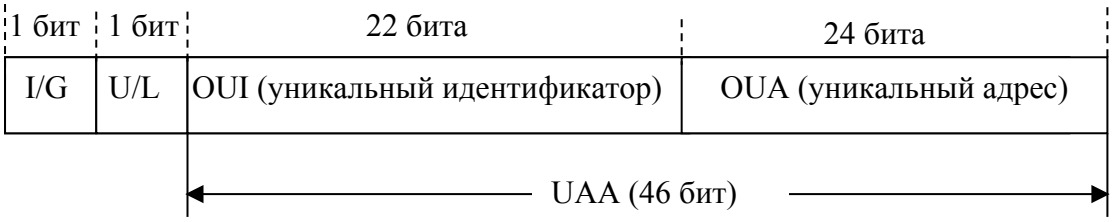

Рис. 1. Структура 48-битного стандартного MAC-адреса

Младшие 24 разряда кода адреса называются OUA (Organizationally Unique Address) – ***уникальный адрес***. Именно их присваивает каждый из зарегистрированных производителей сетевых адаптеров. Всего возможно свыше 16 миллионов комбинаций, то есть каждый изготовитель может выпустить 16 миллионов сетевых адаптеров.

Следующие 22 разряда кода называются OUI (Organizationally Unique Identifier) – ***уникальный идентификатор***. IEEE присваивает один или несколько OUI каждому производителю сетевых адаптеров. Это позволяет исключить совпадения адресов адаптеров от разных производителей. Всего возможно свыше 4 миллионов разных OUI, это означает, что теоретически может быть зарегистрировано 4 миллиона производителей. Вместе OUA и OUI называются UAA (Universally Administered Address) – универсально управляемый адрес или IEEE-адрес.

Два старших разряда адреса управляющие, они определяют тип адреса, способ интерпретации остальных 46 разрядов. Старший бит I/G (Individual/Group) указывает на тип адреса. Если он установлен в 0, то индивидуальный, если в 1, то групповой (многопунктовый или функциональный). Пакеты с групповым адресом получат все имеющие этот

групповой адрес сетевые адаптеры. Причем групповой адрес определяется 46-ю младшими разрядами. Второй управляющий бит U/L (Universal/Local) называется флажком универсального/местного управления и определяет, как был присвоен адрес данному сетевому адаптеру. Обычно он установлен в 0. Установка бита U/L в 1 означает, что адрес задан не производителем сетевого адаптера, а организацией, использующей данную сеть. Это случается довольно редко.

Для широковещательной передачи (то есть передачи всем абонентам сети одновременно) применяется специально выделенный ***сетевой адрес***, все 48 битов которого установлены в единицу. Его принимают все абоненты сети независимо от их индивидуальных и групповых адресов.

Данной системы адресов придерживаются такие популярные сети, как Ethernet, Fast Ethernet, Token-Ring, FDDI, 100VG-AnyLAN. Ее недостатки – высокая сложность аппаратуры сетевых адаптеров, а также большая доля служебной информации в передаваемом пакете.

Во многих сетевых адаптерах предусмотрен так называемый циркулярный режим. В этом режиме адаптер принимает все пакеты, приходящие к нему, независимо от значения поля адреса приемника. Такой режим используется, например, для проведения диагностики сети, измерения ее производительности, контроля ошибок передачи. При этом один компьютер принимает и контролирует все пакеты, проходящие по сети, но сам ничего не передает. В данном режиме работают сетевые адаптеры мостов и коммутаторы, которые должны обрабатывать перед ретрансляцией все пакеты, приходящие к ним.

2. Сетевой адрес

2.1. IP-адресация 4-ой версии

Представление IP-адреса

Адрес IP представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые **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 11111111_2 (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, а 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона: от 0 до 255.

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 $2^N - 2$. 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 $2^{16} - 2 = 65534$ 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.

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

Классы IP-адресов

Существует пять классов IP-адресов: *A, B, C, D* и *E* (см. рис. 1). 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 A*), умеренного числа средних сетей (*класс B*) и большого числа малых сетей (*класс C*).

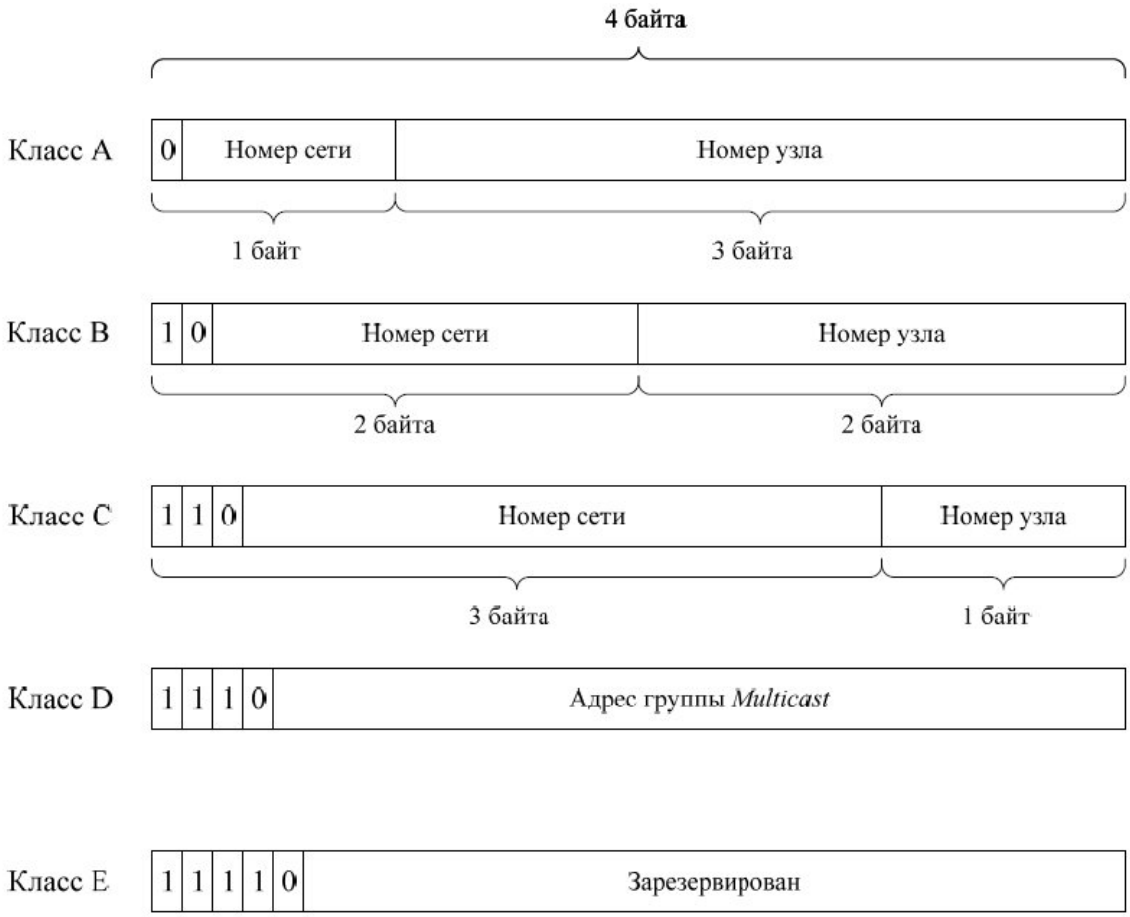

Рис. 1. Классы IP-адресов

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 A* имеют номера в диапазоне от 1 до 126. Сетей *класса A* 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 B*. В сетях класса B под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть *класса B* 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 C*. 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 E* в настоящее время не используются (зарезервированы для будущих применений).

Характеристики адресов разных классов представлены в таблице 1.

Таблица 1

Характеристики IP адресов разных классов

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	

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 B, при этом 64534 адреса не будут использоваться.

Существует два основных способа решения этой проблемы:

- более эффективная схема деления на подсети с использованием масок (RFC 950);
- применение протокола IP версии 6 (IPv6).

Поэтому в настоящее время использовать принцип классов для определения идентификаторов сети и хоста можно и нужно только в случае отсутствия маски подсети.

3. Использование масок

Маска подсети (subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

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).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0).

При использовании масок можно вообще отказаться от понятия классов.

Пример 1.

Пусть задан IP-адрес 17.239.47.94, маска подсети 255.255.0.0 (другая форма записи: 17.239.47.94/16).

Требуется определить ID подсети и ID хоста в обеих схемах адресации.

1) Адресация с использованием классов. Двоичная запись IP-адреса имеет вид:

00010001.11101111.00101111.01011110.

Так как первый бит равен нулю, адрес относится к *классу A*. Следовательно, первый байт отвечает за ID подсети, остальные три байта – за ID хоста:

ID подсети: 17.0.0.0. ID хоста: 0.239.47.94.

2) Адресация с использованием масок. Запишем IP-адрес и маску подсети в двоичном виде:

IP-address: 17.239.47.94 = 00010001.11101111.00101111.01011110 ,
Subnet mask: 255.255.0.0 = 11111111.11111111.00000000.00000000 .

Вспомнив определение маски подсети, можно интерпретировать номер подсети как те биты, которые в маске равны 1, т. е. первые два байта. Оставшаяся часть IP-адреса будет номером узла в данной подсети.

ID подсети: 17.239.0.0. ID хоста: 0.0.47.94.

Номер подсети можно получить другим способом, применив к IP-адресу и маске операцию логического умножения AND:

```
AND 00010001. 11101111. 00101111. 01011110
    11111111. 11111111. 00000000. 00000000 .
    00010001. 11101111. 00000000. 00000000
          17        239         0         0
```

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

Пример 2.

Задан IP-адрес 192.168.89.16, маска подсети 255.255.192.0 (другая форма записи: 192.168.89.16/18).

Требуется определить ID подсети и ID хоста. Воспользуемся операцией AND:

```
IP-address: 17.239.47.94 = AND11000000.10101000.01011001.00010000
Subnet mask: 255.255.0.0 =     11111111.11111111.11000000.00000000
subnet ID:                     11000000.10101000.01000000.00000000
                              192       168      64         0
```

Чтобы получить номер узла, нужно в битах, отвечающих за номер подсети, поставить нули:

Host ID: 00000000.00000000.00011001.00010000 = 0.0.25.16.

Ответ: ID подсети = 192.168.64.0, ID хоста = 0.0.25.16.

Для масок существует важное правило: разрывы в последовательности единиц или нулей недопустимы. Например, не существует маски подсети, имеющей следующий вид:

11111111.11110111.00000000.00001000 (255.247.0.8),

так как последовательности единиц и нулей не являются непрерывными.

С помощью масок администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей.

Пример 3.

Допустим, организации выделена сеть класса *B*: 160.95.0.0 (рис. 2).

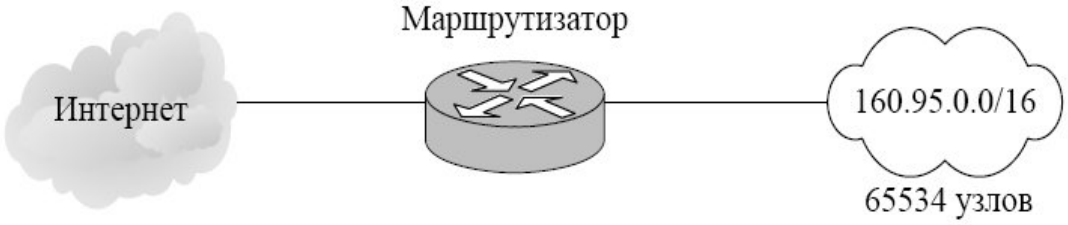

Рис. 2. Сеть *класса B* до деления на подсети

В такой сети может находиться до 65534 узлов. Однако организации требуется 3 независимые сети с числом узлов в каждой не более 254. В этой ситуации можно применить деление на подсети с помощью масок. Например, при использовании маски 255.255.255.0 третий байт адреса будет определять номер внутренней подсети, а четвертый байт – номер узла (рис. 3).

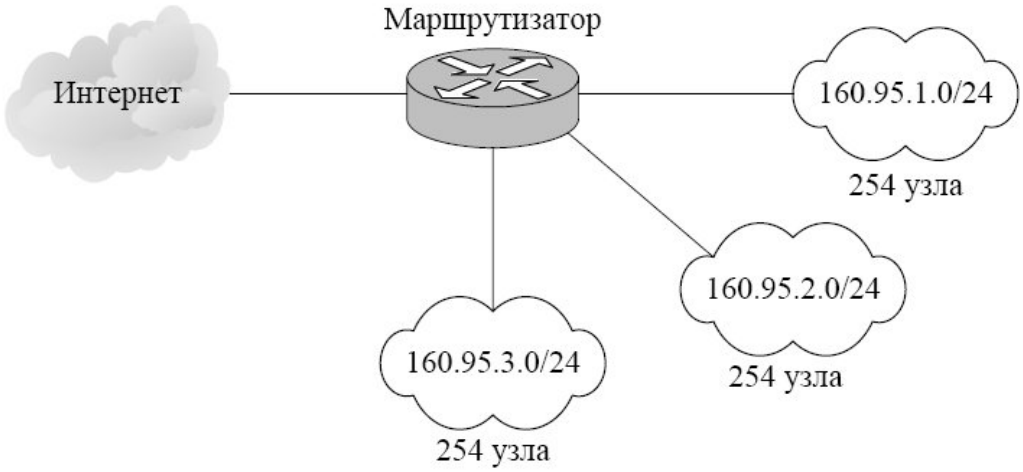

Рис. 3. Сеть класса *B* после деления на подсети

Маршрутизаторы во внешней сети (Интернете) ничего «не знают» о делении сети 160.95.0.0 на подсети, все пакеты направляются на маршрутизатор организации, который переправляет их в требуемую внутреннюю подсеть.

Особые IP-адреса

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

1. Если первый октет ID сети начинается с 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются **loopback** («**петля**», «замыкание на себя») и используются для проверки функционирования стека TCP/IP.
2. Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.
3. Если все биты ID сети равны 0, а все биты ID хоста равны 1, тоадрес называется ***ограниченным широковещательным*** (limited broadcast). Пакеты, направленные по такому адресу рассылаются всем узлам той подсети, в которой находится отправитель пакета. К данному же типу адреса можно относить и IP-адрес, в котором 32 разряда заполнены 1, т.к. пакет с таким адресом устройством, связующим сети, например, коммутатром или маршрутизатором, не будет «выпущен» за пределы сети отправителя.
4. Если все биты ID хоста равны 1, а биты ID сети не равны 0, т.е. однозначно идентифицируют адрес подсети, то адрес называется ***широковещательным*** (broadcast); пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
5. Если все биты ID хоста равны 0, адрес считается **идентификатором подсети** (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети *класса С* не 256, а 254 узлов.

Распределение IPv4-адресов. Частные и публичные адреса

Поскольку каждый узел сети Интернет должен обладать уникальным IP-адресом, то, безусловно, важной является задача координации распределения адресов отдельным сетям и узлам. Такую координирующую роль выполняет Интернет-корпорация по распределению адресов и имен (The Internet Corporation for Assigned Names and Numbers, ICANN).

Естественно, что ICANN не решает задач выделения IP-адресов конечным пользователям и организациям, а занимается распределением диапазонов адресов между крупными организациями-поставщиками услуг по доступу к сети Интернет (Internet Service Provider), которые, в свою очередь, могут взаимодействовать как с более мелкими поставщиками, так и с конечными пользователями. Так, например, функции по распределению IP-адресов в Европе

ICANN делегировал Координационному Центру RIPE (RIPE NCC, The RIPE Network Coordination Centre, RIPE – Reseaux IP Europeens). В свою очередь, этот центр делегирует часть своих функций региональным организациям.

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (1 сеть класса A);

172.16.0.0 – 172.31.255.255 (16 сетей класса B);

192.168.0.0 – 192.168.255.255 (256 сетей класса C).

Любая организация может использовать IP-адреса из этих блоков без согласования с ICANA или Internet-регистраторами. В результате эти адреса используются во множестве организаций. Таким образом, уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. В такой сети каждая рабочая станция может обмениваться информацией с любой другой рабочей станцией частной сети.

Если организации требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Перед распределением адресов из частного и публичного блоков следует определить, какие из рабочих станций сети должны иметь связь с внешними системами на сетевом уровне. Для таких рабочих станций следует использовать публичные адреса, остальным же – можно присваивать адреса из частных блоков, это не помешает им взаимодействовать со всеми рабочими станция частной сети организации, независимо от того, какие адреса используются (частные или публичные). Однако прямой доступ во внешние сети для рабочих станций с адресами из частного блока невозможен. Для организации их доступа во внешние шлюзы придется использовать прокси-серверы.

Перемещение рабочей станции из частной сети в публичную (и обратное) связано со сменой IP-адреса, соответствующих записей DNS и изменением конфигурационных файлов на других рабочих станциях, которые их идентифицируют по IP-адресам. Поскольку частные адреса не имеют глобального значения, маршрутная информация о частных сетях не должна выходить за пределы этих сетей, а пакеты с частными адресами отправителей или получателей не должны передаваться через межсетевые каналы. Предполагается, что маршрутизаторы в публичных сетях (особенно маршрутизаторы провайдеров Internet) будут отбрасывать маршрутную информацию из частных сетей. Если маршрутизатор публичной сети получает такую информацию, ее отбрасывание не должно трактоваться как ошибка протокола маршрутизации.

Также в качестве частной можно выделить еще одну сеть класса B – 169.254.0.0, адреса которой используются для автоматической конфигурации сетевых адаптеров операционной системой Windows при отсутствии либо не работающем DHCP-сервере.

2.2. Протокол IPv6

Общие сведения о протоколе IPv6

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов. Для преодоления ограничений IPv4 был разработан ***протокол IP 6-й версии*** – ***IPv6*** (RFC 2373, 2460).

Протокол IPv6 имеет следующие основные особенности:

- длина адреса 128 бит – такая длина обеспечивает примерно $3{,}4\times10^{38}$ адресов; такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;
- автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP;
- встроенная безопасность – для передачи данных является обязательным использование *протокола защищенной передачи* IPsec (протокол IPv4 также может использовать IPsec, но не обязан этого делать).

В настоящее время многие производители сетевого оборудования включают поддержку *протокола IPv6* в свои продукты, однако преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

Архитектура адресации IPv6

Существует три типа адресов:

- *unicast*: идентификатор одиночного интерфейса. Пакет, посланный по unicast-адресу, доставляется интерфейсу, указанному в адресе. Под интерфейсом в контексте Ipv6 следует понимать это средство подключения узла к каналу.
- *anycast*: идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по anycast-адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации).
- *multicast*: идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по multicast-адресу, доставляется всем интерфейсам, заданным этим адресом.

В отличии от IPv4 протокола, в IPv6 не существует широковещательных адресов − их функции переданы multicast-адресам. Также надо отметить, что в IPv6, все нули и все единицы являются допустимыми кодами для любых полей, если не оговорено исключение.

Модель адресации

Выделяют следующие аспекты модели адресации протокола IPv6:

1. IPv6 адреса всех типов ассоциируются с интерфейсами, а не узлами. Так как каждый интерфейс принадлежит только одному узлу, уникастный адрес интерфейса может идентифицировать узел.

2. IPv6 уникастный адрес соотносится только с одним интерфейсом. Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные). Существует два исключения из этого правила:

a) одиночный адрес может приписываться нескольким физическим интерфейсам, если приложение рассматривает эти несколько интерфейсов как единое целое при представлении его на уровне Интернет.

b) маршрутизаторы могут иметь ненумерованные интерфейсы (например, интерфейсу не присваивается никакого IPv6 адреса) для соединений точка-точка, чтобы исключить необходимость вручную конфигурировать и объявлять эти адреса. Адреса не нужны для соединений точка-точка маршрутизаторов, если эти интерфейсы не используются в качестве точки отправления или назначения при посылке IPv6 дейтограмм.

3. IPv6 соответствует модели IPv4, где подсеть ассоциируется с каналом. Одному каналу могут соответствовать несколько подсетей.

Представление записи Ipv6 адресов

Существует три стандартные формы для представления ipv6 адресов в виде текстовых строк:

1. *Основная форма записи* имеет вид x:x:x:x:x:x:x:x, где 'x' шестнадцатеричные 16-битные числа.

```
fedc:ba98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
```

Необходимо отметить, что ненужно писать начальные нули в каждом из конкретных полей, но в каждом поле должна быть, по крайней мере, одна цифра (за исключением случая, описанного в пункте 2.).

2. *Сокращенная форма записи.* Из-за метода записи некоторых типов IPv6 адресов последние часто содержат длинные последовательности нулевых бит. Для того чтобы сделать запись адресов, содержащих нулевые биты, более удобной, имеется специальный синтаксис для удаления лишних нулей. Использование записи "::" указывает на наличие групп из 16 нулевых бит. Комбинация "::" может появляться только при записи адреса. Последовательность "::" может также использоваться для удаления из записи начальных или завершающих нулей в адресе. Так, например, следующие Ipv6-адреса

1080:0:0:0:8:800:200c:417a	anycast-адрес
ff01:0:0:0:0:0:0:43	multicast-адрес
0:0:0:0:0:0:0:1	адрес обратной связи
0:0:0:0:0:0:0:0	неспецифицированный адрес

могут быть представлены в следующем виде:

1080::8:800:200c:417a	уникаст-адрес
ff01::43	мультикаст адрес
::1	адрес обратной связи
::	не специфицированный адрес

3. *Альтернативная форма записи*, которая более удобна при работе с ipv4 и IPv6, является x:x:x:x:x:x:d.d.d.d, где 'x' шестнадцатеричные 16-битовые коды адреса, а 'd' десятичные 8-битовые, составляющие младшую часть адреса (стандартное IPv4 представление). Прмерами такой записи могут быть следующие Ipv6-адреса:

```
0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38
```

или в сокращенном виде:

```
::13.1.68.3
::FFFF:129.144.52.38
```

Представление типа IPv6-адреса

Специфический тип IPv6 адресов идентифицируется ***лидирующими битами адреса***. Поле переменной длины, содержащее эти лидирующие биты, называется *префиксом формата* (Format Prefix - FP). Некоторые примеры исходных назначений этих префиксов представлены в следующей таблице 2.

Таблица 2

Префиксы IPv6-адресов

Назначение	**Префикс (двоичный)**	**Часть адресного пространства**
Зарезервировано для NSAP	0000 001	1/128
Зарезервировано для IPX	0000 010	1/128
Провайдерские uuunicast-адреса	010	1/8

Зарезервировано для географическихunicast-адресов	100	1/8
Локальные канальные адреса	1111 1110 10	1/1024
Локальные адреса (site)	1111 1110 11	1/1024
multicast-адреса	1111 1111	1/256

Данное распределение адресов поддерживает прямое выделение адресов провайдера, адресов локального применения и multicast-адресов. Зарезервировано место для адресов NSAP, IPX и географических адресов и т.д.

Unicast-адреса отличаются от *multicast-адресов* значением старшего октета: значение FF (11111111) идентифицирует multicast-адрес; любые другие значения говорят о том, что адрес типа unicast. Anycast-адреса берутся из пространства адресов unicast, и синтаксически неотличимы от них. Обычно говорят, что как только один и тот же unicast-адрес присвоен двум и более интерфейсам, то он становится *anycast-адресом*.

Unicast IPv6 адреса

Unicast-адрес служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на unicast-адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным.

Существует шесть типов Unicast адресов:

1. *Global unicast-адрес.*

Global unicast-адрес мало чем отличается от публичного IPv4-адреса. Это адреса, к которым можно проложить маршрут через сеть Интернет, т.е. они являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически.

2. *Link-local адреса.*

Local IPv6-адрес канала (Link-Local Адрес) позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Пакеты с локальным адресом канала источника или назначения не могут быть направлены за пределы того канала, в котором пакет создаётся. В отличие от локальных IPv4-адресов канала, локальные адреса канала IPv6 играют важную роль в различных аспектах сети. Глобальный индивидуальный адрес не обязателен. Однако для содержания локального адреса канала необходим сетевой интерфейс под управлением протокола IPv6. Если локальный адрес канала не настроен вручную на интерфейсе, устройство автоматически создаёт собственный адрес, не обращаясь к DHCP-серверу. Узлы под управлением IPv6 протокола создают локальный IPv6-адрес канала даже в том случае, если устройству не был назначен глобальный IPv6-адрес. Это позволяет устройствам под управлением IPv6 обмениваться данными с другими устройствами под управлением IPv6 в

одной подсети, в том числе со шлюзом по умолчанию (маршрутизатором). Локальные IPv6-адреса канала находятся в диапазоне FE80::/10.

3. *Loopback-адрес.*

Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, и выглядит как ::1/128 или просто ::1 в сокращенном формате.

4. *Unspecified-адрес.*

Неопределённый адрес состоит из нулей и в сокращенном формате представлен как ::/128 или просто :: Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

5. *Unique local адрес.*

Unique local — это IPv6-адреса. которые имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не следует маршрутизировать в глобальном протоколе IPv6. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFF::/7.В случае с IPv4 частные адреса объединены с преобразованием сетевых портов и адресов (NAT) для обеспечения преобразования адресов из частных в публичные. Это делается из-за недостатка адресного пространства IPv4. На многих сайтах также используют частный характер адресов RFC 1918, чтобы обеспечить безопасность или защитить сеть от потенциальных угроз. Однако такая мера никогда не была целью использования данных технологий, и организация IETF всегда рекомендовала предпринимать правильные меры предосторожности при работе маршрутизатора в Интернете. Хотя протокол IPv6 обеспечивает особую адресацию для сайтов, он не предназначен для того, чтобы скрывать внутренние устройства под управлением IPv6 от анализа из сети Интернет IPv6. IETF рекомендует ограничивать доступ к устройствам с помощью специальных (более эффективныз) мер безопасности.

6. *IPv4 embedded адрес.*

Это тип индивидуальных адресов, являющийся адресом со встроенным IPv4-адресом. Использование этих адресов способствует переходу с протокола IPv4 на IPv6.

7. *Global unicast адрес.*

Global unicast IPv6-адреса уникальны по всему миру и доступны для маршрутизации через Интернет IPv6. Эти адреса эквивалентны публичным IPv4-адресам. В настоящее время назначаются только глобальные индивидуальные адреса с первыми тремя битами 001 или 2000::/3. Это лишь 1/8 от всего доступного адресного пространства IPv6. Так, например, адрес 2001:0DB8::/32 был зарезервирован для документации.

В общем случае глобальный индивидуальный адрес состоит из трёх частей (рис. 4).

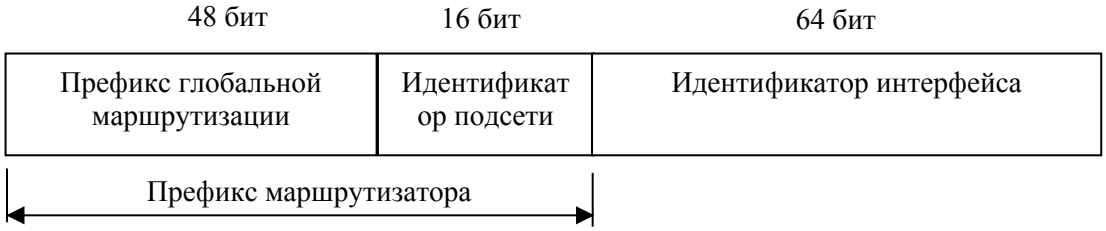

Рис. 4. Структура Global unicast IPv6-адреса

Префикс глобальной маршрутизации – это префиксальная или сетевая часть адреса, назначаемая интернет-провайдером заказчику или узлу. В настоящее время /48 является префиксом глобальной маршрутизации, который интернет-регистраторы назначают своим заказчикам – корпоративным сетям и индивидуальным пользователям. Этого адресного пространства более чем достаточно для большинства заказчиков.

Идентификатор подсети – используется организациями для обозначения подсетей в каждом узле.

Идентификатор интерфейса – эквивалентен узловой части адреса IPv4-адреса. Термин «идентификатор интерфейса» используется в том случае, когда один узел может иметь несколько интерфейсов, каждый из которых обладает одним или более IPv6-адресами.

Multicat IPv6-адреса

Мультикастинг-адрес IPv6 является идентификатором для группы узлов. Узел может принадлежать к любому числу мультикастинг групп. Мультикастинг-адреса имеют следующий формат (рис. 5):

Рис. 5 Структура multicast-адреса

Префикс 11111111 в начале адреса идентифицирует адрес, как multicast-адрес. Структура флагов представлена на рис. 6.

Рис. 6. Структура флагов multicast-адреса

Старшие 3 флага зарезервированы и должны быть обнулены. T = 0 указывает на то, что является стандартным ("*well-known*") multicast-адресом,

официально выделенным для глобального использования в Интернет. T = 1 указывает, что данный multicast-адрес присвоен временно ("*transient*").

Поле *scope* представляет собой 4-битовый код, предназначенный для определения предельной области действия multicastr-группы. Допустимые значения поля scope представлены в табл. 3.

Таблица 3

Допустимые значения поля scope

Значение	Область действия
0	Зарезервировано
1	Область действия ограничена локальным узлом
2	Область действия ограничена локальным каналом
3	(не определено)
4	(не определено)
5	Область действия ограничена локальной сетью
6	(не определено)
7	(не определено)
8	Область действия ограничена локальной организацией
9	(не определено)
A	(не определено)
B	(не определено)
C	(не определено)
D	(не определено)
E	Глобальные пределы (global scope)
F	Зарезервировано

Значение постоянно присвоенного multicast-адреса не зависит от значения поля scope. Например, если "NTP servers group" присвоен постоянный мультикастинг адрес с идентификатором группы 43 (hex), тогда:

FF01:0:0:0:0:0:0:43 означает, что все NTP серверы одного и того же узла рассматриваются как отправители.

FF02:0:0:0:0:0:0:43 означает, что все NTP серверы работают с тем же каналом, что и отправитель.

FF05:0:0:0:0:0:0:43 означает, что все NTP серверы принадлежат той же сети, что и отправитель.

FF0E:0:0:0:0:0:0:43 означает, что все NTP серверы находятся в Интернет.

Непостоянно выделенные multicast-адреса имеют значение только в пределах данного ограничения (scope). Например, группа, определенная непостоянным локальным мультикаст-адресом FF15:0:0:0:0:0:0:43, не имеет никакого смысла для другой локальной сети или непостоянной группы, использующей тот же групповой идентификатор с другим scope, или для постоянной группы с тем же групповым ID.

Multicast адреса не должны использоваться в качестве адреса отправителя в IPv6 пакетах или встречаться в любых заголовках маршрутизации.

Заголовки расширения IPv6

В IPv6, опционная информация уровня Интернет записывается в отдельных заголовках, которые могут быть помещены между IPv6 заголовком и заголовком верхнего уровня пакета. Существует небольшое число таких заголовков, каждый задается определенным значением кода поля *следующий заголовок*. В настоящее время определены заголовки: маршрутизации, фрагментации, аутентификации, инкапсуляции, опций hop-by-hop, места назначения и отсутствия следующего заголовка. Как показано в примерах ниже, IPv6 пакет может нести нуль, один, или более заголовков расширения, каждый задается предыдущим полем *следующий заголовок* (рис. 5):

Рис. 5. Структура вложения пакетов для IPv6