Network Working Group
Request for Comments: 4861
Obsoletes: 2461
Category: Standards Track

T. Narten
IBM
E. Nordmark
Sun Microsystems
W. Simpson
Daydreamer
H. Soliman
Elevate Technologies

September 2007

Обнаружение соседей IPv6

Neighbor Discovery for IP version 6 (IPv6)

Статус документа

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Распространение документа не ограничивается.

Аннотация

Этот документ задаёт протокол обнаружения соседей (Neighbor Discovery или ND) для IP версии 6. Узлы IPv6 на одном канале используют ND для обнаружения присутствия других узлов, определения их адресов канального уровня, поиска маршрутизаторов и поддержки информации о доступности путей к активным соседям.

Оглавление

1. Введение

Эта спецификация определяет протокол обнаружения соседей ND для IPv6. Узлы (хосты и маршрутизаторы) используют протокол ND для определения адресов канального уровня, которые относятся к подключённым каналам? и быстро отбрасывают кэшированные значения, ставшие недействительными. Хосты также используют протокол ND для поиска соседних маршрутизаторов, которые смогут пересылать пакеты от их имени. Наконец, узлы используют протокол для активного отслеживания доступности соседей и обнаружения смены адресов канального уровня. При отказе маршрутизатора или пути хост активно ищет работающие альтернативы ему.

Если не указано иное (в документе, описывающем работу IP на конкретном типе каналов), этот документ применим ко всем типам каналов. Однако, поскольку ND использует групповую адресацию канального уровня для своих служб, возможно, что для некоторых типов каналов (например, NBMA[1]) будут заданы дополнительные протоколы или механизмы реализации этих услуг (в документе, описывающем работу IP на конкретном типе каналов). Описанные в документе службы, которые не зависят напрямую от групповой адресации (типа Redirect, определения Next-hop, Neighbor Unreachability Detection и т. п), предполагаются соответствующими этому документу. Детали использования ND на каналах NBMA рассмотрены в [IPv6-NBMA]. В дополнение к этому в [IPv6-3GPP] и [IPv6-CELL] рассмотрено использование протокола на некоторых каналах сотовой связи, которые относятся к типу NBMA.

2. Терминология

2.1. Общие термины

IP

Протокол IP версии 6. В тех случаях, когда требуется различать версии, применяются обозначения IPv4 и IPv6.

ICMP

Протокол управляющих сообщений для IP версии 6. В тех случаях, когда требуется различать версии, применяются обозначения ICMPv4 и ICMPv6.

node - узел

Устройство, реализующее протокол IP.

router - маршрутизатор

Узел, которые пересылает пакеты, не адресованные явно ему.

host - хост

Любой узел, не являющийся маршрутизатором.

[1]Non-Broadcast Multi-Access - множественный доступ без широковещания.

upper layer - вышележащий уровень

Протокольный уровень, расположенный непосредственно над IP. Примерами могут служить транспортные протоколы TCP и UDP, протокол управления ICMP, протоколы маршрутизации, такие как OSPF, а также протоколы уровня Internet (или ниже) «туннелируемые» через IP (т. е. инкапсулируемые в IP), такие как IPX[1], AppleTalk, IP.

link - канал, соединение

Линия связи или среда, через которую узлы могут взаимодействовать на канальном уровне (уровень, непосредственно ниже IP). Примерами являются Ethernet (простая сеть или с мостами), Token Ring, каналы PPP, сети X.25, Frame Relay или ATM, туннели уровня Internet (или выше), такие как IPv4 или IPv6.

interface - интерфейс

Подключение узла к каналу.

neighbor - сосед

Узел, подключенный к тому же каналу.

address - адрес

Идентификатор уровня IP для интерфейса или набора интерфейсов.

anycast address - универсальный адрес

Идентификатор для множества интерфейсов (обычно относящихся к разным узлам). Пакет, переданный по адресу anycast доставляется одному из интерфейсов, указанных этим адресом («ближайшему» в соответствии с мерой удалённости протокола маршрутизации). См. [ADDR-ARCH].

Отметим, что адрес anycast синтаксически не отличается от индивидуального адреса. Поэтому узлы, передающие пакеты по адресу anycast, обычно не знают о применении такого адреса. Далее в этом документе все, сказанное для индивидуальных адресов, относится и к адресам anycast, если узел не знает, что индивидуальный адрес на самом деле является универсальным.

prefix - префикс

Начальные биты адреса или набор адресов IP, начальные биты которых совпадают.

link-layer address - адрес канального уровня

Идентификатор интерфейса на канальном уровне. Примеры включают адреса IEEE 802 для каналов Ethernet.

on-link - подключён к каналу

Адрес, назначенный интерфейсу на конкретном канале. Узел считается подключённым к каналу (on-link), при выполнении любого из условий:

- адрес входит в один из префиксов канала (например, как указано флагом on-link в опции Prefix Information);
- соседний маршрутизатор указывает адрес в качестве получателя сообщения Redirect;
- получено сообщение Neighbor Advertisement для (целевого) адреса;
- получено любое сообщение ND с этого адреса.

off-link - не подключён к каналу

Антитеза on-link. Адрес, не назначенный какому-либо из интерфейсов данного канала.

longest prefix match - максимальное соответствие префикса

Процесс выбора из набора префиксов, включающих целевой адрес. Адрес считается включённым в префикс, если все биты префикса совпадают с битами левой части адреса. При покрытии адреса множеством префиксов выбирается тот, в котором совпадает максимальное число битов.

reachability - доступность

Наличие (или отсутствие) корректно работающего одностороннего пути «пересылки» к соседу. В частности, доступность означает, что переданный соседу пакет доставляется на уровень IP соседней машины и соответствующим образом обрабатывается принимающим уровнем IP. Для соседнего маршрутизатора доступность означает, что пакеты, переданные IP-уровнем узла, доставляются уровню IP маршрутизатора и маршрутизатор действительно пересылает пакеты (т. е. настроен как маршрутизатор, а не хост). Для хостов доступность означает, что пакеты, отправленные IP-уровнем узла доставляются IP-уровню хоста.

packet - пакет

Заголовок IP и данные (payload).

link MTU - MTU для канала

Максимальный размер блока (пакета), который может быть в один приём передан через канал (в октетах).

target - цель

Адрес, для которого отыскивается информация о преобразовании, или адрес который будет новым первым интервалом пересылки при перенаправлении.

proxy - прокси, посредник

Узел, отвечающий на запросы ND от имени другого узла. Маршрутизатор, действующий от имени мобильного узла выступает для этого узла посредником.

ICMP destination unreachable indication - индикация ICMP о недоступности получателя

Индикация ошибки, возвращённая исходному отправителю пакета, который не удалось доставить по причинам, указанным в [ICMPv6]. Если ошибка возникает на узле, не являющемся инициатором пакета, генерируется сообщение ICMP об ошибке. Если ошибка возникает на узле-инициаторе, генерация и отправка сообщения ICMP об ошибке источнику не требуется, если отправитель вышележащего уровня уведомляется с помощью другого подходящего механизма (например, возврат кода ошибки вызванной процедурой). Следует отметить, что реализация может счесть удобным в некоторых случаях возвращать ошибку отправителю, беря вызвавший ошибку пакет, генерируя сообщение ICMP и затем доставляя его (локально) с использованием базовых процедур обработки ошибок.

random delay - случайная задержка

При передаче сообщений иногда требуется задержать отправку на случайный интервал времени для того, чтобы предотвратить одновременную передачу множеством узлов или устранить ненужную синхронизацию при периодической отправке сообщений [SYNC]. Когда требуется внести случайную составляющую, узел рассчитывает реальную задержку так, чтобы значения равномерно распределялись в диапазоне от минимальной до максимальной задержки. Разработчик должен учесть дискретность случайной компоненты и точность отсчёта таймера, чтобы снизить вероятность выбора одинаковой случайной задержки несколькими узлами.

random delay seed - «затравка» для случайной задержки

Если при расчёте случайной задержки используется генератор псевдослучайных чисел, этот генератор следует инициализировать с использованием уникальной «затравки» (seed) до начала использования. Отметим, что использования в качестве значения затравки идентификатора интерфейса не достаточно, поскольку эти

[1]Internetwork Packet Exchange - межсетевой обмен пакетами.

идентификаторы не всегда уникальны. Для снижения вероятности использования одинаковой затравки её значение должно определяться на основе данных из разных источников (например, узлов машины), которые с большой вероятностью будут различаться в разных устройствах. Например, затравку можно создавать из комбинации серийного номера CPU и идентификатора интерфейса. Дополнительную информацию о генерации случайных значений можно найти в [RAND].

2.2. Типы каналов

Свойства разных канальных уровней различаются. Ниже перечислены свойства, связанные с ND.

multicast capable - поддержка групповой адресации

Канал, который поддерживает естественный механизм канального уровня для передачи пакетов всем (широковещание) или части своих соседей.

point-to-point - «точка-точка»

Канал, соединяющий лишь два интерфейса. Предполагается, что канал «точка-точка» поддерживает групповую адресацию и имеет локальный (link-local) адрес.

non-broadcast multi-access (NBMA) - множественный доступ без широковещания

Канал, к которому может быть подключено два и более интерфейсов, но не поддерживается естественное широковещание или групповая адресация (например, X.25, ATM, Frame Relay). Предполагается, что все типы каналов (включая NBMA) поддерживают услуги групповой адресации для приложений, которым это нужно (например, с помощью multicast-серверов). Однако до конца не решён вопрос, следует ли ND использовать такие возможности или дополнительные механизмы, обеспечивающие эквивалентную поддержку групповой адресации для ND.

shared media - общая среда

Канал, который обеспечивает возможность прямых коммуникаций между множеством устройств, но подключённые узлы настроены так, что они не имеют полной информации о префиксах всех подключённых к каналу адресатов. Т. е. на уровне IP узлы одного канала могут не знать, что они являются соседями и по умолчанию связываться между собой через маршрутизатор. Примерами являются большие (коммутируемые) сети передачи данных общего пользования типа SMDS[1] и B-ISDN[2]. Такие сети называют также «большими облаками» (large cloud, [SH-MEDIA]).

variable MTU - переменный размер MTU

Канал, для которого нет общеизвестного значения MTU (например, IEEE 802.5 Token Ring). Многие каналы (например, Ethernet) имеют стандартное значение MTU, задаваемое протоколом канального уровня или отдельным документом, определяющим работу IP на основе данного канального уровня.

asymmetric reachability - асимметричная доступность

Канал, в котором несимметричная и/или непереходная доступность (связность) является нормальным состоянием. Асимметрия доступности означает, что пакеты проходят от A к B, но не проходят в обратном направлении. Непереходная доступность означает, что пакеты проходят от A к B и от B к C, но не проходят от A к C. Такими свойствами отличаются радиоканалы.

2.3. Адреса

При обнаружении соседей используется множество разных адресов, определённых в [ADDR-ARCH], включая перечисленные ниже.

Групповой адрес all-nodes

Адрес с локальной значимостью для доступа ко всем узлам - FF02::1.

Групповой адрес all-routers

Адрес с локальной значимостью для доступа ко всем маршрутизаторам - FF02::2.

Групповой адрес solicited-node

Групповой адрес с локальной значимостью, который определяется как функция адреса запрошенной цели. Функция описана в [ADDR-ARCH] и выбирается так, что адреса IP, различающиеся только старшими битами (например, при наличии множества префиксов от разных провайдеров), будут отображаться на один адрес solicited-node, что снижает число групповых адресов, которые узел должен присоединить на канальном уровне.

Адрес link-local (локальный)

Индивидуальный адрес с локальной значимостью, который может использоваться для доступа к соседям. Все интерфейсы маршрутизаторов **должны** иметь адреса link-local. Документ [ADDRCONF] требует наличия таких адресов и у интерфейсов хоста.

Незаданный адрес

Зарезервированное значение, которое указывает отсутствие адреса (например, он не известен). Это значение никогда не для получателя, но может служить адресом отправителя, если тот (ещё) не знает своего адреса (например, при проверке незанятости адреса при автоматической настройке конфигурации без учёта состояния [ADDRCONF]). Этот адрес имеет значение 0:0:0:0:0:0:0:0.

Отметим, что данная спецификация не следует строго требованиям согласованности [ADDR-SEL] для области действия адресов получателя и отправителя. В некоторых случаях хосты могут использовать адрес отправителя с большей областью действия, чем у адреса получателя в заголовке IPv6.

2.4. Требования

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

В документе используются внутренние концептуальные переменные для описания поведения протокола и внешние переменные, которые реализация должна позволять устанавливать системному администратору. Имена переменных, способы их изменения и влияние значений переменных на поведение протокола приведены в примерах. Реализации не обязаны точно следовать этим примерам, достаточно обеспечить соответствие видимого извне поведения.

[1]Switched Multimegabit Data Service - коммутируемые услуги передачи данных со скоростью во много Мбит/с.
[2]Broadband Integrated Services Digital Network - широкополосная цифровая сеть с интеграцией услуг.

3. Обзор протокола

Этот протокол решает множество проблем, связанных с взаимодействием между узлами, подключёнными к одному каналу. Протокол определяет механизмы для решения перечисленных ниже проблем.

Router Discovery - обнаружение маршрутизаторов
Способ обнаружения хостом маршрутизаторов, подключённых к каналу.

Prefix Discovery - обнаружение префиксов
Способ обнаружения хостом набора префиксов, определяющего адреса на подключённом канале (on-link). Узлы применяют префиксы, чтобы отличить адресатов на канале от доступных лишь через маршрутизатор.

Parameter Discovery - определение параметров
Способ определения узлом параметров канала (например, MTU) или Internet (например, значения hop limit) для учёта в исходящих пакетах.

Address Autoconfiguration - автоматическая настройка адреса
Механизмы, требуемые для того, чтобы позволить узлам настраивать адрес интерфейса без учёта состояния. Спецификация автоматической настройки без учёта состояния приведена в [ADDRCONF].

Address resolution - распознавание адресов
Определение адреса канального уровня для получателя на том же канале (например, соседа) по его IP-адресу.

Next-hop determination - определение следующего интервала
Алгоритм отображения IP-адреса получателя на IP-адрес соседа, которому следует пересылать трафик для получателя. Следующим интервалом (next-hop) может быть маршрутизатор или сам получатель.

Neighbor Unreachability Detection (NUD) - обнаружение недоступности соседа
Способ, с помощью которого узлы определяют потерю доступности соседа. Для недоступных соседей-маршрутизаторов может предприниматься попытка использовать принятый по умолчанию маршрутизатор. Для маршрутизаторов и хостов может повторяться попытка распознавания адреса.

Duplicate Address Detection (DAD) - детектирование дубликатов адресов
Способ определения доступности желаемого адреса для использования (не занят ли он другим узлом).

Redirect - перенаправление
Способ информирования маршрутизатором хоста о лучшем первом интервале пересылки (first-hop) для определённого адресата.

ND определяет 5 различных типов пакетов ICMP - пары Router Solicitation и Router Advertisement, Neighbor Solicitation и Neighbor Advertisement, а также Redirect.

Router Solicitation (RS) - запрос маршрутизатора
Когда интерфейс включается, хост может передавать сообщения RS, запрашивающие у маршрутизаторов генерацию анонса RA раньше запланированного времени.

Router Advertisement (RA) - анонс маршрутизатора
Маршрутизаторы анонсируют своё присутствие вместе с различными параметрами каналов и Internet периодически или в ответ на сообщение RS. Сообщения RA содержат префиксы, которые используются для проверки, использует ли другой адрес тот же канал (on-link) и/или конфигурацию адреса, определения предложенного значения hop limit и т. п..

Neighbor Solicitation (NS) - запрос соседства
Передаётся узлом для определения соседского адреса канального уровня или проверки доступности соседа по кэшированному адресу канального уровня. Сообщения NS служат также для обнаружения дубликатов адресов (Duplicate Address Detection или DAD).

Neighbor Advertisement (NA) - анонс соседа
Отклик на сообщение Neighbor Solicitation. Узел может также передавать незапрошенные сообщения NA для анонсирования смены своего адреса канального уровня.

Redirect - перенаправление
Используется маршрутизаторами для информирования хостов о наилучшем первом интервале для адресата.

На каналах с поддержкой групповой адресации каждый маршрутизатор периодически отправляет групповой пакет RA, анонсирующий его доступность. Хост, получивший RA от всех маршрутизаторов, создаёт список используемых по умолчанию маршрутизаторов. Маршрутизаторы генерируют RA достаточно часто, чтобы хосты узнавали о присутствии маршрутизатора в течение нескольких минут, но недостаточно часто для детектирования отказов по отсутствию анонсов. Для обнаружения отказов применяется специальный алгоритм обнаружения недоступности соседа (NUD).

Анонс маршрутизатора содержит список префиксов, используемых для определения принадлежности к каналу и/или автономной настройки адресов. Связанные с префиксом флаги задают предполагаемое использование конкретного префикса. Хосты применяют анонсированные для канала префиксы для создания и поддержки списка, применяемого при решении вопроса о присутствии адресата на данном канале или за маршрутизатором. Отметим, что адресат может относиться к данному каналу даже в случае, когда анонсируемый префикс не включает его. В таких случаях маршрутизатор может передать Redirect для информирования отправителя о том, что адресат является соседом.

Анонсы маршрутизаторов и флаги префиксов в них позволяют маршрутизаторам информировать хосты о способах автоматической настройки адресов (Address Autoconfiguration). Например, маршрутизатор может указывать хостам использование DHCPv6 и/или автономную настройку адресов (без учёта состояния).

Сообщение RA содержит также параметры Internet, такие как максимальное число интервалов пересылки (hop limit), которое хосту следует указывать в исходящих пакетах, и (необязательно) параметры канала, такие как MTU. Это упрощает централизованное администрирование важных параметров, которые маршрутизаторы могут задавать и распространять автоматически всем подключённым хостам.

Узлы распознают адреса путём групповой передачи сообщений NS, запрашивающих у соседей их адреса канального уровня. Сообщения NS передаются по групповому адресу solicited-node целевых узлов. Эти узлы возвращают свои адреса канального уровня в сообщениях NA. Одной пары пакетов «запрос-отклик» инициатору и цели достаточно для того, чтобы узнать адрес канального уровня другой стороны. Инициатор включает свой адрес канального уровня в сообщение NS. Сообщения NS могут также применяться для обнаружения дубликатов индивидуальных адресов, как описано в [ADDRCONF].

Механизм NUD обнаруживает отказы соседей или пути пересылки к ним. Для этого требуются подтверждения доставки пакетов соседу и их подобающей обработки уровнем IP у этого соседа. NUD использует подтверждения из двух источников. Когда это возможно, протоколы вышележащих уровней подтверждают, что соединение обеспечивает пересылку (forward progress), т. е. отправленные данные были корректно доставлены, например, отправляя подтверждения о доставке пакетов. Когда подтверждений через такие «подсказки» нет, узел передаёт индивидуальные сообщения NS, которые запрашивают отправку NA в качестве подтверждения доступности от следующего узла пересылки (next hop). Для снижения уровня трафика пробные сообщения передаются лишь соседям, которым узел активно передаёт пакеты.

Помимо решения отмеченных выше задач ND обслуживает перечисленные ниже ситуации.

Смена адреса канального уровня

Узел, знающий о смене своего адреса канального уровня может передать несколько (незапрошенных) групповых пакетов NA всем узлам для быстрого обновления кэшированного адреса, который изменился. Отметим, что отправка незапрошенных анонсов служит лишь повышению производительности (не является надёжной), а алгоритм NUD обеспечивает надёжное обнаружение нового адреса, хотя задержка может быть больше.

Балансировка нагрузки на входе

Узлы с реплицированными интерфейсами могут распределять нагрузку при приёме входящих пакетов между несколькими интерфейсами на одном канале. У таких узлов одному интерфейсу соответствует несколько адресов канального уровня. Например, один драйвер может представлять несколько сетевых адаптеров как один логический интерфейс с множеством адресов канального уровня.

ND позволяет маршрутизатору распределять нагрузку для адресованного ему трафика, разрешая опускать адрес отправителя на канальном уровне в пакетах RA, что вынуждает использовать сообщения NS для определения адресов маршрутизаторов на канальном уровне. Возвращаемые сообщения NA могут тогда содержать адреса канального уровня, которые различаются, например, в зависимости от инициатора запроса. Эта спецификация не задаёт механизмов, позволяющих хостам распределять нагрузку для входящих пакетов (см. [LD-SHRE]).

Anycast-адреса

Anycast-адрес указывает один из набора узлов, обеспечивающих эквивалентные услуги или настраиваемых так, что они способны распознаваться по одному anycast-адресу. ND обрабатывает anycast в предположении получения множества NA для одной цели. Все анонсы anycast-адресов помечаются как non-Override (без переопределения) и не обновляют (не заменяют) информацию, переданную в других анонсах. Эти анонсы далее обсуждаются в контексте сообщений NA. Это вызывают определённые правила для выбора используемых анонсов из числа имеющихся.

Прокси-анонсы

Узел, желающий воспринимать пакеты от имени целевого адреса, не способного отвечать на сообщения NS, может выдавать NA без переопределения. Прокси-анонсы применяются домашними агентами Mobile IPv6 для защиты адреса мобильного устройства при его уходе с канала. Однако это не предназначено для использования в качестве механизма общего назначения, для обработки узлов, которые, например, не реализуют этот протокол.

3.1. Сравнение с IPv4

Протокол обнаружения соседей IPv6 ND соответствует комбинации протоколов IPv4 ARP[1] [ARP], ICMP Router Discovery [RDISC] и ICMP Redirect [ICMPv4]. В IPv4 нет единого протокола или механизма обнаружения недоступности соседа (NUD), хотя в документе Hosts Requirements [HR-CL] указаны возможные алгоритмы обнаружения «мёртвых» шлюзов (Dead Gateway Detection), решающего часть этих задач.

Протокол обнаружения соседей обеспечивает множество улучшений по сравнению с набором протоколов IPv4.

Router Discovery является частью базового протокола и хостам не нужно «влезать» в протоколы маршрутизации.

Сообщения RA содержат адрес канального уровня и не требуется дополнительного обмена пакетами для определения адреса маршрутизатора на канальном уровне.

Сообщения RA содержат префикс для канала, поэтому не нужен отдельный механизм настройки маски сети.

Сообщения RA позволяют автоматически настраивать адреса (Address Autoconfiguration).

Маршрутизаторы могут анонсировать хостам значение MTU на канале, что позволяет всем узлам использовать одно значение MTU на каналах без чётко заданного MTU.

Групповые рассылки распознавания адресов «разбросаны» по 16 миллионам (2^{24}) групповых адресов, что существенно сокращает связанные с распознаванием адресов прерывания на узлах, не являющихся целью. Кроме того, машины, не относящиеся к IPv6 не получают таких прерывания совсем.

Сообщения Redirect включают адрес канального уровня для нового первого узла пересылки (first hop) и не требуется специально распознавать адрес.

С одним каналом может быть связано множество префиксов. По умолчанию хост узнает все префиксы на канале из сообщений RA. Однако на маршрутизаторах можно задать исключение части или всех префиксов из RA. В таких случаях хосты предполагают, что адресаты находятся вне канала (off-link) и передают трафик маршрутизаторам. При необходимости маршрутизатор может выдавать сообщения Redirect.

В отличие от IPv4, получатель IPv6 Redirect предполагает, что новый следующий узел пересылки (next-hop) находятся на канале. В IPv4 хост игнорирует перенаправления, задающие next-hop вне канала, в соответствии с настроенной для канала маской сети. Механизм перенаправления в IPv6 похож на функцию Xredirect, заданную в [SH-MEDIA]. Предполагается, что он будет полезен на каналах с общей средой без широковещания, где узлам нежелательно или невозможно знать все префиксы, находящихся на канале адресатов.

Обнаружение недоступности соседей является частью базового протокола, что значительно повышает надёжность доставки пакетов в случае отказов маршрутизаторов, частичных отказов или разделения каналов и смены узлами адресов канального уровня. Например, мобильные узлы могут уходить с канала без потери связности в результате устаревания кэша ARP.

[1]Address Resolution Protocol - протокол распознавания адресов.

В отличие от ARP, протокол ND обнаруживает отказы «полуканалов» (с помощью NUD) и позволяет избежать отправки трафика соседям, с которыми нет двухсторонней связности.

Поле предпочтений в RA не требуется для работы с маршрутизаторами, различающимися «стабильностью»; NUD обнаружит «мёртвые» маршрутизаторы и переключит на работающие.

Использование адресов link-local для однозначной идентификации маршрутизаторов (в сообщениях RA и Redirect) позволяет хостам поддерживать связь с маршрутизаторами в случаях смены сайтом глобального префикса.

Установка Hop Limit 255 делает ND защищённым от отправителей вне канала (off-link), случайно или преднамеренно передающих сообщения ND. В IPv4 такие отправители могут передавать сообщения ICMP Redirect и RA.

Размещение распознавания адресов на уровне ICMP делает протокол более независимым от среды по сравнению с ARP и позволяет использовать базовые механизмы уровня IP для проверки подлинности и защиты.

3.2. Поддерживаемые типы каналов

Протокол ND работает на каналах с различными свойствами и в некоторых случаях возможна поддержка этой спецификацией лишь части механизмов обнаружения соседей.

Соединения «точка-точка»

ND обслуживает такие соединения подобно групповым (групповую рассылку можно тривиально реализовать на каналах «точка-точка», а интерфейсам можно выделять адреса link-local).

Групповая адресация

ND работает по каналам с поддержкой групповой адресации в соответствии с этим декрементом.

Каналы с множественным доступом без широковещания (NBMA)

Redirect, NUD и определение next-hop следует реализовать в соответствии с этим документом. Распознавание адресов и механизмы доставки сообщений RS и RA на каналах NBMA не заданы в этом документе. Отметим, что хост с возможностью настройки вручную списка используемых по умолчанию маршрутизаторов может динамически получать адреса канального уровня своих соседей из сообщений Redirect.

Общая среда

Сообщение Redirect создано на основе XRedirect в [SH-MEDIA] для упрощения использования протокола на каналах с общим доступом. Эта спецификация не решает для сред с общим доступом вопросов, связанных с маршрутизаторами:

- способ обмена сведения о доступности между маршрутизаторами через канал с общим доступом;
- способ определения маршрутизаторов адреса хоста на канальном уровне при необходимости передать хосту сообщение о перенаправлении;
- способ определения маршрутизатором первого маршрутизатора для пересылки полученного пакета.

Протокол является расширяемым (новые опции) и в будущем могут быть предложены новые решения.

Переменное значение MTU

ND позволяет маршрутизаторам задавать значение MTU для канала, которое будут применять узлы. Для корректной работы групповой рассылки все узлы на канале должны использовать одно значение MTU (или MRU[1]), иначе отправитель, который может не знать, какие узлы получат пакет, не сможет определить размер пакета, который способны обработать все получатели (MRU).

Асимметричная доступность

ND обнаруживает отсутствие симметричной доступности и узел будет избегать пути к соседу, с которым у него нет двухсторонней связности. Механизм NUD обычно будет обнаруживать такие «полусоединения» и узел сможет воздержаться от их использования. Предполагается, что в будущем протокол может быть расширен для поиска жизнеспособных путей в средах без возвратной и переходной связности.

3.3. Защита сообщений Neighbor Discovery

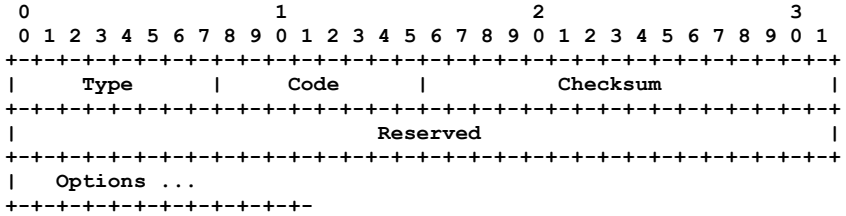
Сообщения ND нужны для решения разных задач. Некоторые функции предназначены для обеспечения хостам возможности заявлять о владении адресом или сопоставлением адреса канального уровня с адресом IP. Связанные с ND уязвимости рассмотрены в параграфе 11.1. Общее решение по защите ND выходит за рамки этой спецификации и рассмотрено в [SEND]. Однако в параграфе 11.2 рассматривается возможность применения протоколов IPsec Authentication Header (AH) и Encapsulating Security Payload (ESP) для защиты Neighbor Discovery.

4. Формат сообщений

В этом разделе даны определения формата всех сообщений, используемых в данной спецификации.

4.1. Формат сообщения RS

Хост передаёт сообщения с запросом маршрутизатора (Router Solicitation или RS), приглашающие маршрутизаторы быстро создать свои анонсы (Router Advertisement или RA).



Поля IP

Source Address

IP-адрес передающего интерфейса или незаданный (unspecified) адрес при отсутствии адреса на интерфейсе.

Destination Address

Обычно групповой адрес all-routers (все маршрутизаторы).

[1]Maximum Receive Unit - максимальный размер принимаемого блока.

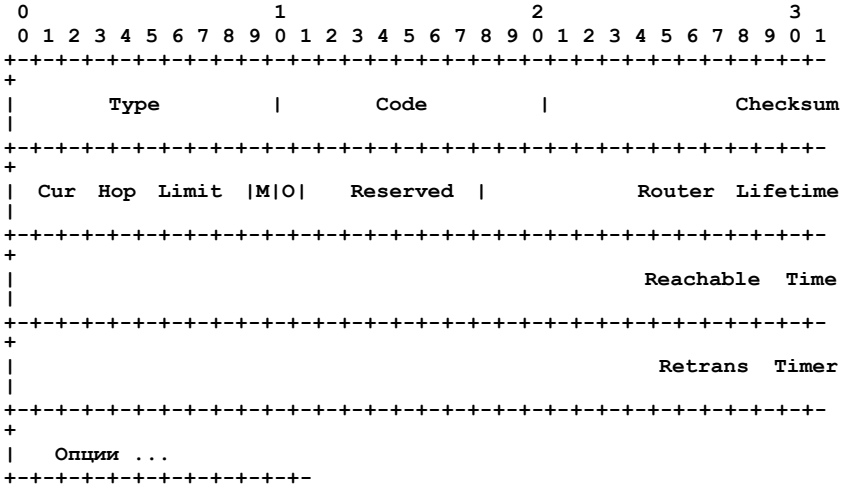
Hop Limit
255
Поля ICMP

Type
133
Code
0
Checksum
Контрольная сумма ICMP [ICMPv6].
Reserved
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.
Допустимые опции

Source link-layer address
Адрес отправителя на канальном уровне, если он известен. Этот адрес **недопустимо** включать, если в поле Source Address содержится неуказанный адрес. В остальных случаях поле **следует** включать для канальных уровней с адресами.
В будущих версиях протокола могут быть добавлены новые опции. Получатели **должны** игнорировать неизвестные опции и продолжать обработку сообщения.

4.2. Формат сообщения RA

Маршрутизаторы передают свои анонсы (Router Advertisement или RA) периодически и в ответ на запросы RS.



Поля IP

Source Address
Должно содержать адрес канального уровня, назначенный передающему сообщение интерфейсу.
Destination Address
Обычно это поле Source Address из соответствующего сообщения RS или групповой адрес all-nodes.
Hop Limit
255
Поля ICMP

Type
134
Code
0
Checksum
Контрольная сумма ICMP [ICMPv6].
Cur Hop Limit
8-битовое целое число без знака, указывающее принятое по умолчанию значение, которое следует помещать в поле Hop Count заголовка IP исходящих пакетов. 0 соответствует незаданному (этим маршрутизатором) значению.
M
Флаг управляемой настройки адресов, установка которого указывает, что адреса доступны по протоколу DHCP [DHCPv6]. При установленном флаге M флаг O становится избыточным и может игнорироваться, поскольку DHCPv6 будут возвращать все доступные данные конфигурации.
O
Флаг дополнительной конфигурации, установка которого указывает доступность по протоколу DHCPv6 других конфигурационных данных. Примерами таких данных являются сведения о DNS или других серверах в сети.
Примечание. Если оба флага M и O сброшены, это говорит о недоступности данных по протоколу DHCPv6.
Reserved
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.
Router Lifetime
16-битовое целое число без знака, указывающее срок действия принятого по умолчанию маршрутизатора в секундах. Поле может содержать значение до 65535 и получателям следует обрабатывать любые значения, хотя правила отправки в разделе 6 ограничивают срок действия 9000 секунд. Значение 0 указывает, что маршрутизатор не используется по умолчанию и его **не следует** включать в соответствующий список. Значение Router Lifetime указывает лишь применимость маршрутизатора по умолчанию и не относится к данным, содержащимся в других полях и опциях сообщения. Опции с ограниченным сроком действия имеют свои поля срока действия.

Reachable Time

32-битовое целое число без знака, указывающее срок, в течение которого сосед считается доступным после приёма подтверждения доступности (в миллисекундах). Значение применяется алгоритмом NUD (7.3. Алгоритм NUD). 0 указывает, что значение не задано этим маршрутизатором.

Retrans Timer

32-битовое целое число без знака, указывающее интервал между сообщениями NS в миллисекундах, используемый алгоритмом NUD (см. 7.2. Распознавание адресов и 7.3. Алгоритм NUD). 0 указывает, что значение не задано этим маршрутизатором.

Возможные опции

Source link-layer address

Адрес канального уровня интерфейса, передающего сообщение RA. Применяется лишь для канальных уровней с адресацией. Маршрутизатор **может** опустить эту опцию для включения балансировки входного трафика через множество адресов канального уровня.

MTU

Следует передавать для каналов с переменным MTU (как указано в документе, описывающем применение IP для канального уровня). **Может** передаваться в другие каналы.

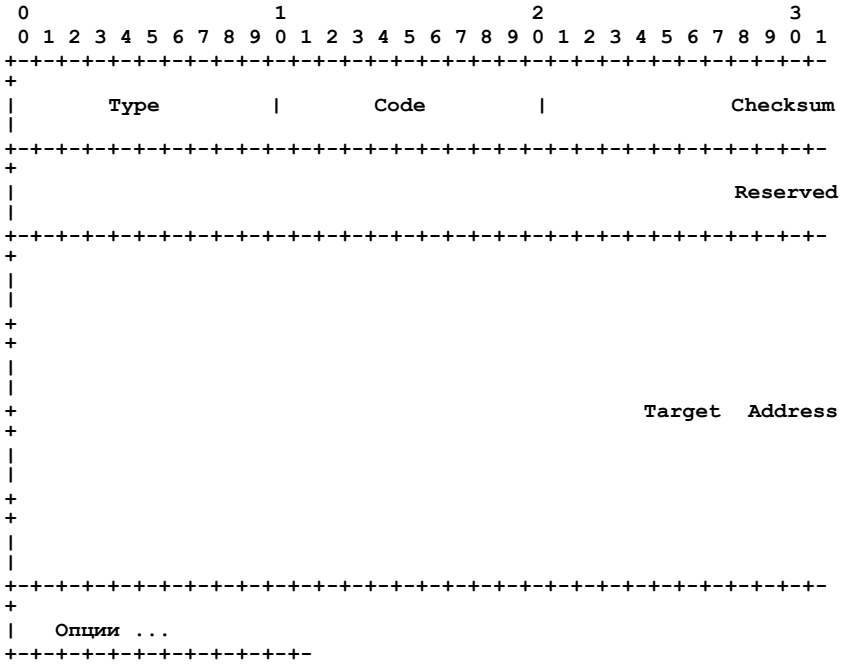
Prefix Information

Задаёт префиксы, относящиеся к каналу и,или используемые для автоматической настройки адресов без учёта состояния. Маршрутизатору **следует** включать все свои префиксы on-link (за исключением префикса link-local), чтобы многодомные хосты имели полные сведения об адресатах, связанных с каналом, куда они подключены. При отсутствии полной информации хост с несколькими интерфейсами не сможет корректно выбрать выходной интерфейс для передачи трафика своим соседям.

В будущих версиях протокола могут быть добавлены новые опции. Получатели **должны** игнорировать неизвестные опции и продолжать обработку сообщения.

4.3. Формат сообщения NS

Узлы передают запросы соседства (Neighbor Solicitation или NS) для получения адреса канального уровня целевого узла, а также указания тому своего адреса на канальном уровне. Сообщения NS являются групповыми, когда узлу нужно распознать адрес, и индивидуальными при проверке узлом доступности соседа.



Поля IP

Source Address

Адрес передающего сообщение интерфейса или незаданный адрес (при использовании DAD [ADDRCONF]).

Destination Address

Групповой адрес solicited-node, соответствующий адресу цели, или адрес самой цели.

Hop Limit

255

Поля ICMP

Type

135

Code

0

Checksum

Контрольная сумма ICMP [ICMPv6].

Reserved

Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

Target Address

IP-адрес цели запроса. Указание группового адреса **недопустимо**.

Возможные опции

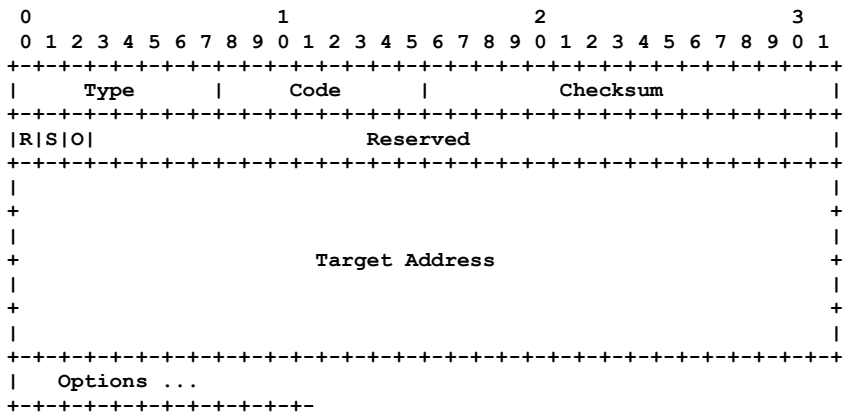
Source link-layer address

Адрес канального уровня для отправителя. Опцию недопустимо включать, если IP-адрес отправителя не задан. В иных случаях при наличии адресов канального уровня эта опция **должна** включаться в групповые запросы и её **следует** включать в индивидуальные запросы.

В будущих версиях протокола могут быть добавлены новые опции. Получатели **должны** игнорировать неизвестные опции и продолжать обработку сообщения.

4.4. Формат сообщения NA

Узел передаёт анонсы соседства (Neighbor Advertisement или NA) в ответ на сообщения NS, а также передаёт незапрошенные NA для быстрого распространения новой информации (без гарантии).



Поля IP

Source Address

Адрес передающего сообщение интерфейса.

Destination Address

Для запрошенных анонсов - Source Address из соответствующего сообщения NS или групповой адрес all-nodes, если в Source Address содержится неуказанный адрес. Для незапрошенных анонсов - обычно групповой адрес all-nodes.

Hop Limit

255

Поля ICMP

Type

136

Code

0

Checksum

Контрольная сумма ICMP [ICMPv6].

R

Флаг, установка которого говорит, что отправитель является маршрутизатором. Флаг R применяет механизм NUD для обнаружения перехода маршрутизатора в статус хоста.

S

Флаг, установка которого говорит, что анонс передан в ответ на сообщения NS от Destination Address. Этот флаг служит подтверждением доступности для NUD. Флаг **недопустимо** устанавливать в групповых анонсах и незапрошенных индивидуальных анонсах.

O

Флаг переопределения, установка которого указывает, что анонсу следует переопределить имеющуюся кэш-запись и обновить кэшированный адрес канального уровня. При сброшенном флаге анонс не будет обновлять кэшированный адрес канального уровня, но обновит имеющуюся запись NCE[1], для которой известен адрес канального уровня. Флаг **не следует** устанавливать в запрошенных анонсах для адресов anycast и в запрошенных прокси-анонсах, в остальных случаях флаг **следует** устанавливать.

Reserved

Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

Target Address

Для запрошенных анонсов это поле Target Address из соответствующего NS, для незапрошенных - адрес, для которого изменился адрес канального уровня. В поле Target Address **недопустимо** указывать групповой адрес.

Возможные опции

Target link-layer address

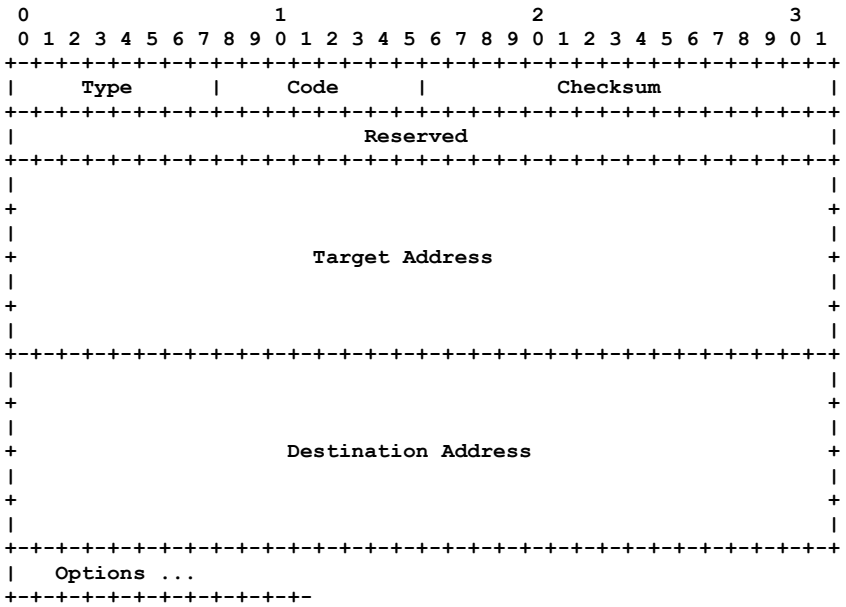
Адрес канального уровня для цели, т. е. отправителя анонса. Эта опция **должна** включаться для канальных уровней с адресацией при отклике на групповые запросы, а также **следует** включать её в отклики на индивидуальные NS. Опция **должна** включаться для групповых запросов во избежание «бесконечной» рекурсии NS, когда у партнерского узла нет кэшированной записи для возврата в сообщении NA. При откликах на индивидуальные запросы опцию можно опускать, поскольку у отправителя запроса имеется корректный адрес канального уровня (без него тот не смог бы отправить индивидуальный запрос). Однако включение адреса канального уровня в таких случаях не ведёт к чрезмерным издержкам и избавляет от возможных проблем при удалении отправителем кэшированного адреса канального уровня до получения отклика на запрос.

В будущих версиях протокола могут быть добавлены новые опции. Получатели **должны** игнорировать неизвестные опции и продолжать обработку сообщения.

[1]Neighbor Cache entry - кэш-запись для соседа.

4.5. Формат сообщения Redirect

Маршрутизаторы передают сообщения Redirect для информирования хоста о лучшем первом узле пересылки (first-hop) на пути к адресату. Хосты могут перенаправляться на более подходящий маршрутизатор или получать сведения о том, что адресат является соседом. Последнее обеспечивается установкой в поле ICMP Target Address значения ICMP Destination Address.



Поля IP

Source Address
Должно содержать адрес link-local, назначенный передающему сообщение интерфейсу.

Destination Address
Source Address из пакета, вызвавшего сообщение о перенаправлении.

Hop Limit
255

Поля ICMP

Type
137

Code
0

Checksum
Контрольная сумма ICMP [ICMPv6].

Reserved
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

Target Address
IP-адрес лучшего следующего узла пересылки для использования в ICMP Destination Address. Если целью является фактическая конечная точка (адресат является соседом), поле **должно** содержать значение, поля ICMP Destination Address. В иных случаях целью является наиболее подходящий маршрутизатор first-hop и поле **должно** содержать адрес link-local этого маршрутизатора, по которому хост может однозначно идентифицировать его.

Destination Address
IP-адрес получателя, который перенаправляется на указанную цель.

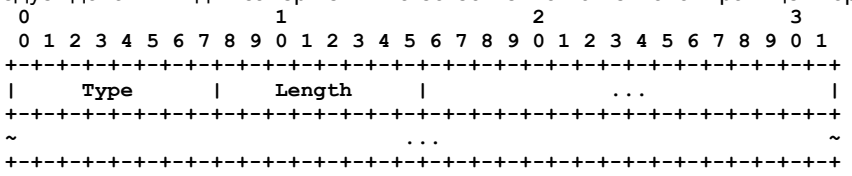
Возможные опции

Target link-layer address
Адрес канального уровня для цели, который **следует** включать (если он известен). Отметим, что на каналах NBMA хосты могут применять опцию Target Link-Layer Address в сообщениях Redirect как способ определения адреса соседа на канальном уровне. В таких случаях опция **должна** включаться в сообщения Redirect.

Redirected Header
Максимально возможная часть пакета IP, вызвавшего отправку Redirect, без превышения перенаправленным пакетом минимального значения MTU, заданного в [IPv6].

4.6. Формат опций

Сообщения ND могут включать опции, часть которых может указываться неоднократно в одном сообщении. Опции при необходимости следует дополнять для завершения на естественной 64-битовой границе. Формат опции показан ниже.



Type
8-битовый идентификатор типа опции. Определённые в этом документе опции приведены в таблице.

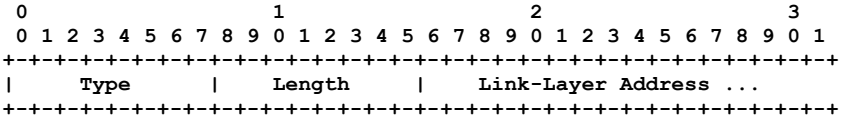
Имя опции	*Тип*
Source Link-Layer Address	1
Target Link-Layer Address	2

Prefix Information	3
Redirected Header	4
MTU	5

Length

8-битовое целое число без знака, указывающее размер опции (все поля) в 8-октетных словах. Значение 0 недействительно и узлы **должны** отбрасывать без уведомления отправителя пакеты ND с опцией размера 0.

4.6.1. Адрес канального уровня отправителя или цели



Type

1 для Source Link-layer Address, 2 для Target Link-layer Address.

Length

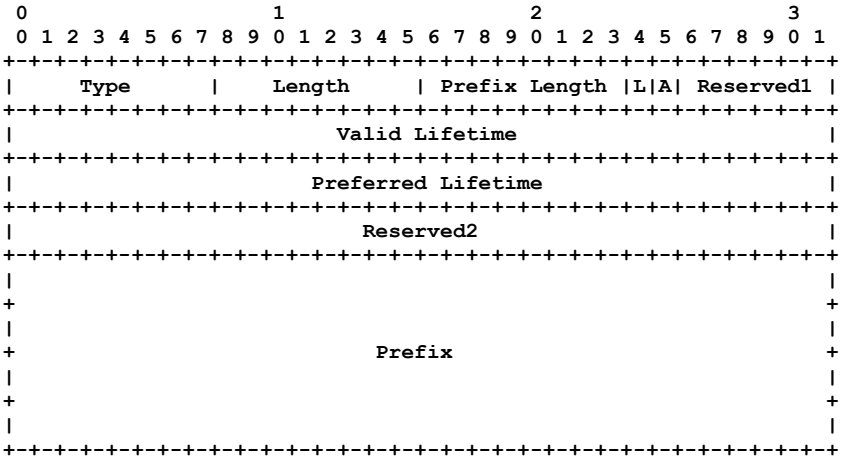
Размер опции (все поля) в 8-октетных словах. Например, размер адреса IEEE 802 составляет 1 [IPv6-ETHER].

Link-Layer Address

Поле переменного размера с адресом канального уровня. Содержимое поля, включая порядок битов и байтов, задано в документах, описывающих IPv6 для соответствующего канального уровня, например, [IPv6-ETHER].

Опция Source Link-Layer Address содержит адрес канального уровня для отправителя пакета и применяется в пакетах NS, RS и RA. Опция Target Link-Layer Address содержит адрес канального уровня для цели и применяется в пакетах NA и Redirect. В остальных сообщениях ND эти опции **должны** игнорироваться.

4.6.2. Информация о префиксе



Type

3

Length

4

Prefix Length

8-битовое целое число без знака, указывающее число действительных начальных битов поля Prefix (0 - 128). Это поле обеспечивает сведения для определения принадлежности к каналу (в комбинации с флагом L), а также помогает при автоматической настройке адресов [ADDRCONF], где могут быть ограничения на размер префикса.

L

Флаг присутствия на канале, указывающий, что этот префикс может служить для определения принадлежности к каналу. При сброшенном флаге анонс ничего не говорит о принадлежности префикса к каналу. Иными словами, если флаг L сброшен, хосту **недопустимо** считать, что выведенный из префикса адрес не относится к каналу (off-link), т. е. **недопустимо** обновлять прежнюю индикацию принадлежности адреса к каналу (on-link).

A

Флаг автономной настройки адреса, установка которого указывает возможность применения префикса для настройки адресов без учёта состояния, как задано в [ADDRCONF].

Reserved1

Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

Valid Lifetime

32-битовое целое число без знака, указывающее срок действия префикса для определения принадлежности к каналу (в секундах с момента отправки пакета). Значение, содержащее только 1 (0xffffffff), указывает неограниченный срок действия. Значение Valid Lifetime используется также в [ADDRCONF].

Preferred Lifetime

32-битовое целое число без знака, указывающее срок (в секундах с момента отправки пакета), в течение которого адрес, созданный из префикса процедурой автоматической настройки адресов без учёта состояния [ADDRCONF], остаётся предпочтительным. Значение, содержащее только 1 (0xffffffff), указывает неограниченный срок. В этом поле **недопустимы** значения больше Valid Lifetime, чтобы недействительный адрес на стал предпочтительным.

Reserved2

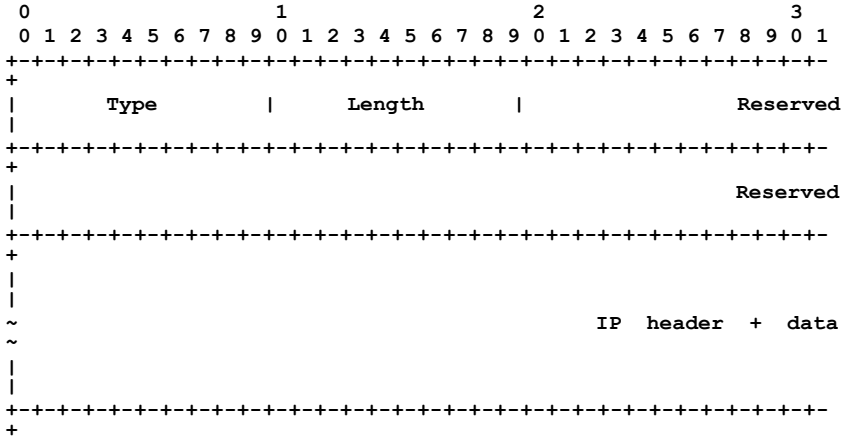
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

Prefix

IP-адрес или префикс IP. Поле Prefix Length указывает число действительных начальных битов префикса. Биты, расположенные после, **должны** устанавливаться в 0 отправителем и игнорироваться получателем. Маршрутизатору **не следует** передавать префикс для link-local, а хостам **следует** игнорировать такие опции.

Опция Prefix Information предоставляет хостам относящиеся к каналу префиксы и префиксы для автоматической настройки адресов. Опция применяется в пакетах RA и **должна** игнорироваться в других сообщениях.

4.6.3. Заголовок перенаправления



Type
4

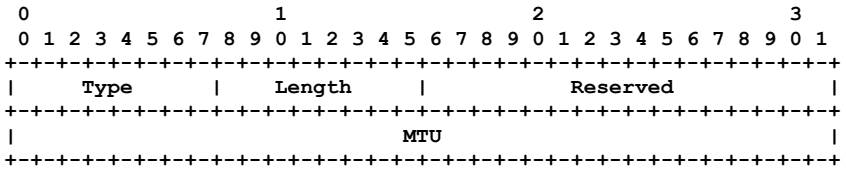
Length
Размер опции в 8-октетных словах.

Reserved
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

IP header + data
Исходный пакет, усечённый так, чтобы размер перенаправленного сообщения не превышал минимальное значение MTU требуемое для поддержки IPv6 [IPv6].

Опция Redirected Header применяется в сообщениях Redirect и содержит весь или часть пакета, который перенаправляется. Опция **должна** игнорироваться в других сообщениях ND.

4.6.4. MTU



Type
5

Length
1

Reserved
Резервное поле, которое **должно** устанавливаться отправителем в 0, а получатель **должен** игнорировать поле.

MTU
32-битовое целое число без знака, указывающее рекомендуемое для канала значение MTU.

Опция MTU применяется в сообщениях RA для того, чтобы все узлы на канале использовали одно значение MTU в случаях, когда MTU на канале не является общеизвестным. Эта опция **должна** игнорироваться в иных сообщениях ND.

В конфигурациях, где с помощью мостов собраны разнородные технологии, максимальное значение MTU может меняться от сегмента к сегменту. Если мосты не создают сообщений ICMP Packet Too Big, взаимодействующие узлы не смогут применять Path MTU для динамического определения подходящего MTU по каждому соседу. В таких случаях можно настроить маршрутизаторы на использование опции MTU для задания максимального значения MTU, поддерживаемого всеми сегментами.

5. Концептуальная модель хоста

В этом разделе рассматривается концептуальная модель возможной структуры данных, которую хосты (с некоторыми исключениями и маршрутизаторы) могут поддерживать для взаимодействия с соседями. Модель предназначена для того, чтобы упростить разъяснение поведения протокола ND. Документ не требует от реализаций следовать этой модели, если их внешнее поведение соответствует описанному в этом документе.

Модель рассматривает лишь аспекты поведения узла, связанные с обнаружением соседей. В частности, не рассматриваются такие вопросы, как выбор адреса отправителя или выходного интерфейса на многодомном хосте.

5.1. Концептуальные структуры данных

Хост будет поддерживать для каждого интерфейса указанную ниже информацию.

Neighbor Cache - кэш соседей
Набор записей об отдельных соседях, которым недавно передавался трафик. Записи привязаны к относящимся к каналу индивидуальным IP-адресам соседа и содержат такие данные, как адрес канального уровня, флаг, указывающий, является сосед маршрутизатором или хостом (IsRouter в этом документе), указатель на пакеты в очереди, ожидающие распознавания адреса и т. п. Запись NCE может также включать сведения, используемые алгоритмом NUD, включая статус доступности, число безответных проб и время, но которое запланировано следующее событие NUD.

Destination Cache - кэш адресатов
набор записей об адресатах, которым недавно отправлялся трафик. Записи относятся к адресатам на канале и вне его и обеспечивают уровень косвенных обращений к кэшу соседей - кэш адресатов сопоставляет IP-адреса

получателей с IP-адресами соседа next-hop. Этот кэш обновляется сведениями из сообщений Redirect. Разработчики могут счесть удобным размещение в кэше дополнительных данных, не связанных напрямую с ND, например Path MTU (PMTU) и время кругового обхода от транспортных протоколов.

Prefix List - список префиксов

Список префиксов, определяющих набор адресов на канале. Записи списка создаются из данных в сообщениях RA и каждая из них имеет таймер аннулирования (извлекается из анонса RA), используемый для объявления префикса недействительным по завершении срока действия. Специальное значение infinity указывает неограниченный срок действия префикса, пока не будет получено новое (конечное) значение в другом анонсе.

Префиксы link-local считаются включёнными в список с бесконечным сроком действия независимо от анонсирования этих префиксов маршрутизаторами. Полученным анонсам RA **не следует** менять значение таймера аннулирования для префиксов link-local.

Default Router List - список заданных по умолчанию маршрутизаторов

Список маршрутизаторов, которым могут передаваться пакеты. Записи списка указывают записи в кэше соседей. Алгоритм выбора принятого по умолчанию маршрутизатора отдаёт предпочтение маршрутизаторам, которые были доступны, по отношению к тем, чья доступность вызывает сомнения. Каждая запись имеет время аннулирования (извлекается из анонса), используемое для удаления записей, которые больше не анонсируются.

Отметим, что упомянутые выше концептуальные структуры данных можно реализовать разными способами. Одним из возможных вариантов является использование одной таблицы маршрутизации по максимальному совпадению для всех указанных структур. Независимо от конкретной реализации очень важно, чтобы запись Neighbor Cache для маршрутизатора совместно использовалась всеми записями Destination Cache, использующими этот маршрутизатор, для предотвращения избыточных проб NUD.

Концептуальные структуры данных могут добавлять и другие протоколы (например, Mobile IPv6). Реализация свободна в выборе и организации таких структур. Например, можно объединить все концептуальные структуры в одну таблицу маршрутизации.

Neighbor Cache содержит сведения, поддерживаемые алгоритмом NUD. Важнейшей частью сведений является состояние доступности соседа, которое может принимать одно из 5 значений, кратко описанных ниже и формально определённых в параграфе 7.3.2.

INCOMPLETE

Происходит распознавание адреса и адрес соседа на канальном уровне ещё не определён.

REACHABLE

Грубо говоря, доступность соседа стала известна недавно (десятки секунд назад).

STALE

О доступности соседа больше не известно, но до отправки ему трафика не следует предпринимать попыток проверки доступности.

DELAY

О доступности соседа больше не известно и ему недавно был передан трафик. Однако отправка зондов для проверки отложена на короткое время, чтобы протоколы вышележащего уровня могли подтвердить доступность.

PROBE

О доступности соседа больше не известно и ему передано индивидуальное сообщение NS для проверки.

5.2. Концептуальный алгоритм передачи

При отправке пакета адресату узел использует комбинацию Destination Cache, Prefix List и Default Router List для определения IP-адреса следующего узла (операция next-hop determination). Когда IP-адрес следующего узла определён выполняется обращение к Neighbor Cache для определения адреса канального уровня.

Для определения следующего узла отправитель выполняет поиск по максимальному совпадению префиксов в Prefix List, чтобы понять, находится ли получатель пакета на канале. Если получатель подключён к каналу, адресом next-hop будет адрес самого получателя, иначе отправитель выбирает маршрутизатор из списка Default Router List, следуя правилам параграфа 6.3.6. Выбор принятого по умолчанию маршрутизатора.

Из соображений эффективности определение next-hop не происходит для каждого передаваемого пакета и вместо этого результат поиска сохраняется в Destination Cache (кэш включает также обновления из сообщений Redirect). Когда у отправителя есть пакет для передачи, он сначала проверяет Destination Cache и лишь при отсутствии кэшированных данных вызывает процедуру определения next-hop для создания записи в Destination Cache.

Когда IP-адрес next-hop известен, отправитель проверяет Neighbor Cache для поиска адреса соседа на канальном уровне. Если записи нет, отправитель создаёт запись с состоянием INCOMPLETE, инициирует распознавание адреса и помещает пакет данных в очередь ожидания адреса. Для интерфейсов с поддержкой групповой адресации распознавание адреса состоит из отправки сообщения NS и ожидания отклика NA. При получении NA адрес канального уровня включается в NCE и пакет из очереди передаётся. Механизм распознавание адресов описан в параграфе 7.2.

Для групповых пакетов next-hop всегда является (групповым) адресом получателя и считается находящимся на канале. Процедуры определения адреса канального уровня, соответствующего групповому адресу IP, описаны в отдельных документах, посвящённых работе IP с конкретными канальными уровнями (например, [IPv6-ETHER]).

При каждом обращении к NCE для передачи индивидуального пакета отправитель проверяет данные о доступности соседа по алгоритму NUD (7.3. Алгоритм NUD). Результатом такой проверки может стать передача отправителем индивидуального сообщения NS для проверки доступности соседа.

Определение next-hop выполняется при первой отправке трафика адресату. Пока связь с этим адресатом продолжается успешно, применяется запись Destination Cache. Если в какой-то момент связь прерывается по данным алгоритма NUD, процедуру определения next-hop потребуется повторить. Например, трафик через отказавший маршрутизатор придётся перенести на другой маршрут. Точно также может перенаправляться трафик мобильного узла к другому «агенту мобильности». При повторном определении next-hop узлом не требуется полностью отбрасывать запись Destination Cache. Обычно полезно сохранять такие сведения, как PMTU и значения таймера кругового обхода.

Маршрутизаторы и многодомные хосты имеют несколько интерфейсов. Далее в документе предполагается, что все передаваемые и принимаемые сообщения ND относятся к контексту соответствующего интерфейса. Например, при ответе на RS сообщение RA передаётся через интерфейс, принявший запрос.

5.3. Сборка мусора и тайм-ауты

Описанные структуры данных применяют разные механизмы отбрасывания потенциально устаревших и неиспользуемых данных. С точки зрения корректности не требуется периодически очищать записи в кэше соседей и адресатов. Хотя устаревшая информация может оставаться в кэше неопределённо долго, алгоритм NUD обеспечивает быстрое удаление устаревших сведений.

Для ограничения размеров хранилища кэшей адресатов и соседей узлу может потребоваться сборщик мусора. Однако следует позаботиться о наличии в хранилище места для хранения рабочего набора активных записей. Слишком малый размер кэша может приводить к отправке избыточного числа сообщений ND, если записи приходится часто отбрасывать и восстанавливать. Любая политика на основе LRU[1], восстанавливающая лишь записи, которые не использовались некоторое время (например, 10 минут и более), обеспечит адекватный сбор мусора.

Узлу следует сохранять записи в Default Router List и Prefix List до истечения срока действия, однако возможна упреждающая сборка мусора при нехватке памяти. Если не все маршрутизаторы хранятся в списке Default Router, узлу следует сохранять по меньшей мере 2 записи в Default Router List (предпочтительно больше) для обеспечения отказоустойчивой связности с узлами вне канала (off-link).

При удалении записи из Prefix List не требуется удалять какие-либо записи в кэше адресатов или соседей, NUD эффективно очищает все недействительные записи. Однако при удалении записи из Default Router List для всех записей Destination Cache, включающих соответствующий маршрутизатор, придётся повторить определение next-hop для выбора нового маршрутизатора, используемого по умолчанию.

6. Обнаружение маршрутизаторов и префиксов

В этом разделе описано поведение маршрутизаторов и хостов, связанное с обнаружением маршрутизаторов (Router Discovery) в ND. Обнаружение маршрутизаторов служит для отыскания соседних маршрутизаторов, а также выяснения префиксов и параметров конфигурации, связанных с автоматической настройкой адресов без учёта состояния.

Процесс обнаружения префиксов (Prefix Discovery) позволяет хостам узнать диапазоны адресов IP, относящихся к каналу и доступных напрямую без маршрутизаторов. Маршрутизаторы передают сообщения RA, указывающие, что их отправитель готов служить принятым по умолчанию маршрутизатором. Эти сообщения также включают опции Prefix Information со списком префиксов для адресов IP на канале (on-link).

Для автоматической настройка адресов без учёта состояния (Stateless Address Autoconfiguration) также нужны префиксы подсетей. Хотя используемые для автоматической настройки адресов префиксы логически отличаются от применяемых для определения принадлежности к каналу, данные для автоматической настройки адресов также включаются в сообщения Router Discovery для снижения объёма трафика. На самом деле одни и те же префиксы могут анонсироваться для определения принадлежности к каналу и автоматической настройки адресов путём установки соответствующих флагов в опциях Prefix Information. Автоматическая настройка адресов описана в [ADDRCONF].

6.1. Проверка сообщений

6.1.1. Проверка сообщения RS

Хосты **должны** отбрасывать без уведомления все принятые сообщения RS. Маршрутизаторы **должны** отбрасывать без уведомления все принятые сообщения RS, которые не соответствуют всем приведённым ниже требованиям:

- поле IP Hop Limit имеет значение 255, т. е. пакет не может пересылаться маршрутизатором;
- поле ICMP Checksum действительно;
- ICMP Code = 0;
- размер ICMP (выводится из размера IP) не менее 8 октетов;
- все включённые опции имеют ненулевой размер;
- если IP-адресом отправителя является незаданный адрес, в сообщении нет адреса отправителя на канальном уровне.

Поле Reserved и все нераспознанные опции **должны** игнорироваться. Будущие совместимые изменения протокола могут задавать иное применение поля Reserved и новые опции, в несовместимых изменениях может применяться другое значение Code. Содержимое любых опций, для которых не указано включение в сообщения RS, **должно** игнорироваться с сохранением обычной обработки сообщения. В настоящее время для RS указана лишь опция Source Link-Layer Address. Прошедшие проверку запросы считаются действительными (valid solicitation).

6.1.2. Проверка сообщений RA

Узел **должен** отбрасывать без уведомления все принятые сообщения RA, не соответствующие всем приведённым ниже требованиям:

- IP Source Address указывает адрес link-local; маршрутизаторы должны использовать свой адрес link-local в поле отправителя для сообщений RA и Redirect, чтобы хосты могли однозначно распознать маршрутизатор;
- поле IP Hop Limit имеет значение 255, т. е. пакет не может пересылаться маршрутизатором;
- поле ICMP Checksum действительно;
- ICMP Code = 0;

[1]Least Recently Used - наиболее давно использовавшийся.

- размер ICMP (выводится из размера IP) не менее 16 октетов;
- все включённые опции имеют ненулевой размер.

Поле Reserved и все нераспознанные опции **должны** игнорироваться. Будущие совместимые изменения протокола могут задавать иное применение поля Reserved и новые опции, в несовместимых изменениях может применяться другое значение Code. Содержимое любых опций, для которых не указано включение в сообщения RS, **должно** игнорироваться с сохранением обычной обработки сообщения. В настоящее время для RA указаны опции Source Link-Layer Address, Prefix Information и MTU. Прошедшие проверку анонсы считаются действительными (valid advertisement).

6.2. Сообщение RS

6.2.1. Переменные конфигурации маршрутизатора

Маршрутизатор **должен** разрешать настройку указанных ниже концептуальных переменных через систему управления. Переменные не требуется именовать в соответствии с этим документом, важно чтобы внешнее поведение соответствовало спецификации. Принятые по умолчанию значение указаны для упрощения настройки в типичных случаях. Заданные по умолчанию значения некоторых переменных могут быть переопределены в документах, описывающих работу IPv6 с конкретными канальными уровнями. Это правило упрощает настройку ND на каналах с разными параметрами производительности. Ниже приведены переменные, задаваемые для каждого интерфейса.

IsRouter
Флаг, указывающий включение маршрутизации на интерфейсе, позволяющее пересылать пакеты через него. По умолчанию FALSE.

AdvSendAdvertisements
Флаг, указывающий передачу маршрутизатором периодических сообщений RA и откликов на RS. По умолчанию FALSE. Отметим, что по умолчанию **должно** устанавливаться AdvSendAdvertisements = FALSE, чтобы узел не мог случайно выступить в качестве маршрутизатора без явной настройки через систему управления для передачи RA.

MaxRtrAdvInterval
Максимальный интервал между отправкой групповых незапрошенных сообщений RA с этого интерфейса (в секундах). Интервал **должен** быть не меньше 4 и не больше 1800 секунд, по умолчанию 600 секунд.

MinRtrAdvInterval
Минимальный интервал между отправкой групповых незапрошенных сообщений RA с этого интерфейса (в секундах). Интервал **должен** быть не меньше 3 секунд и не больше 0,75 * MaxRtrAdvInterval. По умолчанию 0,33 * MaxRtrAdvInterval, если MaxRtrAdvInterval ≥ 9, иначе 0,75 * MaxRtrAdvInterval[1].

AdvManagedFlag
Флаг (TRUE или FALSE) для включения в поле Managed address configuration сообщений RA (см. [ADDRCONF]). По умолчанию FALSE.

AdvOtherConfigFlag
Флаг (TRUE или FALSE) для включения в поле Other configuration сообщений RA (см. [ADDRCONF]). По умолчанию FALSE.

AdvLinkMTU
Значение для включения в передаваемые маршрутизатором опции MTU. 0 указывает, что опции MTU не передаются. По умолчанию 0.

AdvReachableTime
Значение для включения в поле Reachable Time передаваемых маршрутизатором сообщений RA. Значение 0 указывает, что маршрутизатор не задаёт поле. Значение поля **должно** быть не больше 3600000 мсек (1 час). По умолчанию 0.

AdvRetransTimer
Значение для включения в поле Retrans Timer передаваемых маршрутизатором сообщений RA. Значение 0 указывает, что маршрутизатор не задаёт поле. По умолчанию 0.

AdvCurHopLimit
Принятое по умолчанию значение поля Cur Hop Limit в передаваемых маршрутизатором сообщениях RA. В поле следует помещать текущий диаметр Internet. Значение 0 указывает, что маршрутизатор не задаёт поле. По умолчанию используется значение из Assigned Numbers [ASSIGNED] на момент реализации.

AdvDefaultLifetime
Значение для включения в поле Router Lifetime передаваемых с этого интерфейса сообщений RA (в секундах). Это **должно** быть значение из интервала от MaxRtrAdvInterval до 9000 секунд или 0. Нулевое значение указывает, что маршрутизатор не применяется по умолчанию. Ограничения могут переопределяться документами, задающими работу IPv6 с конкретными канальными уровнями. Например, на каналах «точка-точка» у партнёров может достаточно сведений о числе и состоянии устройств на другой стороне, что позволит реже передавать анонсы. По умолчанию 3 * MaxRtrAdvInterval.

AdvPrefixList
Список префиксов, помещаемых в опции Prefix Information сообщений RA, передаваемых с интерфейса. По умолчанию это все префиксы, анонсируемые через протоколы маршрутизации, как относящиеся к каналу для передающего анонсы интерфейса. Префикс link-local **не следует** включать в список анонсируемых префиксов. Каждый префикс включает указанные ниже сведения.

AdvValidLifetime
Значение, помещаемое в поле Valid Lifetime опции Prefix Information (в секундах). Значение, содержащее лишь 1 (0xffffffff) задаёт неограниченный срок. Реализации **могут** указывать AdvValidLifetime двумя способами:
- значение, декрементируемое в реальном масштабе времени, что приводит к Lifetime = 0 в заданное время в будущем;
- фиксированный момент, не меняющийся в последующих анонсах.

По умолчанию принято фиксированное значение 2592000 секунд (30 дней).

AdvOnLinkFlag
Значение помещаемое во флаг L опции Prefix Information. По умолчанию TRUE.

[1] В оригинале допущена ошибка, см. https://www.rfc-editor.org/errata/eid3154. *Прим. перев.*

Для автоматической настройки адресов без учёта состояния [ADDRCONF] с каждым префиксом указываются дополнительные сведения.

AdvPreferredLifetime

Значение, помещаемое в поле Preferred Lifetime опции Prefix Information (в секундах). Значение, содержащее лишь 1 (0xffffffff) задаёт неограниченный срок. Использование этого значения описано в [ADDRCONF]. Реализации **могут** указывать AdvPreferredLifetime двумя способами:

- значение, декрементируемое в реальном масштабе времени, что приводит к Lifetime = 0 в заданное время в будущем;
- фиксированный момент, не меняющийся в последующих анонсах.

По умолчанию принято фиксированное значение 604800 секунд (7 дней). Этому значению **недопустимо** быть больше AdvValidLifetime.

AdvAutonomousFlag

Значение, помещаемое в поле Autonomous Flag опции Prefix Information (см. [ADDRCONF]). По умолчанию TRUE.

Упомянутые выше переменные включают сведения, включаемые в исходящие сообщения RA. Хосты применяют полученные данные для инициализации набора аналогичных переменных, управляющих их внешним поведением (см. параграф 6.3.2). Некоторые из таких переменных хоста (например, CurHopLimit, RetransTimer, ReachableTime) применимы ко всем узлам, включая маршрутизаторы. На деле эти переменные могут отсутствовать в маршрутизаторах, поскольку их можно вывести из описанных выше переменных. Однако внешнее поведение маршрутизатора **должно** совпадать с поведением хоста в части этих переменных. В частности, это включает выполняемую иногда рандомизацию ReachableTime, как описано в параграфе 6.3.2. Переменные хоста.

Константы протокола указаны в разделе 10.

6.2.2. Переход интерфейса в состояние анонсирующего

Анонсирующим считается любой включенный и работающий интерфейс, имеющий хотя бы один индивидуальный адрес IP, для которого соответствующий флаг AdvSendAdvertisements имеет значение TRUE. Маршрутизатору **недопустимо** передавать сообщения RA с интерфейсов, которые не являются анонсирующими.

Интерфейс может стать анонсирующим не только при запуске системы. Например,

- при смене флага AdvSendAdvertisements для включённого интерфейса с FALSE на TRUE;
- при административном включении отключённого ранее интерфейса с AdvSendAdvertisements = TRUE;
- включение пересылки IP (например, хоста становится маршрутизатором) при AdvSendAdvertisements = TRUE.

Маршрутизатор **должен** связать групповой адрес all-routers с анонсирующим интерфейсом. Маршрутизаторы отвечают на запросы RS, переданные по адресу all-routers, и проверяют согласованность RA, переданных соседями.

6.2.3. Содержимое сообщения RA

Маршрутизатор передаёт периодические и запрошенные сообщения RA через свои анонсирующие интерфейсы. Исходящие RA заполняются указанными ниже значениями, в соответствии с форматом, указанным в параграфе 4.2.

- В поле Router Lifetime указывается заданное для интерфейса значение AdvDefaultLifetime.
- Флаги M и O в соответствии с заданными для интерфейса AdvManagedFlag и AdvOtherConfigFlag.
- В поле Cur Hop Limit указывается заданное для интерфейса значение AdvCurHopLimit[1].
- В поле Reachable Time указывается заданное для интерфейса значение AdvReachableTime.
- В поле Retrans Timer указывается заданное для интерфейса значение AdvRetransTimer.
- Опции включаются в соответствии с приведёнными ниже правилами.
  - В опции Source Link-Layer Address указывается адрес канального уровня передающего интерфейса. Опцию **можно** опустить для упрощения балансировки на входе между реплицированными интерфейсами.
  - В опции MTU указывается значение AdvLinkMTU, если оно отлично от 0. При AdvLinkMTU = 0 опция MTU не передаётся.
  - В опции Prefix Information для каждого префикса из списка AdvPrefixList указываются поля записи AdvPrefixList:
    - для флага on-link (L) устанавливается значение AdvOnLinkFlag;
    - в поле Valid Lifetime помещается значение AdvValidLifetime;
    - для флага Autonomous address configuration (A) устанавливается значение AdvAutonomousFlag;
    - в поле Preferred Lifetime помещается значение AdvPreferredLifetime.

Маршрутизатор может передавать RA без анонсирования себя как принятого по умолчанию маршрутизатора. Например, маршрутизатор может анонсировать префиксы для автоматической настройки адресов без учёта состояния, не желая пересылать пакеты. Такой маршрутизатор указывает в исходящих анонсах Router Lifetime = 0.

Маршрутизатор может не включать некоторые опции в незапрошенные RA. Например, если срок действия префикса много больше AdvDefaultLifetime, достаточно его включения в каждые несколько анонсов. Однако при ответе на RS или отправке нескольких первых незапрошенных анонсов маршрутизатору **следует** включать все опции для быстрого распространения всех данных (например, префиксов) в процессе инициализации системы.

Если включение опций ведёт к превышению MTU на канале, можно передать несколько анонсов с частью опций в каждом.

[1] В оригинале ошибочно указано CurHopLimit, см. https://www.rfc-editor.org/errata/eid4461. *Прим. перев.*

6.2.4. Отправка незапрошенных сообщений RA

Хостам **недопустимо** передавать сообщения RA.

Незапрошенные RA не являются строго периодическими, интервал между отправкой меняется случайным образом для предотвращения синхронизации анонсов от разных маршрутизаторов на одном канале [SYNC]. У каждого анонсирующего интерфейса есть свой таймер, для которого при каждой отправке с интерфейса группового анонса устанавливается случайное значение (с однородным распределением) из заданного для интерфейса интервала MinRtrAdvInterval - MaxRtrAdvInterval. По завершении заданного интервала передаётся следующий анонс и для таймера выбирается новое случайное значение.

Для нескольких первых анонсов (до MAX_INITIAL_RTR_ADVERTISEMENTS), передаваемых с интерфейса, ставшего аносирующим, в случае выбора случайного значения больше MAX_INITIAL_RTR_ADVERT_INTERVAL для таймера **следует** установить значение MAX_INITIAL_RTR_ADVERT_INTERVAL. Использование меньшего интервала для начальных анонсов повышает вероятность быстрого обнаружения маршрутизатора, когда он становится доступным, при наличии потери пакетов.

Информацию в анонсах RA могут менять события, связанные с управлением сетью. Например, может поменяться срок действия анонсированных префиксов, могут быть добавлены новые префиксы, маршрутизатор перейдёт в режим хоста и т. п. В таких случаях маршрутизатор **может** передать до MAX_INITIAL_RTR_ADVERTISEMENTS незапрошенных анонсов используя те же правила, которые применяются при переходе интерфейса в статус анонсирующего.

6.2.5. Утрата интерфейсом статуса анонсирующего

Интерфейс может утратить статус анонсирующего в результате действий системы управления:

- смена значения флага AdvSendAdvertisements для включённого интерфейса с TRUE на FALSE;
- административное отключение интерфейса;
- отключение системы (shutdown).

В таких случаях маршрутизатору **следует** передать хотя бы одно (но не более MAX_FINAL_RTR_ADVERTISEMENTS) финальное групповое сообщение RA через интерфейс с установкой Router Lifetime = 0. Если маршрутизатор становится хостом, системе **следует** также выйти из группы all-routers на всех интерфейсах, где поддерживается групповая адресация IP (независимо от того, были ли они анонсирующими). Кроме того, хост **должен** обеспечить в последующих сообщениях NA с данного интерфейса сброс флага маршрутизации R.

Отметим, что система управления может отключить на маршрутизаторе пересылку IP (например, переведя его в статус хоста), но это может не менять для интерфейсов статус анонсирования. В таких случаях последующие анонсы RA **должны** указывать Router Lifetime = 0.

6.2.6. Обработка сообщений RS

Хост **должен** отбрасывать без уведомления все полученные сообщения RS.

Кроме отправки незапрошенных анонсов маршрутизаторы передают анонсы в ответ на запросы, полученные на анонсирующем интерфейсе. Маршрутизатор **может** передавать индивидуальные отклики напрямую отправителям запросов (если запрос не отправлен с неуказанного адреса), но обычно анонсы передаются по групповому адресу all-nodes. В этом случае для таймера интервалов на интерфейсе устанавливается новое случайное значение, как это делается при отправке незапрошенных анонсов (6.2.4. Отправка незапрошенных сообщений RA).

Во всех случаях анонсы RA, передаваемые в ответ на RS, **должны** задерживаться на случайное время от 0 до MAX_RA_DELAY_TIME секунд (при отправке анонса в ответ на несколько запросов задержка отсчитывается от первого запроса). Кроме того, для последовательных RA по групповому адресу all-nodes **должна** быть ограничена частота отправки - не более 1 анонса каждые MIN_DELAY_BETWEEN_RAS секунд.

Маршрутизатор может обрабатывать сообщения RS, как указано ниже.

- После приёма RS рассчитывается случайное значение из диапазона 0 - MAX_RA_DELAY_TIME. Если рассчитанное значение указывает время после запланированной отправки следующего группового сообщения RA, случайная задержка игнорируется и сообщение передаётся в запланированное время.
- Если маршрутизатор передал групповое сообщение RA (запрошенное или незапрошенное) в последние MIN_DELAY_BETWEEN_RAS секунд, планируется отправка анонса через MIN_DELAY_BETWEEN_RAS секунд с дополнительной случайной задержкой после передачи предыдущего анонса. Это обеспечивает ограничение частоты отправки групповых RA.
- В остальных случаях планируется отправка RA в заданное случайным значением время.

Отметим, что маршрутизаторам разрешено передавать групповые RA чаще, чем указано в переменной конфигурации MinRtrAdvInterval, если более частые анонсы являются откликами на RS. Однако во всех случаях незапрошенные групповые анонсы **недопустимо** передавать чаще, чем указывает MinRtrAdvInterval.

По запросам RS, где Source Address содержит неуказанный адрес, **недопустимо** обновляет Neighbor Cache в маршрутизаторе, а запросы с подходящим адресом отправителя обновляют кэш соседей, как описано ниже. Если у маршрутизатора уже есть в кэше соседей запись для отправителя запроса, запрос содержит опцию Source Link-Layer Address и полученный адрес канального уровня отличается от сохранённого в кэше, **следует** обновить адрес канального уровня в соответствующей записи Neighbor Cache, а для состояния доступности в ней **должно** быть установлено значение STALE. Если в кэше нет записи для отправителя запроса, в кэш заносится адрес канального уровня и устанавливается состояние доступности STALE, как указано в параграфе 7.3.3. Если в Neighbor Cache нет записи и в сообщении нет опции Source Link-Layer Address, маршрутизатор может ответить групповым или индивидуальным сообщением RA. Независимо от наличия опции Source Link-Layer Address, если в кэше соседей имеется (или создаётся) запись для отправителя запроса, флаг IsRouter в этой записи **должен** получить значение FALSE.

6.2.7. Согласованность RA

Маршрутизаторам **следует** просматривать действительные анонсы RA от других маршрутизаторов и проверять согласованность анонсируемых сведений в канале. Найденные несоответствия указывают, что один или несколько маршрутизаторов могут быть настроены некорректно и **следует** записывать такие события в системный журнал или систему управления сетью. Минимальный набор проверок указан ниже.

- Значения Cur Hop Limit (за исключением значения 0 несоответствия **следует** фиксировать в журнале системы управления сетью).
- Значения флагов M и O.
- Значения Reachable Time (за исключением значения 0).
- Значения Retrans Timer (за исключением значения 0).
- Значения в опциях MTU.
- Значения Preferred Lifetime и Valid Lifetime для одного префикса. Если AdvPreferredLifetime и/или AdvValidLifetime уменьшаются в реальном масштабе времени, как указано в параграфе 6.2.1, сравнение сроков действия в полях сообщений невозможно по значениям полей в RA, и вместо этого должно сравниваться время, когда префикс становится устаревшим или недействительным. Из-за задержек в канале и, возможно, слабо синхронизированных часов в маршрутизаторах при таком сравнении **следует** учитывать некоторую погрешность.

Отметим, что анонсирование разными маршрутизаторами различных наборов префиксов не является ошибкой. Кроме того, некоторые маршрутизаторы могут не задавать часть полей, оставляя в них 0, тогда как другие будут задавать их. Запись ошибок в журнал **следует** ограничивать сведениями о конфликтах, которые вынуждают хосты переключаться с одного значения на другое при каждом анонсе.

Другие действия при получении маршрутизатором анонсов RA выходят за рамки этой спецификации.

6.2.8. Смена адреса канального уровня

Адресу link-local у маршрутизатора следует меняться редко или не меняться совсем. Узлы, получающие сообщения ND, используют адрес источника для идентификации отправителя. Если множество пакетов от одного маршрутизатора содержит разные адреса отправителя, узлы отнесут их к разным маршрутизаторам, что приведёт к нежелательному поведению. Например, узел будет игнорировать сообщения Redirect, которые он сочтёт отправленными не тем маршрутизатором, который сейчас служит первым узлом пересылки (first-hop). Поэтому адрес отправителя в RA от конкретного маршрутизатора должен совпадать с адресом цели в сообщении Redirect с перенаправлением на этот маршрутизатор.

Использование адреса link-local для однозначной идентификации маршрутизаторов на канале имеет то преимущество, что при смене адресов на сайте этот адрес менять не требуется.

Если маршрутизатор меняет адрес link-local на одном из интерфейсов, ему **следует** уведомить об этом хосты. Маршрутизатору **следует** передать несколько групповых RA со старого адреса link-local с Router Lifetime = 0, а также несколько групповых RA с нового адреса. Результат будет таким же как при утрате статуса анонсирующего одним интерфейсом и получении этого статуса другим.

6.3. Спецификация хоста

6.3.1. Переменные конфигурации хоста

Нет.

6.3.2. Переменные хоста

Хосты поддерживают некоторые связанные с ND переменные в дополнение к структурам данных, определенным в параграфе 5.1. Приведённые ниже имена переменных заданы лишь для удобства и реализация может выбрать свои имена, если обеспечивается описанное в этом документе внешнее поведение.

Переменные имеют заданные по умолчанию значения которые переопределяются значениями из сообщений RA. Заданные по умолчанию значения применяются при отсутствии на канале маршрутизатора или в случаях, когда все полученные сообщения RA содержат незаданные значения конкретных полей. Заданные здесь значения по умолчанию могут быть переопределены документами, задающими работу IP на конкретных канальных уровнях. Это позволяет применять ND на каналах с разными характеристиками. Ниже перечислены переменные для каждого интерфейса.

LinkMTU
MTU для канала. Принятое по умолчанию значение определяется документом, задающим работу IPv6 с конкретным канальным уровнем (например, [IPv6-ETHER]).

CurHopLimit
Принятое по умолчанию ограничение числа интервалов пересылки при отправке пакетов IP. Принятое по умолчанию значение определяется Assigned Numbers [ASSIGNED] на момент реализации.

BaseReachableTime
Базовое значение для расчёта случайного значения ReachableTime. По умолчанию REACHABLE_TIME мсек.

ReachableTime
Время с момента приёма последнего подтверждения доступности, в течение которого хост считается доступным. Это должно быть случайное значение с однородным распределением из интервала MIN_RANDOM_FACTOR - MAX_RANDOM_FACTOR, умноженное на BaseReachableTime (в мсек). Следует рассчитывать новое случайное значение при изменении BaseReachableTime (в RA) или каждые несколько часов даже при отсутствии RA.

RetransTimer
Время между повторами сообщений NS соседу при распознавании адресов или проверке доступности соседа. По умолчанию RETRANS_TIMER мсек.

6.3.3. Инициализация интерфейса

На интерфейсах с поддержкой групповой адресации хост присоединяется к группе all-nodes.

6.3.4. Обработка полученных сообщений RA

При наличии нескольких маршрутизаторов сведения, анонсируемые ими коллективно, могут быть надмножеством данных одного сообщения RA. Более того, информация может также поступать от иных динамических источников, таких как DHCPv6. Хост воспринимает объединение всей полученной информации и сообщению RA **недопустимо** аннулировать все сведения, полученные в предыдущем анонсе или из иных источников. Однако при получении данных для конкретного параметра (например, Link MTU) или опции (например, Lifetime для конкретного префикса), отличающихся от ранее полученной информации используется более свежее значение, если параметр или опция не поддерживает одновременно несколько значений.

Поля RA (например, Cur Hop Limit, Reachable Time, Retrans Timer) могут содержать значение, указывающее, что поле фактически не задано. В таких случаях поле следует игнорировать и хосту следует продолжать использование прежнего значения. В частности, хосту **недопустимо** интерпретировать незаданное значение как возврат к принятому по умолчанию до получения первого анонса RA. Это правило предотвращает безостановочную смену внутренней переменной, когда один маршрутизатор анонсирует конкретное значение, другой - незаданное.

При получении действительного RA хост извлекает из пакета адрес отправителя и выполняет следующие операции:

- если адреса ещё нет в списке хоста Default Router List, а в анонсе указано ненулевое значение Router Lifetime, в список вносится новая запись и для таймера аннулирования устанавливается значение поля Router Lifetime;
- если адрес уже включён в Default Router List из прежних анонсов, для таймера аннулирования устанавливается значение поля Router Lifetime из последнего анонса;
- если адрес уже включён в Default Router List и Router Lifetime = 0, для записи незамедлительно задаётся тайм-аут, как указано в параграфе 6.3.5.

Для ограничения объёма памяти на хранение Default Router List хост **может** хранить не все адреса маршрутизаторов, полученные в анонсах. Однако хост **должен** сохранять адреса по меньшей мере 2 маршрутизаторов и **следует** сохранять больше. Выбор принятого по умолчанию маршрутизатора происходит всякий раз, когда возникает отказ связи с адресатом. Таким образом, большее число маршрутизаторов в списке позволяет быстрее найти другой рабочий маршрут (без ожидания приёма следующего анонса RA).

Если принятое значение Cur Hop Limit не равно 0, хосту **следует** установить это значение в переменной CurHopLimit.

Если принятое значение Reachable Time отлично от 0, хосту **следует** установить его в переменной BaseReachableTime. Если новое значение отличается от прежнего, хосту **следует** рассчитать новое значение ReachableTime, как случайное число с однородным распределением из интервала MIN_RANDOM_FACTOR - MAX_RANDOM_FACTOR, умноженное на BaseReachableTime. Использование случайного значения позволяет избежать синхронизации сообщений NUD. Во многих случаях анонсируемое значение Reachable Time будет совпадать в последовательных сообщениях RA и значение BaseReachableTime на хосте будет меняться редко. В таких случаях реализации **следует** обеспечивать расчёт нового случайного значение не реже 1 раза каждые несколько часов.

Значение переменной RetransTimer **следует** копировать из поля Retrans Timer, если оно отлично от 0.

После извлечения данных из фиксированной части RA анонс сканируется на предмет действительных опций. Если в анонсе имеется опция Source Link-Layer Address, адрес канального уровня **следует** записать в Neighbor Cache (создать запись при необходимости), а для флага IsRouter в NCE **должно** быть установлено значение TRUE. Если опция Source Link-Layer Address не включена, но имеется соответствующая запись NCE, для флага IsRouter в этой записи **должно** быть установлено значение TRUE. Флаг IsRouter используется NUD для определения перехода маршрутизатора в статус хоста (т. е. прекращение пересылки пакетов). Если создаётся запись NCE для маршрутизатора, для неё **должно** быть установлено состояние доступности STALE, как указано в параграфе 7.3.3. Для имеющейся записи, в которой обновляется адрес канального уровня, также **должно** устанавливаться состояние доступности STALE.

При наличии опции MTU хосту **следует** скопировать её значение в LinkMTU при условии, что оно не меньше минимального MTU для канала [IPv6] и не больше максимального LinkMTU, заданного соответствующим канальному уровню документом (например, [IPv6-ETHER]).

Опции Prefix Information с установленным флагом on-link (L) указывают префикс, определяющий диапазон адресов, которые следует считать относящимися к каналу. Отметим однако, что опция Prefix Information со сброшенным флагом L не содержит сведений о принадлежности к каналу и её **недопустимо** считать индикацией того, что префикс не относится к каналу. Единственным способом отменить прежнюю индикацию принадлежности префикса к каналу является анонсирование префикса с установленным флагом L и Lifetime = 0. Принятое по умолчанию (5.2. Концептуальный алгоритм передачи) поведение при отправке пакета по адресу, для которого нет сведений о принадлежности к каналу, заключается в пересылке пакета заданному по умолчанию маршрутизатору. Получение опции Prefix Information со сброшенным флагом L не меняет этого поведения. Причины того, что адрес считается относящимся к каналу, указаны в определении on-link в параграфе 2.1. Префиксы со сброшенным флагом L обычно имеют флаг A и используются [ADDRCONF].

Для каждой опции Prefix Information с установленным флагом L хост выполняет перечисленные ниже действий.

- Если префикс является link-local, опция Prefix Information игнорируется.
- Если префикса ещё нет в Prefix List и в опции Prefix Information поле Valid Lifetime отлично от 0, создаётся новая запись для префикса и для таймера аннулирования устанавливается значение Valid Lifetime из опции.
- Если префикс уже включён в Prefix List прежним анонсом, для таймера аннулирования устанавливается значение Valid Lifetime из опции Prefix Information. Если новое значение Lifetime = 0, префикс сразу же считается устаревшим (см. 6.3.5. Тайм-ауты для префиксов и принятых по умолчанию маршрутизаторов).
- Если в опции Prefix Information поле Valid Lifetime = 0 и префикса нет в Prefix List хоста, опция игнорируется.

Для автоматической настройки адресов [ADDRCONF] в некоторых случаях могут применяться большие значения Valid Lifetime или поле может игнорироваться для предотвращения некоторых DoS[1]-атак. Однако влияние таких атак на список относящихся к каналу префиксов не является катастрофическим (хосты будут отправлять пакеты принятому по умолчанию маршрутизатору вместо передачи соседу напрямую), поэтому протокол ND не задаёт проверки срока действия префикса. [ADDRCONF] может вносить ограничения на размер префиксов для автоматической настройки адресов, поэтому префикс может отвергаться реализацией [ADDRCONF] на хосте. Однако размер префикса остаётся действительным для определения принадлежности к каналу в комбинации с другими флагами опции Prefix Information.

> Примечание. Реализации могут обрабатывать аспекты принадлежности префикса к каналу независимо от аспектов автоматической настройки адресов без учёта состояния, например, передавая копию каждого действительного сообщения RA обеим функциям on-link и addrconf, каждая из которых работает автономно с префиксами, для которых установлен соответствующий флаг.

6.3.5. Тайм-ауты для префиксов и принятых по умолчанию маршрутизаторов

По завершении отсчёта таймера аннулирования для записи Prefix List эта запись отбрасывается, однако имеющиеся записи Destination Cache не требуется обновлять. Если возникает проблема доступности для имеющейся записи NCE, алгоритм NUD будет выполнять требуемое восстановление.

По истечении Lifetime для записи в Default Router List эта запись отбрасывается. При удалении маршрутизатора из списка Default Router узел **должен** обновить Destination Cache, чтобы для всех записей, включающих этот маршрутизатор, была выполнена процедура определения next-hop и трафик не направлялся этому маршрутизатору.

6.3.6. Выбор принятого по умолчанию маршрутизатора

Выбор маршрутизатора отчасти зависит о наличии сведений о его доступности. Детали отслеживания узлом статуса доступности соседа описаны в параграфе 7.3. Алгоритм выбора принятого по умолчанию маршрутизатора вызывается при определении next-hop, когда в Destination Cache нет записи для адресата вне канала (off-link) или связь через имеющийся маршрутизатор представляется отказавшей. В нормальных условиях маршрутизатор выбирается при первой передаче трафика адресату, а для последующего трафика используется маршрутизатор, указанный в Destination Cache с учётом изменений кэша, вызванных сообщениями Redirect. Правила выбора маршрутизатора из Default Router List приведены ниже

1) **Следует** предпочитать маршрутизаторы, которые доступны или могут быть доступны (т. е. состояние отличается от INCOMPLETE), маршрутизаторам, доступность которых неизвестна или кажется сомнительной (т. е. состояние INCOMPLETE или отсутствие записи в Neighbor Cache). Дополнительные рекомендации по выбору принятого по умолчанию маршрутизатора приведены в [LD-SHRE].

2) Если в списке нет маршрутизаторов, которые доступны или могут быть доступны, маршрутизаторы **следует** перебирать по кругу (round-robin), чтобы последующие запросы для принятого по умолчанию маршрутизатора не возвращали тот же маршрутизатор, пока не будут проверены все остальные. Циклический перебор обеспечивает активную проверку всех маршрутизаторов алгоритмом NUD. Запрос принятого по умолчанию маршрутизатора выполняется вместе с отправкой пакета маршрутизатору и проверка доступности маршрутизатора выполняется как побочный эффект.

6.3.7. Отправка сообщений RS

При включении интерфейса хост может не захотеть ждать следующего незапрошенного сообщения RA для получения принятых по умолчанию маршрутизаторов и определения префиксов. Для быстрого получения RA хосту **следует** передать до MAX_RTR_SOLICITATIONS сообщений RS с интервалом не менее RTR_SOLICITATION_INTERVAL секунд. Сообщение RS можно передавать после любого из перечисленных ниже событий:

- инициализация интерфейса при старте системы;
- повторная инициализация интерфейса после его временного отказа или запрета системой управления;
- переход маршрутизатора в статус хоста с отключением пересылки IP системой управления;
- первое подключение хоста к каналу;
- повторное подключение хоста после временного отключения от канала.

Хост передаёт сообщения RS по групповому адресу all-routers. В поле IP-адреса отправителя указывается индивидуальный адрес одного из интерфейсов или незаданный адрес (unspecified). В опции Source Link-Layer Address **следует** указывать адрес хоста на канальном уровне, если IP-адрес не является незаданным.

Перед отправкой первоначального запросу хосту **следует** ввести случайную задержку из диапазона от 0 до MAX_RTR_SOLICITATION_DELAY. Это позволяет снизить нагрузку при одновременном запуске множества хостов на канале, что может происходить при восстановлении после отказа по питанию. Если хост уже использовал случайную задержку после своего (повторного) включения (например, как часть DAD [ADDRCONF]), новая задержка перед отправкой первого RS не требуется.

В некоторых случаях случайную задержку **можно** не вносить. Например, мобильному узлу, использующему [MIPv6], при переходе на новый канал нужно как можно быстрее обнаружить такой переход для минимизации числа пакетов, потерянных в результате изменения топологии. Сообщения RS обеспечивают полезный механизм детектирования перемещения в Mobile IPv6, поскольку они позволяют мобильному узлу видеть переключение на другой канал. Поэтому при получении мобильным узлом сведений канального уровня, говорящих о возможном переключении, он **может** передать сообщение RS без дополнительной случайной задержки. Надёжность такой индикации должна оценивать реализация мобильного узла в зависимости от уровня достоверности сведений от канального уровня, но это выходит за рамки спецификации. Отметим, что ненадлежащее применение механизма (например, на основе слабой или временной индикации) может приводить к пикам отправки RS. Кроме того, одновременное перемещение большого числа мобильных устройств, использующих механизм, может создавать множество одновременных запросов RS.

[1]Denial-of-service - отказ в обслуживании.

После отправки RS и получения действительного RA с отличным от 0 Router Lifetime хост **должен** прекратить отправку дополнительных запросов с этого интерфейса, пока снова не произойдёт одно из указанных выше событий. Хосту **следует** передать хотя бы 1 запрос даже при получении анонса до запроса. Отклики на запросы могут включать больше информации по сравнению с незапрошенными анонсами.

Если хост передал MAX_RTR_SOLICITATIONS запросов и не получил RA в течении MAX_RTR_SOLICITATION_DELAY секунд с момента отправки последнего запроса, он считает, что на канале нет маршрутизаторов для [ADDRCONF]. Однако хост будет получать и обрабатывать сообщения RA при появлении маршрутизаторов на канале.

7. Распознавание адресов и NUD

В этом разделе описаны функции, связанные с сообщениями NS и NA, а также описаны алгоритмы распознавания адресов и обнаружения недоступности соседей (NUD). Сообщения NS и NA применяются также для обнаружения дубликатов адресов (DAD), заданного в [ADDRCONF]. В частности, механизм DAD передаёт сообщения NS с неуказанным адресом источника, нацеленные на его «предварительный» адрес. Такие сообщения инициируют на узлах, уже использующих этот адрес, отправку групповых NA, указывающих, что адрес уже занят.

7.1. Проверка сообщений

7.1.1. Проверка NS

Узел **должен** без уведомления отбрасывать сообщения NS, на соответствующие приведённым ниже условиям:

- поле IP Hop Limit = 255, т. е. пакет не может пересылаться маршрутизаторами;
- значение ICMP Checksum корректно;
- ICMP Code = 0;
- размер ICMP (выводится из размера IP) составляет не менее 24 октетов;
- Target Address не является групповым адресом;
- все включённые опции имеют ненулевой размер;
- если IP-адрес отправителя не задан, IP-адрес получателя является групповым адресом solicited-node;
- если IP-адрес отправителя не задан, в сообщении нет опции Source Link-Layer Address.

Содержимое поля Reserved и все нераспознанные опции **должны** игнорироваться. Будущие совместимые изменения протокола могут менять содержимое поля Reserved или добавлять опции, несовместимые изменения могут использовать другие значения Code.

Содержимое опций, не указанных для сообщений NS, **должно** игнорироваться с продолжением обычной обработки пакета. В настоящее время для сообщений определена лишь опция Source Link-Layer Address.

Сообщения NS, прошедшие проверку, считаются действительными запросами (valid solicitation).

7.1.2. Проверка NA

Узел **должен** без уведомления отбрасывать сообщения NA, на соответствующие приведённым ниже условиям:

- поле IP Hop Limit = 255, т. е. пакет не может пересылаться маршрутизаторами;
- значение ICMP Checksum корректно;
- ICMP Code = 0;
- размер ICMP (выводится из размера IP) составляет не менее 24 октетов;
- Target Address не является групповым адресом;
- если IP Destination Address содержит групповой адрес, флаг Solicited сброшен (0);
- все включённые опции имеют ненулевой размер.

Содержимое поля Reserved и все нераспознанные опции **должны** игнорироваться. Будущие совместимые изменения протокола могут менять содержимое поля Reserved или добавлять опции, несовместимые изменения могут использовать другие значения Code.

Содержимое опций, не указанных для сообщений NA, **должно** игнорироваться с продолжением обычной обработки пакета. В настоящее время для сообщений определена лишь опция Target Link-Layer Address.

Сообщения NA, прошедшие проверку, считаются действительными анонсами (valid advertisement).

7.2. Распознавание адресов

Процесс распознавания адресов служит для определения узлом адреса канального уровня у соседа по его адресу IP. Распознавание выполняется лишь для относящихся к каналу (on-link) адресов, для которых отправитель не знает адрес на канальном уровне (см. 5.2. Концептуальный алгоритм передачи) и не применяется для групповых адресов.

Хост может получить запрос, анонс маршрутизатора или сообщение Redirect без опции с адресом канального уровня. По таким сообщениям **недопустимо** создавать или обновлять записи в кэше соседей, за исключением флага IsRouter в них, как указано в параграфах 6.3.4 и 7.2.5. Если для отправителя такого сообщения нет записи в Neighbor Cache, требуется выполнить распознавание адреса до начала взаимодействия с ним по индивидуальному адресу. Это относится, в частности, к индивидуальным откликам на запросы, где нужен обмен дополнительными пакетами для доставки анонса.

7.2.1. Инициализация интерфейса

При включении интерфейса, поддерживающего групповую адресацию узел **должен** присоединить к этому интерфейсу групповой адрес all-nodes, а также групповой адрес solicited-node, соответствующий каждому IP-адресу интерфейса.

Набор назначенных интерфейсу адресов может меняться с течением времени, т. е. адреса могут добавляться и удаляться с помощью [ADDRCONF]. В таких случаях узел **должен** присоединяться или покидать группу solicited-node, соответствующую адресу. Присоединение группового адреса solicited-node выполняется с использованием обнаружения «групповых слушателей» (Multicast Listener Discovery), такого как протокол [MLD] или [MLDv2]. Отметим, что одному групповому адресу solicited-node может соответствовать несколько индивидуальных адресов и узлу **недопустимо** выходить из группы solicited-node, пока остаётся хотя бы один индивидуальный адрес, соответствующий этой группе.

7.2.2. Отправка сообщений NS

Когда узел имеет индивидуальный пакет для отправки соседу, но не знает его адрес на канальном уровне, он выполняет распознавание адресов. Для интерфейсов с поддержкой групповой адресации это влечёт создание записи Neighbor Cache со статусом INCOMPLETE и передаст сообщения NS, направленного соседу по групповому адресу solicited-node, соответствующему адресу цели.

Если адрес отправителя в пакет, вызывающем запрос, совпадает с одним из адресов передающего интерфейса, этот адрес **следует** поместить в поле IP Source Address исходящего запроса. В иных случаях можно указывать любой из адресов интерфейса. Использование адреса отправителя вызвавшего запрос пакета обеспечивает включение получателем сообщения NS в свой Neighbor Cache адреса IP, который с большой вероятностью будет применяться в последующем обмене трафиком, связанном с вызвавшим «соединение» пакетом.

Если запрос передаётся по групповому адресу solicited-node, отправитель **должен** передать свой адрес канального уровня (при наличии) в опции Source Link-Layer Address. В иных случае отправителю **следует** передать свой адрес канального уровня (при наличии) в опции Source Link-Layer Address. Включение адреса отправителя на канальном уровне в групповой запрос нужно для того, чтобы получатель мог передать сообщение NA. При индивидуальном запросе реализация **может** не включать опцию Source Link-Layer Address. Здесь предполагается, что при наличии в кэше отправителя партнерского адреса канального уровня высока вероятность того, что у партнёра также кэширован адрес отправителя, поэтому его можно не передавать.

В процессе распознавания адреса отправитель **должен** для каждого соседа сохранять небольшую очередь пакетов, ожидающих завершения распознавания. Очередь **должна** вмещать хотя бы 1 пакет и **может** включать больше, однако число пакетов в очереди для одного соседа **следует** делать небольшим. При заполнении очереди новым пакетам **следует** замещать наиболее старые. По завершении распознавания узел передаёт пакеты из очереди.

В процессе ожидания отклика отправителю **следует** повторять сообщения NS примерно каждые RetransTimer мсек, даже если нет другого трафика для соседа. Частота повтора **должна** быть ограничена - не более 1 запроса в течение RetransTimer мсек.

Если не было получено сообщения NA после MAX_MULTICAST_SOLICIT запросов, распознавание адреса считается неудачным и отправитель **должен** вернуть сообщение ICMP о недоступности адресата с кодом 3 (Address Unreachable) для каждого пакета из очереди распознавания адресов.

7.2.3. Приём сообщений NS

Действительные запросы NS, не соответствующие ни одному из приведённых ниже требований, **должны** отбрасываться без уведомления отправителя.

- Target Address является «корректным» индивидуальным адресом принимающего интерфейса [ADDRCONF];
- в Target Address указан индивидуальный или anycast-адрес, для которого узел обеспечивает услуги прокси;
- Target Address содержит «предварительный» адрес, для которого выполняется процедура DAD [ADDRCONF].

Если Target Address является предварительным, запрос NS следует обрабатывать в соответствии с [ADDRCONF], в иных случаях применяется описанная ниже процедура. Если Source Address не является незаданным (unspecified) и на канальных уровнях с адресацией запрос включает опцию Source Link-Layer Address, получателю **следует** создать или обновить запись Neighbor Cache для IP Source Address из запроса. Если записи нет, узлу **следует** создать её и установить статус STALE, как указано в параграфе 7.3.3. Если запись имеется и содержит другой адрес канального уровня (не совпадает с опцией Source Link-Layer Address), запись следует обновить, поместив полученный в опции адрес, а для статуса доступности в записи **должно** быть установлено значение STALE.

При создании NCE для флага IsRouter **следует** устанавливать значение FALSE даже при получении NS от маршрутизатора, поскольку сообщения NS не указывают, является ли отправитель маршрутизатором. Если запрос отправлен маршрутизатором, следующие сообщения NA или RA установят верное значение IsRouter. При наличии записи NCE менять в ней флаг IsRouter **недопустимо**.

Если Source Address содержит неуказанный адрес, узлу **недопустимо** создавать или обновлять NCE.

После обновления Neighbor Cache узел передаёт анонс NA, как указано в следующем параграфе.

7.2.4. Отправка запрошенных сообщений NA

Узел передаёт анонс NA в ответ на действительный запрос NS для одного из адресов узла. Target Address в анонсе копируется из одноимённого поля запроса. Если IP Destination Address в запросе не является групповым адресом, опцию Target Link-Layer Address **можно** не включать, поскольку кэшированное соседом значение должно совпадать с текущим адресом, чтобы запрос был получен. Если IP Destination Address в запросе содержит групповой адрес, в анонс **должна** включаться опция Target Link-Layer. Если узел является маршрутизатором, он **должен** установить флаг Router, который в противном случае **должен** быть сброшен.

Если Target Address является anycast-адресом или индивидуальным адресом, для которого узел служит посредником, или опция Target Link-Layer Address не включена, флаг Override **следует** сбросить (0), в иных случаях флаг O **следует** установить (1). Корректный флаг O гарантирует предпочтение прямых не прокси) анонсов, а также «выиграет» первый анонса для anycast-адреса.

Если запрос отправлен с неуказанного адреса, узел **должен** сбросить флаг Solicited и передать анонс по групповому адресу all-nodes. В иных случаях узел **должен** установить флаг Solicited и передать индивидуальных анонс по Source Address из запроса.

Если Target Address содержит anycast-адрес, отправителю **следует** задержать передачу отклика на случайное время от 0 до MAX_ANYCAST_DELAY_TIME секунд.

Поскольку в индивидуальные NS не требуется включать опцию Source Link-Layer Address, в Neighbor Cache узла, передающего запрошенный анонс NA, может не оказаться соответствующего адреса канального уровня. В таких случаях узлу придётся сначала выполнить процедуру ND для определения адреса соседа на канальном уровне (отправка группового сообщения NS).

7.2.5. Приём сообщений NA

При получении действительного анонса NA (запрошенного или незапрошенного) выполняется поиск в Neighbor Cache записи для цели. Если запись имеется, анонс **следует** отбросить без уведомления. Если записи нет, создавать её не требуется, поскольку отправитель видимо ни инициировал взаимодействия с целью.

После нахождения подходящей NCE действия зависят от статуса этой записи, флагов анонса и представленного адреса канального уровня. Если NCE для цели имеет статус INCOMPLETE при получении анонса, возможны 2 варианта. Если канальный уровень использует адреса и опция Target Link-Layer Address в анонсе отсутствует, принимающему узлу **следует** просто отбросить полученный анонс. В иных случаях выполняются указанные ниже шаги:

- адрес канального уровня записывается в NCE;
- если в анонсе установлен флаг Solicited, запись переходит в состояние REACHABLE, иначе - в STALE;
- в записи устанавливается флаг IsRouter в соответствии с флагом Router из анонса;
- передаются пакеты из очереди, ожидающие распознавания адреса сосед.

Флаг Override игнорируется, если запись имеет состояние INCOMPLETE.

Если состояние NCE при получении анонса отличается от INCOMPLETE, выполняются указанные ниже действия.

I. Если флаг Override сброшен и полученный адрес канального уровня отличается от кэшированного, есть 2 варианта:
   a. запись со статусом REACHABLE переводится в STALE без внесений других изменений;
   b. в иных случаях полученный анонс игнорируется, а обновление кэше **недопустимо**.

II. Если флаг Override установлен и полученный адрес канального уровня совпадает с кэшированным или опция Target Link-Layer Address не включена, полученный анонс **должен** обновлять NCE, как показано ниже.
   - Адрес канального уровня из Target Link-Layer Address **должен** быть помещён в кэш (если он указан и отличается от кэшированного.
   - Если установлен флаг Solicited, для записи **должно** быть установлено состояние REACHABLE. Если флаг Solicited сброшен и адрес канального уровня изменён, **должно** быть установлено состояние STALE. В иных случаях запись не изменяется.

     Флаг Solicited в анонсах следует устанавливать лишь при отклике на NS. Поскольку запросы NUD передаются по кэшированным адресам канального уровня, получение запрошенного анонса указывает, что путь пересылки работает. Приём незапрошенного анонса может указывать наличие у соседа важной информации (например, о смене адреса канального уровня). Если важная информация указывает смену используемых узлом параметров, следует проверить доступность (нового) пути при передаче следующего пакета. Не требуется обновлять состояние по незапрошенным анонсам, не меняющим содержимое кэша.
   - Флаг IsRouter в кэше **должен** устанавливаться в соответствии с флагом Router в полученном анонсе. При смене флага IsRouter с TRUE на FALSE в результате обновления узел **должен** удалить маршрутизатор из Default Router List и обновить записи Destination Cache для всех адресатов, использовавших этого соседа как маршрутизатор, в соответствии с параграфом 7.3.3. Этот нужно для фиксации перехода маршрутизатора в состояние хоста, когда он прекращает пересылать пакеты.

Приведённые выше правила гарантируют обновление кэша, когда анонс является предпочтительным (установлен флаг Override) или NA указывает ранее кэшированный адрес канального уровня. В остальных случаях анонс запрашивает процедуру определения доступности соседа NUD (если ана ещё не запущена) путём смены статуса записи в кэше.

7.2.6. Передача незапрошенных сообщений NA

В некоторых случаях узел способен заметить смену своего адреса на канальном уровне (например, «горячее» переключение сетевого адаптера) и может быстро информировать своих соседей об этом. В таких случаях узел **может** передать до MAX_NEIGHBOR_ADVERTISEMENT незапрошенных анонсов NA по групповому адресу all-nodes. Интервал между этими анонсами **должен** быть не меньше RetransTimer секунд.

В поле Target Address незапрошенных анонсов следует указывать IP-адрес интерфейса, а в опции Target Link-Layer Address - новый адрес канального уровня. Флаг Solicited **должен** быть сброшен для предотвращения путаницы с алгоритмом NUD. Если узел является маршрутизатором, он **должен** установить флаг Router, иначе файл **должен** быть сброшен. Флаг Override **может** иметь любое значение. В любом случае соседние узлы будут сразу же менять статус своих записей NCE для Target Address на STALE, предлагая проверить доступность пути. Если флаг Override

установлен, соседи будут помещать новый адрес канального уровня в свой кэш, в ином случае новый адрес будет игнорироваться с проверкой кэшированного адреса.

Узел с несколькими адресами IP на интерфейсе **может** передать групповые анонсы NA для каждого адреса и в этом случае между анонсами должна задаваться небольшая задержка во избежание потери пакетов от перегрузки.

Прокси **может** передать групповые анонсы NA при смене у него адреса канального уровня или при настройке (системой управления или иным механизмом) на нем функции посредника для адреса. При наличии нескольких прокси им следует предоставлять механизм, препятствующий одновременному групповому анонсированию одного набора адресов разными посредниками для снижения риска избыточного группового трафика. Это требование для других протоколов, которым нужен посредник для NA. Примером узла с прокси-анонсами служит Home Agent из [MIPv6].

Узел, относящийся к anycast-адресу, **может** передавать незапрошенные групповые NA для адреса anycast при смене своего адреса на канальном уровне.

Поскольку незапрошенные анонсы NA не обеспечивают надёжного обновления кэша на всех узлах (анонсы могут не попасть на все узлы), их следует рассматривать лишь как оптимизацию для быстрого обновления кэша у большинства соседей. Алгоритм NUD обеспечивает получение всеми узлами доступного адреса канального уровня, хотя задержка может быть несколько больше.

7.2.7. Anycast-сообщения NA
С точки зрения ND адреса anycast трактуются в большинстве случаев как индивидуальные адреса. Поскольку синтаксически они не отличимы, узлы, выполняющие распознавание адресов или NUD для адреса anycast работают с ним как с индивидуальным адресом. Узлы с адресами anycast на интерфейсах трактуют их как индивидуальные с двумя исключениями. Во-первых, анонсы NA, передаваемые в ответ на NS, **следует** задерживать на случайное время из интервала 0 - MAX_ANYCAST_DELAY_TIME для снижения вероятности перегрузки сети. Во-вторых, флаг Override в анонсах NA **следует** сбрасывать, поэтому при получении нескольких анонсов будет использоваться первый.

Как и для индивидуальных адресов, NUD обеспечивает быстрое обнаружение недействительности привязки anycast.

7.2.8. Proxy NA
В ограниченных случаях маршрутизатор **может** выполнять функции посредника для одного или множества других узлов, указывая через анонсы NA своё желание воспринимать пакеты, не адресованные явно ему. Например, маршрутизатор может воспринимать пакеты от имени мобильного узла, покинувшего канал. Механизмы, применяемые прокси, по сути не отличаются от механизмов, используемых с адресами anycast. Прокси **должен** присоединить групповые адреса solicited-node, соответствующие адресам IP узлов, для которых предоставляются функции посредника. Это **следует** делать с использованием протокола обнаружения групповых слушателей, такого как [MLD] или [MLDv2].

Во всех запрошенных прокси-анонсах NA флаг Override **должен** быть сброшен. Это гарантирует при наличии самого узла на канале предпочтение его анонсам NA (флаг Override установлен) по отношению к анонсам от посредника. Прокси **может** передавать незапрошенные анонсы с установленным флагом Override, как указано в параграфе 7.2.6, но это может приводить к переопределению этими анонсами действительных записей, созданных самим узлом.

При отправке прокси-анонсов в ответ на запросы NS отправителю следует задерживать отклик на время от 0 до MAX_ANYCAST_DELAY_TIME секунд во избежание конфликтов нескольких откликов от разных прокси. Однако в некоторых случаях (например, Mobile IPv6), где имеется лишь один посредник, такая задержка не требуется.

7.3. Алгоритм NUD
Связь с соседом или через него может сталкиваться с отказами по многим причинам, включая отказы оборудования, «горячую» перестановку сетевых интерфейсов и т. п. Если отказ произошёл у адресата, восстановление невозможно и связь теряется, но если отказ возникает в пути, восстановление может оказаться возможным. Таким образом, узел активно отслеживает «состояние» доступности соседей, которым от передаёт пакеты.

NUD применяется на всех путях между хостом и его соседями, включая взаимодействия «хост-хост», «маршрутизатор-хост» и «хост-маршрутизатор», а также может использоваться между маршрутизаторами, но в этом случае не требуется, если имеется эквивалентный механизм, например, в протоколе маршрутизации.

Когда представляется, что путь к соседу не работает, конкретная процедура восстановления зависит от способа использования соседа. Если тот является конечным получателем, можно, например, повторить процедуру распознавания адреса. Если сосед служит маршрутизатором, можно попытаться перейти на другой маршрутизатор. Конкретное восстановление охватывается определением next-hop и NUD указывает необходимость такого определения, удаляя NCE. Процедура NUD выполняется лишь для соседей, которым передаются индивидуальные пакеты, и не используется при передаче по групповым адресам.

7.3.1. Подтверждение доступности
Сосед считается достижимым, если у узла имеется недавнее подтверждение доставки отправленных тому пакетов IP-уровню соседа. Подтверждения могут приходить двумя способами - «подсказки» от вышележащего протокола о «продвижении соединения» (forward progress) и сообщения NA в ответ на запросы NS.

Соединение «продвигается», если пакеты от удалённого партнёра могут приходить лишь в результате фактического получения тем недавно отправленных ему пакетов. Например, в TCP получение (нового) подтверждения указывает, что отправленные ранее данные достигли партнёра, а поступление от партнёра новых данных (не дубликатов) указывает, что прежние подтверждения были доставлены ему. Если пакеты поступили к партнёру, они также должны достигнуть next-hop-соседа отправителя, поэтому «продвижение соединения» подтверждает доступность соседа next-hop. Для адресатов вне канала (off-link) такое «продвижение» предполагает доступность маршрутизатора first-hop. По возможности **следует** использовать эту информацию вышележащего уровня.

В некоторых случаях (например, протоколы на основе UDP и маршрутизаторы, пересылающие пакеты хостам) информация о достижимости от протоколов вышележащего уровня может быть недоступна. Когда нет доступных подсказок и узел передаёт пакеты соседу, он активно зондирует его, используя индивидуальные пакеты NS для проверки работоспособности пути пересылки. Получение запрошенного анонса NA служит подтверждением доступности, поскольку анонсы с установленным флагом Solicited передаются лишь в ответ на запросы NS.

Приём других сообщений ND, например, анонсов RA или NA со сброшенным флагом Solicited **недопустимо** считать подтверждением доступности. Незапрошенные сообщения подтверждают лишь односторонний путь от передающего узла к принявшему. В отличие от этого NUD требует отслеживания узлом доступности прямого пути к соседу со своей (а не соседа) точки зрения. Получение запрошенного анонса указывает, что путь работает в обоих направлениях. Запрос должен попасть к соседу и инициировать отправку отклика, а получение анонса подтверждает работу обратного пути. Однако последнее известно лишь получателю анонса, а у отправителя нет способа узнать напрямую о доставке соседу отправленного анонса. С точки зрения NUD интересная лишь доступность прямого пути.

7.3.2. Состояния NCE

Запись NCE может иметь одно из приведённых ниже пяти состояний.

INCOMPLETE

Для записи происходит распознавание адреса, в частности, отправлен запрос NS по групповому адресу solicited-node для цели, но ответный анонс NA ещё не получен.

REACHABLE

В течение последних ReachableTime мсек получено подтверждение корректной работы пути к соседу. В состоянии REACHABLE для передачи пакетов не требуется каких-либо специальных действий.

STALE

Прошло более ReachableTime мсек с момента последнего подтверждения корректной работы пути к соседу. Для передачи пакетов не требуется каких-либо специальных действий. Переход в состояние STALE происходит при получении незапрошенного сообщения ND, обновляющего кэшированный адрес канального уровня. Такое сообщение не подтверждает доступность, а переход в состояние STALE обеспечивает быструю проверку доступности при фактическом использовании записи, однако без этого доступность не проверяется.

DELAY

Прошло более ReachableTime мсек с момента последнего подтверждения корректной работы пути к соседу и в последние DELAY_FIRST_PROBE_TIME секунд соседу был отправлен пакет. Если не было получено подтверждения в течение DELAY_FIRST_PROBE_TIME секунд после перехода в состояние DELAY, соседу отправляется запрос NS, а состояние меняется на PROBE.

Состояние DELAY обеспечивает протоколам вышележащих уровней время для предоставления сведений о доступности в тех случаях, когда прошло ReachableTime мсек с последнего подтверждения из-за отсутствия трафика. Без такой оптимизации создание соединения TCP после приостановки трафика привело бы к зондирования даже в случае подтверждения доступности трехэтапным согласованием практически сразу.

PROBE

Запрашивается подтверждение доступности путём отправки NS каждые RetransTimer мсек до получения ответа.

7.3.3. Поведение узла

NUD работает параллельно с отправкой пакетов соседу. Заново подтверждая доступность соседа, узел продолжает передавать тому пакеты по кэшированному адресу канального уровня. Если трафик соседу не передаётся, не отправляются и пакеты-зонды.

Когда узлу нужно распознать адрес соседа, он создаёт запись со статусом INCOMPLETE и запускает распознавание, как указано в параграфе 7.2. Если распознать адрес не удалось, запись следует удалить, чтобы последующий трафик к соседу снова вызвал процедуру поиска next-hop, обеспечивающую попытку использовать другие маршрутизаторы.

При получении подтверждения доступности (от вышележащего уровня или анонса NA) состояние записи меняется на REACHABLE. Однако сведения от вышележащего уровня не влияют на записи со статусом INCOMPLETE (например, на те, для которых нет кэшированного адреса канального уровня).

По истечении ReachableTime мсек с момент приёма последнего подтверждения доступности соседа состояние NCE для него меняется с REACHABLE на STALE.

Примечание. Реализация может отложить смену статуса REACHABLE на STALE до отправки пакета соседу, т. е. не требуется явный тайм-аут, связанный с ReachableTime.

При первой отправке пакета соседу, запись для которого имеет статус STALE отправителю следует сменить состояние записи на DELAY и установить для таймера значение DELAY_FIRST_PROBE_TIME секунд. Если запись сохранить состояние DELAY по завершении отсчёта таймера, её состояние меняется на PROBE, если же приходит подтверждение доступности, состояние меняется на REACHABLE.

При переходе записи в состояние PROBE узел передаёт соседу индивидуальное сообщение NS по кэшированному адресу канального уровня и повторяет запросы NS каждые RetransTimer мсек, пока не будет получено подтверждение доступности. Пробы передаются даже при отсутствии других пакетов для соседа. Если в течение RetransTimer мсек после отправки MAX_UNICAST_SOLICIT запросов не получено ответа, передача проб прекращается, а запись **следует** удалить. Последующий трафик к соседу снова создаст запись и повторит распознавание адреса.

Отметим, что для каждого соседа частота отправки NS ограничивается независимо. Узлу **недопустимо** передавать NS одному соседу чаще 1 раза в течение RetransTimer мсек.

NCE переходит в состояние STALE при создании записи в результате приёма пакета, отличного от запрошенного NA (RS, RA, Redirect, NS). Эти пакеты содержат адрес канального уровня отправителя или (в случае Redirect) цели перенаправления. Однако получение такого адреса канального уровня не подтверждает доступность пути к этому узлу. Размещение новой NCE, для которой известен адрес канального уровня, в состоянии STALE обеспечивает быстрое обнаружение отказов на пути. Кроме того при смене адреса канального уровня в результате приёма одного из указанных выше сообщений для записи также **следует** устанавливать статус STALE для быстрой проверки доступности пути к новому адресу канального уровня.

Для правильного определения перехода маршрутизатора в статус хоста (например, в результате отключения системой управления пересылки IP) узел **должен** сравнивать флаг Router в полученных анонсах NA с флагом IsRouter в NCE. При обнаружении перехода соседнего маршрутизатора в статус хоста узле **должен** удалить этот маршрутизатор из списка Default Router List и обновить Destination Cache, как указано в параграфе 6.3.5. Отметим, что маршрутизатора может не быть в Default Router List даже при его указании в Destination Cache (например, хост был перенаправлен на него). В таких случаях для записей Destination Cache, содержащих этот (бывший) маршрутизатор, должна быть выполнена процедура определения next-hop до использования записи.

В некоторых случаях данные канального уровня могут сообщать об отказе на пути к соседу (например, сброс виртуального канала) и эти сведения можно использовать для очистки NCE до того, как это сделает алгоритм NUD. Однако данные канального уровне **недопустимо** применять для подтверждения доступности сосед, поскольку они не содержат сведений о сквозной связности между уровнями IP соседей.

8. Функция перенаправления

В этом разделе рассматривается передача и обработка сообщений Redirect. Эти сообщения передаются лишь маршрутизаторами хостам для указания лучшего первого маршрутизатора на пути к адресату или информирования о том, что адресат является соседом (на канале). Указание обеспечивается значением ICMP Target Address совпадающим с ICMP Destination Address.

Маршрутизатор **должен** быть способен определить адрес link-local для каждого из соседний маршрутизаторов, чтобы гарантировать идентификацию адресом цели в сообщении Redirect соседнего маршрутизатора по его адресу link-local. При статической маршрутизации это предполагает, что адрес next-hop следует указывать адресом link-local для маршрутизатора, при динамической - обмен всеми протоколами маршрутизации IPv6 сведениями об адресах link-local для соседних маршрутизаторов.

8.1. Проверка сообщений Redirect

Хост **должен** без уведомления отбрасывать сообщения Redirect, не соответствующие всем указанным ниже условиям.

- IP Source Address содержит адрес link-local. Маршрутизаторы могут использовать свои адреса в поле отправителя сообщений RA и Redirect так, что хосты могут однозначно распознать маршрутизатор.
- Поле IP Hop Limit имеет значение 255, препятствующее пересылке пакетов маршрутизатором.
- Поле ICMP Checksum корректно.
- ICMP Code = 0.
- Размер ICMP (выводится из размера IP) не менее 40 октетов.
- IP-адрес отправителя Redirect совпадает с адресом первого маршрутизатора для ICMP Destination Address.
- Поле ICMP Destination Address в сообщении не содержит групповой адрес.
- ICMP Target Address является адресом link-local (при перенаправлении на маршрутизатор) или совпадает с ICMP Destination Address (при перенаправлении получателю на канале).
- Размер всех включённых опций отличается от 0.

Содержимое поля Reserved и все нераспознанные опции **должны** игнорироваться. Будущие совместимые изменения протокола могут менять содержимое поля Reserved или добавлять опции, несовместимые изменения могут использовать другие значения Code.

Содержимое опций, не указанных для сообщений Redirect, **должно** игнорироваться с продолжением обычной обработки пакета. В настоящее время для Redirect определены опции Target Link-Layer Address и Redirected Header.

Хосту **недопустимо** считать перенаправление негодным лишь на основании того, что Target Address не принадлежит одному из префиксов канала. Частью семантики Redirect является то, что Target Address относится к каналу.

Сообщения Redirect, прошедшие проверку, считаются действительными перенаправлениями (valid redirect).

8.2. Указание маршрутизатора

Маршрутизатору **следует** передавать сообщения Redirect с учётом ограничения скорости при каждой пересылке пакета, который явно не адресован ему (не задан source-route через маршрутизатор), когда выполняются все условия:

- поле Source Address в пакете указывает соседа;
- маршрутизатор определил (не заданными этой спецификацией способами), что лучший маршрутизатор для Destination Address в пересылаемом пакете расположен на одном канале с передающим узлом;
- Destination Address в пакете не содержит групповой адрес.

Переданный пакет перенаправления содержит в соответствии с форматом, заданным в параграфе 4.5:

- поле Target Address с адресом, куда следует отправлять последующие пакеты для получателя; если целью является маршрутизатор, **должен** применяться адрес link-local, для хоста адрес цели **должен** совпадать с полем Destination Address;
- поле Destination Address содержит адрес получателя из исходного пакета IP.
- опции:
  - Target Link-Layer Address содержит адрес канального уровня для цели (если он известен);
  - Redirected Header содержит часть пересылаемого пакета, которую можно включить без превышения минимального MTU, требуемого для поддержки IPv6, в соответствии с [IPv6].

Маршрутизатор должен ограничивать частоту передачи Redirect для снижения расхода полосы и ресурсов на обработку в случаях, когда отправитель не реагирует корректно или игнорирует неаутентифицированные сообщения. Дополнительная информация об ограничении частоты отправки сообщений ICMP об ошибках приведена в [ICMPv6].

Маршрутизаторам **недопустимо** обновлять свои таблицы маршрутизации на основании сообщений Redirect.

8.3. Указание хоста

Получив действительное сообщение Redirect, хосту **следует** обновить Destination Cache, чтобы последующий трафик шёл к указанной цели. Если в Destination Cache нет записи для адресата, реализации **следует** создать такую запись.

Если Redirect включает опцию Target Link-Layer Address, хост создаёт или обновляет NCE для цели. В обоих случаях адрес канального уровня копируется из опции Target Link-Layer Address. При создании NCE для цели в ней **должен** указываться статус STALE, как указано в параграфе 7.3.3. При обновлении адреса канального уровня в имеющейся записи она **должна** переводиться в состояние STALE. Если же адрес канального уровня для записи не меняется, её статус остаётся прежним.

Если Target Address совпадает с Destination Addresses, хост **должен** считать, что Target находится на канале (on-link). Если адреса различаются, хост **должен** установить для цели IsRouter = TRUE. Однако совпадение адресов Target и Destination не позволяет достоверно считать, что Target Address указывает маршрутизатор. Поэтому для создаваемой вновь NCE хосту следует установить IsRouter = FALSE, но в имеющихся записях флаг не меняется. Если Target является маршрутизатором, последующие сообщения NA или RA установят верный флаг IsRouter.

Сообщения Redirect применимы ко всем потокам в адрес данного получателя, т. е. после получения Redirect для Destination Address все записи Destination Cache для этого адреса следует обновить, указав в них заданный next-hop, независимо от поля Flow Label в заголовке Redirected Header.

Хостам **недопустимо** передавать сообщения Redirect.

9. Расширяемость в части обработки опций

Опции позволяют представлять поля переменного размера или неоднократно включаемые в пакет поля, а также необязательную для пакетов информацию. Опции также позволяют добавлять новые функции в будущие версии ND. Для совместимости будущих расширений с имеющимися реализациями все узлы **должны** игнорировать все непонятные опции в пакетах ND, продолжая обработку пакета. Все заданные в этом документе опции **должны** распознаваться. Узлу **недопустимо** игнорировать действительные опции лишь потому, что в ND есть непонятные.

Текущий набор опций определён так, что получатель может независимо обрабатывать несколько опций одного пакета. Для сохранения этого свойство будущим опциям **следует** соблюдать приведённое ниже простое правило.

> Зависимость опции от наличия или отсутствия других опций **недопустима**. Семантику опции следует основывать лишь на содержимом фиксированной части пакета ND и самой опции.

Соблюдение этого правила обеспечивает ряд преимуществ.

1) Получатели могут обрабатывать опции независимо. Например, реализация может обработать опцию Prefix Information из анонса RA пользовательским процессом, а опцию Link-Layer Address из того же сообщения - подпрограммой ядра.

2) Если число опций ведёт к превышению MTU на канале, их можно разделить по пакетам, сохраняя семантику.

3) Отправитель **может** передать опции в разных пакетах. Например, если Valid Lifetime и Preferred Lifetime для префикса достаточно велики, включение опции Prefix Information в каждый анонс RA может не требоваться. Кроме того, разные маршрутизаторы могут передавать свой набор опций. Поэтому получателю **недопустимо** связывать какое-либо действие с отсутствием опции в пакете. Этот протокол задаёт для получателей действия лишь на основании таймеров и сведений, полученных в пакетах.

Опции в пакетах ND могут указываться в любом порядке и получатель **должен** быть готов обрабатывать их независимо. Сообщение может также включать несколько экземпляров опции (например, Prefix Information).

Если опции в RA ведут к превышению MTU для канала, маршрутизатор может передать несколько анонсов, разделив опции между ними. Объем данных в опции Redirected Header **должен** ограничиваться, чтобы размер пакета не превышал минимальное значение MTU, требуемое для поддержки IPv6, как указано в [IPv6].

Размер всех опций кратен 8 октетам, что обеспечивает их выравнивание без заполнения. Поля опций (а также поля пакетов ND) определены с учётом выравнивания по естественным границам (например, 16-битовое поле выравнивается по 16-битовой границе), за исключением 128-битовых адресов и префиксов IP, выравниваемых по 64-битовой границе. Поля адресов канального уровня содержат неинтерпретируемые строки октетов и выравниваются по 8-битовой границе. Размер пакета ND вместе с заголовком IP ограничен MTU для канала. При добавлении опций в пакет ND **недопустимо** превышение MTU для канала.

В будущих версиях протокола могут появиться новые типы опций и получатели **должны** игнорировать непонятные опции, продолжая обработку сообщения.

10. Константы протокола

Константы маршрутизаторов

MAX_INITIAL_RTR_ADVERT_INTERVAL
16 секунд

MAX_INITIAL_RTR_ADVERTISEMENTS
3 передачи

MAX_FINAL_RTR_ADVERTISEMENTS
3 передачи

MIN_DELAY_BETWEEN_RAS
3 секунды
MAX_RA_DELAY_TIME
0,5 секунды
Константы хостов

MAX_RTR_SOLICITATION_DELAY
1 секунда
RTR_SOLICITATION_INTERVAL
4 секунды
MAX_RTR_SOLICITATIONS
3 передачи
Константы всех узлов

MAX_MULTICAST_SOLICIT
3 передачи
MAX_UNICAST_SOLICIT
3 передачи
MAX_ANYCAST_DELAY_TIME
1 секунда
MAX_NEIGHBOR_ADVERTISEMENT
3 передачи
REACHABLE_TIME
30 000 мсек
RETRANS_TIMER
1,000 мсек
DELAY_FIRST_PROBE_TIME
5 секунд
MIN_RANDOM_FACTOR
0,5
MAX_RANDOM_FACTOR
1,5

В разделе 4 определены форматы сообщений с дополнительными константами протокола. Любые константы могут измениться в будущих версиях протокола. Заданные спецификацией константы могут быть переопределены документами, описывающими работу IPv6 на конкретных канальных уровнях. Это правило позволяет ND работать на каналах с различными характеристиками.

11. Вопросы безопасности

Протокол ND подвержен атакам, которые могут направлять пакеты IP в неожиданные места. Такие атаки могут служить для нарушения работы служб, а также позволяют узлам перехватывать и при желании менять пакеты, предназначенные для других узлов. В этом разделе рассматриваются основные угрозы, связанные с сообщениями ND и возможные механизмы защиты для смягчения таких угроз.

11.1. Анализ угроз

В этом параграфе рассмотрены основные угрозы, связанные с ND, а более подробный анализ приведён в [PSREQ]. Основные уязвимости протоколы делятся на 3 категории: атаки на отказ в обслуживании (Denial-of-Service или DoS), атаки с подменой адресов и атаки с подменой маршрутизаторов.

Примером DoS-атаки является возможность находящегося на канале узла передавать пакеты с произвольным IP-адресом отправителя, анонсирующие узел как принятый по умолчанию маршрутизатор, а также отправлять поддельные анонсы RA, немедленно прекращающие срок действия всех других принятых по умолчанию маршрутизаторов на канале, а также всех префиксов. Злоумышленник может добиться этого, передавая множество RA, по ложному для каждого легитимного маршрутизатора, с адресом другого маршрутизатора в поле отправителя, Router Lifetime = 0, и нулевыми значениями Preferred Lifetime и Valid Lifetime для всех префиксов. Такая атака заставит все пакеты для получателей на канале и вне его проходить через обманный маршрутизатор, который может просматривать, менять или отбрасывать любые пакеты. Алгоритм NUD не увидит такую «чёрную дыру», пока обманный маршрутизатор корректно отвечает на зонды NUD анонсами NA с установленным флагом R.

Любой хост может организовать DoS-атаку на другой хост, препятствуя настройке адреса с помощью [ADDRCONF]. Протокол не позволяет хостам проверить, является ли отправитель NA действительным владельцем включённого в сообщение адреса IP.

Атаки с перенаправлением доступны любому хосту для создания лавины пакетов в адрес жертвы или кражи трафика. Хост может передать анонс NA (в ответ на запрос), содержащий свой адрес IP и адрес жертвы на канальном уровне для создания лавины нежелательного трафика по адресу жертвы, а также NA с IP-адресом жертвы и своим адресом на канальном уровне для переопределения записи в кэше адресатов, приводящего к краже трафика жертвы.

Модель доверия для перенаправлений такая же, как в IPv4 и Redirect воспринимается лишь при получении от того маршрутизатора, который сейчас применятся для адресата. Если хост перенаправляется на другой узел (т. е. адресат вне канала) невозможно предотвратить отправку другого Redirect с другой целью. Однако это воздействие не хуже, чем было до Redirect и подменённая цель всегда может быть маршрутизаторов, отправляющим трафик в другое место.

В протоколе нет механизма управления полномочиями соседе передавать определённые типы сообщений (например, RA) и любой сосед (предположительно даже при наличии аутентификации) может передать анонсы RA, вызывающие отказ в обслуживании. Кроме того, любой сосед может передавать proxy NA, а также незапрошенные анонсы NA для организации DoS-атаки.

Многие канальные уровни также подвержены DoS-атакам, таким как постоянно занятый канал в сети CSMA/CD (детектирование несущей с обнаружением конфликтов) путём беспрерывной отправки пакетов DoS-атак, вставки в

канал сигналов конфликта или порождения пакетов с чем-либо иным, нежели MAC-адрес отправителя с целью запутать, например, коммутаторы Ethernet. С другой стороны, многие из упомянутых здесь угроз менее эффективны или отсутствуют на каналах «точка-точка» и в сотовых сетях, где на канале имеется лишь один сосед, служащий принятым по умолчанию маршрутизатором.

11.2. Защита сообщений ND

Протокол снижает подверженность упомянутым выше атака при отсутствии аутентификации за счёт игнорирования пакетов ND от узлов вне канала. Поле Hop Limit во всех пакетах сравнивается с максимально допустимым значением 255. Поскольку маршрутизаторы декрементируют поле Hop Limit во всех пересылаемых пакетах, значение 255 говорит, что пакет получен от соседа.

Криптографическая защита ND выходит за рамки этого документа и описана в [SEND]. Можно также использовать IPsec для аутентификации на уровне IP [IPv6-SA]. Обмен ключами IKE (Internet Key Exchange) не подходит для создания защищённых связей, которые можно применить для защиты распознавания адресов или сообщений о запросе соседства, как указано в [ICMPIKE].

В некоторых случаях можно применить статические защищённые связи [IPv6-AUTH] или [IPv6-ESP] для защиты сообщений ND. Однако важно отметить, что статически заданные защищённые связи не расширяются (особенно на каналах с групповой адресацией), поэтому ограничены лишь небольшими сетями с известными хостами. В любом случае при использовании [IPv6-AUTH] или [IPv6-ESP] пакеты ND **должны** проверяться на предмет подлинности и не прошедшие проверку пакеты **должны** отбрасываться без уведомления.

12. Смена адресов

Протокол ND вместе с автоматической настройкой адресов IPv6 [ADDRCONF] помогает при смене адресов, позволяя ввести новые префиксы и адреса взамен прежних. Отказоустойчивость этих механизмов основана на том, что все узлы на канале своевременно получают анонсы RA. Однако хост может быть отключён или недоступен достаточно должно (например, несколько месяцев). В таких случаях можно обеспечить надёжную смену адресов, но это вносит ограничения на продолжительность анонсирования префиксов.

Рассмотрим пример, где префиксы анонсированы со сроком действия 2 месяца, но 1 августа принято решение о смене префикса 1 сентября. Это можно сделать путём снижения анонсируемого срока действия до 1 недели, начиная с 1 августа и постепенного снижения срока до анонсирование 1 сентября нулевого срока действия для префикса. Если один или несколько узлов были отключены от канала раньше 1 сентября, они могут считать, что срок действия префикса по-прежнему составляет 2 месяца. Таким образом, узел, отключенный 31 июля, будет считать, что префикс действует до 30 сентября. Единственным способом прекратить использование префикса, объявленного ранее с большим сроком действия, является получение узлом анонса, сокращающего срок действия префикса. В приведённом примере решение простое - анонсировать префикс с нулевым сроком действия в период с 1 сентября до 1 октября.

В общем случае для обеспечения отказоустойчивости при отключении узлов от канала важно отслеживать самое отдалённое будущее, когда конкретный префикс ещё представляется действительным для какого-либо узла на канале. Отозванный префикс должен анонсироваться с нулевым сроком действия до наступления этого момента в будущем. Это время определяется максимальным сроком действия префиксов из всех RA, отправленных к данному моменту.

Сказанное выше важно для префиксов с неограниченным сроком действия. Если префикс, анонсированный с таким сроком, нужно поменять, нежелательно анонсировать для него нулевой срок действия в течение неограниченного времени. Поэтому следует избегать неограниченного срока, либо задавать предельный срок, на который узел может быть отключён от канала с возможностью последующего подключения. Однако способ ограничить период отключения узлов от канала (например, ноутбуков) не ясен.

Администраторам следует серьёзно подумать о применении сравнительно коротких сроков действия (не более нескольких недель). Хотя может казаться, что долгий срок действия помогает обеспечить отказоустойчивость, на деле хост не сможет взаимодействовать с сетью без корректно работающих маршрутизаторов. Такие маршрутизаторы будут передавать анонсы RA с подходящим (и текущим) префиксом. Хост, подключенный к сети без работающих маршрутизаторов, очевидно столкнётся с более существенными проблемами, чем отсутствие действительного префикса и адреса.

Приведённые рассуждения относятся как к Preferred Lifetime, так и к Valid Lifetime. На практике вероятно будет достаточно отслеживать Preferred Lifetime, поскольку этот срок не выходит за пределы Valid Lifetime.

13. Взаимодействие с IANA

Этот документ не требует выделения новых типов или кодов ICMPv6, однако в имеющихся типах ссылка на RFC 2461 заменена ссылкой на этот документ. Процедура выделения значений для ICMPv6 описана в разделе 6 [ICMPv6].

Этот документ использует указанные ниже типы сообщений ICMPv6, определённые в RFC 2461 и выделенные IANA.

Имя	***ICMPv6 Type***
Router Solicitation	133
Router Advertisement	134
Neighbor Solicitation	135
Neighbor Advertisement	136
Redirect	137

Этот документ использует указанные ниже типы опций ND, которые определены в RFC 2461 и выделены IANA.

Имя	***Тип***
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Правила выделения типов опций ND указаны ниже.

1. IANA следует выделять и регистрировать (постоянно) новые типы опций из IETF RFC, включая Standards Track, Informational и Experimental, исходящих от IETF и одобренных для публикации IESG.

2. При согласии рабочих групп IETF и одобрении руководителя направления можно запросить в IANA отзыв выделенного значения для типа опции ND. IANA будет помечать значение как reclaimable in future и такая пометка будет удаляться при публикации RFC с протоколом, как указано в п. 1). Это сделает назначение постоянным и обновит ссылку на Web-сайте IANA.

   При использовании 85% пространства опций IETF будет пересматривать значения со статусом reclaimable in the future и информировать IANA о необходимости переназначения конкретных типов.

3. Запросы на выделение новых типов извне процессов IETF все равно выполняются путём публикации документа IETF, как указано в п. 1). Отметим, что документы, опубликованные как RFC Editor contributions [RFC3667], не считаются документами IETF.

14. Литература

14.1. Нормативные документы

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

[ICMPv6] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

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

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

14.2. Дополнительная литература

[ADDRCONF] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

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

[ARP] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[ASSIGNED] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[DHCPv6] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[HR-CL] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[ICMPIKE] Arkko, J., "Effects of ICMPv6 on IKE", Work in Progress, March 2003.

[ICMPv4] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[IPv6-3GPP] Wasserman, M., Ed., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[IPv6-CELL] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, April 2003.

[IPv6-ETHER] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[IPv6-SA] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

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

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

[LD-SHRE] Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, November 2005.

[MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[MLD] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[MLDv2] Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[PSREQ] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RAND] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RDISC] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[RFC3667] Bradner, S., "IETF Rights in Contributions", RFC 3667, February 2004.

[RTSEL] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[SH-MEDIA] Braden, B., Postel, J., and Y. Rekhter, "Internet Architecture Extensions for Shared Media", RFC 1620, May 1994.

[SEND] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[SYNC] S. Floyd, V. Jacobson, "The Synchronization of Periodic Routing Messages", IEEE/ACM Transactions on Networking, April 1994. ftp://ftp.ee.lbl.gov/papers/sync_94.ps.Z

Приложение A. Многодомные хосты

При использовании ND хостами с множеством интерфейсов возникает ряд осложнений. В этом разделе не предпринимается попыток определить подобающую работу многодомных хостов в части обнаружения соседей, а лишь отмечены проблемы, требующие дальнейшего изучения. Разработчикам рекомендуется поэкспериментировать с различными подходами к ND на многодомных хостах и поделиться своим опытом. Дополнительное рассмотрение этого вопроса приведено в [RTSEL].

Если многодомный хост получает анонсы RA на всех интерфейсах, он (вероятно) узнает на каждом канале префиксы относящихся к тому адресов. Однако при пересылке пакета через маршрутизатор выбор «неверного» маршрутизатора может привести на неоптимальных или неработающий путь. Следует рассмотреть приведённые ниже вопросы.

1) Чтобы маршрутизатор передал Redirect, он должен определить, что пересылаемый им пакет исходит от соседа. Стандартной проверкой в этом случае является сравнение адреса отправителя в пакете со списком префиксов на связанном с интерфейсом канале, откуда был принят пакет. Если хост-источник является многодомным, использованный адрес отправителя может относиться не к тому интерфейсу, который передал пакет. В этом случае маршрутизатор может не передать сообщений Redirect и вероятная неоптимальная маршрутизация. Для перенаправления передающий хост должен всегда отправлять пакеты с интерфейса, соответствующего адресу отправителя. Отметим, что этой проблемы не возникает на хостах с одним интерфейсом. Дополнительное обсуждение этого вопроса приведено в параграфе 3.3.4.2 RFC 1122.

2) Если выбранный первый маршрутизатор (first-hop) не имеет пути к адресату, он не сможет доставить пакет. Однако адресат может быть доступен через другой маршрутизатор на другом интерфейсе. В ND этот вопрос не решается, поскольку он не возникает на хостах с одним интерфейсом.

3) Даже при наличии у первого маршрутизатора пути к адресату, через другой интерфейс может существовать лучший путь. Для многодомных хостов нет механизма обнаружения такого маршрута.

Если многодомный хост не сможет получить анонсы RA на одном или нескольких интерфейсах, он не будет знать (при отсутствии настройки), какие получатели будут на канале соответствующего интерфейса. В результате возникает проблема - если RA получены на некоторых, но не всех интерфейсах, многодомный хост сможет отправлять пакеты лишь с интерфейсов, принявших RA. Принятое здесь важное допущение состоит в том, что маршрутизаторы для этих интерфейсов могут переслать пакеты конечному адресату, даже если этот адресат находится в подсети отправителя, но не имеет информации о префиксе on-link. Если это допущение не выполняется (FALSE) связи будет невозможна. Но даже при соблюдении этого условия путь пакетов будет неоптимальным.

Приложение B. Возможные расширения

Ниже перечислены вопросы для возможного расширения в будущем.

- Использование динамических таймеров для работы на каналах с сильно меняющейся задержкой. Однако измерение времени кругового обхода требует подтверждений и порядковых номеров для сопоставления откликов NA с вызвавшими их запросами NS. Разработчики, желающие провести эксперименты с этим, могли бы сделать это совместимым путём, определив новую опцию с соответствующими данными. Узлы, не понимающие опцию, будут просто игнорировать её.

- Добавление возможностей для облегчения работы по каналам, которые сейчас требуют от хостов регистрации на сервере распознавания адресов. Это может, например, позволить маршрутизаторам запрашивать у хостов периодическую отправку незапрошенных анонсов. Это тоже можно реализовать добавлением опции в RA.

- Добавление дополнительных процедур для каналов в асимметричной и непереходной доступностью в обычный рабочий процесс. Такие процедуры могут позволить хостам и маршрутизаторам находить подходящие пути (например, радиоканалы.

Приложение C: Конечный автомат для статуса доступности

В этом приложении дана сводка правил, заданных в параграфах 7.2 и 7.3. Документ не требует от реализаций придерживаться этой модели, если внешнее поведение соответствует спецификации.

При распознавании адресов и NUD применимы описанные ниже смены состояния в рамках концептуальной модели.

Состояние	***Событие***	***Действие***	***Новое состояние***
-	Пакет для передачи	Создание записи, отправка группового NS, запуск таймера повтора	INCOMPLETE
INCOMPLETE	Тайм-аут повтора, меньше N повторов	Повтор NS, запуск таймера повтора	INCOMPLETE
INCOMPLETE	Тайм-аут повтора, N или больше повторов	Отбрасывание записи, передача сообщения ICMP об ошибке	-
INCOMPLETE	NA, Solicited=0, Override=any	Запись адреса канального уровня, отправка пакетов из очереди	STALE
INCOMPLETE	NA, Solicited=1, Override=any	Запись адреса канального уровня, отправка пакетов из очереди	REACHABLE
INCOMPLETE	NA, Solicited=any, Override=any, нет адреса канального уровня	Обновление флага IsRouter	Не меняется

-	NS, RS, Redirect, нет адреса канального уровня	-	-
!INCOMPLETE	NA, Solicited=1, Override=0, в кэше тот же адрес канального уровня	-	REACHABLE
!INCOMPLETE	NA, Solicited=any, Override=any, нет адреса канального уровня	Обновление флага IsRouter	Не меняется
REACHABLE	NA, Solicited=1, Override=0, в кэше другой адрес канального уровня	-	STALE
STALE, PROBE или DELAY	NA, Solicited=1, Override=0, в кэше другой адрес канального уровня	-	Не меняется
!INCOMPLETE	NA, Solicited=1, Override=1	Запись адреса канального уровня (если он другой)	REACHABLE
!INCOMPLETE	NA, Solicited=0, Override=0	-	Не меняется
!INCOMPLETE	NA, Solicited=0, Override=1, в кэше тот же адрес канального уровня	-	Не меняется
!INCOMPLETE	NA, Solicited=0, Override=1, в кэше другой адрес канального уровня	Запись адреса канального уровня	STALE
!INCOMPLETE	Подтверждение доступности от вышележащего уровня	-	REACHABLE
REACHABLE	Тайм-аут, более N секунд после подтверждения доступности	-	STALE
STALE	Передача пакет	Запуск таймера задержки	DELAY
DELAY	Тайм-аут задержки	Передача индивидуального NS, запуск таймера повтора	PROBE
PROBE	Тайм-аут повтора, меньше N повторов	Повтор NS	PROBE
PROBE	Тайм-аут повтора, не меньше N повторов	Отбрасывание записи	-

Смена состояний при получении незапрошенных данных, отличных от NA, применяется к источнику пакета (для сообщений NS, RS и RA) или целевому адресу (для Redirect), как показано ниже.

Состояние	***Событие***	***Действие***	***Новое состояние***
-	NS, RS, RA, Redirect	Создание записи	STALE
INCOMPLETE	NS, RS, RA, Redirect	Запись адреса канального уровня, отправка пакета из очереди	STALE
!INCOMPLETE	NS, RS, RA, Redirect с отличающимся от кэшированного адресом канального уровня	Обновление адреса канального уровня	STALE
INCOMPLETE	NS, RS без адреса канального уровня	-	Не меняется
!INCOMPLETE	NS, RS, RA, Redirect с кэшированным адресом канального уровня	-	Не меняется

Приложение D. Сводка правил для IsRouter

В этом приложении приведена сводка правил поддержки флага IsRouter в соответствии с этим документом. Правила основаны на явном или неявном присутствии в сообщениях ND сведений о роли отправителя (или Target Address) - хост или маршрутизатор.

- Отправитель анонса RA неявно считается маршрутизатором.
- Запросы NS не содержат явного или неявного указания типа отправителя, их могут передавать хосты и маршрутизаторы.
- Анонсы NA содержат явный флаг IsRouter (бит R).
- Целью перенаправления, когда она не совпадает с адресом получателя в пакете для перенаправления, неявно считается маршрутизатором. Это естественное допущение, поскольку предполагается способность узла переслать пакеты в направлении получателя.
- Цель перенаправления, совпадающая с адресом получателя, не содержит информации, является цель хостом или маршрутизатором. Известно лишь, что получатель (цель) находится на канале (on-link).

Правила установки флага IsRouter основаны на приведённой выше информации. Если сообщение ND содержит явное или неявное указание, приём такого сообщения вызовет обновление флага IsRouter. Однако при отсутствии в ND сведений (маршрутизатор или хост) **недопустимо** менять флаг IsRouter на основании сообщения. При создании записи Neighbor Cache в результате приёма сообщения данные документ задаёт для флага IsRouter значение FALSE. Корректное значение флага IsRouter в таких случаях определяет последующее сообщение NA или RA.

Приложение E. Вопросы реализации

E.1. Подтверждение доступности

Для механизма NUD требуется явное подтверждение доступности прямого пути к соседу. Для избавления от необходимости отправки пробных сообщений NS протоколам вышележащего уровня следует обеспечивать такую индикацию, когда затраты на это невелики. Ориентированные на соединения протоколы с гарантией доставки, такие как TCP, обычно знают о работоспособности прямого пути. Например, при передаче или приёме данных TCP обновляется окно порядковых номеров, запускаются и сбрасываются таймеры повтора и т. п. Ниже указаны конкретные примеры, где обычно указывается корректная работа прямого пути.

- Приём подтверждения, включающего порядковый номер (например, данные), который ещё не был подтверждён, говорит о нормальной работе прямого пути в момент отправки данных.
- Завершение трехэтапного согласования является частным случаем приведённого выше правила. Хотя при согласовании данные не передаются, флаги SYN с точки зрения порядковых номеров служат данными. Это относится как к SYN+ACK для активной стороны соединения, так и к ACK для пассивной.

- Приём новых (т. е. не полученных ранее) данных указывает нормальную работу прямого пути в момент отправки подтверждения, которое привело к сдвигу окна передачи, позволившему отправить новые данные.

Для минимизации расходов на передачу сведений о доступности между уровнями TCP и IP реализация может ограничить частоту отправки подтверждений доступности. Одним из вариантов является обработка данных о доступности через несколько пакетов. Например, можно обновлять сведения о доступности 1 раз за период кругового обхода. Для реализаций, поддерживающих Destination Cache с блоками управления, возможно обновление записей NCE напрямую (т. е. без дорогостоящего поиска) по демультиплексированию пакета TCP в соответствующий блок управления. Для других реализаций может быть возможна привязка подтверждения доступности к представлению уровню IP следующего пакета при условии, что реализация принимает меры против устаревания привязанных подтверждений, когда пакеты не передаются уровню IP достаточно долго.

Протокол TCP также должен обеспечивать защиту от представления «устаревших» сведений как текущего подтверждения доступности. Например, данные, полученные через 30 минут после открытия окна, не подтверждают текущей работоспособности пути, они просто говорят о том, что 30 минут назад обновление окна достигло партнёра, т. е. в тот момент путь работал. Реализация должна также учитывать зонды TCP с нулевым окном, передаваемые даже при разрыве пути, когда обновление окна не приходит к партнёру.

Для приложений UDP (RPC[1], DNS) относительно просто заставить клиента передавать подтверждение доступности при получении пакета с откликом. Сложнее, а в некоторых случаях невозможно генерировать такие подтверждения при отсутствии управления потоком, когда сервер не может определить, указывает ли полученный запрос приём предыдущего отклика.

Отметим, что реализация не может использовать негативные сведения вышележащего уровня как замену алгоритма NUD. Негативные сведения (например, об избыточных повторах TCP) могут служить указанием на то, что прямой путь от отправителя данных может не работать, в результате чего пакеты подтверждений не приходят отправителю.

Приложение F. Отличия от RFC 2461

- Удалены ссылки на IPsec AH и ESP для защиты сообщений и проверки полученных сообщений.
- Добавлен параграф 3.3.
- Обновлён раздел 11 включением подробного обсуждения угроз, ограничений IPsec и применения SEND.
- Исключено допущение принадлежности к каналу в параграфе 5.2 в соответствии с 4943[2] «IPv6 Neighbor Discovery On-Link Assumption Considered Harmful».
- Разъяснено определение поля Router Lifetime в параграфе 4.2.
- Обновлён текст параграфов 4.6.2 и 6.2.1 указанием на то, что значение Preferred Lifetime должно быть не больше Valid Lifetime.
- Ссылка на настройку с учётом состояния заменена ссылкой на DHCPv6.
- В параграф 6.2.1 добавлено определение флага IsRouter, позволяющего выступать хостом или маршрутизатором.
- Мобильным узлам разрешено не вносить случайную задержку при отправке RS в процессе перехода (handover).
- Обновлено определение размера префикса в опции Prefix.
- Обновлены сведения о применимости к каналам NBMA во введении и добавлены ссылки на 3GPP RFC.
- Указано, что распределение нагрузки доступно лишь на маршрутизаторах.
- Разъяснено поведение маршрутизатора при получении RS без опции Source Link-Layer Address Option (SLLAO).
- Отмечено, что проверка несогласованности CurHopLimit выполняется лишь при ненулевых значениях.
- Изменён параграф 7.2.5 для прояснения и описания обработки NA в состоянии INCOMPLETE.
- В параграф 7.2 добавлено разъяснение по части реагирования узлов на сообщения без опции SLLAO.
- Добавлен раздел о взаимодействии с IANA.
- Редакторские правки.

Благодарности

Авторы RFC 2461 хотели бы поблагодарить участников рабочей группы IPV6, в частности, (в алфавитном порядке) Ran Atkinson, Jim Bound, Scott Bradner, Alex Conta, Stephen Deering, Richard Draves, Francis Dupont, Robert Elz, Robert Gilligan, Robert Hinden, Tatuya Jinmei, Allison Mankin, Dan McDonald, Charles Perkins, Matt Thomas, Susan Thomson.

Редактор этого документа (Hesham Soliman) хотел бы поблагодарить рабочую группу IPV6 за большой вклад в этот документ, в частности, (в алфавитном порядке), Greg Daley, Elwyn Davies, Ralph Droms, Brian Haberman, Bob Hinden, Tatuya Jinmei, Pekka Savola, Fred Templin, Christian Vogt.

Адреса авторов

Thomas Narten
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709-2195
USA

[1]Remote Procedure Call - удаленный вызов процедуры.
[2]В оригинале ошибочно сказано RFC 4942, см. https://www.rfc-editor.org/errata/eid1317. *Прим. перев.*

Phone: +1 919 254 7798
EMail: narten@us.ibm.com

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, CA 94025
USA
Phone: +1 650 786 2921
Fax: +1 650 786 5896
EMail: erik.nordmark@sun.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
USA
EMail: william.allen.simpson@gmail.com

Hesham Soliman
Elevate Technologies
EMail: hesham@elevatemobile.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

Полное заявление авторских прав

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 Editor обеспечено Internet Society.