Internet Engineering Task Force (IETF)
Request for Comments: 7915
Obsoletes: 6145
Category: Standards Track
ISSN: 2070-1721

C. Bao
X. Li
CERNET Center/Tsinghua University
F. Baker
Cisco Systems
T. Anderson
Redpill Linpro
F. Gont
Huawei Technologies

June 2016

Алгоритм трансляции IP/ICMP

IP/ICMP Translation Algorithm

Аннотация

Этот документ описывает алгоритм SIIT[1], который служит для преобразования между заголовками пакетов IPv4 и IPv6 (включая заголовки ICMP). Данный документ отменяет действие RFC 6145.

Статус документа

Документ относится к категории Internet Standards Track (проект стандарта).

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[3]. Дополнительная информация о стандартах Internet представлена в разделе 2 RFC 7841.

Информацию о текущем статусе документа, обнаруженных ошибках и способах обратной связи можно получить по ссылке http://www.rfc-editor.org/info/rfc7915.

Оглавление

[1]Stateless IP/ICMP Translation Algorithm — алгоритм трансляции IP/ICMP без учета состояний.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение и мотивация

Данный документ отменяет действие [RFC6145].

Предполагается, что читатели данного документа изучили и поняли модель, описанную в [RFC6144]. Реализации описанной здесь трансляции IPv4/IPv6 **должны** поддерживать хотя бы один алгоритм отображения адресов, как описано в разделе 6.

1.1. Модель трансляции IPv4-IPv6

Модель трансляции включает не менее двух сетевых доменов, соединенных через один или множество трансляторов IP/ICMP (XLAT), как показано на рисунке 1.

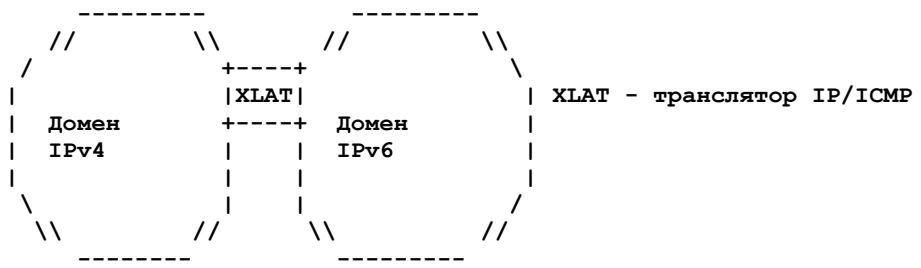

Рисунок 1. Модель трансляции IPv4-IPv6

Сценарии работы модели трансляции рассмотрены в [RFC6144].

1.2. Применимость и ограничения

В этом документе описаны алгоритмы преобразований пакетов между протоколами IPv4 и IPv6.

Как и в [RFC6145], функция преобразования, заданная в этом документе, не транслирует никаких опций IPv4, а также расширенных заголовков IPv6, за исключением Fragment Header.

Проблемы и алгоритмы трансляции дейтаграмм с сегментами TCP описаны в [RFC5382].

Фрагментированные пакеты IPv4 UDP, которые не включают контрольной суммы UDP (т. е., поле контрольной суммы имеет значение 0), нечасто используются в Internet и в общем случае не преобразуются транслятором IP/ICMP (параграф 4.5). Однако, если транслятор настроен на пересылку пакетов без контрольной суммы UDP, фрагментированные пакеты IPv4 UDP будет транслироваться.

Фрагментированные пакеты ICMP/ICMPv6 не будут преобразовываться трансляторами IP/ICMP.

Трансляция заголовков IP/ICMP, описанная в этом документе, совместима с требованиями к групповым заголовкам IP/ICMP. Однако групповые адреса IPv4 [RFC5771] не могут быть отображены на групповые адреса IPv6 [RFC3307] на основе правила отображения индивидуальных адресов [RFC6052]. Пример экспериментов с с отображением групповых адресом рассмотрен в [RFC6219].

1.3. Режимы с учетом и без учета состояния

Транслятор IP/ICMP может работать в двух режимах — без учета состояния (stateless) и с его учетом (stateful) [RFC6144]. В обоих случаях предполагается, что система (узел или приложение), имеющая адрес IPv4, но не имеющая адреса IPv6, взаимодействует с системой, у которой есть адрес IPv6, но нет адреса IPv4, две системы не имеют непрерывной маршрутной связности или взаимодействуют с применением маскирования адресов (hairpinning) [RFC4787] и, следовательно, требуется применять трансляцию.

В режиме, не учитывающем состояний, транслятор IP/ICMP будет преобразовывать адреса IPv4 в адреса IPv6 и наоборот, основываясь на своих конфигурационных параметрах и содержащейся в транслируемых пакетах информации. Например, для определенного в [RFC6052] транслятора по умолчанию некий заданный диапазон адресов IPv6 будет представлять системы IPv4 (преобразованные в IPv4 адреса), а системы IPv6 используют адреса (преобразуемые в IPv4 адреса), которые могут алгоритмически отображаться на подмножество адресов IPv4 из блока сервис-провайдера. В разделе 6 определены другие механизмы трансляции без учета состояний. Не учитывающий состояний транслятор не сохраняет информации о сессиях и привязках, поэтому в данном случае не требуется, чтобы все пакеты одной сессии или потока проходили через один транслятор.

В режиме с учетом состояний системы IPv4 обычно представляет конкретный диапазон адресов IPv6 (состоящий из преобразуемых в IPv4 адресов IPv6). Узлы IPv6 могут использовать любые адреса IPv6 [RFC4291], за исключением этого диапазона. Учитывающий состояния транслятор IP/ICMP постоянно поддерживает таблицу преобразований, содержащую привязки между адресами IPv4 и IPv6, а также идентификаторы транспортного уровня, используемые при трансляции пакетов. Конкретное преобразование адресов для любого данного пакета будет зависеть от привязки этого пакета к сессии или потоку. По этой причине для такой трансляции требуется прохождение всех пакетов одной сессии или потока через один транслятор.

Для успешного преобразования пакетов между протоколами IPv4 и IPv6 транслятор должен поддерживать алгоритм отображения адресов. Данный документ не задает такого алгоритма, но в разделе 6 упомянуты некоторые из возможных алгоритмов отображения.

1.4. Определение Path MTU и фрагментация

По причине различия в размерах заголовков IPv4 и IPv6 (20 и более и 40 октетов, соответственно), обработка пакетов максимального размера имеет критически важное значение для работы трансляторов IPv4/IPv6. Существует три варианта решения этой задачи — определение MTU на пути (PMTUD), фрагментация и согласование на транспортном уровне (типа опции TCP MSS[1] [RFC6691]). Отметим, что транслятор **должен** вести себя, как маршрутизатор, т. е. **должен** передавать сообщения Packet Too Big в случаях, когда размер пакета превышает значение MTU на интерфейсе следующего интервала.

Работа с фрагментами и обработка сообщений ICMP Packet Too Big рассмотрены в разделах 4 и 5 данного документа. Сборка фрагментов в трансляторах с учетом соединений рассмотрена в [RFC6146].

2. Отличия от RFC 6145

Отличия данного документа от RFC 6145 включают:

1. добавление примечаний об обработке расширенных заголовков IPv6 [Err3059], [Err3060], [Err3061] и [Err4090];
2. исключен алгоритм, генерирующий атомарные фрагменты IPv6, по результатам анализа [ATOMIC] и спецификации [IPv6];
3. добавлены примечания по отображению адресов без учета состояний для пакетов ICMPv6 [RFC6791];
4. добавлены новые алгоритмы отображения адресов и обсуждение таких алгоритмов перенесено в раздел 6.

3. Соглашения

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 [RFC2119].

4. Трансляция IPv4 в IPv6

Когда транслятор IP/ICMP получает дейтаграмму IPv4, направленную получателю из домена IPv6, он преобразует в этом пакете заголовок IPv4 в заголовок IPv6. Исходный заголовок IPv4 удаляется из пакета и вместо него размещается заголовок IPv6, контрольные суммы для транспортного уровня при необходимости пересчитываются, если данный транспорт поддерживается транслятором. Данные в пакете сохраняются в неизменном виде. После этого транслятор IP/ICMP пересылает пакет в соответствии с адресом получателя IPv6.

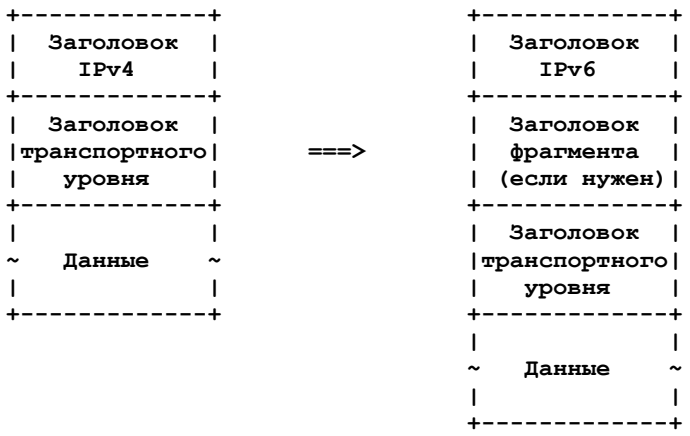

Рисунок 2. Трансляция IPv4 в IPv6

Механизм определения Path MTU является обязательным для IPv6, но не обязателен в IPv4. Маршрутизаторы IPv6 никогда не фрагментируют пакеты, это может делать только отправитель.

Когда узел IPv4 определяет значение MTU для пути (устанавливая флаг DF[2] в заголовке), процедура может быть сквозной (т. е., включающей транслятор). В таких случаях любой из маршрутизаторов IPv4 и IPv6 (включая транслятор) может передать отправителю сообщение ICMP Packet Too Big. Если такое сообщение передает маршрутизатор IPv6, оно будет проходить через транслятор, который преобразует сообщение об ошибке ICMPv6 в понятную отправителю IPv4 форму. Благодаря этому, заголовок IPv6 Fragment Header включается только в тех случаях, когда пакет IPv4 уже был фрагментирован.

Однако в тех случаях, когда отправитель IPv4 не устанавливает бит DF, трянслятор **должен** гарантировать, что размер пакета не превышает MTU на стороне IPv6. Это выполняется путем фрагментирования пакетов IPv4 (с добавлением заголовков Fragment Header) так, чтобы фрагменты помещались в 1280-байтовые пакеты IPv6 (минимальное значение IPv6 MTU). Было показано, что заголовки IPv6 Fragment Header могут вызывать сложности при работе по причине ограниченной поддержки фрагментации на межсетевых экранах и т. п. В средах, где сеть и транслятор принадлежат (обслуживаются) одной организации, трансляторы **должны** обеспечивать сетевым администраторам возможность настройки порогового значения минимума для IPv6 MTU в соответствии с реальным IPv6 MTU в сети (больше 1280 байтов). Это позволит снизить вероятность применения заголовков Fragment Header.

[1]Maximum Segment Size — максимальный размер сегмента.
[2]Don't Fragment — не фрагментировать.

Если отправитель IPv4 не устанавливает флаг DF, транслятору **недопустимо** включать заголовок Fragment Header для нефрагментированных пакетов IPv6.

Приведенные в параграфе 4.1 правила обеспечивают, что в тех случаях, когда пакеты фрагментируются отправителем или маршрутизатором IPv4, младшие 16 битов идентификации фрагмента передаются насквозь без изменений, что обеспечивает возможность корректной сборки фрагментов.

Кроме специальных правил обработки фрагментов и определения MTU на пути, реальная трансляция пакетов включает простые преобразования, определенные ниже. Отметим, что для пакетов ICMPv4 требуется специальная обработка для преобразования сообщений ICMPv4 об ошибках, а также добавления контрольной суммы псевдо-заголовка ICMPv6.

Трансляторам **следует** обеспечивать передачу пакетов одного потока в соответствии с порядком их поступления на данный транслятор.

4.1. Трансляция заголовков IPv4 в заголовки IPv6

Если бит DF не установлен в пакете IPv4 и размер транслированного пакета IPv6 превышает заданное пользователем значение (обычно называемое lowest-ipv6-mtu, которое по умолчанию составляет 1280 байтов), пакет **следует** фрагментировать так, чтобы получаемые в результате пакеты IPv6 (с заголовком Fragment Header для каждого фрашмента) не превышали в размере lowest-ipv6-mtu. Например, если пакеты фрагментируются до трансляции, размер фрагментов IPv4 вместе с их заголовками не должен превышать 1232 байтов (1280 минус 40 байтов на заголовок IPv6 и 8 байтов для Fragment Header). Транслятор **должен** обеспечивать возможность настройки порогового значения IPv6 MTU для установки значений более 1280 в тех случаях, когда администратору известно реальное значение IPv6 MTU. После этого фрагменты транслируются независимо с использованием описанной ниже логики.

Если бит DF установлен и значение MTU на интерфейсе следующего интервала меньше общего размера пакета IPv4 + 20, транслятор **должен** передать сообщение ICMPv4 Fragmentation Needed по адресу отправителя IPv4.

Для полей IPv6 значения устанавливаются, как описано ниже.

Version
6.

Traffic Class
По умолчанию копируется из октета IP TOS[1]. В соответствии с [RFC2474] значение битов этого поля идентично в IPv4 и IPv6. Однако в некоторых средах IPv4 поле типа обслуживания использует старую семантику Type Of Service and Precedence. Реализациям трансляторов **следует** поддерживать опцию для игнорирования IPv4 TOS и установки с поле IPv6 TC[2] значения 0. Кроме того, для трансляторов на административных границах могут применяться фильтры и изменения [RFC2475].

Flow Label
0 (все биты равны 0).

Payload Length
Значение общего размера из заголовка IPv4 за вычетом размера самого заголовка IPv4 и опций (при их наличии).

Next Header
Для ICMPv4 (1) значение меняется на ICMPv6 (58), в остальных случаях **должно** включать значение поля протокола из заголовка IPv4.

Hop Limit
Предельное число интервалов пересылки определяется по значению TTL в заголовке IPv4. Поскольку транслятор является маршрутизатором при пересылке пакетов от него требуется уменьшить на 1 значение IPv4 TTL (до трансляции) или IPv6 Hop Limit (после трансляции). В процессе декрементирования TTL или Hop Limit транслятор (как любой маршрутизатор) **должен** проверить отличие значения поля и передать сообщение об ошибке ICMPv4 TTL Exceeded или ICMPv6 Hop Limit Exceeded, если значение окажется нулевым.

Source Address
Отображается на адрес IPv6 с использованием алгоритмов, представленных в разделе 6.
Если транслятор получает пакет с недопустимым адресом отправителя (например, 0.0.0.0, 127.0.0.1 и т. п.), ему **следует** отбросить такой пакет без уведомления отправителя (как описано в параграфе 5.3.7 [RFC1812]). Отметим, что при трансляции сообщений ICMPv4 об ошибках ICMPv6 недопустимые адреса будут преобразовываться в целях поиска неполадок.

Destination Address
Отображается на адрес IPv6 с использованием алгоритмов, представленных в разделе 6.

При наличии в пакете каких-либо опций IPv4, транслятор **должен** игнорировать их и выполнять обычную обработку пакетов без попыток трансляции опций. Однако при получении пакета с действующей опцией source route такой пакет **должен** отбрасываться, а его отправителю **следует** возвращать сообщение ICMPv4 адресат не доступен, Source Route Failed (Type 3, Code 5).

Если требуется добавление заголовка Fragment Header (пакет является фрагментом или флаг DF не установлен, а размер пакета превышает минимальное значение IPv6 MTU, заданное в конфигурации транслятора), при установке полей используется ряд исключений, описанных ниже.

Поля IPv6

Payload Length
Значение общего размера пакета из заголовка IPv4 за вычетом размера самого заголовка IPv4 и опций (при их наличии) + 8 байтов для Fragment Header.

Next Header
Fragment Header (44).

Поля Fragment Header

Next Header

[1]Type Of Service — тип обслуживания.
[2]Traffic Class — класс трафика.

Для ICMPv4 (1) значение меняется на ICMPv6 (58), в остальных случаях **должно** включать значение поля протокола из заголовка IPv4.

Fragment Offset

Копируется значение поля Fragment Offset из заголовка IPv4.

M flag

Копируется бит More Fragments из заголовка IPv4.

Identification

Младшие 16 битов копируются из поля Identification в заголовке IPv4, а старшие 16 битов устанавливаются в 0.

4.2. Трансляция заголовков ICMPv4 в заголовки ICMPv6

При трансляции сообщений ICMPv4 требуется расчет контрольной суммы ICMPv6, поскольку в ICMPv6, в отличие от ICMPv4, используется контрольная сумма псевдо-заголовка, как в UDP и TCP.

В дополнение к этому для всех пакетов ICMPv4 **должны** транслироваться поля Type, а для сообщений ICMPv4 об ошибках **должен** транслироваться также включенный в них заголовок IP.

Ниже описаны действия, требуемые для трансляции различных сообщений ICMPv4.

Запросы ICMPv4

Echo и Echo Reply (Type 8 и Type 0)

Значения Type меняются на 128 и 129, соответственно, а контрольная сумма пересчитывается заново для учета изменения типа и добавления псевдо-заголовка ICMPv6.

Information Request/Reply (Type 15 и Type 16)

Не используется в ICMPv6. Отбрасывание без уведомления.

Timestamp and Timestamp Reply (Type 13 and Type 14)

Не используется в ICMPv6. Отбрасывание без уведомления.

Address Mask Request/Reply (Type 17 and Type 18)

Не используется в ICMPv6. Отбрасывание без уведомления.

ICMP Router Advertisement (Type 9)

Сообщение single-hop[1]. Отбрасывание без уведомления.

ICMP Router Solicitation (Type 10)

Сообщение single-hop. Отбрасывание без уведомления.

Unknown ICMPv4 types

Отбрасывание без уведомления.

Сообщения IGMP

Хотя сообщения MLD[2], определенные в [RFC2710], [RFC3590] и [RFC3810] являются логическими копиями IPv6 для сообщений IPv4 IGMP, все «нормальные» сообщения IGMP относятся к типу single-hop и трансляторам **следует** отбрасывать их без уведомления. Другие сообщения IGMP могут применяться протоколами групповой маршрутизации и, поскольку попытки организации отношений смежности между маршрутизаторами через транслятор IP/ICMP говорят о конфигурационных ошибках, такие пакеты **следует** отбрасывать без уведомления.

Сообщения ICMPv4 об ошибках

Destination Unreachable (Type 3)

Транслируется значение Code, как описано ниже, устанавливается Type = 1 и корректируется контрольная сумма ICMP для учета изменений типа и кода, а также добавления псевдо-заголовка ICMPv6.

Значения кода транслируются следующим образом:

Code 0, 1 (Net Unreachable, Host Unreachable)

Устанавливается Code = 0 (нет маршрута к адресату).

Code 2 (Protocol Unreachable)

Преобразуется в ICMPv6 Parameter Problem (Type 4, Code 1) и устанавливается указатель (Pointer) на поле IPv6 Next Header.

Code 3 (Port Unreachable)

Устанавливается Code = 4 (порт не доступен).

Code 4 (Fragmentation Needed and DF was Set)

Преобразуется в сообщение ICMPv6 Packet Too Big (Type 2) с Code = 0. Значение MTU **должно** корректироваться с учетом разницы размеров заголовков IPv4 и IPv6, но **недопустимо** устанавливать значения меньше минимального IPv6 MTU (1280 байтов). Т. е., для этого поля следует выбирать большее из значений: 1280, minimum((MTU в сообщении Packet Too Big) + 20, MTU_of_IPv6_nexthop, (MTU_of_IPv4_nexthop) + 20)).

Отметим, что если маршрутизатор IPv4 установил MTU = 0 (т. е., он не поддерживает [RFC1191]), транслятор **должен** использовать заданные в [RFC1191] значения для определения MTU на пути и включить Path MTU в пакет ICMPv6 (следует использовать большее из значений, которое не превышает значения поля Total Length, но не меньше 1280).

См. также требования раздела 7.

Code 5 (Source Route Failed)

Устанавливается Code = 0 (нет маршрута к адресату). Отметим, что такие сообщения маловероятны, поскольку заданные отправителем маршруты (source route) не транслируются.

Code 6, 7, 8

Устанавливается Code = 0 (нет маршрута к адресату).

Code 9, 10 (Communication with Destination Host Administratively Prohibited)

Устанавливается Code = 1 (связь с адресатом запрещена административно).

Code 11, 12

Устанавливается Code = 0 (нет маршрута к адресату).

Code 13 (Communication Administratively Prohibited)

Устанавливается Code = 1 (связь с адресатом запрещена административно).

Code 14 (Host Precedence Violation)

[1]Передается на один интервал маршрутизации.

[2]Multicast Listener Discovery — обнаружение получателей группового трафика.

Отбрасывание без уведомления.

Code 15 (Precedence cutoff in effect)

Устанавливается Code = 1 (связь с адресатом запрещена административно).

Другие значения кодов

Отбрасывание без уведомления.

Redirect (Type 5)

Сообщение single-hop. Отбрасывание без уведомления.

Alternative Host Address (Type 6)

Отбрасывание без уведомления.

Source Quench (Type 4)

Не используется в ICMPv6. Отбрасывание без уведомления.

Time Exceeded (Type 11)

Устанавливается Type = 3 и пересчитывается контрольная сумма ICMP с учетом изменений и добавлением псевдо-заголовка ICMPv6. Значение Code не меняется.

Parameter Problem (Type 12)

Устанавливается Type = 4 и пересчитывается контрольная сумма ICMP с учетом изменений и добавлением псевдо-заголовка ICMPv6.

Значение Code меняется следующим образом:

Code 0 (Pointer indicates the error)

Устанавливается Code = 0 (ошибка в поле заголовка) и обновляется указатель, как показано на рисунке 3 (если исходное значение IPv4 Pointer не указано или для преобразованного IPv6 Pointer указано «-», пакет отбрасывается без уведомления).

Code 1 (Missing a required option)

Отбрасывание без уведомления.

Code 2 (Bad length)

Устанавливается Code = 0 (ошибка в поле заголовка) и обновляется указатель, как показано на рисунке 3 (если исходное значение IPv4 Pointer не указано или для преобразованного IPv6 Pointer указано «-», пакет отбрасывается без уведомления).

Другие значения кодов

Отбрасывание без уведомления.

Неизвестные типы ICMPv4

Отбрасывание без уведомления.

Исходное значение IPv4 Pointer		Транслированное значение IPv6 Pointer	
0	Version/IHL	0	Version/Traffic Class
1	Type Of Service	1	Traffic Class/Flow Label
2,3	Total Length	4	Payload Length
4,5	Identification	-	
6	Flags/Fragment Offset	-	
7	Fragment Offset	-	
8	Time to Live	7	Hop Limit
9	Protocol	6	Next Header
10,11	Header Checksum	-	
12-15	Source Address	8	Source Address
16-19	Destination Address	24	Destination Address

Рисунок 3. Значения указателей для трансляции IPv4 в IPv6

Данные в сообщениях ICMP об ошибках

Если принятый пакет ICMPv4 содержит ICMPv4 Extension [RFC4884], при трансляции размер пакета ICMPv6 изменится. В таких случаях атрибут ICMPv6 Extension **должен** быть соответственно изменен (т. е., увеличен при трансляции из IPv4 в IPv6). Если расширение ICMPv4 Extension ведет к превышению максимального размера сообщения ICMPv6 на выходном интерфейсе, расширение ICMPv4 **следует** просто укорачивать. Расширения, не определенные в [RFC4884], транслятор пропускает без обработки (как строку битов), что может вызывать проблемы при обработке таких расширений ICMP.

4.3. Трансляция сообщений ICMPv4 об ошибках в сообщения ICMPv6

Как указано выше, имеются некоторые различия между форматами сообщений об ошибках в ICMPv4 и ICMPv6. Сообщения ICMP об ошибках, содержащие связанный с ошибкой пакет, **должны** транслироваться подобно обычным пакетам IP (за исключением значения TTL во вложенном пакете IPv4/IPv6). Если при трансляции «пакета с ошибкой» меняется размер дейтаграммы, поле Total Length внешнего заголовка IPv6 **должно** быть изменено.

Трансляция внутреннего заголовка IP может быть выполнена путем вызова функции, используемой для трансляции внешних заголовков IP. Этот процесс **должен** останавливаться на первом вложенном заголовке, а пакеты, содержащие более одного вложенного заголовка отбрасываются.

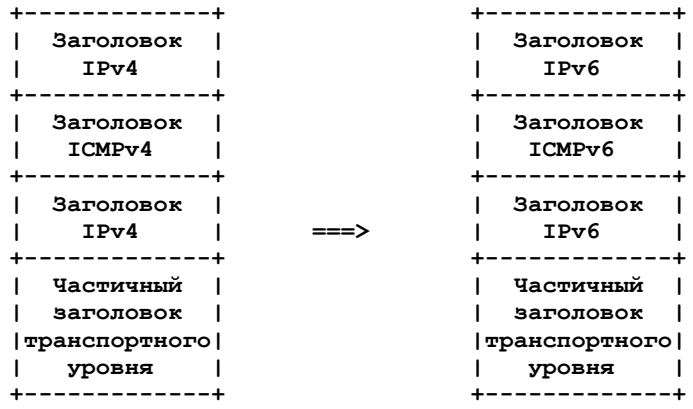

Рисунок 4. Трансляция сообщений ICMP об ошибках из IPv4 в IPv6

4.4. Генерация сообщений ICMPv4 об ошибках

При отбрасывании пакетов IPv4 транслятору **следует** обеспечивать возможность передачи отправителю такого пакета сообщения ICMPv4 об ошибке, если отброшенный пакет сам не является сообщением ICMPv4 об ошибке. Если передается сообщение ICMPv4 об ошибке, в нем указывается Type = 3 (адресат не доступен) и Code = 13 (связь запрещена административно), если в [RFC6146] не указано иное. Трансляторам **следует** обеспечивать администратору возможность задания параметров отправки сообщений ICMPv4 об ошибках (ограничение частоты передачи или отказ от передачи).

4.5. Трансляция заголовков транспортного уровня

Если алгоритм трансляции оказывает влияние на поля, используемые в контрольной сумме (см. параграф 4.1 в [RFC6052]), требуется заново рассчитать и обновить заголовки транспортного уровня, включающие псевдо-заголовки. Трансляторы **должны** делать это для пакетов TCP и ICMP, а также пакетов UDP с контрольной суммой (отличной от 0).

Для пакетов UDP без контрольной суммы (нулевое значение поля) трансляторам **следует** поддерживать функцию, позволяющую настроить:

1. отбрасывание пакетов и генерацию системных событий, указывающих по крайней мере адреса и номера портов из пакета;
2. расчет контрольной суммы IPv6 для пакета и его пересылка (влияет на производительность).

Транслятор без учета состояний не может рассчитать контрольную сумму фрагментированных пакетов UDP, поэтому при получении первого фрагмента пакета UDP IPv4 с нулевым значением контрольной суммы, пакет **следует** отбросить и сгенерировать системное событие, указывающее по крайней мере адреса и номера портов из отброшенного пакета.

Для трансляторов с учетом состояний обработка фрагментированных пакетов UDP IPv4 с нулевым значением контрольной суммы рассмотрена в параграфе 3.4 [RFC6146].

Поддержка других транспортных протоколов (например, DCCP[1]) является **необязательной**. Для упрощения отладки и поиска неполадок трансляторы **должны** пересылать все транспортные протоколы, как указано для поля Next Header в параграфе 4.1.

4.6. Когда нужна трансляция

Если транслятор IP/ICMP поддерживает также функции обычной пересылки и целевой адрес IPv4 доступен по более специфичному маршруту без преобразования, транслятор **должен** переслать пакет по такому маршруту, не преобразуя его. В остальных случаях когда транслятор IP/ICMP получает дейтаграмму IPv4, адресованную получателю IPv4, представляющему хост в домене IPv6, пакет **должен** транслироваться в IPv6.

5. Трансляция IPv6 в IPv4

Когда транслятор IP/ICMP получает дейтаграмму IPv6, адресованную в домен IPv4, он преобразует заголовок IPv6 принятого пакета в заголовок IPv4. Исходный заголовок IPv6 удаляется из пакета и взамен помещается заголовок IPv4. Поскольку заголовки ICMPv6 [RFC4443], TCP [RFC793], UDP [RFC768] и DCCP [RFC4340] содержат контрольную сумму, учитывающую и заголовок IP, если алгоритм отображения меняет поля, учитываемые в контрольной сумме, эта сумма **должна** рассчитываться заново, а после этого **должен** обновляться заголовок ICMP или транспортного уровня. Данные в пакете сохраняются без изменений. После этого транслятор IP/ICMP пересылает пакет получателю IPv4.

Между IPv6 и IPv4 имеются некоторые различия (в части фрагментации и минимального значения MTU), оказывающие влияние на трансляцию. На каналах IPv6 значение MTU не может быть меньше 1280 байтов, а для каналов IPv4 соответствующий порог составляет 68 байтов. Определение Path MTU через транслятор опирается на сообщения ICMP Packet Too Big, получаемые и обрабатываемые хостами IPv6.

[1]Datagram Congestion Control Protocol.

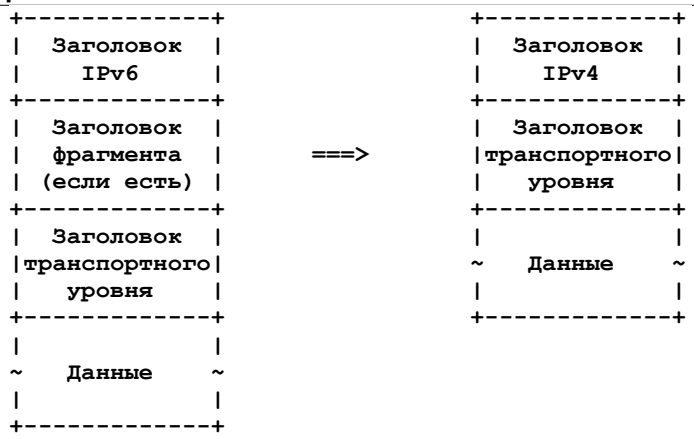

Рисунок 5. Трансляция IPv6 в IPv4

Различия в минимальных значениях MTU для IPv4 и IPv6 преоболеваются следующим образом:

- При трансляции пакетов ICMPv4 Fragmentation Needed значение MTU в результирующем пакете ICMPv6 Packet Too Big всегда будет не меньше 1280. Это означает, что узлы IPv6 никогда не будут сталкиваться со значениями Path MTU меньше минимального IPv6 MTU в 1280 байтов. См. также параграф 4.2.
- Если размер результирующего пакета IPv4 не превышает 1260 байтов, транслятор **должен** передать пакет без флага DF. В остальных случаях флаг запрета фрагментации (DF) **должен** устанавливаться. См. также параграф 5.1.

Эта модель обеспечивает возможность сквозного использования механизма Path MTU Discovery на путях с MTU не меньше минимального IPv6 MTU в 1280 байтов (соответствует MTU в 1260 байтов для домена IPv4). На путях с каналами IPv4, где MTU < 1260, подключенные к таким каналам маршрутизаторы IPv4 будут фрагментировать пакеты в соответствии с параграфом 2.3 [RFC791].

Кроме специальных правил обработки фрагментов и определения MTU для пути, реальное преобразование заголовков пакетов состоит из описанных ниже простых трансляций. Отметим, что для пакетов ICMPv6 требуется специальная обработка с целью трансляции содержимого сообщений ICMPv6 об ошибках и удаления контрольной суммы псевдо-заголовка ICMPv6.

Трансляторам **следует** обеспечивать отправку пакетов одного потока в порядке их приема данным транслятором.

5.1. Трансляция заголовков IPv6 в заголовки IPv4

Если заголовка IPv6 Fragment Header не используется, поля заголовка IPv4 устанавливаются в соответствии с приведенным ниже описанием.

Version
4.

Internet Header Length
5 (без опций IPv4).

Type of Service (TOS) Octet
По умолчанию копируется значение поля IPv6 Traffic Class (все 8 битов). Согласно [RFC2474], значение битов одинаково в IPv4 и IPv6. Однако в некоторых средах IPv4 для этих битов используется старая семантика Type Of Service and Precedence. Реализациям трансляторов **следует** поддерживать возможность игнорировать класс трафика IPv6 и всегда устанавливать для поля IPv4 TOS заданное значение. Кроме того, на административных границах может применяться фильтрация и смена типа обслуживания, как описано в [RFC2475].

Total Length
Значение Payload length из заголовка IPv6, к которому добавлен размер заголовка IPv4.

Identification
Устанавливается в соответствии с генератором значений Fragment Identification на трансляторе.

Flags
Для флага More Fragments устанавливается нулевое значение. Если размер транслированного пакета IPv4 не превышает 1260 байтов, для флага DF устанавливается значение 0, в остальных случаях - 1.

Fragment Offset
Все нули.

Time to Live
Значение поля TTL определяется на основе значения поля Hop Limit в заголовке IPv6. Поскольку транслятор является маршрутизатором, он должен декрементировать значение поля IPv6 Hop Limit (до трансляции) или IPv4 TTL (после трансляции). При декрементировании TTL или Hop Limit транслятор (как любой маршрутизатор) **должен** проверить значение поля и отправить сообщение об ошибке ICMPv4 TTL Exceeded или ICMPv6 Hop Limit Exceeded при достижении нуля.

Protocol
Обработка заголовков IPv6-Frag (44) описана в параграфе 5.1.1. ICMPv6 (58) заменяется на ICMPv4 (1), а данные пакета транслируются в соответствии с параграфом 5.2. Заголовки IPv6 HOPOPT (0), IPv6-Route (43) и IPv6-Opts (60) опускаются при обработке, поскольку они не имеют смысла в IPv4. Для первого Next Header, не относящегося к приведенным выше случаям, значение Next Header (которое соответствует номеру транспортного протокола) копируется в поле протокола заголовка IPv4. Это означает трансляцию всех протоколов транспортного уровня.
Примечание. В некоторых случаях трансляция протоколов будет приводить к отказам — у одних отказы будут возникать при трансляции (например, IPsec Authentication Header (51)), а у других не пройдет проверка контрольной суммы, если алгоритм трансляции будет изменять учитываемые в контрольной сумме поля

[RFC6052], а транслятор не обновит контрольную сумму транспортного протокола (поскольку расчет контрольной суммы для этого протокола не поддерживается, как отмечено в параграфе 5.5).

Header Checksum

Рассчитывается после создания заголовка IPv4.

Source Address

Отображается на адрес IPv4 в соответствии с одним из алгоритмов, указанных в разделе 6.

Если транслятор получает пакет с неприемлемым адресом отправителя (например, ::1), такой пакет **следует** отбросить без уведомления отправителя.

Destination Address

Отображается на адрес IPv4 в соответствии с одним из алгоритмов, указанных в разделе 6.

Если в пакете IPv6 присутствует заголовок Hop-by-Hop Options, Destination Options или Routing с Segments Left = 0, такой заголовок **должен** игнорироваться (без попытки его трансляции), а остальная часть пакета обрабатываться обычным путем. Однако значения полей Total Length и Protocol должны корректироваться с учетом пропущенных заголовков.

При наличии заголовка Routing с отличным от 0 полем Segments Left, трансляция пакета **недопустима** и отправителю **следует** возвращать сообщение об ошибке ICMPv6 Parameter problem/erroneous header field encountered (Type 4, Code 0) с полем Pointer, указывающим на первый байт поля Segments Left.

5.1.1. Обработка фрагментов IPv6

Если пакет IPv6 содержит заголовок Fragment Header, поля заголовка транслируются с учетом перечисленных ниже исключений.

Total Length

Если поле Next Header в заголовке Fragment Header указывает на расширенный заголовок (исключая ESP, но включая AH), пакет **следует** отбросить с внесением записи в системный журнал. В иных случаях в поле Total Length **должно** устанавливаться значение Payload Length из заголовка IPv6 за вычетом размера заголовков расширения до Fragmentation Header, а также 8 байтов Fragment Header и с добавлением размера заголовка IPv4.

Identification

Копируется из младших 16 битов поля Identification в заголовке Fragment Header.

Flags

Флаг IPv4 MF[1] копируется из флага M в заголовке IPv6 Fragment Header. Флаг IPv4 DF сбрасывается для обеспечения возможности дальнейшей фрагментации на маршрутизаторах IPv4.

Fragment Offset

Если поле Next Header в заголовке Fragment Header не указывает на расширенный заголовок (за исключением ESP), значение Fragment Offset **должно** копироваться из поля Fragment Offset в заголовке IPv6 Fragment Header. Если поле Next Header в заголовке Fragment Header указывает расширенный заголовок (за исключением ESP), пакет **следует** отбросив, записав информацию об этом в системный журнал.

Protocol

Для ICMPv6 (58) значение заменяется на ICMPv4 (1), в остальных случаях заголовки расширения пропускаюия и копируется значение поля Next Header из последнего заголовка IPv6.

Если размер пакета IPv6 не превышает 1280 байтов, но размер пакета IPv4 (после трансляции) больше значения MTU на интерфейсе следующего интервала, транслятор **должен** фрагментировать пакет IPv4 для его передачи через канал с ограниченным размером пакетов.

5.2. Трансляция заголовков ICMPv6 в заголовки ICMPv4

При использовании оказывающей влияние на контрольные суммы трансляции адресов в сообщениях ICMPv6 **должна** обновляться контрольная сумма ICMPv4 в процессе трансляции, поскольку ICMPv6 (в отличие от ICMPv4) включает в контрольную сумму псевдо-заголовок, как UDP и TCP.

В дополнение к этому для всех пакетов ICMP **должны** транслироваться значения Type, а для сообщений ICMP об ошибках — еще и включенный в сообщение заголовок IP.

Ниже перечислены действия, требуемые для трансляции разных сообщений ICMPv6.

Информационные сообщения ICMPv6

Echo Request и Echo Reply (Type 128 и 129)

Установить для поля Type значение 8 и 0, соответственно, а также пересчитать контрольную сумму с учетом смены значения и исключения псевдо-заголовка ICMPv6.

MLD Multicast Listener Query/Report/Done (Type 130, 131, 132)

Сообщение Single-hop. Отбрасывание без уведомления.

Neighbor Discover messages (Type 133 - 137)

Сообщение Single-hop. Отбрасывание без уведомления.

Неизвестные информационные сообщения

Отбрасывание без уведомления.

Сообщения ICMPv6 об ошибках

Destination Unreachable (Type 1)

Устанавливается Type = 3 и пересчитывается контрольная сумма ICMP с учетом изменений и добавлением псевдо-заголовка ICMPv6.

Поле Code транслируется следующим образом:

Code 0 (No route to destination)

Устанавливается Code = 1 (хост не доступен).

Code 1 (Communication with destination administratively prohibited)

Устанавливается Code = 10 (связь с хостом запрещена административно).

[1]More Fragments — имеются другие фрагменты.

Code 2 (Beyond scope of source address)
Устанавливается Code = 1 (хост не доступен). Отметим, что такая ошибка маловероятна, поскольку транслируемые адреса IPv4 обычно имеют глобальную значимость.
Code 3 (Address unreachable)
Устанавливается Code = 1 (хост не доступен).
Code 4 (Port unreachable)
Устанавливается Code = 3 (порт не доступен).
Другие коды
Отбрасывание без уведомления.

Packet Too Big (Type 2)
Трансляция в ICMPv4 Destination Unrechable (Type 3) с Code 4 и пересчитывается контрольная сумма ICMP с учетом изменений и исключением псевдо-заголовка ICMPv6. Значение поля MTU **должно** быть изменено с учетом разницы размеров заголовков IPv4 и IPv6, а также наличия в содержащемся внутри сообщения заголовке расширенного заголовка Fragment Header. Для MTU устанавливается меньшее из значений ((MTU в сообщении Packet Too Big Message)-20, MTU_of_IPv4_nexthop, (MTU_of_IPv6_nexthop)-20).
См. также требования раздела 7.

Time Exceeded (Type 3)
Устанавливается Type = 11 и пересчитывается контрольная сумма ICMP с учетом изменений и исключением псевдо-заголовка ICMPv6. Значение Code не меняется.

Parameter Problem (Type 4)
Транслируются значения Type и Code как описано ниже и пересчитывается контрольная сумма ICMP с учетом изменений и исключением псевдо-заголовка ICMPv6.
Трансляция значения Code:
Code 0 (Erroneous header field encountered)
Устанавливается Type 12, Code 0 и обновляется указатель в соответствии с рисунком 6 (если исходное значение IPv6 Pointer не указано в таблице или для транслированного IPv4 Pointer указано «-», пакет отбрасывается без уведомления).
Code 1 (Unrecognized Next Header type encountered)
Транслируется в сообщение ICMPv4 Protocol Unreachable (Type 3, Code 2).
Code 2 (Unrecognized IPv6 option encountered)
Отбрасывание без уведомления.

Неизвестные сообщения об ошибках
Отбрасывание без уведомления.

Исходное значение IPv6 Pointer		Транслированное значение IPv4 Pointer	
0	Version/Traffic Class	0	Version/IHL, Type Of Ser
1	Traffic Class/Flow Label	1	Type Of Service
2,3	Flow Label	-	
4,5	Payload Length	2	Total Length
6	Next Header	9	Protocol
7	Hop Limit	8	Time to Live
08 - 23	Source Address	12	Source Address
24 - 39	Destination Address	16	Destination Address

Рисунок 6. Значения указателей для трансляции IPv6 в IPv4

Данные сообщений ICMP об ошибках
если принятый пакет ICMPv6 содержит расширение ICMPv6 [RFC4884], трансляция будет вызывать изменение размера пакета ICMPv4. В таких случаях атрибут размера ICMPv6 Extension **должен** быть соответствующим образом изменен (например, уменьшен при трансляции IPv6 в IPv4). Расширения, не определенные в [RFC4884], транслятор пропускает как битовые строки и все содержащиеся в них адреса IPv6 не будет преобразовываться в адреса IPv4, что может вызывать проблемы при последующей обработке таких расширений ICMP.

5.3. Трансляция сообщений ICMPv6 об ошибках в ICMPv4

Как было отмечено выше, форматы сообщений об ошибках в ICMPv4 и ICMPv6 несколько различаются. В сообщениях ICMP с содержащимися в них пакетами, которые связаны с ошибкой, эти вложенные пакеты **должны** транслироваться как обычные пакеты IP (однако значения TTL/Hop Limit во вложенных пакетах IPv4/IPv6 при этом не декрементируются). Очевидно, что при трансляции вложенного «ошибочного» пакета общий размер дейтаграммы может измениться, поэтому поле Total Length во внешнем заголовке IPv4 также **должно** быть изменено.

Трансляция вложенного в сообщение заголовка IP может выполняться путем вызова той же функции, которая служит для трансляции внешних заголовков. Этот процесс **должен** прерываться на после первого вложенного заголовка с отбрасыванием пакетов, в которые вложено более одного заголовка.

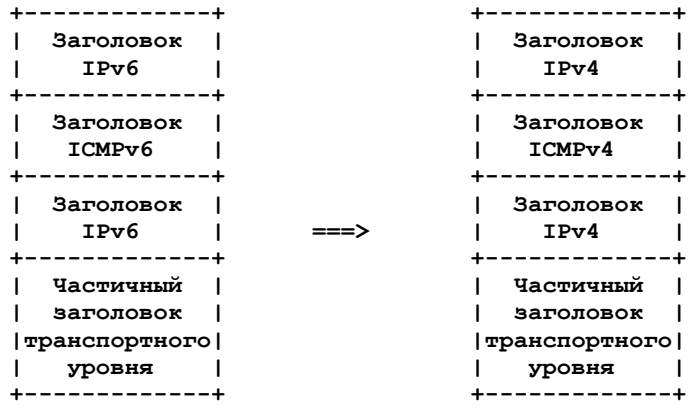

Рисунок 7. Трансляция сообщений ICMP об ошибках из IPv6 в IPv4

5.4. Генерация сообщений ICMPv6 об ошибках

При отбрасывании пакета IPv6 транслятору **следует** вернуть его отправителю сообщение ICMPv6 об ошибке, если отбрасываемый пакет сам не являлся таким сообщением.

В сообщении ICMPv6 **должен** указываться Type = 1 (адресат не доступен) и Code = 1 (связь запрещена административно), если иное не задано в данном документе или [RFC6146]. Трансляторам **следует** обеспечивать администратору возможность управления отправкой сообщений ICMPv6 об ошибках (события, частота передачи).

5.5. Трансляция заголовков транспортного уровня

Если при алгоритм трансляции меняет поля, учитываемые контрольной суммой (см. параграф 4.1 в [RFC6052]), требуется заново рассчитать контрольную сумму и обновить заголовки транспортного уровня, содержащие псевдо-заголовки. Транслятор **должен** делать это для протоколов TCP, UDP и ICMP.

Поддержка других транспортных протоколов (например, DCCP) является **не обязательной**. Для упрощения отладки и поиска неполадок транслятор **должен** пересылать все транспортные протоколы, как указано для поля Protocol в параграфе 5.1.

5.6. Когда нужна трансляция

Если транслятор IP/ICMP поддерживает также обычную пересылку пакетов и адресат доступен по более специфичному маршруту без преобразования, маршрутизатор **должен** переслать такой пакет без трансляции. Когда транслятор IP/ICMP получает дейтаграмму IPv6, направленную по адресу IPv6, представляющему хост в домене IPv4, пакет IPv6 **должен** транслироваться в IPv4.

6. Отображение адресов IP

Транслятор **должен** поддерживать алгоритм отображения адресов без учета состояний [RFC6052], который используется по умолчанию. Пример работы с использованием этого алгоритма показан в Приложении A. Отметим, что [RFC7136] обновляет документ [RFC4291], позволяя использовать индивидуальные адреса без бита u, если они не были созданы на базе адресов IEEE MAC. Следовательно, алгоритм отображения адресов, определенный в [RFC6219], также соответствует архитектуре адресации IPv6.

Трансляторам без учета состояний **следует** поддерживать алгоритм явного отображения адресов [RFC7757].

Трансляторам без учета состояний **следует** поддерживать [RFC6791] для обработки пакетов ICMP/ICMPv6.

Реализации могут поддерживать трансляцию как с учетом состояний, так и без него (например, трансляцию адресов и протоколов от клиентов IPv6 к серверам IPv4 (NAT64) [RFC6146]).

Реализации могут поддерживать не учитывающую состояний функцию NAT64 (например, MAP-T Customer Edge (CE) или MAP-T Border Relay (BR) [RFC7599]).

7. Особый случай ICMPv6 Packet Too Big

Множество исследований показало [ATOMIC], что нет ничего необычного в отбрасывании сетями сообщений ICMPv6 Packet Too Big. Отбрасывание таких пакетов приводит к возникновению «черных дыр» PMTUD [RFC2923], которые можно предотвратить только с помощью PLPMTUD[1] [RFC4821].

8. Вопросы безопасности

Использование трансляторов IP/ICMP не создает каких-либо проблем безопасности в дополнение к тем, которые уже присущи IPv4 и IPv6, а также протоколам маршрутизации, применяемым для доставки пакетов транслятору.

Могут возникать проблемы, связанные с определением адресов IPv4 по адресам IPv6, - в частности появление адресов типа широковещательных или петлевых, а также наличие не преобразуемых в IPv4 адресов IPv6 и т. п. Эти вопросы рассмотрены в [RFC6052].

IPsec Authentication Header [RFC4302] не может применяться с NAT44 или NAT64.

Как и при трансляции адресов IPv4, пакеты ESP[2] могут быть преобразованы, поскольку туннельный режим ESP не зависит от полей заголовков, расположенных перед заголовком ESP. Однако в транспортном режиме ESP трансляция из IPv6 в IPv4 будет приводить к отказам, если не используются «нейтральные к контрольным суммам адреса»

[1]Packetization Layer Path MTU Discovery — определение MTU на уровне пакетизации.
[2]Encapsulating Security Payload — инкапсулированные защищенные данные.

(checksum-neutral addresses). В обоих случаях конечные точки IPsec ESP обычно могут обнаруживать присутствие транслятора и инкапсулировать ESP в пакеты UDP [RFC3948].

9. Литература

9.1. Нормативные документы

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, DOI 10.17487/RFC0768, August 1980, <http://www.rfc-editor.org/info/rfc768>.

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <http://www.rfc-editor.org/info/rfc791>.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <http://www.rfc-editor.org/info/rfc793>.

[RFC1812] Baker, F., Ed., "Requirements for IP Version 4 Routers", RFC 1812, DOI 10.17487/RFC1812, June 1995, <http://www.rfc-editor.org/info/rfc1812>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, DOI 10.17487/RFC3948, January 2005, <http://www.rfc-editor.org/info/rfc3948>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, DOI 10.17487/RFC4340, March 2006, <http://www.rfc-editor.org/info/rfc4340>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, DOI 10.17487/RFC4443, March 2006, <http://www.rfc-editor.org/info/rfc4443>.

[RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, DOI 10.17487/RFC4884, April 2007, <http://www.rfc-editor.org/info/rfc4884>.

[RFC5382] Guha, S., Ed., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, "NAT Behavioral Requirements for TCP", BCP 142, RFC 5382, DOI 10.17487/RFC5382, October 2008, <http://www.rfc-editor.org/info/rfc5382>.

[RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", BCP 51, RFC 5771, DOI 10.17487/RFC5771, March 2010, <http://www.rfc-editor.org/info/rfc5771>.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, DOI 10.17487/RFC6052, October 2010, <http://www.rfc-editor.org/info/rfc6052>.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, DOI 10.17487/RFC6145, April 2011, <http://www.rfc-editor.org/info/rfc6145>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <http://www.rfc-editor.org/info/rfc6146>.

[RFC6791] Li, X., Bao, C., Wing, D., Vaithianathan, R., and G. Huston, "Stateless Source Address Mapping for ICMPv6 Packets", RFC 6791, DOI 10.17487/RFC6791, November 2012, <http://www.rfc-editor.org/info/rfc6791>.

[RFC7757] Anderson, T. and A. Leiva Popper, "Explicit Address Mappings for Stateless IP/ICMP Translation", RFC 7757, DOI 10.17487/RFC7757, February 2016, <http://www.rfc-editor.org/info/rfc7757>.

9.2. Дополнительная литература

[ATOMIC] Gont, F., LIU, S., and T. Anderson, "Generation of IPv6 Atomic Fragments Considered Harmful", Work in Progress, draft-ietf-6man-deprecate-atomfrag-generation-06[1], April 2016.

[Err3059] RFC Errata, Erratum ID 3059, RFC 6145.

[Err3060] RFC Errata, Erratum ID 3060, RFC 6145.

[Err3061] RFC Errata, Erratum ID 3061, RFC 6145.

[Err4090] RFC Errata, Erratum ID 4090, RFC 6145.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", Work in Progress, draft-ietf-6man-rfc2460bis-04, March 2016.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, DOI 10.17487/RFC1191, November 1990, <http://www.rfc-editor.org/info/rfc1191>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", ,RFC 2474 DOI 10.17487/RFC2474, December 1998, <http://www.rfc-editor.org/info/rfc2474>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, DOI 10.17487/RFC2475, December 1998, <http://www.rfc-editor.org/info/rfc2475>.

[1]Работа опубликована в RFC 8021. *Прим. перев.*

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <http://www.rfc-editor.org/info/rfc2710>.

[RFC2923] Lahey, K., "TCP Problems with Path MTU Discovery", RFC 2923, DOI 10.17487/RFC2923, September 2000, <http://www.rfc-editor.org/info/rfc2923>.

[RFC3307] Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", RFC 3307, DOI 10.17487/RFC3307, August 2002, <http://www.rfc-editor.org/info/rfc3307>.

[RFC3590] Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, DOI 10.17487/RFC3590, September 2003, <http://www.rfc-editor.org/info/rfc3590>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <http://www.rfc-editor.org/info/rfc3810>.

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, DOI 10.17487/RFC3849, July 2004, <http://www.rfc-editor.org/info/rfc3849>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <http://www.rfc-editor.org/info/rfc4302>.

[RFC4787] Audet, F., Ed. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, DOI 10.17487/RFC4787, January 2007, <http://www.rfc-editor.org/info/rfc4787>.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <http://www.rfc-editor.org/info/rfc4821>.

[RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, DOI 10.17487/RFC5737, January 2010, <http://www.rfc-editor.org/info/rfc5737>.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, DOI 10.17487/RFC6144, April 2011, <http://www.rfc-editor.org/info/rfc6144>.

[RFC6219] Li, X., Bao, C., Chen, M., Zhang, H., and J. Wu, "The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the Ipv4/IPv6 Coexistence and Transition", RFC 6219, DOI 10.17487/RFC6219, May 2011, <http://www.rfc-editor.org/info/rfc6219>.

[RFC6691] Borman, D., "TCP Options and Maximum Segment Size (MSS)", RFC 6691, DOI 10.17487/RFC6691, July 2012, <http://www.rfc-editor.org/info/rfc6691>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <http://www.rfc-editor.org/info/rfc7136>.

[RFC7599] Li, X., Bao, C., Dec, W., Ed., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", RFC 7599, DOI 10.17487/RFC7599, July 2015, <http://www.rfc-editor.org/info/rfc7599>.

Приложение A. Пример трансляции без учета состояний

Пример трансляции без учета состояний показан на рисунке. В примере используются адреса из блоков, предназначенных для документации 2001:db8::/32 [RFC3849], 192.0.2.0/24 и 198.51.100.0/24 [RFC5737].

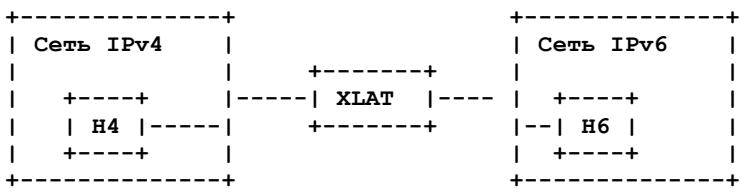

Рисунок 8. Трансляция без учета состояний.

Транслятор (XLAT) соединяет сеть IPv6 с сетью IPv4. XLAT использует префикс NSP[1] 2001:db8:100::/40, определенный в [RFC6052], для представления адресов IPv4 в адресном пространстве IPv6 (преобразованные в IPv4 адреса) и для представления адресов IPv6 (транслируемые в IPv4 адреса) в адресном пространстве IPv4. В этом примере блок адресов 192.0.2.0/24 соответствует преобразуемым в IPv4 адресам.

На основе правила отображения адресов узел IPv6 H6 имеет преобразуемый в IPv4 адрес IPv6 2001:db8:1c0:2:21:: (отображение для адреса 192.0.2.33). Узел IPv4 H4 имеет адрес 198.51.100.2.

Маршрутизация IPv6 настроена так, что пакеты IPv6, адресованные получателям из блока 2001:db8:100::/40, пересылаются на интерфейс IPv6 транслятора XLAT.

Маршрутизация IPv4 настроена так, что пакеты IPv4, адресованные получателям из блока 192.0.2.0/24, пересылаются на интерфейс IPv4 транслятора XLAT.

A.1. H6 организует связь с H4

Узел H6 организует связь с узлом H4.

1. H6 выполняет отображение адресов так, что преобразуемый в IPv4 адрес 2001:db8:1c6:3364:2:: формируется из 198.51.100.2 с использованием алгоритма отображения [RFC6052].
2. H6 передает пакет узлу H4. Пакет отправляется с адреса 2001:db8:1c0:2:21:: по адресу 2001:db8:1c6:3364:2::.
3. Пакет пересылается на интерфейс IPv6 транслятора XLAT (в соответствии с маршрутизацией IPv6).

[1]Network-Specific Prefix — специфический для сети префикс.

4. XLAT принимает пакет и выполняет трансляцию:
   - заголовок IPv6 преобразуется в заголовок IPv4 с использованием алгоритма IP/ICMP Translation Algorithm, определенного в этом документе;
   - XLAT указывает 192.0.2.33 в качестве адреса отправителя пакета, а 198.51.100.2 — в качестве адреса получателя. Отметим, что адреса 192.0.2.33 и 198.51.100.2 напрямую извлекаются из адреса отправителя IPv6 2001:db8:1c0:2:21:: (транслируемый в IPv4 адрес) и получателя IPv6 2001:db8:1c6:3364:2:: (преобразованный в IPv4 адрес) в принятом для трансляции пакете.
5. XLAT передает транслированный пакет через свой интерфейс IPv4 и пакет прибывает на узел H4.
6. H4 отвечает на принятый пакет своим пакетом с адресом получателя 192.0.2.33 и адресом отправителя 198.51.100.2.
7. Пакет пересылается на интерфейс IPv4 транслятора XLAT (в соответствии с маршрутизацией IPv4). XLAT выполняет трансляцию:
   - заголовок IPv4 преобразуется в заголовок IPv6 с использованием алгоритма IP/ICMP Translation Algorithm, определенного в этом документе;
   - XLAT указывает 2001:db8:1c0:2:21:: в качестве адреса получателя, а 2001:db8:1c6:3364:2:: - в качестве адреса отправителя преобразованного пакета. Отметим, что адреса 2001:db8:1c0:2:21:: и 2001:db8:1c6:3364:2:: формируются непосредственно из адресов IPv4 для получателя (192.0.2.33) и отправителя (198.51.100.2) в заголовке принятого для трансляции пакета.
8. Транслированный пакет передается через интерфейс IPv6 узлу H6.

Обмен пакетами между узлами H6 и H4 продолжается до завершения сессии.

A.2. H4 организует связь с H6

Узел H4 организует связь с узлом H6.

1. H4 выполняет отображение для адреса получателя так, что формируется адрес 192.0.2.33 из транслируемого в IPv4 адреса 2001:db8:1c0:2:21:: на основе алгоритма отображения адресов [RFC6052].
2. H4 отправляет пакет узлу H6. Пакет передается с адреса 198.51.100.2 по адресу 192.0.2.33.
3. Пакет приходит на интерфейс IPv4 транслятора XLAT (в соответствии с маршрутизацией IPv4).
4. XLAT принимает пакет и выполняет трансляцию:
   - заголовок IPv4 преобразуется в заголовок IPv6 с использованием алгоритма IP/ICMP Translation Algorithm, определенного в этом документе;
   - XLAT включает в пакет адрес отправителя 2001:db8:1c6:3364:2:: и адрес получателя 2001:db8:1c0:2:21::. Отметим, что адреса 2001:db8:1c6:3364:2:: (преобразованный в IPv4 адрес) и 2001:db8:1c0:2:21:: (транслируемый в IPv4 адрес) получаются непосредственно из адресов IPv4 для отправителя (198.51.100.2) и получателя (192.0.2.33) из заголовка транслируемого пакета IPv4.
5. XLAT передает пакет через интерфейс IPv6 и пакет прибывает на узел H6.
6. Узел H6 отвечает на принятый пакет своим пакетом с адресом получателя 2001:db8:1c6:3364:2:: и адресом отправителя 2001:db8:1c0:2:21::.
7. Пакте пересылается на интерфейс IPv6 транслятора XLAT (в соответствии с маршрутизацией IPv6). XLAT выполняет трансляцию:
   - заголовок IPv6 преобразуется в IPv4 с использованием алгоритма IP/ICMP Translation Algorithm, определенного в этом документе;
   - XLAT указывает адрес получателя 198.51.100.2 и адрес отправителя 192.0.2.33. Отметим, что адреса 198.51.100.2 и 192.0.2.33 формируются непосредственно из адресов получателя IPv6 2001:db8:1c6:3364:2:: и отправителя IPv6 2001:db8:1c0:2:21:: в заголовке транслируемого пакета IPv6.
8. Транслированный пакет передается через интерфейс IPv4 узлу H4.

Обмен пакетами между узлами H4 и H6 продолжается до завершения сессии.

Благодарности

Gandhar Gokhale, Wesley Eddy и Fernando Gont отметили ошибки и обработали их [RFC6145]. Fernando Gont, Will (Shucheng) Liu и Tore Anderson выполнили анализ безопасности и предложили обновления, относящиеся к атомарным фрагментам. В дополнение к этому Tore Anderson и Alberto Leiva предложили алгоритм EAM[1].

Адреса авторов

Congxiao Bao
CERNET Center/Tsinghua University
Room 225, Main Building, Tsinghua University
Beijing 100084
China
Phone: +86 10-62785983
Email: congxiao@cernet.edu.cn

[1]Explicit Address Mapping — явное отображение адресов.

Xing Li
CERNET Center/Tsinghua University
Room 225, Main Building, Tsinghua University
Beijing 100084
China
Phone: +86 10-62785983
Email: xing@cernet.edu.cn

Fred Baker
Cisco Systems
Santa Barbara, California 93117
United States
Phone: +1-408-526-4257
Email: fred@cisco.com

Tore Anderson
Redpill Linpro
Vitaminveien 1A
0485 Oslo
Norway
Phone: +47 959 31 212
Email: tore@redpill-linpro.com
URI: http://www.redpill-linpro.com

Fernando Gont
Huawei Technologies
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina
Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru