Протокол IPv6 (Internet Protocol version 6).

1. Проблема нехватки адресного пространства.

Важной проблемой развития компьютерных сетей, функционирующих на базе сетевого протокола IP версии 4 является **острая нехватка адресного пространства**. В условиях бурного развития информационных технологий потребность в сетевых адресах должна удовлетворяться как минимум в количестве 1 адрес на одного жителя планеты. В 2015 году численность населения составляла порядка 7 432 663 000 человек (https://populationpyramid.net/ru/мир-земля/2016/). Как известно, для нумерации узлов в сети адресуемой по IP версии 4 используется 32-х разрядное число, в результате чего в сети может находиться не более, чем 2^{32} = 4 294 967 296 уникальных узлов (не учитывая служебные адреса, диапазоны частных сетей, технологии трансляции адресов (NAT) и т.п.)., что делает очевидным нехватку сетевых адресов для населения земли.

Выделением адресного пространства занимаются Агентство выделения интернет адресов (IANA, США) и несколько региональных агентств (RIR): Африканское (AfrNIC), Азия/Атлантика (APNIC), Канада, США и некоторый Карибские острова (ARIN), Латинская Америка и некоторые Карибские острова (LACNIC), Европа, Ближний восток и Центральная Азия (RIPE NCC). Существуют локальные регистратора адресов (LIR), которые отвечают за регистрацию адресов в своих областях. В 2015 году все агентства, кроме AfrNIC, уже заявили о том, что ими закончено выделение общих блоков адресов (см. рис. 1). Первым о таком событии сообщило агентство APNIC 15 апреля 2011 года.

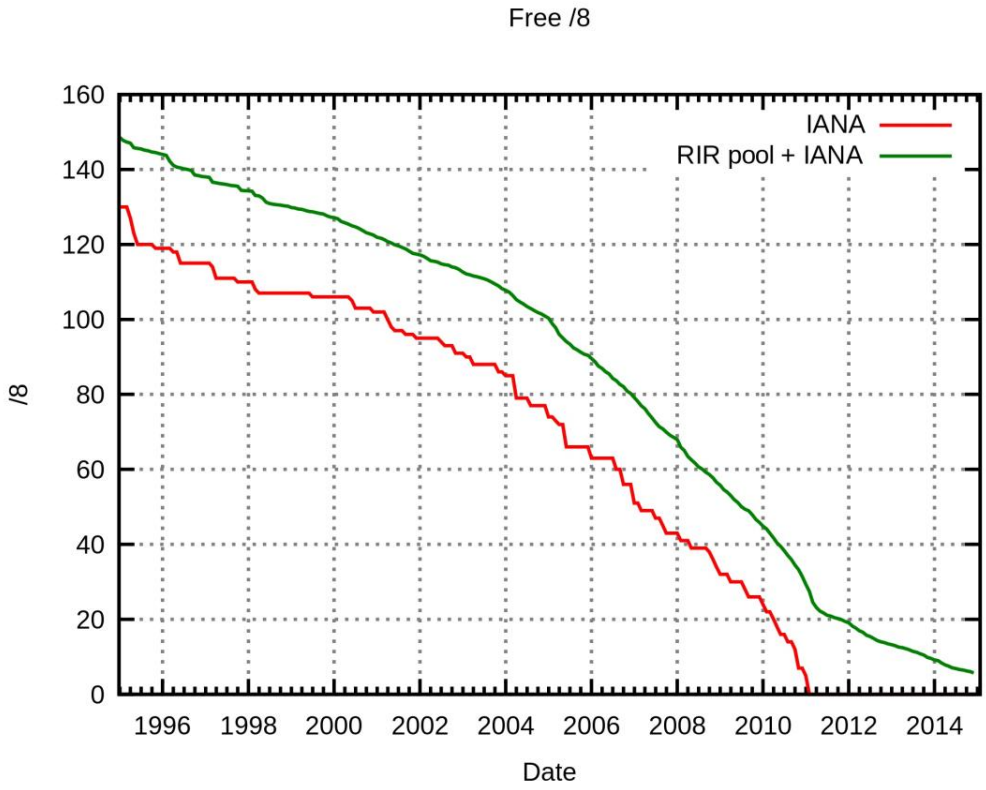


Рис.1. Свободные блоки адресов IPv4 (https://commons.wikimedia.org/wiki/File:Ipv4-exhaust.svg?uselang=ru).

Распределением адресного пространства IPv6 занимаются те же агентства, что и распределяли адреса IPv4: IANA, AfrNIC, APNIC, ARIN, LACNIC, RIPE NCC. Несмотря на острую нехватку адресов, внедрение IPv6 идёт относительно медленными темпами. Например, в январе 2016 года, популярным поисковым сервисом Google зарегистрировано менее 10% запросов, поступивших с использованием IPv6 (см. рис. 2).

Первая спецификация протокола IP версии 6 была опубликована в декабре 1995 года в RFC 1883 (https://tools.ietf.org/html/rfc1883). Версия 6 протоколу была присвоена потому, что ранее был зарегистрирован экспериментальный протокол версии 5, предназначавшийся для «обогащения» протокола версии 4 средствами потоковой передачи видео и аудио. Этот протокол был описан в RFC 1190 и RFC 1819.

В протоколе IPv6 для нумерации адресов используется 128-ми разрядное число, что позволяет адресовать приблизительно 340 ундециллионов сетевых узлов

340 282 366 920 938 463 463 374 607 431 768 211 456.

В результате допускается адресация порядка 1000 сетевых узлов на каждый грамм земли, что явно закладывает определённый резерв развития сети Интернет на ближайшие десятилетия.

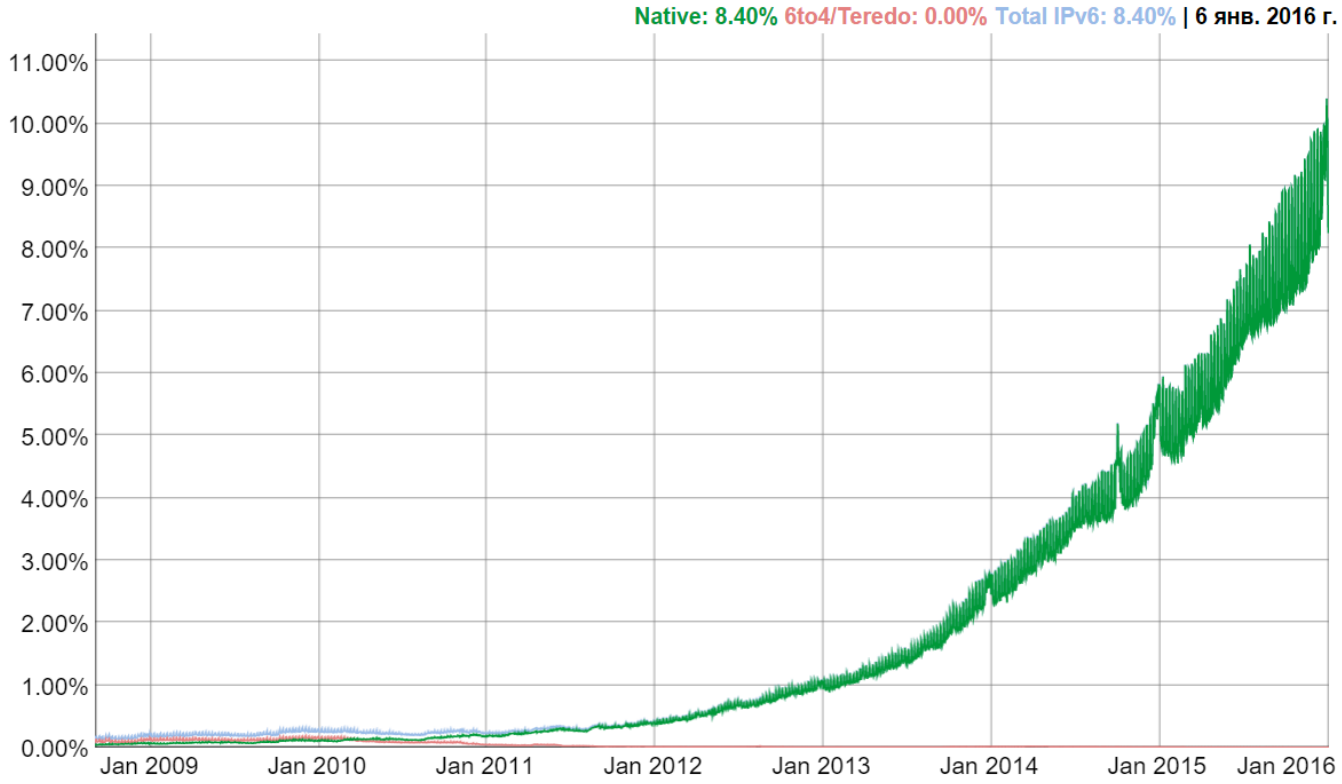


Рис. 2. Статистика запросов к поисковому сервису Google с использованием протокола IPv6 (январь 2016 года) https://www.google.com/intl/en/ipv6/statistics.html.

2. Разработка IPv6.

В начале 1990 года начала работать группа проектирования Интернета IETF над новой версией сетевого протокола - IPv6.

Протокол IPv6 (Internet Protocol version 6) — это новая версия интернет протокола (IP), созданная с целью решения проблем, с которыми столкнулась предыдущая версия (IPv4) при её использовании в интернете, одна из которых – это использование длины адреса 128 бит вместо 32.

2.1. Основные задачи решаемые группой по IPv6.

- Возможность доступа к глобальной сети миллиардов хостов даже при нерациональном использовании адресного пространства.
- Сокращение размера таблиц маршрутизации
- Упрощение протокола для ускорения обработки пакетов маршрутизации
- Повышение уровня безопасности протокола
- Упрощение работы многоадресных рассылок с помощью указания областей рассылки.
- Перспективы дальнейшего развития протокола в будущем
- Организация совместимости старого и нового протокола

Протокол IPv6 был разработан в конце 1992 года, см. RFC 2460 (Dec.1998).

Сейчас IPv6 активно используется во множестве сетей по всему миру, но ещё не получил столь широкого распространения в Интернете, как IPv4. IPv6 хорошо справляется с основными поставленными задачами. IPv6 лишен некоторых недостатков и обладает некоторыми новыми возможностями.

В общем случае протокол IPv6 несовместим с протоколом IPv4, но зато совместим со всеми остальными протоколами Интернета, включая TCP, UDP, ICMP, OSPF, DNS для чего иногда требуются небольшие изменения.

2.2. Особенности IPv6.

- Протокол IPv6 имеет длину 16 байт, что решает основную проблему - обеспечить практически неограниченный запас интернет – адресов.
- Протокол IPv6 по сравнению с IPv4 имеет более простой заголовок пакета. Таким образом, маршрутизаторы могут быстрее обрабатывать пакеты, что повышает производительность.
- Улучшенная поддержка необязательных параметров. Подобное изменение действительно было существенным, так как в новом заголовке требуемые прежде поля стали необязательными.
- Повышен уровень безопасности, аутентификация и конфиденциальность являются ключевыми чертами нового IP-протокола
- Уделено больше внимание типу представляемых услуг. Для этой цели в заголовке пакета IPv4 было отведено 8-разрядное поле.

3. Заголовок IPv6.

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00	Version=4				IHL				Type Of Service								Total Length															
04	Identification																Flags			Fragment Offset											
08	Time To Live								Protocol								Header Checksum															
12	Source IP Address																															
16	Destination IP Address																															
20	Options (variable dimension) min=0, max=10x32 bit																														PAD	
	Data (variable dimension)																															

Octet	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00	Версия=6				Приоритет				Метка потока																							
04	Длина полезной нагрузки																Следующий заголовок								Max число транзит.узлов							
08-23	Source IP Address																															
24-35	Destination IP Address																															
40	Дополнительный заголовок (variable dimension) min=0																															
	Data (variable dimension)																															

Рис. 3. Структуры пакетов IPv4 и IPv6 для сравнения представлены рядом.

3.1. Основной заголовок.

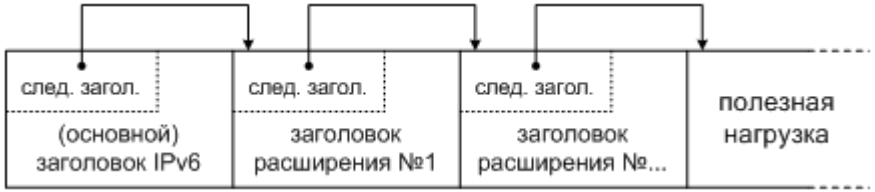
Изменение формата заголовка в IPv6 позволило уменьшить объем служебной информации, передаваемой с каждым пакетом. Для этого в новом протоколе IP были введены понятия основного и дополнительных заголовков.

Основной заголовок присутствует всегда и имеет фиксированную длину в 40 байт, его формат (см. рис. выше):

- **Версия** — для IPv6 значение поля должно быть равно 6.
- **Приоритет** – используется для того, чтобы различать пакеты с разными требованиями к доставке в реальном времени.
- **Метка потока** – применяется для установки между отправителем и получателем псевдо-соединения с определенными свойствами и требованиями. Например поток пакетов между двумя процессами на разных хостах может обладать строгими требованиями к задержкам, что потребует резервирование пропускной способности.
- **Длина полезной нагрузки** – сколько байт информации следует за заголовком.
- **Следующий заголовок** – содержит данные, определяющие тип заголовка, который следует за данным. Каждый следующий дополнительный заголовок также содержит поле следующего заголовка. Если IP-пакет не содержит дополнительных заголовков, то в этом поле будет значение, соответствующее полю Protocol в IPv4 – номер закрепленный за протоколом TCP, UDP, RIP, OSPF или другим, определенным в стандарте IPv4.
- **Max число транзитных узлов** – аналог времени жизни (TTL).

3.2. Дополнительные заголовки.

IPv6 пакет имеет следующий формат:



В IPv6 пока определены следующие типы дополнительных заголовков:

- Hop-by-hop – разнообразная информация для маршрутизаторов необходимая для последовательной обработки пакетов на каждом маршрутизаторе;
- Параметры получения – дополнительная информация для узла назначения;
- Маршрутизация – частичный или полный список транзитных маршрутизаторов на пути пакета при маршрутизации от источника;
- Фрагментация – управление фрагментами дейтаграмм (обрабатывается только в конечных узлах);
- Аутентификация – информация, необходимая для аутентификации конечных узлов и обеспечения целостности содержимого IP-пакетов;
- Шифрованные данные – информация, необходимая для обеспечения конфиденциальности передаваемых данных путем шифрования и дешифрирования.

Заголовки расширения не рассматриваются и не обрабатываются узлами по пути доставки. Содержимое и семантика каждого заголовка расширения определяет следующий заголовок. Следовательно, заголовки расширения должны обрабатываться строго в порядке их выкладки в пакете. Получатель, например, не должен просматривать пакет, искать определённый тип заголовка расширения и обрабатывать его до обработки предыдущих заголовков.

Единственное исключение из этого правила касается заголовка опций hop-by-hop, несущего в себе информацию, которая должна быть рассмотрена и обработана каждым узлом по пути доставки, включая отправителя и получателя. Заголовок опций hop-by-hop, если он присутствует, должен следовать непосредственно сразу после IPv6-заголовка. Его присутствие отмечается записью нуля в поле следующий заголовок заголовка IPv6.

Если в результате обработки заголовка узлу необходимо перейти к следующему заголовку, а код поля следующий заголовок не распознается, необходимо игнорировать данный пакет и послать соответствующее сообщение ICMP (parameter problem message) отправителю пакета. Это сообщение должно содержать код ICMP=2 ("unrecognized next header type encountered " - встретился нераспознаваемый тип следующего заголовка) и поле - указатель на не узнанное поле в пакете. Аналогичные действия следует предпринять, если узел встретил код следующего заголовка равный нулю в заголовке, отличном от IPv6- заголовка.

Каждый заголовок расширения имеет длину кратную 8 октетам.

4. Снижение нагрузки на маршрутизаторы в IPv6.

Главной целью изменения системы адресации в IPv6 было не механическое увеличение адресного пространства, а повышения эффективности работы стека TCP/IP в целом.

В IPv6 не поддерживаются классы адресов (A, B, C, D, E), но широко используется технология CIDR. Благодаря этому, а также усовершенствованной системе групповой адресации и введению адресов нового типа, IPv6 позволяет снизить затраты на маршрутизацию.

Для того чтобы повысить производительность маршрутизаторов Интернета в части выполнения их основной функции — продвижения пакетов, в IPv6 предпринят ряд мер по освобождению маршрутизаторов от некоторых вспомогательных задач.

- Перенесение функций фрагментации с маршрутизаторов на конечные узлы. Конечные узлы в версии IPv6 обязаны найти минимальное значение MTU вдоль всего пути, соединяющего исходный узел с узлом назначения (эта техника под названием Path MTU Discovery уже используется в IPv4). Маршрутизаторы IPv6 не выполняют фрагментацию, а только посылают ICMP-сообщение о слишком длинном пакете конечному узлу, который должен уменьшить размер пакета.
- Агрегирование адресов IPv6 ведет к уменьшению размера адресных таблиц маршрутизаторов, а значит сокращает время просмотра и обновления таблиц. При этом также сокращается служебный трафик, порождаемый протоколами маршрутизации.

- Широкое использование маршрутизации от источника. При маршрутизации от источника узел-источник задает полный маршрут прохождения пакета через сети. Такая техника освобождает маршрутизаторы от необходимости просмотра адресных таблиц при выборе следующего маршрутизатора.
- Отказ от обработки не обязательных параметров заголовка.
- Использование в адресе в качестве номера узла его MAC-адреса избавляет маршрутизаторы от необходимости применять протокол ARP.

5. Формы представления адреса IPv6.

5.1. Нормальная форма.

Эта форма является предпочтительной и имеет вид n:n:n:n:n:n:n:n. Каждый знак n соответствует 4-х значному шестнадцатеричному числу (всего 8 шестнадцатеричных чисел, для каждого числа отводится 16 бит). Регистр используемых букв A-F значения не имеет.

Например: 1FA9:FFFF:2621:ACDA:2245:BF98:3412:4167, FEDC:0A98:0:0:0:0:7654:3210.

5.2. Сжатые формы.

По причине большой длины адреса и из-за специфики «расточительного» распределения адресов, адрес IPv6 обычно содержит много нулей подряд.

Для упрощения записи адреса IPv6 используется сокращение записи нулей, см. рис. 5.:

- в каждой группе допускается не писать лидирующие (старшие) нули;
- если в адресе имеется одна или несколько последовательно идущих групп, в которых записаны только нули, то один раз допускается пропустить все эти группы, заменив их на два последовательно идущих символа двоеточие;
- допускается запись вида «::», определяющая адрес, в котором содержатся только нули (такой адрес называется **неопределённым**).

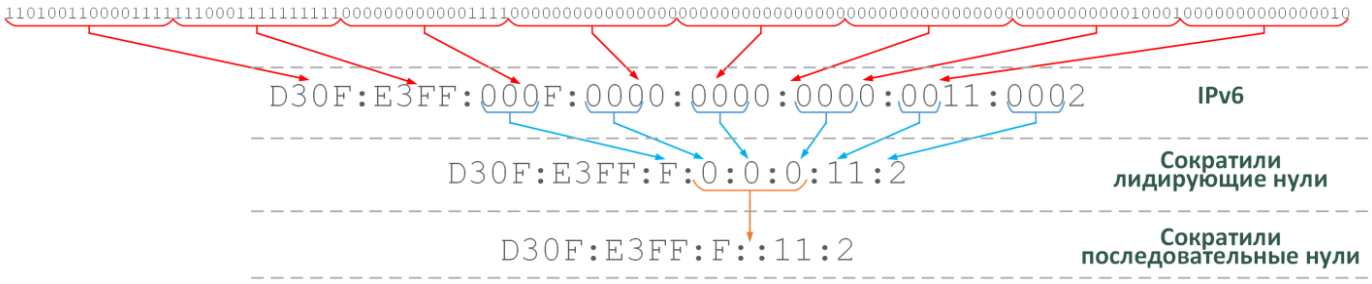


Рис. 5. Формы записи IPv6 адресов.

Например:

- адрес групповой рассылки FFED:0000:0000:0000:0000:BA98:3210:4562 имеет сокращённую форму FFED:0:0:0:0:BA98:3210:4562 и более сжатую форму FFED::BA98:3210:4562;
- адрес одноадресной рассылки 3FFE:FFFF:0:0:8:800:20C4:0 в сжатой форме имеет вид: 3FFE:FFFF::8:800:20C4:0;
- шлейфовый адрес 0:0:0:0:0:0:0:1 в сжатой форме выглядит так ::1;
- неопределенный адрес 0:0:0:0:0:0:0:0 превращается в :: .

Дополнительно к адресу узла может указываться маска сети или номер интерфейса, к которому этот адрес относится.

5.2.1. Маска сети.

Маска сети задается в форме префикса (после символа /), указывающего сколько разрядов начиная со старшего указывают номер сети, к которой относится этот адрес. Оставшаяся часть адреса определяет номер сетевого узла (интерфейса).

FE80::1/64

5.2.2. Идентификатор интерфейса.

Идентификатор интерфейса (в форме имени или номера) указывается после адреса с разделением символом %. Такая форма записи используется в случаях, когда один и тот же адрес задан нескольким интерфейсам сетевого узла.

FE80::1%1

5.2.3. Запись в URI.

Для записи IPv6 в URI адрес указывается в квадратных скобках, например:

http://[2001:DB8::3]:8080/index.html.

5.3. Смешанные (переходные) формы.

Для обеспечения плавного перехода с версии 4 на версию 6 предусмотрены специальные форматы IPv6 адресов. Эта форма представляет собой сочетание адресов протоколов IPv4 и IPv6. Адрес имеет формат n:n:n:n:n:n:d.d.d.d, где каждый символ n соответствует 4-х значному шестнадцатеричному числу (6 шестнадцатеричных чисел, для каждого числа отводится 16 бит), а d.d.d.d - часть адреса, записанная в формате IPv4 (32 бита).

Например:

- 0:0:0:0:0:0:19.8.62.32
- 0:0:0:0:0:FFFF:111.214.2.34
- ::73.3.68.45
- ::F2F3:129.131.32.31
- ::192.168.1.1/96 – старшие 96 разрядов нулевые, а оставшиеся 32 бита записываются в виде IPv4. Такая форма записи используется для узлов, которые реализуют двойной стек протоколов (и IPv4 и IPv6), но данные передаются по сети на базе IPv4;
- ::FFFF:123.123.123.123/96 – старшие 80 разрядов нулевые, затем группа из 16 единиц и оставшиеся 32 бита записываются в форме IPv4. Такая запись указывает на то, что узел использует только IPv4 и не поддерживает IPv6.

6. Переход на версию IPv6.

Переход на всеобщее применение новой версии протокола связан с огромными финансовыми затратами на модернизацию сетевой инфраструктуры. Очевидно, что в таких условиях требуется обеспечить переходный процесс, в котором в сети будет одновременно функционировать две версии протокола IP.

При разработке IPv6 была предусмотрена возможность плавного перехода к новой версии, когда довольно значительное время будут сосуществовать островки Интернета, работающие по протоколу IPv6, и остальная часть Интернета, работающая по протоколу IPv4. Существует несколько подходов к организации взаимодействия узлов, использующих разные стеки TCP/IP.

6.1. Трансляция протоколов.

Трансляция протоколов реализуется шлюзами, которые устанавливаются на границах сетей, использующих разные версии протокола IP. Согласование двух версий протокола IP происходит путем преобразования пакетов IPv4 в IPv6, и наоборот.

Для упрощения преобразования адресов между версиями используется специальный подтип IPv4-совместимых IPv6-адресов, который в младших 4-х байтах переносит IPv4-адрес, а в старших 12 байтах содержит нули (см. рис. 6).

Это позволяет получать IPv4-адрес из IPv6-адреса простым отбрасыванием старших байтов.

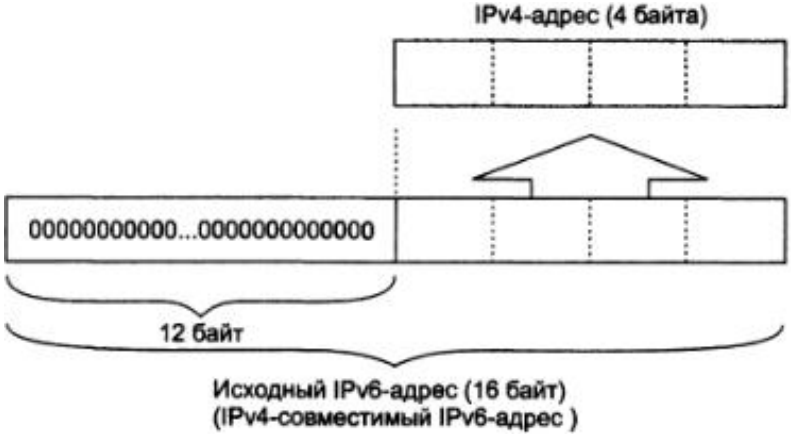


Рис. 6. Преобразование IPv6 в IPv4.

Для решения обратной задачи — передачи пакетов IPv4 через части Интернета, работающие по протоколу IPv6, — предназначен IPv4-отображенный IPv6-адрес. Этот тип адреса также содержит в 4-х младших байтах IPv4-адрес, в старших 10-ти байтах — нули, а в 5-м и 6-м байтах IPv6-адреса — единицы, которые показывают, что узел поддерживает только версию 4 протокола IP (см. рис. 7).

Рис. 7. Преобразование IPv4 в IPv6.

6.2. Мультиплексирование стеков протоколов.

Мультиплексирование стеков протоколов означает установку на взаимодействующих хостах сети обеих версий протокола IP. Обе версии стека протоколов должны быть развернуты также на разделяющих эти хосты маршрутизаторах. В том случае, когда IPv6-хост отправляет сообщение IPv6-хосту, он использует стек IPv6, а если тот же хост взаимодействует с IPv4-хостом — стек IPv4. Маршрутизатор с установленными на нем двумя стеками называется маршрутизатором IPv4/IPv6, он способен обрабатывать трафики разных версий независимо друг от друга.

6.3. Инкапсуляция, или туннелирование.

Инкапсуляция может применяться, когда две сети одной версии IP, необходимо соединить через транзитную сеть, работающую на другой версии IP (см. рис. 8). Пакеты IPv4 помещаются в пограничных устройствах (маршрутизаторах) в пакеты IPv6 и переносятся через «туннель», проложенный в IPv6-сети. Такой способ имеет недостаток заключающийся в том, что узлы IPv4-сетей не имеют возможности взаимодействовав с узлами транзитной IPv6-сети.

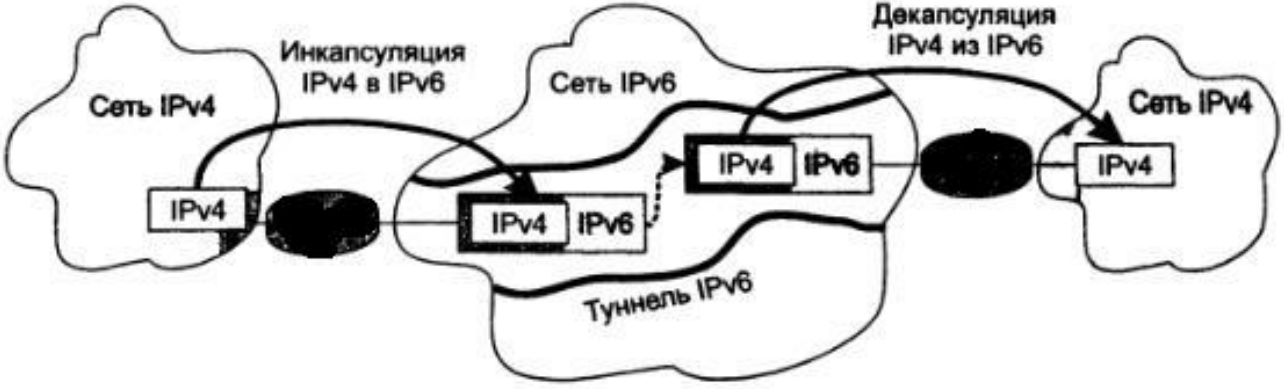


Рис. 8. Согласование технологий IPv4 и IPv6 путем туннелирования (инкапсуляции).

Аналогичным образом может происходить и туннелирование IPv6 через сеть IPv4.

7. Модель адресации IPv6.

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

Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные). Существует два исключения из этого правила:

- Одиночный адрес может приписываться нескольким физическим интерфейсам, если приложение рассматривает эти несколько интерфейсов как единое целое при представлении его на уровне Интернет.
- Маршрутизаторы могут иметь безадресные интерфейсы (не присваивается никакого IPv6 адреса) для соединений точка-точка, чтобы исключить ручной конфигурирации и объявления этих адресов (если эти интерфейсы не используются в качестве точки отправления или назначения при посылке IPv6 дейтаграмм). Маршрутизация здесь осуществляется по схеме близкой к используемой протоколом CIDR в IPv4.

Субсети IPv4 ассоциируется с каналом IPv6. Одному каналу могут соответствовать несколько субсетей.

В IPv6, все нули и все единицы являются допустимыми кодами для любых полей, если не оговорено исключение.

7.1. Типы (форматы) адресов IPv6.

В IPv6 предусмотрено три основных категории адресов:

- **Unicast** - Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.
- **Anycast** - Идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по эникастному 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 мультикастинг-адресу, доставляется всем этим интерфейсам.

В IPv6 не существует широковещательных (Broadcast) адресов, их функции переданы мультикастинг-адресам. В IPv6 не используются маски подсетей.

7.1.1. FP - Format Prefix и разделение адресного пространства в IPv6.

Адреса в IPv6 делятся на несколько типов. Конкретный тип адреса IPv6 определяется значением нескольких старших (левых) битов, которые называются префиксом типа (Type Prefix), или префиксом формата (FP – Format Prefix), или адресным префиксом.

Format Prefix имеет переменную длину и он однозначно определяет формат следующих за ним частей адреса. Таблица ниже показывает префиксы всех типов адресов IPv6. В третьей колонке показана доля каждого из типов адресов от всего адресного пространства.

Type Prefix (bin)	Type Prefix (hex)	Type	Fraction	IPv4 Analog
0000 0000	0000::/8	Reserved	1/256	
0000 0001	0100::/8	Unassigned	1/256	
0000 001	0200::/7	ISO network address	1/128	
0000 010	0400::/7	IPX (Novell) network Address	1/128	
0000 011	0600::/7	Unassigned	1/128	
0000 1	0800::/5	Unassigned	1/32	
0001	1000::/4	Reserved	1/16	
001	2000::/3	Global unicast address	1/8	Классы A,B,C
010	4000::/3	Provider-based unicast address	1/8	
011	6000::/3	Unassigned	1/8	
100	8000::/3	Geographic-based unicast address	1/8	
101	A000::/3	Unassigned	1/8	
110	C000::/3	Unassigned	1/8	
1110	E000::/4	Unassigned	1/16	
1111 0	F000::/5	Unassigned	1/32	
1111 10	F800::/6	Unassigned	1/64	
1111 110	FC00::/7	**Unique local address**	1/128	10.0.0.0/8 и др.
1111 1110 0	FE00::/9	Unassigned	1/512	
1111 1110 10	FE80::/10	**Link local address**	1/1024	169.254.0.0/16
1111 1110 11	FEC0::/10	Reserved (Site local address)	1/1024	
1111 1111	FF00::/8	Multicast address	1/256	Класс D

7.2. Unicast адреса.

В одноадресной передаче пакеты предназначаются только одному сетевому узлу. В IPv6 индивидуальные адреса делятся на несколько подтипов:

- **global unicast** (глобальные сетевые адреса). Это так называемые «белые адреса», которые глобально маршрутизируются по всей сети Интернет. К этой группе относят адреса из диапазона 2000::/3;
- **unique local** (локальные сетевые адреса). Являются аналогами «серых адресов» в протоколе IPv4 (10.0.0.0/8 и др). Доступны для свободного использования в локальных сетях, т.к. не требуют регистрации и не являются глобально маршрутизируемыми. К этой группе относятся адреса из диапазона FC00::/7.
- **site local** устарело (используемый в рамках одной организации). Изначально стандартом предусматривался ещё один диапазон адресов FEC0::/10, но, в дальнейшем этот тип локальных адресов был помечен как «устаревший», а диапазон адресов перешел в статус «зарезервировано»;
- **link local** (адреса локального подключения). Используются для выполнения служебных функций (автоматическая конфигурация сетевых узлов, общение между маршрутизаторами и т.п.). В IPv4 аналог 169.254.0.0/16. Такие адреса не маршрутизируемые. Допускается назначение в рамках одного сетевого узла одинаковых адресов разным интерфейсам. К этой группе относятся адреса из диапазона FE80::/10.

7.2.1. Global unicast адресация.

Основным подтипом индивидуального адреса является глобальный агрегируемый уникальный адрес. Такие адреса могут агрегироваться для упрощения маршрутизации.

В отличие от уникальных адресов узлов версии IPv4, которые состоят из двух уровней иерархии адреса (номер сети и номер узла) в IPv6 имеется 4 уровня, из которых три уровня агрегации (TLA, NLA, SLA) используются для идентификации сетей, а один для идентификации узлов сети.

Глобальные агрегируемые уникальные адреса IPv6 имеют структуру, включающую шесть полей (см. рис. 9 для 200A:00C9:7405/48)

Octet	0		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Bits	3	13		8	24			16		64							
Field	FP	TLA		R	NLA			SLA		Interface ID							
Example	001	0000000000010		00000000	110010010111010000000101												

Рис. 9. Структура глобального агрегируемого уникального адреса в пакете IPv6.

- **Поле FP** - Format Prefix (префикс формата) для этого типа адресов имеет размер 3 бита и значение 001.
- **Поле TLA** - Top-Level Aggregation предназначено для идентификации сетей самых

крупных поставщиков услуг. Конкретное значение этого поля соответствует номеру поставщика услуг и представляет собой общую часть адресов, которыми располагает данный поставщик. Сравнительно небольшое количество разрядов, отведенных под это поле (13 бит), выбрано специально для ограничения размера таблиц маршрутизации в магистральных маршрутизаторах самого верхнего уровня Интернета. Это поле позволяет пронумеровать 8196 сетей поставщиков услуг верхнего уровня, а значит, число записей, описывающих маршруты между этими сетями, также будет ограничено значением 8196, что ускорит работу магистральных маршрутизаторов.

- **Поле R** – Reserve, следующие 8 битов равны 0 и зарезервированы на будущее для расширения при необходимости поля TLA.
- **Поле NLA** - Next-Level Aggregation предназначено для нумерации сетей средних и мелких поставщиков услуг. Значительный размер поля NLA (24 бита) позволяет путем агрегирования адресов отразить многоуровневую иерархию поставщиков услуг.
- **Поле SLA** - Site-Level Aggregation (16 бит) предназначено для адресации подсетей отдельного абонента, например подсетей одной корпоративной сети.
- **Поле Interface ID** - идентификатор интерфейса является аналогом номера узла в IPv4. Отличием версии IPv6 является то, что в общем случае идентификатор интерфейса просто совпадает с его локальным (аппаратным) адресом, а не представляет собой произвольно назначенный администратором номер узла. Идентификатор интерфейса имеет длину 64 бита, что позволяет поместить туда MAC-адрес (48 бит), или адрес конечного узла ATM (48 бит) или номер виртуального соединения ATM (до 28 бит), а также, вероятно, даст возможность использовать локальные адреса технологий, которые могут появиться в будущем (например, адрес EUI-64).

  Такой подход делает **ненужным протокол ARP**, поскольку процедура отображения IP-

адреса на локальный адрес становится тривиальной — она сводится к простому отбрасыванию старшей части адреса. Кроме того, в большинстве случаев отпадает необходимость ручного конфигурирования конечных узлов, так как младшую часть адреса — идентификатор интерфейса — узел узнает от аппаратуры (сетевого адаптера и т. п.), а старшую — номер подсети — ему сообщает маршрутизатор.

7.2.2. Пример Global Unicast адресации.

Пусть клиент получил от поставщика услуг пул адресов IPv6, определяемый префиксом 200A:00C9:7405/48 (рис. 10). Поскольку первые три бита этого числа равны 001, это — глобальный агрегируемый уникальный адрес.

TLA. Этот адрес принадлежит поставщику услуг верхнего уровня, у которого все сети имеют префикс 200A/16. Он может выделить поставщику услуг второго уровня некоторый диапазон адресов с общим префиксом, образованным его собственным префиксом, а также частью поля NLA. Длина поля NLA, отводимая под префикс, определяется маской, которую поставщик услуг верхнего уровня также должен сообщить своему клиенту — поставщику услуг второго уровня. Пусть в данном примере маска состоит из 32 единиц в старших разрядах, а результирующий префикс поставщика услуг второго уровня имеет вид 200A:00C9/32.

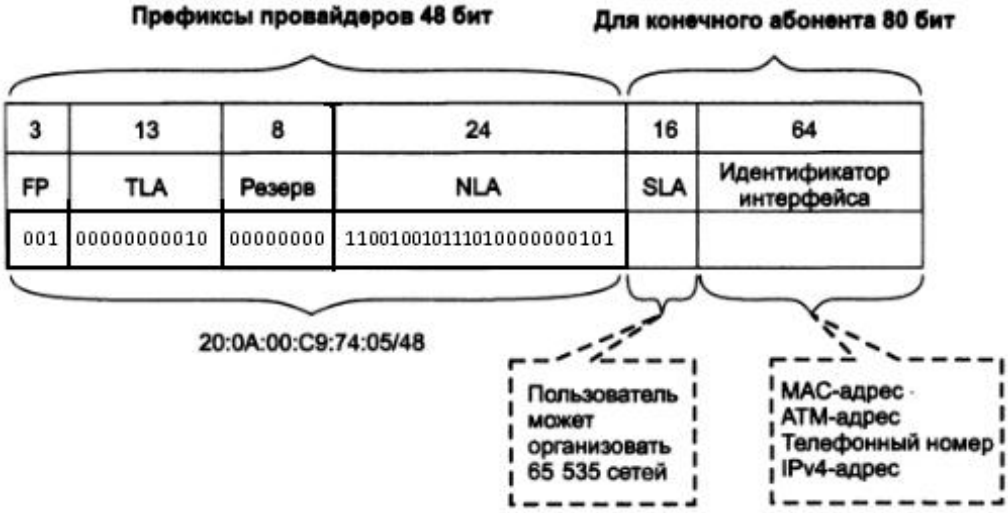


Рис. 10. Пример глобального агрегируемого адреса.

NLA. В распоряжении поставщика услуг второго уровня остается 16 разрядов поля NLA для нумерации сетей своих клиентов. В качестве клиентов могут выступать поставщики услуг третьего и более низких уровней, а также конечные абоненты — предприятия и организации. Пусть, например, следующий байт (01110100) в поле NLA поставщик услуг использовал для передачи поставщику услуг более низкого (третьего) уровня, а тот, в свою очередь, использовал последний байт поля NLA для назначения пула адресов клиенту. Таким образом, с участием поставщиков услуг трех уровней был сформирован префикс 200A:00C9:7405/48, который получил клиент.

SLA. Протокол IPv6 оставляет в полном распоряжении клиента 2 байта (поле SLA) для нумерации сетей и 8 байт (поле идентификатора интерфейса) для нумерации узлов. Имея такой огромный диапазон номеров подсетей, администратор получает широкие возможности. Для сравнительно небольшой сети он может выбрать плоскую организацию, назначая каждой имеющейся подсети произвольные неповторяющиеся значения из диапазона в 65 535 адресов, игнорируя оставшиеся. В крупных сетях более эффективным способом (сокращающим размеры таблиц корпоративных маршрутизаторов) может оказаться иерархическая структуризация сети на основе агрегирования адресов. В этом случае используется та же технология CIDR, но уже не поставщиком услуг, а администратором корпоративной сети.

Очевидно, что при таком изобилии сетей, которое предоставляется клиенту **в IPv6, совершенно теряет смысл операция использования масок для разделения сетей на подсети**, в то время как обратная процедура — объединение подсетей или агрегирование — приобретает важное значение.

Примечание.

Работа по детализации подтипов адресов протокола IPv6 еще далека от завершения. Сегодня определено назначение только 15 % адресного пространства IPv6, а оставшаяся часть адресов еще ждет своей очереди, чтобы найти применение для решения какой-либо из многочисленных проблем Интернета.

7.3. Multicast адреса.

Для адресации групповой передачи данных используются диапазон адресов FF00::/8.

Идентификатор в адресе определяет набор интерфейсов (обычно принадлежащих различным узлам). Пакет, посланный на такой адрес, доставляется всем интерфейсам, идентифицирующимся этим адресом. Типы групповых адресов замещают широковещательные адреса протокола IPv4. Мультикастинг-адрес IPv6 является идентификатором для группы узлов. Узел может принадлежать к любому числу мультикастинг групп. Мультикастинг-адреса имеют следующий формат (см. рис. 11 для FF0E::43):

Octet	0	1		2	3	4	5	6	7	8	9	10	11	12	13	14	15
Bits	8	4	4	112													
Field	FP	Flags	Scope	Groupe ID													
Example	1111 1111	0000	1110	0000000000000000000000000000000000000000000000000000000000000000 0100 0011													

Рис. 11. Формат мультикастинг-адреса IPv6.

- **Поле FP** - Format Prefix (префикс формата) в начале адреса идентифицирует адрес, как мультикатинг-адрес, имеет размер 8 бит и значение 11111111.
- **Поле Flags** - старшие 3 флага зарезервированы и должны быть обнулены.

Флаг T = 0 указывает, что адрес является стандартным ("well-known") мультикастным, официально выделенным для глобального использования в Интернет.
Флаг T = 1 указывает, что данный мультикастинг-адрес присвоен временно ("transient").

- **Поле Scope** (собирание) представляет собой 4-битовый код мультикастинга, предназначенный для определения предельной области действия мультикастинг-группы. Допустимые значения:
  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
- **Поле Groupe ID** - идентификатор группы идентифицирует мультикастинг-группы, постоянной или переходной (transient), в пределах заданных ограничений (scope).

Значение постоянно присвоенного мультикастинг-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 мультикаст-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.

Мультикастинг адреса не должны использоваться в качестве адреса отправителя в IPv6 дейтаграммах или встречаться в любых заголовках маршрутизации.

7.4. Anycast адреса.

Адреса типа anycast используются для обеспечения отказоустойчивости сетевых узлов. По сути anycast адрес – это специальным образом отмеченный unicast. Такие одинаковые адреса допускается назначать нескольким сетевым интерфейсам разных узлов в одной сети, чем обеспечивается их отказоустойчивость.

7.5. Служебные адреса.

Как и в версии 4 протоколом IPv6 предусмотрены служебные адреса:

- ::/128 – неопределённый адрес. Используется в протоколах автоматической конфигурации сетевых узлов;
- ::1/128 – единственный кольцевой адрес (loopback), в IPv4 используется избыточная сеть 127.0.0.0/8, хотя хватало одного адреса 127.0.0.1;
- 2001:DB8::/32 – диапазон адресов, используемый для примеров в учебно-методических материалах и для описаний в различной документации.
- FE80::/64 - адреса локального подключения, в IPv4 используется 169.254.0.0/16.

Адреса локального подключения задаются фактически произвольным образом. Единственное условие – такие адреса должны быть уникальны в рамках одного сетевого сегмента. Для автоматического формирования таких адресов часто применяется технология, основанная на использовании уже имеющихся и уникальных MAC адресов сетевых карт.

7.6. Адреса локального подключения.

Адреса локального подключения FE80::/64 используются при автоматической настройке узлов в простой одноранговой сети. Пакеты с адресами из этого блока не должны покидать пределов одного канала и подключенных к нему узлов.

Порядок формирования адреса локального подключения на основе MAC адреса сетевой карты представлен на рисунке 12. Адрес формируется отображением EUI-48 в EUI-64, заменой 7-го бита на 1 (начиная со старшего – для инверсной записи этот бит означает локальн=1/глобально=0 установленный MAC-адрес) и добавлением префикса FE80::/64.

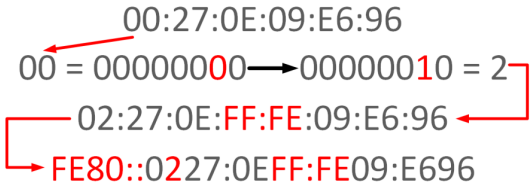


Рис. 12. Формирование адреса локального подключение на основе MAC.

Тип адреса	Исходный вид	Отображение в EUI 64
EUI 48	xx-yy-zz-ww-vv-tt	xx-yy-zz-FF-FE-ww-vv-tt
MAC 48	xx-yy-zz-ww-vv-tt	xx-yy-zz-FF-FF-ww-vv-tt

То есть между OUI и добавочным идентификатором возникают еще два байта с определенными значениями: FF-FE в случае EUI-48 и FF-FF в случае MAC 48. Например, из EUI-48 02-35-AB-00-64-C1 получится такой EUI 64: 02-35-AB-FF-FE-00-64-C1.

По этой причине IEEE не разрешает производителям оборудования расходовать добавочные идентификаторы EUI-64, которые начинаются с FF-FE и FF-FF.

В чём разница между EUI-48 и MAC-48? Оба типа находятся в ведении IEEE. По первоначальной задумке, MAC-48 служили канальными адресами IEEE 802, а EUI 48 — идентификаторами в прочих технологиях. Однако сегодня MAC-48 — это устаревший термин для подмножества EUI-48. Поэтому можно забыть о правиле преобразования MAC-48 в EUI-64 и пользоваться только правилом для EUI-48.

7.6.1. SLAAC - State-Less Address AutoConfiguration.

IPv6 имеет встроенный механизм SLAAC - автоматического распространения по сети информации о префиксах, которые в этой сети должны использоваться и об имеющихся маршрутизаторах сети. Сетевой узел используя имеющийся адрес локального подключения с помощью многоадресной рассылки запрашивает информацию о имеющихся в сети маршрутизаторах и номеров сетей, к которым они подключены. Получив информацию от маршрутизатора, узел автоматически конфигурирует свой глобальный сетевой адрес с использованием того же механизма EUI-64, что и при формировании адреса локального подключения, но с префиксом сети. После формирования адреса сетевой узел проверяет нет ли в сети узлов с таким адресом и если нет, то заканчивает конфигурацию.

7.7. Адреса узлов.

IPv6 адреса всех типов ассоциируются с интерфейсами, а не узлами. Так как каждый интерфейс принадлежит только одному узлу, то уникастный адрес интерфейса может идентифицировать узел. Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, аникастные и мультикстные).

Как правило, узел всегда имеет адрес локальной связи. Также у него могут быть адрес локального сайта и один или несколько глобальных адресов.

Конкретный тип адреса протокола IPv6 определяют его начальные биты. Поле, содержащее эти биты, называется префиксом формата (FP) или адресным префиксом и имеет переменную длину.

Адрес одноадресной рассылки в протоколе IPv6 разделяется на две части. Первая часть содержит адресный префикс, а вторая – идентификатор интерфейса.

Краткий способ представления адреса выглядит следующим образом:

ipv6-адрес/длина префикса.

Пример адреса с 64-битным префиксом. 3FFF:FFFF:0:CD30:0:0:0:0/64. Префиксом в этом примере является 3FFE:FFFF:0:CD30.

В IPv6 отсутствует такое понятия, как маска подсети. IPv6-адрес делится на три части:

- Глобальный префикс (Global Routing Prefix) – аналогичен идентификатору сети (Network ID) в IPv4 и присваивается провайдерам. Определяется он тремя первыми блоками адреса из восьми.
- Идентификатор подсети (Subnet ID) – представлен четвертым блоком и, по сути, очень похож на идентификатор подсети (Subnet ID) в IPv4.
- Идентификатор интерфейса (Interface ID) – аналог Host ID в IPv4, определяет уникальный адрес хоста вашей сети.

Существует несколько способов получения уникального 64-bit идентификатора интерфейса:

- он может быть настроен вручную,
- определен DCHP- сервером,
- получен путем преобразования MAC-адреса сетевой карты.

Вместо маски в IPv6 указывается префикс – это количество бит, которые определяют часть блоков, отвечающих за Global Routing Prefix. Пишется префикс через косую черту после самого адреса.

Возьмем для примера IPv6-адрес: 2001:0f68:0000:0000:0000:0000:1986:69af/48. Поскольку префикс (/48) указывает на первые 48 бит, можно считать, что 2001:0f68:0000 будет являться частью Global Routing Prefix. Следующее поле, 0000, указывает на идентификатор подсети. Оставшиеся блоки 0000:0000:1986:69af – это идентификатор интерфейса.

8. Упражнения.

1. Кратко опишите как устроен сетевой адрес протокола IPv6?
2. Каким образом происходит сокращение записи IPv6 адреса?
3. Напишите границы диапазона глобально регистрируемых адресов, локальные сетевые адреса и адресов локального подключения.
4. Какого типа связи нет в IPv6, который имеется в IPv4? Что предусмотрено взамен?
5. Что означает запись вида FE80:F:0::1%7?
6. Как происходит формирование адреса при SLAAC?
7. Чем отличается маршрутизация в IPv6?
8. Какие из нижеприведенных записей адреса IPv6 эквивалентны 2001:DB8:0:0:123::456?
    a) 2001:DB8::123:0:456
    b) 2001:DB8::123::456
    c) 2001:DB8::123:000:000:456
    d) 2001:0DB8:0:0:0123:0::0456
9. Какие из этих префиксов содержатся в адресе IPv6 2001:DB8:1234:5678::9ABC:DEF0?
    a) 2001:DB8:1234:5::/52
    b) 2001:DB8:1234:5678::9AB8:0/109
    c) 2001:0DB8:1234:5660::/59
    d) 2001:DB80::/27
10. Какие из этих адресов содержат в себе префикс IPv6 2001:DB8:ABC::/46?
    a) 2001:DB8:0ABE:F000::46
    b) 2001:0DB8:ABD0::46
    c) 2001:DB8::ABC:46

d) 2001:DB80:ABC0::46
e) 2001:0DB8:ABD::46

11. К какому типу относится адрес IPv6 FF02::DB8:314:2718?
    a) групповой
    b) индивидуальный внутриканальный
    c) иное
12. Какие проблемы возникают при переход с IPv4 на IPv6? Почему быстро перейти не получается?