Internet Engineering Task Force (IETF) W. Townsley
Request for Comments: 5969 O. Troan
Category: Standards Track Cisco
ISSN: 2070-1721 August 2010

Быстрое развертывание IPv6 на инфраструктурах IPv4 (6rd) - Спецификация протокола

IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification

Тезисы

В этом документе дана спецификация механизма автоматического туннелирования разработанного специально для ускорения развертывания IPv6 для конечных пользователей через сетевую инфраструктуру IPv4 сервис-провайдеров. Ключевые аспекты предлагаемого механизма включают автоматическое делегирование сайтам префиксов IPv6, работа без учета состояний, простота обеспечения и обслуживания, что обеспечивает эквивалент естественной реализации IPv6 на сайтах, использующих этот механизм.

Статус документа

Этот документ содержит проект стандарта Internet.

Документ является результатом работы IETF[1] и представляет согласованное мнение сообщества IETF. Документ был вынесен на открытое обсуждение и одобрен для публикации IESG[2]. Не все документы, одобренные IESG, претендуют на статус тех или иных стандартов Internet (см. раздел 2 документа RFC 5741).

Информация о статусе этого документа, обнаруженных ошибках и способах обратной связи доступна по ссылке http://www.rfc-editor.org/info/rfc5969.

Оглавление

1. Введение

Исходная идея и название механизма 6rd описаны в [RFC5569], где подробно рассмотрено коммерчески эффективное «быстрое развертывание» 6rd провайдерами домашних сетей. Рекомендуется прочесть упомянутый документ. В

[1]Internet Engineering Task Force.
[2]Internet Engineering Steering Group.

данном документе описан механизм 6rd, который был расширен для использования в средах общего назначения. В документе используется термин 6to4 для обозначения механизма, описанного в [RFC3056] и 6rd - для описанного здесь механизма.

6rd задает протокольный механизм развертывания IPv6 на сайтах через сети IPv4 сервис-провайдеров (SP[1]). Механизм базируется на 6to4 [RFC3056], а основное отличие состоит в использовании принадлежащего SP префикса IPv6 вместо префикса общего пользования (2002::/16). В результате использования операторского префикса IPv6 область действия 6rd ограничивается сетью SP и находится под его непосредственным контролем. С точки зрения пользовательских сайтов и сети IPv6 Internet в целом, обеспечиваемые услуги IPv6 эквивалентны естественному развертыванию IPv6.

Механизм 6rd основан на алгоритмическом отображении между адресами IPv6 и IPv4, выделенными для использования в сети SP. Это отображение обеспечивает возможность автоматического определения конечных точек туннеля IPv4 из префикса IPv6, позволяя 6rd работать без учета состояния соединений.

6rd рассматривает сеть IPv4, как канальный уровень для IPv6 и поддерживает абстракцию автоматического туннелирования, подобно модели NBMA[2] [RFC2491].

Домен 6rd состоит из краевых маршрутизаторов 6rd CE[3] и одного или нескольких граничных трансляторов 6rd BR[4]. Пакеты IPv6, инкапсулируемые 6rd следуют топологии маршрутизации IPv4 внутри сети SP между устройствами CE и BR. Через трансляторы 6rd BR проходят только пакеты IPv6, адресованные за пределы домена 6rd сервис-провайдера или приходящие в этот домен извне. Поскольку 6rd работает без учета состояния соединений, доступ к шлюзам BR можно обеспечить с использованием адресации anycast для отказоустойчивости и надежности (подобно [RFC3068]).

На «клиентской» (т. е. ЛВС) стороне CE реализация IPv6 осуществляется как для любого естественного сервиса IP, предоставляемого SP, и дальнейшее рассмотрение работы IPv6 на стороне ЛВС устройства CE выходит за пределы документа. На «операторской» (т. е. WAN) стороне 6rd CE сам интерфейс WAN, инкапсуляция в Ethernet, ATM или PPP, а также протоколы управления (PPPoE, IPCP, DHCP и т. п.) остаются неизменными (как они используются в текущей среде IPv4). Хотя технология 6rd была разработана в основном для поддержки развертывания IPv6 на клиентской стороне (например, в домовых сетях SP), она подходит и для отдельных хостов IPv6, действующих, как CE.

Механизм 6rd опирается на IPv4 и разработан для предоставления высококачественных услуг IPv6 через сеть IPv4 с минимальным изменением инфраструктуры и работы сети IPv4. Естественное развертывание IPv6 в сети SP может происходить независимо для решения внутренних задач SP, а доставка услуг IPv6 на сайты клиентов будет обеспечиваться 6rd. После того, как сеть SP будет полностью (доступ и транспорт) переведена на IPv6, использование 6rd может быть прекращено.

6rd использует такую же инкапсуляцию и базовый механизм, какие применяются в 6to4, и может рассматриваться, как надмножество 6to4 (6to4 можно получить, установив для 6rd префикс 2002::/16). В отличие от 6to4, механизм 6rd предназначен для использования только в средах, где сервис-провайдер управляет доставкой услуг IPv6. Маршруты 6to4 с префиксом 2002::/16 могут использоваться совместно с 6rd в маршрутизаторе 6rd CE и это может обеспечить некоторые преимущества при непосредственном взаимодействии с маршрутизаторами 6to4.

Канальная модель 6rd может быть расширена для поддержки групповой адресации IPv6. Вопрос поддержки групповой адресации IPv6 оставлен для рассмотрения в будущем.

Вопросы использования предлагаемого механизма, наряду с другими вопросами развертывания и эксплуатации выходят за пределы данного документа.

2. Язык описания требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

3. Терминология

6rd prefix - префикс 6rd

Префикс IPv6, выбранный сервис-провайдером для использования в домене 6rd. Для данного домена 6rd используется в точности один префикс 6rd. SP может реализовать 6rd на базе одного или множества доменов 6rd.

6rd Customer Edge (6rd CE) - краевой маршрутизатор

Устройство, функционирующее в качестве граничного маршрутизатора на стыке с клиентом в 6rd. В домовых широкополосных системах устройства такого типа иногда называют «домовыми шлюзами» (RG[5]) или оборудованием CPE[6]. Типичное устройство 6rd CE в домовом сайте имеет один интерфейс WAN, один или множество интерфейсов ЛВС и виртуальный интерфейс 6rd. В контексте 6rd устройства 6rd CE часто называют просто CE.

6rd delegated prefix - делегированный префикс 6rd

Префикс IPv6, рассчитанный устройством CE для использования на клиентской стороне, путем комбинирования префикса 6rd и адреса CE IPv4, полученного с помощью средств настройки конфигурации IPv4. Это префикс можно рассматривать, как логический эквивалент делегированного префикса DHCPv6 IPv6 [RFC3633].

6rd domain - домен 6rd

Множество устройств 6rd CE и BR, подключенных к одному виртуальному каналу 6rd. Сервис-провайдер может развернуть 6rd с одним или множеством доменов 6rd. Для каждого домена нужен отдельный префикс 6rd.

CE LAN side - сторона ЛВС

Функциональность устройства 6rd CE, используемая для обслуживания ЛВС или «клиентской» стороны CE. Интерфейс клиентской стороны CE полностью поддерживает IPv6.

[1]Service provider.
[2]Non-Broadcast Multiple Access - множественный доступ без широковещания.
[3]Customer Edge - граница с клиентами.
[4]Border Relay.
[5]Residential Gateway.
[6]Customer Premises Equipment.

CE WAN side - сторона WAN

Функциональность 6rd CE, используемая для обслуживания провайдерской или WAN-стороны CE. Интерфейс CE WAN поддерживает только IPv4.

6rd Border Relay (BR) - граничный транслятор 6rd

Поддерживающий 6rd маршрутизатор, управляемый сервис-провайдером и расположенный на краю домена 6rd. Маршрутизатор BR имеет по крайней мере по одному из перечисленных интерфейсов: IPv4, виртуальный интерфейс 6rd (конечная точка туннеля 6rd IPv6 в IPv4), IPv6, подключенный к сети IPv6. В контексте 6rd маршрутизатор 6rd BR может называться просто BR.

BR IPv4 address - адрес BR IPv4

Адрес IPv4 маршрутизатора 6rd BR для данного домена 6rd. Этот адрес используется устройствами CE для передачи маршрутизатору BR пакетов, адресованных получателям IPv6 за пределами домена 6rd.

6rd virtual interface - виртуальный интерфейс 6rd

Внутренний многоточечный туннельный интерфейс, на котором выполняется инкапсуляция и декапсуляция 6rd пакетов IPv6 в IPv4. Для типовой реализации CE или BR требуется только один виртуальный интерфейс 6rd. Маршрутизатору BR для работы во множестве доменов 6rd может потребоваться более одного виртуального интерфейса 6rd (но не более одного интерфейса на каждый домен 6rd).

CE IPv4 address - адрес CE IPv4

Адрес IPv4, выделенный устройству CE для обычного доступа IPv4 Internet (т. е., настроенный через DHCP, PPP и т. п.). Этот адрес может быть глобальным или приватным [RFC1918] в рамках домена 6rd. Адрес используется только устройством 6rd CE для создания делегируемого префикса 6rd, а также передачи и приема инкапсулированных в IPv4 пакетов IPv6.

4. Делегирование префиксов 6rd

Делегируемый префикс 6rd для использования на клиентской стороне создается путем комбинирования префикса 6rd и полного или частичного адреса CE IPv4. Из этих элементов делегируемый префикс 6rd автоматически создается маршрутизатором CE для клиентского сайта при обнаружении сервиса IPv4. Делегированный префикс 6rd используется точно так же, как префикс, полученный через делегирование DHCPv6 [RFC3633].

В 6to4 подобная операция выполняется за счет встраивания полного адреса IPv4 в фиксированную позицию общеизвестного префикса /16 IPv6. В 6rd префикс IPv6, позиция встраивания и число битов встраиваемого адреса IPv4 отличаются для разных доменов 6rd. Механизм 6rd позволяет оператору подстраивать размер префикса 6rd, число битов, используемых 6rd, и число битов, остающихся для делегирования сайтам клиентов. Для обеспечения возможности автоматической настройки конфигурации без учета состояния на стороне ЛВС **следует** использовать делегируемый префикс 6rd размером /64 или короче.

Делегируемый префикс 6rd создается путем конкатенации префикса 6rd и набора последовательных битов адреса CE IPv4 с сохранением их порядка. Размер делегируемого префикса 6rd равен сумме размеров префикса 6rd (n) и числа битов из адреса CE IPv4 (o).

На рисунке показан формат адреса IPv6 (параграф 2.5.4 в [RFC4291]) с префиксом 6rd и встроенным адресом CE IPv4.

```
|     n битов    |    o битов    |   m битов |    128-n-o-m битов      |
+----------------+---------------+-----------+-------------------------+
|  префикс 6rd   | адрес IPv4    | ID подсети|      ID интерфейса      |
+----------------+---------------+-----------+-------------------------+
|<-делегированный префикс 6rd->|
```

Рисунок 1

Если используется префикс 6rd размером /32 и 24 бита адреса CE IPv4 (например, все адреса CE IPv4 могут агрегироваться в 10.0.0.0/8), делегируемый префикс 6rd для каждого CE будет автоматически задан с размером /56 (32 + 24 = 56).

Встраивание в делегируемый префикс лишь части из 32 битов адреса CE IPv4 возможно только в тех случаях, когда для данного домена 6rd доступен агрегированный блок адресов IPv4. Это может оказаться непрактичным для глобальных адресов IPv4, но достаточно часто встречаются сети, где устройствам CE выделяются приватные адреса. Если приватные адреса перекрываются для данной инсталляции 6rd, можно организовать несколько доменов 6rd, вероятно с использованием такой же топологии линий, которая требуется для развертывания IPv4 на базе NAT. В этом случае для каждого домена используется свой префикс 6rd.

Каждый домен 6rd может использовать свое представление встроенных адресов IPv4 даже в рамках одного сервис-провайдера. Например, при использовании множества адресных блоков IPv4 с различными уровнями агрегирования число битов IPv4, требуемое для представление делегируемого префикса 6rd, может отличаться для каждого блока. В этом случае могут использоваться разные префиксы 6rd (и, следовательно, разные домены) для поддержки разного представления.

Поскольку делегируемый префикс 6rd выбирается алгоритмически на основе адреса IPv4, смена этого адреса будет приводить к изменению делегируемого префикса IPv6 и соответствующим негативным эффектам для клиентского сайта. Для предотвращения этого сервис-провайдерам рекомендуется выделять адреса CE IPv4 с достаточно большим сроком жизни.

Выделение адресов 6rd IPv6 и, следовательно, сам сервис IPv6 замыкаются на выделение (аренду) адресов IPv4; т. о, услуги 6rd также связаны с этим в плане проверки полномочий, учета использования услуг и т. п. Например, делегируемый префикс 6rd имеет такой же срок жизни, как и связанный с ним адрес IPv4. Время жизни префиксов, анонсируемое в Router Advertisement или используемое сервером DHCP на строне ЛВС устройства CE, **должно** быть не больше времени аренды адреса IPv4. Если время аренды адреса IPv4 не известно, в качестве времени жизни делегируемого префикса 6rd **следует** использовать принятое по умолчанию значение, заданное в [RFC4861].

5. Поиск неисправностей и трассировка

Адрес 6rd IPv6 и связанный с ним адрес IPv4 для данного клиента всегда можно определить алгоритмически со стороны сервис-провайдера, обслуживающего данный домен 6rd. Это может быть полезно при работе сервис-провайдера с системными журналами и другими данными в тех случаях, когда инструменты анализа данных более

приспособлены для IPv4, нежели для IPv6. Это позволяет также использовать мониторинг путей данных, узлов и конечных пользователей IPv4 для протокола IPv6.

Устройствам CE и BR в 6rd **следует** поддерживать адрес IPv6 Subnet-Router [RFC4291] для своего делегируемого префикса 6rd. Это позволит, например, виртуальному интерфейсу 6rd передавать сообщения IPv6 ICMP echo самому себе для поиска неисправностей в работе 6rd на данном CE или BR. В случае BR адрес IPv4, используемый для расчета делегируемого префикса 6rd, является заданным конфигурацией BR адресом IPv4.

6. Выбор адреса

Все адреса, выделяемые из делегированных префиксов 6rd, следует трактовать, как естественные адреса IPv6. Не требуется вносить какие-либо изменения в таблицу политики выбора адресов отправителей и получателей [RFC3484].

7. Конфигурация 6rd

Для данного домена 6rd устройства BR и CE **должны** быть настроенными с перечисленными ниже четырьмя элементами 6rd. Значения этих параметров 6rd идентичны для всех устройств CE и BR в данном домене 6rd.

IPv4MaskLen
: Число старших битов, которые совпадают для всех адресов CE IPv4 в данном домене 6rd. Например, при отсутствии идентичных битов IPv4MaskLen = 0 и для делегируемого префикса 6rd используется полный адрес CE IPv4. Если в адресах совпадает 8 битов (например, приватные адреса IPv4 из блока 10.0.0.0/8), IPv4MaskLen = 8 и восемь старших битов адреса IPv4 не используются при создании соответствующего делегируемого префикса 6rd.

6rdPrefix
: Префикс 6rd IPv6 для данного домена 6rd.

6rdPrefixLen
: Размер префикса 6rd IPv6 для данного домена 6rd.

6rdBRIPv4Address
: Адрес IPv4 маршрутизатора 6rd BR для данного домена 6rd.

7.1. Конфигурация на клиентской стороне

Для четырех элементов 6rd устанавливаются одинаковые значение на всех CE в домене 6rd. Эти значения могут быть заданы разными способами, включая такие, как интерфейс управления домовыми шлюзами TR-69 [TR069], объект на базе XML, получаемый после организации соединения IPv4, запись DNS, SMIv2 MIB [RFC2578], PPP IPCP или настройка администратором вручную. В этом документе описана настройка требуемых конфигурационных параметров с использованием DHCP. Устройствам CE, которые позволяют настраивать конфигурацию IPv4 по протоколу DHCP, **следует** поддерживать этот вариант. Для других вариантов настройки и управления могут использоваться форматы, описанные для этого варианта, в целях совместимости и удобства реализации на CE, поддерживающих разные опции настройки конфигурации.

Единственной недостающей информацией, которая требуется CE для расчета делегируемых префиксов 6rd и обеспечения связности IPv6, является адрес IPv4 для CE. Этот адрес CE IPv4 задается в процессе получения доступа IPv4 в Internet (т. е. через DHCP, PPP или иным способом). Адрес может быть глобальным или приватным [RFC1918] в домене 6rd.

Одно устройство 6rd CE **может** быть подключено к множеству доменов 6rd просто, как любой маршрутизатор может быть подключен к множеству сервис-провайдеров IPv6 и иметь множество делегированных префиксов, полученных через DHCPv6 или иным способом. Каждый домен данного CE будет требовать своего набора конфигурационных элементов 6rd и будет генерировать свой делегируемый префикс 6rd.

7.1.1. Опция 6rd DHCPv4

option-code
: OPTION_6RD (212)

option-length
: Размер опции DHCP в октетах (22 октета с одним адресом BR IPv4).

IPv4MaskLen
: Число старших битов адреса, совпадающих на всех интерфейсах CE IPv4 в данном домене 6rd. Это поле может принимать значения от 0 до 32. Все значения, превышающие 32, являются некорректными.

6rdPrefixLen
: Размер префикса IPv6 (SP 6rd IPv6) в битах. В целях контроля границ октетов при обработке опции DHCP сумма (32 - IPv4MaskLen) + 6rdPrefixLen **должна** иметь значение не более 128.

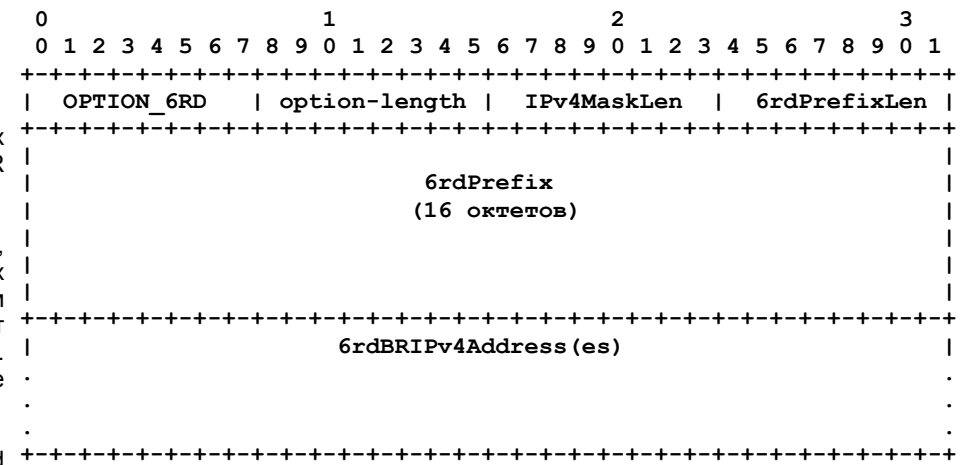

Рисунок 2

6rdBRIPv4Address
: Один или множество адресов IPv4 маршрутизатора(ов) 6rd BR данного домена 6rd.

6rdPrefix
: Принадлежащий провайдеру префикс 6rd IPv6, представленный в форме 16-октетного адреса IPv6. Биты префикса после 6rdPrefixlen являются резервными и **должны** устанавливаться в 0 отправителем и игнорироваться получателем.

Маршрутизатор CE **должен** включать опцию Parameter Request List Option [RFC2132] для OPTION_6RD. Поскольку OPTION_6RD содержит один блок IPv4MaskLen/6rdPrefixLen/6rdPrefix, а DHCP не может передавать более одного

экземпляра опции, OPTION_6RD предоставляется не более, чем одному домену 6rd. Предоставление опции маршрутизатором CE, подключенным к множеству доменов 6rd, выходит за пределы спецификации протокола.

Наличие опции DHCP OPTION_6RD служит индикацией доступности сервиса 6rd. По умолчанию получение корректной опции 6rd DHCP поддерживающим 6rd маршрутизатором CE приводит к настройке виртуального интерфейса 6rd и делегированию префикса для использования на стороне ЛВС устройства CE. Маршрутизатор CE **должен** иметь конфигурационную опцию отключения механизма 6rd; в этом случае принятые опции 6rd DHCP просто игнорируются.

Подробное рассмотрение поведения CE с использованием множества адресов BR IPv4 оставлено на будущее. В таких случаях CE **должен** по крайней мере один адрес BR IPv4 и **может** поддерживать множество адресов.

При включенном 6rd типичный маршрутизатор CE будет устанавливать маршрут по умолчанию к BR, «черную дыру» (black hole route) для делегированного префикса 6rd и маршруты для любой стороны ЛВС, получившей и анонсирующей префикс. Рассмотрим пример, где CE использует адрес IPv4 10.100.100.1, BR - 10.0.0.1, IPv4MaskLen = 8, 2001:db8::/32 служит префиксом 6rdPrefix, а для стороны ЛВС выделен префикс /64. Таблица маршрутизации типичного CE будет иметь вид:

```
::/0 -> 6rd-virtual-int0 via 2001:db8:0:100:: (маршрут по умолчанию)
2001:db8::/32 -> 6rd-virtual-int0 (прямое подключение к 6rd)
2001:db8:6464:100::/56 -> Null0 (null-маршрут к делегированному префиксу)
2001:db8:6464:100::/64 -> Ethernet0 (интерфейс ЛВС)
```

7.2. Конфигурация граничного транслятора

Маршрутизатор 6rd BR **должен** настраиваться с такими же элементами конфигурации 6rd, как устройства 6rd CE в том же домене.

Для повышения надежности и балансирования нагрузки в качестве адреса BR IPv4 может использоваться адрес anycast, совместно используемый в данном домене 6rd. Поскольку 6rd не учитывает состояния соединений, в любой момент можно работать с любым из маршрутизаторов BR. Если BR использует anycast-адрес IPv4, он **должен** устанавливать этот адрес IPv4 в поле отправителя пакетов, транслируемых маршрутизаторам CE.

Поскольку в 6rd используется адресное пространство провайдера, для работы 6rd не требуется анонсировать специфические маршруты за пределы домена ни для IPv6, ни для IPv4 BGP. Однако при использовании для трансляторов 6rd IPv4 адресов anycast эти адреса должны анонсироваться в IGP[1] провайдера.

8. Детектирование недоступности соседа

Механизм детектирования отсутствия соседа (NUD[2]) для туннелей описан в параграфе 3.8 документа [RFC4213]. В 6rd все маршрутизаторы CE и BR можно рассматривать, как подключенные к одному виртуальному каналу и, следовательно, все они являются соседями один другому. В этом параграфе описан механизм детектирования недоступности соседа, не оказывающий негативного влияния на масштабируемость 6rd.

Типовая реализация 6rd может содержать очень большое число маршрутизаторов CE в одном домене. Связность между CE основана на маршрутизации IPv4 и передача NUD или других периодически повторяемых пакетов между устройствами 6rd CE за исключением случаев поиска неисправностей 6rd **не рекомендуется**.

Хотя детектирование доступности между данным 6rd CE и BR не требуется для корректной работы 6rd, в случаях, когда CE имеет множество путей для достижения BR, такое детектирование может быть полезным. Передача сообщений NUD маршрутизатору BR, повторяемая периодически очень большим числом маршрутизаторов CE, может вызвать перегрузку системы обработки управляющих сообщений в BR и это оказывает негативное влияние на масштабируемость 6rd. Вместо этого CE, которому нужно проверить доступность BR, **должен** использовать метод, который позволяет пакетам детектирования доступности следовать по обычному пути пересылки данных без специальной обработки на BR. Один из таких методов описан ниже.

1. CE создает произвольные данные любого размера для передачи BR (например, пустой блок данных размером 0, блок заполненный произвольными данными для тестирования MTU, сообщение NUD и т. п.). Формат данных сообщения не имеет никакого значения, поскольку BR не будет обрабатывать эти данные.
2. Данные инкапсулируются в пакет с внутренним заголовком IPv6 и внешним заголовком IPv4:
   - в качестве адреса получателя IPv6 указывается адрес из делегированного префикса 6rd, который связан с виртуальным интерфейсом CE;
   - в качестве адреса отправителя IPv6 устанавливается адрес из делегированного префикса 6rd (можно тот же, который указан в качестве адреса отправителя IPv6);
   - заголовок IPv4 добавляется обычным путем, как для любого пакета, адресованного BR (т. е. в качестве адреса получателя IPv4 указывается адрес BR, а в качестве адреса отправителя - CE IPv4).
3. CE передает подготовленный пакет через интерфейс, для которого проверяется доступность BR. При получении пакета маршрутизатор BR **должен** декапсулировать его и переслать обычным способом. Заголовок IPv4 декапсулируется, как обычно, показывая, что IPv6-адресатом пакета является CE, что приводит в результате к пересылке пакета этому CE с использованием механизма 6rd (т. е., адресатом получателя IPv4 будет CE, создавший пакет, отправителем IPv4 - маршрутизатор BR).
4. Прибытие сконструированного для проверки пакета IPv6 по адресу CE IPv6 завершает круговой обход до BR и обратно, а маршрутизатор BR не выполняет никаких операций по обработке тестового пакета, сверх его обычной пересылки. CE обрабатывает пакет IPv6 подобающим образом (обновляет таймер keepalive, метрику и т. п.).

[1]Протокол внутренней маршрутизации.
[2]Neighbor Unreachability Detection.

Поле данных пакета может быть пустым или содержать значения, имеющие смысл для CE. Для некоторых реализаций может оказаться удобной передача сообщений NUD (отметим, что BR будет уменьшать значение поля IPv6 hop limit). Поскольку BR пересылает тестовый пакет, как обычный пакет данных без специальной обработки содержащихся в нем данных, выбор формата данных пакета остается за разработчиком.

9. Инкапсуляция IPv6 в IPv4

Действия, выполняемые при инкапсуляции IPv6 в IPv4 и пересылке (например, обработка маркеров пакета, подсчет контрольных сумм и т. п.) выполняются в соответствии с параграфом 3.5 документа [RFC4213] и совпадают с операциями, используемыми 6to4 [RFC3056]. Сообщения об ошибках ICMPv4 обрабатываются в соответствии с параграфом Section 3.4 [RFC4213]. По умолчанию поле IPv6 Traffic Class **должно** копироваться в поле IPv4 ToS[1]. Такое поведение **может** быть изменено конфигурационными параметрами. В документах [RFC2983] и [RFC3168] приведена дополнительная информация, относящаяся к дифференцированным услугам IP и туннелированию.

Пакеты IPv6 от CE инкапсулируются в пакеты IPv4, когда они покидают сайте через интерфейс CE WAN. Для передачи и приема пакетов через этот интерфейс на CE **должен** адрес IPv4.

Канал 6rd моделируется, как канал NBMA, подобно другим механизмам автоматического туннелирования IPv6 в IPv4 типа [RFC5214] и все устройства 6rd CE и BR определяются как соседи. Адрес link-local виртуального интерфейса 6rd, выполняющего инкапсуляцию 6rd будет (при необходимости, формироваться, как описано в параграфе 3.7 [RFC4213]. Однако обмена данными с использованием адреса link-local происходить не будет.

9.1. MTU

MTU[2] и фрагментация для инкапсуляции IPv6 в IPv4 подробно рассмотрены в параграфе 3.2 RFC 4213 [RFC4213]. Область действия 6rd ограничена сетью сервис-провайдера. При выборе значения MTU для туннеля **можно** использовать механизм IPv4 Path MTU, как описано в параграфе 3.2.2 RFC 4213 [RFC4213] или явно задать значение 6rd Tunnel MTU в параметрах конфигурации.

Использование в качестве адреса отправителя anycast-адреса может приводить к тому, что сообщения ICMP об ошибках, генерируемые на пути, будут передаваться разным BR. Следовательно, использование динамического значения MTU для туннеля в соответствии с параграфом 3.2.2 [RFC4213] может приводить к «черным дырам» IPv4 Path MTU.

Множество маршрутизаторов BR, использующих один anycast-адрес отправителя, могут передавать одновременно фрагменты пакетов одному устройству IPv6 CE. Если в пакетах от разных BR окажется одинаковый номер фрагмента, при сборке могут возникнуть ошибки. По этой причине BR, использующие anycast-адрес отправителя **должны** устанавливать флаг IPv4 Don't Fragment.

Если управление MTU организовано так, что значение IPv4 MTU на интерфейсе CE WAN обеспечивает предотвращение фрагментации в рамках сети SP, для 6rd Tunnel MTU следует установить значение IPv4 MTU за вычетом размера инкапсулирующего заголовка IPv4 (20 байтов). Например, если IPv4 MTU = 1500 байтов, для 6rd Tunnel MTU может быть установлено значение 1480 байтов. При отсутствии информации для установки 6rd Tunnel MTU **следует** использовать принятое по умолчанию значение 1280 байтов.

9.2. Правила приема

Для предотвращения использования обманных адресов IPv6 (spoofing) устройства 6rd BR и CE **должны** MUST сравнивать адрес отправителя IPv4 инкапсулированных пакетов IPv6 с адресом отправителя IPv4, заданным в конфигурации домена 6rd. Если адреса отправителей не совпадают, пакет **должен** быть отброшен с увеличеснием значения счетчика для индикации потенциальной атаки с подменой адресов. Кроме того, маршрутизатор CE **должен** разрешать пересылку пакетов, исходящих с заданного конфигурацией адреса.

По умолчанию маршрутизатор CE **должен** отбрасывать пакеты, полученные на виртуальном интерфейсе 6rd (т. е., после декапсуляции IPv4) для получателей IPv6, не относящихся к своему делегированному префиксу 6rd.

10. Процесс перехода на IPv6

Сеть SP может перейти на IPv6 в своем темпе, практически не оказывая воздействия на клиентов, получающих услуги IPv6 через 6rd. После организации естественной связности IPv6 администратор может отключить 6rd.

SP может выбрать отдельный блок адресов IPv6 для естественного сервиса или использовать для этого префикс 6rd. При использовании отдельного блока переход с 6rd на естественную реализацию IPv6 будет выглядеть для клиентов просто, как смена адресов IPv6. Замены адресов можно избежать за счет вставки делегируемого префикса 6rd в домен маршрутизации IPv6 сервис-провайдера. Дальнейшее рассмотрение вопросов перехода от 6rd к естественному развертыванию IPv6 выходит за рамки спецификации данного протокола.

11. Использование адресного пространства IPv6

6rd использует адресное пространство сервис-провайдера, которое тот получает от регионального регистратора (RIR[3]), и для работы 6rd не требуется запрашивать у IANA выделение глобального блока адресов типа 6to4 2002::/16.

Префикс сервис-провайдера должен быть достаточно коротким для представления уникальных битов всех адресов IPv4 в данном домене 6rd и достаточно длинным для предоставления адресов IPv6 всем клиентам в жилых зонах. В самом худшем случае использования всех 32 битов адреса IPv4 и в предположении выделения префикса /56 для пользовательских сайтов, каждому сервис-провайдеру, использующему 6rd, будет требоваться блок /24 для 6rd в дополнение к другим блокам адресов IPv6. Предполагая, что развертывание 6rd будет весьма успешным и произойдет

[1]Type of Service - тип обслуживания.
[2]Maximum transmission unit - максимальный передаваемый блок.
[3]Regional Internet Registry.

почти во всех автономных системах (AS[1]), число владельцев которых составляет сегодня примерно 32K, общий размер адресного блока для 6rd можно оценить в /9. Если SP будет делегировать сайтам префиксы /60, ему потребуется блок размером /28, а общий расход адресов для 6rd будет эквивалентен размеру блока /13. Отметим, что эти оценки основаны на предположении о том, что 6rd используется одновременно всеми владельцами AS в современной сети IPv4 Internet никто из них не использует методов компрессии адресов 6rd и никто не использует естественное развертывание IPv6, а для 6rd не выделяется адресное пространство, использованное ранее для других целей.

Для смягчения проблемы использования адресного пространства 6rd позволяет оставить избыточные биты префикса IPv4 при представлении адреса IPv4 внутри адреса 6rd IPv6. Наиболее полезно это в тех случаях, когда адресное пространство IPv4 очень хорошо агрегировано. Например, для обеспечения каждого клиента префиксом /60 при условии, что все клиенты IPv4 адресуются префиксом /12 для представления адреса IPv4 требуется только 20 битов и сервис-провайдеру будет достаточно префикса /40 IPv6 для 6rd. Если используется приватное адресное пространство, для блока 10/8 потребуется префикс /36. При использовании множества доменов 10/8 до 16 таких доменов можно поддерживать в /32.

Если сервис-провайдер имеет неагрегируемое пространство адресов IPv4 и требуется использовать все 32 бита адреса IPv4 при кодировании адресов 6rd IPv6, префикс 6rd **должен** иметь размер не более /32 для того, чтобы предлагать делегируемый префикс 6rd размером, по крайней мере, /64.

Адресный блок 6rd можно использовать для других целей после перехода всех пользователей на естественный сервис IPv6. Это может потребовать смены адресов на сайтах клиентов и выделения дополнительного адресного пространства на переходный период.

12. Вопросы безопасности

Транслирующий маршрутизатор 6to4, как отмечено в [RFC3056], может быть использован в качестве открытого транслятора для анонимизации и трансляции трафика IPv6. Ограничение домена 6rd сетью провайдера приводит к тому, что CE может принимать пакеты лишь от одного или немногих известных ему адресов IPv4 устройств 6rd BR. По этой причине многие из угроз для 6to4, описанных в [RFC3964], не применимы к 6rd.

При реализации правил приема, описанных в параграфе 9.2, пакеты IPv6 защищены от подмены адресов, если пакеты IPv4 приходят из сети SP или от других маршрутизаторов CE в домене 6rd[2].

Злоумышленник, осведомленный о домене 6rd и адресе BR IPv4, может использовать эту информацию для создания пакетов, которые будут заставлять транслятор BR отражать туннелированные пакеты за пределы обслуживаемого им домена. Если атакующий создаст пакеты должным образом и сможет вставить пакет с адресовм отправителя IPv6, который выглядит, как исходящий из другого домена 6rd, может возникнуть циклическая пересылка пакетов (петля) между парой доменов 6rd, позволяющая злоумышленнику реализовать атаку packet amplification между двумя доменами [RoutingLoop].

Одним из способов предотвращения такой угрозы является закрытие доступа по адресу BR IPv4 извне (не из домена 6rd данного SP). В этом случае специально подготовленные пакеты IPv6 будут по-прежнему отражаться маршрутизатором BR, но циклической пересылки не возникнет. Можно также отфильтровывать туннелированные пакеты с адресом BR IPv4 в поле отправителя для предотвращения туннелей, выходящих из домена 6rd.

Для предотвращения циклической пересылки через другие внутренние трансляторы на маршрутизаторе BR следует использовать фильтрацию входящих и исходящих пакетов IPv4, отбрасывая пакеты с известными адресами внутренних 6rd BR, маршрутизаторов ISATAP и трансляторов 6to4, а также общеизвестными адресами anycast пространства 6to4.

Другой вариант предотвращения петель описан в работе [V6OPS-LOOPS].

Маршрутизатор BR **должен** организовать null-маршрут [RFC4632] для своего делегируемого префикса 6rd, созданного на основе адреса BR IPv4, с исключением адреса IPv6 Subnet-Router anycast.

13. Согласование с IANA

Агентство IANA выделило новый код опции DHCP для OPTION_6RD (212) с размером данных 18 + N (OPTION_6RD с адресами N/4 6rd BR).

14. Благодарности

Этот документ основан на идее Remi Despres, описанной в [RFC5569], и работе, выполненной Rani Assaf, Alexandre Cassen, и Maxime Bizon в компании Free Telecom. Brian Carpenter и Keith Moore документировали механизм 6to4, на котором основан данный протокол. Мы благодарим Fred Templin за его комментарии и предложения, а также его опыт работы с ISATAP. Комментарии и предложения предоставили также многие другие люди, особенно следует отметить Chris Chase, Thomas Clausen, Wouter Cloetens, Wojciech Dec, Bruno Decraene, Remi Despres, Alain Durand, Washam Fan, Martin Gysi, David Harrington, Jerry Huang, Peter McCann, Alexey Melnikov, Dave Thaler, Eric Voit и David Ward.

15. Литература

15.1. Нормативные документы

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[1]Autonomous System.

[2]В исходном документе указано, что от спуфинга защищены только пакеты, находящиеся в сети SP. Это признано ошибочным и в текст добавлено упоминание других CE того же домена. См. http://www.rfc-editor.org/errata_search.php?eid=3049. *Прим. перев.*

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2491] Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, January 1999.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

15.2. Дополнительная литература

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2983] Black, D., "Differentiated Services and Tunnels", RFC 2983, October 2000.

[RFC3068] Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, June 2001.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC3964] Savola, P. and C. Patel, "Security Considerations for 6to4", RFC 3964, December 2004.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

[RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.

[RFC5569] Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, January 2010.

[RoutingLoop] Nakibly and Arov, "Routing Loop Attacks using IPv6 Tunnels", August 2009, <http://www.usenix.org/event/woot09/tech/full_papers/nakibly.pdf>.

[TR069] "TR-069, CPE WAN Management Protocol v1.1, Version: Issue 1 Amendment 2", December 2007.

[V6OPS-LOOPS] Nakibly, G. and F. Templin, "Routing Loop Attack using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", Work in Progress, May 2010.

Адреса авторов

Mark Townsley

Cisco

Paris,

France

EMail: mark@townsley.net

Ole Troan

Cisco

Bergen,

Norway

EMail: ot@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com