Internet Engineering Task Force (IETF)
Request for Comments: 6264
Category: Informational
ISSN: 2070-1721

S. Jiang
D. Guo
Huawei
B. Carpenter
University of Auckland

June 2011

Инкрементная модель CGN для перехода на IPv6

An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition

Тезисы

Глобальное развертывание IPv6 оказалось значительно более медленным, нежели предполагалось. По мере исчерпания адресов IPv4 вопросы перехода с IPv4 на IPv6 становятся все более важными и решаются сложнее. Механизмы перехода на уровне хостов, использующие среду с двумя стеками протоколов, не могут удовлетворить все требования. Большинство конечных пользователей не имеет опыта, требуемого для настройки и поддержки таких механизмов. Устройства CGN[1] со встроенными механизмами перехода могут снизить операционные издержки в период перехода с IPv4 на IPv6 и совместного использования обоих протоколов.

В этом документе предлагается инкрементная модель CGN для перехода на IPv6. Эта модель позволяет обеспечить услуги доступа к IPv6 для хостов IPv6 и услуги доступа к IPv4 для хостов IPv4, обеспечивая существующим ISP возможность не менять свою сетевую инфраструктуру на начальном этапе перехода от IPv4 к IPv6. В отличие от CGN, как таковой, инкрементная модель CGN также поддерживает плавный переход (и способствует ему) к сетям ISP[2] с двумя стеками протоколов или только IPv6. Описаны интегрируемое настраиваемое устройство CGN и адаптивный домашний шлюз (HG[3]). Оба типа устройств могут использоваться на разных стадиях перехода, что избавляет от необходимости многократного обновления устройств. Такое решение позволяет постепенно переходить на IPv6 в соответствии с реальными потребностями пользователей.

Статус документа

Этот документ не является спецификацией проекта стандарта Internet и публикуется с информационными целями.

Документ является результатом работы IETF[4] и представляет согласованное мнение сообщества IETF. Документ был вынесен на открытое обсуждение и одобрен для публикации IESG[5]. 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/rfc6264.

Оглавление

[1]Carrier-Grade NAT - система трансляции сетевых адресов в масштабе оператора.
[2]Internet Service Provider. *Прим. перев.*
[3]Home gateway.
[4]Internet Engineering Task Force.
[5]Internet Engineering Steering Group.

1. Введение

Глобального перехода на Ipv6, как прогнозировалось 10 лет назад, не произошло. Сетевые операторы не решились сделать первый шаг, поскольку IPv4 работал и продолжает работать хорошо. Однако полное истощение адресов IPv4 неизбежно. Этот вопрос анализируется в динамически обновляемом документе IPv4 Address Report[1] [IPUSAGE]. Пул нераспределенных адресов IANA закончился в феврале 2011 года и на момент публикации данного документа указанный сайт предсказывал неизбежное истощение адресных пулов региональных регистраторов (RIR[2]). С учетом этих обстоятельств похоже, что индустрия Internet достигла согласия по вопросу неизбежности глобального развертывания IPv6 и необходимости сделать это как можно скорее.

В связи с этим вопросы перехода с IPv4 на IPv6 становятся более важными и усложняются необходимостью глобального развертывания IPv6. Механизмы перехода на уровне хостов сами по себе не способны выполнить все требования для перехода. Следовательно, требуются функции поддержки на уровне сетей и/или новые механизмы перехода, обеспечивающие простоту операций на пользовательской стороне.

Системы трансляции адресов на уровне оператора (CGN[3]) [CGN-REQS], которые называют также NAT444 CGN и Large Scale NAT, позволяют решить эксплуатационные проблемы IPv4, но никак не способствуют переходу с IPv4 на IPv6. Развертывание NAT444 CGN позволяет ISP отложить переход и, следовательно, вдвое повышает расходы, связанные с переходом (сначала на добавление CGN, а потом на поддержку IPv6).

Реализации CGN, интегрирующие множество механизмов перехода, могут упростить операции по обслуживанию конечных пользователей в процессе перехода с IPv4 на IPv6 и в период сосуществования протоколов. Системы CGN развертываются на строне сети и управляются/поддерживаются профессионалами. На пользовательской стороне могут потребоваться домашние шлюзы (HG). Эти устройства могут предоставляться пользователям операторами в зависимости от конкретных бизнес-моделей. Упрощенные устройства с двумя стеками протоколов (DS-Lite[4]) [DS-LITE] представляют собой основанное на CGN решение, которое поддерживает переход, но требуют от ISP незамедлительно перевести свою сеть на IPv6. Многие ISP не решаются сделать этот первый шаг. Теоретически устройства DS-Lite можно использовать с двойной инкапсуляцией (IPv4-in-IPv6-in-IPv4), но такое решение вряд ли будет принято ISP и не рассматривается в этом документе.

Данный документ предлагает инкрементную модель CGN для перехода на IPv6. В документе не определяются новые протоколы или механизмы, но описано использование комбинации имеющихся предложений для постепенного перехода. Модель похожа на DS-Lite, но работает иначе. Она, прежде всего, объединяет функции трансляции v4-v4 NAT с туннелированием v6-over-v4. Эта модель позволяет обеспечить услуги доступа IPv6 для хостов, поддерживающих IPv6 и услуги IPv4 для хостов IPv4 без изменения инфраструктуры IPv4 сервис-провайдера (ISP). Развертывание этой технологии не оказывает никакого влияния на унаследованные хосты IPv4 с глобально доступными адресами IPv4. Технология подходит для начальной стадии перехода с IPv4 на IPv6. Она также поддерживает переход к сетям ISP с двумя стеками протоколов и сетям, использующим только IPv6.

В документе описан также механизм постепенного перехода. Этот механизм использует интегрируемые и настраиваемые устройства CGN, а также адаптивные устройства HG. Оба типа устройств (CGN и HG) могут использоваться на разных стадиях перехода и не потребуют замены. Это позволяет переходить на IPv6 постепенно в соответствии с реальными потребностями пользователей.

2. Инкрементная модель CGN

Сегодня большинство пользователей работает с адресами IPv4. Сервис-провайдеры начинают предоставлять услуги доступа IPv6 конечным пользователям. На начальном этапе перехода от IPv4 к IPv6 связность и трафик IPv4 будут сохранять свое присутствие (и преобладание) в сетях большинства ISP. Сервис-провайдеры хотят минимизировать изменения в своих сетях IPv4. Переход всей сети ISP на использование только IPv6 будет рассматриваться, как радикальная стратегия. Переход всей сети ISP на использование двух протоколов не столь радикален, но усложняет сеть и требует дополнительных расходов. Хотя некоторые ISP успешно развернули сети с двумя протоколами, остальные предпочитают не делать этого в качестве первого этапа своего перехода на IPv6. Однако в настоящее время требуется достаточно срочно решать две проблемы - преодоление текущего дефицита адресов IPv4 путем развертывания того или иного механизма совместного использования адресов и подготовки к активному использованию адресного пространства и услуг IPv6. ISP решают одну из двух проблем путем адаптации CGN (для преодоления дефицита адресов IPv4) или 6rd (для предоставления услуг подключения по IPv6). Описанная здесь модель предназначена для решения обеих проблем за счет комбинирования технологий v4-v4 CGN и туннелирования v6-over-v4.

2.1. Обзор инкрементной модели CGN

Инкрементная модель CGN, предлагаемая здесь, схематически показана на рисунке 1.

Как показано на рисунке 1, ISP не требуется существенно менять свою сеть IPv4. Эта модель обеспечивает хостам IPv4 доступ в сеть IPv4 Internet, а хостам IPv6 - доступ в сеть IPv6 Internet. Хосты с двумя стеками протоколов трактуются, как хосты IPv4, при использовании ими услуг доступа IPv4 и, как хосты Ipv6, при использовании услуг доступа IPv6. Для обеспечения хостам IPv4 возможности доступа в сеть IPv6 Internet, а хостам IPv6 - в сеть IPv4 Internet можно интегрировать NAT64 с CGN (более подробное описание взаимодействия IPv4/IPv6 приведено в параграфе 2.6). Рассмотрение интеграции таких механизмов выходит за пределы этого документа.

В рассматриваемой модели нужны два типа устройств: домашние шлюзы с двумя стеками протоколов (HG) и устройства CGN с двумя стеками. Домашние шлюзы с двумя стеками протоколов интегрируют пересылку для протоколов IPv6 и IPv4 с функциями туннелирования v6-over-v4. Такие устройства следует выполнять в соответствии с

[1]Отчет об адресах IPv4.
[2]Regional Internet Registry.
[3]Carrier-Grade NAT.
[4]Dual-stack lite.

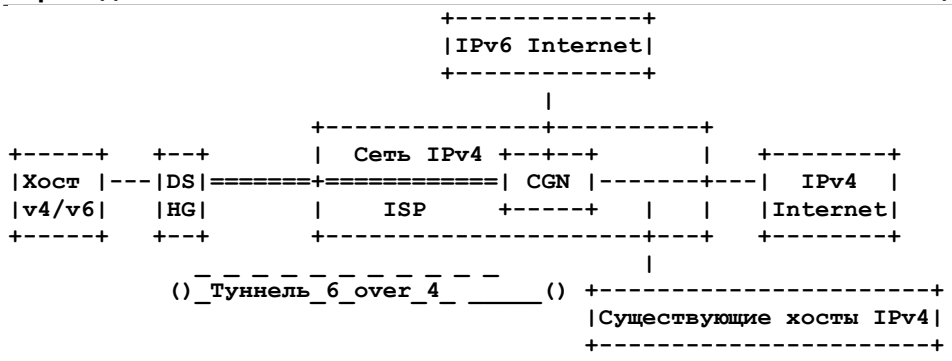

Рисунок 1 Инкрементная модель CGN для сети IPv4 Internet-провайдера
DS HG - домашний шлюз с двумя протоколами (CPE - оборудование на стороне пользователя).

требованиями [RFC6204], включая делегирование префиксов IPv6. Они могут также поддерживать функциональность v4-v4 NAT. Устройства CGN с двумя стеками протоколов интегрируют функции туннелирования v6-over-v4 и v4-v4 CGN, а также стандартную маршрутизацию IPv6 и IPv4.

Модель не требует использования новых механизмов пересылки пакетов IP, а также инкапсуляции и декапсуляции в конечных точках туннелей. В последующих параграфах описано взаимодействие HG с инкрементным CGN.

2.2. Выбор технологии туннелирования

В принципе, эта модель будет работать с любой формой туннеля между HG с двойным стеком и CGN с двойным стеком. Однако туннели, требующие явной настройки, очевидно будут нежелательны ввиду связанных с ними операционных расходов. Следовательно, настраиваемые туннели [RFC4213] не подойдут. Туннельный брокер [RFC3053] также требует операционных расходов и будет нежелателен для домашних пользователей.

Технология 6rd [RFC5569, RFC5969] представляется подходящим решением для поддержки туннелей v6-over-v4 с низкими операционными расходами. Инкапсуляция GRE[1] [RFC2784] с дополнительным механизмом автоматической настройки конфигурации также подходит для поддержки туннелей v6-over-v4. Могут рассматриваться и другие механизмы туннелирования типа 6over4 [RFC2529], 6to4 [RFC3056], ISATAP[2] [RFC5214] или VET[3] [RFC5558]. Если ISP имеет полнофункциональную инфраструктуру MPLS между HG и CGN с двойным стеком, можно использовать также туннели 6PE[4] [RFC4798] непосредственно в MPLS. Однако это решение подойдет только для устройств HG с расширенными функциями, которые сложно отнести к числу потребительских устройств, поэтому оно не будет рассматриваться подробно. Для простоты предположим использование туннелей 6rd.

2.3. Поведение шлюза с двумя стеками протоколов

Когда домашний шлюз с двойным стеком протоколов принимает пакет от хоста, он будет квалифицировать этот пакет, как IPv4 или IPv6. Принятый пакет в зависимости от результата определения будет обрабатываться стеком IPv4 или IPv6. Для IPv4 при отсутствии на шлюзе HG трансляции адресов v4-v4 NAT стек будет просто пересылать пакет устройству CGN, в качестве которого в общем случае будет служить используемый по умолчанию маршрутизатор IPv4. Если на шлюзе включена трансляция v4-v4 NAT, HG изменит в заголовке пакета адрес отправителя с приватного адреса IPv4 в зоне действия HG на адрес IPv4 в зоне действия CGN, при необходимости выполнит трансляцию портов и перешлет пакет в направлении CGN. Шлюз HG будет сохранять данные о трансляции адресов и отображении портов v4-v4 для входящих пакетов, подобно другим системам NAT.

Для IPv6 шлюз HG должен инкапсулировать данные в туннель IPv4, для которого адресатом IPv4 служит устройство CGN с двойным стеком. HG передает новый пакет IPv4 в направлении CGN, используя (например) 6rd.

Если шлюз HG связан с множеством устройств CGN, он будет сохранять данные отображения между туннелем и адресом отправителя IPv6 для входящих пакетов. Подробное рассмотрение работы множества CGN с одним шлюзом HG оставлено на будущее.

Пакеты IPv4 от CGN и инкапсулированные пакеты IPv6 от CGN будут транслироваться или декапсулироваться в соответствии с сохраненными данными об отображении и пересылаться на пользовательскую сторону шлюза HG.

2.4. Поведение CGN с двумя стеками протоколов

Когда CGN с двойным стеком протоколов получает пакет данных IPv4 от домашнего шлюза с двойным стеком, он будет определять, является ли этот пакет обычным пакетом IPv4 (без инкапсуляции) или туннелируемым пакетом v6-over-v4, адресованным конечной точке туннеля внутри этого CGN. Для обычного пакета IPv4 устройство CGN транслирует адрес отправителя в пакете из области IPv4 этого CGN в публичный адрес IPv4, выполняя при необходимости отображение портов, и затем обычным путем пересылает этот пакет в IPv4 Internet. CGN записывает данные трансляции адресов v4-v4 и отображения портов для последующей обработки входящих пакетов, как это делают обычные устройства NAT. Для туннелируемый пакетов v6-over-v4 конечная точка туннеля в CGN будет декапсулировать пакет в обычный пакет IPv6 и затем пересылать его в IPv6 Internet. CGN записывает информацию об отображении туннеля на адреса отправителя IPv6 для последующей обработки входящих пакетов.

В зависимости от места установки CGN это устройство может использовать дополнительный туннель v6-over-v4 для подключения к IPv6 Internet.

[1]Generic Routing Encapsulation - базовая инкапсуляция маршрутной информации.
[2]Intra-Site Automatic Tunnel Addressing Protocol - протокол автоматической адресации туннелей внутри сайта.
[3]Virtual Enterprise Traversal - виртуальный проход через сеть предприятия.
[4]IPv6 Provider Edge.

Пакеты из IPv4 Internet будут соответствующим образом транслироваться устройством CGN и пересылаться устройству HG, а пакеты из IPv6 Internet будут туннелироваться в соответствующий шлюз HG с использованием при сохраненной информации об отображениях.

2.5. Влияние на имеющиеся хосты и необновленные сети

Эта модель не оказывает никакого влияния на неизменяемые части сети ISP. Унаследованные сети IPv4 ISP и устройства IPv4 в них продолжат работать, как обычно. Имеющиеся хосты IPv4, показанные прямоугольником в нижнем правом углу на рисунке 1 и имеющие публичные (глобальные) адреса IPv4 или расположенные за трансляторами v4-v4 NAT, могут подключаться к IPv4 Internet обычным способом. Эти хосты при переходе к двойному стеку протоколов смогут подключаться к IPv6 Internet через сеть IPv4 ISP, используя туннелирование Ipv6-over-IPv4 (см. параграф 2.7, где рассмотрен размер MTU).

2.6. Связь между IPv4 и IPv6

По очевидным коммерческим причинам понятно, что полного перехода публичных услуг на IPv6 не следует ожидать, пока сохраняется достаточно большое число пользователей IPv4. Однако взаимодействие между IPv4 и IPv6 может сталкиваться с проблемами во многих вариантах реализации.

Предполагается, IETF стандартизует рекомендуемый алгоритм перехода от IPv4 к IPv6, иногда называемый NAT64. Этот алгоритм описан в перечисленных ниже документах.

- Framework for IPv4/IPv6 Translation [RFC6144];
- IPv6 Addressing of IPv4/IPv6 Translators [RFC6052];
- DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers [RFC6147];
- IP/ICMP Translation Algorithm [RFC6145];
- Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers [RFC6146];
- An FTP ALG for IPv6-to-IPv4 Translation [FTP-ALG].

Сервис, как описано в документе IETF «Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment» [RFC6180], обеспечивает трансляцию без учета состояний (stateless) между хостами в домене только-IPv4 или хостами, предоставляющими только услуги IPv4, и хостами с адресом IPv6, имеющими встроенный адрес IPv4 (IPv4-embedded IPv6), в домене только-IPv6. В дополнение к этому он обеспечивает доступ с хостов IPv6 с адресами общего формата к хостам в домене только-IPv4 или хостам, предоставляющим только услуги IPv4. Сервис не обеспечивает трансляции «все во все» (any-to-any). Одним из результатов является то, что хосты в домене IPv6 получают услуги IPv4 через трансляцию с учетом состояния (stateful). Другой результат состоит в том, что оператор сети IPv6 получает вариант переноса серверов в домен только-IPv6, сохраняя доступ к ним для клиентов только-IPv4 через трансляцию без учета состояния в адреса IPv6 со встроенными адресами IPv4.

Документ «Architectural Implications of NAT» [RFC2993] применим к службе так же, как к обычной трансляции IPv4/IPv4, с учетом того, что система с адресом IPv6, включающим адрес IPv4, доступна через NAT. Документ «Architectural Implications of NAT» [RFC2993] применяется к сервису просто как к трансляции IPv4/IPv4 за исключением того, что системы с адресом IPv6, содержащим IPv4, достижимы через NAT и в отличие от IPv4, любые допущения приложения о значимости локального адреса для удаленного партнера и любое использование адреса IP буквально в данных приложения являются прерогативой источника сервиса. В общем случае для снижения риска рекомендуются указанные ниже меры.

- В идеале приложениям следует использовать имена DNS, а не адреса IP в идентификаторах URL, URI и ссылках, что обеспечит независимость от сетевого уровня.
- Если этого не делается, сеть может предоставлять транслятор или прокси, охватывающий домены. Например, агент SMTP MTA[1] с подключением IPv4 и IPv6 четко обрабатывает трансляцию IPv4/IPv6 на прикладном уровне.

2.7. Обсуждение

Для трафика IPv4 модель постепенного перехода CGN наследует все проблемы методов совместного использования адресов CGN [ADDR-ISSUES] (например, расширяемость и сложность поддержки общеизвестных портов для входящего трафика). Проблемы прикладного уровня, вызываемые двойным преобразованием NAT, выходят за рамки этого документа.

Для трафика IPv6 пользователи, находящиеся за DS HG, будут видеть обычный сервис IPv6. Было замечено, что MTU туннелей IPv6 размером не меньше 1500 байтов обеспечивает механизм, не вызывающий избыточной фрагментамии трафика IPv6 или избыточных взаимодействий по определению IPv6 path MTU. Вместе с отстутствием проблем NAT для IPv6 это будет стимулом для пользователей и провайдеров приложений к переходу на IPv6.

Фильтрация ICMP [RFC4890] может быть включена как часть функций CGN.

3. Плавный переход к инфраструктуре IPv6

Переход от «чистого» NAT444 CGN или 6rd к инкрементному CGN прост. Устройства HG и CGN и их местоположение не меняются и может потребоваться лишь обновление программ. В описанной ниже идеальной модели не требуется даже обновления программ и достаточно лишь изменить конфигурацию. NAT444 CGN решает проблему нехватки публичных адресов в современной инфраструктуре IPv4. Однако это не способствует развертыванию IPv6 в целом. Инкрементный CGN может наследовать функции NAT444 CGN, обеспечивая при этом наложенные услуги IPv6. механизмы 6rd можно плавно преобразовать в эту инкрементную модель CGN. Однако домашние шлюзы предется обновить для выполнения описанных ниже действий.

[1]Mail Transfer Agent - агент доставки почты.

Инкрементный CGN можно легко перевести в поддерживающую IPv6 инфраструктуру, где сеть ISP использует оба протокола или только IPv6.

Если ISP предпочтет перейти на маршрутизацию для двух протоколов (dual-stack routing), HG следует просто отключить свою функцию v6-over-v4 при наличии трафика IPv6 RA[1] или DHCPv6 и пересылать трафик IPv6 и IPv4 напрямую, а в CGN с двумя стеками сохранить лишь функцию v4-v4 NAT.

Однако предполагается, что ISP выберут подход, описанный как инкрементный CGN в этом документе, поскольку это позволит избежать маршрутизации для двух протоколов и постепенно перейти от маршрутизации IPv4 к маршрутизации только IPv6. В этом случае идеальной модель для инкрементного CGN будет интегрированное настраиваемое устройство CGN и адаптивное устройство HG. Интегрированное устройство CGN сможет поддерживать множество функций, включая NAT444 CGN, маршрутизатор 6rd (или дополнительный механизм туннелирования), DS-Lite и пересылку для двух протоколов.

HG интегрирует соответствующие функции и сможет детектировать соответствующие инкрементные изменения на стороне CGN. Обычно HG будет время от времени опрашивать CGN для определения работающих функций. Например, начав с поддержки только IPv4 (в этом случае HG считает CGN принятым по умолчанию маршрутизатором IPv4), HG обнаружит (путем нечастого опроса) доступность 6rd. Тогда домашние пользователи будут получать адреса IPv6. Позднее HG обнаружит появление естественных сообщений IPv6 Route Advertisement или DHCPv6 для определения доступности сервиса IPv6, включая DS-Lite. Таким образом, когда ISP решит перейти от инкрементного CGN на DS-Lite CGN, потребуется лишь изменить конфигурацию и слегка обновить программы на устройствах CGN. Домашние шлюзы увидят эти изменения и автоматически переключатся в режим DS-Lite. Единственным влиянием на домашних пользователей будет изменение префикса IPv6.

В модели плавного перехода устройства CGN и HG могут использоваться повторно на разных этапах перехода. Это позволяет избежать многократного обновления. Разные участки сети одного ISP могут находиться на разных этапах перехода, использующих идентичные устройство с разными конфигурациями инкрементного CGN в каждом участке сети. Таким образом, переход на IPv6 может обеспечиваться постепенно в соответствии с реальными потребностями пользователей и ISP.

4. Вопросы безопасности

Вопросы безопасности, связанные с NAT, были рассмотрены в [RFC2663] и [RFC2993]. Проблемы безопасности для крупномасштабного использования общих адресов, включая CGN, рассмотрены в [ADDR-ISSUES]. Этот документ не добавляет новых функций в CGN и поэтому не созлает новых проблем безопасности. Вопросы безопасности 6rd рассмотрены в [RFC5569] и [RFC5969], а DS-Lite - в [DS-LITE].

Поскольку предложенные здесь туннели полностью размещаются в сети одного ISP между устрогйствами HG/CPE и CGN, модель угроз относительно проста. В [RFC4891] описана защита туннелей с использованием IPsec, но ISP могут обоснованно считать свою инфраструктуру достаточно защищенной без применения IPsec. Внутренние риски туннелей описаны в [RFC6169], где рекомендуется не передавать туннелируемый трафик через граничные маршрутизаторы. В инкрементной модели CGN эта рекомендация учтена. Для предотвращения других рисков, связанных с туннелями, важно, чтобы все механизмы защиты, основанные на проверке пакетов и все реализации входных фильтров применялись к пакетам IPv6 после их декапсуляции устройством CGN. Домашним шлюзам с двумя стеками протоколов нужно поддерживать базовые функции защиты для IPv6 [RFC6092]. Другие вопросы рассмотрены в[RFC4864].

5. Благодарности

Множество полезных замечаний было получено от Fred Baker, Dan Wing, Fred Templin, Seiichi Kawamura, Remi Despres, Janos Mohacsi, Mohamed Boucadair, Shin Miyakawa, Joel Jaeggli, Jari Arkko, Tim Polk, Sean Turner и других членов рабочей группы IETF V6OPS.

6. Литература

6.1. Нормативные документы

[RFC2529] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529, March 1999.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

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

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

6.2. Дополнительная литература

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC2993] Hain, T., "Architectural Implications of NAT", RFC 2993, November 2000.

[RFC3053] Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

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

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

[1]Router Advertisement - анонс маршрутизатора.

[RFC4798] De Clercq, J., Ooms, D., Prevost, S., and F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)", RFC 4798, February 2007.

[RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.

[RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.

[RFC4891] Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.

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

[RFC5558] Templin, F., Ed., "Virtual Enterprise Traversal (VET)", RFC 5558, February 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from Ipv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. Van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.

[RFC6169] Krishnan, S., Thaler, D., and J. Hoagland, "Security Concerns with IP Tunneling", RFC 6169, April 2011.

[RFC6180] Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, May 2011.

[RFC6204] Singh, H., Beebee, W., Donley, C., Stark, B., and O. Troan, Ed., "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011.

[IPUSAGE] G. Huston, IPv4 Address Report, June 2011, http://www.potaroo.net/tools/ipv4/index.html.

[DS-LITE] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", Work in Progress[1], May 2011.

[ADDR-ISSUES] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", Work in Progress[2], March 2011.

[CGN-REQS] Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for IP address sharing schemes", Work in Progress[3], March 2011.

[FTP-ALG] van Beijnum, I., "An FTP ALG for Ipv6-to-IPv4 Translation", Work in Progress[4], May 2011.

Адреса авторов

Sheng Jiang

Huawei Technologies Co., Ltd

Huawei Building, No.3 Xinxi Rd.,

Shang-Di Information Industry Base, Hai-Dian District

Beijing 100085

P.R. China

EMail: jiangsheng@huawei.com

Dayong Guo

Huawei Technologies Co., Ltd

Huawei Building, No.3 Xinxi Rd.,

Shang-Di Information Industry Base, Hai-Dian District

Beijing 100085

P.R. China

EMail: guoseu@huawei.com

[1]Работа опубликована в RFC 6333. *Прим. перев.*
[2]Работа опубликована в RFC 6269. *Прим. перев.*
[3]Работа опубликована в RFC 6888. *Прим. перев.*
[4]Работа опубликована в RFC 6384. *Прим. перев.*

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand
EMail: brian.e.carpenter@gmail.com

Перевод на русский язык

Николай Малых
nmalykh@gmail.com