

Протокол IPv6

Формат заголовка IPv6



<i>Версия</i>	4-битный код номера версии Интернет протокола (версия Интернет протокола для IPv6= 6)
<i>Приор.</i>	4-битный код приоритета
<i>Метка потока</i>	24-битный код метки потока (для мультимедиа)
<i>Размер поля данных</i>	16-битовое число без знака. Несет в себе код длины поля данных в октетах, которое следует сразу после заголовка пакета. Если код равен нулю, то длина поля данных записана в поле данных jumbo, которое в свою очередь хранится в зоне опций.
<i>Следующий заголовок</i>	8-битовый разделитель. Идентифицирует тип заголовка, который следует непосредственно за IPv6 заголовком. Использует те же значения, что и протокол IPv4 [RFC-1700].
<i>Предельное число шагов</i>	8-битовое целое число без знака. Уменьшается на 1 в каждом узле, через который проходит пакет. При предельном числе шагов, равном нулю, пакет удаляется.
<i>Адрес отправителя</i>	128-битовый адрес отправителя пакета. См. RFC-1884.
<i>Адрес</i>	128-битовый адрес получателя пакета (возможно не конечный получатель, если

IP версия 6 архитектуры адресации

- unicast:** Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.
- anycast:** Идентификатор набора интерфейсов (принадлежащих разным узлам). Пакет, посланный по уникастному адресу, доставляется одному из интерфейсов, указанному в адресе (ближайший, в соответствии с мерой, определенной протоколом маршрутизации).
- multicast:** Идентификатор набора интерфейсов (обычно принадлежащих разным узлам). Пакет, посланный по мультикастинг-адресу, доставляется всем интерфейсам, заданным этим адресом.

В IPv6 не существует широковещательных адресов, их функции переданы мультикастинг-адресам.

В IPv6, все нули и все единицы являются допустимыми кодами для любых полей, если не оговорено исключение.

Модель адресации

IPv6 адреса всех типов ассоциируются с интерфейсами, а не узлами. Так как каждый интерфейс принадлежит только одному узлу, уникальный адрес интерфейса может идентифицировать узел.

IPv6 уникальный адрес соотносится только с одним интерфейсом. Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные). Существует два исключения из этого правила:

1. Одиночный адрес может приписываться нескольким физическим интерфейсам, если приложение рассматривает эти несколько интерфейсов как единое целое при представлении его на уровне Интернет.
2. Маршрутизаторы могут иметь нenumерованные интерфейсы (например, интерфейсу не присваивается никакого IPv6 адреса) для соединений точка-точка, чтобы исключить необходимость вручную конфигурировать и объявлять (advertise) эти адреса. Адреса не нужны для соединений точка-точка маршрутизаторов, если эти интерфейсы не используются в качестве точки отправления или назначения при посылке IPv6 дейтограмм. Маршрутизация здесь осуществляется по схеме близкой к используемой протоколом CIDR в IPv4.

IPv6 соответствует модели IPv4, где субсеть ассоциируется с каналом. Одному каналу могут соответствовать несколько субсетей.

Представление записи адресов (текстовое представление адресов)

1. Основная форма имеет вид x:x:x:x:x:x:x:x, где 'x' шестнадцатеричные 16-битовые числа.

Примеры:

fedc:ba98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

Например:

1080:0:0:0:8:800:200c:417a

уникаст-адрес

ff01:0:0:0:0:0:0:43

мультикаст адрес

0:0:0:0:0:0:0:1

адрес обратной связи

0:0:0:0:0:0:0:0

неспецифицированный адрес

Сокращенная запись:

1080::8:800:200c:417a

уникаст-адрес

ff01::43

мультикаст адрес

::1

адрес обратной связи

::

не специфицированный адрес

2. Альтернативной формой записи, которая более удобна при работе с ipv4 и IPv6, является x:x:x:x:x:x:d.d.d.d, где 'x' шестнадцатеричные 16-битовые коды адреса, а 'd' десятичные 8-битовые, составляющие младшую часть адреса (стандартное IPv4 представление). Например:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

или в сжатом виде:

::13.1.68.3

::FFFF:129.144.52

Представление типа адреса

Специфический тип IPv6 адресов идентифицируется лидирующими битами адреса. Поле переменной длины, содержащее эти лидирующие биты, называется префиксом формата (Format Prefix - FP). И

Назначение	Префикс (двоичный)	Часть адресного пространства
Зарезервировано	0000 0000	1/256
Не определено	0000 0001	1/256
Зарезервировано для NSAP	0000 001	1/128
Зарезервировано для IPX	0000 010	1/128
Не определено	0000 011	1/128
Не определено	0000 1	1/32
Не определено	0001	1/16
Объединяемые глобальные уникаст-адреса	001	1/8
Провайдерские уникаст-адреса	010	1/8
Не определено	011	1/8
Зарезервировано для географических уникаст-	100	1/8

Не определено	101	1/8
Не определено	110	1/8
Не определено	1110	1/16
Не определено	1111 0	1/32
Не определено	1111 10	1/64
Не определено	1111 110	1/128
Не определено	1111 1110 0	1/512
Локальные (на линке) канальные адреса	1111 1110 10	1/1024
Локальные адреса (site)	1111 1110 11	1/1024
Мультикаст-адреса	1111 1111	1/256

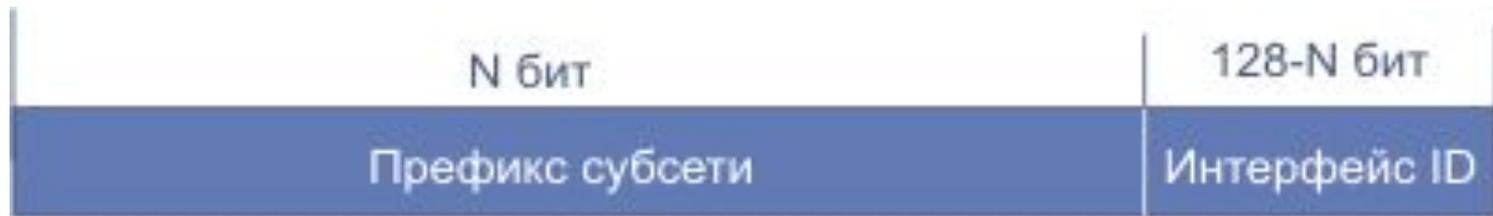
Замечание: Не специфицированные адреса, адреса обратной связи и IPv6 адреса со встроенными IPv4 адресами, определены вне “0000 0000” префиксного пространства.

Уникастные адреса отличаются от мультикастных значением старшего октета: значение FF (11111111) идентифицирует мультикастинг-адрес; любые другие значения говорят о том, что адрес уникастный. Эникастные (anycast) адреса берутся из уникастного пространства, и синтаксически неотличимы от них.

Уникастные адреса

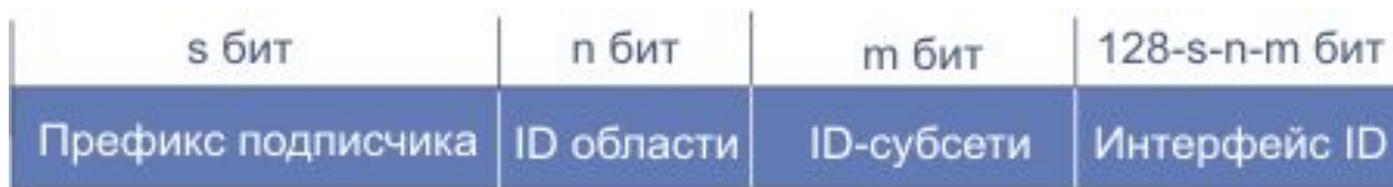
IPv6 уникастные адреса, сходны с традиционными IPv4 адресами при бесклассовой междоменной маршрутизации (Class-less InterDomain Routing - CIDR).

ЭВМ может дополнительно знать о префиксе субсети для каналов, с которыми она соединена, где различные адреса могут иметь разные значения n:



Где 48-битовый идентификатор интерфейса представляет собой IEEE-802 MAC адрес. Использование IEEE 802 mac адресов в качестве идентификаторов интерфейсов будет стандартным в среде, где узлы имеют IEEE 802 MAC адреса. В других средах, где IEEE 802 MAC адреса не доступны, могут использоваться другие типы адресов связанного уровня, такие как E.164 адреса, в качестве идентификаторов интерфейсов.

Другой формат уникастного адреса относится к случаю, когда локальная сеть или организация нуждаются в дополнительных уровнях иерархии. В этом примере идентификатор субсети делится на идентификатор области и идентификатор субсети. Формат такого адреса имеет вид:



Эта схема может быть развита с тем, чтобы позволить локальной сети или организации добавлять новые уровни внутренней иерархии. Может быть, желательно использовать идентификатор интерфейса меньше чем 48-разрядный IEEE 802 MAC адрес, с тем, чтобы оставить больше места для полей, характеризующих уровни иерархии. Это могут быть идентификаторы интерфейсов, сформированные администрацией локальной сети или организации.

Не специфицированный адрес

Адрес 0:0:0:0:0:0:0:0 называется не специфицированным адресом. Он не должен присваиваться какому-либо узлу. Этот адрес указывает на отсутствие адреса.

Примером использования такого адреса может служить поле адреса отправителя любой IPv6 дейтограммы, посланной инициализируемой ЭВМ до того, как она узнала свой адрес.

Не специфицированный адрес не должен использоваться в качестве указателя места назначения IPv6 дейтограмм или в IPv6 заголовках маршрутизации.

Адрес обратной связи

Уникальный адрес 0:0:0:0:0:0:0:1 называется адресом обратной связи. Он может использоваться для отправки IPv6 дейтограмм самому себе.

Его нельзя использовать в качестве идентификатора интерфейса.

Адрес обратной связи не должен применяться в качестве адреса отправителя в IPv6 дейтограммах, которые посылаются за пределы узла.

IPv6 дейтограмма с адресом обратной связи в качестве адреса места назначения не может быть послана за пределы узла.

IPv6 адреса с вложенными IPv4 адресами

Алгоритмы IPv6 включают в себя механизм (для ЭВМ и маршрутизаторов) организации туннелей для IPv6 пакетов через маршрутную инфраструктуру IPv4. Узлам IPv6, которые используют этот метод, присваиваются специальные IPv6 уникастные адреса, которые в младших 32 битах содержат адрес IPv4. Этот тип адреса называется "IPv4-compatible IPv6 address" и имеет формат, изображенный на рис. :

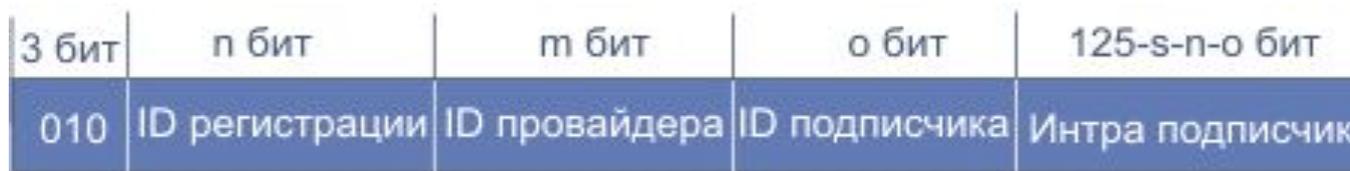


Определен и второй тип IPv6 адреса, который содержит внутри IPv4 адрес. Этот адрес используется для представления IPv6 адресов узлам IPv4 (тем, что не поддерживают IPv6). Этот тип адреса называется "IPv4-mapped IPv6 address" и имеет формат показанный на рис. :



Провайдерские глобальные уникаст-адреса

Глобальный уникаст-адрес провайдера имеет назначение, описанное в [ALLOC]. Исходное назначение этих уникаст-адресов аналогично функции IPv4 адресов в схеме CIDR [см. CIDR]. Глобальный IPv6 уникаст-адрес провайдера имеет формат, отображенный ниже на рис. :



Старшая часть адреса предназначена для определения того, кто определяет часть адреса провайдера, подписчика и т.д.

Идентификатор регистрации определяет регистратора, который задает провайдерскую часть адреса. Термин "префикс регистрации" относится к старшей части адреса, включая поле идентификатор регистрации (ID).

Идентификатор провайдера задает специфического провайдера, который определяет часть адреса подписчика. Термин "префикс провайдера" относится к старшей части адреса включая идентификатора провайдера.

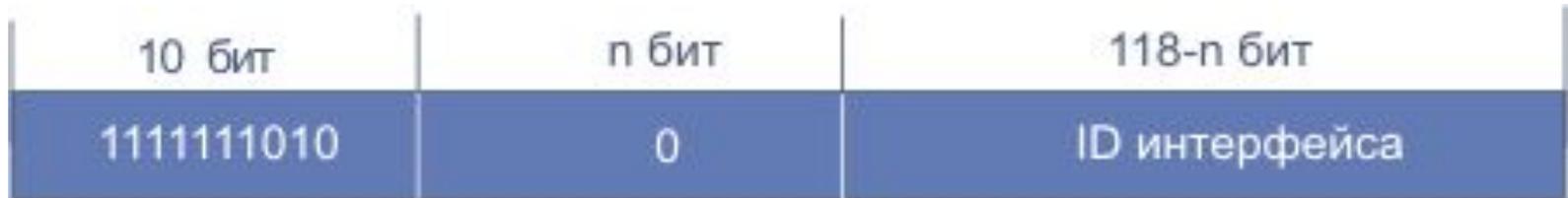
Идентификатор подписчика позволяет разделить подписчиков, подключенных к одному и тому же провайдеру. Термин "префикс подписчика" относится к старшей части адреса, включая идентификатор подписчика.

Часть адреса *интра-подписчик* определяется подписчиком и организована согласно местной топологии Интернет подписчика. Возможно, что несколько подписчиков пожелают использовать область адреса *интра-подписчик* для одной и той же субсети и интерфейса. В этом случае идентификатор субсети определяет специфический физический канал, а идентификатор интерфейса - определенный интерфейс субсети.

Локальные уникаст-адреса IPv6

Существует два типа уникастных адресов локального использования. Имеются локальные адреса сети и канала. Локальный адрес канала предназначен для работы с одним каналом, а локальный адрес сети - с одной локальной сетью (site).

Локальный IPv6 уникаст-адрес канала имеет формат, отображенный ниже на рис.



Локальные адреса канала предназначены для обращения через определенный канал, например, для целей авто-конфигурации адресов, поиска соседей или в случае отсутствия маршрутизатора. Маршрутизаторы не должны переадресовывать пакеты с локальными адресами отправителя.

Локальный адрес сети

10 бит	n бит	m бит	118-n-m бит
1111111011	0	ID субсети	ID интерфейса

Локальные адреса сети могут использоваться для локальных сетей или организаций, которые (пока еще) не подключены к глобальному Интернет. Им не нужно запрашивать или “красть” префикс адреса из глобального адресного пространства Интернет. Вместо этого можно использовать локальный адрес сети IPv6. Когда организация соединяется с глобальным Интернет, она может сформировать глобальные адреса путем замещения локального префикса сети префиксом подписчика.

Маршрутизаторы не должны переадресовывать пакеты с локальными адресами сети отправителя.

Unicast адреса IPv6

1111111010	Все нули	Номер интерфейса
------------	----------	------------------

Локальный на линке IPv6 адрес

1111111011	Все нули	Номер подсети	Номер интерфейса
------------	----------	---------------	------------------

Локальный на сайте IPv6 адрес

001	TLA	RES	NLA	Номер подсети	Номер интерфейса
-----	-----	-----	-----	---------------	------------------

Глобальный unicast IPv6 адрес

- TLA** - агрегат первого уровня, отдельные TLA могут выдаваться только очень крупным первичным операторам связи INTERNET. Имеет длину 13 бит.
- RES** - зарезервированное поле. Имеет длину 8 бит.
- NLA** - агрегат следующего уровня, этих агрегатов гораздо больше, чем агрегатов TLA. Первичные операторы связи могут выдавать диапазоны идентификаторов NLA вторичным операторам, которые, в свою очередь, могут выдавать отдельные NLA конкретным организациям. Имеет длину 24 бита.
- Sub ID** - номер подсети. Организация, получившая в свое распоряжение отдельный префикс NLA (точнее номер сети), вольна разбить его на несколько подсетей по своему усмотрению. Всего можно организовать до 65535 подсетей с фактически неограниченным числом хостов в каждой из них, так как номер хоста занимает 64 бита.

Эникаст-адреса

Эникаст-адрес IPv6 является адресом, который приписан нескольким интерфейсам (обычно принадлежащим разным узлам), при этом пакет, посланный по эникастному адресу, будет доставлен ближайшему интерфейсу в соответствии с метрикой протокола маршрутизации.

эникастные адреса синтаксически неотличимы от уникастных адресов. Когда уникальный адрес приписан более чем одному интерфейсу, он превращается в эникастный адрес и узлы, которым он приписан, должны быть сконфигурированы так, чтобы распознавать этот адрес.

Для любого эникастного адреса существует адресный префикс P , который определяет топологическую область, где находятся все соответствующие ему интерфейсы. В пределах области, заданной P , каждый член эникастной (anycast) группы должен быть объявлен, как отдельный вход в маршрутной системе; вне области, заданной P , эникастный адрес может быть занесен в маршрутную запись для префикса p .

Эникаст-адреса

Одним ожидаемым применением эникастных адресов является идентификация набора маршрутизаторов, принадлежащих Интернет сервис провайдеру.

Такие адреса в маршрутном заголовке IPv6 могут использоваться в качестве промежуточных, чтобы обеспечить доставку пакета через определенного провайдера или последовательность провайдеров.

Другим возможным применением может стать идентификация набора маршрутизаторов, связанных с определенной субсетью, или набора маршрутизаторов, обеспечивающих доступ в определенный домен.

Имеются следующие ограничения при использовании эникастных IPv6 адресов:

Эникастный адрес не может использоваться в качестве адреса отправителя в ipv6 пакете.

Эникастный адрес не может быть приписан ЭВМ IPv6, таким образом, он может принадлежать только маршрутизатору.

Необходимые эникаст-адреса

Эникаст-адрес маршрутизатора субсети предопределен и имеет формат, отображенный на рис.



Префикс субсети в эникастном адресе является префиксом, который идентифицирует определенный канал. Этот эникастный адрес является синтаксически идентичным уникастному адресу для интерфейса канала с идентификатором интерфейса равным нулю.

Пакеты, посланные группе маршрутизаторов с эникастным адресом, будут доставлены всем маршрутизаторам субсети. При этом все маршрутизаторы субсети должны поддерживать работу с эникастными адресами. Реальный обмен будет осуществлен лишь с тем маршрутизатором, который ответит первым.

Эникастный адрес маршрутизатора субсети предполагается использовать в приложениях, где необходимо взаимодействовать с одним из совокупности маршрутизаторов удаленной субсети. Например, когда мобильный хост хочет взаимодействовать с одним мобильным агентом в его “домашней” субсети.

Мульткаст-адреса

Мультикастинг-адрес IPv6 является идентификатором для группы узлов. Узел может принадлежать к любому числу мультикастинг групп. Мультикастинг-адреса имеют следующий формат:



11111111 в начале адреса идентифицирует адрес, как мультикастинг-адрес.



Старшие 3 флага зарезервированы и должны быть обнулены.

t = 0 указывает на то, что адрес является стандартным ("well-known") мультикастинг-адресом, официально выделенным для глобального использования в Интернет.

T = 1 указывает, что данный мультикастинг-адрес присвоен временно ("transient").

Мульткаст-адреса

Поле *score* представляет собой 4-битовый код мультикастинга, предназначенный для определения предельной области действия мультикастинг-группы. Допустимые значения:

- 0 зарезервировано
- 1 Область действия ограничена локальным узлом
- 2 Область действия ограничена локальным каналом
- 3 (не определено)
- 4 (не определено)
- 5 Область действия ограничена локальной сетью
- 6 (не определено)
- 7 (не определено)
- 8 Область действия ограничена локальной организацией
- 9 (не определено)
- A (не определено)
- B (не определено)
- C (не определено)
- D (не определено)
- E глобальные пределы (global scope)
- F зарезервировано

Мульткаст-адреса

Идентификатор группы идентифицирует мультикастинг-группы, постоянной или переходной (transient), в пределах заданных ограничений (scope).

Значение постоянно присвоенного мультикастинг-адреса не зависит от значения поля *scope*. Например, если "NTP servers group" присвоен постоянный мультикастинг адрес с идентификатором группы 43 (hex), тогда:

FF01:0:0:0:0:0:0:43 означает, что все ntp серверы одного и того же узла рассматриваются как отправители.

FF02:0:0:0:0:0:0:43 означает, что все NTP серверы работают с тем же каналом, что и отправитель.

FF05:0:0:0:0:0:0:43 означает, что все NTP серверы принадлежат той же сети, что и отправитель.

FF0E:0:0:0:0:0:0:43 означает, что все NTP серверы находятся в Интернет.

Мультикастинг адреса не должны использоваться в качестве адреса отправителя в IPv6 дейтограммах или встречаться в любых заголовках маршрутизации.

Предопределенные мультикаст-адреса

Приведенные ниже мультикаст-адреса являются зарезервированными (предопределенными):

FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Перечисленные выше мультикаст-адреса зарезервированы и не будут присваиваться каким-либо мультикаст-группам.

Предопределенные мультикаст-адреса

Адреса для обращения ко всем узлам:

FF01:0:0:0:0:0:0:1
FF02:0:0:0:0:0:0:1

Приведенные выше адреса идентифицируют группу, включающую в себя все IPv6 узлы в пределах группы 1 (локальные узлы) или 2 (локально связанные узлы).

Адреса всех маршрутизаторов:

FF01:0:0:0:0:0:0:2
FF02:0:0:0:0:0:0:2

Приведенные выше мультикаст-адреса идентифицируют группу всех IPv6 маршрутизаторов в пределах области 1 (локальные узлы) или 2 (связанные локально узлы).

Необходимые адреса узлов

ЭВМ должна распознавать следующие адреса, как обращенные к нему:
Её локальный адрес канала для каждого из интерфейсов

Выделенные уникаст-адреса
Адрес обратной связи

Мультикастинг-адрес для обращения ко всем узлам
Мультикастинг-адрес активного узла (solicited-node multicast address) для каждого из приписанных ей уникаст и эникастных адресов

Мультикаст-адреса всех групп, к которым принадлежит ЭВМ.

Маршрутизатор должен распознавать следующие адреса (as identifying itself):

Его локальный адрес канала для каждого из интерфейсов

Выделенные уникаст-адреса

Адрес обратной связи

Эникастные адреса маршрутизатора субсети для каналов, где он имеет интерфейсы.

Все другие эникастные адреса, которые использовались при маршрутизации.

Мультикастинг-адрес для обращения ко всем узлам

Мультикастинг-адрес для обращения ко всем маршрутизаторам

Мультикаст-адрес активного узла (solicited-node multicast address) для каждого приписанного ему уникаст и эникастного адресов.

Мультикастные адреса всех прочих групп, принадлежащих маршрутизатору.

**Приложение должно предопределить только следующие
адресные префиксы:**

Не специфицированный адрес

Адрес обратной связи

Мультикаст-префикс (FF)

Локально используемые префиксы (link-local и site-local)

Предопределенные мультикаст-адреса

Префиксы, совместимые с IPv4

Приложения должны считать все остальные адреса уникастными, если противоположное не оговорено при конфигурации (например, эникастные адреса).

Заголовки расширения IPv6

В IPv6, опционная информация уровня Интернет записывается в отдельных заголовках, которые могут быть помещены между IPv6 заголовком и заголовком верхнего уровня пакета.

В настоящее время определены заголовки: маршрутизации, фрагментации, аутентификации, инкапсуляции, опций hop-by-hop, места назначения и отсутствия следующего заголовка.

Существует небольшое число таких заголовков, каждый задается определенным значением кода поля *следующий заголовок*.



заголовки расширения должны обрабатываться строго в порядке их выкладки в пакете.

Заголовки расширения IPv6

Каждый заголовок расширения имеет длину кратную 8 октетам.

Многооктетные поля в заголовке расширения выравниваются в соответствии с их естественными границами, т.е., поля с шириной в n октетов помещаются в n октетов, начиная с начала заголовка, для $n = 1, 2, 4$ или 8 .

IPv6 включает в себя следующие заголовки расширения:

- Опции hop-by-hop

- Маршрутизация (routing; тип 0)

- Фрагмент

- Опции места назначения

- Проверка прав доступа (authentication)

- Поле безопасных вложений (encapsulating security payload)

Последние два описаны в RFC-1826 и RFC-1827.

Порядок заголовков расширения

Когда используется более одного заголовков расширения в одном пакете, рекомендуется помещать их в следующем порядке:

IPv6 заголовок

Заголовок опций hop-by-hop

Заголовок опций места назначения (destination options header, (1))

Заголовок маршрутизации

Заголовок фрагмента

Заголовок authentication (2)

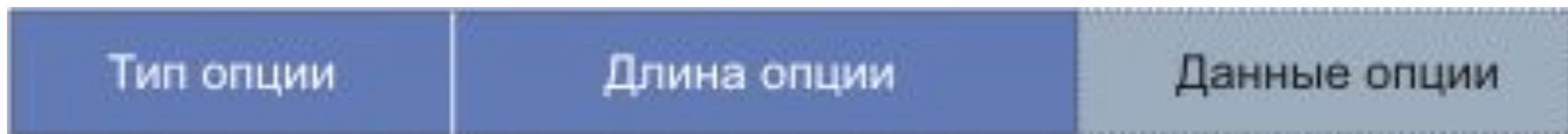
Заголовок безопасных вложений (encapsulating security payload, (2))

Заголовок опций места назначения (destination options header (3))

Заголовок верхнего уровня.

Опции

Два из определенных в настоящее время заголовков расширения - заголовок опций hop-by-hop и заголовок опций места назначения - несут в себе переменное число TLV-кодированных (type-length-value) опций следующего формата



Тип опции	8-битовый идентификатор типа опции.
Длина опции	8-битовое целое число без знака. Длина поля <i>данных опции</i> в октетах.
Данные опции	Поле переменной длины. Данные зависят от <i>типа опции</i> .

Последовательность опций в заголовке должна обрабатываться строго в соответствии с их порядком записи.

Идентификаторы *типа опций* кодируются так, что их старшие два бита характеризуют операцию, которая должна быть выполнена, если узел не узнает тип опции:

Опции

00	обойти эту опцию и продолжить обработку заголовка.
01	выбросить данный пакет.
10	выбросить данный пакет и вне зависимости от того, является ли адрес назначения мультикастинговым, послать отправителю ICMP-пакет с кодом parameter problem (код=2), с указателем на не узнанный код опции.
11	выбросить данный пакет и, если адрес места назначения не мультикастинговый, послать отправителю icmp пакет с кодом parameter problem (код=2) с указателем на не узнанный код опции.

Третий старший бит типа опции определяет, может ли информация в поле опция измениться по пути до места назначения пакета. Когда в пакете присутствует заголовок аутентификации, для любой опции, информация которой может измениться по пути, должна рассматриваться как нулевые октеты при определении значения идентификации. Значения этого бита:

0 - Данные опции не меняют маршрута

1 - Информация опции может изменить маршрут.

Опции

Отдельные опции могут требовать определенного выравнивания, с тем, чтобы обеспечить выкладку мультиоктетного значения данных поля опции. Требование выравнивания опции описывается с помощью выражения $xn+y$, означающего, что поле *тип опции* должно находиться через целое число, кратное x октетам плюс y октетов (отсчет от начала заголовка). Например:

$2n$ означает любое двухоктетное смещение от начала заголовка.

$8n+2$ означает любое 8-октетное смещение от начала заголовка плюс 2 октета.

Опции

Существует две опции заполнения, которые используются, когда необходимо выровнять последующие опции и вывести границу заголовка на значение кратное 8 октетам. Эти заполняющие опции должны распознаваться всеми приложениями IPv6:

Опция Pad1 (выравнивание не требуется)

Опция Pad1 используется для введения одного октета заполнителя в зону опций заголовка. Если требуется более одного октета, используется опция Padn.

Опция **padn** (выравнивание не требуется)



Опция Padn используется для введения двух и более октетов заполнителей в поле опций заголовка. Для n октетов заполнителя поле OPT data Len содержит значение $n-2$, а поле *данных опции* состоит из $n-2$ нулевых октетов

Опции заголовка Hop-by-Hop (шаг за шагом)

Заголовок опций hop-by-hop (шаг за шагом) используется для опционной информации, которая просматривается каждым узлом по пути доставки. Заголовок опций hop-by-hop идентифицируется кодом поля *следующий заголовок* 0 в IPv6 заголовке и имеет формат рис.



Следующий заголовок

8-битовый селектор. Определяет тип заголовка, который следует непосредственно за заголовком опций hop-by-hop. Использует те же значения поля протоколов, что и IPv4 [RFC-1700]

HDR EXT LEN

8-битовое число без знака. Длина заголовка поля опций hop-by-hop в октетах, исключая первые 8 октетов.

Опции

Поле переменной длины. Содержит один или более TLV-закодированных опций.

В дополнение к Pad1 и Padn опциям определены следующие опции hop-by-hop:

Опция Jumbo Payload (необходимо выравнивание: $4n + 2$)



Опция Jumbo payload используется для отправки пакетов IPv6 с полем данных, превосходящим 65535 октетов. Длина Jumbo Payload характеризует длину пакета в октетах, исключая заголовок IPv6, но включая заголовок опций hop-by-hop; Это поле должно содержать код более чем 65535. Если получен пакет с опцией *Jumbo payload*, содержащей код длины меньше или равный 65535, посылается сообщение ICMP (parameter problem, код 0) с указателем на старший октет поля длины Jumbo payload.

Поле *длины* Payload length IPv6 заголовка должно быть равно нулю для каждого пакета с опцией Jumbo payload.

Если получен пакет с корректным значением опции *Jumbo Payload* и ненулевым кодом длины поля данных, посылается сообщение ICMP (parameter problem код 0) с указателем на поле тип опции.

Опция Jumbo payload не может использоваться в пакетах, которые несут в себе заголовок *фрагмента*. Если заголовок *фрагмента* встретится в пакете, содержащем корректную опцию jumbo payload, посылается сообщение ICMP (parameter problem, код 0) с указателем на первый октет заголовка *фрагмента*.

Приложения, которые не поддерживают опцию *Jumbo Payload*, не могут иметь интерфейсы для каналов с MTU больше 65575 (40 октетов IPv6 заголовка плюс 65535 октетов данных).

Маршрутный заголовок

Заголовок маршрутизации используется отправителем, чтобы заставить пакет посетить один или более промежуточных узлов на пути к месту назначения.

Следующий заголовок	8-битовый селектор. Определяет тип заголовка, который следует непосредственно за заголовком маршрутизации. Использует те же коды протоколов, что и IPv4 [RFC-1700].
hdr ext len	8-битовое целое без знака. Длина заголовка маршрутизации выражается в 8-октетных блоках, и не включает в себя первые 8 октетов.
Тип маршрутизации	8-битовый идентификатор конкретного варианта маршрутизации
Оставшиеся сегменты	8-битовое число без знака. Число остающихся сегментов пути, т.е. число промежуточных узлов, которые должны быть посещены пакетом по пути к месту назначения.
Данные, зависящие от типа	Поле переменной длины, формат зависит от кода поля <i>тип маршрутизации</i> . а длина

Если в процессе обработки входного пакета встретится заголовок маршрутизации с не узнанным полем *тип маршрутизации*, то поведение узла зависит от содержимого поля *число оставшихся сегментов пути*.

1. Если число оставшихся сегментов пути равно нулю, узел должен проигнорировать заголовок маршрутизации и продолжить работу со следующим заголовком, чей тип указан в поле *следующий заголовок* заголовка маршрутизации.
2. Если число оставшихся сегментов пути не равно нулю, узел должен выбросить пакет и послать сообщение ICMP (parameter problem, код 0) с указателем на поле не узнанного типа маршрутизации. Заголовок маршрутизации типа 0 имеет следующий формат

Следующий заголовок	Hdr Ext Len	Тип маршрутизации=0	Оставшиеся сегменты
Резерв	Strict/Loose Bit Map		
Адрес [1]			
Адрес [2]			
.....			
Адрес [N]			

Следующий заголовок	8-битовый селектор. Идентифицирует тип заголовка, следующего непосредственно за заголовком маршрутизации. Использует те же коды протоколов, что и IPv4 [RFC-1700].
hdr ext len	8-битовое целое без знака. Длина заголовка маршрутизации в 8-октетных блоках, исключая первые 8 октетов. Для заголовков маршрутизации типа 0 hdr ext len равна удвоенному числу адресов в заголовке, должно быть четным числом меньше или равным 46.
Тип маршрутизации	0.
Оставшиеся сегменты	8-битовое целое без знака. Число оставшихся сегментов пути, т.е., число узлов, которые следует посетить на пути к месту назначения. Максимально допустимое число = 23
Резерв	8-битовое поле резерва. Инициализируется нулем при передаче и игнорируется при приеме.
strict/loose bit map	24-битовый код-маска, биты пронумерованы, начиная с 0 до 23, слева направо. Для каждого из сегментов пути указывает должен ли следующий узел быть соседом: 1 означает strict (должен быть соседом), 0 означает пропустить (не должен быть соседом).
Адрес[1..n]	Вектор 128-битовых адресов, пронумерованных с 1 до n.

Мультикастинг-адреса не должны встречаться в заголовке маршрутизации типа 0, или в поле места назначения IPv6 пакета, несущего в себе заголовок маршрутизации типа 0.

Если бит 0 поля Strict/loose bit map имеет значение 1, поле адреса места назначения IPv6 заголовка в исходном пакете должно идентифицировать соседа. Если бит 0 имеет значение 0, отправитель может использовать любой легальный не мультикастинговый адрес в качестве адреса места назначения.

Биты с номерами более n, где n - число адресов в заголовке маршрутизации, должны быть обнуляться отправителем и игнорироваться получателем.

Заголовок маршрутизации не рассматривается и не анализируется до тех пор, пока пакет не достигнет места назначения, указанного в поле IPv6

Заголовок фрагмента

Заголовок фрагмента используется отправителем IPv6 для посылки пакетов длиннее, чем MTU пути до места назначения.

(Замечание: в отличие от IPv4, фрагментация в IPv6 выполняется только узлами-отправителями, а не маршрутизаторами вдоль пути доставки).

Заголовок фрагментации идентифицируется кодом поля следующий заголовок, равным 44 и имеет следующий формат



Следующий заголовок	8-битовый селектор. Идентифицирует тип исходного заголовка фрагментируемой части исходного пакета. Использует те же коды протоколов, что и IPv4 [RFC-1700].
Резерв	8-битовое резервное поле. Инициализируется нулем при передаче и игнорируется при приеме.
Fragment offset	13-битовое число без знака. Смещение в 8-октетном блоке, для данных, которые следуют за этим заголовком, началом отсчета является начало фрагментируемой части исходного пакета.
Резерв (второй)	2-битовое резервное поле. Инициализируется нулем при передаче и игнорируется при приеме.
m флаг	1 = есть еще фрагменты; 0 = последний фрагмент.
Идентификация	32 бита

Для того чтобы послать пакет с длиной больше MTU пути, узел-отправитель может разделить пакет на фрагменты и послать каждый фрагмент в виде отдельного пакета, сборка исходного пакета будет проведена получателем.

Для каждого пакета, который должен быть фрагментирован, узел-отправитель генерирует код *идентификации*.

Этот код должен отличаться от аналогичных кодов идентификации, используемых для других фрагментируемых пакетов, которые пересылаются в данный момент.

Под "данным моментом" подразумевается период времени жизни пакета, включая время распространения кадра от источника до получателя и время, необходимое для сборки исходного (оригинального) пакета получателем.

Однако не предполагается, чтобы отправитель знал максимальное время жизни пакета. Скорее предполагается, что данное требование будет удовлетворено с помощью простого 32-разрядного счетчика, инкрементируемого всякий раз, когда очередной пакет должен быть фрагментирован.

Схема реализации генератора кода идентификации оставляется на усмотрение приложения. Если присутствует заголовок маршрутизации, под адресом получателя подразумевается конечное место назначения.

Под исходным большим, не фрагментированным пакетом подразумевается “оригинальный” пакет. Предполагается, что он состоит из двух частей, как показано на рисунке. Исходный пакет:



Не фрагментированная часть состоит из IPv6 заголовка плюс любых заголовков расширения, которые должны быть обработаны узлами по пути до места назначения. Таким образом, нефрагментированная часть включает в себя все заголовки вплоть до заголовка маршрутизации, если таковой присутствует, или до заголовка опций hop-by-hop, если он присутствует.

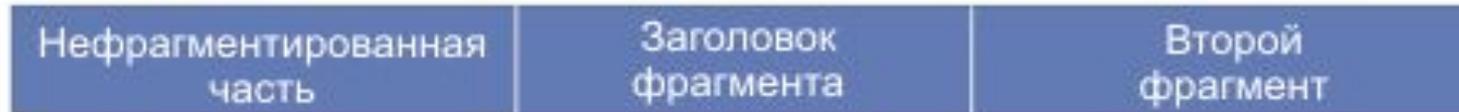
Фрагментируемая часть представляет собой остальную часть пакета, т.е. включает в себя заголовки расширений, которые должны быть обработаны в узле места назначения, заголовок верхнего уровня и данные.

Фрагментируемая часть оригинального пакета делится на фрагменты с длиной кратной 8 октетам. Фрагменты пересылаются независимо с помощью пакетов-фрагментов. Как показано на рис.

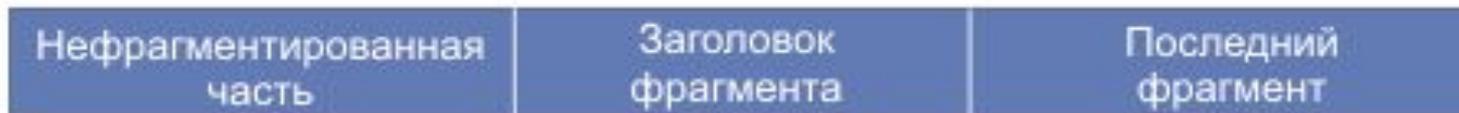
Исходный пакет:



Пакеты-фрагменты



.....



Каждый пакет-фрагмент состоит из:

(1) Не фрагментируемой части оригинального пакета, с длиной поля данных оригинального IPv6 заголовка, измененной для того чтобы соответствовать длине фрагмента пакета (исключая длину самого IPv6-заголовка), а код поля *следующий заголовок* последнего заголовка не фрагментируемой части меняется на 44.

(2) Заголовка фрагмента, включающего в себя:

Код поля *следующий заголовок*, идентифицирующий первый заголовок фрагментируемой части оригинального пакета.

Смещение фрагмента, выражаемое в 8-октетных блоках и отсчитываемое от начала фрагментируемой части оригинального пакета. Смещение первого фрагмента (самого левого) равно нулю.

Код M-флага равен нулю, если фрагмент является последним (самым правым), в противном случае флаг равен 1.

(3) Сам фрагмент.

Длина фрагментов должна выбираться такой, чтобы пакеты-фрагменты соответствовали значению MTU для маршрута к месту назначения (назначений). В узле места назначения из пакетов-фрагментов восстанавливается оригинальный пакет в не фрагментированной форме.

Заголовок опций места назначения

Заголовок опции *места назначения* используется для передачи опционной информации, которая должна анализироваться только узлом (узлами) назначения. Заголовок опции места назначения идентифицируется кодом поля *следующий заголовок* равным 60 предшествующего заголовка имеет формат:



Следующий заголовок - 8-битовый селектор. Идентифицирует тип заголовка, который непосредственно следует за заголовком опций места назначения. Использует те же коды протокола, что и IPv4 [RFC-1700].

Hdr Ext Len - 8-битовое целое без знака. Длина заголовка опций места назначения в 8-октетных блоках, исключая первые 8 октетов.

Опции - поле переменной длины, кратное 8 октетам. Содержит одну или более TLV-закодированных опций.

Отсутствие следующего заголовка

Код **59** в поле *следующий заголовок* IPv6 заголовка или любой другой заголовок расширения указывает, что за этим заголовком ничего не следует.

Если поле *длина данных* заголовка IPv6 указывает на присутствие октетов после конца заголовка, содержащего код 59 в поле *следующий заголовок*, эти октеты должны быть проигнорированы и переданы без изменений при переадресации пакета.

О размере пакетов

Протокол IPv6 требует, чтобы каждый канал в Интернет имел MTU = 576 октетов или более.

Для каждого канала, который не способен обеспечить длину пакетов в 576 октетов должна быть обеспечена фрагментация/дефрагментация на уровне ниже IPv6.

Настоятельно рекомендуется, чтобы узлы IPv6 использовали механизм определения MTU пути [RFC-1191] для использования преимущества большого значения MTU. Однако в минимальной конфигурации IPv6 (например, в BOOT ROM) может ограничивать себя в пределах 576 октетов и не использовать path MTU discovery.

Узел должен быть способен принимать фрагментированные пакеты, которые после сборки имеют размер 1500 октетов, включая IPv6 заголовок.

Узлу позволено принимать пакеты, которые после сборки имеют размер более 1500 октетов.

Однако узел не должен посылать фрагменты, которые после сборки образуют пакеты длиннее 1500 октетов, если он не уверен, что получатель способен их воспринять и дефрагментировать.

Замечание: Анализ MTU пути должно проводиться даже в случае, когда узел “думает”, что адресат находится на том же канале что и сам узел.

Замечание: В отличие от IPv4, в IPv6 не нужно устанавливать флаг "don't fragment" (не фрагментировать) в заголовках пакетов, для того чтобы выполнить операцию определения величины mtu канала; так как это является атрибутом любого IPv6 пакета по умолчанию. Части процедур из RFC-1191, которые включают в себя использование таблиц MTU, не применимы к IPv6, так как версия сообщения IPv6 "datagram too big" всегда указывает на точное значение MTU, которое следует использовать.

Метки потоков

24-битовое поле *метки потока* в заголовке IPv6 может использоваться отправителем для выделения пакетов, для которых требуется специальная обработка в маршрутизаторе, такая например, как нестандартная QoS или "real-time " сервис. Этот аспект IPv6 является пока экспериментальным и может быть изменен позднее. Для ЭВМ или маршрутизаторов, которые не поддерживают функцию пометки потоков, это поле должно быть обнулено при формировании пакета, сохраняться без изменения при переадресации и игнорироваться при получении.

Поток это последовательность пакетов, посылаемых отправителем определенному адресату, при этом предполагается, что все пакеты данного потока должны быть подвергнуты определенной обработке. Характер этой специальной обработки может быть передан маршрутизатору посредством протокола управления или внутри самих пакетов, например, в опции hop-by-hop.

Допускается несколько потоков между отправителем и получателем, а также обмен, не ассоциированный ни с одним из потоков. Поток однозначно описывается комбинацией адреса отправителя и ненулевой меткой потока. Пакеты, не принадлежащие ни одному из потоков, имеют метку равную нулю.

Приоритет

4-битовое поле приоритета в IPv6 заголовке позволяет отправителю идентифицировать относительный приоритет доставки пакетов. Значения приоритетов делятся на два диапазона.

Коды от 0 до 7 используются для задания приоритета трафика, для которого отправитель осуществляет контроль перегрузки (например, снижает поток TCP в ответ на сигнал перегрузки).

Значения с 8 до 15 используются для определения приоритета трафика, для которого не производится снижения потока в ответ на сигнал перегрузки, например, в случае пакетов “реального времени”, посылаемых с постоянной частотой.

Значения кодов приоритета

Код приоритета	Назначение
0	Нехарактеризованный трафик
1	Заполняющий трафик (например, сетевые новости)
2	Несущественный информационный трафик (например, электронная почта)
3	Резерв
4	Существенный трафик (напр., FTP, HTTP, NFS)
5	Резерв
6	Интерактивный трафик (напр. telnet, x)
7	Управляющий трафик Интернет (напр., маршрутные протоколы, snmp)

Предполагается, что чем больше код, тем выше приоритет данных, тем быстрее они должны быть доставлены.

О протоколе верхнего уровня

Контрольные суммы верхнего уровня

Любой транспортный или другой протокол верхнего уровня, который включает адреса IP-заголовка в свою контрольную сумму, должен быть модифицирован, чтобы работать с 128-битовыми IPv6адресами вместо 32-битовых IPv4. В частности, ниже показаны псевдо-заголовки для TCP и UDP в IPv6

Адрес отправителя	
Адрес получателя	
Длина поля данных	
Нуль	Следующий заголовок

Если пакет содержит заголовок маршрутизации, в качестве **адреса места назначения** в псевдо-заголовке используется окончательный адрес. В исходном узле этот адрес будет последним элементом заголовка маршрутизации; для узла получателя он будет находиться в поле **адрес места назначения IPv6** заголовка.

Код поля **следующий заголовок** в псевдо-заголовке идентифицирует протокол верхнего уровня (например, 6 для TCP или 17 для UDP). Он будет отличаться от кода поля **следующий заголовок** в IPv6 заголовке, если имеются заголовки расширения между заголовком IPv6 и заголовком протокола верхнего уровня.

В качестве **кода длины поля данных** в псевдо-заголовке используется длина пакета протокола верхнего уровня, включая заголовок верхнего уровня. Он будет меньше длины поля данных в заголовке (или в опции Jumbo Payload), если имеются заголовки расширения между IPv6 заголовком и заголовком верхнего уровня.

В отличие от IPv4, при формировании udp пакетов в IPv6 узле, контрольная сумма не является опциональной.

Поэтому при формировании UDP-пакета IPv6 узел должен вычислить контрольную UDP сумму пакета и псевдо-заголовка и, если вычисление дает в качестве результата нуль, он должен быть заменен на FFFF для помещения в UDP заголовок.

IPv6-получатели должны выбрасывать UDP пакеты, содержащие нулевую контрольную сумму и фиксировать при этом состояние ошибки.

Максимальное время жизни пакета

В отличие от IPv4, узлы IPv6 не требуют установки максимального времени жизни пакетов.

По этой причине поле IPv4 "time to live" (TTL) переименовано в "hop limit" (предельное число шагов) для IPv6.

На практике очень немногие IPv4 приложения, используют ограничения по TTL, так что фактически это не принципиальное изменение.

Максимальный размер поля данных для протоколов высокого уровня

При вычислении максимального размера поля данных, доступного для протокола верхнего уровня, должен приниматься во внимание большой размер заголовка IPv6 относительно IPv4.

Например, в IPv4, **MSS** опция TCP вычисляется как максимальный размер пакета (значение по умолчанию или величина полученная из MTU) минус 40 октетов (20 октетов для минимальной длины IPv4 заголовка и 20 октетов для минимальной длины TCP заголовка).

При использовании TCP поверх IPv6, **MSS** должно быть вычислено как максимальная длина пакета минус 60 октетов, так как минимальная длина заголовка IPv6 (т.е., IPv6 заголовков без заголовков расширения) на 20 октетов больше, чем для IPv4.

Протокол управляющих сообщений (ICMPv6) для спецификации IPv6 (RFC-1885)

Протокол IPv6 является новой версией IP. IPv6 использует протокол управляющих сообщений (ICMP) так, как это определено для IPv4 [RFC-792], но с некоторым количеством изменений. Протокол подключения к группам (IGMP), специфицированный для IPv4 [RFC-1112] был также пересмотрен и включен в протокол ICMP для IPv6. Результирующий протокол называется ICMPv6, и имеет код следующего заголовка 58.

ICMPv6 (ICMP для IPv6)

- ICMPv6 используется узлами IPv6 для сообщений об ошибках при обработке пакетов, и для выполнения других функций уровня Интернет, таких как диагностика (ICMPv6 "ping") и сообщение об участии в мультикастинг группах. Протокол ICMPv6 является интегрированной частью IPv6 и должен реализовываться каждым узлом, поддерживающим IPv6.

Общий формат сообщений

- Сообщения ICMPv6 образуют два класса: сообщения об ошибках и информационные сообщения. Сообщения об ошибках идентифицируются по нулю в старшем бите поля *тип*. Таким образом, сообщения об ошибках могут иметь код поля *тип* от 0 до 127; информационные сообщения имеют коды поля *тип* от 128 до 255.
- В данном документе определены форматы для следующих сообщений ICMPv6:
- **Сообщения об ошибках ICMPv6:**
- 1 destination unreachable (место назначения недоступно)
2 packet too big (пакет слишком велик)
3 time exceeded (время превышено)
4 parameter problem (проблема с параметрами)

- **Информационные сообщения ISMPv6:**
- 128 echo request (Запрос эхо)
- 129 echo reply (Эхо-отклик)
- 130 group membership query (запрос участия в группе)
- 131 group membership report (отчет об участии в группе)
- 132 group membership reduction (сокращение числа участников в группе)

- Каждое сообщение ICMPv6 начинается с заголовка IPv6, за которым следует нуль или более заголовков расширения IPv6. Заголовок ICMPv6 идентифицируется кодом следующего заголовка 58 в предыдущем заголовке.

(Заметим: этот код отличается от значения, принятого для ICMP IPv4.)

- Сообщения ICMPv6 имеют следующий общий формат (рис. 4.4.1.1.33):

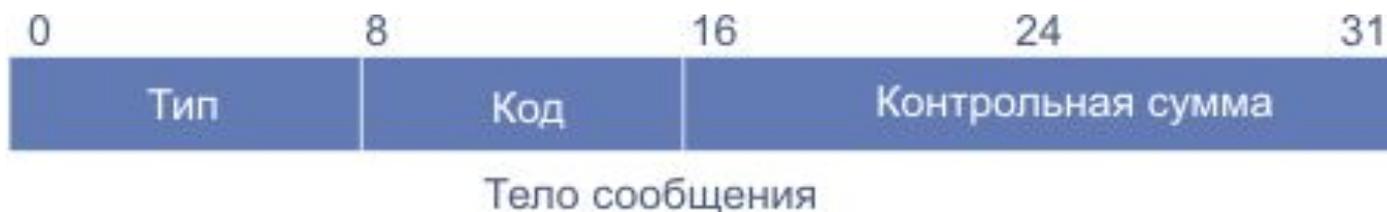


Рис. 4.4.1.1.33. Общий формат сообщений ICMPv6

- Поле *тип* указывает на тип сообщения. Его значение определяет формат последующих данных.
- Поле *код* зависит от типа сообщения. Оно используется для создания дополнительного уровня структуризации сообщения. Поле *контрольная сумма* используется для обнаружения повреждений сообщения ICMPv6 и заголовка IPv6.

Узел отправитель сообщения ISMPv6 должен определить IPv6-адреса отправителя и получателя до вычисления контрольной суммы. Если узел имеет более одного уникастного адреса, то он должен выбрать адрес отправителя следующим образом:

- Если сообщение является откликом на сообщение, полученное по одному из уникаст адресов, адресом отправителя должен стать именно этот адрес.
- Если сообщение является откликом на мультикаст- или эникаст-сообщение группе, в которую входит данный узел, адресом отправителя должен стать никастный адрес интерфейса, откуда пришло сообщение-первопричина отклика.
- Если сообщение является откликом на сообщение, посланное по адресу, который не принадлежит данному узлу, в качестве адреса отправителя следует выбрать уникаст адрес, принадлежащий узлу и обещающий наибольшую диагностическую полезность. Например, если сообщение является откликом на операцию переадресации пакета, которая не может быть завершена успешно, в качестве адреса отправителя должен быть взят уникаст-адрес интерфейса, переадресация на который не удалась.
- В противном случае, должна быть просмотрена таблица маршрутизации узла и выяснено, какой интерфейс должен быть использован для достижения места назначения сообщения. Уникастный адрес этого интерфейса и должен быть выбран в качестве адреса отправителя.

Контрольная сумма

- является 16-битным дополнением по модулю 1 суммы всего сообщения ICMPv6, начиная с поля *тип* сообщения ICMPv6, дополненного полями псевдозаголовка IPv6.
- Код поля *следующий заголовок* для псевдозаголовка выбирается равным 58.
(Заметим: включение псевдозаголовка в контрольную сумму ICMPv6 является изменением по отношению к протоколу IPv4; обоснование причин этого см. в [IPv6]).
- Перед вычислением контрольной суммы поле *контрольная сумма* обнуляется.

Приложения должны следовать следующим правилам при обработке сообщений ICMPv6 (из [RFC-1122]):

- Если получено сообщение о неизвестной ошибке ICMPv6, оно должно быть передано верхнему уровню.
- Если получено информационное сообщение ICMPv6 неизвестного типа, оно должно быть выброшено.
- Каждое ICMPv6 сообщение об ошибке (тип < 128) включает в себя целиком или частично IPv6 пакет, вызвавший ошибку, при условии, что сообщение об ошибке превысит 576 октетов.
- В тех случаях, когда протокол интернет-уровня нуждается в передаче сообщения об ошибке ICMPv6 вышерасположенному уровню, тип протокола верхнего уровня извлекается из исходного пакета (содержащегося в теле сообщения об ошибке ICMPv6) и используется для выбора соответствующего протокола верхнего уровня при последующей обработке сообщения об ошибке.

Если исходный пакет имеет необычно большое число заголовков расширения, возможно, что тип протокола верхнего уровня может отсутствовать в сообщении ICMPv6, из-за укорочения исходного пакета до уровня 576 октетов. В этом случае сообщение об ошибке отбрасывается после обработки уровня IPv6.

Сообщение об ошибке ICMPv6 не должно посылаться в качестве результата получения:

- **(е.1)** сообщения об ошибке ICMPv6, или
- **(е.2)** пакета, направленного по IPv6 мультикаст-адресу (существует два исключения из этого правила: **(1)** сообщения packet too big - пакет слишком велик) - чтобы позволить скорректировать MTU прохода, и **(2)** сообщения parameter problem (проблема с параметрами), Код 2, оповещающий о нераспознанной опции), или
- **(е.3)** мультикастинг-пакета канального уровня, (исключения пункта е.2 применимы и здесь), или
- **(е.4)** широковещательного пакета канального уровня, (исключения пункта е.2 применимы и здесь), или
- **(е.5)** пакета, чей адрес отправителя не однозначно определяет какой-то узел, например, не специфицированный адрес IPv6, мультикаст-адрес IPv6 или эникаст-адрес.

(f) Наконец, узел IPv6 должен ограничить частоту посылки сообщений об ошибке, если адресат на них не реагирует. Это ограничит загрузку канала.

Существует много способов ограничения частоты посылки сообщений, например:

- **(f.1)** Таймерный метод. Передача сообщений производится не чаще, чем раз за указанное число T миллисекунд.
- **(f.2)** Метод полосы пропускания. Сообщения об ошибке должны занимать не более определенной доли F полосы пропускания канала.
- Ограничивающие параметры (например, T или F в вышеприведенных примерах) должны задаваться узлом со значениями по умолчанию (напр., $T = 1$ сек, и $F = 2\%$, не 100% !).

Заключение

IPv6 представляет собой новую версию протокола Интернет (RFC-1883), являющуюся преемницей версии 4 (IPv4; RFC-791). Изменения IPv6 по отношению к IPv4 можно поделить на следующие группы:

- *Расширение адресации*

В IPv6 длина адреса расширена до 128 бит (против 32 в IPv4), что позволяет обеспечить больше уровней иерархии адресации, увеличить число адресуемых узлов, упростить авто-конфигурацию. Для расширения возможности мультикастинг-маршрутизации в адресное поле введено субполе "scope" (группа адресов). Определен новый тип адреса "anycast address" (эникастный), который используется для отправки запросов клиента любой группе серверов. Эникаст адресация предназначена для использования с набором взаимодействующих серверов, чьи адреса не известны клиенту заранее.

- ***Спецификация формата заголовков***
Некоторые поля заголовка IPv4 отбрасываются или делаются опциональными, уменьшая издержки, связанные с обработкой заголовков пакетов с тем, чтобы уменьшить влияние расширения длины адресов в IPv6.
- ***Улучшенная поддержка расширений и опций***
Изменение кодирования опций IP-заголовков позволяет облегчить переадресацию пакетов, ослабляет ограничения на длину опций, и делает более доступным введение дополнительных опций в будущем.
- ***Возможность пометки потоков данных***
Введена возможность пометить пакеты, принадлежащие определенным транспортным потокам, для которых отправитель запросил определенную процедуру обработки, например, нестандартный тип TOS (вид услуг) или обработка данных в реальном масштабе времени.
- ***Идентификация и защита частных обменов***
В IPv6 введена спецификация идентификации сетевых объектов или субъектов, для обеспечения целостности данных и при желании защиты частной информации.
- Формат и семантика адресов IPv6 описаны в документе RFC-1884. Версия ICMP IPv6 рассмотрена в RFC-1885.

Сообщения об ошибках ICMPv6

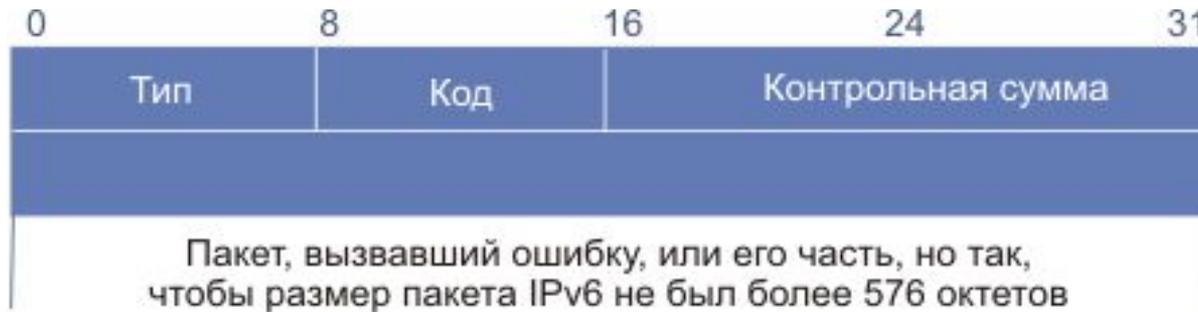


Рис. 4.4.1.1.34. Формат сообщения о недостижимости адресата

Поля IPv6:

- Адрес места назначения копируется из поля адрес отправителя пакета, вызвавшего ошибку.

Поля ICMPv6:

- Тип = 1
Код = 0 - нет маршрута до места назначения
1 - связь с адресатом административно запрещена
2 - не сосед
3 - адрес не достижим
4 - порт не достижим
- Не используется. Это поле не используется при всех значениях поля код. Оно должно быть обнулено отправителем и игнорироваться получателем.

Описание

- Сообщение *адресат не достижим* (destination unreachable) должно генерироваться маршрутизатором, или уровнем IPv6 узла-отправителя, в случае, когда пакет не может быть доставлен адресату не по причине перегрузки. (Сообщение ICMPv6 не должно посылаться при потере пакета из-за перегрузки).
- Если причиной потери пакета является недостаток места в маршрутной таблице узла, поле *код* должно принять значение 0 (Заметим, что такая ошибка может произойти только при наличии в таблице маршрута по умолчанию).
- Если причиной потери пакета является административный запрет, например, Firewall, поле код принимает значение 1.
- Если причиной потери пакета является то, что следующий узел в маршрутной таблице не является соседом данного узла, то поле *код* принимает значение 2.
- Если имеет место какая-то другая причина недоставки пакета, в поле код заносится значение 3.
- Узел места назначения может посылать сообщение “адресат не достижим” с кодом 4, когда транспортный протокол пакета (напр., UDP) не имеет получателя, а другого метода, уведомить об этом отправителя нет.
- Узел, получивший сообщение ICMPv6 “адресат не достижим” должен уведомить об этом протокол вышележащего уровня.



Рис. 4.4.1.1.35. Сообщение *packet too big* (пакет слишком велик)

Поля IPv6:

- Адрес места назначения копируется из поля *адрес отправителя* пакета, вызвавшего ошибку.

Поля ICMPv6:

- Тип 2
Код 0
mtu *mtu* следующего шага.

Описание

- Сообщение *packet too big* (пакет слишком велик) должно посылаться маршрутизатором в ответ на получение пакета, который не может быть переадресован, из-за того, что он длиннее, чем MTU выходного канала. Информация в этом сообщении используется в качестве части процесса определения MTU прохода [RFC-1191].
- Пришедшее сообщение *packet too big* должно быть передано протоколу верхнего уровня.

Формат сообщения о превышении времени аналогичен формату сообщения о недостижимости адресата (рис. 4.4.1.1.33).

Поля ICMPv6:

- *Тип 3*
Код 0 - при передаче превышен лимит числа шагов
1 - превышено время восстановления сообщения из фрагментов.
- *Не используется.* Это поле не используется при всех значениях поля код. Оно должно быть обнулено отправителем и игнорироваться получателем.

Описание

- Если маршрутизатор получает пакет с предельным значением числа шагов равным нулю ($hop\ limit = 0$), или маршрутизатор после декрементации получил нулевое значение поля *hop limit*, он должен выбросить такой пакет и послать отправителю пакета сообщение ICMPv6 о превышении времени (*time exceeded*) со значением поля код равным 0. Это указывает на заикливание маршрута или на слишком малое значение поля *hop limit*.
- Посылая сообщение ICMPv6 о превышении времени (*time exceeded*) со значением поля код равным нулю, маршрутизатор должен рассматривать входной интерфейс, в соответствии с правилом выбора адреса отправителя (d).
- Пришедшее сообщение *time exceeded* должно быть передано протоколу верхнего уровня.

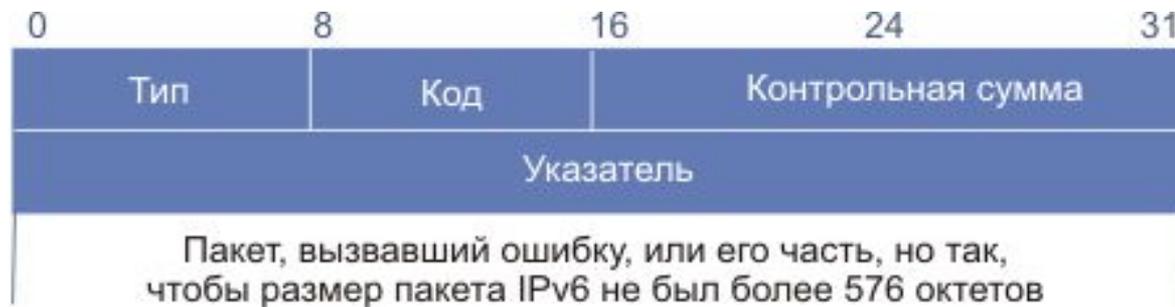


Рис. 4.4.1.1.36. Сообщение о конфликте параметров

Поля ICMPv6:

- *Тип* 4
Код 0 - встретилась ошибка в поле заголовка
 1 - встретился неопознанный код поля *следующий заголовок*
 2 - встретилась неопознанная опция IPv6
Указатель. Идентифицирует смещение в октетах в пакете, вызвавшем ошибку.
- Указатель отмечает позицию в пакете, если размер пакета ICMPv6 не позволяет поместить его в отклик полностью, а ошибочное поле в сообщении не поместилось.

Описание

- Если узел IPv6, обрабатывающий пакет, обнаруживает какую-то проблему с одним из полей заголовка или заголовков расширения, такую, что дальнейшая обработка невозможна, он должен выбросить пакет и послать сообщение ICMPv6 parameter problem (проблема с параметрами) отправителю пакета с указанием типа и позиции ошибки.
- Поле *указатель* идентифицирует октет заголовка исходного пакета, где обнаружена ошибка. Например, сообщение ICMPv6 с полем *тип* = 4, полем *код* = 1 и полем *указатель* = 40 указывает на то, что заголовок расширения IPv6, следующий за заголовком IPv6 исходного пакета содержит нераспознанный код следующего заголовка.

Информационные сообщения ICMPv6



Рис. 4.4.1.1.37. Сообщение запрос эхо

Поля IPv6:

- Адрес места назначения - любой легальный IPv6-адрес

Поля ICMPv6:

- *Тип* 128
Код 0
Идентификатор. Идентификатор, который помогает друг с другом связать запрос эхо и эхо-отклик. Может равняться нулю.
- *Номер по порядку*
Номер по порядку имеет целью связать друг с другом запрос эхо и эхо-отклик. Может равняться нулю.
- *Информация.* Нуль или более октетов произвольных данных.

Описание

- Каждый узел должен реализовать функцию эхо-отклика ICMPv6 при получении запроса эхо. Узлу следует также предоставить пользовательский интерфейс для отправки запросов эхо и получения эхо-откликов для целей диагностики.

- Формат сообщения эхо-отклик идентичен формату запроса эхо (рис. 20.5).

Поля IPv6:

- Адрес места назначения копируется из поля *адрес отправителя* пакета *запрос эхо*.

Поля ICMPv6:

- *Тип* 129

Код 0

Идентификатор. Идентификатор из исходного запроса эхо (echo request).

Номер по порядку. Номер по порядку из исходного запроса эхо.

Информация. Данные из исходного запроса эхо.

Описание

- Каждый узел должен иметь встроенную функцию отклика ICMPv6, которая получает запросы эхо и посылает соответствующие эхо-отклики. Узел должен также реализовать интерфейс прикладного уровня для посылки запросов эхо и получения эхо-откликов для диагностических целей.
- Адрес отправителя эхо-отклика, посылаемого в ответ на уникальный запрос эхо должен быть тем же самым, что и адрес места назначения в запросе эхо.
- Эхо-отклик должен быть послан в ответ на запрос эхо, посланный по мультикастному адресу. Адрес отправителя в отклике должен быть уникальным адресом, принадлежащим интерфейсу, через который был получен мультикастный запрос эхо.
- Информация, полученная в ICMPv6 сообщении запроса эхо, должна быть полностью возвращена без модификации в ICMPv6 эхо-отклике, если эхо-отклик не превысит MTU обратного прохода, в противном случае пакет укорачивается.
- Оповещение верхнего уровня
- Сообщения эхо-отклик должны передаваться пользовательскому интерфейсу ICMPv6, если соответствующий запрос эхо исходит не из IP-уровня.

Сообщение о членстве в группе имеет следующий формат:

0	8	16	24	31
Тип	Код	Контрольная сумма		
Максимальная задержка отклика		Не используется		
Мультикаст-адрес				

Рис. 4.4.1.1.38. Сообщения участия в группе

Поля IPv6:

Адрес места назначения

- В сообщении-запросе о членстве в группе запрашивается мультикаст-адрес группы.
- В отчете о членстве в группе или в сообщении о сокращении членства в группе сообщается мультикаст-адрес группы.
- Поле Hop Limit = 1 (предельное число шагов)

Поля ICMPv6:

- *Тип* 130 - Запрос членства в группе
- 131 - Отчет о членстве в группе
- 132 - Сокращение членства в группе
- Код* 0

Максимальное время отклика

- В сообщениях запросах - это максимальное время в миллисекундах, на которое может задержаться сообщение-отчет. В сообщениях-отчетах и сообщениях о сокращении в это поле отправитель записывает нуль, а получатель его игнорирует.
- *Не используется.* Отправитель записывает нуль, получатель игнорирует.
- *Мультикаст-адрес*
- Адрес мультикаст-группы, сообщение о которой послано. В сообщениях-запросах поле мультикаст-адреса может равняться нулю, что означает запрос ко всем группам.

Описание

- Сообщения ISMPv6 о членстве в группе используются для передачи информации о членстве в мультикаст-группе от узлов к их ближайшим маршрутизаторам. Подробности их использования можно найти в [RFC-1112].

Спасибо за внимание!

Лекция окончена