

Network Working Group
Request for Comments: 4443
Obsoletes: 2463
Updates: 2780
Category: Standards Track

A. Conta
Transwitch
S. Deering
Cisco Systems
M. Gupta, Ed.
Tropos Networks
March 2006

Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

Спецификация протокола управляющих сообщений (ICMPv6) для IPv6

Статус документа

В этом документе приведена спецификация проекта стандартного протокола Internet. Документ служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущий статус стандартизации протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Документ может распространяться без ограничений.

Авторские права

Copyright (C) The Internet Society (2006).

Аннотация

В этом документе описан формат набора управляющих сообщений, используемых в протоколе ICMPv6 (Internet Control Message Protocol), служащем протоколом управляющих сообщений для IPv6.

Оглавление

1. Введение.....	1
2. ICMPv6 (ICMP для IPv6).....	2
2.1. Базовый формат сообщения.....	2
2.2. Определение адреса отправителя для сообщения.....	2
2.3. Расчёт контрольной суммы сообщения.....	3
2.4. Правила обработки сообщений.....	3
3. Сообщения ICMPv6 об ошибках.....	4
3.1. Destination Unreachable.....	4
3.2. Packet Too Big.....	4
3.3. Time Exceeded.....	5
3.4. Parameter Problem.....	5
4. Информационные сообщения ICMPv6.....	6
4.1. Echo Request.....	6
4.2. Echo Reply.....	6
5. Вопросы безопасности.....	7
5.1. Проверка подлинности и конфиденциальность сообщений ICMP.....	7
5.2. Атаки на ICMP.....	7
6. Взаимодействие с IANA.....	8
6.1. Процедура выделения новых значений ICMPV6 Type и Code.....	8
6.2. Выделенные значения.....	8
7. Литература.....	8
7.1. Нормативные документы.....	8
7.2. Дополнительная литература.....	8
8. Благодарности.....	9
Приложение А. Отличия от RFC 2463.....	9

1. Введение

Протокол Internet версии 6 (IPv6) использует протокол управляющих сообщений (Internet Control Message Protocol или ICMP), определённый для IPv4 [RFC-792], с множеством изменений. Полученный в результате протокол назван ICMPv6 и использует значение IPv6 Next Header 58.

В этом документе описан формат набора управляющих сообщений, применяемых в ICMPv6. Документ не включает процедуры использования сообщений для решения задач, подобных Path MTU, которые описываются в отдельных документах (например, [PMTU]). В других документах могут также добавляться типы сообщений ICMPv6, такие как Neighbor Discovery [IPv6-DISDISC], в соответствии с базовыми правилами для сообщений ICMPv6, приведёнными в разделе 2 этого документа.

В документе используются термины, определённые в спецификации протокола IPv6 [IPv6] и спецификации адресации и маршрутизации IPv6 [IPv6-ADDR].

Этот документ отменяет действие RFC 2463 [RFC-2463] и обновляет RFC 2780 [RFC-2780].

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

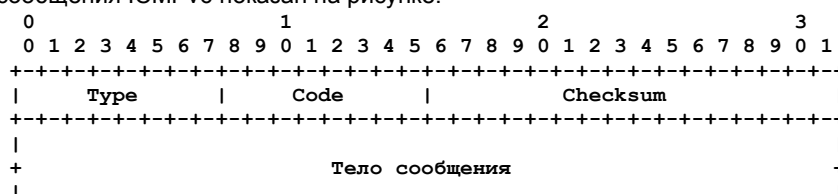
2. ICMPv6 (ICMP для IPv6)

ICMPv6 применяется узлами IPv6 для информирования об ошибках при обработке пакетов и решения других задач сетевого уровня, таких как диагностика (ICMPv6 ping). Протокол ICMPv6 является частью IPv6 и базовый протокол (все сообщения и поведение, описанные в этой спецификации) **должны** полностью поддерживаться узлом IPv6.

2.1. Базовый формат сообщения

Каждое сообщение ICMPv6 имеет заголовок IPv6 и может включать заголовки расширения IPv6. Заголовок ICMPv6 указывается значением Next Header = 58 непосредственно перед сообщением (это отличается от значения, используемого в ICMP для IPv4).

Базовый формат сообщения ICMPv6 показан на рисунке.



Поле Type указывает тип сообщения и определяет формат оставшейся части сообщения, поле Code зависит от типа сообщения и позволяет задать дополнительный уровень детализации. Поле Checksum служит для обнаружения повреждений в сообщении ICMPv6 и частях заголовка IPv6.

Сообщения ICMPv6 делятся на два класса - информационные и сообщения об ошибках. Ошибки указываются значением 0 в первом бите поля Type, т. е. типами от 0 до 127, а информационные сообщения имеют тип 128 - 255.

В этом документе определены форматы для перечисленных ниже сообщений ICMPv6.

Сообщения ICMPv6 об ошибках:

- 1 Destination Unreachable (адресат недоступен, параграф 3.1);
- 2 Packet Too Big (пакет слишком велик, параграф 3.2);
- 3 Time Exceeded (срок действия истёк, параграф 3.3);
- 4 Parameter Problem (проблема с параметрами, параграф 3.4);
- 100 Private experimentation (частные эксперименты);
- 101 Private experimentation (частные эксперименты);
- 127 Резерв для расширения сообщений ICMPv6 об ошибках.

Информационные сообщения ICMPv6:

- 128 Echo Request (запрос эхо, параграф 4.1);
- 129 Echo Reply (эхо-отклик, параграф 4.2);
- 200 Private experimentation (частные эксперименты);
- 201 Private experimentation (частные эксперименты);
- 255 Резерв для расширения информационных сообщений ICMPv6.

Типы 100, 101, 200, 201 зарезервированы для частных экспериментов и не могут применяться для общего пользования. Предполагается возможность одновременного проведения множества экспериментов с этими типами. Для любого широкомасштабного или неконтролируемого использования следует получать код в соответствии с разделом 6.

Значения 127 и 255 зарезервированы для будущего расширения диапазонов при возникновении нехватки. Детали расширения оставлены на будущее. Одним из возможных вариантов, не вызывающих проблем с имеющимися реализациями, является использование для нового назначения для нового значения с типом 127 или 255 поля кода. Имеющиеся реализации будут игнорировать новые назначения, как описано в п. (b) параграфа 2.4. Новые сообщения, использующие эти расширенные типы, могут использовать в качестве кода поля в теле сообщения.

В разделах 3 и 4 описан формат сообщений ICMPv6 об ошибках с типами 1 - 4 и информационных сообщений типов 128 и 129.

Включение в сообщение ICMPv6 об ошибке по меньшей мере начальной части вызвавшего ошибку пакета позволяет создателю этого пакета идентифицировать протокол вышележащего уровня и приложение, передавшее пакет.

2.2. Определение адреса отправителя для сообщения

Создающий сообщение ICMPv6 узел определяет адреса отправителя и получателя в заголовке IPv6 до расчёта контрольной суммы. Если у узла более 1 индивидуального адреса, он **должен** выбирать Source Address в соответствии с приведёнными ниже правилами.

- (a) Если сообщение является откликом на сообщение, направленное по индивидуальному адресу узла, поле Source Address в отклике **должно** содержать этот адрес.

(b) Если сообщение является откликом на сообщение, направленное по любому другому адресу, такому как:

- групповой адрес (multicast);
- универсальный адрес (anycast), имеющийся на узле;
- индивидуальный адрес, не относящийся к узлу,

поле Source Address в пакете ICMPv6 **должно** содержать индивидуальный адрес, относящийся к узлу. Этот адрес **следует** выбирать по правилам, которые применяются для выбора адреса в других пакетах от данного узла с учётом получателя пакета. Однако адрес **можно** выбрать иным способом, обеспечивающим более информативный выбор адреса, доступного для получателя пакета ICMPv6.

2.3. Расчёт контрольной суммы сообщения

Контрольная сумма представляет собой 16-битовое дополнение до 1 суммы дополнений до 1 всего сообщения ICMPv6, начиная с поля типа ICMPv6, с добавлением перед ним полей псевдозаголовка IPv6 в соответствии с параграфом 8.1 [IPv6]. Используемое в псевдозаголовке поле Next Header имеет значение 58 (включение псевдозаголовка в контрольную сумму ICMPv6 отличается от IPv4, см. обоснование в [IPv6]).

При расчёте контрольной суммы значение поля контрольной суммы принимается нулевым.

2.4. Правила обработки сообщений

При обработке сообщений ICMPv6 реализации **должны** соблюдать приведённые ниже правила (из [RFC-1122]).

- (a) При получении адресатом сообщения ICMPv6 об ошибке неизвестного типа оно **должно** передаваться процессу вышележащего уровня, создавшему связанный с ошибкой пакет, если этот процесс можно определить (параграф 2.4, (d)).
- (b) При получении информационного сообщения ICMPv6 неизвестного типа оно **должно** отбрасываться.
- (c) Каждое сообщение ICMPv6 об ошибке (тип < 128) **должно** включать как можно большую часть вызвавшего ошибку пакета IPv6 с учётом минимального значения IPv6 MTU [IPv6] на пути передачи.
- (d) В случаях, когда от протокола сетевого уровня требуется передать сообщение ICMPv6 об ошибке процессу вышележащего уровня, протокол вышележащего уровня извлекается из исходного пакета (в теле сообщения ICMPv6) и используется для выбора подходящего процесса вышележащего уровня для обработки ошибки.

Если тип протокола вышележащего уровня невозможно узнать из сообщения ICMPv6, это сообщение отбрасывается после обработки на уровне IPv6. Одним из примеров служит сообщение ICMPv6, включающее слишком много заголовков расширения и не включающее тип вышележащего протокола в соответствии с ограничением IPv6 MTU [IPv6]. Другим примером является сообщение ICMPv6 с расширением ESP, из которого невозможно расшифровать исходный пакет по причине отсечки или недоступности требуемого для расшифровки состояния.

- (e) **Недопустимо** генерировать сообщения ICMPv6 об ошибках в результате получения:

(e.1) сообщения ICMPv6 об ошибке;

(e.2) сообщения ICMPv6 Redirect [IPv6-DISC];

(e.3) пакета, направленного по групповому адресу IPv6 (здесь имеется 2 исключения: (1) сообщение Packet Too Big (параграф 3.2), позволяющее использовать групповые сообщения при определении Path MTU и (2) Parameter Problem с кодом 2 (параграф 3.4), указывающее нераспознанную опцию IPv6 (см. параграф 4.2 в [IPv6]), имеющую в 2 старших битах Option Type значение 10);

(e.4) пакета, переданного по групповому адресу канального уровня (с исключениями из п. e.3);

(e.5) пакета, переданного по широковещательному адресу канального уровня (с исключениями из п. e.3);

(e.6) пакета, в котором адрес отправителя не указывает один узел, например, IPv6 Unspecified Address, групповой адрес IPv6 или адрес, который создатель сообщения ICMP считает универсальным (anycast).

- (f) Для снижения расхода пропускной способности и затрат на пересылку, связанных с отправкой сообщений ICMPv6 об ошибках, узел IPv6 **должен** ограничивать частоту отправки сообщений ICMPv6 об ошибках. Это может потребоваться, когда источник потока ошибочных пакетов не учитывает принятые сообщения ICMPv6. Ограничение частоты передачи сообщений ICMP выходит за рамки этой спецификации.

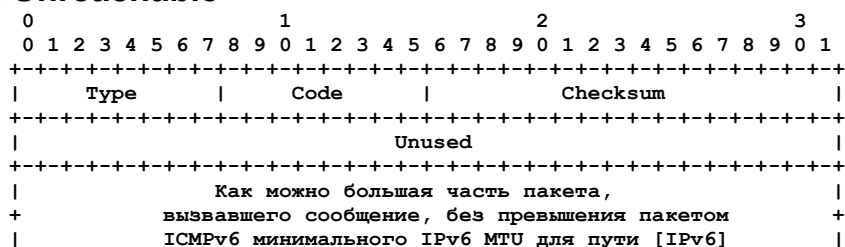
Рекомендуется контроль частоты передачи с помощью «ведра маркеров» (token bucket), ограничивающего среднюю скорость передачи значением N в пакетах за секунду или доле пропускной способности выходного канала, но разрешающего передачу до B сообщений разом при условии соблюдения средней скорости. Механизмы, не способные контролировать пики трафика (например, traceroute), не рекомендуются. Например, неразумно применять простое ограничение по таймеру, разрешающее передавать сообщение об ошибке каждые T мсек (даже при малых значениях T). Параметры ограничения скорости **следует** делать настраиваемыми. В случае реализации token-bucket принятые по умолчанию значения зависят от места развёртывания реализации (маршрутизатор или хост). Например, для небольшого устройства можно установить B=10, N=10/сек.

Примечание. Ограничения (e) и (f) имеют преимущество перед другими ограничениями, заданными в этом документе для генерации сообщений ICMP об ошибках.

В следующих параграфах описаны форматы упомянутых выше сообщений ICMPv6.

3. Сообщения ICMPv6 об ошибках

3.1. Destination Unreachable



Поля IPv6.

Destination Address

Копируется из поля Source Address вызвавшего сообщение пакета.

Поля ICMPv6.

Type

1

Code

- 0 - нет маршрута к получателю;
- 1 - связь с адресатом административно запрещена;
- 2 - выход за пределы области действия адреса отправителя;
- 3 - адрес недоступен;
- 4 - порт недоступен;
- 5 - адрес отправителя не соответствует правилам на входе или выходе;
- 6 - отвергнут маршрут к адресату.

Unused

Поле не используется для кодов, должно устанавливаться в 0 отправителем и игнорироваться получателем.

Сообщения Destination Unreachable **следует** создавать маршрутизаторам или уровню IPv6 у отправителя в ответ на пакет, который не может быть доставлен адресату по причинам, не связанным с перегрузкой (сообщения ICMPv6 **недопустимо** передавать для пакетов, отброшенных в результате перегрузки).

Если причиной отказа служит отсутствие соответствующей записи в таблице маршрутизации пересылающего узла, устанавливается Code = 0 (это может происходить лишь на узлах без принятой по умолчанию записи в таблице маршрутов). Если причиной служит административный запрет (например, фильтр в межсетевом экране), устанавливается Code = 1.

Если причиной отказа является нахождение получателя за пределами действия адреса отправителя, устанавливается Code = 2. Область действия адреса получателя определяется областью действия адреса и приёмного интерфейса для пакета, как указано в разделе 9 [IPv6-SCOPE]. Область действия адреса отправителя также определяется адресом и интерфейсом. Это условие может возникнуть, когда передача пакета на выбранный интерфейс next-hop выводит пакет за пределы действия адреса отправителя¹.

Если причину отказа невозможно связать ни с одним кодом, устанавливается Code = 3. Примером таких случаев является невозможность преобразовать адрес получателя IPv6 в соответствующий адрес канального уровня или иные проблемы, связанные с каналом. Одной из конкретных ситуаций создания сообщения Destination Unreachable с кодом 3 является отклик на пакет, принятый маршрутизатором из канала «точка-точка» и предназначенный для получателя в подсети, относящейся к тому же каналу, но не приёмному интерфейсу маршрутизатора. В этом случае пакет **недопустимо** пересылать обратно в канал.

Получателю **следует** передать сообщение Destination Unreachable с Code = 4 в ответ на пакет, для которого транспортный протокол (например, UDP) не прослушивает заданный порт, если у этого протокола нет иных способов информировать отправителя.

Если причиной отказа является несоответствие адреса отправителя правилам фильтрации на входе или выходе, в сообщении указывается Code = 5. Если причина отказа заключается в том, что маршрут к получателю отвергнут, устанавливается Code = 6. Это может быть результатом ошибочной настройки отклонения маршрутов к определённому префиксу. Коды 5 и 6 являются более конкретными вариантами кода 1.

Из соображений безопасности реализациям **следует** разрешать отключение отправки сообщения ICMP о недоступности адресата (предпочтительно на уровне интерфейса).

Уведомление вышележащего уровня

Узел, получивший сообщение ICMPv6 Destination Unreachable, **должен** уведомить процесс вышележащего уровня, если этот процесс можно определить (параграф 2.4, (d)).

3.2. Packet Too Big

Поля IPv6.

¹В оригинале текст этого абзаца содержал неточности. См. <https://www.rfc-editor.org/errata/eid6153>. Прим. перев.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Code										Checksum																			
										MTU																													
										Как можно большая часть пакета,										вызвавшего сообщение, без превышения пакетом																			
										ICMPv6 минимального IPv6 MTU для пути [IPv6]																													

Destination Address

Копируется из поля Source Address вызвавшего сообщение пакета.

Поля ICMPv6.

Type

2

Code

Устанавливается в 0 отправителем и игнорируется получателем.

MTU

Максимальный размер передаваемого блока в канале к следующему узлу пересылки или получателю (next-hop). Сообщение Packet Too Big **должен** передавать маршрутизатор в ответ, на пакет который он не может переслать по причине превышения MTU на исходящем канале. Информация из таких сообщений служит для определения MTU на пути (Path MTU Discovery) [PMTU].

Отправка сообщений Packet Too Big является исключением из приведённых выше правил для сообщений ICMPv6 об ошибках. В отличие от других сообщений они передаются для пакетов, направленных по групповым адресам получателей IPv6, а также групповым и широковещательным адресам канального уровня.

Уведомление вышележащего уровня

Входящее сообщение Packet Too Big **должно** передаваться соответствующему процессу вышележащего уровня, если его можно определить (параграф 2.4, (d)).

3.3. Time Exceeded

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										Code										Checksum																			
																				Unused																			
										Как можно большая часть пакета,										вызвавшего сообщение, без превышения пакетом																			
										ICMPv6 минимального IPv6 MTU для пути [IPv6]																													

Поля IPv6.

Destination Address

Копируется из поля Source Address вызвавшего сообщение пакета.

Поля ICMPv6.

Type

3

Code

0 - достигнут предел узлов пересылки (Hop limit);

1 - превышено время сборки фрагментов.

Unused

Поле не используется для всех кодов, должно устанавливаться в 0 отправителем и игнорироваться получателем. Если маршрутизатор получает пакет с Hop Limit = 0 или декрементирует это поле до 0, он **должен** отбросить пакет и передать сообщение ICMPv6 Time Exceeded с Code = 0 для отправителя пакета. Это говорит о петле в маршрутизации или слишком малом значении Hop Limit в исходном пакете.

ICMPv6 Time Exceeded с Code = 1 служит для информирования о тайм-ауте при сборке фрагментов, как указано в параграфе 4.5 [IPv6].

Уведомление вышележащего уровня

Входящее сообщение Time Exceeded **должно** передаваться соответствующему процессу вышележащего уровня, если его можно определить (параграф 2.4, (d)).

3.4. Parameter Problem

Поля IPv6.

**Destination Address**

Копируется из поля Source Address вызвавшего сообщение пакета.

Поля ICMPv6.

Type

4

Code

- 0 - ошибка в поле заголовка;
- 1 - нераспознанный тип Next Header;
- 2 - нераспознанная опция IPv6.

Pointer

Указывает смещение октета, связанного с ошибкой в вызвавшем сообщении пакете. Указатель может выходить за пределы пакета ICMPv6, если поле с ошибкой не включено в него в силу ограничений размера сообщения ICMPv6.

Если узел IPv6, обрабатывающий пакет, обнаруживает проблему в поле заголовка IPv6 или заголовков расширения, не позволяющую полностью обработать пакет, он **должен** отбросить пакет, а также **следует** передать сообщение ICMPv6 Parameter Problem отправителю исходного пакета, указывающее тип и местоположение ошибки.

Коды 1 и 2 являются более информативными вариантами кода 0.

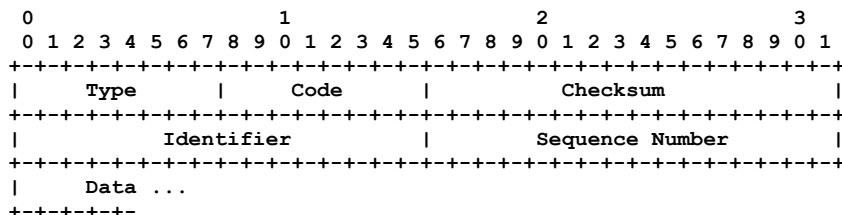
Указатель идентифицирует октет в заголовке исходного пакета, где была обнаружена ошибка. Например, сообщение ICMPv6 с Type = 4, Code = 1 и Pointer = 40 будет говорить о нераспознанном значении поля Next Header в заголовке расширения IPv6, следующем после заголовка IPv6 в исходном пакете.

Уведомление вышележащего уровня

Узел, получивший это сообщение, **должен** уведомить процесс вышележащего уровня, если этот процесс можно определить (параграф 2.4, (d)).

4. Информационные сообщения ICMPv6

4.1. Echo Request



Поля IPv6.

Destination Address

Любой действительный адрес IPv6.

Поля ICMPv6.

Type

128

Code

0

Identifier

Идентификатор, используемый для сопоставления Echo Reply с данным Echo Request. Может иметь значение 0.

Sequence Number

Порядковый номер для сопоставления Echo Reply с данным Echo Request. Может иметь значение 0.

Data

Необязательные октеты произвольных данных.

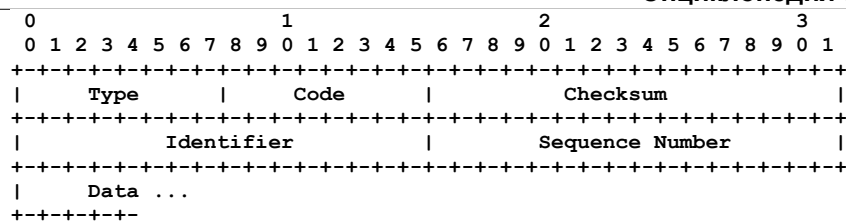
Каждый узел **должен** реализовать функцию ответа на сообщения ICMPv6 Echo Request соответствующими сообщениями Echo Reply. Узлу **следует** также реализовать интерфейс прикладного уровня для генерации Echo Request и приёма Echo Reply в целях диагностики.

Уведомление вышележащего уровня

Сообщения Echo Request **могут** передаваться процессам, обрабатывающим сообщения ICMP.

4.2. Echo Reply

Поля IPv6.

**Destination Address**

Копируется из поля Source Address в соответствующем пакете Echo Request.

Поля ICMPv6.

Type

129

Code

0

Identifier

Идентификатор из соответствующего сообщения Echo Request.

Sequence Number

Порядковый номер из соответствующего сообщения Echo Request.

Data

данные из соответствующего сообщения Echo Request.

Каждый узел **должен** реализовать функцию ответа на сообщения ICMPv6 Echo Request соответствующими сообщениями Echo Reply. Узлу **следует** также реализовать интерфейс прикладного уровня для генерации Echo Request и приёма Echo Reply в целях диагностики.

Адрес отправителя Echo Reply в ответ на индивидуальное сообщение Echo Request **должен** совпадать с адресом получателя в Echo Request.

Echo Reply **следует** передавать в ответ на сообщение Echo Request по групповому адресу IPv6 или anycast-адресу. В этом случае адресом отправителя в отклике **должен** быть индивидуальный адрес интерфейса, через который было получено сообщение Echo Request.

Данные, полученные в сообщении ICMPv6 Echo Request, **должны** полностью возвращаться без изменений в сообщении ICMPv6 Echo Reply.

Уведомление вышележащего уровня

Сообщение Echo Reply **должно** передаваться процессу, отправившему сообщение Echo Request и **может** передаваться другим процессам.

Отметим, что объем данных в Echo Request и Echo Reply не ограничивается.

5. Вопросы безопасности

5.1. Проверка подлинности и конфиденциальность сообщений ICMP

Подлинность обмена пакетами протокола ICMP можно проверить с помощью заголовка аутентификации IP (Authentication Header) [IPv6-AUTH] или заголовка IP ESP (Encapsulating Security Payload) [IPv6-ESP]. Конфиденциальность обмена пакетами ICMP можно обеспечить с помощью IP ESP [IPv6-ESP]. В [SEC-ARCH] подробно описано использование IPsec для трафика ICMP.

5.2. Атаки на ICMP

Сообщения ICMP могут подвергаться разным атакам. Полное рассмотрение этого вопроса приведено в документе IP Security Architecture [IPv6-SA], а ниже кратко рассмотрены атаки и способы их предотвращения.

1. Сообщения ICMP могут подвергаться действиям, направленным на то, чтобы получатель принял ложного отправителя за настоящего. Защитой от таких атак может быть применение механизма аутентификации IPv6 Authentication [IPv6-AUTH] для сообщений ICMP.
2. Сообщения ICMP могут подвергаться действиям, направленным на то, чтобы сообщение или ответ на него было отправлено в другое место. Защиту от таких атак можно обеспечить с помощью заголовков AH [IPv6-AUTH] или ESP [IPv6-ESP]. AH обеспечивает защиту от изменения адресов отправителя и получателя в пакете IP, а ESP не обеспечивает такой защиты, но позволяет включить адреса в контрольную сумму ICMP и защитить её. Поэтому комбинация контрольной суммы ICMP и заголовка ESP также защищает от таких атак. Защита с помощью ESP слабее защиты AH.
3. Сообщения ICMP могут подвергаться действиям, направленным на изменение полей заголовка или данных. Аутентификация [IPv6-AUTH] или шифрование [IPv6-ESP] сообщений ICMP защитят от таких атак.
4. Сообщения ICMP могут применяться для атак на службы (denial-of-service или DoS) за счёт возврата ошибочный пакетов IP. Реализация, корректно соблюдающая правило (f) из параграфа 2.4 в данной спецификации, будет защищена механизмом ограничения скорости передачи сообщений ICMP об ошибках.
5. Второе исключение из правила e.3 в параграфе 2.4 даёт злонамеренному узлу возможность вызвать DoS-атаку на источник групповой рассылки. Такой узел может отправить групповой пакет с неизвестной получателем опцией, помеченной как обязательная, и адресом отправителя IPv6, содержащим действительный групповой адрес. В результате множество получателей отправит сообщение ICMP Parameter Problem групповому источнику, вызывая DoS-атаку. Способ пересылки группового трафика multicast-маршрутизаторами требует для организации такой атаки, чтобы злонамеренный узел находился в корректном пути группового трафика, т. е. вблизи источника. Таких атак можно избежать лишь защитой группового трафика. Источнику такого трафика

следует быть осторожным при передаче групповых пакетов с пометкой опций как обязательных, поскольку это может вызвать DoS-атаку, если опцию многие получатели не поймут.

6. Сообщения ICMP передаются процессам вышележащего уровня и этим можно применить для атак на вышележащий протокол (например, TCP) с помощью ICMP [TCP-attack]. Вышележащим уровням рекомендуется применять ту или иную форму проверки сообщений ICMP (используя информацию из поля данных ICMP) до реагирования на них. Реальная проверка зависит от вышележащего уровня и выходит за рамки этого документа. Защита вышележащего уровня с помощью IPsec ослабляет такие атаки.

Сообщения ICMP об ошибках указывают проблемы, возникшие в сети при обработке дейтаграмм IP. В зависимости от конкретной ситуации сообщаемые ошибки могут (не всегда) быть устранены в ближайшем будущем. Поэтому реакция на сообщения ICMP об ошибках может зависеть не только от типа ошибки, но и от других факторов, таких как время приёма сообщения, прежние сведения об условиях в сети, а также условия работы принявшего сообщение хоста.

6. Взаимодействие с IANA

6.1. Процедура выделения новых значений ICMPV6 Type и Code

Определённый в этом документе заголовок IPv6 ICMP содержит поля Type и Code с управляемыми IANA пространствами имён. Значения кодов определяются отдельно для каждого типа.

Значения полей IPv6 ICMP Type выделяются с использованием описанных ниже процедур.

1. IANA следует выделять и регистрировать на постоянной основе новые значения типов ICMPv6 из публикаций IETF RFC. Это относится ко всем типам RFC, включая проекты стандартов, экспериментальные и информационные документы, исходящие от IETF и одобренные IESG для публикации.
2. Рабочие группы IETF по внутреннему согласованию и одобрению руководителя направления могут запрашивать возвращаемые значения для типов ICMPv6, которые IANA помечает как подлежащие возврату в будущем (reclaimable in future). Такая пометка может быть удалена при публикации RFC для протокола, как указано в п. 1, что делает выделение постоянным с обновлением ссылки на web-страницах IANA.

При заполнении пространства типов ICMPv6 на 85% IETF будет рассматривать назначения с пометкой «reclaimable in the future» и информировать IANA о возможности их возврата и повторного выделения.

3. Запросы на выделение новых типов ICMPv6 вне процессов IETF выполняются лишь путём публикации документа IETF, как указано в п. 1. Отметим, что документы со статусом RFC Editor contributions [RFC-3978], не считаются документами IETF.

Назначение новых значений Code для значений Type, определённых в этом документе, требует стандартизации и одобрения IESG. Политику назначения Code для новых IPv6 ICMP Type следует задавать в документах, определяющих новый тип.

6.2. Выделенные значения

Обновляемый список выделенных значений доступен по ссылке <http://www.iana.org/assignments/icmpv6-parameters>. Агентство IANA заново выделило для ICMPv6 типа 1 Destination Unreachable код 2, назначенный в [RFC-2463]:

2 - Beyond scope of source address

Агентство IANA выделило два новых кода для ICMPv6 типа 1 Destination Unreachable:

5 - Source address failed ingress/egress policy

6 - Reject route to destination

Агентство IANA выделило новые значения типов:

100 Private experimentation

101 Private experimentation

127 Reserved for expansion of ICMPv6 error messages

200 Private experimentation

201 Private experimentation

255 Reserved for expansion of ICMPv6 informational messages

7. Литература

7.1. Нормативные документы

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.

[IPv6-DISC] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.

[IPv6-SCOPE]¹ Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", [RFC 4007](#), March 2005.

[RFC-792] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.

[RFC-2463] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [RFC 2463](#), December 1998.

[RFC-1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, [RFC 1122](#), October 1989.

¹В оригинале эта ссылка отсутствует. См. <https://www.rfc-editor.org/errata/eid6153>. Прим. перев.

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

[RFC-3978] Bradner, S., "IETF Rights in Contributions", BCP 78, RFC 3978, March 2005.

7.2. Дополнительная литература

[RFC-2780] Bradner, S. and V. Paxson, "IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers", BCP 37, RFC 2780, March 2000.

[IPv6-ADDR] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", [RFC 3513](#), April 2003.

[PMTU] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[IPv6-SA] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.

[IPv6-AUTH] Kent, S., "IP Authentication Header", [RFC 4302](#), December 2005.

[IPv6-ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", [RFC 4303](#)¹, December 2005.

[SEC-ARCH] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[TCP-attack] Gont, F., "ICMP attacks against TCP", Work in Progress².

8. Благодарности

Документ основан на прежних публикациях по ICMP рабочих групп SIPP и IPng.

Рабочая группа IPng и, в частности, Robert Elz, Jim Bound, Bill Simpson, Thomas Narten, Charlie Lynn, Bill Fink, Scott Bradner, Dimitri Haskin, Bob Hinden, Jun-ichiro Itojun Hagino, Tatuya Jinmei, Brian Zill, Pekka Savola, Fred Templin, Elwyn Davies (в хронологическом порядке) предоставили обстоятельные рецензии и отклики.

Bob Hinden был редактором этого документа.

Приложение А. Отличия от RFC 2463

- Раздел «Аннотация» стал более подробным.
- Исправлены опечатки в параграфе 2.4, где ссылки на е.2 заменены ссылками на е.3.
- Удалены механизмы ограничения скорости передачи сообщений ICMP об ошибках на основе скорости и пропускной способности, а вместо них предложен механизм Token-bucket.
- Все сообщения ICMP об ошибках содержат в точности 32 бита зависящих от типа данных, чтобы получатель мог надёжно найти вложенную часть исходного пакета, если он не распознал тип сообщения ICMP.
- В описание сообщения Destination Unreachable с кодом Code 3 добавлено правило, запрещающее пересылку пакета обратно в канала «точка-точка», если адресат относится к тому же каналу (предотвращение «пинг-понга»).
- Добавлено описание Time Exceeded для кода 1 (тайм-аут при сборке фрагментов).
- Добавлены сообщения «beyond scope of source address», «source address failed ingress/egress policy», «reject route to destination» в группу сообщений о недоступности адресата (параграф 3.1).
- Зарезервированы типы ICMP для экспериментов.
- Добавлено примечание в параграфе 2.4, указывающее приоритет правил обработки сообщений ICMP.
- Добавлено сообщение ICMP REDIRECT в п. (е) параграфа 2.4, для случаев, когда сообщения ICMP об ошибках не создаются.
- Внесены правки в параграф 2.3 для расчёта контрольной суммы и параграф 5.2.
- В параграф 4.2 внесены разъяснения для сообщения Echo Reply в части использования индивидуального адреса отправителя откликов на anycast-запросы Echo Request, как в случае multicast.
- Пересмотрен раздел «Вопросы безопасности». Добавлено использование заголовков ESP для аутентификации. Требование для опции запрета неаутентифицированных сообщений ICMP сменено со **следует** на **можно**.
- Добавлена новая атака в список возможных атак на ICMP параграфа 5.2.
- Ссылки разделены на нормативные и дополнительные документы.
- Добавлена ссылка на RFC 2780 «IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers», а также примечание, что этот документ обновляет RFC 2780.
- Добавлена процедура выделения новых типов и кодов в раздел «Взаимодействие с IANA».
- Слово «передать» (send) заменено словом «создать» (originate), чтобы прояснить, что вопросы пересылки пакетов ICMP выходят за рамки спецификации.
- Изменены ссылки для ESP и AH на обновлённые документы.
- Добавлена ссылка на обновлённый документ IPsec Security Architecture.
- Добавлено требование **следует** в части контроля запрета отправки сообщений ICMP о недоступности адресата.

¹В оригинале ошибочно указано RFC 4203. См. <https://www.rfc-editor.org/errata/eid1918>. Прим. перев.

²Работа опубликована в RFC 5927. Прим. перев.

- Упрощён выбор адреса отправителя для пакетов ICMPv6.
- Изменён базовый формат сообщений (параграф 2.1).
- Добавлен текст об атаках на транспортные протоколы, которые можно организовать с помощью ICMP.

Адреса авторов

Alex Conta

Transwitch Corporation
3 Enterprise Drive
Shelton, CT 06484
USA
EMail: aconta@txc.com

Stephen Deering

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Mukesh Gupta, Ed.

Tropos Networks
555 Del Rey Avenue
Sunnyvale, CA 94085
Phone: +1 408-331-6889
EMail: mukesh.gupta@tropos.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

Copyright (C) The Internet Society (2006).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке <http://www.ietf.org/ipr>.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC обеспечено IETF Administrative Support Activity (IASA).