

МСС-MSN

Тема 6. Лекция 3

Технологии МСС/L3

IPv6

Костюкович А.Е.
Каф.АЭС, СибГУТИ
www.aek-54.ru

IPv6

Стандарт на IPv6 принят IETF в 1995г (RFC-1883), изменен в 1998 (RFC 2460).

Изменения IPv6 по отношению к **IPv4** можно поделить на следующие группы:

1. Расширение адресации

- В IPv6 длина адреса расширена до 128 бит, что позволяет обеспечить больше уровней иерархии адресации, увеличить число адресуемых узлов, упростить авто-конфигурацию.
- Для расширения возможности мультикастинг-маршрутизации в адресное поле введено субполе "scope" (группа адресов).
- Определен новый тип адреса "anycast address", который используется для запросов клиента группе серверов, чьи адреса не известны клиенту заранее.

2. Спецификация формата заголовков

- Некоторые поля заголовка IPv4 отбрасываются, уменьшая издержки, связанные с обработкой заголовков пакетов.
- Улучшенная поддержка расширений и опций
- Изменение кодирования опций IP-заголовков позволяет облегчить переадресацию пакетов, ослабляет ограничения на длину опций, и делает более доступным введение дополнительных опций в будущем.

IPv6

3. Возможность пометки потоков данных

- Введена возможность пометить пакеты, принадлежащие определенным транспортным потокам, например, указав тип ToS для данных в реальном масштабе времени.

4. Идентификация и защита частных обменов

- В IPv6 введена спецификация идентификации сетевых объектов или субъектов, для обеспечения целостности данных и при желании защиты частной информации.
- Формат и семантика адресов IPv6 описаны в документе RFC-1884.
- Версия ICMP IPv6 рассмотрена в RFC-1885 и RFC-4861 (обновленная версия).
- Протокол ICMPv6 выполняет также функцию получения данных о соседях (аналог протокола ARP). Для этой цели используется посылка мультикастинг-сообщений.

IPv6

Попытки остаться с IPv4, используя NAT, приводят к неизбежным конфликтам между адресом IP и номером приложения из-за занятости портов, так как современные технологии требуют реализации слишком большого числа одновременно работающих приложений (до 500).

Задержки с внедрением IPv6 препятствуют использованию беспроводной техники 4G/LTE, которая ориентирована исключительно на IPv6.

Альтернативы переходу на IPv6 нет, можно только обсуждать время, когда это следует делать.

IPv6

Препятствует такому переходу ряд обстоятельств:

1. Некоторое снижение пропускной способности из-за увеличения размера заголовка.
2. Необходимость адаптации существующих программ управления и мониторинга к IPv6.
3. Необходимость переписывания некоторых прикладных программ, например, фильтрующих SPAM.
4. Необходимость перепланировки IP-сетей.

Существуют также проблемы, сопряженные с обеспечением безопасности в переходный период.

С 30-го сентября 2012 года все агентства правительства США переведены на IPv6.

IPv6

Формат заголовка IPv6 (40 или более байт):

0	4	12	16	24	31
Версия 4 бит	Приоритет 8 бит	Метка потока (Flow Label) 20 бит			
Размер поля данных 16 бит			Next Header 8 бит	Hop Limit 8 бит	
Адрес отправителя 128 бит (16 байт)					
Адрес получателя 128 бит (16 байт)					

Из 40 байт – $(16 + 16) = 32$ байта занимает адрес
8 байт на остальные 6 полей

IPv6

Поля заголовка IPv6

Версия	4-битный код версии Интернет протокола (для IPv6 – V=6 или 0110)
Приоритет	8-битный код приоритета (RFC-2460, RFC-2474)
Метка потока	20-битный код метки потока (для мультимедиа) (RFC-2460, RFC-2474)
Размер поля данных	16 бит – Код длины поля данных (в октетах), которое следует сразу после заголовка пакета. Если код равен нулю, то длина поля данных записана в поле данных jumbo (в зоне опций).

IPv6

Поля заголовка IPv6

Next Header Следующий заголовок	8 бит. Идентифицирует тип заголовка, который следует непосредственно за IPv6 заголовком. Использует те же значения, что и протокол IPv4 [RFC-1700]
Max Hop Предельное число шагов	8 бит. Уменьшается на 1 в каждом узле, через который проходит пакет. При предельном числе шагов, равном нулю, пакет удаляется. Почти аналогично полю TTL в IPv4
Адрес отправителя	128-битовый адрес отправителя пакета. RFC-1884
Адрес получателя	128-битовый адрес получателя пакета. RFC-1884

Адресация IPv6

Существует три типа адресов IPv6:

unicast	Адрес <u>одиночного интерфейса</u> . Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.
anycast	Адрес <u>набора интерфейсов</u> (принадлежащих разным узлам). Пакет, посланный по эникастному адресу, доставляется <u>одному из интерфейсов</u> , указанному в адресе (ближайшему, в соответствии с метрикой протокола маршрутизации).
multicast	Адрес <u>набора интерфейсов</u> (принадлежащих разным узлам). Пакет, посланный по мультикастинг-адресу, доставляется <u>всем интерфейсам</u> , заданным этим адресом.

Особенности IPv6

В IPv6 не существует широковещательных адресов, их функции переданы мультикастинг-адресам.

В IPv6 все нули и все единицы являются допустимыми адресами, если не оговорено исключение.

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

IPv6 уникастный адрес связан только с одним интерфейсом. Но любому интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные).

Особенности IPv6

В IPv6 упрощена маршрутизация:

- В основном заголовке отсутствует фрагментация пакетов. На переходный период информация о фрагментации содержится в расширении заголовка.
- Исчезла контрольная сумма, т.к. ошибки в пакетах проверяют Ethernet и TCP-UDP. Это значительно упростило работу каждого маршрутизатора, т.к. при уменьшении поля **TTL** или **hop limit** на единицу, в IPv4 необходим пересчёт суммы.

Улучшения IPv6 по сравнению с IPv4

- На сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) - до 4 гигабайт;
- Появились метки потоков и классы трафика для мультимедийного трафика;
- Появилось многоадресное вещание;
- Протокол IPSec стал обязательным, что делает сети IPv6 более безопасными.

Представление записи адресов IPv6

Существует **три стандартные формы** для представления IPv6 адресов в виде текстовых строк:

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

Примеры:

FВ2С:DA98:7654:3210:FEDC:BA98:7654:3210

1780:0:0:0:8:800:200C:417A

Здесь не нужно писать начальные нули в каждом из полей, но в каждом поле должна быть, по крайней мере, одна цифра

Представление записи адресов IPv6

2. Записи некоторых типов IPv6 адресов 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.

Представление записи адресов IPv6

Последовательность "::" может использоваться для удаления из записи начальных **или** завершающих нулей в адресе.

Например:

1080:0:0:0:8:800:200c:417a 1080::8:520:340a:215c	Уникаст-адрес
ff01:0:0:0:0:0:0:43 ff01::41	Мультикаст-адрес
0:0:0:0:0:0:0:1 ::1	Адрес обратной связи (LoopBack)
0:0:0:0:0:0:0:0 ::	Неспецифицированный адрес

Представление записи адресов IPv6

3. Альтернативной формой 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 (0...255) (стандартное IPv4 представление).

Например:

Полный вид записи	Сжатый вид
0:0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

Метки потока в заголовке IPv6

20-битовое поле **метки потока** используется отправителем для выделения пакетов, которым требуется специальная обработка в маршрутизаторе, например, "real-time" сервис.

Метка IPv6 является неким аналогом Label в MPLS и позволяет для потока пакетов организовать один путь передачи из-конца-в-конец.

Поток однозначно описывается комбинацией адреса отправителя и меткой потока. Допускается несколько потоков между отправителем и получателем.

Метка потока присваивается узлом отправителя.

Метки потоков выбираются псевдослучайным образом из диапазона чисел 1 - FFFFFF

Приоритет – Класс трафика (Traffic Class)

Целью этого 8-битного поля является приоритизация трафика и предоставление услуг с гарантией качества.

IPv6 не обеспечивает гарантии скорости передачи данных или фиксированную задержку.

Однако, с помощью IPv6 можно предоставлять дифференцированные услуги, которые используют для передачи своих данных поле «класс трафика» или DSCP.

6 бит	2 бита
Класс трафика (DSCP)	ECN

Приоритет – Класс трафика (Traffic Class)

ECN (Explicit Congestion Notification) - Явное Уведомление о Перегрузке (RFC 3168).

ECN позволяет узлу уведомлять о возникновении затора на маршруте не прибегая к отбрасыванию пакетов

Биты ECN кодируются:

- 00 - поток не поддерживающий ECN: Not-ECN-Capable Transport (Not-ECT)
- 01 и 10 - поток поддерживающий ECN: ECN-Capable Transport (ECT) (например, TCP)
- 11 - подтвержденная перегрузка: Congestion Experienced (CE)

Приоритет – Класс трафика (Traffic Class)

6-бит поля «**Класс трафика**» позволяют отправителю указать приоритет доставки пакетов (от 0 до 63).

Пока стандартизованы 16 значений этого поля:

- Коды от 0 до 7 используются для задания приоритета трафика, для которого отправитель осуществляет контроль перегрузки (например, снижает поток ТСР в ответ на сигнал перегрузки).
- Значения с 8 до 15 используются для определения приоритета трафика, например, для пакетов “реального времени” с постоянной скоростью.

Приоритет

Для трафика, управляемого сигналами перегрузки (ECN), рекомендуются следующие значения приоритета для конкретных категорий приложений

Код приоритета	Назначение
0	Нехарактеризованный трафик
1	Заполняющий трафик (например, сетевые новости)
2	Несущественный информационный трафик (например, электронная почта)
3	Резерв
4	Существенный трафик (напр., FTP, HTTP, NFS)
5	Резерв
6	Интерактивный трафик (напр. telnet, x)
7	Управляющий трафик Интернет (напр., OSPF, SNMP)

Приоритет

Чем больше код приоритета, тем выше приоритет данных и тем быстрее они должны быть доставлены.

Например, для передачи мультимедийной информации, уровень приоритета должен лежать в пределах 8-15.

Практически, уровни приоритета **выше или равные 8 зарезервированы для передачи данных в реальном масштабе времени.**

Hop Limit

В отличие от IPv4, узлы IPv6 не требуют установки максимального времени жизни пакетов.

По этой причине поле TTL в IPv4 переименовано в "**Hop Limit**" (предельное число шагов) для IPv6.

На практике очень немногие IPv4 приложения, используют ограничения по TTL, так что фактически это не принципиальное изменение

Расширения заголовка в IPv6

RFC 2460 определил шесть расширений заголовка:

1. hop-by-hop,
2. маршрутизации,
- 3. фрагментации,**
4. места назначения,
5. аутентификации (AH), и
6. инкапсулирующее поле данных безопасности (ESP).

СПАСИБО за ВНИМАНИЕ

