Internet Engineering Task Force (IETF)
Request for Comments: 9568
Obsoletes: 5798
Category: Standards Track
ISSN: 2070-1721

A. Lindem
LabN Consulting, L.L.C.
A. Dogra
Cisco Systems

April 2024

Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

Протокол резервирования виртуальных маршрутизаторов (VRRP) версии 3 для IPv4 и IPv6

Аннотация

Этот документ определяет версию 3 протокола резервирования виртуальных маршрутизаторов (Virtual Router Redundancy Protocol или VRRP) для IPv4 и IPv6. Документ заменяет собой RFC 5798, ранее задававший VRRP (версия 3). RFC 5798 отменил RFC 3768, задававший VRRP (версия 2) для IPv4. VRRP задаёт протокол выбора для динамического назначения ответственности за виртуальный маршрутизатор одному из маршрутизаторов VRRP в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4 или IPv6, связанные с виртуальным маршрутизатором, (Virtual Router или VR) называется активным (Active Router или AR) и пересылает пакеты на эти адреса IPv4 или IPv6. На активных маршрутизаторах настраиваются виртуальные адреса IPv4 или IPv6, а резервные маршрутизаторы (Backup Router или BR) определяют семейство виртуальных адресов для анонсирования на основе версии протокола IP. Внутри маршрутизатора VRRP виртуальные маршрутизаторы для каждого из семейств адресов IPv4 и IPv6 независимы один от другого и всегда считаются отдельными экземплярами VR. Процесс выбора обеспечивает динамический перенос ответственности пересылку, если AR становится недоступным. Для IPv4 преимуществом использования VRRP является более высокая доступность принятого по умолчанию маршрута без необходимости менять настройки протоколов динамической маршрутизации и обнаружения маршрутизаторов на каждом конечном хосте. Для IPv6 преимуществом является более быстрое переключение на BR, чем при использовании стандартных механизмов IPv6 Neighbor Discovery.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9568.

Авторские права

Авторские права (Copyright (c) 2024) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, перечисленные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно, поскольку в них описаны права и ограничения, относящиеся к данному документу. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа Trust Legal Provisions, без каких-либо гарантий (как указано в Revised BSD License).

Оглавление

1. Введение....2
1.1. Отличия от RFC 5798....2
1.2. Примечание по терминологии....3
1.3. IPv4....3
1.4. IPv6....3
1.5. Уровни требований....4
1.6. Область действия....4
1.7. Определения....4
2. Требуемые свойства....4
2.1. Резервирование адресов IPvX....4
2.2. Указание предпочтительного пути....5
2.3. Минимизация прерывания обслуживания....5
2.4. Эффективная работа в расширенных ЛВС....5
2.5. Субсекундные операции для IPv4 и IPv6....5
3. Обзор VRRP....5
4. Примеры сетей VRRP....6
4.1. Пример 1....6
4.2. Пример 2....6
5. Протокол....7
5.1. Формат пакетов VRRP....7
5.1.1. Описание полей IPv4....7

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

5.1.1.1. Source Address....7
5.1.1.2. Destination Address....7
5.1.1.3. TTL....7
5.1.1.4. Protocol....7
5.1.2. Описание полей IPv6....8
5.1.2.1. Source Address....8
5.1.2.2. Destination Address....8
5.1.2.3. Hop Limit....8
5.1.2.4. Next Header....8
5.2. Описание полей VRRP....8
5.2.1. Version....8
5.2.2. Type....8
5.2.3. Virtual Rtr ID (VRID)....8
5.2.4. Priority....8
5.2.5. IPvX Addr Count....8
5.2.6. Reserve....8
5.2.7. Max Advertise Interval....8
5.2.8. Checksum....8
5.2.9. Адреса IPvX....8
6. Конечный автомат протокола....9
6.1. Параметры виртуального маршрутизатора....9
6.2. Таймеры....9
6.3. Диаграмма смены состояний....9
6.4. Описания состояний....9
6.4.1. Initialize....10
6.4.2. Backup....10
6.4.3. Active....11
7. Передача и приём пакетов VRRP....12
7.1. Приём пакетов VRRP....12
7.2. Передача пакетов VRRP....12
7.3. MAC-адрес VR....13
7.4. Идентификаторы интерфейсов IPv6....13
8. Вопросы эксплуатации....13
8.1. IPv4....13
8.1.1. ICMP Redirect....13
8.1.2. Запросы ARP от хостов....13
8.1.3. Proxy ARP....13
8.2. IPv6....13
8.2.1. ICMPv6 Redirect....13
8.2.2. ND Neighbor Solicitation....14
8.2.3. Анонсы маршрутизаторов....14
8.2.4. Незапрошенные анонсы соседей....14
8.3. IPvX....14
8.3.1. Возможные петли при пересылке....14
8.3.2. Рекомендации по установке приоритета....14
8.4. Взаимодействие VRRPv3 и VRRPv2....14
8.4.1. Допущения....14
8.4.2. Поддержка взаимодействия с VRRPv2 в VRRPv3....15
8.4.2.1. Вопросы взаимодействия....15
8.4.2.1.1. Медленные AR с высоким приоритетом....15
8.4.2.1.2. Перегрузка резервных маршрутизаторов VRRPv2....15
9. Вопросы безопасности....15
10. Взаимодействие с IANA....15
11. Литература....16
11.1. Нормативные документы....16
11.2. Дополнительная литература....16
Благодарности....17
Адреса авторов....17

1. Введение

Этот документ определяет версию 3 протокола резервирования виртуальных маршрутизаторов (VRRP) для IPv4 и IPv6. Документ заменяет собой RFC 5798, ранее задававший VRRP (версия 3). RFC 5798 отменил RFC 3768, задававший VRRP (версия 2) для IPv4. VRRP задаёт протокол выбора для динамического назначения ответственности за виртуальный маршрутизатор (см. парагра 1.7) одному из маршрутизаторов VRRP в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4 или IPv6, связанные с виртуальным маршрутизатором, (VR) называется активным (AR) и пересылает пакеты на эти адреса IPv4 или IPv6 (за исключением пакетов, адресованных на эти адреса, как указано в параграфе 8.3.1). На активных маршрутизаторах настраиваются виртуальные адреса IPv4 или IPv6, а резервные маршрутизаторы (BR) определяют семейство виртуальных адресов для анонсирования на основе версии протокола IP. Внутри маршрутизатора VRRP виртуальные маршрутизаторы для каждого из семейств адресов IPv4 и IPv6 независимы один от другого и всегда считаются отдельными экземплярами VR. Процесс выбора обеспечивает динамический перенос ответственности пересылку, если AR становится недоступным.

VRRP обеспечивает функции, похожие на функции фирменных протоколов Hot Standby Router Protocol (HSRP) [RFC2281] IP Standby Protocol [IPSTB].

1.1. Отличия от RFC 5798

Ниже перечислены изменения, внесённые в [RFC5798].

1. Обновлена терминология VRRP в соответствии с рекомендациями по всеохватному языку для технологий IETF, в качестве которых выбран документ Национального института стандартов и технологий (National Institute of Standards and Technology или NIST) Guidance for NIST Staff on Using Inclusive Language in Documentary Standards [NISTIR8366].
2. Термин VRRP Router для маршрутизатора, принимающего на себя ответственность за пересылку пакетов, был заменён на Active Router в соответствии со всеохватывающей терминологией IETF. Кроме того, исправлены несоответствия терминов [RFC5798] Active Router и Backup Router, а также изменён нежелательный термин для привлечения и отбрасывания нежелательных пакетов.
3. Исправлены ошибки, относящиеся в конечному автомату, в разделе 6.
4. Уточнён расчёт контрольных сумм в параграфе 5.2.8 для точного указания включаемых частей для псевдозаголовка IPv4.
5. При получении анонса VRRP от маршрутизатора VRRP с меньшим приоритетом активный маршрутизатор VRRP незамедлительно отправляет анонс VRRP, чтобы мосты с обучением могли пересылать пакеты в корректный сегмент Ethernet (см. параграф 6.4.3).
6. Удалены приложения, описывающие работу с устаревшими технологиями (Fiber Distributed Data Interface (FDDI), Token Ring, ATM LAN Emulation).
7. Добавлены рекомендации, указывающие, что анонсы IPv6 Unsolicited Neighbor Advertisement следует воспринимать активным и резервным маршрутизаторам (параграф 8.2.4).
8. Рекомендуется проверять совпадение Maximum Advertisement Interval, хотя это не влияет на отбрасывание пакетов VRRP (параграф 7.1).
9. Внесены редакционные правки для улучшения читаемости.
10. Раздел «Взаимодействие с IANA» дополнен сведениями о выделении групповых адресов IPv4/IPv6 и MAC-адресов Ethernet.

1.2. Примечание по терминологии

В документе рассматриваются операции IPv4 и IPv6, для которых применительно к протоколу VRRP описания и процедуры совпадают. Было бы уместно использовать термин IP для обозначения IPv4 или IPv6, однако его часто относят только к IPv4. Поэтому в спецификации применяется обозначение IPvX (где X - 4 или 6) для обозначения обоих протоколов. Там, где версия IP имеет значение, указывается полный протокол, а термин IP не применяется.

1.3. IPv4

Имеется множество методов, с помощью которых конечный хост IPv4 может определить первый маршрутизатор (first-hop) на пути к целевому адресу IPv4. Они включают запуск (или отслеживание) протокола динамической маршрутизации, такого как Routing Information Protocol (RIP) [RFC2453] или OSPF версии 2 [RFC2328], запуск клиента обнаружения маршрутизаторов по ICMP [RFC1256], запуск DHCPv4 [RFC2131] или использование заданного статически маршрута по умолчанию.

Запуск протокола динамической маршрутизации на каждом конечном хосте может быть нецелесообразным по многим причинам, включая издержки администрирования и обработки, вопросы безопасности, отсутствие реализаций для конкретной платформы. Протоколы обнаружения соседей или маршрутизаторов могут требовать активного участия всех хостов сети, что потребует больших значений таймеров для снижения издержек протокола, связанных с обработкой пакетов протокола на каждом хосте. Это может приводить к существенным задержкам при обнаружении недоступности маршрутизатора, а такая задержка может приводить к неприемлемым периодам недоступности принятого по умолчанию маршрута.

Настройка принятого по умолчанию маршрута вручную (статическая или через DHCPv4) достаточно популярна, поскольку это минимизирует издержки настройки и обработки на конечных хостах и поддерживается практически всеми реализациями IPv4. Однако в этом случае возникает критически важная точка отказа. Потеря принятого по умолчанию маршрута ведёт к катастрофическим событиям, изолируя все конечные хосты, которые не смогут найти доступный альтернативный путь.

Протокол резервирования виртуального маршрутизатора (VRRP) разработан для устранения критической точки отказа, присущей сетям с использованием принятого по умолчанию маршрута. VRRP задаёт протокол выбора, который динамически назначает ответственность за VR одному из маршрутизаторов VRRP в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4, связанные с VR, называется активным маршрутизатором (AR) и пересылает пакеты, переданные по этим адресам IPv4. Процесс выбора обеспечивает динамическую передачу ответственности за пересылку, когда AR становится недоступным. Любой из адресов IPv4 виртуального маршрутизатора ЛВС можно использовать конечным хостам в качестве принятого по умолчанию первого маршрутизатора. Преимуществом применения VRRP является повышение доступности принятого по умолчанию пути без необходимости настройки протокола динамической маршрутизации или обнаружения маршрутизаторов на каждом конечном хосте.

1.4. IPv6

Хоты IPv6 в ЛВС обычно узнают о принятых по умолчанию маршрутизаторах из полученных анонсов Router Advertisement протокола обнаружения соседей IPv6 (Neighbor Discovery или ND) [RFC4861]. Групповые (multicast) анонсы Router Advertisement передаются периодически с такой скоростью, что хостам может потребоваться более 10 секунд, чтобы узнать о принятых по умолчанию маршрутизаторах в ЛВС. Анонсы передаются не настолько часто, чтобы полагаться на отсутствие Router Advertisement для обнаружения отказов маршрутизаторов.

Протокол ND включает механизм детектирования недоступности соседей (Neighbor Unreachability Detection) для обнаружения отказов соседних узлов (маршрутизаторов или хостов) или путей пересылки к соседям. Это выполняется путём отправки соседям индивидуальных сообщений ND Neighbor Solicitation. Для снижения издержек, связанных с этим сообщения Neighbor Solicitation передаются лишь соседям, которым узел активно отправляет трафик и лишь при

отсутствии положительной индикации активности маршрутизатора в течение некоторого времени. При использовании принятых по умолчанию параметров ND хосту может потребоваться более 10 секунд для обнаружения недоступности маршрутизатора, чтобы переключиться на другой маршрутизатор, заданный по умолчанию. Такая задержка заметна для пользователей и может приводить к тайм-аутам некоторых реализаций транспортных протоколов.

Хотя обнаружение недоступности соседа можно ускорить за счёт настройки таймеров (в настоящее время нижний предел составляет 5 секунд), это приведёт к росту издержек на трафик ND, особенно если все хосты будут пытаться определить доступность одного или нескольких маршрутизаторов.

Протокол VRRP для IPv6 обеспечивает более быстрое переключение на другой маршрутизатор, нежели стандартные процедуры ND. При использовании VRRP маршрутизатор BR может заменить принятый по умолчанию примерно за 3 секунды (с принятыми по умолчанию парамерами VRRP). Это происходит без взаимодействия с хостами и при минимальном трафике VRRP.

1.5. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

1.6. Область действия

Далее в документе рассматриваются свойства, цели разработки и теория операций VRRP. Представлены форматы сообщений, правила обработки и конечный автомат, гарантирующие сходимость к одному активному маршрутизатору (AR). В заключение рассматриваются вопросы, связанные с отображением MAC-адресов, обработкой сообщений ARP, генерацией сообщений ICMP о перенаправлении и соображения безопасности.

1.7. Определения

VRRP Router - маршрутизатор VRRP
: Маршрутизатор, на котором работает протокол VRRP. Он может участвовать в одном или нескольких VR.

Virtual Router - виртуальный маршрутизатор
: Абстрактный объект, управляемый VRRP и выступающий принятым по умолчанию маршрутизатором для хостов общей ЛВС. VR имеет идентификатор (Virtual Router Identifier) и набор связанных с ним адресов IPv4 или IPv6 из общей ЛВС. Маршрутизатор VRRP может служить резервным (Backup Router) для одного или нескольких VR.

Virtual Router Identifier - идентификатор виртуального маршрутизатора
: Целое число (1-255), указывающее экземпляр VR в ЛВС. Используется также аббревиатура VRID.

Virtual Router MAC Address - MAC-адрес виртуального маршрутизатора
: Групповой адрес Ethernet MAC, используемый в анонсах VRRP для VRID (см. параграф 7.3).

IP Address Owner - владелец адреса IP
: Маршрутизатор VRRP, имеющий адреса VR IPvX в качестве адресов реальных интерфейсов. Это маршрутизатор, который, будучи работающим, отвечает за пакеты, направленные по этим адресам IPvX, для ICMP, запросов соединений TCP и т. п.

Primary IP Address - первичный адрес IP
: В IPv4 - это адрес IPv4, выбранный из набора реальных адресов интерфейса. Одним из возможных алгоритмов является выбор первого адреса. В IPv4 анонсы VRRP всегда передаются с использованием первичного адреса IPv4 в поле отправителя пакета IPv4. В IPv6 применяется локальный для канала адрес (link-local) интерфейса, через который передаётся пакет.

Forwarding Responsibility - ответственность за пересылку
: Ответственность за пересылку пакетов, переданных по адресам IPvX, связанным с VR. Это включает восприятие пакетов, переданных по MAC-адресу VR, пересылку пакетов в соответствии с локальной базой маршрутной информации (Routing Information Base или RIB) и пересылки (Forwarding Information Base или FIB), ответы на запросы ARP для адресов IPv4 и на запросы ND для адресов IPv6.

Active Router - активный маршрутизатор
: Маршрутизатор VRRP, принимающий на себя ответственность за пересылку пакетов, переданных по адресам IPvX, связанным с VR, отклики на запросы ARP (для IPv4) и ND (для IPv6. Отметим, что при доступности владельца адреса IPvX он всегда будет AR.

Backup Router(s) - резервные маршрутизаторы
: Набор маршрутизаторов VRRP, доступных для принятия ответственности за VR в случае отказа текущего AR.

Drop Route - маршрут отбрасывания
: Маршрут в базе RIB, который будет приводить к отбрасыванию трафика, соответствующего ему.

2. Требуемые свойства

В этом разделе описаны свойства, которые считались обязательными при разработке VRRP.

2.1. Резервирование адресов IPvX

Резервирование адресов IPvX является основной функцией VRRP. При обеспечении выбора AR и описанных ниже дополнительных функций протоколу следует стремиться:

- минимизировать продолжительность недоступности;
- минимизировать расход пропускной способности в установившемся режиме и сложность обработки;
- работать с широким спектром технологий ЛВС с множественным доступом, способных поддерживать IPvX;
- разрешать несколько VR в сети для распределения нагрузки;
- поддерживать множество логических подсетей IPvX в одном сегменте ЛВС.

2.2. Указание предпочтительного пути

Простая модель выбора AR из набора избыточных маршрутизаторов заключается в предоставлении всем маршрутизаторам одинаковых предпочтений и выборе того маршрутизатора, который стал в конечном итоге активным. Вероятно имеется много сред, где избыточные маршрутизаторы будут иметь разные предпочтения (или диапазоны предпочтений). Например, предпочтения могут основываться на стоимости или скорости каналов, производительности или надёжности маршрутизаторов, а также соображениях политики. Протоколу следует разрешать указание относительного уровня предпочтений в интуитивно понятной форме и гарантировать сходимость выбора AR к наиболее предпочтительному из доступных маршрутизаторов VR.

2.3. Минимизация прерывания обслуживания

После выбора AR любое ненужное переключение на BR может приводить к прерыванию обслуживания. Протоколу следует гарантировать, что после выбора AR не будет переключения на какой-либо BR с тем же или меньшим предпочтением, пока текущий маршрутизатор AR обеспечивает корректную работу.

В некоторых средах может быть предпочтительным даже переключение на резервный маршрутизатор, который предпочтительней текущего AR и может оказаться полезным предотвращение незамедлительного восстановления наиболее предпочтительного пути.

2.4. Эффективная работа в расширенных ЛВС

Передача пакетов IPvX (IPv4 или IPv6) в ЛВС с множественным доступом требует сопоставления адресов IPvX с адресами MAC. Использование MAC-адреса VR в расширенной ЛВС с обучающимися мостами может существенно влиять на издержки пропускной способности для пакетов, передаваемых виртуальному маршрутизатору. Если MAC-адрес VR не применяется как адрес отправителя в кадрах канального уровня, местоположение этого MAC-адреса не будет определено, что приведёт к лавинной передаче всех пакетов, отправленных маршрутизатору VR. Для повышения эффективности в таких средах протоколу следует:

1. использовать MAC-адрес VR в поле отправителя пакетов от маршрутизатора AR для изучения MAC;
2. выдавать сообщение срезу после переключения AR для обновления MAC-адресов;
3. периодически передавать сообщения от AR для поддержки кэша MAC-адресов.

2.5. Субсекундные операции для IPv4 и IPv6

Для сред IPv4 и IPv6 требуется обнаружение отказа AR за доли секунды. В предыдущих работах были предложены субсекундные операции для IPv6, а данная спецификация использует этот подход для IPv4 и IPv6.

Одной из возможных проблемных ситуаций при использовании малых значений Advertisement_Interval (см. параграф 6.1) является генерация маршрутизатором VRRP большего числа пакетов, нежели он способен передать, и рост очереди на этом маршрутизаторе. В таких случаях пакеты для передачи в защищаемую VRRP ЛВС могут задерживаться в очереди на время, превышающее наименьшее значение Advertisement_Interval. При этом интервал Active_Down_Interval (см. параграф 6.1) может быть настолько малым, что даже обычные задержки в очереди могут заставить резервный маршрутизатор сделать вывод об отказе AR и предложить себя в качестве нового AR. Вскоре после этого задержанные пакеты от исходного AR заставят маршрутизатор VRRP снова переключиться на BR и это может происходить много раз в секунду, вызывая значительные перебои в трафике. Для смягчения этой проблемы следует рассмотреть возможность предоставления пакетам VRRP приоритета на выходном интерфейсе. Если AR замечает такую ситуацию, ему **следует** указать это в системном журнале (с учётом ограничения частоты записей).

3. Обзор VRRP

VRRP задаёт протокол выбора для обеспечения функций VR, описанных выше. Обмен сообщениями протокола выполняется с помощью групповых дейтаграмм IPv4 или IPv6, поэтому протокол может работать в разных ЛВС с множественным доступом, поддерживающих групповую адресацию IPvX. С каждым каналом виртуального маршрутизатора VRRP связан 1 общеизвестный MAC-адрес. Этот документ в задаёт детали отображения лишь для сетей, использующих 48-битовые адреса MACIEEE 802. MAC-адрес VR указывается в поле отправителя всех периодических сообщений VRRP, передаваемых AR, чтобы стало возможным изучение MAC на канальном уровне (L2) мостами расширенных ЛВС.

VR указывается идентификатором VRID и набором адресов IPv4 или IPv6. Маршрутизатор VRRP может связывать VR с реальным адресом на своём интерфейсе. Область действия каждого VR ограничивается одной ЛВС. На маршрутизаторе VRRP могут настраиваться дополнительные отображения VR и приоритеты для VR, которые маршрутизатор готов реализовать. Сопоставление VRID с адресами IPvX должно быть настраиваемым для всех маршрутизаторов VRRP в ЛВС.

Не задаётся ограничений на многократное использование VRID с другими сопоставлениями адресов в разных ЛВС и применение одного VRID для набора адресов IPv4 и IPv6. Однако это будут разные маршрутизаторы VR.

Для минимизации трафика периодические сообщения VRRP Advertisement для каждого VR передаёт лишь AR. Маршрутизатор BR не пытается вытеснить AR, пока у него нет более высокого приоритета. Это исключает перебои в обслуживании, пока не появится более предпочтительный путь. Можно также административно запретить попытки вытеснение AR. Единственным исключением является то, что маршрутизатор VRRP всегда будет становиться AR для любого VR, связанного с адресом, которым он владеет. Если AR становится недоступным, BR с наивысшим приоритетом становится AR с небольшой задержкой, обеспечивая контролируемую передачу ответственности за VR с минимальным прерыванием обслуживания.

Протокол VRRP обеспечивает быстрый переход BR в состояние AR для минимизации перебоев в обслуживании и включает оптимизацию, снижающую сложность протокола в сочетании с гарантиями контролируемого перехода в состояние AR для типичных рабочих ситуаций. Эта оптимизация обеспечивает протокол выбора с минимальными требованиями к рабочим состояниям, минимальным набором активных состояний протокола и одним типом сообщений и отправителем. Определены типовые рабочие сценарии с двумя резервными маршрутизаторами и/или разными

предпочтениями путей для каждого маршрутизатора. Побочным эффектом несоблюдения этих допущений, т. е. наличия более двух резервных путей с одинаковым предпочтением, является кратковременная пересылка дубликатов пакетов в течение короткого периода выбора AR. Однако допущение типичных сценариев, вероятно, верно для большинства ситуаций - потеря AR случается достаточно редко, а ожидаемая продолжительность процесса выбора AR достаточно мала (< 4 секунд для принятого по умолчанию Advertisement_Interval с возможностью снижения до значений < 1/25 секунды). Таким образом, оптимизация VRRP значительно упрощает устройство протокола при сохранении невысокой вероятности кратковременных нарушений работы.

4. Примеры сетей VRRP

4.1. Пример 1

На рисунке 1 показана простая сеть с двумя маршрутизаторами VRRP, реализующими один VR.

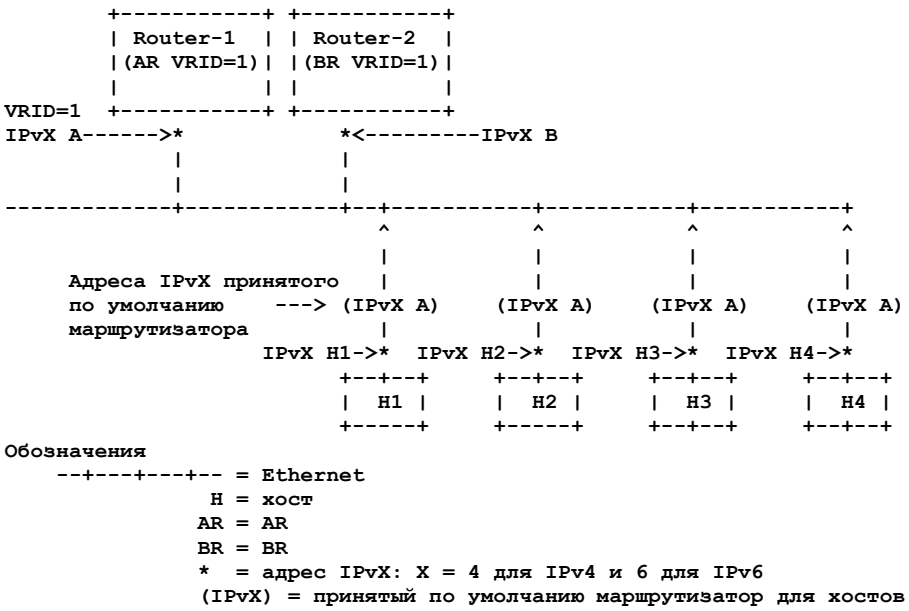

Рисунок 1. Пример сети VRRP.

В случае IPv4 (IPvX на рисунке обозначает IPv4) на каждом маршрутизаторе заранее назначается адрес IPv4 на интерфейсе ЛВС (на Router-1 это IPv4 A, на Router-2 - IPv4 B), а на каждом хосте устанавливается принятый по умолчанию маршрут (по протоколу DHCPv4 или настройку статического маршрута) через один из маршрутизаторов (на рисунке все хосты используют адрес IPv4 A). В случае IPv6 (IPvX на рисунке обозначает IPv6) каждый маршрутизатор имеет свой адрес IPv6 link-local на интерфейсе ЛВС и адрес IPv6 link-local для VRID, который является общим для всех маршрутизаторов с одним VRID. Каждый хост узнаёт принятый по умолчанию маршрут из сообщений Router Advertisement от одного из этих маршрутизаторов (на рисунке все хосты используют IPv6 Link-Local A).

В среде VRRP IPv4 каждый маршрутизатор поддерживает приём и передачу для одного и того же адреса IPv4. Router-1 является владельцем IPv4 A, а Router-2 - IPv4 B. VR определяется привязкой уникального идентификатора VRID к адресу, принадлежащему Router-1. В среде VRRP IPv6 каждый маршрутизатор поддерживает приём и передачу для адресов IPv6, связанных с VRID. Router-1 является владельцем IPv6 A, а Router-2 - IPv6 B. VR определяется привязкой уникального идентификатора VRID к адресу, принадлежащему Router-1. В обоих случаях (IPv4 и IPv6) протокол VRRP обеспечивает переключения VR при отказе на BR.

В примере показан VR, настроенный на охват адреса IPvX, принадлежащего Router-1 (VRID=1, IPvX_Address=A). При включении VRRP на Router-1 для VRID=1 этот маршрутизатор будет заявлять себя как AR с priority = 255, поскольку он владеет адресом IPvX для VR. При включении VRRP на Router-2 для VRID=1 этот маршрутизатор будет заявлять себя как BR с priority = 100 (принятое по умолчанию значение), поскольку он не является владельцем адреса IPvX. При отказе Router-1 протокол VRRP переведёт Router-2 в состояние AR, временно передав ему ответственность за пересылку IPvX A для обеспечения бесперебойного обслуживания хостов.

Отметим, что для обоих случаев на рисунке IPvX B не резервируется и используется только маршрутизатором Router-2 в качестве адреса на интерфейсе. Для резервирования IPvX B требуется настроить второй VR, как показано ниже.

4.2. Пример 2

На рисунке 2 показана конфигурация с двумя VR, между которыми хосты распределяют трафик.

В примере для IPv4 (IPvX на рисунке обозначает адрес IPv4) половина хостов настраивается со статическим маршрутом по умолчанию через IPv4 A (Router-1), остальные используют IPv4 B (Router-2). Настройка VR с VRID=1 совпадает с предыдущим примером (параграф 4.1), а второй VR добавлен для охвата адреса IPv4, принадлежащего Router-2 (VRID=2, IPv4_Address=B). В этом случае Router-2 будет заявлять себя как AR для VRID=2, а Router-1 будет служить BR. Это демонстрирует развёртывание с распределением нагрузки при доступности обоих маршрутизаторов с обеспечением полного резервирования для отказоустойчивости.

В примере для IPv6 (IPvX на рисунке обозначает адрес IPv6) половина хостов настраивается с маршрутом по умолчанию через IPv6 A (Router-1), остальные используют IPv6 B(Router-2). Настройка VR с VRID=1 совпадает с предыдущим примером (параграф 4.1), а второй VR добавлен для охвата адреса IPv6, принадлежащего Router-2 (VRID=2, IPv6_Address=B). В этом случае Router-2 будет заявлять себя как AR для VRID=2, а Router-1 будет служить BR. Это демонстрирует развёртывание с распределением нагрузки при доступности обоих маршрутизаторов с обеспечением полного резервирования для отказоустойчивости.

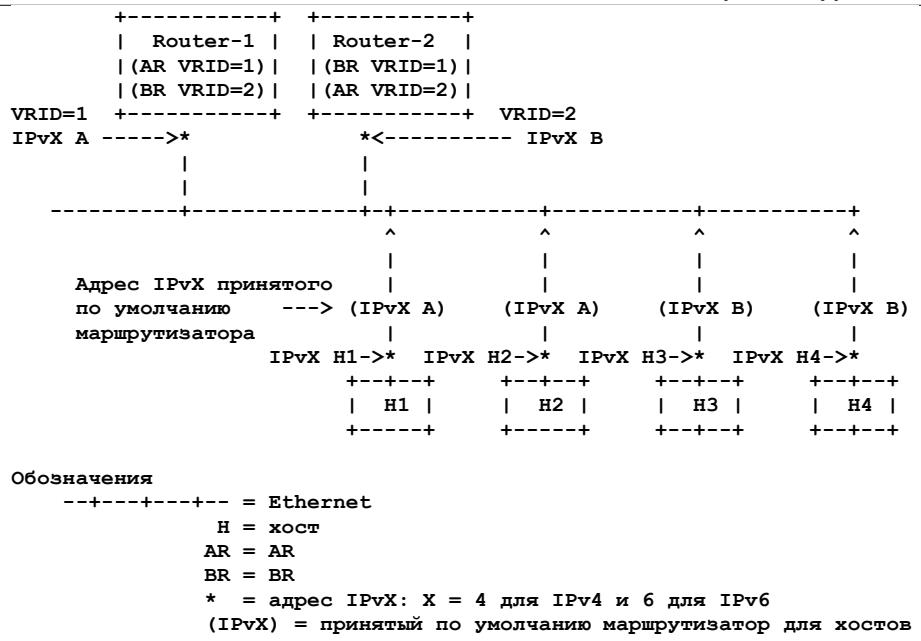

Рисунок 2. Пример сети VRRP.

Отметим, что детали распределения нагрузки выходят за рамки этого документа. Если серверам нужны различные веса, полагаться на сообщения Router Advertisement для распределения трафика между маршрутизаторами может быть бессмысленно [RFC4311].

5. Протокол

Назначением VRRP Advertisement является передача всем маршрутизаторам VRRP значения Maximum Advertisement Interval и адреса IPvX маршрутизатора AR, связанного с VRID.

Когда VRRP служит для защиты адреса IPv4, пакеты VRRP инкапсулируются в пакеты IPv4, которые передаются по групповому адресу IPv4, назначенному VRRP. При использовании VRRP для защиты адреса IPv6 пакеты VRRP инкапсулируются в пакеты IPv6, которые передаются по групповому адресу IPv6, назначенному VRRP.

5.1. Формат пакетов VRRP

В этом параграфе описан формат пакетов VRRP и соответствующих полей заголовков IPvX (с учётом семейства).

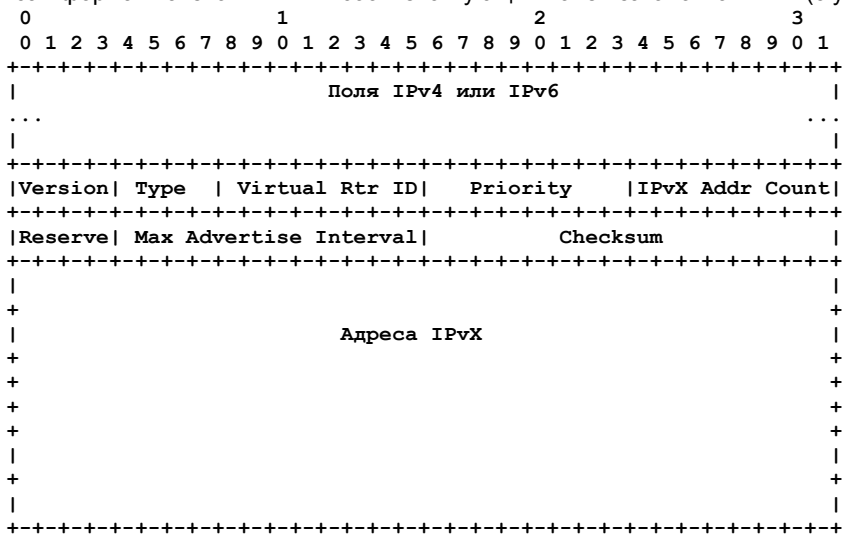

Рисунок 3. Формат пакетов IPv4/IPv6 VRRP Advertisement.

5.1.1. Описание полей IPv4

5.1.1.1. Source Address

Первичный адрес IPv4 на интерфейсе, с которого передаётся пакет.

5.1.1.2. Destination Address

Групповой адрес IPv4, назначенный IANA для протокола VRRP (224.0.0.18). Это групповой адрес, действующий на локальном канале. Маршрутизаторам **недопустимо** пересылать такие дейтаграммы независимо от значения TTL.

5.1.1.3. TTL

Должно иметь значение 255. Маршрутизатор VRRP **должен** отбрасывать пакеты с иным значением [RFC5082].

5.1.1.4. Protocol

Номер протокола IPv4, выделенный IANA для VRRP (десятичное значение 112).

5.1.2. Описание полей IPv6

5.1.2.1. Source Address
Адрес IPv6 link-local на интерфейсе, с которого передаётся пакет.

5.1.2.2. Destination Address
Групповой адрес IPv6, назначенный IANA для протокола VRRP (ff02:0:0:0:0:0:0:12). Это групповой адрес, действующий на локальном канале. Маршрутизаторам **недопустимо** пересылать такие дейтаграммы при любом значении Hop Limit.

5.1.2.3. Hop Limit
Должно иметь значение 255. Маршрутизатор VRRP **должен** отбрасывать пакеты с иным значением [RFC5082].

5.1.2.4. Next Header
Протокол IPv6 Next Header, выделенный IANA для VRRP (десятичное значение 112).

5.2. Описание полей VRRP

5.2.1. Version
Версия протокола VRRP для этого пакета. Этот документ задаёт версию 3.

5.2.2. Type
Указывает тип пакета VRRP. В этой версии протокола определён лишь один тип:

1
ADVERTISEMENT (анонс).

Пакеты неизвестного типа **должны** отбрасываться.

5.2.3. Virtual Rtr ID (VRID)
Поле Virtual Rtr ID указывает VR, для которого пакет указывает состояние.

5.2.4. Priority
8-битовое целое число без знака, указывающее приоритет передающего маршрутизатора VRRP для VR. Большие значения указывают более высокий приоритет. Для маршрутизатора VRRP, владеющего адресом IPvX, связанным с VR, поле **должно** иметь значение 255 (десятичное).

Маршрутизаторы VRRP, резервирующие VR, **должны** использовать для приоритета десятичные значения 1-254. По умолчанию для маршрутизаторов VRRP, резервирующих VR, используется десятичное значение 100. Рекомендации по выбору приоритета приведены в параграфе 8.3.2. Значение приоритета 0 указывает, что текущий AR прекратил своё участие в VRRP. Это служит для того, чтобы маршрутизаторы BR приступали к выбору AR, не ожидая завершения текущего Active_Down_Interval (см. параграф 6.1).

5.2.5. IPvX Addr Count
Поле IPvX Addr Count указывает число адресов (IPv4 или IPv6) в анонсе VRRP и должно иметь значение не меньше 1. Анонсы VRRP со значением 0 **должны** игнорироваться.

5.2.6. Reserve
В поле Reserve **должно** устанавливаться значение 0, а при получении поле игнорируется.

5.2.7. Max Advertise Interval
12-битовое поле, указывающее интервал между анонсами в сотых долях секунды (по умолчанию 100 - 1 секунда).

Отметим, что высокоприоритетные AR с более низкой скоростью, чем у их BR, будут нестабильны, поскольку BR с низким приоритетом и более высокой скоростью могут присоединиться к ЛВС и решить, что им следует быть AR до получения сигнала от медленного AR с высоким приоритетом. Это временное явление и после получения узлом с низким приоритетом сообщения от высокоприоритетного AR он откажется от своего статуса AR.

5.2.8. Checksum
Поле контрольной суммы служит для обнаружения повреждений данных в сообщениях VRRP. Для семейств адресов IPv4 и IPv6 контрольная сумма представляет собой 16-битовое дополнение до 1 суммы дополнений до 1 для сообщения VRRP. При расчёте контрольной суммы значение поля Checksum принимается равным 0. Детали расчёта контрольных сумм описаны в [RFC1071].

Для адресов IPv4 при расчёте контрольной суммы используются поля сообщения VRRP, начиная с поля Version и заканчивая последним адресом IPv4 (см. параграф 5.2). Для адресов IPv6 в расчёт контрольной суммы включается также добавленный в начало псевдозаголовок, определённый в параграфе 8.1 [RFC8200]. В поле Next Header псевдозаголовка для протокола VRRP следует устанавливать десятичное значение 112.

5.2.9. Адреса IPvX
Эти поля относятся к одному или нескольким адресам IPvX, связанным с VR. Число адресов указывается в поле IPvX Addr Count. Поля применяются для поиска и устранения неполадок в настройках маршрутизаторов. При отправке более одного адреса рекомендуется настраивать на всех маршрутизаторах передачу адресов в одном порядке, чтобы упростить сравнение.

Для IPv4 эти поля содержат один или несколько адресов IPv4, резервируемых маршрутизатором VR.

Для IPv6 первым **должен** указываться адрес IPv6 link-local, связанный с VR.

Эти поля содержат 1 или несколько адресов IPv4 или IPv6. Семейство (IPv4 или IPv6, но не сочетание) **должно** совпадать с семейством адреса в заголовке IPvX пакета VRRP.

6. Конечный автомат протокола

6.1. Параметры виртуального маршрутизатора

VRID

Идентификатор VR - настраиваемое десятичное значение от 1 до 255. Значение по умолчанию отсутствует.

Priority

Значение приоритета, используемое маршрутизатором VRRP при выборе AR для данного VR. Десятичное значение 255 зарезервировано для маршрутизатора, владеющего адресом IPvX, связанным с VR, значение 0 зарезервировано для AR с целью указания снятия ответственности за VR. Десятичные значения 1-254 доступны для маршрутизаторов VRRP, резервирующих VR. Большее значение указывает более высокий приоритет. По умолчанию используется десятичное значение 100.

IPv4_Addresses

Один или несколько адрес IPv4, связанный с VR. Настраиваемый список адресов без значения по умолчанию.

IPv6_Addresses

Один или несколько адрес IPv6, связанный с VR. Настраиваемый список адресов без значения по умолчанию. Первым в списке **должен** быть адрес Link-Local, связанный с VR.

IPvX_Addresses

Адрес IPv4 или IPv6, связанный с этим VR (см. выше IPv4_Addresses и IPv6_Addresses).

Advertisement_Interval

Интервал времени между анонсами VRRP Advertisement, передаваемых эти VR (в сотых долях секунды). По умолчанию установлено значение 100 (1 секунда).

Active_Adver_Interval

Интервал анонсирования, содержащийся в VRRP Advertisement, полученных от AR (в сотых долях секунды). Это значение сохраняется маршрутизаторами VR в состоянии Backup и применяется для расчёта Skew_Time (см. параграф 8.3.2) и Active_Down_Interval. Исходное значение совпадает с Advertisement_Interval.

Skew_Time

Время для изменения Active_Down_Interval в сотых долях секунды. Рассчитывается по формуле (((256 - Priority) * Active_Adver_Interval) / 256).

Active_Down_Interval

Интервал времени, по истечение которого BR объявляет AR отказавшим в сотых долях секунды. Рассчитывается по формуле (3 * Active_Adver_Interval) + Skew_Time.

Preempt_Mode

Указывает, будет ли BR с более высоким приоритетом (при запуске или перезапуске) вытеснять AR с низким приоритетом. Значение True (принято по умолчанию) разрешает вытеснение, False - запрещает.

Примечание. Маршрутизатор, владеющий адресом IPvX, связанным с VR использует вытеснение всегда, независимо от установки этого флага.

Accept_Mode

Указывает, будет ли VR в состоянии Active воспринимать пакеты, направленные владельцу адреса IPvX, как свои, даже если они ему не принадлежат. По умолчанию установлено значение False. Системы, полагающиеся, например, на ping IPvX-адреса владельца, могут пожелать установить Accept_Mode = True.

Примечание. Сообщения IPv6 Neighbor Solicitation и Neighbor Advertisement **недопустимо** отбрасывать при Accept_Mode = False.

Virtual_Router_MAC_Address

MAC-адрес, используемый в поле MAC отправителя анонсов VRRP и анонсируемый в сообщениях ARP/ND как MAC-адрес для использования в IPvX_Addresses.

6.2. Таймеры

Active_Down_Timer

Таймер, срабатывающий при отсутствии VRRP Advertisement в течение Active_Down_Interval (только BR).

Adver_Timer

Таймер для запуска передачи VRRP Advertisement по времени Advertisement_Interval (только AR).

6.3. Диаграмма смены состояний

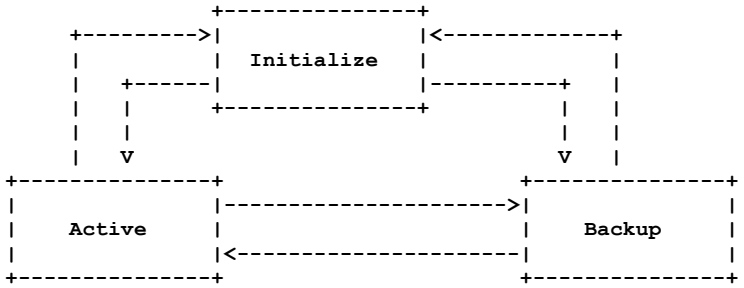

Рисунок 4. Диаграмма смены состояний.

6.4. Описания состояний

В описаниях ниже имена состояний указываются как {state-name}, а пакеты - заглавными буквами.

Маршрутизатор VRRP реализует экземпляр конечного автомата для каждого VR, в котором он участвует.

6.4.1. Initialize

Это состояние предназначено для ожидания события Startup, т. е. зависящего от реализации механизма инициализации протокола после его настройки. Этот механизм выходит за рамки спецификации.

По событию Startup выполняются указанные ниже действия.

- Если Priority = 255, т. е. маршрутизатор владеет адресами IPvX, связанными с VR:
  - передаётся сообщение ADVERTISEMENT;
  - если защищаемый адрес IPvX является IPv4:
    - для каждого адреса IPv4, связанного с VR, передаётся широковещательное беспричинное сообщение ARP с IPv4-адресом[1] VR и MAC-адресом VR в качестве целевого адреса канального уровня;
  - иначе // IPv6
    - для каждого адреса IPv6, связанного с VR, передаётся незапрошенный анонс ND Neighbor Advertisement с установленным флагом Router Flag (R), сброшенным флагом Solicited Flag (S), установленным флагом Override flag (O), целевым адресом IPv6 для VR и MAC-адресом VR в качестве целевого адреса канального уровня;
  - завершение проверки семейства адресов;
  - для Adver_Timer устанавливается значение Advertisement_Interval;
  - состояние меняется на {Active};
- иначе // маршрутизатор не является владельцем адреса
  - для Active_Adver_Interval устанавливается значение Advertisement_Interval;
  - для Active_Down_Timer устанавливается значение Active_Down_Interval;
  - состояние меняется на {Backup};
- завершение проверки условия Priority = 255.

На этом обработка события Startup завершается.

6.4.2. Backup

Состояние {Backup} предназначено для отслеживания доступности и статуса AR. В приведённом ниже описании применяется групповой адрес Solicited-Node [RFC4291].

Находясь в состоянии {Backup} маршрутизатор VRRP **должен** выполнять указанные ниже действия.

- Если защищаемый адрес IPvX является IPv4:
  - маршрутизатору **недопустимо** отвечать на запросы ARP, для адресов IPv4 маршрутизатора VR;
- иначе // защищаемый адрес относится к IPv6
  - маршрутизатору **недопустимо** отвечать на сообщения ND Neighbor Solicitation для адресов IPv6, связанных с VR;
  - маршрутизатору **недопустимо** передавать сообщения ND Router Advertisement для VR;
- завершение проверки принадлежности защищаемого адреса к IPv4;
- маршрутизатор **должен** отбрасывать пакеты с MAC-адресом получателя, совпадающим с MAC-адресом VR;
- маршрутизатору **недопустимо** воспринимать пакеты, направленные по адресам IPvX, связанным с VR;
- по событию Shutdown:
  - отключается таймер Active_Down_Timer;
  - состояние меняется на {Initialize};
- завершение обработки события Shutdown;
- по срабатыванию таймера Active_Down_Timer:
  - передаётся сообщение ADVERTISEMENT;
- если защищаемый адрес IPvX является IPv4:
  - для каждого адреса IPv4, связанного с VR передаётся широковещательное беспричинное сообщение ARP, содержащее IPv4-адрес[1] VR и MAC-адрес VR в качестве целевого адреса канального уровня;
  - иначе // IPv6
    - рассчитывается присоединяется групповой адрес Solicited-Node [RFC4291] для адресов IPv6, связанных с VR;
    - для каждого адреса IPv6, связанного с VR, передаётся незапрошенный анонс ND Neighbor Advertisement с установленным флагом Router Flag (R), сброшенным флагом Solicited Flag (S), установленным флагом Override flag (O), целевым адресом IPv6 для VR и MAC-адресом VR в качестве целевого адреса канального уровня;

[1] В оригинале ошибочно указан MAC-адрес, см. https://www.rfc-editor.org/errata/eid7947. *Прим. перев.*

- завершение проверки принадлежности защищаемого адреса к IPv4;
- для Adver_Timer устанавливается значение Advertisement_Interval;
- состояние меняется на {Active};

- завершение обработки по таймеру Active_Down_Timer;
- при получении сообщения ADVERTISEMENT:
  - если Priority в ADVERTISEMENT имеет ненулевое значение:
    - для Active_Down_Timer устанавливается значение Skew_Time;
  - завершение обработки ненулевого приоритета;
    - если Preempt_Mode = False или Priority в ADVERTISEMENT не меньше локального Priority:
      - для Active_Adver_Interval устанавливается значение Max Advertise Interval из ADVERTISEMENT;
      - заново рассчитывается Skew_Time;
      - заново рассчитывается Active_Down_Interval;
      - для Active_Down_Timer устанавливается значение Active_Down_Interval;
    - иначе // вытеснение было разрешено, а приоритет в анонсе меньше локального;
      - ADVERTISEMENT отбрасывается;
    - завершение проверки возможности вытеснения;
  - завершение обработки нулевого приоритета;
- завершение проверки получения анонса.

На этом обработка в состоянии {Backup} завершается.

6.4.3. Active

В состоянии {Active} маршрутизатор выполняет пересылку для адресов IPvX, связанных с VR. Флаг Preempt_Mode Flag в режиме {Active} не принимается во внимание.

В состоянии {Active} маршрутизатор VRRP **должен** выполнять указанные ниже действия.

- Если защищаемый адрес IPvX относится к IPv4:
  - маршрутизатор **должен** отвечать на запросы ARP для адресов IPv4, связанных с VR;
- иначе // IPv6
  - маршрутизатор **должен** быть членом группы Solicited-Node для адресов IPv6, связанных с VR;
  - маршрутизатор **должен** отвечать на сообщения ND Neighbor Solicitation (с установленным флагом Router Flag (R)) для адресов IPv6, связанных с VR;
  - маршрутизатор **должен** передавать сообщения ND Router Advertisement для VR;
  - если Accept_Mode = False:
    - маршрутизатору **недопустимо** отбрасывать IPv6 Neighbor Solicitation и Neighbor Advertisement;
- завершение проверки семейства адресов;
- маршрутизатор **должен** пересылать пакеты с MAC-адресом получателя, совпадающим с MAC-адресом VR;
- маршрутизатор **должен** воспринимать пакеты, направленные по адресам IPvX, связанным с VR, если он владеет этим адресом IPvX или Accept_Mode = True, в иных случаях воспринимать пакеты **недопустимо**;
- по событию Shutdown:
  - выключается таймер Adver_Timer;
  - передаётся ADVERTISEMENT с Priority = 0;
  - состояние меняется на {Initialize};
- завершение обработки Shutdown;
- по таймеру Adver_Timer:
  - передаётся ADVERTISEMENT;
  - для Adver_Timer устанавливается значение Advertisement_Interval;
- завершение обработки по таймеру анонсов;
- при получении сообщения ADVERTISEMENT:
  - если поле Priority в ADVERTISEMENT имеет значение 0:
    - передаётся ADVERTISEMENT;
    - для Adver_Timer устанавливается значение Advertisement_Interval;
  - иначе // приоритет отличен от 0;

- если Priority в ADVERTISEMENT больше локального Priority или приоритеты совпадают и первичный адрес IPvX отправителя больше локального первичного адреса IPvX (сравнение как целых чисел без знака с сетевым порядком байтов):
  - выключается таймер Adver_Timer;
  - для Active_Adver_Interval устанавливается значение Max Advertise Interval из ADVERTISEMENT;
  - заново рассчитывается Skew_Time;
  - заново рассчитывается Active_Down_Interval;
  - для Active_Down_Timer устанавливается значение Active_Down_Interval;
  - состояние меняется на {Backup};
- иначе // логика нового AR
  - ADVERTISEMENT отбрасывается;
  - незамедлительно передаётся ADVERTISEMENT для подтверждения статуса {Active} передавшему анонс маршрутизатору VRRP и обновления обучающихся мостов указанием корректного пути к активному маршрутизатору VRRP;
- завершение обработки при обнаружении нового AR;

- завершение обработки по приоритету;

- завершение обработки полученного анонса.

На этом работа в состоянии {Active} завершается.

Примечание. Пакеты VRRP передаются с MAC-адресом VR в поле отправителя, чтобы обеспечить обучающимся мостам корректное определение сегмента ЛВС, к которому подключён VR.

7. Передача и приём пакетов VRRP

7.1. Приём пакетов VRRP

При получении пакета VRRP должны выполняться указанные ниже действия.

- Если получен пакет IPv4:
  - **должно** проверяться наличие значения 255 в поле IPv4 TTL;
- иначе // получен пакет VRRP IPv6;
  - **должно** проверяться наличие значения 255 в поле IPv6 Hop Limit;
- завершение обработки по семейству адресов;
- **должен** проверяться номер версии VRRP (3);
- **должно** проверяться значение типа пакета VRRP (1 - ADVERTISEMENT);
- **должна** проверяться полнота полученного пакета VRRP (включая фиксированные поля и адрес IPvX);
- **должна** проверяться контрольная сумма VRRP;
- **должна** выполняться проверка настройки VRID на принявшем пакет интерфейсе и того, что локальный маршрутизатор не является владельцем адреса IPvX (Priority = 255).

При отрицательном результате любой из этих проверок получатель **должен** отбросить пакет, **следует** внести запись об этом в системный журнал (с учётом ограничения частоты записей) и **можно** указать ошибку через систему управления.

Получателю **следует** проверять, что Max Advertise Interval в принятом пакете VRRP совпадает со значением Advertisement_Interval настроенным для VRID, поскольку при различии интервалов может возникать нестабильность (см. параграф 5.2.7). При отрицательном результате проверки **следует** внести запись об этом в системный журнал (с учётом ограничения частоты записей) и **можно** указать некорректность настройки через систему управления.

Получатель **может** проверить соответствие IPvX Addr Count и списка адресов IPvX настроенным для VRID адресам IPvX. При отрицательном результате проверки **следует** внести запись об этом в системный журнал (с учётом ограничения частоты записей) и **можно** указать некорректность настройки через систему управления.

7.2. Передача пакетов VRRP

При передаче пакета VRRP **должны** выполняться указанные ниже действия.

- Заполнение полей пакета VRRP в соответствии с состоянием конфигурации VR.
- Расчёт контрольной суммы VRRP.
- Установка в поле MAC-адреса отправителя значения MAC-адреса VR.
- Если защищаемым адресом является IPv4,
  - установка в поле адреса отправителя IPv4 первичного адреса IPv4 на интерфейсе
- иначе // IPv6
  - установка в поле адреса отправителя IPv6 адреса IPv6 link-local для интерфейса

- завершение обработки по семействам адресов;
- установка для протокола IPvX значения VRRP;
- передача пакета VRRP в группу IPvX VRRP.

Примечание. Пакеты VRRP передаются с MAC-адресом VR в поле MAC отправителя, чтобы обучающиеся мосты могли корректно определить сегмент ЛВС, к которому подключён VR.

7.3. MAC-адрес VR

MAC-адрес, связанный с Virtual является адресом IEEE 802 MAC [RFC9542] в формате

```
IPv4: 00-00-5E-00-01-{VRID} (шестнадцатеричное с сетевым порядком байтов)
```

Три первых октета взяты из уникального идентификатора IANA (Organizationally Unique Identifier или OUI), следующие 2 (00-01) указывают блок адресов, выделенных VRRP для протокола IPv4. {VRID} - это идентификатор VR. Этот формат позволяет иметь в ЛВС до 255 маршрутизаторов IPv4 VRRP.

```
IPv6: 00-00-5E-00-02-{VRID} (шестнадцатеричное с сетевым порядком байтов)
```

Три первых октета взяты из IANA OUI, следующие 2 (00-01) указывают блок адресов, выделенных VRRP для протокола IPv6. {VRID} - это идентификатор VR. Формат позволяет иметь в ЛВС до 255 маршрутизаторов IPv6 VRRP.

7.4. Идентификаторы интерфейсов IPv6

В [RFC8064] указано, что [RFC7217] применяется в качестве принятой по умолчанию схемы создания стабильных адресов при автоматической настройке IPv6 без поддержки состояний (Stateless Address Autoconfiguration или SLAAC) [RFC4862]. MAC-адрес VR **недопустимо** применять для параметра Net_Iface в алгоритмах создания идентификаторов интерфейсов (Interface Identifier или IID) [RFC7217] и [RFC8981].

Эта спецификация VRRP описывает, как анонсируется и преобразуется адрес IPv6 link-local маршрутизатора VRRP и связанные с ним адреса IPv6 в MAC-адрес VR.

8. Вопросы эксплуатации

8.1. IPv4

8.1.1. ICMP Redirect

Перенаправление ICMP можно использовать при работе VRRP между группой маршрутизаторов, что позволяет принять VRRP в средах с несимметричной топологией.

Адресу отправителя IPv4 в перенаправлении ICMP следует быть адресом, который конечный хост использовал при принятии решения о следующем маршрутизаторе (next-hop). Если маршрутизатор VRRP является AR для VR, содержащих адреса, которыми он не владеет, при выборе адреса источника перенаправления этот маршрутизатор должен определить, какому из VR был направлен пакет. Одним из методов определения VR является изучение MAC-адреса получателя в пакете, вызвавшем перенаправление.

При использовании VRRP для распределения нагрузки между маршрутизаторами в симметричной топологии может быть полезно отключение перенаправлений.

8.1.2. Запросы ARP от хостов

Когда хост передаёт запрос ARP для обного из адресов IPv4 маршрутизатора VR, маршрутизатор AR **должен** отвечать сообщением ARP, указывающим MAC-адрес VR. Отметим, что адресом отправителя в кадре Ethernet с откликом ARP является физический MAC-адрес физического маршрутизатора. Маршрутизатору AR **недопустимо** указывать свой физический MAC-адрес в отклике ARP. Это позволяет хостам всегда использовать один MAC-адрес, независимый от текущего AR.

При загрузке или перезагрузке маршрутизатора VRRP ему **не следует** передавать каких-либо сообщений ARP, использующих его физический MAC-адрес для адреса IPv4, которым он владеет (в соответствии с параграфом 1.7), и следует передавать лишь сообщения ARP с MAC-адресом VR. Это означает соблюдение указанных ниже условий.

- При настройке интерфейса маршрутизаторам AR **следует** широковещательно передавать беспричинное сообщение ARP с MAC-адресом VR для каждого адреса IPv4 на этом интерфейсе.
- При инициализации интерфейсов для операций VRRP в процессе загрузки системы беспричинные сообщения ARP **должны** задерживаться до момента установки адреса IPv4 и MAC-адреса VR.
- При доступе к конкретному маршрутизатору VRRP, например, с помощью Secure Shell (SSH), **следует** использовать адрес IPv4, заведомо принадлежащий этому маршрутизатору.

8.1.3. Proxy ARP

При использовании Proxy ARP на маршрутизаторе VRRP он **должен** анонсировать MAC-адрес VR в сообщении Proxy ARP, поскольку в противном случае хосты получат реальный MAC-адрес маршрутизатора VRRP.

8.2. IPv6

8.2.1. ICMPv6 Redirect

Перенаправления ICMPv6 обычно могут применяться при работе VRRP на группе маршрутизаторов [RFC4443]. Это позволяет использовать VRRP в средах, где топология не симметрична, например, маршрутизаторы VRRP не соединены с одними и теми же получателями. В качестве адреса отправителя ICMPv6 **следует** указывать адрес, который конечный хост использовал при выборе next-hop. Если маршрутизатор VRRP играет роль AR для маршрутизатора(ов) VR, содержащих адреса, которыми он не владеет, при выборе адреса источника перенаправления

нужно определить, какому VR был направлен пакет. Определение выполняется по MAC-адресу получателя в пакете, вызвавшем перенаправление.

8.2.2. ND Neighbor Solicitation

Когда хост передаёт сообщение ND Neighbor Solicitation для обного из адресов IPv6 маршрутизатора VR, маршрутизатор AR **должен** отвечать на него, указывая MAC-адрес VR. Маршрутизатору AR **недопустимо** указывать свой физический MAC-адрес в отклике. Это позволяет хостам всегда использовать один MAC-адрес, независимый от текущего AR.

При передаче маршрутизатором AR сообщения ND Neighbor Solicitation для адреса хоста IPv6 он **должен** включать в это сообщение MAC-адрес VR, если в сообщении передаётся опция адреса канального уровня отправителя. Использовать свой физический MAC-адрес в качестве канального адреса источника **недопустимо**.

При загрузке или перезагрузке маршрутизатора VRRP ему **не следует** передавать каких-либо сообщений ND, использующих его физический MAC-адрес для адреса IPv6, которым он владеет, и следует передавать лишь сообщения ND с MAC-адресом VR. Это означает соблюдение указанных ниже условий.

- При настройке интерфейса маршрутизаторам AR **следует** передавать незапрошенное сообщение ND Neighbor Advertisement с MAC-адресом VR для адреса IPv6 на этом интерфейсе.
- При инициализации интерфейсов для операций VRRP в процессе загрузки системы все сообщения ND Router Advertisement, ND Neighbor Advertisement и ND Neighbor Solicitation **должны** задерживаться до момента установки адреса IPv6 и MAC-адреса VR.

При перезапуске AR, где защищаемый VRRP адрес является адресом интерфейса (т. е. маршрутизатор владеет адресом) обнаружения дубликатов адресов (Duplicate Address Detection) может не срабатывать, поскольку BR **может** сообщать, что адрес принадлежит ему. Одним из решений является отказ от обнаружения дубликатов в таких случаях.

8.2.3. Анонсы маршрутизаторов

Когда резервный маршрутизатор VRRP становится AR для VR, он отвечает за передачу сообщений Router Advertisement для VR, как указано в параграфе 6.4.3. Маршрутизаторы BR **должны** быть настроены для передачи тех же опций Router Advertisement, что и владелец адреса.

Опции Router Advertisement, анонсирующие особые службы, такие как Home Agent Information Option, которые присутствуют у владельца адреса, владельцу **не следует** передавать, пока маршрутизаторы BR не подготовлены для полного предоставления таких же услуг и не имеют полной и синхронизированной базы данных для этих услуг.

8.2.4. Незапрошенные анонсы соседей

Маршрутизатору VRRP, действующему как AR или BR для IPv6, **следует** воспринимать сообщения Unsolicited Neighbor Advertisement и обновлять соответствующий кэш соседей [RFC4861]. Поскольку эти анонсы передаются по групповому адресу IPv6 all-nodes (ff02::1) [RFC4861] млм IPv6 all-routers (ff02::2), они будут получены. Сообщения Unsolicited Neighbor Advertisement передаются при смене адреса канального уровня [RFC4861] и для незапрошенного обнаружения первого маршрутизатора (first-hop) [RFC9131]. Может потребоваться дополнительная настройка, чтобы сообщения Unsolicited Neighbor Advertisement обновляли соответствующий кэш соседей.

8.3. IPvX

8.3.1. Возможные петли при пересылке

Маршрутизатору VRRP, не являющемуся владельцем адреса, **не следует** пересылать пакеты, направленные по адресу IPvX, для которого он стал AR, поскольку такая пересылка создаёт ненужный трафик. Кроме того, при получении ЛВС пакетов, которые эта сеть передала, могут возникать петли, исчезающие лишь по завершении IPvX TTL. Одним из механизмов предотвращения таких петель маршрутизаторами VRRP является добавление (удаление) Drop Route для хостов на каждом не принадлежащем маршрутизатору адресе IPvX при переходе в состояние AR (выходе из него).

8.3.2. Рекомендации по установке приоритета

Значение приоритета 255 указывает, что конкретный маршрутизатор является владельцем адреса IPvX для VRID. Маршрутизатор VRRP с приоритетом 255 при старте будет вытеснять маршрутизаторы с меньшим приоритетом. Для VRID значение 255 **следует** назначать лишь одному маршрутизатору VRRP на канале. При обнаружении нескольких таких маршрутизаторов этот факт **следует** указать в системном журнале (соблюдая ограничения по частоте записей). При отсутствии таких маршрутизаторов VRRP вытеснения не происходит.

Чтобы избежать одновременного перехода нескольких BR в состояние AR при отказе или выключении прежнего AR, все VR **следует** настраивать с разными приоритетами. Разница должна быть достаточно большой, чтобы BR с низким приоритетом не переходили в состояние Active до получения анонса от BR с самым высоким приоритетом о его переходе в состояние AR. При обнаружении нескольких VRRP, анонсирующих одинаковый приоритет, этот факт **можно** указать в системном журнале (соблюдая ограничения по частоте записей).

Поскольку значение Skew_Time снижается при увеличении приоритета, для предпочтительного BR можно обеспечить более быстрое схождение за счёт высокого приоритета. Однако следует соблюдать разницу приоритетов, как отмечено выше.

8.4. Взаимодействие VRRPv3 и VRRPv2

8.4.1. Допущения

1. Функциональная совместимость VRRPv2 и VRRPv3 не является обязательной.
2. Смешение VRRPv2 и VRRPv3 следует допускать лишь при переходе от VRRPv2 к VRRPv3 и не оставлять в качестве постоянного решения.

8.4.2. Поддержка взаимодействия с VRRPv2 в VRRPv3

Как отмечено выше такая поддержка предназначена для перехода и **не рекомендуется** как постоянное решение.

Реализация **может** использовать флаг конфигурации, указывающий поддержку приёма и передачи анонсов VRRPv2 и VRRPv3.

Когда VR настроен таким образом и является AR, он **должен** передавать оба типа анонсов с настроенной скоростью, даже если она субсекундная. Настроенный таким образом VR, являющийся BR, **должен** использовать тайм-аут на основе скорости, анонсированной AR. В случае VRRPv2 AR это означает, что маршрутизатор **должен** перевести полученное значение тайм-аута (в секундах) в сотые доли секунды. Маршрутизатору BR **следует** игнорировать анонсы VRRPv2 от текущего AR, если от него приходят и пакеты VRRPv3it. BR **может** сообщать, что VRRPv3 AR не передаёт пакетов VRRPv2, поскольку это говорит о несогласии поддерживать взаимодействие с VRRPv2.

8.4.2.1. Вопросы взаимодействия

8.4.2.1.1. Медленные AR с высоким приоритетом

Этот вопрос рассмотрен в параграфе 5.2.7.

VRRPv2 AR, взаимодействующий с субсекундным VRRPv3 BR является наиболее важным примером такой ситуации.

Для реализации VRRPv2 **не следует** задавать приоритет выше, чем у реализации VRRPv2 или VRRPv3 с которой она взаимодействует, при субсекундной скорости передачи анонсов VRRPv2 или VRRPv3.

8.4.2.1.2. Перегрузка резервных маршрутизаторов VRRPv2

Возможно, что VRRPv3 AR, передающий анонсы с субсекундной скоростью, перегрузит VRRPv2 BR с потенциально неопределённым результатом

В случае обновления следует сначала запускать VRRPv3 AR с более низкой частотой анонсов, например, 100 (1 анонс в секунду), пока маршрутизаторы VRRPv2 не будут обновлены. После проверки корректности работы VRRPv3 поддержку VRRPv2 можно отключить и настроить субсекундную скорость передачи.

9. Вопросы безопасности

VRRP для IPvX не поддерживает проверки подлинности. Прежние версии VRRP включали несколько типов аутентификации (от её отсутствия до строгой проверки подлинности). Опыт эксплуатации и анализ показали, что это не обеспечивает достаточной защиты для преодоления уязвимости из-за неверно настроенных секретов, что приводило к выбору нескольких AR сразу. В силу особенностей протокола VRRP даже криптографическая защита сообщений VRRP не препятствует враждебным узлам выдавать себя за AR, создавая в сети сразу несколько AR. Аутентификация сообщений VRRP может предотвратить переход всех нормально работающих маршрутизаторов в состояние Backup из-за действий враждебных узлов. Однако наличие нескольких AR может создать больше проблем, чем отсутствие маршрутизаторов, но аутентификация это не препятствует. Даже если враждебный узел не может нарушить работу VRRP, он способен повредить ARP/ND и результат будет таким же, как при переходе всех маршрутизаторов в состояние Backup.

Некоторые коммутаторы L2 способны фильтровать, например, сообщения ARP и/или ND от конечных хостов по портам коммутатора. Этот механизм позволяет фильтровать и сообщения VRRP с портов коммутатора, связанных с конечными хостами, и может рассматриваться для внедрения в сетях с недоверенными хостами.

Следует отметить, что такие атаки являются подмножеством атак, которые может организовать любой подключенный к ЛВС узел независимо от VRRP, включая:

- неразборчивый (promiscuous) приём пакетов с любого MAC-адреса маршрутизатора;
- передача пакетов с MAC-адресом маршрутизатора в поле MAC отправителя заголовка L2, чтобы вынудить коммутаторы L2 отправлять адресованные маршрутизатору пакеты вредоносному узлу;
- отправка перенаправления, указывающих всем хостам направлять свои пакеты в другое место;
- передача незапрошенных откликов ND;
- отклики на запросы ND и т. п.

Все означенное может происходить независимо от VRRP и протокол не добавляет уязвимостей, а большинство из них устраняется независимо, например с помощью защищённого обнаружения соседей (SEcure Neighbor Discovery или SEND) [RFC3971].

VRRP включает механизм (установка значения 255 в IPv4 TTL и IPv6 Hop Limit и проверка при получении), защищающий от внедрения пакетов VRRP из удалённой сети [RFC5082]. Это ограничивает возможности атак.

VRRP не обеспечивает конфиденциальности, которая и не требуется для корректной работы протокола. В сообщениях VRRP нет сведений, которые нужно хранить в секрете от других узлов ЛВС.

В контексте IPv6 при наличии SEND протокол VRRP совместим с режимами SEND trust anchor (привязка доверия) и trust anchor or CGA (привязка доверия или CGA) [RFC3971]. В настройках SEND нужно предоставлять маршрутизаторам AR и BR одинаковое делегирование префиксов, чтобы те и другие анонсировали общий набор префиксов подсети. Однако AR и BR следует иметь свои пары ключей, чтобы избежать применения общего секретного ключа.

В контексте IPv6 **рекомендуется** следовать руководству по защите из параграфа 2.3 в [RFC9099].

10. Взаимодействие с IANA

Агентство IANA обновило в своих реестрах ссылки на [RFC5798] ссылками на данный документ, как указано ниже.

Выделено значение 112 для VRRP в реестре Assigned Internet Protocol Numbers.

В реестре Local Network Control Block (224.0.0.0 - 224.0.0.255 (224.0.0/24)) внутри IPv4 Multicast Address Space Registry [RFC5771] агентство IANA выделило для VRRP групповой адрес IPv4 224.0.0.18.

В реестре Link-Local Scope Multicast Addresses внутри IPv6 Multicast Address Space Registry [RFC3307] агентство IANA выделило групповой адрес IPv6 link-local ff02:0:0:0:0:0:0:12 для VRRP с протоколом IPv6.

В реестре IANA MAC ADDRESS BLOCK [RFC9542] агентство IANA выделило блоки индивидуальных адресов Ethernet, приведённые в таблице 1 (в шестнадцатеричном формате).

Таблица 1.

Адреса	***Использование***	***Документ***
00-01-00 - 00-01-FF	VRRP (Virtual Router Redundancy Protocol)	RFC 9568
00-02-00 - 00-02-FF	VRRP IPv6 (Virtual Router Redundancy Protocol IPv6)	RFC 9568

11. Литература

11.1. Нормативные документы

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

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

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

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/info/rfc5082>.

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC9542] Eastlake 3rd, D., Abley, J., and Y. Li, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 9542, DOI 10.17487/RFC9542, April 2024, <https://www.rfc-editor.org/info/rfc9542>.

11.2. Дополнительная литература

[IPSTB] Higginson, P. and M. Shand, "Development of Router Clusters to Provide Fast Failover in IP Networks", Digital Technical Journal, Volume 9, Number 3, 1997.

[NISTIR8366] National Institute of Standards and Technology (NIST), "Guidance for NIST Staff on Using Inclusive Language in Documentary Standards,", NISTIR 8366, DOI 10.6028/NIST.IR.8366, April 2021, <https://doi.org/10.6028/NIST.IR.8366>.

[RFC1071] Braden, R., Borman, D., and C. Partridge, "Computing the Internet checksum", RFC 1071, DOI 10.17487/RFC1071, September 1988, <https://www.rfc-editor.org/info/rfc1071>.

[RFC1256] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, DOI 10.17487/RFC1256, September 1991, <https://www.rfc-editor.org/info/rfc1256>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2281] Li, T., Cole, B., Morton, P., and D. Li, "Cisco Hot Standby Router Protocol (HSRP)", RFC 2281, DOI 10.17487/RFC2281, March 1998, <https://www.rfc-editor.org/info/rfc2281>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[RFC2338] Knight, S., Weaver, D., Whipple, D., Hinden, R., Mitzel, D., Hunt, P., Higginson, P., Shand, M., and A. Lindem, "Virtual Router Redundancy Protocol", RFC 2338, DOI 10.17487/RFC2338, April 1998, <https://www.rfc-editor.org/info/rfc2338>.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, DOI 10.17487/RFC2453, November 1998, <https://www.rfc-editor.org/info/rfc2453>.

[RFC3768] Hinden, R., Ed., "Virtual Router Redundancy Protocol (VRRP)", RFC 3768, DOI 10.17487/RFC3768, April 2004, <https://www.rfc-editor.org/info/rfc3768>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC4311] Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, DOI 10.17487/RFC4311, November 2005, <https://www.rfc-editor.org/info/rfc4311>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5798] Nadas, S., Ed., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, DOI 10.17487/RFC5798, March 2010, <https://www.rfc-editor.org/info/rfc5798>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9099] Vyncke, É., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <https://www.rfc-editor.org/info/rfc9099>.

[RFC9131] Linkova, J., "Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers", RFC 9131, DOI 10.17487/RFC9131, October 2021, <https://www.rfc-editor.org/info/rfc9131>.

[VRRP-IPv6] Hinden, R. and J. Cruz, "Virtual Router Redundancy Protocol for IPv6", Work in Progress, Internet-Draft, draft-ietf-vrrp-ipv6-spec-08, 5 March 2007, <https://datatracker.ietf.org/doc/html/draft-ietf-vrrp-ipv6-spec-08>.

Благодарности

Текст для IPv6 в этой спецификации основан на [RFC2338], авторами которого являются S. Knight, D. Weaver, D. Whipple, R. Hinden, D. Mitzel, P. Hunt, P. Higginson, M. Shand, A. Lindem. Авторы [VRRP-IPv6] признательны Erik Nordmark, Thomas Narten, Steve Deering, Radia Perlman, Danny Mitzel, Mukesh Gupta, Don Provan, Mark Hollinger, John Cruz, Melissa Johnson за их полезные предложения.

Текст для IPv4 в этой спецификации основан на [RFC3768]. Авторы спецификации благодарны Glen Zorn, Michael Lane, Clark Bremer, Hal Peterson, Tony Li, Barbara Denny, Joel Halpern, Steve M. Bellovin, Thomas Narten, Rob Montgomery, Rob Coltun, Radia Perlman, Russ Housley, Harald Alvestrand, Ned Freed, Ted Hardie, Bert Wijnen, Bill Fenner, Alex Zinin за их комментарии и предложения.

Спасибо Steve Nadas за работу по объединению и редактированию [RFC3768] и [VRRP-IPv6], приведшему в итоге к [RFC5798].

Спасибо Stewart Bryant, Sasha Vainshtein, Pascal Thubert, Alexander Okonnikov, Ben Niven-Jenkins, Tim Chown, Mališa Vučinić, Russ White, Donald Eastlake, Dave Thaler, Eric Kline, Vijay Gurbani за комментарии к текущему документу (RFC 9568). Спасибо Gyan Mishra, Paul Congdon, Jon Rosen за обсуждения, связанные с исключением приложений для устаревших технологий. Спасибо Dhruv Dhody и Donald Eastlake за комментарии и предложения для улучшения раздела IANA. Спасибо Sasha Vainshtein за рекомендации по проверке Maximum Advertisement Interval. Спасибо Tim Chown и Fernando Gont за дискуссии и обновления, связанные с IPv6 SLAAC. Особая благодарность Quentin Armitage за подробную рецензию и обширные комментарии к текущему документу (RFC 9568).

Адреса авторов

Acee Lindem
LabN Consulting, L.L.C.
301 Midenhall Way
Cary, NC 27513
United States of America
Email: acee.ietf@gmail.com

Aditya Dogra
Cisco Systems
Sarjapur Outer Ring Road
Bangalore 560103
Karnataka
India
Email: addogra@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru