Протоколы, сервисы и услуги
в Интернет и IP-сетях

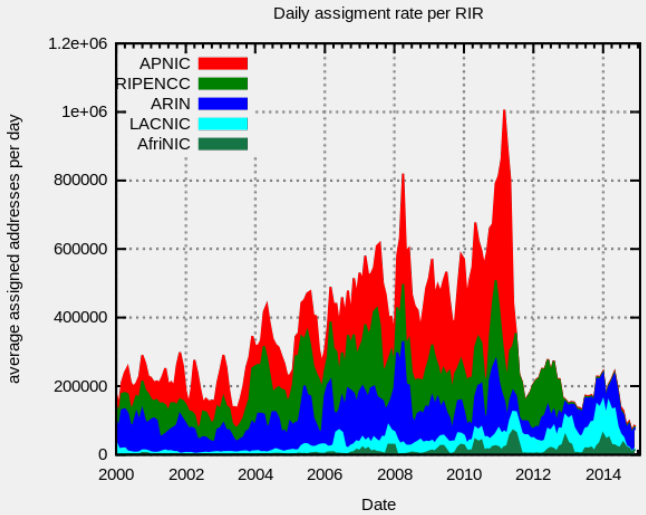
Тема № 7
Протокол IPv6

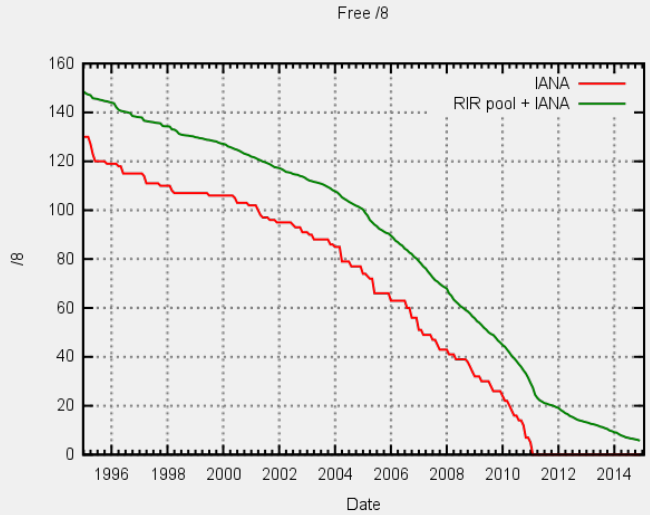
доц. каф. СС и ПД, к.т.н. С. С. Владимиров

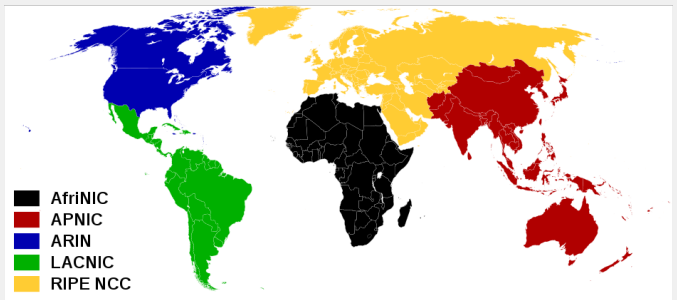
2017 г.

IPv6 (Internet Protocol version 6)

Новая версия протокола IP, использующая длину адреса 128 бит вместо 32. Основной причиной появления IPv6 стало понимание того, что адресное пространство IPv4 рано или поздно будет исчерпано. Первые варианты новых сетевых протоколов появились в 1992. Тогда же IETF объявила конкурс для рабочих групп на создание интернет-протокола следующего поколения (IP Next Generation — IPng). 25 июля 1994 года IETF утвердила модель IPng, с образованием нескольких рабочих групп IPng. Первым документом, определяющим спецификации IPv6, стал RFC 1883, опубликованный в декабре 1995 года. IETF назначила новому протоколу версию 6, так как версия 5 была ранее назначена экспериментальному протоколу, предназначенному для передачи видео и аудио. Позднее, в 1998, RFC 1883 был заменен на RFC 2460 и в дальнейшем дополнялся другими RFC.



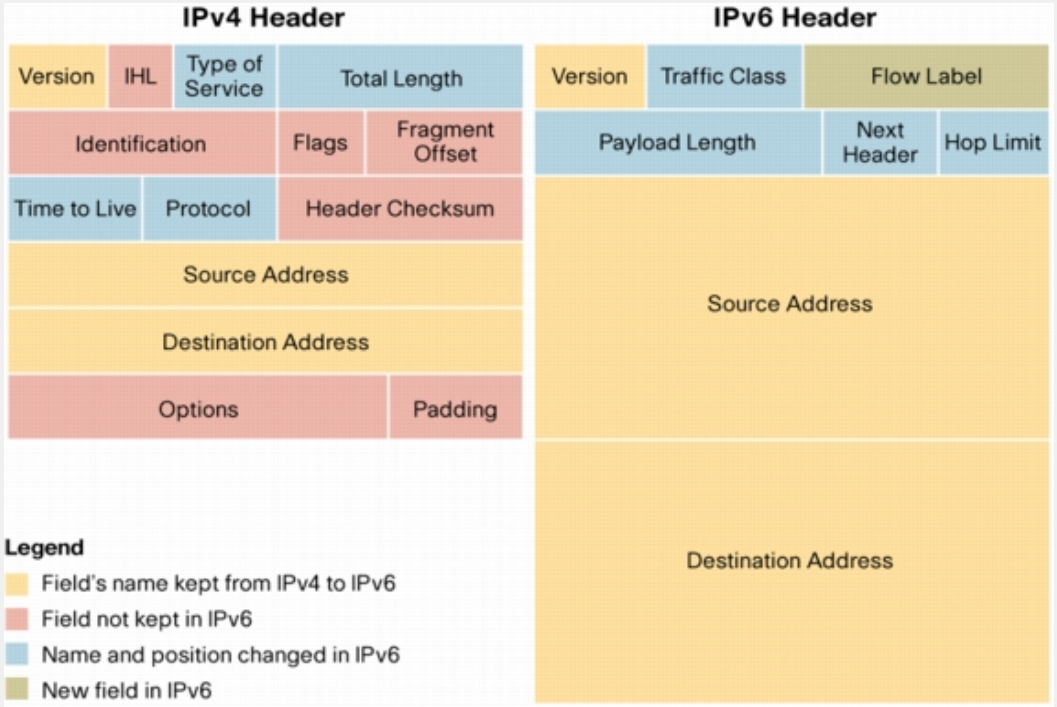




На рисунках показано распределение адресов IPv4 региональными интернет-регистраторами (RIR), а также процесс исчерпания пула IPv4 сетей с маской `/8`.

Формат пакета IPv6

Заголовок IPv6 в сравнении с IPv4



Одним из основных конструктивных улучшений протокола IPv6 по сравнению с IPv4 является упрощённый заголовок IPv6. Заголовок IPv4 состоит из 20 октетов (до 60 байт, если используется поле «Параметры») и 12 основных полей заголовка, не учитывая поля «Параметры» и «Заполнитель». Заголовок IPv6 состоит из 40 октетов (главным образом из-за длины адресов IPv6 источника и назначения) и 8 полей заголовков (3 основных поля заголовков IPv4 и 5 дополнительных полей). Кроме того, в IPv6 добавлено новое поле, которое не используется в протоколе IPv4.

Упрощённый заголовок IPv6 предлагает ряд преимуществ по сравнению с IPv4: повышенная эффективность маршрутизации для масштабируемости производительности и скорости пересылки; не требуется обработка контрольных сумм (выигрыш в том, что не требуется пересчитывать CS при уменьшении TTL); упрощённые и более эффективные механизмы заголовков расширений (в отличие от поля «Параметры» в IPv4); поле «Метка потока» предназначена для обработки по потокам без необходимости открывать транспортный внутренний пакет для определения различных потоков трафика.

Поля заголовка IPv6

Версия (Version)

Поле, содержащее 4-битное двоичное значение, которое определяет версию IP-пакета. Для пакетов IPv6 в этом поле всегда указано значение `0b0110`, т. е. 6.

Класс трафика (Traffic Class)

8-битное поле, соответствующее полю «Type of service» в заголовке IPv4. Оно содержит 6-битное значение точки кода дифференцированных сервисов (DSCP), которое используется для классификации пакетов, а также 2-битное значение явного уведомления о перегрузке (ECN), используемое для управления перегрузками трафика.

Метка потока (Flow Label)

20-битное поле, предоставляющее специальную службу для приложений реального времени. Используя это поле, маршрутизаторам и коммутаторам передается информация о необходимости поддерживать один и тот же путь для потока пакетов, что поможет избежать их переупорядочивания.
Метка потока присваивается узлом-отправителем путём генерации псевдослучайного 20-битного числа. Все пакеты одного потока должны иметь одинаковые заголовки, обрабатываемые маршрутизатором.
При получении первого пакета с меткой потока маршрутизатор анализирует дополнительные заголовки, выполняет предписанные этими заголовками функции и запоминает результаты обработки (адрес следующего узла, опции заголовка переходов, перемещение адресов в заголовке маршрутизации и т. д.) в локальном кэше. Ключом для такой записи является комбинация адреса источника и метки потока. Последующие пакеты с той же комбинацией адреса источника и метки потока обрабатываются с учётом информации кэша без детального анализа всех полей заголовка. Время жизни записи в кэше составляет не более 6 секунд, даже если пакеты этого потока продолжают поступать. При обнулении записи в кэше и получении следующего пакета потока пакет обрабатывается в обычном режиме, и для него происходит новое формирование записи в кэше. Указанное время жизни потока может быть явно определено узлом отправителем с помощью протокола управления или опций заголовка переходов и может превышать 6 секунд.

Поля заголовка IPv6

Длина полезной нагрузки (Payload Length)

16-битное поле, соответствующее полю «Общая длина» в заголовке IPv4. Оно определяет размер всего пакета (фрагмента) после заголовка, включая дополнительные расширения.

Следующий заголовок (Next Header)

8-битное поле, соответствующее полю «Протокол» в заголовке IPv4. Оно указывает тип полезной нагрузки данных, которые переносит пакет, что позволяет сетевому уровню пересылать данные на соответствующий протокол более высокого уровня. Это поле также используется в тех случаях, когда в пакет IPv6 добавляются дополнительные заголовки расширений.

Предел перехода (Hop Limit)

8-битное поле, заменяющее поле «Время жизни» (TTL) в IPv4. Это значение уменьшается на единицу каждым маршрутизатором, пересылающим пакет. Когда счетчик достигает 0, пакет отбрасывается, и на отправляющий узел пересылается сообщение ICMPv6, которое означает, что пакет не достиг своего назначения.

Адрес источника (Source Address)

128-битовое поле, определяющее IPv6-адрес принимающего узла.

Адрес назначения (Destination Address)

128-битное поле, определяющее IPv6-адрес принимающего узла.

Расширенные заголовки (Extension headers)

Расширенные заголовки (или *заголовки расширений*) содержат дополнительную информацию и размещены между фиксированным заголовком и заголовком протокола более высокого уровня. Тип первого расширенного заголовка указывается в поле Next Header фиксированного заголовка, а каждый расширенный заголовок имеет аналогичное поле в котором хранится тип следующего расширенного заголовка. В поле Next Header последнего заголовка находится тип протокола более высокого уровня, находящегося в качестве полезных данных.
Каждый расширенный заголовок должен иметь размер в октетах, кратный 8. Некоторые заголовки необходимо расширить до нужного размера.
Расширенные заголовки должны быть обработаны только конечным узлом, за исключением заголовка Hop-By-Hop Options, который должен быть обработан каждым промежуточным узлом на пути пакета, включая отправителя и получателя. Если расширенных заголовков в пакете несколько, то рекомендуется отсортировать их как указано в таблице ниже. Отметим, что все расширенные заголовки являются необязательными и не должны появиться в пакете более одного раза, за исключением заголовка Destination Options, который может появиться дважды.
Если узел не может обработать какой-то расширенный заголовок, то он должен отбросить пакет и отправить сообщение Parameter Problem (ICMPv6 тип 4, код 1). Если в поле Next Header расширенного заголовка будет 0, то узел должен сделать то же самое.

Некоторые расширенные заголовки

Расширенный заголовок	**Тип**	**Описание**
Hop-by-Hop Options	0	Параметры, которые должны быть обработаны каждым транзитным узлом.
Destination Options	60	Параметры которые должны быть обработаны только получателем.
Routing	43	Позволяет отправителю определять список узлов, которые пакет должен пройти.
Fragment	44	Заголовок содержит информацию по фрагментации пакета.
Authentication Header (AH)	51	Содержит информацию, для аутентификацию большей части пакета.
Encapsulating Security Payload (ESP)	50	Осуществляет шифрование данных для безопасных подключений.

Определение размера пакета в IPv6

Маршрутизаторы IPv6 больше не должны фрагментировать пакет, вместо этого пакет отбрасывается с ICMP-уведомлением о превышении MTU. Передающая сторона в IPv6, таким образом, должна или использовать технологию Path MTU discovery (RFC 1191), или использовать минимальный MTU. Для лучшей работы протоколов, требовательных к потерям, минимальный MTU поднят до 1280 байт. Фрагментация поддерживается как опция (информация о фрагментации пакетов вынесена из основного заголовка в расширенные) и возможна только по инициативе передающей стороны.

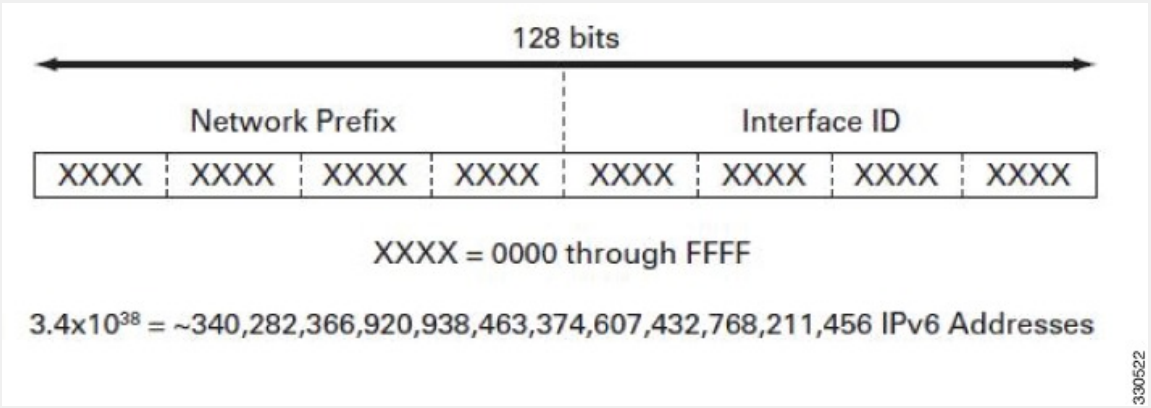
Термин Path MTU означает наименьший MTU на пути следования пакета в сети.

Узел, значение MTU которого меньше размера пакета, отклоняет передачу пакета и отправляет сообщение ICMP «необходима фрагментация, но установлен флаг её запрета (Don't Fragment)». Хост-отправитель уменьшает размер пакета и отсылает его заново. Такая операция происходит до тех пор, пока пакет не будет достаточно мал, чтобы дойти до хоста-получателя без фрагментации.

Существуют потенциальные проблемы. Некоторые маршрутизаторы настраиваются администраторами на полное блокирование ICMP пакетов. В результате, если размер пакета не соответствует значению MTU на определённом участке, пакет отбрасывается, а хост-отправитель не может получить информацию о значении MTU и не отправляет пакет заново. Поэтому соединение между хостами не устанавливается. Проблема получила название MTU Discovery Black Hole (RFC 2923), и протокол был модифицирован для детектирования таких маршрутизаторов.

Существует несколько вариантов решения этой проблемы. Самым простым является отмена фильтрации пакетов ICMP. Поскольку зачастую подобная операция находится вне компетенции пользователя, проблему решают путем ручной настройки размера передаваемого пакета на шлюзе пользователя. Для этого меняют значение MSS (максимальный размер сегмента, то есть величина, меньшая MTU на 40 байт в случае протокола IPv4). При установке соединения хосты обмениваются информацией о максимальном размере сегмента, который каждый из них сможет принять. Поэтому, меняя значение MSS, заставляют оба хоста обмениваться пакетами, которые шлюз пользователя сможет заведомо принять без фрагментации.

Адрес IPv6



Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. 4 бита представлены одной шестнадцатеричной цифрой. Всего 32 цифры. Адресация IPv6 определена в RFC 4291.

Правила сокращенного представления IPv6 адресов

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

1. Пропуск всех ведущих 0 в шестнадцатеричной записи

```
01AB -> 1AB     09F0 -> 9F0     0A00 -> A00     00AB -> AB
```

```
2001:db8:85a3:0:0:8a2e:370:7334
```

   Это правило применяется только к ведущим нулям, а НЕ к последующим, иначе адрес будет записан неясно.

2. Двойное двоеточие (::) может заменить любую единую, смежную строку одного или нескольких 16-битных сегментов (хекстетов), состоящих из нулей. Двойное двоеточие (::) может использоваться в адресе только один раз.

```
2001:db8:85a3::8a2e:370:7334
```

   Неверный адрес:

```
2001:0DB8::ABCD::1234
```

Типы IPv6-адресов. Unicast адреса

Классификация по способу адресации

- Unicast адреса идентифицируют только один сетевой интерфейс. Протокол IPv6 доставляет пакеты, отправленные на такой адрес, на конкретный интерфейс. Существует шесть типов Unicast адресов
- Anycast адреса назначаются группе интерфейсов, обычно принадлежащих различным узлам. Пакет, отправленный на такой адрес, доставляется на один из интерфейсов данной группы, как правило наиболее близкий к отправителю с точки зрения протокола маршрутизации.
- Multicast адрес также используется группой узлов, но пакет, отправленный на такой адрес, будет доставлен каждому узлу в группе. Различают два типа Multicast адресов.

В IPv6 не реализованы широковещательные адреса. Традиционная роль широковещательной рассылки реализована с помощью групповой рассылки на адрес `ff02::1`, однако использование не рекомендуется.

Global unicast

Global unicast адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически.

Loopback

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, который выглядит как `::1/128` или просто `::1` в сжатом формате.

Unicast адреса

Link-local

Local IPv6-адрес канала 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 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`.

Unspecified address

Неопределённый адрес состоит из нулей и в сжатом 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.

Unicast адреса

Unique local

Unique local IPv6-адреса (RFC 4193) имеют некоторые общие особенности с частными («серыми») адресами 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/PAT) для обеспечения преобразования адресов из частных в публичные. Это делается из-за недостатка адресного пространства IPv4. Во многих сетях 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 Интернета IPv6. IETF рекомендует ограничивать доступ к устройствам с помощью наилучших мер безопасности.

IPv4 embedded

Встроенные IPv4-адреса. Использование этих адресов способствует переходу с протокола IPv4 на IPv6. Эти адреса определены в RFC 6052. Выделяют так называемый *IPv4 совместимый IPv6 адрес* вида `::FFFF:xx.xx.xx.xx/96`, в котором нижние 32 бита это адрес IPv4. Устарел и больше не используется. Также выделяют *адрес IPv4, отображённый на IPv6* вида `::xx.xx.xx.xx/96`.

Global unicast IPv6

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 `0b001` или `2000::/3`. Это лишь 1/8 от всего доступного адресного пространства IPv6. Адрес `2001:0DB8::/32` был зарезервирован для документации, в том числе для использования в примерах.

Структура Global unicast адреса

- Префикс глобальной маршрутизации — Префикс глобальной маршрутизации — это префиксальная или сетевая часть адреса, назначаемая интернет-провайдером заказчику или узлу. В настоящее время `/48` является префиксом глобальной маршрутизации, который в настоящее время интернет-регистраторы назначают своим заказчикам — корпоративным сетям и индивидуальным пользователям. Этого адресного пространства более чем достаточно для большинства заказчиков.
- Идентификатор подсети — Идентификатор подсети используется организациями для обозначения подсетей в каждом узле.
- Идентификатор интерфейса — Идентификатор IPv6-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.

Процесс EUI-64

Организация IEEE разработала расширенный уникальный идентификатор (EUI) или изменённый процесс EUI-64. Этот процесс использует 48-битный MAC-адрес Ethernet клиента и в середину этого адреса вставляет ещё 16 бит для создания 64-битного идентификатора интерфейса. Преимущество EUI-64 MAC-адреса Ethernet заключается в том, что его можно использовать для определения идентификатора интерфейса. Кроме того, сетевые администраторы могут легко отслеживать IPv6-адрес до конечных устройств с помощью уникального MAC-адреса.
Однако, именно возможность отследить как пакеты устройства, так и перемещение самого устройства между сетями привела к тому, что были высказаны опасения о нарушении приватности пользователей, а также ою уменьшении уровня безопасности сети. Соответственно, современные ОС на конечных устройствах генерируют идентификатор интерфейса случайным образом.

1 шаг: EUI-48 $\longrightarrow$ EUI-64

```
02:0C:29:0C:47:D5 ==> 02:0C:29:FF:FE:0C:47:D5
```

2 шаг: инверсия бита Unique/Local

```
02:0C:29:FF:FE:0C:47:D5 ==> 00:0C:29:FF:FE:0C:47:D5
```

Пример получения адреса IPv6 из локального MAC-адреса

```
02:00:00:00:00:01 ==> FE80::FF:FE00:1
```

Multicast IPv6. Assigned multicast

Multicast IPv6-адреса мало чем отличаются от multicast IPv4-адресов. Multicast адрес используется для отправки одного пакета по одному или нескольким назначениям (группе мультивещания). Multicast IPv6-адреса имеют префикс `FF00::/8`. Multicast адреса могут быть только адресами назначения, а не адресами источника. Существует два типа:

1. Назначенные (присвоенные) (Assigned multicast)
2. Запрошенные (Solicited multicast)

Присвоенные групповые адреса (Assigned multicast)

Присвоенные групповые адреса зарезервированы для заданных групп устройств. Присвоенный групповой адрес — это один адрес, используемый для осуществления связи с группой устройств, работающих на одном протоколе или сервисе. Присвоенные групповые адреса используются вместе с конкретными протоколами, например с протоколом DHCPv6. Есть две распространённые группы присвоенных групповых IPv6-адресов.

1. Группа мультивещания для всех IPv6-узлов `FF02::1`, к которой подключены все устройства под управлением протокола IPv6. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-интерфейсами в канале или сети. Эта группа адресов работает так же, как широковещательный адрес в протоколе IPv4.
2. Группа мультивещания для всех маршрутизаторов `FF02::2`, к которой подключены все IPv6-маршрутизаторы. Пакет для этой группы получается и обрабатывается всеми IPv6-маршрутизаторами в канале или сети.

Групповой IPv6-адрес запрашиваемого узла (Solicited multicast)

Групповой IPv6-адрес запрашиваемого узла создаётся автоматически при назначении глобального индивидуального адреса или локального адреса канала. Групповой IPv6-адрес запрашиваемого узла создаётся посредством объединения специального префикса `FF02:0:0:0:0:1:FF00::/104` с крайними правыми 24 битами его индивидуального адреса.
Очень редко в идентификаторах интерфейса устройств встречаются одинаковые крайние правые 24 бита. Это не влечёт за собой никаких проблем, поскольку устройство по-прежнему будет обрабатывать инкапсулированное сообщение, в котором содержится полный IPv6-адрес запрашиваемого устройства.

Разбиение на подсети

Разбиение IPv6-сети на подсети подразумевает использование другого подхода, чем разбиение на подсети IPv4-сети. Пространство IPv6-адресов разбивается не с целью экономии адресов, а для обеспечения иерархической логической структуры сети. Разбиение на подсети в IPv6 возможно провести двумя вариантами.

Разбиение на подсети с использованием идентификатора подсети

Блок IPv6-адресов с префиксом `/48` содержит 16 бит идентификатора подсети. Разбиение на подсети с использованием 16 бит идентификатора подсети даёт 65536 возможных подсетей `/64`. Поэтому нет необходимости заимствовать биты из идентификатора интерфейса или узловой части адреса. Каждая IPv6-подсеть `/64` содержит примерно $18 \cdot 10^{18}$ адресов, что гораздо больше, чем когда-либо понадобится в одном сегменте IP-сети. Подсети, созданные из идентификатора подсети, легко представить, поскольку не нужно выполнять преобразование в двоичный формат. Чтобы определить следующую доступную подсеть, достаточно рассчитать следующее шестнадцатеричное число. Необходимо применить расчёт части идентификатора подсети в шестнадцатеричной системе счисления. Префикс глобальной маршрутизации является одинаковым для всех подсетей. Для каждой подсети увеличивается только четырёхразрядный идентификатор подсети.

Разбиение на подсети

Разбиение на подсети с использованием идентификатора интерфейса

В IPv6-сетях по аналогии с заимствованием бит из узловой части IPv4-адреса можно позаимствовать биты из идентификатора интерфейса для создания дополнительных IPv6-подсетей. Как правило, это делается по соображениям безопасности, чтобы уменьшить число узлов в подсети и создавать дополнительные подсети. При расширении идентификатора подсети путём заимствования бит из идентификатора интерфейса рекомендуется создавать подсеть на границе полубайта (4 бита или одна шестнадцатеричная цифра). Префикс подсети `/64` расширяется на четыре бита или один полубайт до подсети `/68`. Это позволяет уменьшить размер идентификатора на 4 бита (с 64 до 60). Разбиение на подсети по границе полубайта имеет значение только для масок подсетей, выровненных по полубайту. Начиная с `/64`, масками подсети, выровненными по полубайту, будут являться маски `/68`, `/72`, `/76`, `/80` и т. д. Разбиение на подсети по границе полубайта позволяет создать подсети с использованием дополнительного шестнадцатеричного значения. Можно создать подсеть в пределах полубайта, используя шестнадцатеричную цифру, однако это не рекомендуется и, кроме того, в этом нет необходимости. Разбиение на подсети в пределах полубайта сводит на нет преимущества быстрого определения префикса из идентификатора интерфейса. Например, если используется длина префикса `/66`, первые два бита были бы частью идентификатора подсети, а вторые два бита — частью идентификатора интерфейса.

Источники

- Материалы с сайта `https://wikipedia.org/`
- Материалы с сайта `https://www.rfc-editor.org/`
- RFC 4291. IP Version 6 Addressing Architecture.
- IPV6 — это весело. Часть 1. URL: `https://habrahabr.ru/post/253803/`