УДК 004.716

А. Ж. ТОЙГОЖИНОВА

(Алматинский университет энергетики и связи, г. Алматы)

ПЕРЕХОД НА НОВЫЙ ИНТЕРНЕТ – ПРОТОКОЛ IPv6

Аннотация

В ближайшие несколько лет сетевым администраторам придется искать ответ на вопрос, как безбо-лезненно перейти на новую версию протокола Internet. В данной статье описываются механизмы перехода с IPv4 на IPv6, протоколы инкапсуляции, метод подключения к интернету через IPv6.

Ключевые слова: Интернет – протокол, IPv4, IPv6, протоколы инкапсуляции, смешанные сети.

Кілт сөздер: ғаламтор хаттамасы, IPv4, IPv6, инкапсуляция хаттамалары, аралас желілер.

Keywords: Internet Protocol, IPv4, IPv6, encapsulation protocols, mixed network.

Введение. При сохранении существующих темпов роста Internet такие особенности протокола IPv4 как недостаточный объем адресного пространства и неэффективный способ распределения адресов, станут неминуемо сдерживать ее развитие. Большинство специалистов в области технологий Internet уверены в необходимости перехода на новую, шестую версию протокола IP. Косвенным свидетельством этому служит постоянно увеличивающееся число организаций, компаний-разработчиков сетевого оборудования и программного обеспечения, принимающих участие в Международном форуме IPv6. Вместе с тем, многие считают, что переходный период может затянуться на длительное, практически неограниченное время, в течение которого две версии протокола IP должны мирно сосуществовать. Поэтому способ перехода должен предусматривать сохранение совместимости новых узлов и сетей с доминирующим сейчас в Сети протоколом IPv4. Логика работы и форматы данных двух протоколов существенно отличаются, поэтому их совместимость должна обеспечиваться внешними по отношению к ним механизмами.

При правильном использовании механизмов перехода процесс смены версий протокола IP может оказаться не таким уж сложным, как это представляется сейчас.

Существующие механизмы. Взаимодействие систем, работающих с разными стеками протоколов, осуществляется обычно с использованием следующих методов:

– трансляция;

– мультиплексирование;

– инкапсуляция (туннелирование).

Трансляция обеспечивает согласование стеков протоколов путем преобразования форматов сообщений, а также отображения адресов узлов и сетей, различным образом трактуемых в этих протоколах. Транслирующий элемент, в качестве которого могут выступать, например, программный или аппаратный шлюз, мост, коммутатор или маршрутизатор, размещается между взаимодействующими сетями и служит посредником в их «диалоге».

Другой подход к согласованию протоколов получил название мультиплексирования стеков протоколов. Он заключается в том, что в сетевое оборудование или в операционные системы серверов и рабочих станций встраиваются несколько стеков протоколов. При их мультиплексировании на узлы сети устанавливается несколько стеков коммуникационных протоколов – по числу сетей с различающимися сетевыми протоколами. Для того чтобы запрос от прикладного процесса был правильно обработан и прошел через соответствующий стек, необходимо наличие специального программного элемента – мультиплексора протоколов, называемого также менеджером протоколов. Он должен определять, куда в какую конкретно сеть направлен запрос клиента.

Инкапсуляция или туннелирование – это еще один метод решения задачи согласования протоколов. Инкапсуляция может применяться, когда две сети с одной технологией необходимо соединить через транзитную сеть, где используется другая технология.

В процессе инкапсуляции принимают участие три типа протоколов:

– транспортируемый протокол;

– несущий протокол;

– протокол инкапсуляции.

Протокол объединяемых сетей является транспортируемым, а протокол транзитной сети – несущим. Пакеты транспортируемого протокола помещаются в поле данных пакетов несущего протокола с помощью протокола инкапсуляции. Пакеты-«пассажиры» никаким образом не обрабатываются при транспортировке их по транзитной сети. Инкапсуляцию выполняет пограничное устройство (как правило, маршрутизатор или шлюз), которое располагается на границе между исходной и транзитной сетями. Извлечение пакетов транспортируемого протокола из несущих пакетов выполняет второе пограничное устройство, которое находится на границе между транзитной сетью и сетью назначения. Пограничные устройства указывают в несущих пакетах свои адреса, а не адреса узлов в сети назначения.

Обычно инкапсуляция оказывается более простым и быстрым решением по сравнению с транс-ляцией, поскольку решает частную задачу, не обеспечивая взаимодействия узлов связываемых сетей с узлами транзитной сети.

В смешанных сетях IPv6–IPv4 наиболее часто используется мультиплексирование, а также туннелирование. Использование этих средств позволяет системам IPv6 обмениваться информацией с другими узлами IPv6 через сети IPv4. Для того чтобы узлы, поддерживающие только протокол IPv6, могли обращаться к ресурсам в сети IPv4, необходимо наличие дополнительных систем: шлюзов прикладного или транспортного уровня, трансляторов протоколов. Сейчас основные усилия разработчиков направлены на создание механизмов, позволяющих протоколу IPv6 беспрепятственно работать поверх сетей, поддерживающих только IPv4. Однако в будущем по-требуются средства, обеспечивающие передачу IPv4 через сети, где используюется исключительно IPv6, так как большинство систем в Internet перейдет на этот протокол.

Итак, для того чтобы вычислительные платформы работали в сетях IPv4 так же, как в IPv6, необходима одновременная поддержка и того, и другого стека. Расширенная версия интерфейса socket дает приложению возможность указать, каким адресом – IPv6 или IPv4 – оно желает воспользоваться для установления соединения. Если приложение выдает адрес IPv6, то операционная система будет создавать соединение по протоколу IPv6. Системы с двойным стеком могут принимать, отправлять и обрабатывать пакеты обоих протоколов. Соответственно, каждая из таких систем должна иметь как минимум по одному никак не связанных друг с другом адресу IPv4 и IPv6.

Поскольку шестнадцатибайтный адрес IPv6 запомнить сложнее, чем четырехбайтный IPv4, то роль службы DNS в сетях IPv6 становится еще более значимой. Стандарт DNS определяет новые типы записей о ресурсах для установления соответствия между именем системы и ее адресами в форматах IPv4 и IPv6. Какой из протоколов будет задействован для того или иного соединения, зависит от порядка записей, предоставляемых службой DNS приложению. Например, система может предоставлять только адрес IPv4, или только IPv6, или возвращать все имеющиеся в DNS адресные записи, относящиеся к запрошенному имени.

Доставка пакетов IPv6 конечным системам возможна при условии существования общей для этих систем инфраструктуры доставки. Поскольку сети, поддерживающие IPv6, составляют пока лишь малую часть всего Internet, будучи «островами» в «океане» IPv4, то для обеспечения соединений между ними широко применяется метод туннелирования. Несущим протоколом здесь является IPv4, а транспортируемым – IPv6. Пакет IPv6 помещается в поле данных пакета IPv4 и передается по обычной сети IPv4. По окончании передачи он извлекается из поля данных и обрабатывается обычным образом – т.е. либо отправляется в дальнейший путь (уже по сети IPv6), либо используется непосредственно получившей его системой. В общем случае полный маршрут пакета IPv6 может включать несколько туннелей через транзитные сети IPv4.

Минимальное значение максимального размера пакета, который может быть отправлен через интерфейс (Maximum Transmission Unit, MTU) для IPv6 составляет 1280 байт. Для того чтобы избежать излишней фрагментации, инкапсулирующая система должна, по возможности, использовать такое значение MTU для пакета IPv6, чтобы он помещался вместе со своим заголовком в разрешенном значении MTU для IPv4. Если размер присылаемого пакета IPv6 не позволяет разместить его целиком в поле данных пакета IPv4, инкапсулирующий узел может отправить узлу-источнику трафика IPv6 управляющее сообщение ICMPv6. При передаче трафика IPv6 через туннель в сети IPv4 протокол IPv4 играет роль канальной среды, поэтому, когда пакет проходит через туннель, счетчик транзитных узлов маршрута (hop counter) уменьшается на 1. Это делает туннель прозрачным на уровне IPv6, а для инструментов сетевой диагностики (например, traceroute) – невидимым.

При приеме пакета IPv4, несущего в поле данных пакет IPv6, система должна применить к нему стандартные методы фильтрации трафика по исходному адресу IPv4: пакет отбрасывается, если это особый адрес – для многоадресной или широковещательной рассылки, 0.0.0.0 или 127.x.x.x (loopback). Затем, отбросив инкапсулирующий заголовок IPv4, аналогичную фильтрацию необ-ходимо выполнить для адресов IPv6. К числу особых в протоколе IPv6 относятся адреса много-адресной рассылки, неопределенные адреса (unspecified address – 0.0.0.0/32 для IPv4 и ::/128 для IPv6), адреса обратной петли, а также особые адреса IPv4, полученные отображением на IPv6. Далее пакет передается стеку IPv6 и обрабатывается им как обычный пакет IPv6. Единственное исключение состоит в том, что узел не должен осуществлять дальнейшую маршрутизацию данного пакета, если только такая возможность не разрешена конфигурацией для адреса IPv4, с которого пришел пакет, т. е. если этот узел не сконфигурирован как конечная точка туннеля, начальной точкой которого является рассматриваемый адрес IPv4.

Поскольку начальная точка туннеля, осуществляющая инкапсуляцию пакетов IPv6 в пакеты IPv4, – это узел-отправитель по отношению к пакетам IPv4, она может получить сообщение протокола ICMP об ошибке, возникшей при передаче пакета IPv4 по сети. В некоторых случаях, в зависимости от типа сообщения, появляется необходимость передачи информации об ошибке узлу-отправителю вложенного пакета IPv6. Например, если сообщение ICMPv4 сигнализирует о превы-шении допустимого размера пакета, то система должна вести себя в соответствии со специфи-кацией определения максимального для маршрута IPv4 блока данных, который может быть отправ-лен по данному маршруту без фрагментации (Path MTU, PMTU). Т. е. необходимо зарегистри-ровать значение Path MTU для IPv4 и определить, следует ли генерировать информацию ICMPv6 о превышении размера пакета. Обработка других типов сообщений ICMPv4 зависит от того, какая часть пакета, вызвавшего ошибку, содержится в сообщении ICMP. В зависимости от реализации ICMP помимо внешнего заголовка IPv4 может быть передано либо 8, либо более начальных байт поля данных пакета, к которому относится это сообщение. Если оно содержит достаточно инфор-мации для реконструкции заголовка пакета IPv6, то инкапсулирующий узел может воспользоваться этими данными для составления сообщения ICMPv6 и отправки его узлу-источнику данного пакета IPv6.

Как подключиться к Интернету по IPv6. Если сетевой администратор реализует поддержку протокола IPv6 на всех конечных системах и маршрутизаторах, а собственного провайдера услуг IPv6 у организации нет, то единственным способом подключения к Internet по протоколу IPv6 является создание туннелей. Они могут быть проложены ко всем сетям, с которыми необходим обмен трафиком. Однако в типичном случае подключение производят к крупной магистральной сети IPv6; она и обеспечивает дальнейшую связь.

При выборе провайдера услуг Internet администратор сети IPv6 должен выполнить следующие действия:

– найти сеть, у которой был бы хороший канал связи с магистральными сетями IPv6 и владелец которой был бы готов предоставить сервис по транзиту трафика клиента IPv6;

– определить в этой сети наиболее эффективный маршрут для туннеля;

– заключить соглашение с администрацией выбранной сети относительно предоставления услуги туннелирования трафика IPv6;

– определить порядок обмена маршрутной информацией и технические параметры туннеля;

– проверить совместимость реализаций всех протоколов, планируемых для установки на марш-рутизаторах сетей клиента и провайдера, и при необходимости заменить имеющиеся продукты на совместимые.

ЛИТЕРАТУРА

1 Нэйэл Ричард Мэрфи, Дэвид Мэлоун. IPv6. Администрирование сетей. – КУДИЦ: Пресс, 2007. – 320 с.

2 Cisco Press. IPv6 для корпоративных сетей. – Вильямс, 2011. – 400 с.

3 www.ipv6forum.com

REFERENCES

1 Neyel Richard Murphy, David Malone. IPv6. Network administration. – KUDIC: Press, 2007. – 320 c.
2 Cisco Press. IPv6 for enterprise networks. – Williams, 2011. – 400 c.
3 www.ipv6forum.comCisco

Резюме

А. Ж. Тойғожинова

(Алматы энергетика және байланыс университеті, Алматы қ.)

ЖАҢА ҒАЛАМТОР – IPv6 ХАТТАМАСЫНА ӨТУ

Алдағы бірнеше жылда желі администраторлары Internet хаттамасының жаңа түріне ауыртпалықсыз өту жолдарын іздейтін болады. Ұсынылып отырған мақалада IPv4-тен IPv6-ға өту механизмдері, инкапсуляция хаттамалары, IPv6 хаттамасы арқылы ғаламторға қосылу әдісі сипатталады.

Кілт сөздер: ғаламтор хаттамасы, IPv4, IPv6, инкапсуляция хаттамалары, аралас желілер.

Summary

A. J. Toigojinova

(Almaty University of Power Engineering & Telecommunication, Almaty)

TRANSITION TO A NEW INTERNET – PROTOCOL IPv6

In the next few years, network administrators will have to find an answer to the question of how to move smoothly to the new version of the protocol Internet. This article describes the mechanisms of the transition from IPv4 to IPv6, protocol encapsulation method of connecting to the Internet via IPv6.

Keywords: Internet Protocol, IPv4, IPv6, encapsulation protocols, mixed network.

Поступила 27.02.2013 г.