Internet Engineering Task Force (IETF)
Request for Comments: 5798
Obsoletes: 3768
Category: Standards Track
ISSN: 2070-1721

S. Nadas, Ed.
Ericsson

March 2010

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

Протокол резервирования виртуального маршрутизатора (VRRP) версии 3 для IPv4 и IPv6

Аннотация

Этот документ определяет протокол резервирования виртуального маршрутизатора (Virtual Router Redundancy Protocol или VRRP) для IPv4 и IPv6. Это третья (3) версия протокола, основанная на VRRP (версии 2) для IPv4, определённом в RFC 3768, и Virtual Router Redundancy Protocol for IPv6. VRRP задаёт протокол выбора, автоматически назначающего ответственность за виртуальный маршрутизатор одному из VRRP-маршрутизаторов в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4 или IPv6, связанные с виртуальным маршрутизатором, называется ведущим (Master) и пересылает пакеты, направленные по этим адресам IPv4 или IPv6. Маршрутизаторы VRRP Master настраиваются на виртуальные адреса IPv4 или IPv6, а резервные маршрутизаторы VRRP (Backup) выводят семейство виртуальных адресов, передаваемых на основе транспортного протокола. В маршрутизаторе VRRP виртуальные маршрутизаторы каждого из семейств IPv4 и IPv6 образуют отдельные, не перекрывающиеся домены. Процесс выбора обеспечивает динамическую обработку отказов при пересылке, если Master становится недоступным. Для IPv4 преимущество применения VRRP заключается в высокой доступности принятого по умолчанию пути без необходимости настройки протоколов динамической маршрутизации или обнаружения маршрутизаторов на каждом конечном хосте. Для IPv6 преимущества применения VRRP заключаются в более быстром переключении на резервные маршрутизаторы (Backup), нежели обеспечивают стандартные механизмы 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 5741.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке http://www.rfc-editor.org/info/rfc5798.

Авторские права

Авторские права ((c) 2010) принадлежат IETF Trust и лицам, являющимся авторами документа. Все права защищены.

К этому 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. 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 Simplified BSD License).

Документ может содержать материалы из IETF Document или IETF Contribution, опубликованных или публично доступных до 10 ноября 2008 года. Лица, контролирующие авторские права на некоторые из таких документов, могли не предоставить IETF Trust права разрешать внесение изменений в такие документы за рамками процессов IETF Standards. Без получения соответствующего разрешения от лиц, контролирующих авторские права этот документ не может быть изменён вне рамок процесса IETF Standards, не могут также создаваться производные документы за рамками процесса IETF Standards за исключением форматирования документа для публикации или перевода с английского языка на другие языки.

Оглавление

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

1. Введение

Этот документ определяет протокол VRRP для IPv4 и IPv6. Это третья (3) версия протокола, основанная на VRRP (версии 2) для IPv4, определённой в [RFC3768], и [VRRP-IPv6]. VRRP задаёт протокол выбора, автоматически назначающего ответственность за виртуальный маршрутизатор одному из VRRP-маршрутизаторов в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4 или IPv6, связанные с виртуальным маршрутизатором, называется ведущим (Master) и пересылает пакеты, направленные по этим адресам IPv4 или IPv6. Маршрутизаторы VRRP Master настраиваются на виртуальные адреса IPv4 или IPv6, а резервные маршрутизаторы VRRP (Backup) выводят семейство виртуальных адресов, передаваемых на основе транспортного протокола. В маршрутизаторе VRRP виртуальные маршрутизаторы каждого из семейств IPv4 и IPv6 образуют отдельные, не перекрывающиеся домены. Процесс выбора обеспечивает динамическую обработку отказов при пересылке, если Master становится недоступным.

VRRP обеспечивает функцию, похожую на фирменные (proprietary) протоколы Hot Standby Router Protocol (HSRP) [RFC2281] и IP Standby Protocol [IPSTB].

1.1. Замечание по терминологии

В этом документе рассматриваются операции IPv4 и IPv6, многие из которых применительно VRRP имеют общие описания и процедуры. В документе можно было бы использовать краткое обозначение IP для обоих протоколов IPv4 и IPv6. Однако исторически IP обычно указывает IPv4, поэтому здесь применяется обозначение IPvX (где X - 4 или 6) для обоих протоколов сразу. Там, где версия IP имеет значение, применяется соответствующее обозначение.

1.2. IPv4

Имеются методы, позволяющие конечному хосту IPv4 определить первый (first-hop) маршрутизатор в направлении конкретного получателя IPv4. Они включают применение (или отслеживание) протоколов динамической маршрутизации, таких как RIP [RFC2453] или OSPF версии 2 [RFC2328], применение клиента обнаружения маршрутизаторов ICMP [RFC1256], статическая настройка принятого по умолчанию маршрута.

Применение протокола динамической маршрутизации на каждом конечном хосте может быть невозможно по разным причинам, включая административные издержки, дополнительную обработку, проблемы безопасности, отсутствие реализации протокола для некоторых платформ. Протоколы обнаружения соседей или маршрутизаторов могут потребовать вовлечения всех хостов сети, что ведёт к большим значениям таймеров для снижения издержек протокола при большом числе хостов. Это может приводить к значительным задержкам обнаружения потери соседа, что может создавать длительные «чёрные дыры».

Применение статически заданных маршрутов по умолчанию (default) достаточно популярно, оно минимизирует издержки конечных хостов на настройку и обработку и поддерживается практически каждой реализацией IPv4. Этот режим работы будет, скорей всего, сохраняться по мере развёртывания протокола динамической настройки конфигурации хостов [RFC2131], который обычно задаёт для конечного хоста адрес IPv4 и принятый по умолчанию шлюз. Потеря заданного по умолчанию маршрута ведёт к возникновению больших проблем, изолируя все конечные хосты, которые не могут обнаружить какой-либо альтернативный путь.

Протокол VRRP предназначен для устранения критической точки отказа, присущей среде с заданным по умолчанию маршрутом. VRRP задаёт протокол выбора, который динамически назначает ответственность за виртуальный маршрутизатор одному из маршрутизаторов VRRP в ЛВС. Маршрутизатор VRRP, контролирующий адреса IPv4, связанные с виртуальным маршрутизатором, называется ведущим (Master) и пересылает пакеты, направленные по этим адресам IPv4. Процесс выбора обеспечивает динамическую обработку отказов при пересылке, если Master становится недоступным. После этого конечные хосты могут применять любой из адресов IPv4 виртуального маршрутизатора в ЛВС как принятый по умолчанию адрес первого маршрутизатора. Преимуществом применения VRRP является высокая доступность заданного по умолчанию пути без настройки динамической маршрутизации или обнаружения маршрутизаторов на каждом конечном хосте.

1.3. IPv6

Хосты IPv6 в ЛВС обычно узнают об одном или нескольких заданных по умолчанию маршрутизаторах из анонсов Router Advertisement, передаваемых с использованием протокола обнаружения соседей IPv6 (Neighbor Discovery или ND) [RFC4861]. Анонсы периодически передаются по групповым адресам с частотой, позволяющей хостам узнать о маршрутизаторах в течение нескольких минут. Это недостаточно часто, чтобы полагаться на такие анонсы для обнаружения отказов принятых по умолчанию маршрутов.

ND включает механизм обнаружения недоступности соседа (Neighbor Unreachability Detection) для обнаружения отказов соседа (хоста или маршрутизатора) или пути пересылки к соседу. Это выполняется путём отправки соседу индивидуальных сообщений ND Neighbor Solicitation. Для снижения связанных с этим издержек, такие сообщения передаются лишь соседям, которым активно отправляется трафик и лишь в тех случаях, когда в течение определённого времени не было никаких признаков активности маршрутизатора. При использовании принятых по умолчанию параметров ND хосту потребуется около 38, чтобы узнать о недоступности маршрутизатора, прежде чем он переключится на другой маршрутизатор, заданный по умолчанию. Такая задержка очень заметна для пользователей и вызывает тайм-ауты в некоторых реализациях транспортных протоколов.

Хотя обнаружение недоступности в ND можно было бы ускорить, изменив параметры в сторону повышения активности (отметим, что текущий нижний предел составляет 5 секунд), это существенно повысит связанные с трафиком ND издержки, особенно для хостов, пытающихся определить доступность одного из нескольких маршрутизаторов.

Протокол VRRP для IPv6 обеспечивает более быстрое переключение на другой маршрутизатор, заданный по умолчанию, нежели стандартные процедуры ND. Используя VRRP, маршрутизатор Backup может заменить неисправный маршрутизатор, принятый по умолчанию, примерно за 3 секунды (с принятыми по умолчанию параметрами VRRP). Это делается без взаимодействия с хостами и с минимальным объёмом трафика VRRP.

1.4. 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), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

1.5. Область действия

В оставшейся части документа описаны функции, цели создания и теория работы VRRP. Представлены форматы сообщений, правила обработки и конечный автомат, гарантирующие сходимость выбора к одному Virtual Router Master. Рассмотрены также операционные вопросы, связанные с сопоставлением MAC-адресов, обработкой запросов ARP, генерацией сообщения ICMP и вопросы безопасности.

1.6. Определения

VRRP Router - маршрутизатор VRRP

Маршрутизатор, на котором работает протокол VRRP. Он может выступать как 1 или несколько виртуальных маршрутизаторов.

Virtual Router - виртуальный маршрутизатор

Абстрактный объект, поддерживаемый VRRP и выступающий принятым по умолчанию маршрутизатором для хостов общей ЛВС. Он включает Virtual Router Identifier и набор связанных адресов IPv4 или IPv6 для общей ЛВС. Маршрутизатор VRRP может поддерживать 1 или несколько виртуальных маршрутизаторов.

IP Address Owner - владелец адреса IP

Маршрутизатор VRRP имеющий адреса виртуальных маршрутизаторов IPvX как адреса реальных интерфейсов. Это маршрутизатор, который, будучи включённым, отвечает на пакеты, направленные по одному из этих адресов IPvX для ICMP ping, соединений TCP и т. п.

Primary IP Address - первичный (основной) адрес IP

В IPv4 это адрес IPv4, выбранный из набора реальных адресов интерфейсов. Одним из возможных вариантов является выбор первого адреса. В режиме IPv4 анонсы VRRP всегда передаются с использованием первичного адреса IPv4 в качестве адреса отправителя. В IPv6 используется адрес link-local интерфейса, с которого передаётся пакет.

Virtual Router Master - первичный (ведущий) виртуальный маршрутизатор

Маршрутизатор VRRP, который предполагается ответственным за пересылку пакетов, направленных по адресу IpvX, связанному с виртуальным маршрутизатором, ответы на запросы ARP для адресов IPv4 и запросы ND для адресов IPv6. Отметим, что при доступности владельца адреса IPvX он всегда играет роль ведущего (Master).

Virtual Router Backup - резервный виртуальный маршрутизатор

Набор маршрутизаторов VRRP, которые могут принять ответственность за пересылку для виртуального маршрутизатора в случае отказа текущего первичного маршрутизатора (Master).

2. Требуемые функции

В этом разделе очерчен набор функций, которые сочтены обязательными и которыми руководствовались при разработке VRRP.

2.1. Резервирование адресов IPvX

Резервирование адресов IPvX является основной функцией VRRP. Обеспечивая выбор ведущего виртуального маршрутизатора (Virtual Router Master) и описанные ниже дополнительные функции, протоколу следует также:

- минимизировать продолжительность «чёрных дыр» в маршрутизации;
- минимизировать расход пропускной способности в установившемся состоянии и сложность обработки;
- работать с разными технологиями множественного доступа в ЛВС, способными поддерживать трафик IpvX;
- поддерживать в сети несколько виртуальных маршрутизаторов для распределения нагрузки;
- поддерживать множество подсетей IPvX в одном сегменте ЛВС.

2.2. Индикация предпочтительного пути

Простая модель выбора ведущего (Master) маршрутизатора из числа избыточных состоит в рассмотрении всех с одинаковым предпочтением и назначения ведущим любого маршрутизатора после сходимости к нему. Однако, скорей всего, во многих средах будут свои предпочтения (или диапазоны предпочтений) для разных маршрутизаторов из числа доступных. Например, предпочтения могут опираться на «стоимость» или скорость канала доступа, надёжность или производительность маршрутизатора, соображения политики. Протоколу следует разрешать выражение относительных предпочтений пути понятным интуитивно способом и обеспечивать выбор в качестве Master наиболее подходящего маршрутизатора из числа доступных.

2.3. Минимизация ненужного нарушения обслуживания

После выбора ведущего маршрутизатора ненужные переходы между Master и Backup могут приводить к нарушению обслуживания. Протоколу следует обеспечивать после выбора Master предотвращение смены состояния, вызванной любым Backup-маршрутизатором, имеющим предпочтение не выше, чем у продолжающего корректно работать Master.

В некоторых средах может давать преимущество предотвращение смены состояния при доступности текущего Master-маршрутизатора. Может оказаться полезным предотвращение немедленного схождения к предпочтительному пути.

2.4. Эффективная работа в расширенных ЛВС

Отправка пакетов IPvX (IPv4 или IPv6) в ЛВС с множественным доступом требует сопоставления адресов IPvX и MAC. Применение MAC-адреса виртуального маршрутизатора в расширенной ЛВС, использующей мосты с обучением, может оказывать существенное влияние на расход полосы пакетами, переданными виртуальному маршрутизатору. Если MAC-адрес виртуального маршрутизатора не применяется как адрес отправителя кадров канального уровня, его местоположение не будет известно и это ведёт к лавинной рассылке всех пакетов, адресованных виртуальному маршрутизатору. Для повышения эффективности таких сред протоколу следует 1) использовать MAC-адрес виртуального маршрутизатора в пакетах, передаваемых Master-маршрутизатором для включения этого адреса в процесс обучения, 2) передавать сообщение сразу по переходе в режим Master для обновления адреса на станциях и 3) периодически отправлять сообщения от Master для поддержки кэша адресов на станциях.

2.5. Субсекундные операции IPv4 и IPv6

Субсекундное обнаружение отказов маршрутизатора Master VRRP требуется в обеих средах IPv4 и IPv6. Ранее была предложена субсекундная оптимизация для IPv6, а данная спецификация использует этот подход для IPv4 и IPv6.

Один из возможных проблемных вариантов при использовании малых значений VRRP_Advertisement_Interval может возникать в случае, когда маршрутизатор доставляет в ЛВС больше пакетов, нежели сеть может воспринять и в маршрутизаторе возникает очередь. Задержка в такой очереди может превысить минимальное значение VRRP Advertisement_Interval. В этом случае значение Master_Down_Interval будет достаточно мало, чтобы обычные задержки в очереди могли привести к решению VRRP Backup о том, что маршрутизатор Master не работает и предложить себя в качестве нового ведущего. Вскоре после этого задержанные на ведущем маршрутизаторе пакеты Master вызовут обратный переход в состояние Backup. Этот процесс может многократно повторяться в течение 1 секунды, вызывая существенное нарушение трафика. Для смягчения этой проблемы следует рассмотреть приоритетную пересылку пакетов VRRP. Для VRRP Master следует поддерживать возможность наблюдать частое возникновение описанной ситуации и по меньшей мере записывать это в системный журнал (log).

3. Обзор VRRP

VRRP задаёт протокол выбора для обеспечения описанной выше функции виртуального маршрутизатора. Все сообщения протокола передаются в групповых (multicast) дейтаграммах IPv4 или IPv6, что позволяет применять протокол с разными технологиями ЛВС с множественным доступом, поддерживающие групповую передачу IPvX. Каждому каналу виртуального маршрутизатора VRRP выделяется 1 общеизвестный MAC-адрес. Этот документ определяет отображение лишь для сетей, использующих 44-битовые MAC-адреса IEEE 802. Адрес MAC используется как адрес отправителя во всех периодических сообщениях VRRP, передаваемых Master-маршрутизатором для обучения мостов в расширенной ЛВС.

Виртуальный маршрутизатор определяется идентификатором VRID (virtual router identifier) и набором адресов IPv4 или IPv6. Маршрутизатор VRRP может связать виртуальный маршрутизатор с реальным адресом на интерфейсе. Область действия каждого виртуального маршрутизатора ограничена одной ЛВС. На маршрутизаторе VRRP можно настроить дополнительные отображения и приоритеты виртуальных маршрутизаторов, которые будут служить резервными. Сопоставления VRID и адресов IPvX должны быть согласованы между всеми маршрутизаторами VRRP в ЛВС.

На повторное использование VRID с другим сопоставлением адресов в другой ЛВС, а также применение одного VRID для набора адресов IPv4 и IPv6, однако это будут разные виртуальные маршрутизаторы.

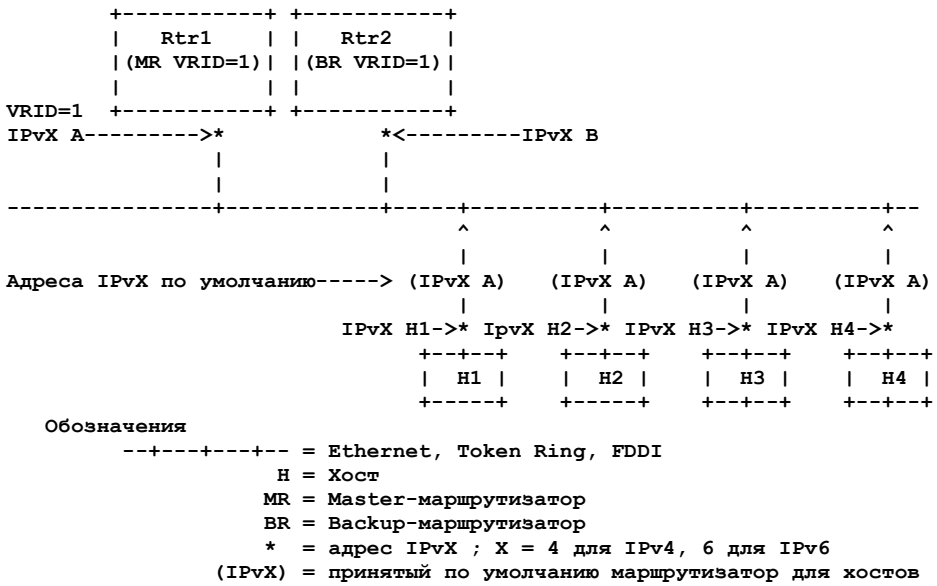
Для минимизации сетевого трафика только Master для каждого виртуального маршрутизатора передаёт периодические сообщения VRRP Advertisement. Маршрутизатор Backup не пытается вытеснить Master, пока у него нет более высокого приоритета. Это устраняет перебои в обслуживании, пока не станет доступным более предпочтительный путь. Можно также административно запретить попытки вытеснения. Единственным исключением является то, что маршрутизатор VRRP всегда принимает роль Master для любого виртуального маршрутизатора, связанного с адресом, которым он владеет. Если Master становится недоступным, маршрутизатор Backup с высшим приоритетом переходит в статус Master с короткой задержкой, обеспечивая контролируемый переход ответственности виртуального маршрутизатора с минимальным прерыванием обслуживания.

Устройство протокола VRRP обеспечивает быстрый переход маршрутизатора Backup в состояние Master для минимизации перерыва в обслуживании и включает оптимизацию, устраняющую сложности протокола при гарантии контролируемого перехода в состояние Master для типичных сценариев. Результатом оптимизации служит протокол выбора с минимальными рабочими требованиями к состоянию, минимальным числом активных состояний, одним типом сообщений и отправителем. Типовые сценарии работы определяются как наличие двух избыточных (резервных) маршрутизаторов и/или разных предпочтений пути для каждого маршрутизатора. Побочным эффектом нарушения этих допущений (т. е. наличия более 2 избыточных путей с одинаковым предпочтением) является возможность передачи дубликатов пакетов в течение короткого интервала выбора Master. Однако допущения для типового сценария, вероятно, охватывают большинство развёртываний, потери Master-маршрутизатора редки, а ожидаемая сходимость выбора Master достаточно мала (<< 1 секунды). Таким образом, оптимизация VRRP обеспечивает значительное упрощение протокола, при этом вероятность кратковременного нарушения работы сети незначительна.

4. Примеры конфигурации

4.1. Пример 1

На рисунке показана простая сеть с двумя маршрутизаторами VRRP, реализующими 1 виртуальный маршрутизатор.



Исключив упоминания VRRP (VRID=1) на рисунке, можно считать это типичным развёртыванием.

В случае IPv4 (т. е. IPvX = IPv4 на рисунке) каждому маршрутизатору назначается постоянный адрес IPv4 на интерфейсе ЛВС (Rtr1 получает IPv4 A, а Rtr2 - IPv4 B), а каждый хост устанавливает принятый по умолчанию маршрут через один из маршрутизаторов (в этом примере используется Rtr1 с адресом IPv4 A).

В случае IPv6 (т. е. IPvX = IPv6 на рисунке) каждый маршрутизатор имеет адрес IPv6 link-local на интерфейсе ЛВС (Rtr1 получает IPv6 Link-Local A, а Rtr2 - IPv6 Link-Local B), а каждый хост узнает принятый по умолчанию маршрут из Router Advertisement от одного из этих маршрутизаторов (в этом примере используется Rtr1 с адресом IPv6 Link-Local A).

В среде IPv4 VRRP каждый маршрутизатор имеет в точности 1 постоянно назначенный адрес IPv4. О Rtr1 говорят, что он имеет адрес IPv4 A, а Rtr2 - IPv4 B. Затем виртуальный адрес определяется назначением уникального идентификатора с адресом, принадлежащим маршрутизатору.

В среде IPv6 VRRP каждый маршрутизатор имеет в точности 1 постоянно назначенный адрес IPv6 Link-Local. Rtr1 получает адрес IPv6 A, а Rtr2 - IPv6 B. Затем виртуальный адрес определяется назначением уникального идентификатора с адресом, принадлежащим маршрутизатору.

В обоих случаях (IPv4 и IPv6) протокол VRRP управляет переключением виртуального маршрутизатора на Backup.

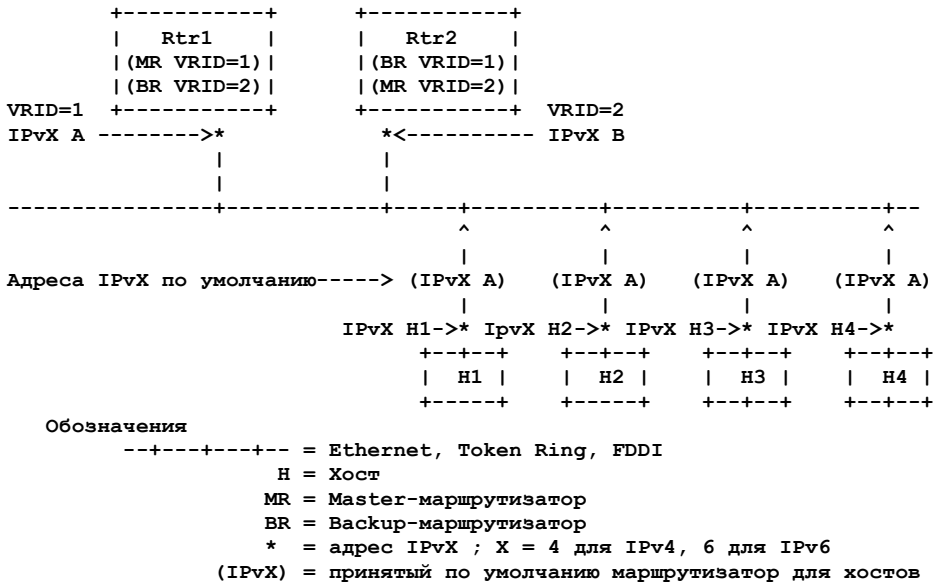
Приведённый выше пример для IPv4 показывает виртуальный маршрутизатор, настроенный на адрес IPv4, принадлежащий Rtr1 (VRID=1, IPv4_Address=A). Когда протокол VRRP включён на Rtr1 для VRID=1, этот маршрутизатор будет заявлять себя как Master с приоритетом 255, поскольку он является владельцем адреса IP виртуального маршрутизатора. Когда VRRP включён на Rtr2 для VRID=1, этот маршрутизатор будет в состоянии Backup с приоритетом 100 (задан по умолчанию), поскольку он не владеет адресом IPv4. При отказе Rtr1 протокол VRRP переведёт Rtr2 в состояние Master, временно передавая ему ответственность за пересылку IPv4 A для обеспечения непрерывного обслуживания хостов. При восстановлении Rtr1 он снова примет роль Master.

Приведённый выше пример для IPv6 показывает виртуальный маршрутизатор, настроенный на адрес IPv6, принадлежащий Rtr1 (VRID=1, IPv6_Address=A). Когда протокол VRRP включён на Rtr1 для VRID=1, этот маршрутизатор будет заявлять себя как Master с приоритетом 255, поскольку он является владельцем адреса IPv6 виртуального маршрутизатора. Когда VRRP включён на Rtr2 для VRID=1, этот маршрутизатор будет в состоянии Backup с приоритетом 100 (задан по умолчанию), поскольку он не владеет адресом IPv6. При отказе Rtr1 протокол VRRP переведёт Rtr2 в состояние Master, временно передавая ему ответственность за пересылку IPv6 A для обеспечения непрерывного обслуживания хостов.

Отметим, что для обоих случаев в этом примере IPvX B не резервируется и лишь применяется в качестве адреса интерфейса Rtr2. Для резервирования IPvX B требуется второй виртуальный маршрутизатор, как показано ниже.

4.2. Пример 2

На рисунке показана схема с двумя виртуальными маршрутизаторами и распределением между ними трафика хостов.



В случае IPv4 (т. е. IPvX = IPv4 на рисунке) половина хостов настроена на маршрут через IPv4 A маршрутизатора Rtr1, другая - через IPv4 B. Настройка виртуального маршрутизатора VRID=1 совпадает с предыдущим примером (параграф 4.1. Пример 1) и добавлен второй виртуальный маршрутизатор с адресом IPv4, принадлежащим Rtr2 (VRID=2, IPv4_Address=B). В этом случае Rtr2 будет заявлять себя как Master для VRID=2, а Rtr1 будет Backup. Этот вариант демонстрирует развёртывание, где доступны оба маршрутизатора и обеспечивается полное резервирование для отказоустойчивости.

В случае IPv6 (т. е. IPvX = IPv6 на рисунке) половина хостов настроена на маршрут через IPv6 A маршрутизатора Rtr1, другая - через IPv6 B. Настройка виртуального маршрутизатора VRID=1 совпадает с предыдущим примером (параграф 4.1. Пример 1) и добавлен второй виртуальный маршрутизатор с адресом IPv6, принадлежащим Rtr2 (VRID=2, IPv6_Address=B). В этом случае Rtr2 будет заявлять себя как Master для VRID=2, а Rtr1 будет Backup. Этот вариант демонстрирует развёртывание, где доступны оба маршрутизатора и обеспечивается полное резервирование для отказоустойчивости.

Детали распределения нагрузки выходят за рамки этого документа. Однако в случае, когда серверам нужны разные веса, может не иметь смысла полагаться лишь на анонсы маршрутизаторов для распределения между ними нагрузки.

5. Протокол

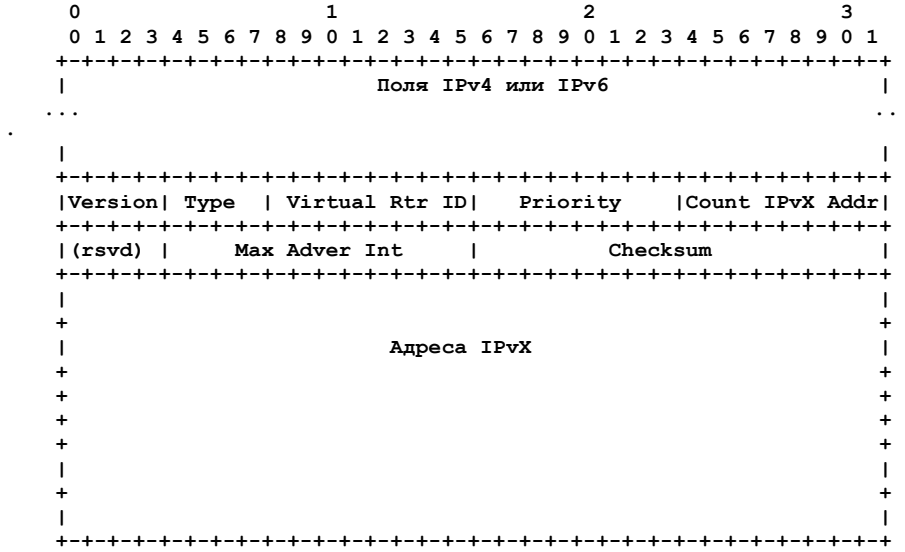
Пакет VRRP предназначен для передачи всем маршрутизаторам VRRP приоритета и состояния ведущего (Master) маршрутизатора, связанного с VRID.

Когда VRRP защищает адрес IPv4, пакеты VRRP инкапсулируются в IPv4 и передаются по групповому адресу IPv4, выделенному для VRRP.

Когда VRRP защищает адрес IPv6, пакеты VRRP инкапсулируются в IPv4 и передаются по групповому адресу IPv6, выделенному для VRRP.

5.1. Формат пакета VRRP

В этом разделе определён формат пакета VRRP и соответствующие поля заголовка IP.



5.1.1. Описания полей IPv4

5.1.1.1. Source Address

Основной адрес IPv4 на интерфейсе, с которого передаётся пакет.

5.1.1.2. Destination Address

Групповой адрес IPv4, выделенный IANA для VRRP (224.0.0.18) с действием на локальном канале (link-local). Маршрутизаторам **недопустимо** пересылать дейтаграммы с таким адресом получателя независимо от TTL.

5.1.1.3. TTL

Поле TTL должно иметь значение 255. Маршрутизатор VRRP **должен** отбрасывать принятые пакеты с иным TTL.

5.1.1.4. Protocol

Номер протокола IPv4, выделенный IANA для VRRP - 112 (десятичный).

5.1.2. Описания 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, выделенный IANA для VRRP - FF02:0:0:0:0:0:0:12. Это групповой адрес с действием на локальном канале (link-local). Маршрутизаторам **недопустимо** пересылать дейтаграммы с таким адресом получателя независимо от Hop Limit.

5.1.2.3. Hop Limit

Поле Hop Limit должно иметь значение 255. Маршрутизатор VRRP **должен** отбрасывать принятые пакеты с иным Hop Limit.

5.1.2.4. Next Header

Протокол IPv6 Next Header, выделенный IANA для VRRP - 112 (десятичный).

5.2. Описания полей VRRP

5.2.1. Version

Поле, указывающее версию протокола VRRP для данного пакета. Этот документ определяет версию 3.

5.2.2. Type

Поле указывает тип данного пакета VRRP. В этой версии протокола определён единственный тип

```
1 ADVERTISEMENT
```

Пакеты неизвестного типа **должны** отбрасываться.

5.2.3. Virtual Rtr ID (VRID)
Поле Virtual Rtr ID указывает виртуальный маршрутизатор, статус которого передаёт этот пакет.

5.2.4. Priority
Это поле указывает приоритет передающего маршрутизатора VRRP для виртуального маршрутизатора. Большее значение указывает более высокий приоритет. Значения интерпретируются как 8-битовое целое число без знака.

Поле приоритета для маршрутизатора VRRP, владеющего адресом IPvX, назначенным виртуальному маршрутизатору, должно иметь значение 255 (десятичное).

Маршрутизаторы VRRP, резервирующие виртуальный маршрутизатор, **должны** использовать значения приоритета от 1 до 254 (десятичные). По умолчанию приоритет маршрутизатора VRRP, резервирующего виртуальный маршрутизатор имеет значение 100 (десятичные).

Нулевой приоритет (0) имеет особое значение, указывающее, что текущий маршрутизатор Master прекратил участие в VRRP. Это служит для быстрого перехода маршрутизатора Backup в состояние Master без тайм-аута ведущего.

5.2.5. Count IPvX Addr
Число адресов IPv4 или IPv6 в этом анонсе VRRP (не менее 1).

5.2.6. Rsvd
Это поле должно иметь значение 0 при передаче и **должно** игнорироваться при получении.

5.2.7. Максимальный интервал между анонсами (Max Adver Int)
12-битовое поле, указывающее максимальный интервал между анонсами в сотых долях секунды. По умолчанию установлено значение 100 (1 секунда).

Отметим, что Master-маршрутизаторы с высоким приоритетом и меньшей частотой передачи по сравнению с Backup-маршрутизаторами, нестабильны. Это связано с тем, что маршрутизатор с меньшим приоритетом и более частой передачей анонсов может принять решение о том, что ему следует стать ведущим, до того, как услышит что-либо от приоритетного Master с низкой частотой анонсов. Это переключение будет временным, поскольку получив анонс от Master с высоким приоритетом, этот маршрутизатор вернётся к прежней роли.

5.2.8. Checksum
Поле контрольной суммы служит для обнаружения повреждений данных в сообщении VRRP.

Контрольная сумма представляет собой 16-битовое дополнение до 1 суммы дополнений до 1 слов всего сообщения VRRP, начиная с поля версии и заканчивая псевдозаголовком, определенным в параграфе 8.1 [RFC2460]. В поле next header псевдозаголовка должно быть установлено значение 112 (десятичное) для VRRP. При расчёте контрольной суммы значение поля checksum считается 0. Детали расчёта контрольных сумм приведены в [RFC1071].

5.2.9. IPvX Address
Это поле содержит 1 или несколько адресов IpvX, связанных с виртуальным маршрутизатором. Число адресов указано в поле Count IP Addr. Эти поля служат для поиска ошибок в конфигурации маршрутизаторов. Если указано несколько адресов, на всех маршрутизаторах, где эти адреса настроены, рекомендуется указывать их в одинаковом порядке для упрощения сравнений.

Для IPv4 это поле содержит 1 или несколько адресов IPv4, резервируемых виртуальным маршрутизатором.

Для IPv6 первым должен быть адрес IPv6 link-local, связанный с виртуальным маршрутизатором.

Это поле может содержать лишь адреса одного семейства (IPv4 или IPv6), т. е. смешивать IPv4 и IPv6 **недопустимо**.

6. Конечный автомат протокола

6.1. Параметры на уровне виртуального маршрутизатора

VRID
: Идентификатор виртуального маршрутизатора - от 1 до 255 (десятичное). Значение по умолчанию не задано.

Priority
: Приоритет, используемый данным маршрутизатором VRRP при выборе Master для этого виртуального маршрутизатора. Значение 255 (десятичное) зарезервировано для маршрутизатора, владеющего адресом IpvX, связанным с виртуальным маршрутизатором, значение 0 зарезервировано для маршрутизатора Master, указывающего снятие ответственности за виртуальный маршрутизатор. Значения от 1 до 254 (десятичные) доступны для маршрутизаторов VRRP, резервирующих виртуальный маршрутизатор. Большее значение задаёт более высокий приоритет. По умолчанию используется значение 100 (десятичное).

IPv4_Addresses
: Один или несколько адресов IPv4, связанных с данным маршрутизатором. Значение по умолчанию не задано.

IPv6_Addresses
: Один или несколько адресов IPv6, связанных с данным маршрутизатором. Значение по умолчанию не задано. Первым в списке должен быть адрес Link-Local, связанный с виртуальным маршрутизатором.

Advertisement_Interval
: Время между ADVERTISEMENTS (в сотых долях секунды). По умолчанию задано 100 (1 секунда).

Master_Adver_Interval
: Интервал анонсов, содержащихся в ADVERTISEMENTS от Master (в сотых долях секунды). Это значение сохраняют виртуальные маршрутизаторы в состоянии Backup и оно применяется при расчёте Skew_Time и Master_Down_Interval. Исходное значение совпадает с Advertisement_Interval.

Skew_Time

Величина смещения Master_Down_Interval в сотых долях секунды. Рассчитывается как **(((256 - priority) * Master_Adver_Interval) / 256)**.

Master_Down_Interval

Интервал времени для Backup, чтобы объявить отказ Master (в сотых долях секунды). Рассчитывается как **(3 * Master_Adver_Interval) + Skew_time**.

Preempt_Mode

Определяет, будет ли (запускаемый или перезапускаемый) маршрутизатор Backup с более высоким приоритетом вытеснять Master с меньшим приоритетом. True (по умолчанию) разрешает вытеснение, False - запрещает.

Примечание. Маршрутизатор, владеющий адресом IpvX, связанным с виртуальным маршрутизатором, использует вытеснение независимо от этого флага.

Accept_Mode

Определяет, будет ли виртуальный маршрутизатор в состоянии Master воспринимать пакеты, адресованные владельцу IPvX, как свои, если IPvX ему не принадлежит. По умолчанию задано False. Развертывания, полагающиеся, например на ping для владельца адреса IPvX, могут устанавливать Accept_Mode = True.

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

Virtual_Router_MAC_Address

MAC-адрес, указываемый в поле отправителя анонсов VRRP и в откликах ARP как MAC-адрес для IP_Addresses.

6.2. Таймеры

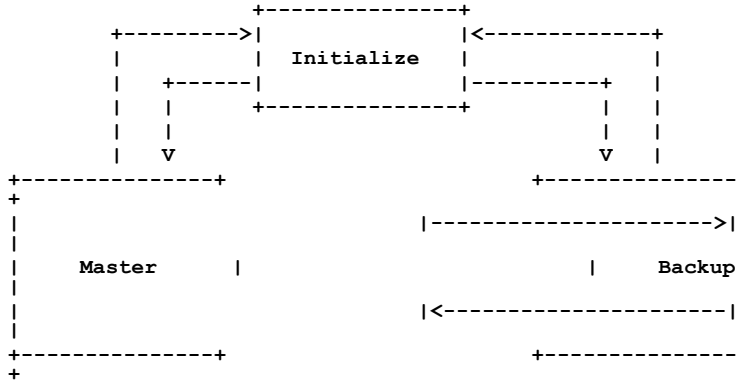
Master_Down_Timer

Таймер, срабатывающий при отсутствии ADVERTISEMENT в течение Master_Down_Interval.

Adver_Timer

Таймер, вызывающий отправку ADVERTISEMENT на основе Advertisement_Interval.

6.3. Диаграмма смены состояний



6.4. Описание состояний

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

Маршрутизатор VRRP реализует экземпляр конечного автомата для каждого выбора виртуального маршрутизатора, где он участвует.

6.4.1. Initialize

В этом состоянии маршрутизатор ожидает события Startup, т. е. определяемого реализацией механизма, запускающего протокол после его настройки. Механизм настройки выходит за рамки спецификации.

```
(100) По событию Startup выполняются указанные ниже действия.
   (105) Если Priority = 255 (маршрутизатор владеет адресом IPvX,
         связанным с виртуальным маршрутизатором,
      (110) передаётся ADVERTISEMENT.
      (115) Если защищаемый адрес IPvX является IPv4,
         (120) передаётся широковещательный беспричинный запрос ARP с
               MAC-адресом виртуального маршрутизатора для каждого
               адреса IP, связанного с виртуальным маршрутизатором,
      (125) иначе, // IPv6
         (130) для каждого адреса IPv6, связанного с виртуальным
               маршрутизатором, передаётся незапрошенный анонс
               ND Neighbor Advertisement с установленным флагом R
               (Router), сброшенным флагом S (Solicited ),
               установленным влагом O (Override), целевым адресом IPv6
               виртуального маршрутизатора и целевым адресом канального
               уровня, содержащим MAC-адрес виртуального маршрутизатора.
      (135) endif // защищаемый адрес является IPv4?
      (140) Устанавливается Adver_Timer = Advertisement_Interval.
      (145) Переход в состояние {Master}.
   (150) Иначе // маршрутизатор не владеет виртуальным адресом
      (155) Устанавливается Master_Adver_Interval = Advertisement_Interval.
      (160) Устанавливается Master_Down_Timer = Master_Down_Interval.
      (165) Переход в состояние {Backup}.
   (170) endif // приоритет не был равен 255
(175) endif // было принято событие Startup
```

6.4.2. Backup

В состоянии {Backup} отслеживается доступность и состояние маршрутизатора Master.

```
(300) Маршрутизатор VRRP ДОЛЖЕН выполнять указанные ниже действия.
   (305) Если защищаемый адрес IPvX является IPv4,
      (310) НЕДОПУСТИМО отвечать на запросы ARP для адресов IPv4,
            связанных с виртуальным маршрутизатором,
   (315) иначе // IPv6
      (320) НЕДОПУСТИМО отвечать на сообщения ND Neighbor Solicitation
            для адресов IPv6, связанных с виртуальным маршрутизатором.
      (325) НЕДОПУСТИМО передавать сообщения ND Router Advertisement
            для виртуального маршрутизатора.
   (330) endif // защищаемый адрес является IPv4?
   (335) ДОЛЖНЫ отбрасываться пакеты с MAC-адресом получателя,
         совпадающим с MAC-адресом виртуального маршрутизатора.
   (340) НЕДОПУСТИМО воспринимать пакеты, направленные по адресам IPvX,
         связанным с виртуальным маршрутизатором.
   (345) При получении события Shutdown
      (350) отключается таймер Master_Down_Timer,
      (355) состояние меняется на {Initialize}.
   (360) endif // событие Shutdown
   (365) При завершении отсчёта Master_Down_Timer
      (370) передаётся ADVERTISEMENT.
      (375) Если защищаемый адрес IPvX является IPv4,
         (380) передаётся широковещательный беспричинный запрос ARP с
               MAC-адресом виртуального маршрутизатора для каждого
               адреса IPv4, связанного с виртуальным маршрутизатором,
      (385) иначе // IPv6
         (390) вычисляется и присоединяется групповой адрес Solicited-
               Node [RFC4291] для адресов IPv6, связанных с
               виртуальным маршрутизатором.
         (395) Для каждого адреса IPv6, связанного с виртуальным
               маршрутизатором передаётся незапрошенный анонс
               ND Neighbor Advertisement с установленным флагом R
               (Router), сброшенным флагом S (Solicited ),
               установленным влагом O (Override), целевым адресом IPv6
               виртуального маршрутизатора и целевым адресом канального
               уровня, содержащим MAC-адрес виртуального маршрутизатора.
      (400) endif // защищаемый адрес является IPv4?
      (405) Устанавливается Adver_Timer = Advertisement_Interval.
      (410) Переход в состояние {Master}.
   (415) endif // завершение Master_Down_Timer.
   (420) Если получен анонс ADVERTISEMENT,
      (425) Если в ADVERTISEMENT поле Priority = 0,
         (430) Устанавливается Master_Down_Timer = Skew_Time,
      (440) иначе // Priority отличается от 0.
         (445) Если Preempt_Mode = False или Priority в
               ADVERTISEMENT не меньше локального Priority,
            (450) Устанавливается Master_Adver_Interval = интервалу
                  анонсирования из ADVERTISEMENT
            (455) Пересчитывается Master_Down_Interval.
            (460) Master_Down_Timer сбрасывается в Master_Down_Interval.
         (465) Иначе // вытеснение включено и [1] приоритет меньше
            (470) Отбрасывается ADVERTISEMENT
         (475) endif // проверка вытеснения
      (480) endif // Priority = 0?
   (485) endif // был получен анонс ADVERTISEMENT?
(490) endwhile // состояние Backup
```

6.4.3. Master

В состоянии {Master} маршрутизатор выполняет пересылку для адресов IPvX, связанных с виртуальным маршрутизатором. Поле Preempt_Mode в этом состоянии не принимается во внимание.

```
(600) Маршрутизатор VRRP ДОЛЖЕН выполнять указанные ниже действия.
   (605) Если защищаемый адрес IPvX является IPv4,
      (610) маршрутизатор ДОЛЖЕН отвечать на запросы ARP для адресов
            IPv4, связанных с виртуальным маршрутизатором,
   (615) иначе // IPv6
      (620) маршрутизатор ДОЛЖЕН входить в группу Solicited-Node
            для адресов IPv6, связанных с виртуальным маршрутизатором,
      (625) ДОЛЖЕН отвечать на сообщения ND Neighbor Solicitation
            для адресов IPv6, связанных с виртуальным маршрутизатором,
      (630) ДОЛЖЕН передавать ND Router Advertisement для
            виртуального маршрутизатора.
      (635) Если Accept_Mode = False, НЕДОПУСТИМО отбрасывать IPv6
            Neighbor Solicitation и Neighbor Advertisement.
   (640) endif // IPv4?
   (645) ДОЛЖЕН пересылать пакеты с MAC-адресом получателя,
         совпадающим с MAC-адресом виртуального маршрутизатора.
   (650) ДОЛЖЕН воспринимать пакеты, направленные по адресам IPvX,
         связанным с виртуальным маршрутизатором, если он владеет
         адресом IPvX или Accept_Mode = True. В иных случаях
         НЕДОПУСТИМО воспринимать пакеты.
   (655) Если получено событие Shutdown,
      (660) отключается Adver_Timer,
      (665) передаётся ADVERTISEMENT с Priority = 0,
      (670) состояние меняется на {Initialize}.
```

[1] В оригинале ошибочно сказано «или», см. https://www.rfc-editor.org/errata/eid4698. *Прим. перев.*

```
      (675) endif // событие Shutdown.
      (680) Если завершён отсчёт Adver_Timer,
         (685) передаётся ADVERTISEMENT,
         (690) Adver_Timer сбрасывается в Advertisement_Interval.
      (695) endif // завершение отсчёта Adver_Timer
      (700) Если получен анонс ADVERTISEMENT,
         (705) Если Priority = 0,
            (710) передается ADVERTISEMENT,
            (715)  Adver_Timer сбрасывается в Advertisement_Interval,
         (720) иначе // Priority отличается от 0
            (725) Если Priority в ADVERTISEMENT больше локального,
            (730) или
            (735) если Priority в ADVERTISEMENT совпадает с локальным
                  и первичный адрес IPvX у отправителя больше локального
                  первичного адреса IPvX,
               (740) отключается Adver_Timer,
               (745) устанавливается Master_Adver_Interval = интервал
                     анонсов из ADVERTISEMENT,
               (750) пересчитывается  Skew_Time,
               (755) пересчитывается Master_Down_Interval,
               (760) устанавливается Master_Down_Timer = Master_Down_Interval
               (765) состояние меняется на {Backup},
            (770) иначе // новый Master
               (775) отбрасывается ADVERTISEMENT
            (780) endif // новый Master?
         (785) endif // Priority = 0?
      (790) -endif // получен анонс ADVERTISEMENT
   (795) endwhile // состояние Master.
```

7. Передача и приём пакетов VRRP

7.1. Приём пакетов VRRP

При получении пакета VRRP выполняются указанные ниже действия

- Если принят пакет IPv4,
  - **должно** проверяться условие IPv4 TTL = 255,
- иначе // принят пакет IPv6
  - **должно** проверяться условие IPv6 Hop Limit = 255.
- endif
- **Должна** проверяться версия VRRP 3.
- **Должна** проверяться полнота полученного пакета VRRP (фиксированные поля и адреса IPvX).
- **Должна** проверяться контрольная сумма VRRP.
- **Должна** проверяться настройка VRID на приёмном интерфейсе и то, что локальный маршрутизатор не является владельцем адреса IPvX (Priority = 255).

При отрицательном результате любой из проверок получатель **должен** отбросить пакет, **следует** записать событие в системный журнал (log) и **можно** указать ошибку через систему управления сетью.

- **Можно** проверить, что Count IPvX Addrs и список адресов IPvX, соответствуют адресам, заданным для VRID.

Если эта проверка не проходит, получателю **следует** записать событие в системный журнал (log) и **можно** указать ошибку конфигурации через систему управления сетью.

7.2. Передача пакетов VRRP

При передаче пакета VRRP должны выполняться указанные ниже операции.

- Поля пакета VRRP заполняются в соответствии с состоянием конфигурации виртуального маршрутизатора.
- Рассчитывается контрольная сумма VRRP.
- Если защищаемым адресом является IPv4,
  - устанавливается MAC-адрес отправителя в соответствии с MAC-адресом виртуального маршрутизатора;
  - для адреса отправителя IPv4 устанавливается первичный адрес интерфейса IPv4,
- иначе, // IPv6
  - устанавливается MAC-адрес отправителя в соответствии с MAC-адресом виртуального маршрутизатора;
  - для адреса отправителя IPv6 устанавливается адрес интерфейса IPv6 Link-Local.
- endif
- Для протокола IPvX указывается значение VRRP.
- Пакет VRRP передаётся в группу VRRP IPvX (multicast).

Примечание. Пакеты VRRP передаются с MAC-адресом виртуального маршрутизатора в качестве MAC источника, чтобы обучающиеся мосты могли корректно определить сегмент ЛВС, куда подключён виртуальный маршрутизатор.

7.3. MAC-адрес виртуального маршрутизатора

MAC-адрес виртуального маршрутизатора является адресом IEEE 802 MAC в показанном ниже формате.

Для IPv4: 00-00-5E-00-01-{VRID} (шестнадцатеричные цифры со стандартным для Internet порядком битов)
Первые 3 октета выводятся из уникального идентификатора организации IANA OUI (Organizational Unique Identifier). Следующие 2 октета (00-01) указывают адресный блок, выделенный для протокола VRRP с IPv4, {VRID} указывает идентификатор виртуального маршрутизатора. Это позволяет организовать в сети до 255 маршрутизаторов IPv4 VRRP.

Для IPv6: 00-00-5E-00-02-{VRID} (шестнадцатеричные цифры со стандартным для Internet порядком битов)
Первые 3 октета выводятся из IANA OUI. Следующие 2 октета (00-02) указывают адресный блок, выделенный для протокола VRRP с IPv6, {VRID} указывает идентификатор виртуального маршрутизатора. Это позволяет организовать в сети до 255 маршрутизаторов IPv6 VRRP.

7.4. Идентификаторы интерфейсов IPv6

Маршрутизаторы IPv6 с работающим VRRP должны создавать идентификаторы своих интерфейсов обычным путём (например, Transmission of IPv6 Packets over Ethernet Networks [RFC2464]). Им **недопустимо** использовать MAC-адрес виртуального маршрутизатора для создания идентификаторов EUI-64 (Modified Extended Unique Identifier).

Эта спецификация VRRP описывает, как анонсировать и распознавать адреса IPv6 Link-Local маршрутизаторов VRRP и преобразовывать другие адреса IPv6 в MAC-адреса виртуального маршрутизатора.

8. Операционные вопросы

8.1. IPv4

8.1.1. ICMP Redirect

Сообщения ICMP Redirect могут использоваться обычным способом при работе VRRP между группой маршрутизаторов. Это позволяет применять VRRP в средах с асимметричной топологией.

Адресом источника IPv4 в ICMP Redirect следует быть адресу, используемому конечным хостом при выборе следующего узла пересылки (next-hop). Если маршрутизатор VRRP выступает как Master для виртуальных маршрутизаторов, содержащих адреса, которыми он не владеет, маршрутизатор должен определить, какому из виртуальных маршрутизаторов был отправлен пакет, для указания адреса перенаправления. Одним из способов определения использованного виртуального маршрутизатора служит проверка MAC-адреса получателя в вызвавшем перенаправление пакете.

В случаях, когда VRRP применяется для распределения нагрузки между маршрутизаторами в симметричной топологии, может быть полезно отключить перенаправления.

8.1.2. Запросы ARP от хостов

Когда хост передаёт запрос ARP для одного из адресов IPv4 виртуального маршрутизатора, Virtual Router Master **должен** отвечать откликом ARP, указывающим виртуальный MAC-адрес для виртуального маршрутизатора. Отметим, что адресом источника в кадре Ethernet с таким откликом ARP является физический MAC-адрес физического маршрутизатора. Маршрутизатору Virtual Router Master **недопустимо** указывать свой физический MAC-адрес в отклике ARP. Это позволяет клиенту всегда применять один и тот же адрес MAC, независимо от текущего Master.

При загрузке или перезапуске маршрутизатора VRRP ему **не следует** передавать сообщений ARP с использованием своего физического MAC-адреса для принадлежащих ему адресов IPv4. Ему следует передавать лишь сообщения ARP с виртуальным MAC-адресом.

Это может повлечь указанные ниже последствия.

- При настройке интерфейса маршрутизаторам Virtual Router Master следует передавать широковещательный беспричинный запрос ARP с MAC-адресом виртуального маршрутизатора и адресом этого интерфейса IPv4.
- При загрузке системы, когда инициализируются интерфейсы для операций VRRP беспричинные запросы и отклики ARP задерживаются, пока не будут настроены адрес IPv4 и MAC-адрес виртуального маршрутизатора.
- Когда нужен доступ, например, ssh, к конкретному маршрутизатору VRRP, должен применяться адрес IP, заведомо принадлежащий этому маршрутизатору.

8.1.3. Proxy ARP

При использовании Proxy ARP на маршрутизаторе VRRP этот маршрутизатор должен анонсировать MAC-адрес виртуального маршрутизатора в сообщениях Proxy ARP. Иное поведение может приводить к тому, что хосты получат реальный MAC-адрес маршрутизатора VRRP.

8.2. IPv6

8.2.1. ICMPv6 Redirect

Сообщения ICMPv6 Redirect можно применять обычным способом при работе VRRP между группой маршрутизаторов [RFC4443]. Это позволяет применять VRRP в средах с асимметричной топологией (например, маршрутизаторы VRRP не соединены с одними и теми же получателями).

Адресом источника IPv6 в ICMPv6 Redirect следует быть адресу, используемому конечным хостом при выборе следующего узла пересылки (next-hop). Если маршрутизатор VRRP выступает как Master для виртуальных маршрутизаторов, содержащих адреса, которыми он не владеет, маршрутизатор должен определить, какому из виртуальных маршрутизаторов был отправлен пакет, для указания адреса перенаправления. Одним из способов

определения использованного виртуального маршрутизатора служит проверка MAC-адреса получателя в вызвавшем перенаправление пакете.

8.2.2. ND Neighbor Solicitation
Когда хост передаёт сообщение ND Neighbor Solicitation для адреса IPv6 виртуального маршрутизатора, Virtual Router Master **должен** отвечать сообщением ND Neighbor Solicitation, указывающим виртуальный MAC-адрес виртуального маршрутизатора. Маршрутизатору Virtual Router Master **недопустимо** указывать свой физический MAC-адрес в отклике. Это позволяет клиенту всегда применять один и тот же адрес MAC, независимо от текущего Master.

Когда Virtual Router Master передаёт сообщение ND Neighbor Solicitation для адреса хоста IPv6, он **должен** включать виртуальный MAC-адрес виртуального маршрутизатора, если он указывает опцию адреса источника на канальном уровне в сообщение Neighbor Solicitation. **Недопустмо** использовать свой физический MAC-адрес в опции адреса канального уровня для отправителя.

При загрузке или перезапуске маршрутизатора VRRP ему не следует передавать сообщений ND с использованием своего физического MAC-адреса для принадлежащих ему адресов IPv6. Ему следует передавать лишь сообщения ND с виртуальным MAC-адресом.

Это может повлечь указанные ниже последствия.

- При настройке интерфейса маршрутизаторам Virtual Router Master следует передавать незапрошенное сообщение ND Neighbor Advertisement с MAC виртуального маршрутизатора и IPv6 на этом интерфейсе.
- При загрузке системы, когда инициализируются интерфейсы для операций VRRP все сообщения ND Router Advertisement, Neighbor Advertisement и Solicitation должны задерживаться, пока не будут настроены адрес IPv6 и MAC-адрес виртуального маршрутизатора.

Отметим, что при перезапуске Master, когда защищаемый VRRP адрес является адресом интерфейса (Priority = 255) обнаружение дубликатов адресов (duplicate address detection или DAD) может не сработать, поскольку маршрутизатор Backup может ответить, что он владеет этим адресом. Решением является отказ от запуска DAD в этом случае.

8.2.3. Router Advertisement
Когда Backup VRRP становится Master для виртуального маршрутизатора, он отвечает за передачу анонсов Router Advertisement для виртуального маршрутизатора, как указано в параграфе 6.4.3. Master. Маршрутизаторы Backup должны быть настроены для отправки таких же опций Router Advertisement, какие применяет владелец адреса.

Опции Router Advertisement, анонсирующие особые услуги (например, Home Agent Information Option), присутствующие у владельца адреса, ему не следует передавать, пока маршрутизаторы Backup не готовы предоставлять полностью те же услуги и не имеют полной и синхронизированной базы данных для них.

8.3. IPvX

8.3.1. Возможные петли пересылки
Если маршрутизатор VRRP не является владельцем адреса, ему **не следует** пересылать пакеты, направленные по адресу IPvX, для которого он становится Master. Пересылка таких пакетов ведёт к ненужному трафику. Кроме того, в ЛВС, которые получают передаваемые пакеты (например, Token Ring), это может приводить к петлям пересылки, завершающимся лишь по IPvX TTL.

Одним из механизмов для маршрутизаторов VRRP является добавление и удаление отклонения (reject) маршрута к хосту для каждого принятого адреса IPvX при переходе в состояние MASTER и выходе из него.

8.3.2. Рекомендации по значениям приоритета
Значение приоритета 255 указывает конкретный маршрутизатор как владельца адреса IPvX. Нужно соблюдать осторожность, чтобы не указать таким способом больше 1 маршрутизатора на канале для одного VRID.

Маршрутизаторы с приоритетом 255 будут при запуске вытеснять маршрутизаторы с меньшим приоритетом. На канале настраивается не более 1 маршрутизатора с приоритетом 255, особенно при включённом вытеснении. Если нет маршрутизатора с таким приоритетом и вытеснение отключено, его (вытеснения) не будет.

При наличии нескольких маршрутизаторов Backup их значения приоритета следует распределять однородно. Например, если один маршрутизатор Backup имеет принятый по умолчанию приоритет 100 и добавляется другой Backup, приоритет 50 для него будет лучшим выбором, нежели 99 или 100, для более быстрого схождения.

8.4. Взаимодействие VRRPv3 и VRRPv2

8.4.1. Допущения
1. Совместная работа VRRPv2 и VRRPv3 не обязательна.
2. Смешивать VRRPv2 и VRRPv3 следует лишь на время перехода от VRRPv2 к VRRPv3. Смешение двух версий не следует принимать как постоянное решение.

8.4.2. Поддержка VRRPv2 в VRRPv3
Как отмечено выше, эта поддержка предназначена для сценариев обновления и **не** рекомендуется для постоянного развёртывания.

Реализация может включать флаг конфигурации, указывающий, что она принимает и передаёт анонсы VRRPv2 и VRRPv3. Когда виртуальный маршрутизатор настроен так и является Master, он **должен** передавать оба типа с заданной частотой (даже субсекундной).

Когда виртуальный маршрутизатор настроен таким образом и служит Backup, ему следует вводить тайм-аут на основе частоты, анонсируемой маршрутизатором Master. В случае VRRPv2 Master это означает, что он должен транслировать полученное значение тайм-аута (в секундах) в сотые доли секунды. Кроме того, маршрутизатору Backup следует игнорировать анонсы VRRPv2 от текущего Master, если от того приходят также пакеты VRRPv3. Он **может** когда VRRPv3 Master **не** передаёт пакетов VRRPv2, это говорит о том, не согласована поддержка маршрутизаторов VRRPv2.

8.4.3. Вопросы поддержки VRRPv2 в VRRPv3

8.4.3.1. Медленные, высокоприоритетные Master

См. также параграф 5.2.7. Максимальный интервал между анонсами (Max Adver Int).

VRRPv2 Master, взаимодействующий с субсекундным VRRPv3 Backup, является наиболее важным примером.

Реализации VRRPv2 не следует давать более высокий приоритет, чем реализации VRRPv2/VRRPv3, с которой она взаимодействует, если VRRPv2/VRRPv3 использует субсекундную скорость.

8.4.3.2. Перегрузка VRRPv2 Backup

Представляется возможным, что маршрутизатор VRRPv3 Master, передающий с интервалом в сотые доли секунды, может перегрузить VRRPv2 Backup с неочевидными результатами.

В случае обновления следует поначалу запускать маршрутизаторы VRRPv3 Master с более низкой частотой (например, 100 = 1 секунда), пока маршрутизаторы VRRPv2 не будут обновлены. Затем, когда станет ясно, что VRRPv3 работает правильно, поддержку VRRPv2 можно отключить и задать субсекундную скорость.

9. Вопросы безопасности

VRRP для IPvX сейчас не включает проверки подлинности. Прежние версии VRRP (для IPv4) включали несколько типов аутентификации от простой до строгой. Опыт эксплуатации и дальнейший анализ показали, что это не обеспечивает достаточной защиты для преодоления уязвимостей, связанных с неверно заданными секретами, что вело к выбору нескольких маршрутизаторов Master. По природе протокола VRRP даже криптозащита сообщений VRRP не мешает враждебным узлам вести себя как VRRP Master и создавать несколько ведущий. Аутентификация сообщений VRRP может помешать враждебному узлу перевести все корректно работающие маршрутизаторы в состояние Backup. Однако наличие нескольких Master может вызывать столько же проблем, как и отсутствие маршрутизаторов и аутентификация не может это предотвратить. Кроме того, даже если враждебный узел не может нарушить работу VRRP, он способен помешать ARP и создать такой же эффект, как переход всех маршрутизаторов в состояние Backup.

Некоторые коммутаторы L2 поддерживают фильтрацию, например, сообщений ARP и/или ND от конечных хостов по портам коммутатора. Этот механизм может также фильтровать сообщения VRRP от портов коммутатора, связанных с конечными хостами и его можно рассматривать в системах с недоверенными хостами.

Следует отметить, что эти атаки ничем не хуже и являются подмножеством атак, которые любой узел, подключенный к ЛВС, может организовать независимо от VRRP. Атаки, которые злонамеренный узел ЛВС может организовать, включают неразборчивый (promiscuous) приём пакетов для любого MAC-адреса маршрутизатора, передачу пакетов с MAC-адресом маршрутизатора в качестве адреса источника в заголовке L2, чтобы вынудить коммутаторы L2 передавать адресованные маршрутизатору пакеты злонамеренному узлу, передачу перенаправлений (redirect), вынуждающих хосты передавать свой трафик не туда, передачу незапрошенных откликов ND и ответы на запросы ND и т. п. Все это возможно независимо от реализации VRRP и протокол VRRP не добавляет таких уязвимостей.

Независимо от типа аутентификации, VRRP включает механизм (установка TTL = 255 и проверка при получении), защищающий VRRP от внедрения пакетов из удалённой сети. Это избавляет от большинства удалённых атак.

VRRP не обеспечивает конфиденциальности. Она не требуется для корректной работы VRRP и в сообщениях VRRP нет сведений, которые нужно было бы скрывать от других узлов ЛВС.

В контексте IPv6 при развёртывании защищённого обнаружения соседей (SEcure Neighbor Discovery или SEND) протокол VRRP совместим с режимами trust anchor и trust anchor or cga в SEND [RFC3971]. Конфигурация SEND должна давать маршрутизаторам Master и Backup одинаковое делегирование префикса в сертификатах, чтобы Master и Backup анонсировали один набор префиксов подсетей. Однако маршрутизаторам Master и Backup следует иметь свои пары ключей, чтобы секретный ключ не был общим.

10. Участники работы и благодарности

Редактор благодарен V. Ullanatt за рецензирование ранней версии. Этот документ содержит мало нового материала (новый текст содержится в Приложении A) и был создан путём слияния xml-представления [VRRP-IPv6] и [RFC3768] с последующим внесением изменений, обсуждавшихся недавно в почтовой конференции рабочей группы VRRP. R. Hinden является автором, а J. Cruz - редактором первого. Участники разработки второго указаны ниже.

Связанный с IPv6 текст 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.

Автор [VRRP-IPv6] признателен Erik Nordmark, Thomas Narten, Steve Deering, Radia Perlman, Danny Mitzel, Mukesh Gupta, Don Provan, Mark Hollinger, John Cruz, Melissa Johnson за полезные предложения.

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

11. Взаимодействие с IANA

Агентство IANA выделило групповой адрес IPv6 link-local для работы VRRP по протоколу IPv6

```
FF02:0:0:0:0:0:0:12
```

Присвоенные значения адресов вводятся в соответствии с параграфом 5.1.2.2. Destination Address.

Агентство IANA зарезервировало блок индивидуальных адресов IANA Ethernet для работы VRRP по протоколу IPv6

```
00-00-5E-00-02-00 - 00-00-5E-00-02-FF (шестнадцатеричные)
```

Назначения указаны на сайте http://www.iana.org.

12. Литература

12.1. Нормативные документы

[ISO.10038.1993] International Organization for Standardization, "Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges", ISO Standard 10038, 1993.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460[1], December 1998.

[RFC3768] Hinden, R., "Virtual Router Redundancy Protocol (VRRP)", RFC 3768, April 2004.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4443] 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.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

12.2. Дополнительная литература

[VRRP-IPv6] Hinden, R. and J. Cruz, "Virtual Router Redundancy Protocol for IPv6", Work in Progress, March 2007.

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

[IPX] Novell Incorporated, "IPX Router Specification Version 1.10", October 1992.

[RFC1071] Braden, R., Borman, D., Partridge, C., and W. Plummer, "Computing the Internet checksum", RFC 1071, September 1988.

[RFC1256] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[RFC1469] Pusateri, T., "IP Multicast over Token-Ring Local Area Networks", RFC 1469, June 1993.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2281] Li, T., Cole, B., Morton, P., and D. Li, "Cisco Hot Standby Router Protocol (HSRP)", RFC 2281, March 1998.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[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, April 1998.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[TKARCH] IBM Incorporated, "IBM Token-Ring Network, Architecture Specification, Publication SC30-3374-02, Third Edition", September 1989.

Приложение A. Работа через FDDI, Token Ring, ATM LANE

A.1. Работа через FDDI

Интерфейсы FDDI удаляют из кольца FDDI кадры с MAC-адресом источника, совпадающим с аппаратным адресом устройства. При некоторых условиях, таких как изоляция маршрутизатора, повреждение кольца, протокольные переходы и т. п., VRRP может приводить к наличию нескольких маршрутизаторов Master. Если Master устанавливает MAC-адрес виртуального маршрутизатора на устройстве FDDI, анонсы ADVERTISEMENTS от других ведущих будут удаляться из кольца при выборе Master и схождения не произойдет.

Для предотвращения этого реализации **следует** настраивать MAC-адрес виртуального маршрутизатора с использованием индивидуального (unicast) фильтра MAC в устройстве FDDI вместо смены аппаратного адреса MAC. Это предотвратит удаление маршрутизатором Master анонсов ADVERTISEMENTS, исходящих от других.

A.2. Работа через Token Ring

Некоторые характеристики Token Ring осложняют работу VRRP, как указано ниже.

- Для переключения на новый маршрутизатор Master, размещённый в другом сегменте моста Token-Ring при использовании мостов source-route требуется механизм обновления кэшированных данных source-route.
- Не поддерживается общего для старых и новых реализаций адаптера Token-Ring не поддерживается общий механизм групповой передачи. Хотя многие из новых адаптеров Token-Ring поддерживают групповые адреса,

[1]Заменён RFC 8200. *Прим. перев.*

поддержка функциональных адресов Token-Ring является единственным общедоступным механизмом групповой передачи. Ограниченное число функциональных адресов Token-Ring может вызывать конфликты при их использовании.

Из-за этих сложностей предпочтительным режимом работы через Token Ring является применение функциональных адресов Token-Ring для виртуальных MAC-адресов VRID. В этих функциональных адресах Token-Ring два старших бита первого октета MAC имеют значение 1[1]. Адреса занимают диапазон от 03-00-00-00-00-80 до 03-00-02-00-00-00 (канонический формат). Однако в отличие от групповых адресов для каждой битовой позиции имеется лишь 1 функциональный адрес. Адреса от 03-00-00-10-00-00 до 03-00-02-00-00-00 зарезервированы архитектурой Token-Ring [TKARCH] для определяемых пользователями приложений. Однако, поскольку имеется лишь 12 определяемых пользователем функциональных адресов Token-Ring, могут существовать отличные от IPvX протоколы, применяющие те же адреса. Поскольку протокол Novell IPX [IPX] использует функциональный адрес 03-00-00-10-00-00, при работе VRRP через Token Ring следует избегать его применения. В общем случае пользователи Token-Ring VRRP отвечают за конфликты при распознавании других определяемых пользователем функциональных адресов Token-Ring.

VRID напрямую сопоставляются с функциональными адресами Token-Ring. Для снижения вероятности конфликтов выделение начинается с большего функционального адреса. Большинство отличных от IPvX протоколов используют первый адрес или пару пользовательских функциональных адресов и предполагается, что пользователи VRRP будут выбирать VRID последовательно, начиная с 1.

VRID	***Функциональный адрес Token-Ring***
1	03-00-02-00-00-00
2	03-00-04-00-00-00
3	03-00-08-00-00-00
4	03-00-10-00-00-00
5	03-00-20-00-00-00
6	03-00-40-00-00-00
7	03-00-80-00-00-00
8	03-00-00-01-00-00
9	03-00-00-02-00-00
10	03-00-00-04-00-00
11	03-00-00-08-00-00

Более кратко, октеты 3 и 4 функционального адреса имеют значение (0x4000 >> (VRID - 1)) в неканоническом формате.

Поскольку функциональные адреса не могут применяться в качестве адреса источника на уровне MAC в анонсах VRRP адресом источника служит реальный MAC-адрес. Это не является проблемой для мостов, поскольку пакеты, направленные по функциональным адресам, будут передаваться по пути проводника (explorer) связующего дерева [ISO.10038.1993].

Режим работы с функциональным адресом должен быть реализован на маршрутизаторах VRRP в сети Token Ring.

Кроме того, маршрутизаторы могут поддерживать индивидуальный (unicast) режим работы, чтобы использовать преимущества новых реализаций адаптеров Token-Ring, поддерживающих избирательное получение для множества индивидуальных адресов MAC, и избежать как группового трафика, так и конфликтов, связанных с применением функциональных адресов Token-Ring. Индивидуальный режим использует такое же сопоставление VRID с виртуальными MAC-адресами, как Ethernet. Однако имеется важное различие - пакеты запросов и откликов ND содержат виртуальный MAC-адрес в качестве адреса источника. Причина этого заключается в том, что реализации драйверов Token-Ring сохраняют кэш сопоставления адресов MAC и данных source-routing независимо от кэша ND.

Следовательно, эти реализации должны получать пакет с виртуальным MAC-адресом источника для передачи по этому адресу в сети с мостами source-route.

Для индивидуального режима Token Ring следует учитывать одно ограничение. Если маршрутизаторы VRID расположены в разных сегментах source-route-bridge и имеются реализации хостов, хранящие свои сведения source-route в кэше ND и не слушающие беспричинные ND, эти хосты не будут корректно обновлять свои данные ND source-route при смене ведущего маршрутизатора. Единственным решением является размещение всех маршрутизаторов с одним VRID в одном сегменте source-route-bridge и применение методов предотвращения критических отказов в этом сегменте. Эти методы выходят за рамки документа.

При индивидуальном и групповом режиме работы анонсы VRRP, передаваемые по адресу 224.0.0.18, следует инкапсулировать в соответствии с [RFC1469].

A.3. Работа через ATM LANE

Работа VRRP через ATM LANE на маршрутизаторах с интерфейсами ATM LANE и/или маршрутизаторах за прокси-LEC (LAN Emulation Client) выходит за рамки этого документа.

Адрес автора

Stephen Nadas (editor)
Ericsson
900 Chelmsford St., T3 4th Floor
Lowell, MA 01851
USA
Phone: +1 978 275 7448
EMail: stephen.nadas@ericsson.com

Перевод на русский язык

[1]Порядок битов в адресе Token Ring отличается. Для преобразования значений можно воспользоваться таблицей. *Прим. перев.*

Николай Малых

nmalykh@protokols.ru