

Лекция 8.

Протокол IPv6

8.1. Основные недостатки IPv4, и цели и краткая история создания IPv6

Уже при рассмотрении нами бесклассовой адресации по маске и внутренних адресов протокола IPv4 нами отмечался один из основных недостатков протокола IPv4, состоящий в довольно таки жесткой ограниченности предоставляемого этим протоколом адресного пространства. При этом разработчики протокола IPv4 уже к началу 1990-х годов осознали, что введение бесклассовой адресации по метке и внутренних адресов являются лишь временными мерами, позволяющим отодвинуть срок, но не предотвратить момент наступления события, состоящего в полном исчерпании доступных для распределения IPv4 адресов.

Кроме наличия указанной проблемы протокол IPv4 обладает и другими недостатками, основными из которых является крайне высокая нагрузка на маршрутизаторы (особенно - магистральные) сети, что предъявляет очень высокие требования к производительности этих маршрутизаторов, а также ограниченный функционал протокола IPv4 в части поддержки служб качества сетевого обслуживания QoS, средств обеспечения информационной безопасности (протокол IPsec) и отсутствия возможности расширения этого функционала.

После осознания того, что бесклассовая адресация и введение внутренних IP-адресов не в состоянии предотвратить полного ичерпания адресного пространства IP адресов, к 1992 году было подготовлено несколько различных предложений по развитию протокола IP и к концу 1992 года Инженерный совет Интернет IETF (Internet Engineering Task Group) объявил конкурс для рабочих групп на создание интернет-протокола следующего поколения (IP Next Generation — IPng).

К 1996 году под руководством IETF была выпущена серия RFC, определяющих Интернет протокол версии 6 (IPv6) (версия 5 протокола IP к тому моменту была уже назначена экспериментальному протоколу передачи видео и аудио информации).

Конкретизируем основные цели и задачи, которые ставились разработчикам протокола IP следующего поколения, для обеспечения устранения отмеченных

выше недостатков текущей версии протокола IP. Основными целями создания и протокола IP следующего поколения :

1. создание масштабируемой системы адресации
2. уменьшение нагрузки на маршрутизаторы и повышение скорости работы сети
3. предоставление базовых средств для организации службы QoS
4. предоставление базовых средств обеспечения информационной безопасности
5. Возможности расширения функционала протокола

При этом была поставлена задача создания новой версии протокола IP, обеспечивающей не только достижение указанных целей, но и возможность плавного перехода от старой версии к новой, предполагающего достаточно продолжительное во времени сосуществование и взаимодействие старой и новой версий протоколов IP.

Как отмечено выше поставленные цели были достигнуты к 1996 г. С этого момента начался очень плавный переход к новой версии протокола IPv6. Вплоть до конца 2010-х годов этот протокол использовался преимущественно в экспериментальных сетях. На конец 2015 года лишь около 1% пользователей интернета работали на IPv6 адресах. И это при том, что ведущие производители сетевого оборудования, разработчики сетевого программного обеспечения и владельцы основных интернет-сайтов уже давно выпустили версии своих продуктов, работающих с использованием протокола IPv6.

Такое положение дел во многом объясняется, с одной стороны, высокой степенью ответственности производителей сетевого оборудования, программного обеспечения и интернет-сайтов перед уже почти вплотную приблизившейся угрозой полного исчерпания адресного пространства IPv4. К настоящему моменту лишь регистраторы IP-адресов Европы, Азии и Латинской Америки (RIPE NIC, APNIC и LACNIC) все еще продолжают выдачу IP-адресов IPv4, но всего лишь блоками /22 (по 1024 адреса или 4 сети класса C). В Северной Америке последний адресный блок IPv4 был распределён ещё в мае 2017. Поэтому упомянутые производители полностью подготовились к неизбежной интенсификации перехода все новых сетей и подсетей на протоколы IPv6.

С другой стороны позиция руководства корпоративных сетей, не спешащего переводить свои сети на новые протоколы, объясняется довольно здоровым консерватизмом: коли уж IP-адреса версии 4 выделены, их никто не отберет, а

значит – переход на новые протоколы можно отложить на более поздний срок, когда переход станет достаточно массовым и будет накоплен достаточно большой опыт по эффективному выполнению такого перехода. **А массовым переход станет тогда,** когда не только у всех регистраторов IP-адресов не останется свободных блоков IP-адресов 4-й версии, но **когда и у операторов связи не останется никаких “запасов” таких адресов.** *Тогда они будут просто вынуждены выполнять подключения всех новых абонентских сетей только по протоколам IPv6.*

8.2. Система адресации IPv6

8.2.1. Новый формат записи IP-адресов

В IPv6 длина IP-адреса увеличена вчетверо по сравнению с предыдущей версией IP с **32 до до 128 бит (с 4 до 16 байт).** А это значит, что представимое в поле IP-адреса количество различных значений достигает космических масштабов. Если предположить, что все население Земли составляет порядка 7 миллиардов, то **на каждого жителя Земли можно выделить более $5 \cdot 10^{28}$ различных IP-адресов.** Конечно, если учесть, что поле IP-адреса является структурированным и содержит некоторые подполя лишь с частично используемыми диапазонами их значений, указанное количество снизится на несколько порядков, но все равно останется космически большим. **До переполнения такого адресного пространства немислимо добраться даже в том случае, если каждый человек окружит себя тысячами и миллионами подключенных к интернету устройств.**

Естественно, что простое **механическое увеличение разрядности IP-адреса** хотя и позволяет снять пределы масштабирования адресного пространства, но, без дополнительной структуризации IP-адреса **не позволяет, например, уменьшить размер маршрутных таблиц и тем самым повысить скорость выполнения маршрутизации пакетов.** Уменьшение размеров таблиц маршрутизации **может быть достигнуто за счет увеличения количества уровней иерархии сетей, нашедшее свое отражение в полях IP-адреса.** В отличие от одного уровня номера подсети, входящего в структуру адреса IPv4 **в адресе IPv6 используется целых 3 уровня иерархически вложенных сетей,** что позволяет существенно уменьшить размер таблиц маршрутизации.

Вместе с разрядностью IP-адреса и введением в него дополнительных полей **изменилась и форма его записи.** Использование десятичной системы счисления

неудобно при работе с двоичными данными. Особенно это заметно при работе с масками подсети. Поэтому для представления адресов IPv6 выбрана шестнадцатеричная система счисления, позволяющая записать значение каждого байта в виде пары шестнадцатеричных цифр.

Каждый IPv6 адрес записывается в виде разделенных символом двоеточия ":" восьми пар байтов, каждый из которых записывается в виде 4-х 16-ричных цифр (от "0" до "F"). При этом может использоваться несколько приемов сокращения записи. Так одна (и только одна) последовательность из одного или несколько нулевых полей может опускаться вместе разделяющими эти нулевые поля символами двоеточия при расположении этой последовательности в середине IP-адреса. Ведущие нули в начале значения каждого поля адреса тоже могут опускаться.

Кроме того, для сетей поддерживающих обе версии протокола IPv6 и IPv4, значения 4-х последних байт могут записываться в традиционной для IPv4 десятичной форме.

8.2.2. Типы адресов IPv6

В IPv6 используются 3 основных типа IP-адресов:

- unicast ("одноточечный", классы A-C в IPv4)
- multicast (групповой, класс D в IPv4), broadcast стал частным случаем multicast'a
- anycast (новый тип адреса, поясняется ниже).

Принадлежность адреса тому или иному типу определяется на основе поля префикса формата FP (Format Prefix), располагающегося в старших битах IP-адреса и имеющего различную длину для адресов различных типов.

Адреса типа unicast имеют несколько подтипов (различаются на основе FP) и подробно рассматриваются ниже.

Адреса типа multicast имеют FP "FF" ("FFFF" для broadcast'a). Адрес этого типа включает поле области действия Score этого адреса, например, одну подсеть, либо все подсети данной организации, либо весь интернет.

Anycast адрес определяет группу IP адресов интерфейсов маршрутизаторов. Пакет с таким адресом получателя доставляется «любому» (фактически – ближайшему в соответствии с таблицей маршрутизации источника пакета) маршрутизатору. Может назначаться ТОЛЬКО интерфейсам маршрутизатора, которые должны иметь и уникальные unicast-адреса.

При этом в качестве **anycast-группы** обычно указываются внешние порты всех пограничных маршрутизаторов некоторой сети (например – AS). **Такой тип адреса удобен для описания полного маршрута передачи пакета** получателю, в котором указываются не абсолютно все промежуточные маршрутизаторы, а лишь **anycast-адреса всех промежуточных сетей (не задавая маршрутов внутри этих подсетей)**. Такой способ адресации получателя пакета путем задания маршрута **следования к получателю называется маршрутизацией от источника (Source Routing)** и, благодаря превносимым адресами типа anycast возможностями описания “укрупненного” маршрута через промежуточные сети может достаточно широко использоваться в IPv6.

Отметим, что в IPv6 есть специальные адреса, предназначенные для локального использования, но смысл их коренным образом отличается от смысла внутренних адресов IPv4. **Адреса для локального использования в IPv6 предназначены для применения в сетях, не связанных с интернетом и далее нами не рассматриваются.**

Виды unicast адресов

Глобальный unicast адрес, его формат представлен на рис. 1. Как упоминалось выше, в нем выделены 3 уровня иерархии номеров сетей.

3	13	8	24	16	64
FP	TLA	Резерв	NLA	SLA	Inteface ID

Рис. 1. Формат глобального unicast адреса

Длины полей в битах указаны над этими полями. Здесь:

FP (Format Prefix) принимает двоичное значение “001”.

TLA - Top Level Aggregation (Верхний уровень агрегации адресов) - адреса сетей крупных интернет провайдеров.

Резерв - это поле зарезервировано для дальнейших расширений (для использования этого поля некоторыми дополнительными функциями).

NLA - Next Level Aggregation (следующий уровень агрегации адресов) - адреса сетей средних и мелких интернет провайдеров.

SLA - Site Level Aggregation (уровень агрегации адресов сети абонента), обратите внимание на то, как много сетей имеется в распоряжении владельцев корпоративных сетей.

Interface ID - идентификатор интерфейса компьютера. В качестве такого идентификатора в IPv6 используется **значение MAC адреса**. Разрядность этого поля (64) превышает максимальную разрядность (60) всех известных сетевых технологий. За счет использования в качестве идентификатора интерфейса значения соответствующего MAC адреса **можно избавиться от необходимости использования протокола ARP**, что позволяет снизить нагрузку на маршрутизаторы.

Отметим также, что **использование иерархии адресов сетей позволяет сократить размеры таблиц маршрутизации**, что также влечет снижение нагрузки на маршрутизаторы. **Дополнительное сокращение таблиц маршрутизации может быть обеспечено агрегацией групп смежных сетей таблицы маршрутизации** с использованием маски подсети. Подчеркнем, что этот механизм доступен и в IPv6, однако **только для агрегации сетей, а не для их разбиения на** части, потребность в котором полностью отпадает ввиду возможности использования до $2^{16}-2$ номеров подсетей корпоративной сети.

Специальные unicast адреса.

В протоколе IPv6 используются несколько типов специальных unicast адресов, а именно:

- **адрес обратной связи** PF = "0000 0000" (полный адрес 0::1 – аналог адреса 127.0.0.1 для IPv4);
- **неопределенный адрес** 0::0; этот адрес не может встречаться в IP-пакетах, он лишь присваивается по умолчанию не проинициализированным интерфейсам;
- **две разновидности, предназначенные для обеспечения взаимодействия с сетями IPv4:**
 - **IPv4-совместимые** – содержат нули во всех байтах, кроме 4-х последних (в которых содержится IPv4 адрес); пакеты с такими адресами могут легко передаваться между двумя подсетями IPv6 через сеть IPv4;
 - **IPv4-отображенные** – 4 последних байта как в совместимых, а 5-6 младшие байты содержат значение FFFF:FFFF, которое является признаком того, что адресуемый узел понимает только протокол IPv4;
- **IPX-отображенные** – Префикс формата содержат "0000 0010", остальные 121 бит содержат адрес IPX и, возможно (стандартом еще не определено), какую-то дополнительную информацию.

8.3. Гибкий формат заголовка пакета IPv6

Заголовок пакета IPv6 содержит обязательный основной заголовок и может содержать несколько необязательных дополнительных заголовков.

8.3.1. Формат основного заголовка

Основной заголовок имеет длину 40 байт (в отличие от 20 байт заголовка пакета IPv4) и формат, представленный на рис.2.

Версия	Класс трафика	Метка потока	
Размер пакета		След. заголовок	TTL
IP-адрес получателя			
IP-адрес источника			

Рис 2. Формат основного заголовка пакета IPv6

Рассмотрим назначение и разрядность полей основного заголовка пакета.

- 4-битовое поле “версия” содержит значение “0110” .
- 8-битовое поле “класс трафика” состоит из двух подполей: старшие 6 бит используются для классификации (задания приоритетов обработки и удаления пакетов), оставшиеся два бита используются для контроля перегрузок.
- 20-битовое поле “метка потока” однозначно идентифицирует последовательности пакетов, пересылаемых между одной парой адресатов. Каждый адресат идентифицируется своими IP-адресом и номером порта прикладного процесса (номера портов входят в заголовок пакета транспортного уровня. Отметим, что значения двух последних полей основного заголовка и всех дополнительных заголовков пакета для всех

пакетов одного потока должны совпадать). Для ускорения обработки потока пакетов при обработке 1-го пакета потока маршрутизатор запоминает в кэш-памяти параметры обработки дополнительных заголовков потока и для последующих пакетов этого же потока не анализирует этих дополнительных заголовков, что существенно снижает нагрузку на маршрутизатор и увеличивает скорость его работы.

- 16-битовое поле “размер пакета” задает размер пакета в байтах и включает суммарный размер данных и дополнительных заголовков, но не основного заголовка.
- 8-битовое поле “следующий заголовок” задает смещение следующего дополнительного заголовка; если дополнительных заголовков нет, или это поле указано в последнем дополнительном заголовке, то значением этого поля является код протокола более высокого уровня (TCP, UDP и пр.).
- 8-битовое поле TTL имеет такой же смысл, что и в IPv4.
- И, наконец, 2 последних 128-битовых поля задают адреса получателя и отправителя IP-пакета.

8.3.2. Основные типы дополнительных заголовков.

Рассмотрим основные типы и назначение наиболее часто используемых дополнительных заголовков пакетов IPv6:

- **Routing** – полный маршрут к получателю, заданный методом Source Routing с использованием anycast адресов; существенно снижает нагрузку на маршрутизаторы и увеличивает скорость их работы.
- **Fragmentation** - обеспечивает поддержку выбора MTU конечными узлами (отправителем и получателем), а не каждой парой соседних по направлению пересылки пакетов маршрутизаторов; что обеспечивает существенное уменьшение нагрузки на маршрутизаторы.
- **Authentication** – поддерживает возможность аутентификации с целью повышения уровня информационной безопасности.
- **Encapsulation** - для шифрования передаваемых данных в целях информационной безопасности)

8.4. Оценка достижения целей, поставленных при разработке IPv6

На основании рассмотрения основных возможностей, предоставляемых протоколом IPv6 можно прийти к однозначному выводу о том, что все поставленные цели полностью достигнуты. Для каждой поставленной цели прокомментируем, что сделано для ее достижения.

1. Создание масштабируемой системы адресации. Цель достигнута за счет введения нового формата IP-адреса.
2. Уменьшение нагрузки на маршрутизаторы и повышение скорости работы сети. Цель достигнута за счет введения 3-х уровней агрегации сетей (и соответствующего уменьшения таблиц маршрутизации), ускорения маршрутизации потоков пакетов на базе поля “метка потока”, отказа от ARP, возможностей широкого использования маршрутизации от источника, ускорения обработки потоков пакетов и путем перенесения нагрузки на фрагментацию/дефрагментацию пакетов с маршрутизаторов на конечные узлы.
3. Предоставление базовых средств для организации службы QoS. Для достижения этой цели в формат основного заголовка IPv6 пакета включено поле “класс трафика”, в котором для представления приоритета используется 6 (а не 3, как в IPv4 бит). Кроме того, значение поля “метка потока” может использоваться для идентификации соединений между конкретной парой программных процессов, работающих на различных компьютерах сети.
4. Предоставление средств обеспечения информационной безопасности. Для поддержки информационной безопасности в гибкий формат пакета введены 2 типа дополнительных заголовков: Authentication и Encapsulation.
5. Возможности расширения протокола IPv6 дополнительной функциональностью поддерживаются наличием 8-битного поля “расширение” в формате IP-адреса а также возможностью введения дополнительных заголовков пакетов требуемого типа.

8.5. О возможностях плавного перехода с IPv4 на IPv6

Выше упоминалось, что перед разработчиками IPv6, в частности ставилась задача обеспечения возможности плавного перехода с IPv4 на IPv6,

предполагающая достаточно продолжительное существование и взаимодействие сетей, работающих в этих двух протоколах (до полного завершения процесса перехода на IPv6).

8.5.1. Методы сосуществования и взаимодействия сетей IPv4 и IPv6.

С момента практической реализации протокола IPv6 была создана магистральная сеть 6Bone (Bone - магистраль), состоящая из подсетей, работающих в протоколе IPv6 и связанных друг с другом через объемлющий "океан" сетей IPv4 через IP-туннели.

Уже такое решение обеспечило возможность всем подключенным к 6Bone сетям прозрачно взаимодействовать друг с другом (не замечая существования сетей IPv4). Однако использование лишь одного механизма *IP-туннелей* не позволяет решить задачу взаимодействия двух компьютеров, один из которых работает в сети IPv4, а другой - в сети IPv6. Для решения этой задачи дополнительно доступны следующие механизмы и возможности:

1. *Мультиплексирование стеков протоколов.* На взаимодействующих компьютерах можно установить оба стека протоколов. А дальнейшая организация взаимодействия может базироваться, например, на мультиплексировании стека протоколов по всей части маршрута между взаимодействующими компьютерами, проходящей через сеть IPv4.
2. Трансляция протоколов, то есть преобразование пакетов одного протокола в пакеты другого протокола. За счет использования IPv4 совместимых и IPv4 отображенных адресов возможна трансляция любых IPv4 пакетов в пакеты IPv6. Поэтому при взаимодействии двух IPv4 компьютеров, один из которых находится внутри IPv6 сети (и работает в двух стеках протоколов), на той части маршрута от этого компьютера к его партнеру по взаимодействию (находящемуся в сети IPv4), которая проходит от 1-го компьютера до ближайшего шлюза между сетями IPv6 и IPv4 мультиплексирование протоколов не требуется. На этом участке через сеть могут пересылаться пакеты IPv6 с IPv4 совместимыми и/или отображенными адресами, которые при прохождении через шлюз IPv6/IPv4 просто транслируются в адреса IPv4 и далее также пересылаются без всяких туннелей. Организации пересылки и в противоположном направлении выполняется симметрично.

Рассмотрев решение задачи сосуществования и взаимодействия сетей IPv4 и IPv6 перейдем к практическим вопросам перехода на IPv6.

8.5.2. О возможностях и порядке перехода к IPv6.

Технически возможность перехода с IPv4 на IPv6 в настоящее время полностью обеспечена: практически все ведущие производители маршрутизаторов и сетевого программного обеспечения уровней от межсетевого до прикладного включительно уже достаточно давно выпускают версии своих продуктов, предназначенные для использования в IPv6 сетях. И основным вопросом является лишь вопрос грамотной организации работы по выбору конкретных моделей и версий сетевого программного обеспечения, их конфигурированию и переходу к их использованию. К сожалению, ответ на этот вопрос выходит за рамки настоящего учебника. Но у читателей всегда остается мощная возможность обратиться за рекомендациями к поисковым системам интернета с вопросом "Как начать переход на IPv6?". И, вне всякого сомнения, среди выданных поисковой системой ответов найдутся самые актуальные ответы на момент задания вопроса, а не на момент написания настоящего учебника.