МЕТКИ ПОТОКОВ IPV6

Н. Н. Диваков
Кафедра автоматизированных систем обработки информации, Гомельский государственный университет имени Франциска Скорины,физический факультет
Гомель, Республика Беларусь
E-mail: divakovn@gmail.com

Адресное пространство IPv6 будет распределяться IANA(Internet Assigned Numbers Authority - комиссия по стандартным числам в Интернет [RFC-1881]). В качестве советников будут выступать IAB (internet architecture board - совет по архитектуре Интернет) и IESG (Internet Engineering Steering Group - инженерная группа управления Интернет). IANA будет делегировать права выдачи IP-адресов региональным сервис-провайдерам, субрегиональным структурам и организациям. Отдельные лица и организации могут получить адреса непосредственно от регионального распределителя или сервис провайдера.

Введение

IPv6 (англ. Intenet Protocol version 6) — это новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при её использовании в Интернете. В настоящее время протокол IPv6 проходит тестирование и ещё не получил широкого распространения в Интернете, где преимущественно используется IPv4. Протокол был разработан исследовательском центре Xerox PARC. Протокол IP в настоящее время столкнулся с рядом проблем, таких как проблема масштабируемости сети, неприспособленность протокола к передаче мультисервисной информации с поддержкой различных классов обслуживания, включая обеспечение информационной безопасности. Указанные проблемы обусловили развитие классической версии протокола IPv4 в направлении разработки версии IPv6.

Содержание документа

Протокол IPv6 требует, чтобы каждый канал в Интернет имел MTU = 576 октетов или более. Для каждого канала, который не способен обеспечить длину пакетов в 576 октетов должна быть обеспечена фрагментация/дефрагментация на уровне ниже IPv6. Настоятельно рекомендуется, чтобы узлы IPv6 использовали механизм определения MTU пути [RFC-1191] для использования преимущества большо-го значения MTU. Однако в минимальной конфигурации IPv6 (например, в BOOT ROM) может ограничивать себя в пределах 576 октетов и не использо-вать path MTU discovery[3]. Для того чтобы послать пакет длиннее чем MTU канала, узел может использовать заголовок фрагментации IPv6. Однако использование такой фрагментации заблокировано в приложениях, где используется настройка по измеренному значению MTU пути. Узел должен быть способен принимать фрагментированные пакеты, которые после сборки имеют размер 1500 октетов, включая IPv6 заголовок. Узлу позволено принимать пакеты, которые после сборки имеют размер более 1500 октетов. Однако узел не должен посылать фрагменты, которые после сборки образуют пакеты длиннее 1500 октетов, если он не уверен, что получатель способен их воспринять и дефрагментировать. Метка потока присваивается потоку узлом отправителя. Новые метки потоков должны выбираться псевдослучайным образом из диапазона чисел 1 - FFFFFF. Целью псевдослучайного выбора метки является возможность использования любого набора бит поля метки потока в качестве хэш ключа маршрутизаторами для контроля состояния соответствующего потоку[1]. Все пакеты, принадлежащие одному потоку, должны быть посланы одним отправителем, иметь один и тот же адрес места назначения, приоритет и метку потока. Если какой-либо из этих пакетов включает в себя заголовок опций hop-by-hop, тогда все они должны начинаться с одного и того же содержания заголовка опций hop-by-hop (исключая поле следующий заголовок заголовка опций hop-by-hop). Если любой из этих пакетов включает заголовок маршрутизации, тогда все они должны иметь идентичные заголовки расширения, включая заголовок маршрутизации но исключая поле следующий заголовок заголовка маршрутизации. Маршрутизаторы и узлы-адресаты могут проверять эти требования (хотя это и необязательно). Если обнаружено нарушение, должно быть послано ICMP сообщение отправителю (problem message, код 0) с указателем на старший октет поля метка потока (т.е., смещение 1 в IPv6 пакете). Отправитель не должен использовать старую метку для нового потока в пределах времени жизни любого потока. Так как режим обработки потока на 6 секунд может быть установлен для любого потока, минимальный интервал между последним пакетом одного потока и первым пакетом нового, исполь-зующего ту же метку, должно быть равно 6 секундам. Метки потока, которые используются для потоков, существующих более продолжительное время не должны использоваться соответственно дольше. Когда узел останавливает или перезапускает процесс (например, в слу-

чае сбоя), он должен позаботиться о том, чтобы метка потока была уникальной и не совпадала с другой еще действующей меткой. Это может быть сделано путем записи используемых меток в стабильную память, так чтобы ею можно было воспользоваться даже после серьезного сбоя в системе. Если известно минимальное время перезагрузки системы (time for rebooting, обычно более 6 секунд), это время можно использовать для задания времени жизни меток потоков[3]. Не требуется, чтобы все или даже большинство пакетов принадлежали потокам с ненулевыми метками. Например, было бы неумно сконструировать маршрутизатор так, чтобы он работал только с пакетами, принадлежащими к тому или иному потоку, или создать схему сжатия заголовков, которая работает только с помеченными потоками. 4-битовое поле приоритета в IPv6 заголовке позволяет отправителю идентифицировать относительный приоритет доставки пакетов. Значения приоритетов делятся на два диапазона. Коды от 0 до 7 используются для задания приоритета трафика, для которого отправитель осуществляет контроль перегрузки (например, снижает поток TCP в ответ на сигнал перегрузки). Значения с 8 до 15 используются для определения приоритета трафика, для которого не производится снижения потока в ответ на сигнал перегрузки, например, в случае пакетов “реального времени”, посылаемых с постоянной частотой. Предполагается, что чем больше код, тем выше приоритет данных, тем быстрее они должны быть доставлены. Так для передачи мультимедийной информации, где управление скоростью передачи не возможно, уровень приоритета должен лежать в пределах 8-15. Практически, уровни приоритета выше или равные 8 зарезервированы для передачи данных в реальном масштабе времени. IPv6 версия ICMP-пакетов [RFC-1885] включает псевдо-заголовок в вычисление контрольной суммы; это отличается от IPv4 версии ICMP, которая не включает псевдо-заголовок в контрольную сумму. Причина изменения связана с попыткой защитить ICMP от некорректной доставки или искажений важных полей в IPv6 заголовке, который в отличие от IPv4 не защищен контрольным суммированием на интернет-уровне. Поле следующий заголовок в псевдо-заголовке для ICMP содержит код 58, который идентифицирует IPv6 версию ICMP. В отличие от IPv4, узлы IPv6 не требуют установки максимального времени жизни пакетов. По этой причине поле IPv4 "time to live"(TTL) 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[2]. При вычислении максимального размера поля данных, доступного для протокола верхнего уровня, должен приниматься во внимание большой размер заголовка IPv6 относительно IPv4. Например, в IPv4, mss-опция TCP вычисляется как максимальный размер пакета (значение по умолчанию или величина полученная из MTU) минус 40 октетов (20 октетов для минимальной длины IPv4 заголовка и 20 октетов для минимальной длины TCP заголовка). При использовании TCP поверх IPv6, MSS должно быть вычислено как максимальная длина пакета минус 60 октетов, так как минимальная длина заголовка IPv6 (т.е., IPv6 заголовок без заголовков расширения) на 20 октетов больше, чем для IPv4.

Заключение

24-битовое поле метки потока в заголовке IPv6 может использоваться отправителем для выделения пакетов, для которых требуется специальная обработка в маршрутизаторе, такая например, как нестандартная QoS или "real-time "сервис, также возможно будет некоторая поддержка ориентированных на соединение сервисов (имеется в виду соединение на уровне ip, а не tcp), которые имеют свои преимущества (маршрутизация выполняется только один раз, нагрузка на сеть заранее планируется), и недостатки (при выходе из строя одного маршрутизатора, все соединения проходящие через него разрываются) но их обсуждение выходит за рамки статьи. К тому же этот аспект IPv6 является пока экспериментальным и может быть изменен позднее. Для ЭВМ или маршрутизаторов, которые не поддерживают функцию пометки потоков, это поле должно быть обнулено при формировании пакета, сохраняться без изменения при переадресации и игнорироваться при получении. Возможно существование нескольких потоков между отправителем и получателем. Практическое значение меток еще не до конца определено, и исследования в этой области еще продолжаются.

1. Ли ,Т. Microsoft Windows 2000. TCP/IP. Протоколы и службы / Т.Ли, Д Дэвис // –М.:Axioma, 2005. – 700 с.
2. Нэйл, Р. М. IPv6. Администрирование сетей / Р. М. Нэйл, Д. Мэлоун – М.:КУДИЦ-Пресс, 2007. – 320 с.
3. Стивенс У. Р. UNIX: разработка сетевых приложений / У. Р. Стивенс, Б. Феннер, Э. М. Рудофф // – Сп.: – 2007. – 399 с.