Функции и возможности протокола HSRP (Hot Standby Router Protocol)

Содержание

Введение

В этом документе описываются функции и возможности протокола HSRP (Hot Standby Router Protocol).

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Данный документ не ограничивается отдельными версиями программного и аппаратного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические термины Cisco. Условные обозначения.

Теория и принцип работы HSRP

Один из способов добиться доступности сети, близкой к 100%, — использование протокола HSRP, который обеспечивает избыточность IP-сетей, предоставляя возможность немедленного прозрачного восстановления пользовательского трафика в случае отказа первого перехода в оконечных сетевых устройствах или каналах доступа.

Благодаря совместному использованию IP-адреса и MAC-адреса (уровень 2), два и более маршрутизаторов могут действовать как единый "виртуальный" маршрутизатор. Члены группы виртуальных маршрутизаторов непрерывно обмениваются сообщениями о состоянии. Это позволяет маршрутизаторам подменять другие маршрутизаторы при их запланированном или незапланированном отключении. Узлы продолжают переадресовать IP-пакеты на согласованный IP- и MAC-адрес, и аварийное переключение устройств, производящих маршрутизацию, происходит незаметно для пользователей и приложений.

Динамические механизмы обнаружения маршрутизатора

Ниже приведены описания динамических механизмов обнаружения маршрутизатора, которые доступны узлам. Многие из этих механизмов не обеспечивают устойчивость сети к восстановлению, в которой нуждаются сетевые администраторы. Это может быть вызвано тем, что протокол не был изначально предназначен для обеспечения устойчивости сети, либо работа протокола поддерживается не всеми узлами в сети. Помимо сведений, которые приводятся ниже, важно учесть, что многие узлы допускают только настройку шлюза по умолчанию.

ARP-прокси (Address Resolution Protocol)

Некоторые IP-узлы используют для выбора маршрутизатора протокол ARP-прокси. Если узел выполняет задачу ARP-прокси, он посылает запрос ARP на IP-адрес удаленного узла, с которым необходимо установить связь. Маршрутизатор A в сети отвечает от имени удаленного узла и сообщает свой собственный MAC-адрес. При использовании ARP-прокси, узел ведет себя так, как если бы удаленный узел был подключен к тому же сегменту сети. Если на маршрутизаторе A возникает сбой, узел продолжит пересылать пакеты удаленному узлу на MAC-адрес маршрутизатора A, несмотря на то, что эти пакеты пересылаются "в никуда" и теряются. Можно либо дождаться запроса протоколом ARP MAC-адреса другого маршрутизатора (маршрутизатора Б) в локальном сегменте путем передачи нового ARP-запроса, либо перезагрузить узел, что вынудит его послать ARP-запрос. В обоих случаях узел будет не в состоянии обмениваться данными с удаленным узлом в течение значительного периода времени, несмотря на то, что ситуация предусмотрена протоколом, а маршрутизатор Б готов передавать пакеты, которые должны были проходить через маршрутизатор A.

Протокол DRP (Dynamic Routing Protocol)

Некоторые IP-узлы используют для обнаружения маршрутизаторов такие протоколы, RIP (Dynamic Routing Protocol) и OSPF (Open Shortest Path First). Недостаток протокола RIP заключается в том, что он медленно адаптируется к изменениям топологии. Выполнение протокола DRP на всех узлах может оказаться неприемлемым по многим причинам, включая административные издержки, издержки обработки данных, проблемы безопасности или отсутствие поддержки протокола на некоторых платформах.

IRDP (ICMP Router Discovery Protocol)

Некоторые современные IP-узлы используют протокол IRDP (RFC 1256) для поиска нового маршрутизатора, когда текущий становится недоступен. Узел, на котором запущен протокол IRDP, отслеживает мультиадресные сообщения приветствия от текущего маршрутизатора, и выбирает альтернативный маршрутизатор, когда перестает получать эти сообщения. Значения таймера по умолчанию протокола IRDP делают его для обнаружения сбоев при первом переходе. По умолчанию объявления создаются один раз в 7-10 минут, срок действия объявлений по умолчанию — 30 минут.

Протокол DHCP (Dynamic Host Configuration Protocol)

Протокол DHCP (RFC 1531) обеспечивает механизм передачи данных конфигурации на узлы сети TCP/IP. Узел, на котором работает DHCP-клиент, запрашивает данные конфигурации с DHCP-сервера при загрузке в сеть. Обычно эти данные включают IP-адрес и шлюз по умолчанию. Механизм переключения на альтернативный маршрутизатор при сбое шлюза по умолчанию отсутствует.

Принцип работы HSRP

Многочисленный класс традиционных узлов не поддерживает динамическое обнаружение, но поддерживает настройку маршрутизатора по умолчанию. Запуск механизма динамического обнаружения маршрутизатора на всех узлах может оказаться неприемлемым по многим причинам, включая административные издержки, издержки обработки данных, проблемы безопасности или отсутствие поддержки протокола на некоторых платформах. HSRP предоставляет таким узлам возможности аварийного переключения.

При использовании HSRP несколько маршрутизаторов могут работать совместно, создавая иллюзию одного виртуального маршрутизатора для узлов локальной сети. Такой набор называют группой HSRP или резервной группой. Один маршрутизатор, выбранный из группы, отвечает за переадресацию пакетов, отправленных узлами на виртуальный маршрутизатор. Этот маршрутизатор известен как активный маршрутизатор. Еще один маршрутизатор выбирается резервным маршрутизатором. В случае сбоя активного маршрутизатора резервный берет на себя обязанности активного маршрутизатора по переадресации пакетов. Хотя HSRP может работать на любом количестве маршрутизаторов, только активный маршрутизатор может переадресовать пакеты, отправленные на виртуальный маршрутизатор.

Чтобы минимизировать сетевой трафик, только активные и резервные маршрутизаторы посылают периодические сообщения HSRP после того, как протокол завершает процесс выбора. При сбое активного маршрутизатора, происходит переключение на резервный маршрутизатор. Если резервный маршрутизатор отключается или становится активным маршрутизатором, другой маршрутизатор выбирается в качестве резервного.

В некоторых локальных сетях поддерживается совместная работа и даже перекрытие нескольких групп "горячего" резерва. Каждая группа эмулирует один виртуальный маршрутизатор. Отдельные маршрутизаторы могут входить в несколько групп. В этом случае в группах используются отдельные состояния и таймеры.

Каждая резервная группа имеет единственный известный MAC-адрес, а также IP-адрес.

Адресация HSRP

В большинстве случаев после настройки маршрутизаторов в качестве членов группы HSRP они прослушивают MAC-адрес HSRP этой группы, а также свои собственные прошитые MAC-адреса. Исключением являются маршрутизаторы, Ethernet-контроллеры которых могут распознавать только один MAC-адрес (например, контроллер Lance на маршрутизаторе Cisco 2500 и Cisco 4500). Эти маршрутизаторы используют MAC-адреса HSRP, когда играют роль активных маршрутизаторов и прошитый адрес, когда не являются активными

HSRP использует следующие MAC-адреса для всех сред, кроме Token Ring:

```
0000.0c07.ac**   (where ** is the HSRP group number)
```

В интерфейсах Token Ring в качестве MAC-адреса HSRP используются функциональные адреса. Функциональные адреса — единственный доступный механизм мультиадресной рассылки. Доступное количество функциональных адресов Token Ring ограниченно, многие из них зарезервированы для других функций. Для протокола HSRP можно использовать следующие три адреса:

```
c000.0001.0000   (group 0)
c000.0002.0000   (group 1)
c000.0004.0000   (group 2)
```

Примечание: Если HSRP работает в многокольцевой среде мостовой передачи с маршрутизацией SRB (source-route bridging), и маршрутизаторы HSRP находятся на разных кольцах, использование функциональных адресов может привести к конфликтам в поле RIF (Routing Information Field). Например, в среде SRB возможно размещение резервного маршрутизатора HSRP активного

маршрутизатора в разных кольцах. Когда этот резервный маршрутизатор становится активным, станции на одном кольце с прежним активным маршрутизатором требуют обновления RIF для отправки пакетов на новый активный маршрутизатор. Однако, станции не знают о необходимости отправки запроса нового RIF, поскольку резервный (новый активный) маршрутизатор использует тот же функциональный адрес, что и предыдущий. Поэтому была введена команда **use-bia**.

Таблица функций HSRP и версий Cisco IOS

В этом документе показано, какие функции HSRP поддерживаются в тех или иных версиях ПО Cisco IOS®. Щелкните функцию, чтобы посмотреть подробное описание. Номер промежуточной версии указывает версию, в которой функция появилась впервые, или версию, в которой изменились возможности этой функции.

Функция	**10.0**	**10.2**	**10.3**	**11.0**	**11.1**	**11.2**	**11.3**	**12.0**	**12.0T**	**12.1**	**12.1T**
Приоритетное прерывание обслуживания	X	X	X	X	X	X	X	X	X	X	X
Несколько групп (MHSRP)	—	—	X	X	X	X	X	X	X	X	X
Ethernet 802.10 SDE	—	—	—	—	X	X	X	X	X	X	X
Отслеживание интерфейсов	—	—	—	—	X	X	X	X	X	X	X
Использование BIA	—	—	—	—	8.0	X	X	X	X	X	X
Задержка приоритетного прерывания обслуживания	—	—	—	—	—	X	X	6.1	X	X	X
Ethernet LANE	—	—	—	—	—	X	X	X	X	X	X
Token Ring LANE	—	—	—	—	—	—	X	X	X	X	X
ISL	—	—	—	—	—	—	X	X	X	X	X
Поддержка системного журнала	—	—	—	—	—	—	X	X	X	X	X
Интервал обновления MAC	—	—	—	—	—	—	—	1.0	X	X	X

SNMP MIB	—	—	—	—	—	—	—	—	3.0	X	X
MHSRP и использование BIA	—	—	—	—	—	—	—	—	3.4	X	X
IP-избыточность	—	—	—	—	—	—	—	—	3.4	X	X
BVI	—	—	—	—	—	—	—	—	6.2	X	X
802.1Q	—	—	—	—	—	—	—	—	8.1	X	X
Расширенная отладка HSRP	—	—	—	—	—	—	—	—	—	0.2	X
Переадресация HSRP ICMP	—	—	—	—	—	—	—	—	—	—	3
Виртуальные частные сети HSRP MPLS	—	—	—	—	—	—	—	—	—	—	3

Загрузочные образы Cisco IOS и функциональные возможности HSRP

Функциональность HSRP была включена в загрузочные образы Cisco IOS до интеграции Cisco Bug ID CSCec16720 (только для зарегистрированных клиентов). Cisco Bug ID CSCec16720 подразумевает к удаление HSRP из загрузочных образов за исключением:

- c7200-boot-mz
- c7200-kboot-mz
- c10k-eboot-mz
- c4500-boot-mz
- c7200-boot-mz
- c7200-kboot-mz
- c7400-kboot-mz
- ubr7200-boot-mz
- c6400r-boot-mz
- rpm-boot-mz
- rpmxf-boot-mz
- rsp-boot-mz
- urm-wboot-mz
- c5350-boot-mz

- c5400-boot-mz
- c7301-boot-mz
- c5850-boot-mz
- c4gwy-cboot-mz
- ubr910-rboot-mz
- ubr910-rboot-mz
- ubr925-k8boot-mz
- c5850tb-boot-mz

Функции HSRP

Приоритетное прерывание обслуживания

Функция приоритетного прерывания обслуживания HSRP позволяет маршрутизатору с самым высоким приоритетом немедленно становиться активным маршрутизатором. В первую очередь приоритет определяется по установленному пользователем значению приоритета, а затем по IP-адресу. В обоих случаях, чем больше значение, тем выше приоритет.

При прерывании обслуживания маршрутизатор с более высоким приоритетом отправляет сообщение coup маршрутизатору с более низким приоритетом. Когда активный маршрутизатор с меньшим приоритетом получает сообщение coup или сообщение приветствия от активного маршрутизатора с более высоким приоритетом, он переходит в состояние разговора и отправляет сообщение об отказе.

Задержка приоритетного прерывания обслуживания

Функция задержки приоритетного прерывания обслуживания позволяет отложить прерывание на указанное в настройках время, что дает маршрутизатору возможность заполнить таблицу маршрутизации перед переходом в режим активного маршрутизатора.

До версии 12.0(9) ПО Cisco IOS задержка начиналась в момент перезагрузки маршрутизатора. В версии Cisco IOS 12.0(9) задержка начинается, одновременно с первой попыткой приоритетного прерывания обслуживания.

Чтобы настроить приоритет и приоритетное прерывание обслуживания HSRP, используйте команду **standby [*группа*] [priority *значение*] [preempt [delay [minimum] *секунды*] [sync *секунды*]]**.

Дополнительные сведения о настройке HSRP см. в Документации по HSRP.

Отслеживание интерфейсов

Отслеживание интерфейсов позволяет настроить другой интерфейс на маршрутизаторе, который будет отслеживаться процессом HSRP для изменения приоритета HSRP для заданной группы.

Если происходит сбой линейного протокола указанного интерфейса, приоритет HSRP этого маршрутизатора уменьшается, что позволяет другому маршрутизатору HSRP с более высоким приоритетом стать активным (если для него включено приоритетное прерывание обслуживания).

Для настройки отслеживания интерфейса HSRP используйте команду **standby [group] track interface [priority]**.

Когда несколько отслеживаемых интерфейсов отключается, приоритет уменьшается на совокупную величину. При явном задании значения декремента значение уменьшается на заданную величину при отказе интерфейса, при этом происходит накопление декрементов. Если явное значение декремента не задано, приоритет уменьшается на 10 для каждого интерфейса, вышедшего из строя. Декременты накапливаются.

В следующем примере используется конфигурация со значением декремента по умолчанию (10).

Примечание: Если номер группы HSRP не указан, по умолчанию устанавливается номер группы 0.

```
interface ethernet0
    ip address 10.1.1.1 255.255.255.0
    standby ip  10.1.1.3
    standby priority 110
    standby track serial0
    standby track serial1
```

Поведение HSRP в этой конфигурации:

- 0 неисправных интерфейсов = уменьшения нет (приоритет равен 110)
- 1 неисправный интерфейс = уменьшение на 10 (приоритет снижается до 100)
- 2 неисправных интерфейса = уменьшение на 10 (приоритет снижается до 90)

Такое поведение HSRP наблюдается, даже если значения декремента заданы явно, как описано ниже.

```
interface ethernet0
    ip address 10.1.1.1 255.255.255.0
    standby ip  10.1.1.3
    standby priority 110
    standby track serial0 10
    standby track serial1 10
```

До версии Cisco IOS 12.1 при запуске маршрутизатора с неработающим интерфейсом отслеживание интерфейса HSRP воспринимало интерфейс как работающий.

Этот дефект имеет идентификатор Cisco Bug ID CSCdp32289 (только для зарегистрированных клиентов).

Использование прошитого адреса

Функция "прошитый адрес" (BIA) позволяет группам HSRP использовать прошитый MAC-адрес интерфейса вместо MAC-адреса HSRP. Функция BIA была впервые включена в версию Cisco IOS 11.1(8). Чтобы настроить HSRP на использование BIA, введите команду **standby use-bia [scope interface]**.

Команда **use-bia** была введена, чтобы избежать ограничений на использование функционального адреса в качестве MAC-адреса HSRP на интерфейсах Token Ring.

Примечание: Если HSRP работает в многокольцевой среде мостовой передачи с маршрутизацией SRB (source-route bridging), и маршрутизаторы HSRP находятся на разных кольцах, использование функциональных адресов может привести к конфликтам в поле RIF (Routing Information Field). Поэтому была введена команда **use-bia**.

Кроме того, функция **use-bia** позволяет использовать MAC-адрес DECnet (BIA) в качестве MAC-адреса HSRP, что позволяет применять функции DECnet, XNS и HSRP на одном маршрутизаторе. Команда **use-bia** полезна также в сетевых сценариях, когда BIA-адрес устройства настроен на других устройствах в локальной сети.

Однако, команда **use-bia** имеет несколько недостатков:

- Когда маршрутизатор становится активным, виртуальный IP-адрес переводится на другой MAC-адрес. Маршрутизатор, ставший

активным, посылает ненужный ARP-отклик. Не все узлы могут корректно обработать такой отклик.

- При настройке **use-bia** происходит прерывание работы ARP-прокси. Резервный маршрутизатор не может заменить утерянную базу данных ARP-прокси неисправного активного маршрутизатора.
- До версии Cisco IOS 12.0(3.4)T при использовании **use-bia** была разрешена только одна группа HSRP.

При настройке команды **use-bia** в субинтерфейсе она отображается только на главном интерфейсе и применяется ко всем субинтерфейсам. В версии 12.0(6.2) Cisco IOS или выше в команду **use-bia** добавлены дополнительные ключевые слова, определяющие диапазон интерфейсов, которые позволяют применять команду к одному субинтерфейсу.

Эта ошибка имеет идентификатор Cisco bug ID CSCdp32289 (только для зарегистрированных клиентов).

Несколько групп HSRP

Возможность использования нескольких групп HSRP (MHSRP) была добавлена в версии Cisco IOS 10.3. Эта функция повышает избыточность и возможности разделения нагрузки внутри сетей, а также позволяет более эффективно использовать избыточные маршрутизаторы. Маршрутизатор, который переадресует трафик одной группы HSRP, может находится в состоянии резервный (standby) или прослушивание (listen) в другой группе.

В версии Cisco IOS 12.0(3.4)T команду **use-bia** можно использовать, если включены несколько групп HSRP.

Настраиваемый MAC-адрес

Как правило, HSRP используется, чтобы помочь конечным станциям обнаружить шлюз первого перехода при IP-маршрутизации. Для конечных станций указывается маршрутизатор по умолчанию. Однако, HSPR может обеспечить избыточность первого перехода для других протоколов. Некоторые протоколы, такие APPN, используют MAC-адрес для определения первого перехода маршрутизации.

В этом случае часто возникает необходимость в задании виртуального MAC-адреса при помощи команды **standby mac-address**. Виртуальный IP-адрес для этих протоколов не имеет значения. Фактический синтаксис команды имеет следующий вид: **standby [group] mac-address mac-address**.

Примечание: Эту команду нельзя использовать для интерфейса Token Ring.

Поддержка системного журнала

Поддержка сообщений системного журнала, содержащих сведения HSRP, была добавлена в версии Cisco IOS 11.3. Эта функция обеспечивает более эффективное ведения журнала и отслеживание для текущих активных и резервных маршрутизаторов на серверах системного журнала.

Отладка HSRP

До версии Cisco IOS 12.1 команда отладки HSRP была относительно простой. Чтобы включить отладку HSRP можно было воспользоваться командой **debug standby**, которая выводила выходные данные о состоянии HSRP и пакетах для всех резервных групп на всех интерфейсах.

Условие отладки, добавленное в версии Cisco IOS 12.0(2.1), позволяет фильтровать выходные данные команды **standby debug** в зависимости от интерфейса и числа групп. В этой команде используется парадигма **debug condition**, представленная в версии Cisco IOS 12.0, как показано в следующем примере. **debug condition standby *interface group***. Необходимо указать допустимый интерфейс с поддержкой HSRP. Группа может быть любой (0-255).

Можно задавать условия отладки и для несуществующих групп, что позволяет получать данные отладки во время инициализации новой группы.

Необходимо включить параметр **standby debug**, чтобы выводились все выходные данные отладки. Если не указаны условия **standby debug**, выходные данные отладки создаются для всех групп на всех интерфейсах. Если указано хотя бы одно условие **standby debug**, выходные данные команды **standby debug** фильтруются в соответствии с условиями **standby debug**.

Расширенная отладка HSRP

До версии Cisco IOS 12.1(0.2) отладка HSRP была ограничена из-за потерь данных, связанных с шумом от периодических сообщений приветствия. Поэтому в версию Cisco IOS 12.1(0.2) была добавлена функция расширенной отладки.

В следующей таблице описаны параметры расширенной отладки.

Команда	Описание
debug standby	Отображает сведения обо всех ошибках, событиях и пакетах HSRP.
debug standby terse	Отображает сведения обо всех ошибках, событиях и пакетах HSRP, кроме пакетов приветствия и объявления.
debug standby errors	Отображает сведения обо всех ошибках HSRP.
debug standby events [[all | terse] | [icmp | protocol | redundancy | track]] [detail]	Отображает сведения о событиях HSRP.
debug standby packets [[all | terse] | [advertise | coup | hello | resign]] [detail]	Отображает сведения о пакетах HSRP.

Выходные данные команды **debug** можно фильтровать, с помощью условной отладки интерфейса и групп HSRP. Чтобы включить условную отладку интерфейса, используйте команду **debug condition interface *interface***. Чтобы включить условную отладку HSRP, используйте команду **debug condition standby *interface group***.

Условие отладки интерфейса применяется, только условия **standby debug** не заданы. В версии Cisco IOS 12.1(1.3) в отладку HSRP внесены дополнительные улучшения, основанные на улучшениях таблицы состояний HSRP.

Эта ошибка имеет идентификатор Cisco bug ID CSCdp32289 (только для зарегистрированных клиентов).

Эти усовершенствования подразумевают отображение данных о событиях таблицы состояний HSRP. В выходных данных ниже параметры **a/**, **b/**, **c/** и т. д. относятся к событиям конечного автомата HSRP, описанных в стандарте RFC 2281 .

```
SB1: Ethernet0/2 Init: a/HSRP enabled
SB1: Ethernet0/2 Active: b/HSRP disabled (interface down)
SB1: Ethernet0/2 Listen: c/Active timer expired (unknown)
SB1: Ethernet0/2 Active: d/Standby timer expired (20.0.0.3)
SB1: Ethernet0/2 Speak: f/Hello rcvd from higher pri Speak router
SB1: Ethernet0/2 Active: g/Hello rcvd from higher pri Active router
SB1: Ethernet0/2 Speak: h/Hello rcvd from lower pri Active router
SB1: Ethernet0/2 Standby: i/Resign rcvd
SB1: Ethernet0/2 Active: j/Coup rcvd from higher pri router
SB1: Ethernet0/2 Standby: k/Hello rcvd from higher pri Standby router
SB1: Ethernet0/2 Standby: l/Hello rcvd from lower pri Standby router
```

```
SB1: Ethernet0/2 Active: m/Standby mac address changed
SB1: Ethernet0/2 Active: n/Standby IP address configured
```

Аутентификация

Аутентификация HSRP использует общие нешифрованные ключи, которые включаются в пакеты HSRP. Эта функция предотвращает получение маршрутизатором с более низким приоритетом резервного IP-адреса и значений резервного таймера от маршрутизатора с более высоким приоритетом.

Настройка строки аутентификации HSRP выполняется с помощью команды **standby authentication *string***.

Избыточность IP

HSRP обеспечивает независимую избыточность маршрутизации IP без учета состояния. Сам протокол HSRP ограничен поддержкой собственного состояния. Он предполагает, что все маршрутизаторы создают и поддерживают собственные таблицы маршрутизации независимо от других маршрутизаторов. Функция избыточности IP предоставляет механизм, который позволяет HSRP обслуживать клиентские приложения, обеспечивая аварийное переключение с учетом состояния.

Избыточность IP не предоставляет одноранговым приложениям механизм обмена данными о состоянии. Реализация этой функции возложена на сами приложения. Это необходимо, если приложения должны обеспечивать аварийное переключение с учетом состояния.

В настоящий момент (январь 2006 г.) избыточность IP реализована только для приложения Mobile IP Home Agent. Ниже приводится пример конфигурации:

```
configure terminal
router mobile
ip mobile home-agent standby hsrp-group1
!
interface e0/2
no shutdown
ip address 20.0.0.1 255.0.0.0
standby 1 ip 20.0.0.11
standby 1 name hsrp-group1
```

Примечание: В версии Cisco IOS 12.1(3)T ключевое слово **redundancy** используется наряду с ключевым словом **standby**. Ключевое слово **standby** будет исключено в следующих выпусках Cisco IOS. Правильная форма команды будет выглядеть следующим образом: **ip mobile home-agent redundancy hsrp-group1**.

В будущем среди сценариев использования избыточности IP могут появиться:

- NAT — избыточные шлюзы.
- IPSEC — синхронизация данных о состоянии для совместной работы с HSRP.
- DHCP-сервер — внедрение DHCP-серверов в различных маршрутизаторах.
- NBAR, CBAC — зеркалирование состояний брандмауэра при асимметричной маршрутизации.
- GPRS — способы отслеживания состояния TCP.
- PIX

Таблицы SNMP MIB

Поддержка таблиц SNMP MIB была добавлена в версии Cisco IOS 12.0(3.0)T. С протоколом HSRP связаны две базы MIB:

- ciscoMgmt 106: Модуль MIB для управления HSRP
- ciscoMgmt 107: Расширенный модуль MIB для управления HSRP

До выхода версии Cisco IOS 12.0(6.1)T обход расширенной базы HSRP MIB при наличии виртуального интерфейса мостовой группы (BVI) вызывал сбой маршрутизатора.

Эта ошибка имеет идентификатор Cisco bug ID CSCdm61257 (только для зарегистрированных клиентов).

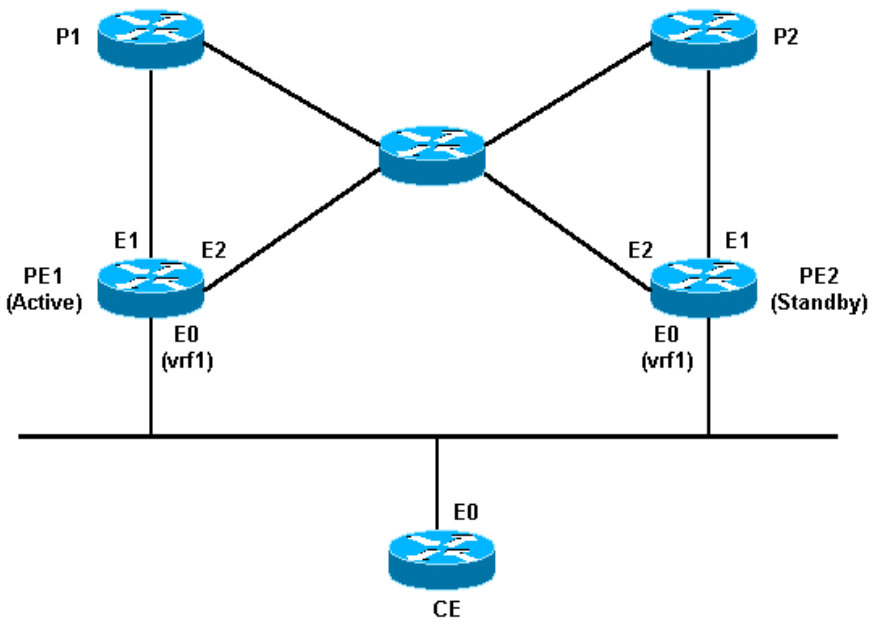
Поддержка сетей MPLS VPN (Multiprotocol Label Switching Virtual Private Networks) в протоколе HSRP

Поддержка сетей MPLS VPN (Multiprotocol Label Switching Virtual Private Networks) для протокола HSRP была добавлена в версии Cisco IOS 12.1(3)T.

Использование HSRP в интерфейсе MPLS VPN полезно, если используется Ethernet-соединение между двумя PE-маршрутизаторами и одна из следующих конфигураций:

- Оконечное устройство абонентской сети (CE) с маршрутом по умолчанию к виртуальному IP-адресу HSRP.
- Один или несколько узлов с виртуальным IP-адресом HSRP настроены в качестве шлюза по умолчанию.

На схеме сети ниже указаны два PE с протоколом HSRP, который работает между VPN-интерфейсами маршрутизации и переадресации (VRF). Модуль CE был настроен с виртуальным IP-адресом HSRP в качестве маршрута по умолчанию. Протокол HSRP настроен на отслеживание интерфейсов, соединяющих PE с остальной частью сети поставщика. Например, в случае отказа интерфейса E1 в PE1 приоритет HSRP снижается, и переадресация пакетов по виртуальному IP- или MAC-адресу передается PE2.



Конфигурации представлены ниже.

Маршрутизатор PE1	Маршрутизатор PE2
conf terminal ! ip cef !	conf terminal ! ip cef !

```
ip vrf vrf1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface ethernet0
no shutdown
ip vrf forwarding vrf1
ip address 10.2.0.1 255.255.0.0
standby 1 ip 10.2.0.20
standby 1 priority 105
standby 1 preempt delay minimum 10
standby 1 timers 3 10
standby 1 track ethernet1 10
standby 1 track ethernet2 10
```

```
ip vrf vrf1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface ethernet0
no shutdown
ip vrf forwarding vrf1
ip address 10.2.0.2 255.255.0.0
standby 1 ip 10.2.0.20
standby 1 priority 100
standby 1 preempt delay minimum 10
standby 1 timers 3 10
standby 1 track ethernet1 10
standby 1 track ethernet2 10
```

Чтобы убедиться, что виртуальный IP-адрес HSRP относится к правильному VRF ARP и таблице переадресации Cisco Express, используйте следующие команды:

```
ed1-pe1# show ip arp vrf vrf1
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.2.0.1                -   00d0.bbd3.bc22  ARPA   Ethernet0/2
Internet  10.2.0.20               -   0000.0c07.ac01  ARPA   Ethernet0/2

ed1-pe1# show ip cef vrf vrf1
Prefix              Next Hop             Interface
0.0.0.0/0           10.3.0.4             Ethernet0/3
0.0.0.0/32          receive
10.1.0.0/16         10.2.0.1             Ethernet0/2
10.2.0.0/16         attached             Ethernet0/2
10.2.0.1/32         receive
10.2.0.20/32        receive
224.0.0.0/24        receive
255.255.255.255/32  receive
```

Поддержка перенаправлений ICMP в протоколе HSRP

Протокол HSRP основан на концепции, в соответствии с которой маршрутизаторы HSRP одного уровня, защищающие подсеть, могут предоставить доступ всем другим подсетям, входящим в состав сети. Поэтому не имеет значения, какой маршрутизатор становится активным маршрутизатором HSRP, поскольку все маршрутизаторы имеют доступ ко всем подсетям.

HSRP использует специальные виртуальные IP-адреса и виртуальные MAC-адреса, логически подключенные к активному маршрутизатору HSRP. При использовании HSRP в интерфейсе перенаправления ICMP автоматически отключаются. Начиная с версии IOS 12.1(3)T функция перенаправления ICMP поддерживается в интерфейсах, использующих HSRP. Дополнительные сведения см. в документе Поддержка перенаправлений ICMP в протоколе HSRP. Это делается для того, чтобы предотвратить перенаправление узлов от виртуального IP-адреса HSRP. Возможно, что два (или более) маршрутизатора в подсети не имеют идентичного подключения к остальной сети. То есть, для определенного IP-адреса назначения в том или ином маршрутизаторе может быть задан лучший путь к этому адресу, или он может оказаться единственным маршрутизатором, подключенным к этому адресу.

Протокол ICMP позволяет маршрутизатору заставить конечную станцию отправлять пакеты в определенное место назначения через другой маршрутизатор в той же подсети, если первому маршрутизатору известно, что другой маршрутизатор имеет лучший путь к этому месту назначения. Как и в случае с шлюзами по умолчанию, если маршрутизатор, к которому была перенаправлена конечная станция для конкретного назначения, дает сбой, то пакеты конечной станции до этого назначения не будут доставлены. Именно это происходит при использовании стандартного протокола HSRP. Поэтому рекомендуется отключать переадресацию ICMP, если включен протокол HSRP.

Решение этой проблемы может быть получено путем расширения связи перенаправлений ICMP и протокола HSRP, которое позволит использовать преимущества протокола HSRP и перенаправлений ICMP одновременно. Две (или более) группы HSRP работают в каждой подсети, причем по меньшей мере с таким количеством настроенных групп HSRP, которое соответствует числу задействованных маршрутизаторов. Приоритеты настроены так, что каждый из маршрутизаторов является основным как минимум в одной группе HSRP. Если один из маршрутизаторов решает перенаправить конечную станцию на другой маршрутизатор при работе с определенным местом назначения, вместо перенаправления конечной станции на IP-адрес этого маршрутизатора он находит группу HSRP, поддерживаемую этим маршрутизатором, и перенаправляет конечную станцию на соответствующий виртуальный IP-адрес. Если после этого происходит отказ маршрутизатора назначения, HSRP передает его функции другому маршрутизатору и перенаправляет конечную станцию на другой, также виртуальный, маршрутизатор.

Поддержка интерфейсов и носителей в протоколе HSRP

В этом разделе приведены сведения о поддержке протоколом HSRP интерфейсов и сред, а также об особенностях работы HSRP с этими средами.

Начиная с версии Cisco IOS 10.0 функциональность HSRP доступна для интерфейсов Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI). Кроме того, протокол HSRP поддерживает интерфейсы Fast Ethernet и ATM.

Виртуальные локальные сети (VLAN) позволяют логическим сетевым топологиям накладываться на физическую коммутируемую инфраструктуру так, чтобы любой произвольный набор портов локальной сети мог объединяться в автономную пользовательскую группу или сообщество интересов. Поддержка HSRP VLAN была добавлена в версии Cisco IOS 11.1 для IEEE 802.10 Secure Data Exchange (SDE) и Cisco IOS 11.3 для Cisco Inter-Switch Link (ISL).

Ethernet

Некоторые контроллеры Ethernet (Lance и QUICC) в продуктах младших моделей поддерживают только один MAC-адрес для одноадресной рассылки в фильтре адресов. На этих платформах разрешена только одна группа HSRP, а адрес интерфейса изменяется на виртуальный MAC-адрес HSRP, когда группа становится активной. Если HSRP используется на маршрутизаторе с несколькими интерфейсами данного типа, необходимо настроить различные номера группы HSRP для каждого интерфейса.

Примечание: Маршрутизатор Cisco 7200 также использует контроллер Lance Ethernet, однако для него предусмотрена программная поддержка MHSRP.

Компания Cisco рекомендует задействовать на более 24-х интерфейсных процессоров Ethernet (EIP) на HSRP, поскольку обновление адресных фильтров для HSRP занимает достаточно длительное время. Наличие более двадцати четырех HSRP EIP может вызвать нестабильность и избыточную загрузку ЦП.

Эта ошибка имеет идентификатор Cisco Bug ID CSCdj29595 (только для зарегистрированных клиентов).

При наличии более двадцати четырех EIP, попробуйте заменить их модулями VIP и адаптерами портов Ethernet. VIP были одобрены для сред, включающих до 80 групп HSRP. Можно также сократить число групп HSRP и увеличить время приветствия и удержания HSRP.

Token Ring

Ограничение при использовании HSRP на основе интерфейса Token Ring состоит в невозможности перепрограммирования фильтра адресов в чипсете Token Ring способом, аналогичным Ethernet, FDDI или эмуляции ATM. Token Ring использует функциональные адреса, лишь малая часть которых не вызывает конфликтов с другими устройствами, использующими пространство функциональных адресов.

Использование HSRP в среде SRB с использованием функциональных адресов может вызвать конфликт RIF. Дополнительные сведения см. в разделе Адресация HSRP. Кроме того, попробуйте настроить команду **use-bia**.

802.1Q

Для HSRP поверх 802.1Q, Cisco рекомендует использовать Cisco IOS версии 12.0(8.1)T или выше.

ISL

Протокол HSRP поверх ISL доступен в версиях Cisco IOS 11.2(6)F, 11.3, 12.X. Во избежание проблем, описанных в документе Cisco Bug ID CSCdm68811 (только для зарегистрированных клиентов), рекомендуется использовать версию 12.0(7) или выше.

FDDI

Адаптер порта FDDI снимает кадры с кольца, если видит один из своих собственных MAC-адресов в источнике MAC. Если событие в сети вызывает активацию обоих маршрутизаторов, оба они отсылают пакеты приветствия HSRP с одним и тем же виртуальным MAC-адресом. Оба маршрутизатора по ошибке сбрасывают пакеты приветствия и остаются активными.

Эта ошибка имеет идентификатор Cisco Bug ID CSCdj30049 (только для зарегистрированных клиентов).

Для решения этой проблемы версия Cisco IOS 11.2(11.1) использует уникальные прошитые MAC-адреса маршрутизаторов HSRP в среде FDDI для обмена сообщениями и протокола HSRP. Для этого мосты и коммутаторы создают в кэше правильную запись порта для виртуальных MAC-адресов, кроме того активный маршрутизатор отправляет периодические сообщения с обновлениями, используя MAC-адреса HSRP.

Примечание: Таблица CAM маршрутизатора Cisco 4500 на интерфейсе FDDI после перезагрузки может быть заполнена неверно, если было настроено несколько сетей RIP и групп HSRP. Единственный способ решения этой проблемы в настоящий момент — очистка интерфейсов для восстановления CAM. Эта ошибка имеет идентификатор Cisco Bug ID CSCdm93122 (только для зарегистрированных клиентов).

Обновление MAC

Маршрутизаторы HSRP в среде FDDI используют свой уникальный прошитый MAC-адрес для обмена сообщениями и выполнения протокола HSRP. Чтобы убедиться, что обучающиеся мосты и коммутаторы сохранили верную запись порта для виртуального MAC-адреса, активный маршрутизатор посылает периодические сообщения с обновлениями через MAC-адрес HSRP. Эта ошибка имеет идентификатор Cisco Bug ID CSCdj30049 (только для зарегистрированных клиентов).

Если в сети нет коммутаторов или обучающихся мостов, можно запретить отсылку пакетов обновлений, как показано ниже:

```
interface fddi 1/0/0
ip address 10.1.1.1 255.255.255.0
standby ip 10.1.1.250
standby mac-refresh 0
```

Виртуальный интерфейс мостовой группы

Поддержка HSRP в виртуальных интерфейсах мостовой группы (BVI) была добавлена в версии Cisco IOS 12.0(6.2)T.

Субинтерфейсы

Группы HSRP на субинтерфейсах должны иметь уникальный номер группы среди групп субинтерфейсов на одном интерфейсе. Это вызвано тем, что субинтерфейсы не получают уникальный индекс интерфейса SNMP. Если существует две группы с номером N на разных субинтерфейсах, в таблице MIB группа N на субинтерфейсе 1 и группа N на субинтерфейсе 2 будут выглядеть как одна и та же группа.

Дополнительные сведения

- **Страница поддержки HSRP**
- **Техническая поддержка и документация — Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010