# First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15S

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

CHAPTER 15

CHAPTER 16

CHAPTER 1

# Configuring GLBP

Gateway Load Balancing Protocol (GLBP) protects data traffic from a failed device or circuit, like Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP), while allowing packet load sharing between a group of redundant devices.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for GLBP

Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with GLBP in SSO mode.

# Prerequisites for GLBP

Before configuring GLBP, ensure that the devices can support multiple MAC addresses on the physical interfaces. For each GLBP forwarder to be configured, an additional MAC address is used.

# Information About GLBP

## GLBP Overview

GLBP provides automatic device backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop devices on the LAN combine to offer a single virtual first-hop IP device while sharing the IP packet forwarding load. Other devices on the LAN act as redundant GLBP devices that will become active if any of the existing forwarding devices fail.

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple devices to participate in a virtual device group configured with a virtual IP address. One member is elected to be the active device to forward packets sent to the virtual IP address for the group. The other devices in the group are redundant until the active device fails. These standby devices have unused bandwidth that the protocol is not using. Although multiple virtual device groups can be configured for the same set of devices, the hosts must be configured for different default gateways, which results in an extra administrative burden. The advantage of GLBP is that it additionally provides load balancing over multiple devices (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all devices in a GLBP group rather than being handled by a single device while the other devices stand idle. Each host is configured with the same virtual IP address, and all devices in the virtual device group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, UDP port 3222 (source and destination).

### GLBP Packet Types

GLBP uses 3 different packet types to operate. The packet types are Hello, Request, and Reply. The Hello packet is used to advertise protocol information. Hello packets are multicast, and are sent when any virtual gateway or virtual forwarder is in Speak, Standby or Active state. Request and Reply packets are used for virtual MAC assignment. They are both unicast messages to and from the active virtual gateway (AVG).

## GLBP Active Virtual Gateway

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG if the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

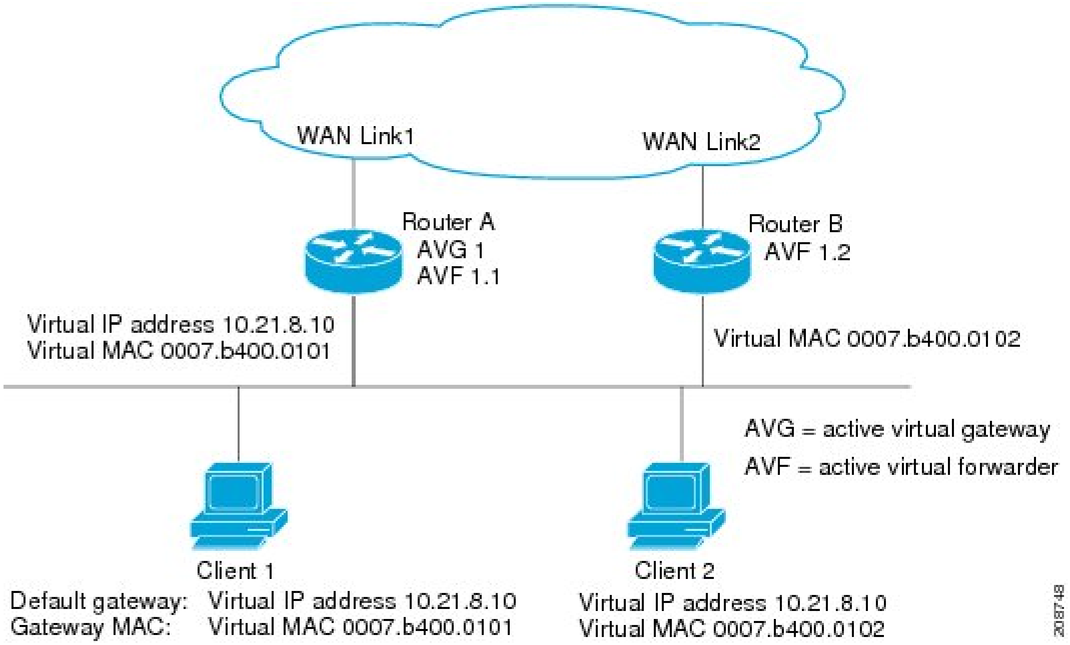
The AVG is also responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

Prior to Cisco IOS Release 15.0(1)M1 and 12.4(24)T2, when the **no glbp load-balancing** command is configured, the AVG always responds to ARP requests with the MAC address of its AVF.

In Cisco IOS Release 15.0(1)M1 and 12.4(24)T2, and later releases, when the **no glbp load-balancing** command is configured, if the AVG does not have an AVF, it preferentially responds to ARP requests with the MAC address of the first listening virtual forwarder (VF), which will causes traffic to route via another gateway until that VF migrates back to being the current AVG.

In the figure below, Router A (or Device A) is the AVG for a GLBP group, and is responsible for the virtual IP address 10.21.8.10. Router A is also an AVF for the virtual MAC address 0007.b400.0101. Router B (or Device B) is a member of the same GLBP group and is designated as the AVF for the virtual MAC address 0007.b400.0102. Client 1 has a default gateway IP address of 10.21.8.10 and a gateway MAC address of 0007.b400.0101. Client 2 shares the same default gateway IP address but receives the gateway MAC address 0007.b400.0102 because Router B is sharing the traffic load with Router A.

***Figure 1: GLBP Topology***


WAN Link1
WAN Link2
Router A
AVG 1
AVF 1.1
Router B
AVF 1.2
Virtual IP address 10.21.8.10
Virtual MAC 0007.b400.0101
Virtual MAC 0007.b400.0102
AVG = active virtual gateway
AVF = active virtual forwarder
Client 1
Client 2
Default gateway: Virtual IP address 10.21.8.10
Gateway MAC: Virtual MAC 0007.b400.0101
Virtual IP address 10.21.8.10
Virtual MAC 0007.b400.0102
208748

If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for the entire GLBP group. Communication for the GLBP members continues despite the failure of a device in the GLBP group.

# GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

# GLBP Virtual Gateway Redundancy

GLBP operates virtual gateway redundancy in the same way as HSRP. One gateway is elected as the AVG, another gateway is elected as the standby virtual gateway, and the remaining gateways are placed in a listen state.

If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IP address. A new standby virtual gateway is then elected from the gateways in the listen state.

# GLBP Virtual Forwarder Redundancy

Virtual forwarder redundancy is similar to virtual gateway redundancy with an AVF. If the AVF fails, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

The new AVF is also a primary virtual forwarder for a different forwarder number. GLBP migrates hosts away from the old forwarder number using two timers that start as soon as the gateway changes to the active virtual forwarder state. GLBP uses the hello messages to communicate the current state of the timers.

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When the redirect time expires, the AVG stops using the old virtual forwarder MAC address in ARP replies, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

The secondary holdtime is the interval during which the virtual forwarder is valid. When the secondary holdtime expires, the virtual forwarder is removed from all gateways in the GLBP group. The expired virtual forwarder number becomes eligible for reassignment by the AVG.

# GLBP Gateway Priority

GLBP gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails.

Priority also determines if a GLBP device functions as a backup virtual gateway and the order of ascendancy to becoming an AVG if the current AVG fails. You can configure the priority of each backup virtual gateway with a value of 1 through 255 using the **glbp priority** command.

In the "GLBP Topology" figure, if Router A (or Device A)—the AVG in a LAN topology—fails, an election process takes place to determine which backup virtual gateway should take over. In this example, Router B (or Device B) is the only other member in the group so it will automatically become the new AVG. If another device existed in the same GLBP group with a higher priority, then the device with the higher priority would be elected. If both devices have the same priority, the backup virtual gateway with the higher IP address would be elected to become the active virtual gateway.

By default, the GLBP virtual gateway preemptive scheme is disabled. A backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. You can enable the GLBP virtual gateway preemptive scheme using the **glbp preempt** command. Preemption allows a backup virtual gateway to become the AVG, if the backup virtual gateway is assigned a higher priority than the current AVG.

## GLBP Gateway Weighting and Tracking

GLBP uses a weighting scheme to determine the forwarding capacity of each device in the GLBP group. The weighting assigned to a device in the GLBP group can be used to determine whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets. Thresholds can be set to disable forwarding when the weighting for a GLBP group falls below a certain value, and when it rises above another threshold, forwarding is automatically reenabled.

The GLBP group weighting can be automatically adjusted by tracking the state of an interface within the device. If a tracked interface goes down, the GLBP group weighting is reduced by a specified value. Different interfaces can be tracked to decrement the GLBP weighting by varying amounts.

By default, the GLBP virtual forwarder preemptive scheme is enabled with a delay of 30 seconds. A backup virtual forwarder can become the AVF if the current AVF weighting falls below the low weighting threshold for 30 seconds. You can disable the GLBP forwarder preemptive scheme using the **no glbp forwarder preempt** command or change the delay using the **glbp forwarder preempt delay minimum** command.

## GLBP MD5 Authentication

GLBP MD5 authentication uses the industry-standard MD5 algorithm for improved reliability and security. MD5 authentication provides greater security than the alternative plain text authentication scheme and protects against spoofing software.

MD5 authentication allows each GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and, if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can either be given directly in the configuration using a key string or supplied indirectly through a key chain. The key string cannot exceed 100 characters in length.

A device will ignore incoming GLBP packets from devices that do not have the same authentication configuration for a GLBP group. GLBP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

GLBP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packet.
- MD5 digests differ on the device and in the incoming packet.
- Text authentication strings differ on the device and in the incoming packet.

## ISSU-GLBP

GLBP supports In Service Software Upgrade (ISSU). ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.

ISSU provides the ability to upgrade or downgrade from one supported Cisco IOS release to another while continuing to forward packets and maintain sessions, thereby reducing planned outage time. The ability to upgrade or downgrade is achieved by running different software versions on the active RP and standby RP for a short period of time to maintain state information between RPs. This feature allows the system to switch over to a secondary RP running upgraded (or downgraded) software and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* in the *Cisco IOS High Availability Configuration Guide*

For detailed information about ISSU on the 7600 series devices, see the *ISSU and eFSU on Cisco 7600 Series Routers* document.

## GLBP SSO

With the introduction of the GLBP SSO functionality, GLBP is stateful switchover (SSO) aware. GLBP can detect when a device is failing over to the secondary router processor (RP) and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Without SSO-awareness, if GLBP is deployed on a device with redundant RPs, a switchover of roles between the active RP and the standby RP results in the device relinquishing its activity as a GLBP group member and then rejoining the group as if it had been reloaded. The GLBP SSO feature enables GLBP to continue its activities as a group member during a switchover. GLBP state information between redundant RPs is maintained so that the standby RP can continue the device's activities within the GLBP during and after a switchover.

This feature is enabled by default. To disable this feature, use the **no glbp sso** command in global configuration mode.

For more information, see the *Stateful Swithover* document in the *Cisco IOS High Availability Configuration Guide*.

## GLBP Benefits

### Load Sharing

You can configure GLBP in such a way that traffic from LAN clients can be shared by multiple devices, thereby sharing the traffic load more equitably among available devices.

### Multiple Virtual Devices

GLBP supports up to 1024 virtual devices (GLBP groups) on each physical interface of a device and up to four virtual forwarders per group.

### Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway (AVG) with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.

### Authentication

GLBP supports the industry-standard message digest 5 (MD5) algorithm for improved reliability, security, and protection against GLBP-spoofing software. A device within a GLBP group with a different authentication string than other devices will be ignored by other group members. You can alternatively use a simple text password authentication scheme between GLBP group members to detect configuration errors.

# How to Configure GLBP

## Enabling and Verifying GLBP

Perform this task to enable GLBP on an interface and verify its configuration and operation. GLBP is designed to be easy to configure. Each gateway in a GLBP group must be configured with the same group number, and at least one gateway in the GLBP group must be configured with the virtual IP address to be used by the group. All other required parameters can be learned.

### Before You Begin

If VLANs are in use on an interface, the GLBP group number must be different for each VLAN.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group* **ip** [*ip-address* [**secondary**]]
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Specifies an interface type and number, and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **glbp** *group* **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# glbp 10 ip 10.21.8.10` | Enables GLBP on an interface and identifies the primary IP address of the virtual gateway.<br>• After you identify a primary IP address, you can use the **glbp** *group* **ip** command again with the **secondary** keyword to indicate additional IP addresses supported by this group. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode, and returns the device to global configuration mode. |
| **Step 7** | **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]<br>**Example:**<br>`Device(config)# show glbp 10` | (Optional) Displays information about GLBP groups on a device.<br>• Use the optional **brief** keyword to display a single line of information about each virtual gateway or virtual forwarder. |

### Example

In the following example, sample output is displayed about the status of the GLBP group, named 10, on the device:

```
Device# show glbp 10

GigabitEthernet0/0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication text "stringabc"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
```

```
Weighting 105 (configured 110), thresholds: lower 95, upper 105
  Track object 2 state Down decrement 5
Load balancing: host-dependent
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 23:50:15
  MAC address is 0007.b400.0101 (default)
  Owner ID is 0005.0050.6c08
  Redirection enabled
  Preemption enabled, min delay 60 sec
  Active is local, weighting 105
```

# Customizing GLBP

Customizing the behavior of GLBP is optional. Be aware that as soon as you enable a GLBP group, that group is operating. It is possible that if you first enable a GLBP group before customizing GLBP, the device could take over control of the group and become the AVG before you have finished customizing the feature. Therefore, if you plan to customize GLBP, it is a good idea to do so before enabling GLBP.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp** *group* **timers redirect** *redirect timeout*
7. **glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp** *group* **priority** *level*
9. **glbp** *group* **preempt** [**delay minimum** *seconds*]
10. **glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*]
11. **glbp** *group* **name** *redundancy-name*
12. **exit**
13. **no glbp sso**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface fastethernet 0/0` | Specifies an interface type and number, and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*<br>**Example:**<br>`Device(config-if)# glbp 10 timers 5 18` | Configures the interval between successive hello packets sent by the AVG in a GLBP group.<br>• The *holdtime* argument specifies the interval in seconds before the virtual gateway and virtual forwarder information in the hello packet is considered invalid.<br>• The optional **msec** keyword specifies that the following argument will be expressed in milliseconds, instead of the default seconds. |
| **Step 6** | **glbp** *group* **timers redirect** *redirect timeout*<br>**Example:**<br>`Device(config-if)# glbp 10 timers redirect 1800 28800` | Configures the time interval during which the AVG continues to redirect clients to an AVF. The default is 600 seconds (10 minutes).<br>• The *timeout* argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid. The default is 14,400 seconds (4 hours).<br>**Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, and the device fails, new hosts continue to be assigned to the failed device instead of being redirected to the backup. |
| **Step 7** | **glbp** *group* **load-balancing** [**host-dependent** \| **round-robin** \| **weighted**]<br>**Example:**<br>`Device(config-if)# glbp 10 load-balancing host-dependent` | Specifies the method of load balancing used by the GLBP AVG. |
| **Step 8** | **glbp** *group* **priority** *level* | Sets the priority level of the gateway within a GLBP group. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-if)# glbp 10 priority 254` | • The default value is 100. |
| **Step 9** | **glbp** *group* **preempt** [**delay minimum** *seconds*]<br>**Example:**<br>`Device(config-if)# glbp 10 preempt delay minimum 60` | Configures the device to take over as AVG for a GLBP group if it has a higher priority than the current AVG.<br>• This command is disabled by default.<br>• Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVG takes place. |
| **Step 10** | **glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*]<br>**Example:**<br>`Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245` | (Optional) Enables the GLBP client cache.<br>• This command is disabled by default.<br>• Use the *number* argument to specify the maximum number of clients the cache will hold for this GLBP group. The range is from 8 to 2000.<br>• Use the optional **timeout** *minutes* keyword and argument pair to configure the maximum amount of time a client entry can stay in the GLBP client cache after the client information was last updated. The range is from 1 to 1440 minutes (one day).<br>**Note** For IPv4 networks, Cisco recommends setting a GLBP client cache timeout value that is slightly longer than the maximum expected end-host Address Resolution Protocol (ARP) cache timeout value. |
| **Step 11** | **glbp** *group* **name** *redundancy-name*<br>**Example:**<br>`Device(config-if)# glbp 10 name abc123` | Enables IP redundancy by assigning a name to the GLBP group.<br>• The GLBP redundancy client must be configured with the same GLBP group name so the redundancy client and the GLBP group can be connected. |
| **Step 12** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode, and returns the device to global configuration mode. |
| **Step 13** | **no glbp sso**<br>**Example:**<br>`Device(config)# no glbp sso` | (Optional) Disables GLBP support of SSO. |

# Configuring GLBP MD5 Authentication Using a Key String

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication md5 key-string** [ **0** | **7**] *key*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. Repeat Steps 1 through 6 on each device that will communicate.
8. **end**
9. **show glbp**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Ethernet0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **glbp** *group-number* **authentication md5 key-string** [ **0** \| **7**] *key* | Configures an authentication key for GLBP MD5 authentication.<br>• The key string cannot exceed 100 characters in length. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a` | • No prefix to the *key* argument or specifying **0** means the key is unencrypted.<br>• Specifying **7** means the key is encrypted. The key-string authentication key will automatically be encrypted if the **service password-encryption** global configuration command is enabled. |
| **Step 6** | **glbp** *group-number* **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# glbp 1 ip 10.0.0.10` | Enables GLBP on an interface and identifies the primary IP address of the virtual gateway. |
| **Step 7** | Repeat Steps 1 through 6 on each device that will communicate. | — |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show glbp**<br>**Example:**<br>`Device# show glbp` | (Optional) Displays GLBP information.<br>• Use this command to verify your configuration. The key string and authentication type will be displayed if configured. |

# Configuring GLBP MD5 Authentication Using a Key Chain

Perform this task to configure GLBP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. GLBP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*
11. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
12. Repeat Steps 1 through 10 on each device that will communicate.
13. **end**
14. **show glbp**
15. **show key chain**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)# key chain glbp2` | Enables authentication for routing protocols and identifies a group of authentication keys and enters key-chain configuration mode. |
| **Step 4** | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 100` | Identifies an authentication key on a key chain.<br>• The value for the *key-id* argument must be a number. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **key-string** *string*<br>**Example:**<br>`Device(config-keychain-key)# key-string abc123` | Specifies the authentication string for a key and enters key-chain key configuration mode.<br>• The value for the *string* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to key-chain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Ethernet0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 9** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.21.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 10** | **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*<br>**Example:**<br>`Device(config-if)# glbp 1 authentication md5 key-chain glbp2` | Configures an authentication MD5 key chain for GLBP MD5 authentication.<br>• The key chain name must match the name specified in Step 3. |
| **Step 11** | **glbp** *group-number* **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# glbp 1 ip 10.21.0.12` | Enables GLBP on an interface and identifies the primary IP address of the virtual gateway. |
| **Step 12** | Repeat Steps 1 through 10 on each device that will communicate. | — |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 14** | **show glbp**<br>**Example:**<br>`Device# show glbp` | (Optional) Displays GLBP information.<br>- Use this command to verify your configuration. The key chain and authentication type will be displayed if configured. |
| **Step 15** | **show key chain**<br>**Example:**<br>`Device# show key chain` | (Optional) Displays authentication key information. |

# Configuring GLBP Text Authentication

Text authentication provides minimal security. Use MD5 authentication if security is required.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication text** *string*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. Repeat Steps 1 through 6 on each device that will communicate.
8. **end**
9. **show glbp**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Ethernet0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **glbp** *group-number* **authentication text** *string*<br>**Example:**<br>`Device(config-if)# glbp 10 authentication text stringxyz` | Authenticates GLBP packets received from other devices in the group.<br>• If you configure authentication, all devices within the GLBP group must use the same authentication string. |
| **Step 6** | **glbp** *group-number* **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# glbp 1 ip 10.0.0.10` | Enables GLBP on an interface and identifies the primary IP address of the virtual gateway. |
| **Step 7** | Repeat Steps 1 through 6 on each device that will communicate. | — |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show glbp**<br>**Example:**<br>`Device# show glbp` | (Optional) Displays GLBP information.<br>• Use this command to verify your configuration. |

# Configuring GLBP Weighting Values and Object Tracking

GLBP weighting is used to determine whether a GLBP group can act as a virtual forwarder. Initial weighting values can be set and optional thresholds specified. Interface states can be tracked and a decrement value set to reduce the weighting value if the interface goes down. When the GLBP group weighting drops below a specified value, the group will no longer be an active virtual forwarder. When the weighting rises above a specified value, the group can resume its role as an active virtual forwarder.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
7. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]
8. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
9. **exit**
10. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [ **brief**] | **resolution** | **timers**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** \| **ip routing**}<br>**Example:**<br>`Device(config)# track 2 interface POS 6/0/0 ip routing` | Configures an interface to be tracked where changes in the state of the interface affect the weighting of a GLBP gateway, and enters tracking configuration mode.<br>• This command configures the interface and corresponding object number to be used with the **glbp weighting track** command.<br>• The **line-protocol** keyword tracks whether the interface is up. The **ip routing** keywords also check that IP routing is enabled on the interface, and an IP address is configured. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-track)# exit` | Returns to global configuration mode. |
| **Step 5** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |
| **Step 6** | **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]<br>**Example:**<br>`Device(config-if)# glbp 10 weighting 110 lower 95 upper 105` | Specifies the initial weighting value, and the upper and lower thresholds, for a GLBP gateway. |
| **Step 7** | **glbp** *group* **weighting track** *object-number* [**decrement** *value*]<br>**Example:**<br>`Device(config-if)# glbp 10 weighting track 2 decrement 5` | Specifies an object to be tracked that affects the weighting of a GLBP gateway.<br>• The *value* argument specifies a reduction in the weighting of a GLBP gateway when a tracked object fails. |
| **Step 8** | **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]<br>**Example:**<br>`Device(config-if)# glbp 10 forwarder preempt delay minimum 60` | Configures the device to take over as AVF for a GLBP group if the current AVF for a GLBP group falls below its low weighting threshold.<br>• This command is enabled by default with a delay of 30 seconds.<br>• Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVF takes place. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Returns to privileged EXEC mode. |
| **Step 10** | **show track** [*object-number* \| **brief**] [**interface** [**brief**] \| **ip route** [ **brief**] \| **resolution** \| **timers**]<br>**Example:**<br>`Device# show track 2` | Displays tracking information. |

# Troubleshooting GLBP

GLBP introduces five privileged EXEC mode commands to enable display of diagnostic output concerning various events relating to the operation of GLBP. The **debug condition glbp**,**debug glbp errors**, **debug glbp events**, **debug glbp packets**, and **debug glbp terse** commands are intended only for troubleshooting purposes because the volume of output generated by the software can result in severe performance degradation on the device. Perform this task to minimize the impact of using the **debug glbp** commands.

This procedure will minimize the load on the device created by the **debug condition glbp**or **debug glbp** command because the console port is no longer generating character-by-character processor interrupts. If you cannot connect to a console directly, you can run this procedure via a terminal server. If you must break the Telnet connection, however, you may not be able to reconnect because the device may be unable to respond due to the processor load of generating the debugging output.

### Before You Begin

This task requires a device running GLBP to be attached directly to a console.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Use Telnet to access a device port and repeat Steps 1 and 2.
5. **end**
6. **terminal monitor**
7. **debug condition glbp** *interface-type interface-number group* [*forwarder*]
8. **terminal no monitor**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no logging console** | Disables all logging to the console terminal. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# no logging console` | • To reenable logging to the console, use the**logging console** command in global configuration mode. |
| **Step 4** | Use Telnet to access a device port and repeat Steps 1 and 2. | Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits to privileged EXEC mode. |
| **Step 6** | **terminal monitor**<br>**Example:**<br>`Device# terminal monitor` | Enables logging output on the virtual terminal. |
| **Step 7** | **debug condition glbp** *interface-type interface-number group* [*forwarder*]<br>**Example:**<br>`Device# debug condition glbp GigabitEthernet0/0/0 1` | Displays debugging messages about GLBP conditions.<br>• Try to enter only specific **debug condition glbp** or **debug glbp** commands to isolate the output to a certain subcomponent and minimize the load on the processor. Use appropriate arguments and keywords to generate more detailed debug information on specified subcomponents.<br>• Enter the specific **no debug condition glbp** or **no debug glbp** command when you are finished. |
| **Step 8** | **terminal no monitor**<br>**Example:**<br>`Device# terminal no monitor` | Disables logging on the virtual terminal. |

# Configuration Examples for GLBP

## Example: Customizing GLBP Configuration

```
Device(config)# interface fastethernet 0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 timers 5 18
Device(config-if)# glbp 10 timers redirect 1800 28800
Device(config-if)# glbp 10 load-balancing host-dependent
Device(config-if)# glbp 10 priority 254
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

## Example: Configuring GLBP MD5 Authentication Using Key Strings

The following example shows how to configure GLBP MD5 authentication using a key string:

```
Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Device(config-if)# glbp 2 ip 10.0.0.10
```

## Example: Configuring GLBP MD5 Authentication Using Key Chains

In the following example, GLBP queries the key chain “AuthenticateGLBP” to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Device(config-if)# glbp 2 ip 10.0.0.10
```

## Example: Configuring GLBP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 authentication text stringxyz
Device(config-if)# glbp 10 ip 10.21.8.10
```

## Example: Configuring GLBP Weighting

In the following example, the device is configured to track the IP routing state of the POS interface 5/0/0 and 6/0/0, an initial GLBP weighting with upper and lower thresholds is set, and a weighting decrement value of 10 is set. If POS interface 5/0/0 and 6/0/0 go down, the weighting value of the device is reduced.

```
Device(config)# track 1 interface POS 5/0/0 ip routing
Device(config)# track 2 interface POS 6/0/0 ip routing
Device(config)# interface fastethernet 0/0/0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1 decrement 10
Device(config-if)# glbp 10 weighting track 2 decrement 10
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

## Example: Enabling GLBP Configuration

In the following example, the device is configured to enable GLBP, and the virtual IP address of 10.21.8.10 is specified for GLBP group 10:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

# Additional References for GLBP

### Related Documents

| Related Topic | Document Title |
|---|---|
| GLBP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | Cisco IOS IP Application Services Command Reference |
| In Service Software Upgrade (ISSU) configuration | "In Service Software Upgrade" process module in the *Cisco IOS High Availability Configuration Guide* |
| Key chains and key management commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Routing Protocol-Independent Command Reference* |
| Object tracking | "Configuring Enhanced Object Tracking" module |
| Stateful Switchover | The "Stateful Switchover" module in the *Cisco IOS High Availability Configuration Guide* |
| VRRP | "Configuring VRRP" module |
| HSRP | "Configuring HSRP" module |
| GLBP Support for IPv6 | “FHRP - GLBP Support for IPv6” module |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for GLBP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 1: Feature Information for GLBP***

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| Gateway Load Balancing Protocol | 15.2(1)S | GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while allowing packet load sharing between a group of redundant routers.<br>The following commands were introduced or modified by this feature: **glbp forwarder preempt**, **glbp ip** , **glbp load-balancing** , **glbp name**, **glbp preempt** , **glbp priority** , **glbp sso** , **glbp timers** , **glbp timers redirect**, **glbp weighting** , **glbp weighting track**, **show glbp**. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| GLBP MD5 Authentication | 15.2(1)S | MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and, if the hash within the incoming packet does not match the generated hash, the packet is ignored.<br>The following commands were modified by this feature: **glbp authentication**, **show glbp**. |
| ISSU—GLBP | 15.2(1)S | GLBP supports In Service Software Upgrade (ISSU). ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.<br>This feature provides customers with the same level of HA functionality for planned outages due to software upgrades as is available with SSO for unplanned outages. That is, the system can switch over to a secondary RP and continue forwarding packets without session loss and with minimal or no packet loss.<br>This feature is enabled by default.<br>There are no new or modified commands for this feature. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| SSO—GLBP | 15.2(1)S | GLBP is now SSO aware. GLBP can detect when a router is failing over to the secondary RP and continue in its current GLBP group state.<br>Prior to being SSO aware, GLBP was not able to detect that a second RP was installed and configured to take over in the event that the primary RP failed. When the primary failed, the GLBP device would stop participating in the GLBP group and, depending on its role, could trigger another router in the group to take over as the active router. With this enhancement, GLBP detects the failover to the secondary RP and no change occurs to the GLBP group. If the secondary RP fails and the primary is still not available, then the GLBP group detects this and re-elects a new active GLBP router.<br>This feature is enabled by default.<br>The following commands were introduced or modified by this feature: **debug glbp events**,**glbp sso**, **show glbp**. |

# Glossary

**active RP—**The Route Processor (RP) controls the system, provides network services, runs routing protocols and presents the system management interface.

**AVF—**active virtual forwarder. One virtual forwarder within a GLBP group is elected as active virtual forwarder for a specified virtual MAC address, and it is responsible for forwarding packets sent to that MAC address. Multiple active virtual forwarders can exist for each GLBP group.

**AVG—**active virtual gateway. One virtual gateway within a GLBP group is elected as the active virtual gateway, and is responsible for the operation of the protocol.

**GLBP gateway—**Gateway Load Balancing Protocol gateway. A router or gateway running GLBP. Each GLBP gateway may participate in one or more GLBP groups.

**GLBP group—**Gateway Load Balancing Protocol group. One or more GLBP gateways configured with the same GLBP group number on connected Ethernet interfaces.

**ISSU—**In Service Software Upgrade. A process that allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows  software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

**NSF—**nonstop forwarding. The ability of a router to continue to forward traffic to a router that may be recovering from a failure. Also, the ability of a router recovering from a failure to continue to correctly forward traffic sent to it by a peer.

**RP—**Route Processor. A generic term for the centralized control unit in a chassis. Platforms usually use a platform-specific term, such as RSP on the Cisco 7500, the PRE on the Cisco 10000, or the SUP+MSFC on the Cisco 7600.

**RPR—**Route Processor Redundancy. RPR provides an alternative to the High System Availability (HSA) feature. HSA enables a system to reset and use a standby Route Processor (RP) if the active RP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RP if the active RP experiences a fatal error.

**RPR+—**An enhancement to RPR in which the standby RP is fully initialized.

**SSO—**Stateful Switchover. Enables applications and features to maintain state information between an active and standby unit.

**standby RP—**An RP that has been fully initialized and is ready to assume control from the active RP should a manual or fault-induced switchover occur.

**switchover—**An event in which system control and routing protocol execution are transferred from the active RP to the standby RP. Switchover may be a manual operation or may be induced by a hardware or software fault. Switchover may include transfer of the packet forwarding function in systems that combine system control and packet forwarding in an indivisible unit.

**vIP—**virtual IP address. An IPv4 address. There must be only one virtual IP address for each configured GLBP group. The virtual IP address must be configured on at least one GLBP group member. Other GLBP group members can learn the virtual IP address from hello messages.

CHAPTER 2

# HSRP for IPv6

IPv6 routing protocols ensure device-to-device resilience and failover. However, in situations in which the path between a host and the first-hop device fails, or the first-hop device itself fails, first hop redundancy protocols (FHRPs) ensure host-to-device resilience and failover.

The Hot Standby Router Protocol (HSRP) protects data traffic in case of a gateway failure.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for HSRP for IPv6

HSRP version 2 must be enabled on an interface before HSRP for IPv6 can be configured.

# Information About HSRP for IPv6

## HSRP for IPv6 Overview

The HSRP is an FHRP designed to allow for transparent failover of the first-hop IP device. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet configured with a default gateway IP address. HSRP is used in a group of devices for selecting an active device and a standby device. In a group of device interfaces, the active device is the device of choice for routing packets; the standby device is the device that takes over when the active device fails or when preset conditions are met.

IPv6 hosts learn of available IPv6 devices through IPv6 neighbor discovery RA messages. These are multicast periodically, or may be solicited by hosts. HSRP is designed to provide only a virtual first hop for IPv6 hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number, and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic RAs are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent when the group leaves the active state.

Periodic RAs for the interface link-local address stop after a final RA is sent while at least one virtual IPv6 link-local address is configured on the interface. No restrictions occur for the interface IPv6 link-local address other than that mentioned for the RAs. Other protocols continue to receive and send packets to this address.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device.

## HSRP IPv6 Virtual MAC Address Range

HSRP IPv6 uses a different virtual MAC address block than does HSRP for IP:

0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses)

## HSRP IPv6 UDP Port Number

Port number 2029 has been assigned to HSRP IPv6.

# How to Enable HSRP for IPv6

## Enabling an HSRP Group for IPv6 Operation

HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

## Enabling HSRP Version 2

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby version** {**1** | **2**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Specifies an interface type and number, and places the device in interface configuration mode. |
| **Step 4** | **standby version** {**1** \| **2**}<br>**Example:**<br>`Device(config-if)# standby version 2` | Changes the version of the HSRP.<br>• Version 1 is the default. |

## Enabling and Verifying an HSRP Group for IPv6 Operation

In this task, when you enter the **standby ipv6** command, a link-local address is generated from the link-local prefix, and a modified EUI-64 format interface identifier is generated in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need site-local or globally unique addresses to communicate.

In IPv6, a device on the link advertises in RA messages any site-local and global prefixes, and its willingness to function as a default device for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure site-local and global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}
6. **standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*]
7. **standby** [*group-number*] **priority** *priority*
8. **exit**
9. **show standby** [*type number* [*group*]] [**all** | **brief**]
10. **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ipv6 unicast-routing**<br>**Example:**<br>`Device(config)# ipv6 unicast-routing` | Enables the forwarding of IPv6 unicast datagrams.<br>• The **ipv6 unicast-routing** command must be enabled for HSRP for IPv6 to work. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **interface** *type* *number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Specifies an interface type and number, and places the device in interface configuration mode. |
| **Step 5** | **standby** [*group-number*] **ipv6** {*link-local-address* \| **autoconfig**}<br>**Example:**<br>`Device(config-if)# standby 1 ipv6 autoconfig` | Activates the HSRP in IPv6. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay minimum** *seconds* \| **reload** *seconds* \| **sync** *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption and preemption delay. |
| **Step 7** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Returns the device to privileged EXEC mode. |
| **Step 9** | **show** **standby** [*type number* [*group*]] [**all** \| **brief**]<br>**Example:**<br>`Device# show standby` | Displays HSRP information. |
| **Step 10** | **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]<br>**Example:**<br>`Device# show ipv6 interface GigabitEthernet 0/0/0` | Displays the usability status of interfaces configured for IPv6. |

# Configuration Examples for HSRP for IPv6

## Example: Configuration and Verification for an HSRP Group

The following example shows configuration and verification for an HSRP group for IPv6 that consists of Device1 and Device2. The **show standby** command is issued for each device to verify the device's configuration:

**Device 1 configuration**

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Device1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

**Device 2 configuration**

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese
Device2# show standby
```

```
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |
| HSRP | *Configuring HSRP* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### MIBs

| MIB | MIBs Link |
|---|---|
| | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 2: Feature Information for HSRP for IPv6*

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP for IPv6 | 12.2(46)SE<br>12.2(52)SG<br>12.2(33)SRB<br>12.2(33)SXI<br>12.4(4)T<br>15.0(2)SG<br>15.3(1)S<br>15.3(2)T | The HSRP is an FHRP that allows transparent failover of the first-hop IPv6 device.<br>The following commands were introduced or modified: **show standby**, **standby ipv6**, **standby preempt**, **standby priority**. |

# Glossary

- **CPE** --Customer premises equipment
- **FHRP** --First hop redundancy protocol
- **GLBP** --Gateway load balancing protocol
- **HSRP** --Hot standby routing protocol
- **NA** --Neighbor advertisement
- **ND** --Neighbor Discovery
- **NS** --Neighbor solicitation
- **PE** --Provider equipment
- **RA** --Router advertisement
- **RS** --Router solicitation

CHAPTER 3

# Configuring HSRP

The Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) designed to allow for transparent failover of the first-hop IP device. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active device and a standby device. In a group of device interfaces, the active device is the device of choice for routing packets; the standby device is the device that takes over when the active device fails or when preset conditions are met.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for HSRP

- HSRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. HSRP is not intended as a replacement for existing dynamic protocols.

# Information About HSRP

## HSRP Operation

Most IP hosts have an IP address of a single device configured as the default gateway. When HSRP is used, the HSRP virtual IP address is configured as the host's default gateway instead of the IP address of the device.

HSRP is useful for hosts that do not support a discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new device when their selected device reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of devices running HSRP. The address of this HSRP group is referred to as the *virtual IP address*. One of these devices is selected by the protocol to be the active device. The active device receives and routes packets destined for the MAC address of the group. For *n* devices running HSRP, *n*+ 1 IP and MAC addresses are assigned.

HSRP detects when the designated active device fails, at which point a selected standby device assumes control of the MAC and IP addresses of the Hot Standby group. A new standby device is also selected at that time.

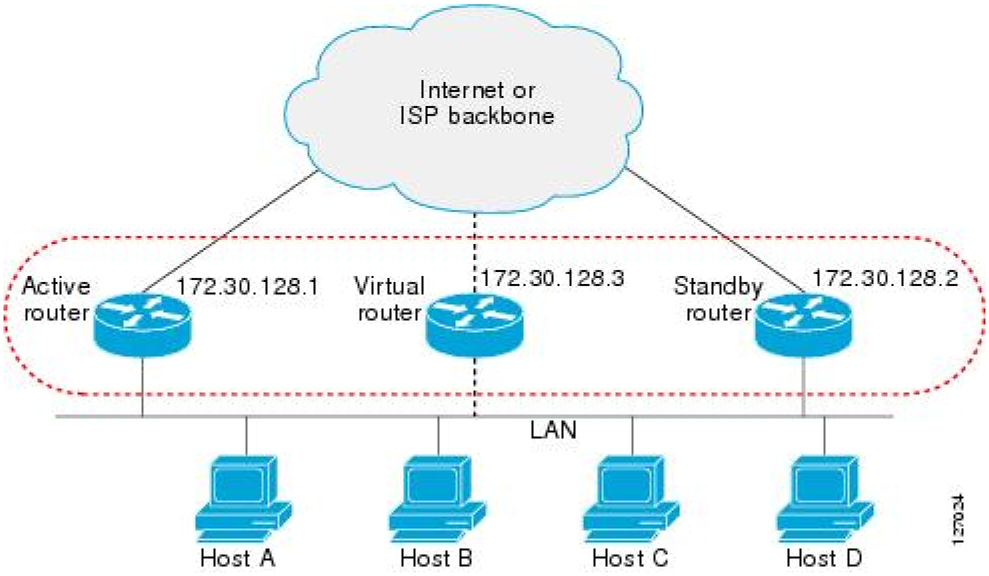
HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device.

Devices that are running HSRP send and receive multicast UDP-based hello messages to detect device failure and to designate active and standby devices. When the active device fails to send a hello message within a configurable period of time, the standby device with the highest priority becomes the active device. The transition of packet forwarding functions between devices is completely transparent to all hosts on the network.

You can configure multiple Hot Standby groups on an interface, thereby making fuller use of redundant devices and load sharing.

The figure below shows a network configured for HSRP. By sharing a virtual MAC address and IP address, two or more devices can act as a single *virtual router*. The virtual device does not physically exist but represents the common default gateway for devices that are configured to provide backup to each other. You do not need to configure the hosts on the LAN with the IP address of the active device. Instead, you configure them with the IP address (virtual IP address) of the virtual device as their default gateway. If the active device fails to send a hello message within the configurable period of time, the standby device takes over and responds to the virtual addresses and becomes the active device, assuming the active device duties.

*Figure 2: HSRP Topology*



# HSRP Version 2 Design

HSRP version 2 is designed to address the following restrictions in HSRP version 1:

- In HSRP version 1, millisecond timer values are not advertised or learned. HSRP version 2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
- HSRP version 2 provides improved management and troubleshooting. With HSRP version 1, you cannot use HSRP active hello messages to identify which physical device sent the message because the source MAC address is the HSRP virtual MAC address. The HSRP version 2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.
- The multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing.

Version 1 is the default version of HSRP.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, used by HSRP version 1. This new multicast address allows CGMP leave processing to be enabled at the same time as HSRP.

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF. The increased group number range does not imply that an interface can, or should, support that many HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

HSRP version 2 has a different packet format than HSRP version 1. The packet format uses a type-length-value (TLV) format. HSRP version 2 packets received by an HSRP version 1 device will have the type field mapped to the version field by HSRP version 1 and subsequently ignored.

The Gateway Load Balancing Protocol (GLBP) also addresses the same restrictions relative to HSRP version 1 that HSRP version 2 does. See the *Configuring GLBP* document for more information on GLBP.

### Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

## HSRP Configuration Changes

With CSCsv12265, an HSRP group may be configured with a virtual IP address that matches the subnet of an IP address of a secondary interface.

When the virtual IP address of an HSRP group is configured with the same network ID as a secondary interface IP address, the source address of HSRP messages is automatically set to the most appropriate interface address. This configuration change allows the following configuration:

```
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 secondary
 standby 1 ip 192.168.1.254
 standby 1 priority 105
 standby 1 preempt
 standby 2 ip 192.168.2.254 !Same network ID as secondary interface
```

Prior to CSCsv12265, an HSRP group remained in INIT state unless the HSRP virtual IP address had the same network ID as the primary interface address.

In addition, the following warning message is displayed if an HSRP group address is configured when no interface addresses are configured:

```
% Warning: address is not within a subnet on this interface
```

## HSRP Benefits

### Redundancy

HSRP employs a redundancy scheme that is time proven and deployed extensively in large networks.

### Fast Failover

HSRP provides transparent fast failover of the first-hop device.

### Preemption

Preemption allows a standby device to delay becoming active for a configurable amount of time.

### Authentication

HSRP message digest 5 (MD5) algorithm authentication protects against HSRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

## HSRP Groups and Group Attributes

You can use the CLI to apply group attributes to:

- A single HSRP group—performed in interface configuration mode and applies to a group.
- All groups on the interface—performed in interface configuration mode and applies to all groups on the interface.
- All groups on all interfaces—performed in global configuration mode and applies to all groups on all interfaces.

## HSRP Preemption

When a newly reloaded device becomes HSRP active, and there is already an HSRP active device on the network, HSRP preemption may appear to not function. HSRP preemption may appear not function correctly because the new HSRP active device did not receive any hello packets from the current HSRP active device, and the preemption configuration never factored into the new device's decision making.

HSRP may appear to not function on some larger hardware platforms where there can be a delay in an interface receiving packets.

In general, we recommend that all HSRP devices have the following configuration:

**standby delay minimum 30 reload 60**

The **standby delay minimum reload** interface configuration command delays HSRP groups from initializing for the specified time after the interface comes up.

This is a different command than the **standby preempt delay** interface configuration command, which enables HSRP preemption delay.

## HSRP Priority and Preemption

Preemption enables the HSRP router with the highest priority to immediately become the active router. Priority is determined first by the configured priority value, and then by the IP address. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. In each case, a higher value is of greater priority. If you do not use the **standby preempt** interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

A standby router with equal priority but a higher IP address will not preempt the active router.

When a router first comes up, it does not have a complete routing table. You can set a preemption delay that allows preemption to be delayed for a configurable time period. This delay period allows the router to populate its routing table before becoming the active router.

If preemption is not enabled, then a router may appear to preempt the active router if it does not receive any Hello messages from the active router.

# How Object Tracking Affects the Priority of an HSRP Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to HSRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced. The HSRP device with the higher priority can become the active device if it has the **standby preempt** command configured.

# HSRP Addressing

HSRP devices communicate between each other by exchanging HSRP hello packets. These packets are sent to the destination IP multicast address 224.0.0.2 (reserved multicast address used to communicate to all devices) on UDP port 1985. The active device sources hello packets from its configured IP address and the HSRP virtual MAC address while the standby device sources hellos from its configured IP address and the interface MAC address, which may or may not be the burned-in MAC address (BIA).

Because hosts are configured with their default gateway as the HSRP virtual IP address, hosts must communicate with the MAC address associated with the HSRP virtual IP address. This MAC address will be a virtual MAC address in the format of 0000.0C07.AC*xy*, where *xy* is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group one will use the HSRP virtual MAC address of 0000.0C07.AC01. Hosts on the adjoining LAN segment use the normal Address Resolution Protocol (ARP) process to resolve the associated MAC addresses.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, which is used by version 1. This new multicast address allows Cisco Group Management Protocol (CGMP) leave processing to be enabled at the same time as HSRP.

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF.

# HSRP Virtual MAC Addresses and BIA MAC Addresses

A device automatically generates a virtual MAC address for each HSRP device. However, some network implementations, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, specify the virtual MAC address by using the **standby mac-address** command in the group; the virtual IP address is unimportant for these protocols.

The **standby use-bia** command was implemented to overcome the limitations of using a functional address for the HSRP MAC address on Token Ring interfaces. This command allows HSRP groups to use the burned-in MAC address of an interface instead of the HSRP virtual MAC address. When HSRP runs on a multiple-ring, source-routed bridging environment and the HSRP devices reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

The **standby use-bia** command is used for an interface and the **standby mac-address** command is used for an HSRP group.

# HSRP Timers

Each HSRP device maintains three timers that are used for timing hello messages: an active timer, a standby timer, and a hello timer. When a timer expires, the device changes to a new HSRP state. Devices for which timer values are not configured can learn timer values from the active or standby device. The timers configured on the active device always override any other timer settings. All devices in a Hot Standby group should use the same timer values.

For HSRP version 1, nonactive devices learn timer values from the active device, unless millisecond timer values are being used. If millisecond timer values are being used, all devices must be configured with the millisecond timer values. This rule applies if either the hello time or the hold time is specified in milliseconds. This configuration is necessary because the HSRP hello packets advertise the timer values in seconds. HSRP version 2 does not have this limitation; it advertises the timer values in milliseconds.

### Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

# HSRP MAC Refresh Interval

When HSRP runs over FDDI, you can change the interval at which a packet is sent to refresh the MAC cache on learning bridges and switches. HSRP hello packets on FDDI interfaces use the burned-in address (BIA) instead of the MAC virtual address. Refresh packets keep the MAC cache on switches and learning bridges current. Refresh packets are also used for HSRP groups configured as multigroup slaves because these do not send regular Hello messages.

You can change the refresh interval on FDDI rings to a longer or shorter interval, thereby using bandwidth more efficiently. You can prevent the sending of any MAC refresh packets if you do not need them (if you have FDDI but do not have a learning bridge or switch).

# HSRP Text Authentication

HSRP ignores unauthenticated HSRP protocol messages. The default authentication type is text authentication.

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.

- Text authentication strings differ on the device and in the incoming packet.

## HSRP MD5 Authentication

Before the introduction of HSRP MD5 authentication, HSRP authenticated protocol packets with a simple plain text string. HSRP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain.

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device.

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.
- MD5 digests differ on the device and in the incoming packet.
- Text authentication strings differ on the device and in the incoming packet.

## HSRP Support for IPv6

Most IPv4 hosts have a single router’s IP address configured as the default gateway. When HSRP is used, then the HSRP virtual IP address is configured as the host’s default gateway instead of the router’s IP address. Simple load sharing may be achieved by using two HSRP groups and configuring half the hosts with one virtual IP address and half the hosts with the other virtual IP address.

In contrast, IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery Router Advertisement (RA) messages. These are multicast periodically, or may be solicited by hosts. HSRP is designed to provide only a virtual first hop for IPv6 hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number, and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. HSRP IPv6 uses the MAC address range 0005.73A0.0000 to 0005.73A0.0FFF. Periodic RAs are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent when the group leaves the active state.

Periodic RAs for the interface link-local address stop after a final RA is sent while at least one virtual IPv6 link-local address is configured on the interface. No restrictions occur for the interface IPv6 link-local address other than that mentioned for the RAs. Other protocols continue to receive and send packets to this address.

HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

For more information see the "Configuring First Hop Redundancy Protocols in IPv6" chapter of the *Cisco IOS IPv6 Configuration Guide*.

## HSRP Messages and States

Devices configured with HSRP exchange three types of multicast messages:

- Coup—When a standby device wants to assume the function of the active device, it sends a coup message.
- Hello—The hello message conveys to other HSRP device the HSRP priority and state information of the device.
- Resign—A device that is the active device sends this message when it is about to shut down or when a device that has a higher priority sends a hello or coup message.

At any time, a device configured with HSRP is in one of the following states:

- Active—The device is performing packet-transfer functions.
- Init or Disabled—The device is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other devices on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state.
- Learn—The device has not determined the virtual IP address and has not yet seen an authenticated hello message from the active device. In this state, the device still waits to hear from the active device.
- Listen—The device is receiving hello messages.
- Speak—The device is sending and receiving hello messages.
- Standby—The device is prepared to assume packet-transfer functions if the active device fails.

HSRP uses logging Level 5 for syslog messages related to HSRP state changes to allow logging of an event without filling up the syslog buffer on the device with low-priority Level 6 messaging.

## HSRP Group Linking to IP Redundancy Clients

HSRP provides stateless redundancy for IP routing. HSRP by itself is limited to maintaining its own state. Linking an IP redundancy client to an HSRP group provides a mechanism that allows HSRP to provide a service to client applications so they can implement stateful failover.

IP redundancy clients are other Cisco IOS processes or applications that use HSRP to provide or withhold a service or resource dependent upon the state of the group.

HSRP groups have a default name of **hsrp**-*interface-group* so specifying a group name is optional. For example, Group 1 on Ethernet0/0 has a default group name of "hsrp-Et0/0-1."

## HSRP Object Tracking

Object tracking separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process as well as HSRP. The priority of a device can change dynamically when it has been configured for object tracking and the object that is being tracked goes down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

A client process such as HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) can register its interest in tracking objects and then be notified when the tracked object changes state.

For more information about object tracking, see the "Configuring Enhanced Object Tracking" document.

## HSRP Group Shutdown

The FHRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down. Use the **standby track** command with the **shutdown** keyword to configure HSRP group shutdown.

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

## HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of Internet Control Message Protocol (ICMP) redirect messages is enabled on devices running HSRP.

ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP can send error packets to a host and can send redirect packets to a host.

When HSRP is running, preventing hosts from discovering the interface (or real) IP addresses of devices in the HSRP group is important. If a host is redirected by ICMP to the real IP address of a device, and that device later fails, then packets from the host will be lost.

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.

## ICMP Redirects to Active HSRP Devices

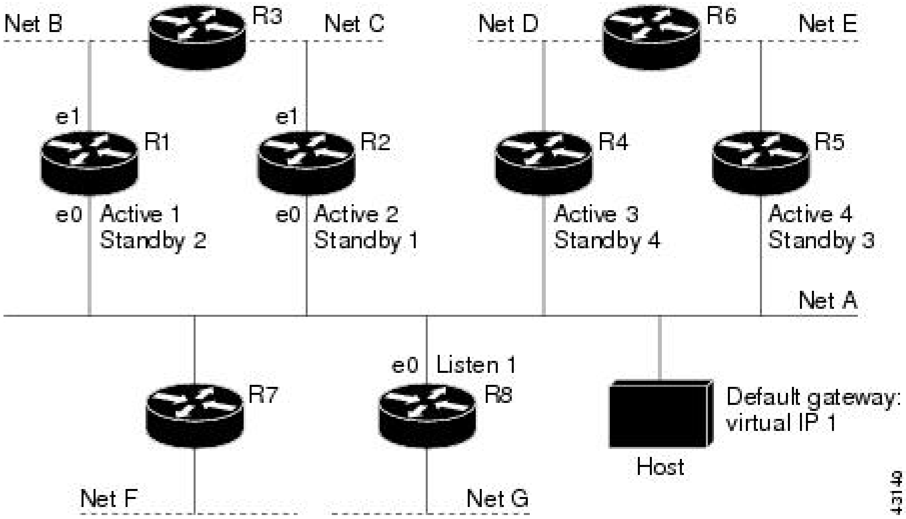
The next-hop IP address is compared to the list of active HSRP devices on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

If no match is found, then the ICMP redirect message is sent only if the device corresponding to the new next hop IP address is not running HSRP. Redirects to passive HSRP devices are not allowed (a passive HSRP device is a device running HSRP, but which contains no active HSRP groups on the interface).

For optimal operation, every device in a network that is running HSRP should contain at least one active HSRP group on an interface to that network. Every HSRP device need not be a member of the same group. Each HSRP device will snoop on all HSRP packets on the network to maintain a list of active devices (virtual IP addresses versus real IP addresses).

Consider the network shown in the figure below, which supports the HSRP ICMP redirection filter.

*Figure 3: Network Supporting the HSRP ICMP Redirection Filter*



If the host wants to send a packet to another host on Net D, then it first sends it to its default gateway, the virtual IP address of HSRP group 1.

The following is the packet received from the host:

```
dest MAC          = HSRP group 1 virtual MAC
source MAC        = Host MAC
dest IP           = host-on-netD IP
source IP         = Host IP
```

Device R1 receives this packet and determines that device R4 can provide a better path to Net D, so it prepares to send a redirect message that will redirect the host to the real IP address of device R4 (because only real IP addresses are in its routing table).

The following is the initial ICMP redirect message sent by device R1:

```
dest MAC          = Host MAC
source MAC        = router R1 MAC
dest IP           = Host IP
source IP         = router R1 IP
gateway to use    = router R4 IP
```

Before this redirect occurs, the HSRP process of device R1 determines that device R4 is the active HSRP device for group 3, so it changes the next hop in the redirect message from the real IP address of device R4 to the virtual IP address of group 3. Furthermore, it determines from the destination MAC address of the packet that triggered the redirect message that the host used the virtual IP address of group 1 as its gateway, so it changes the source IP address of the redirect message to the virtual IP address of group 1.

The modified ICMP redirect message showing the two modified fields (*) is as follows:

```
dest MAC          = Host MAC
source MAC        = router R1 MAC
dest IP           = Host IP
source IP*        = HSRP group 1 virtual IP
gateway to use*   = HSRP group 3 virtual IP
```

This second modification is necessary because hosts compare the source IP address of the ICMP redirect message with their default gateway. If these addresses do not match, the ICMP redirect message is ignored. The routing table of the host now consists of the default gateway, virtual IP address of group 1, and a route to Net D through the virtual IP address of group 3.

# ICMP Redirects to Passive HSRP Devices

ICMP redirects to passive HSRP devices are not permitted. Redundancy may be lost if hosts learn the real IP addresses of HSRP devices.

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R8 is not allowed because R8 is a passive HSRP device. In this case, packets from the host to Net D will first go to device R1 and then be forwarded to device R4; that is, they will traverse the network twice.

A network configuration with passive HSRP devices is considered a misconfiguration. For HSRP ICMP redirection to operate optimally, every device on the network that is running HSRP should contain at least one active HSRP group.

# ICMP Redirects to Non-HSRP Devices

ICMP redirects to devices not running HSRP on their local interface are permitted. No redundancy is lost if hosts learn the real IP address of non-HSRP devices.

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R7 is allowed because R7 is not running HSRP. In this case, the next hop IP address is unchanged. The source IP address is changed dependent upon the destination MAC address of the original packet. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

# Passive HSRP Advertisement Messages

Passive HSRP devices send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP devices can determine the HSRP group state of any HSRP device on the network. These advertisements inform other HSRP devices on the network of the HSRP interface state, as follows:

- Active—Interface has at least one active group. A single advertisement is sent out when the first group becomes active.
- Dormant—Interface has no HSRP groups. A single advertisement is sent once when the last group is removed.
- Passive—Interface has at least one nonactive group and no active groups. Advertisements are sent out periodically.

You can adjust the advertisement interval and hold-down time using the **standby redirect timers** command.

## ICMP Redirects Not Sent

If the HSRP device cannot uniquely determine the IP address used by the host when it sends the packet that caused the redirect, the redirect message will not be sent. The device uses the destination MAC address in the original packet to make this determination. In certain configurations, such as the use of the **standby use-bia** interface configuration command specified on an interface, redirects cannot be sent. In this case, the HSRP groups use the interface MAC address as their virtual MAC address. The device now cannot determine if the default gateway of the host is the real IP address or one of the HSRP virtual IP addresses that are active on the interface.

The IP source address of an ICMP packet must match the gateway address used by the host in the packet that triggered the ICMP packet, otherwise the host will reject the ICMP redirect packet. An HSRP device uses the destination MAC address to determine the gateway IP address of the host. If the HSRP device is using the same MAC address for multiple IP addresses, uniquely determining the gateway IP address of the host is not possible, and the redirect message is not sent.

The following is sample output from the **debug standby events icmp** EXEC command if HSRP could not uniquely determine the gateway used by the host:

```
10:43:08: HSRP: ICMP redirect not sent to 10.0.0.4 for dest 10.0.1.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

## HSRP Support for MPLS VPNs

HSRP support for a Multiprotocol Label Switching (MPLS) VPN interface is useful when an Ethernet LAN is connected between two provider edge (PE) devices with either of the following conditions:

- A customer edge (CE) device with a default route to the HSRP virtual IP address
- One or more hosts with the HSRP virtual IP address configured as the default gateway

Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding table
- Set of interfaces that use the Cisco Express Forwarding forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of routing and Cisco Express Forwarding tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a device within the VPN.

HSRP adds ARP entries and IP hash table entries (aliases) using the default routing table instance. However, a different routing table instance is used when VRF forwarding is configured on an interface, causing ARP and ICMP echo requests for the HSRP virtual IP address to fail.

HSRP support for MPLS VPNs ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table.

# HSRP Multiple Group Optimization

The configuration of many hundreds of subinterfaces on the same physical interface, with each subinterface having its own HSRP group, can cause the processes of negotiation and maintenance of multiple HSRP groups to have a detrimental impact on network traffic and CPU utilization.

Only one HSRP group is required on a physical interface for the purposes of electing active and standby devices. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups.

The HSRP group state of the client groups follows that of the master group. Client groups do not participate in any sort of device election mechanism.

Client groups send periodic messages in order to refresh their virtual MAC addresses in switches and learning bridges. The refresh message may be sent at a much lower frequency compared with the protocol election messages sent by the master group.

# HSRP—ISSU

The In Service Software Upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* document in the *High Availability Configuration Guide*.

# SSO HSRP

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

With this functionality, HSRP SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP device, then the standby HSRP device takes over as the active HSRP device.

The feature is enabled by default when the redundancy mode of operation is set to SSO.

## SSO Dual-Route Processors and Cisco Nonstop Forwarding

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

SSO is generally used with Cisco nonstop forwarding (NSF). Cisco NSF enables forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, users are less likely to experience service outages.

### HSRP and SSO Working Together

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Prior to introduction of the SSO HSRP feature, when the primary RP of the active device failed, it would stop participating in the HSRP group and trigger another switch in the group to take over as the active HSRP switch.

SSO HSRP is required to preserve the forwarding path for traffic destined to the HSRP virtual IP address through an RP switchover.

Configuring SSO on the edge device enables the traffic on the Ethernet links to continue during an RP failover without the Ethernet traffic switching over to an HSRP standby device (and then back, if preemption is enabled).

**Note** You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

## HSRP BFD Peering

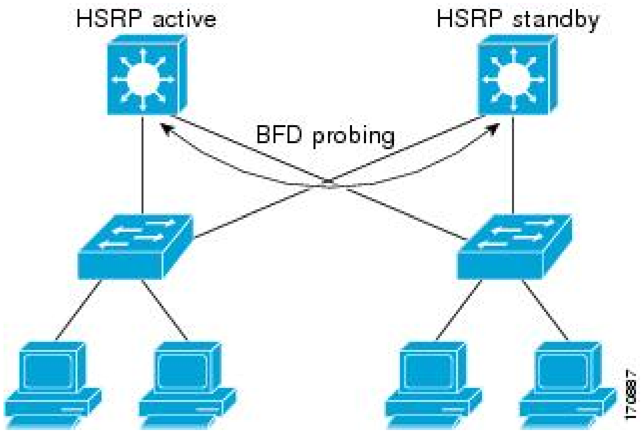
The HSRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the Hot Standby Router Protocol (HSRP) group member health monitoring system. HSRP supports BFD as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with hello and hold timers, in milliseconds. BFD runs as a pseudopreemptive process and can therefore be guaranteed to run when required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

This feature is enabled by default. The HSRP standby device learns the real IP address of the HSRP active device from the HSRP hello messages. The standby device registers as a BFD client and asks to be notified if the active device becomes unavailable. When BFD determines that the connections between standby and active devices has failed, it will notify HSRP on the standby device which will immediately take over as the active device.

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent devices, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between devices. Therefore, to create a BFD session, you must configure BFD on both systems (or BFD peers). When BFD is enabled on the interfaces and at the device level for HSRP, a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols such as, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Hot Standby Router Protocol (HSRP), Intermediate System To Intermediate System (IS-IS), and Open Shortest Path First (OSPF). By sending rapid failure detection notices to the routing protocols in the local device to initiate the routing table recalculation process, BFD contributes to greatly reduce overall network convergence time. The figure below shows a simple network with two devices running HSRP and BFD.

*Figure 4: HSRP BFD Peering*



For more information about BFD, see the *IP Routing: BFD Configuration Guide*.

# HSRP MIB Traps

HSRP MIB supports Simple Network Management Protocol (SNMP) Get operations, to allow network devices to get reports about HSRP groups in a network from the network management station.

Enabling HSRP MIB trap support is performed through the CLI, and the MIB is used for getting the reports. A trap notifies the network management station when a device leaves or enters the active or standby state. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

Cisco software supports a read-only version of the MIB, and set operations are not supported.

This functionality supports four MIB tables, as follows:

- cHsrpGrpEntry table defined in CISCO-HSRP-MIB.my
- cHsrpExtIfTrackedEntry, defined in CISCO-HSRP-EXT-MIB.my
- cHsrpExtSecAddrEntry, defined in CISCO-HSRP-EXT-MIB.my
- cHsrpExtIfEntry defined in CISCO-HSRP-EXT-MIB.my

The cHsrpGrpEntry table consists of all the group information defined in RFC 2281, *Cisco Hot Standby Router Protocol*; the other tables consist of the Cisco extensions to RFC 2281, which are defined in CISCO-HSRP-EXT-MIB.my.

# How to Configure HSRP

## Enabling HSRP

Perform this task to enable HSRP.

The **standby ip** interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the virtual IP address for the Hot Standby group. For HSRP to elect a designated device, you must configure the virtual IP address for at least one of the devices in the group; it can be learned on the other devices in the group.

### Before You Begin

You can configure many attributes in HSRP such as authentication, timers, priority, and preemption. You should configure the attributes before enabling the HSRP group. This practice avoids authentication error messages and unexpected state changes in other routers that can occur if the group is enabled first and then there is a long enough delay (one or two hold times) before the other attribues are configured.

We recommend that you always specify an HSRP IP address.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **end**
7. **show standby** [**all**] [**brief**]
8. **show standby** *type number* [*group-number* | **all**] [**brief**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 172.16.6.5 255.255.255.0` | Configures an IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 172.16.6.100` | Activates HSRP.<br>• If you do not configure a group number, the default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.<br>• The value for the *ip-address* argument is the virtual IP address of the virtual device. For HSRP to elect a designated device, you must configure the virtual IP address for at least one of the devices in the group; it can be learned on the other devices in the group. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show standby** [**all**] [**brief**]<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• This command displays information for each group. The **all** option displays groups that are learned or that do not have the **standby ip** command configured. |
| **Step 8** | **show standby** *type number* [*group-number* \| **all**] [**brief**]<br>**Example:**<br>`Device# show standby GigabitEthernet 0` | (Optional) Displays HSRP information about specific groups or interfaces. |

# Delaying the Initialization of HSRP on an Interface

The **standby delay** command is used to delay HSRP initialization either after a reload and/or after an interface comes up. This configuration allows the interface and device time to settle down after the interface up event and helps prevent HSRP state flapping.

We recommend that you use the **standby minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby delay minimum** *min-seconds* **reload** *reload-seconds*
6. **standby** [*group-number* ] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby delay** [*typenumber*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 1/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies an IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **standby delay minimum** *min-seconds* **reload** *reload-seconds*<br>**Example:**<br>`Device(config-if)# standby delay minimum 30 reload 60` | (Optional) Configures the delay period before the initialization of HSRP groups.<br>• The *min-seconds* value is the minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events.<br>• The *reload-seconds* value is the time period to delay after the device has reloaded. This delay period applies only to the first interface-up event after the device has reloaded.<br>**Note** The recommended *min-seconds* value is 30 and the recommended *reload-seconds* value is 60. |
| **Step 6** | **standby** [*group-number* ] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3 255.255.255.0` | Activates HSRP. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show standby delay** [*typenumber*]<br>**Example:**<br>`Device# show standby delay` | (Optional) Displays HSRP information about delay periods. |

# Configuring HSRP Priority and Preemption

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **ip** *ip-address* [**secondary**]]
8. **end**
9. **show standby** [**all**] [**brief**]
10. **show standby** *type number* [*group-number* | **all**] [**brief**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies an IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority.<br>• The default priority is 100. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt delay minimum 380` | Configures HSRP preemption and preemption delay.<br>• The default delay period is 0 seconds; if the device wants to preempt, it will do so immediately. By default, the device that comes up later becomes the standby. |
| **Step 7** | **standby** [*group-number*] **ip** *ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3 255.255.255.0` | Activates HSRP. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show standby** [**all**] [**brief**]<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• This command displays information for each group. The **all** option displays groups that are learned or that do not have the **standby ip** command configured. |
| **Step 10** | **show standby** *type number* [*group-number* \| **all**] [**brief**]<br>**Example:**<br>`Device# show standby GigabitEthernet 0/0/0` | (Optional) Displays HSRP information about specific groups or interfaces. |

# Configuring HSRP Object Tracking

Perform this task to configure HSRP to track an object and change the HSRP priority based on the state of the object.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes use this number to track a specific object.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** \| **ip routing**}<br>**Example:**<br>`Device(config)# track 100 interface GigabitEthernet 0/0/0 line-protocol` | Configures an interface to be tracked and enters tracking configuration mode. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-track)# exit` | Returns to global configuration mode. |
| **Step 5** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 6** | **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**] | Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-if)# standby 1 track 100 decrement 20` | • By default, the priority of the device is decreased by 10 if a tracked object goes down. Use the **decrement** *priority-decrement* keyword and argument combination to change the default behavior.<br>• When multiple tracked objects are down and *priority-decrement* values have been configured, these configured priority decrements are cumulative. If tracked objects are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative.<br>• Use the **shutdown** keyword to disable the HRSP group on the device when the tracked object goes down.<br>**Note** If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.10.10.0` | Activates HSRP.<br>• The default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show track** [*object-number* \| **brief**] [**interface** [**brief**] \| **ip route** [**brief**] \| **resolution** \| **timers**]<br>**Example:**<br>`Device# show track 100 interface` | Displays tracking information. |

# Configuring HSRP MD5 Authentication Using a Key String

**Note** Text authentication cannot be combined with MD5 authentication for an HSRP group at any one time. When MD5 authentication is configured, the text authentication field in HSRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving device also has MD5 authentication enabled.

**Note** If you are changing a key string in a group of devices, change the active device last to prevent any HSRP state change. The active device should have its key string changed no later than one hold-time period, specified by the **standy timers** interface configuration command, after the nonactive devices. This procedure ensures that the nonactive devices do not time out the active device.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **terminal interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*]
8. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **terminal interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **authentication md5 key-string** [**0** \| **7**] *key* [**timeout** *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30` | Configures an authentication string for HSRP MD5 authentication.<br>• The *key* argument can be up to 64 characters in length. We recommended that at least 16 characters be used.<br>• No prefix to the *key* argument or specifying **0** means the key will be unencrypted.<br>• Specifying **7** means the key will be encrypted. The key-string authentication key will automatically be encrypted if the **service password-encryption** global configuration command is enabled.<br>• The **timeout** value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key. |
| **Step 8** | **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | Repeat Steps 1 through 8 on each device that will communicate. | — |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Configuring HSRP MD5 Authentication Using a Key Chain

Perform this task to configure HSRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **standby** [*group-number*] **priority** *priority*
11. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
12. **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*
13. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
14. Repeat Steps 1 through 12 on each device that will communicate.
15. **end**
16. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)# key chain hsrp1` | Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode. |
| **Step 4** | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 100` | Identifies an authentication key on a key chain and enters key-chain key configuration mode.<br>• The value for the*key-id* argument must be a number. |
| **Step 5** | **key-string** *string*<br>**Example:**<br>`Device(config-keychain-key)# key-string mno172` | Specifies the authentication string for a key.<br>• The value for the *string* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to key-chain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 10** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 11** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 12** | **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*<br>**Example:**<br>`Device(config-if)# standby 1 authentication md5 key-chain hsrp1` | Configures an authentication MD5 key chain for HSRP MD5 authentication.<br>• The key chain name must match the name specified in Step 3. |
| **Step 13** | **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.21.8.12` | Activates HSRP. |
| **Step 14** | Repeat Steps 1 through 12 on each device that will communicate. | — |
| **Step 15** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 16** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Troubleshooting HSRP MD5 Authentication

Perform this task if HSRP MD5 authentication is not operating correctly.

## SUMMARY STEPS

1. **enable**
2. **debug standby errors**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug standby errors**<br>**Example:**<br>`Device# debug standby errors` | Displays error messages related to HSRP.<br>• Error messages will be displayed for each packet that fails to authenticate, so use this command with care. |

### Examples

In the following example, Device A has MD5 text string authentication configured, but Device B has the default text authentication:

```
Device# debug standby errors

A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 confgd
 but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth
 failed
```

In the following example, both Device A and Device B have different MD5 authentication strings:

```
Device# debug standby errors

A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth
failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth
failed
```

# Configuring HSRP Text Authentication

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **authentication text** *string*<br>**Example:**<br>`Device(config-if)# standby 1 authentication text authentication1` | Configures an authentication string for HSRP text authentication.<br>• The default string is cisco. |
| **Step 8** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 9** | Repeat Steps 1 through 8 on each device that will communicate. | -- |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Configuring HSRP Timers

**Note** We recommend configuring a minimum hello-time value of 250 milliseconds and a minimum hold-time value of 800 milliseconds.

You can use the **standby delay** command to allow the interface to come up completely before HSRP initializes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]]
5. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Gigabit Ethernet 0/0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*<br>**Example:**<br>`Device(config-if)# standby 1 timers 5 15` | Configures the time between hello packets and the time before other devices declare the active Hot Standby or standby device to be down. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |

# Configuring an HSRP MAC Refresh Interval

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby mac-refresh** *seconds*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby mac-refresh** *seconds*<br>**Example:**<br>`Device(config-if)# standby mac-refresh 100` | Changes the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI.<br>• This command applies to HSRP running over FDDI only. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |

# Configuring Multiple HSRP Groups for Load Balancing

Perform this task to configure multiple HSRP groups for load balancing.

Multiple HSRP groups enable redundancy and load-sharing within networks and allow redundant devices to be more fully utilized. A device actively forwarding traffic for one HSRP group can be in standby or in the listen state for another group.

If two devices are used, then Device A would be configured as active for group 1 and standby for group 2. Device B would be standby for group 1 and active for group 2. Fifty percent of the hosts on the LAN would be configured with the virtual IP address of group 1 and the remaining hosts would be configured with the virtual IP address of group 2. See the Example: Configuring Multiple HSRP Groups for Load Balancing for a diagram and configuration example.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.
9. **exit**
10. Repeat Steps 3 through 9 on another device.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *delay*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address*] **secondary**]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 8** | On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups. | For example, Device A can be configured as an active device for group 1 and be configured as an active or standby device for another HSRP group with different priority and preemption values. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits to global configuration mode. |
| **Step 10** | Repeat Steps 3 through 9 on another device. | Configures multiple HSRP and enables load balancing on another device. |

# Improving CPU and Network Performance with HSRP Multiple Group Optimization

Perform this task to configure multiple HSRP client groups.

The **standby follow** command configures an HSRP group to become a slave of another HSRP group.

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

Use the **standby mac-refresh** *seconds* command to directly change the HSRP client group refresh interval. The default interval is 10 seconds and can be configured to as much as 255 seconds.

**Note**

- Client or slave groups must be on the same physical interface as the master group.
- A client group takes its state from the group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
    % Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

### Before You Begin

Configure the HSRP master group using the steps in the Configuring Multiple HSRP Groups for Load Balancing section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby mac-refresh** *seconds*
6. **standby** *group-number* **follow** *group-name*
7. **exit**
8. Repeat Steps 3 through 6 to configure additional HSRP client groups.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby mac-refresh** *seconds*<br>**Example:**<br>`Device(config-if)# standby mac-refresh 30` | Configures the HSRP client group refresh interval. |
| **Step 6** | **standby** *group-number* **follow** *group-name*<br>**Example:**<br>`Device(config-if)# standby 1 follow HSRP1` | Configures an HSRP group as a client group. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits to global configuration mode. |
| **Step 8** | Repeat Steps 3 through 6 to configure additional HSRP client groups. | Configures multiple HSRP client groups. |

# Enabling HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of ICMP redirect messages is enabled on devices running HSRP. Perform this task to reenable this feature on your device if it is disabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby redirect** [**timers** *advertisement holddown*] [**unknown**]
5. **end**
6. **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **standby redirect** [**timers** *advertisement holddown*] [**unknown**]<br>**Example:**<br>`Device(config-if)# standby redirect` | Enables HSRP filtering of ICMP redirect messages.<br>• You can also use this command in global configuration mode, which enables HSRP filtering of ICMP redirect messages on all interfaces configured for HSRP. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]<br>**Example:**<br>`Device# show standby redirect` | (Optional) Displays ICMP redirect information on interfaces configured with HSRP. |

# Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses

**Note** You cannot use the **standby use-bia** and **standby mac-address** commands in the same configuration; they are mutually exclusive.

The **standby use-bia** command has the following disadvantages:

- When a device becomes active the virtual IP address is moved to a different MAC address. The newly active device sends a gratuitous ARP response, but not all host implementations handle the gratuitous ARP correctly.
- Proxy ARP does not function when the **standby use-bia** command is configured. A standby device cannot cover for the lost proxy ARP database of the failed device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. Enter one of the following commands:
    - **standby** [*group-number*] **mac-address** *mac-address*
    - or
    - **standby use-bia** [**scope interface**]
    - or
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 172.16.6.5 255.255.255.0` | Configures an IP address for an interface. |
| **Step 5** | Enter one of the following commands:<br>• **standby** [*group-number*] **mac-address** *mac-address*<br>• or<br>• **standby use-bia** [**scope interface**]<br>• or<br>**Example:**<br>`Device(config-if)# standby 1 mac-address 5000.1000.1060`<br>**Example:**<br>`Device(config-if)# standby use-bia` | Specifies a virtual MAC address for HSRP.<br>• This command cannot be used on a Token Ring interface.<br>or<br>Configures HSRP to use the burned-in address of the interface as its virtual MAC address.<br>• The **scope interface** keywords specify that the command is configured just for the subinterface on which it was entered, instead of the major interface. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 172.16.6.100` | Activates HSRP. |

# Linking IP Redundancy Clients to HSRP Groups

### Before You Begin

Within the client application, you must first specify the same name as configured in the **standby name** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **name** [*redundancy-name*]
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface Ethernet 0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies an IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **name** [*redundancy-name*] | Configures the name of the standby group. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-if)# standby 1 name HSRP-1` | • HSRP groups have a default name of **hsrp**-*interface-group* so specifying a group name is optional. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.11` | Activates HSRP. |

# Changing to HSRP Version 2

HSRP version 2 was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.

**Note**

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 will not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same device. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby version** {**1** | **2**}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface vlan 400` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.10.28.1 255.255.255.0` | Sets an IP address for an interface. |
| **Step 5** | **standby version** {**1** \| **2**}<br>**Example:**<br>`Device(config-if)# standby version 2` | Changes the HSRP version. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 400 ip 10.10.28.5` | Activates HSRP.<br>• The group number range for HSRP version 2 is 0 through 4095. The group number range for HSRP version 1 is 0 through 255. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-if)# end` | Ends the current configuration session and returns to privileged EXEC mode. |
| **Step 8** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• HSRP version 2 information will be displayed if configured. |

# Enabling SSO Aware HSRP

The SSO aware HSRP is enabled by default when the redundancy mode is set to SSO. Perform this task to reenable HSRP to be SSO aware if it has been disabled.

**Note** You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **exit**
6. **no standby sso**
7. **standby sso**
8. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **redundancy**<br>**Example:**<br>`Device(config)# redundancy` | Enters redundancy configuration mode. |
| **Step 4** | **mode sso**<br>**Example:**<br>`Device(config-red)# mode sso` | Enables the redundancy mode of operation to SSO.<br>• HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-red)# exit` | Exits redundancy configuration mode. |
| **Step 6** | **no standby sso**<br>**Example:**<br>`Device(config)# no standby sso` | Disables HSRP SSO mode for all HSRP groups. |
| **Step 7** | **standby sso**<br>**Example:**<br>`Device(config)# standby sso` | Enables the SSO HSRP feature if you have disabled the functionality. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Ends the current configuration session and returns to privileged EXEC mode. |

# Verifying SSO Aware HSRP

To verify or debug HSRP SSO operation, perform the following steps from the active RP console.

## SUMMARY STEPS

1. **show standby**
2. **debug standby events ha**

## DETAILED STEPS

**Step 1** **show standby**

Use the **show standby** command to display the state of the standby RP, for example:

**Example:**

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
 State is Active (standby RP)
 Virtual IP address is 10.1.0.7
 Active virtual MAC address is unknown
```

```
  Local virtual MAC address is 000a.f3fd.5001 (bia)
 Hello time 1 sec, hold time 3 sec
 Authentication text “authword”
 Preemption enabled
 Active router is unknown
 Standby router is unknown
 Priority 110 (configured 120)
  Track object 1 state Down decrement 10
 Group name is “name1” (cfgd)
```

**Step 2** **debug standby events ha**

Use the**debug standby events ha** command to display the active and standby RPs, for example:

**Example:**

```
Device# debug standby events ha

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active
```

# Enabling HSRP MIB Traps

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps hsrp**
4. **snmp-server host** *host community-string* **hsrp**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server enable traps hsrp**<br>**Example:**<br>`Device(config)# snmp-server enable traps hsrp` | Enables the device to send SNMP traps and informs, and HSRP notifications. |
| **Step 4** | **snmp-server host** *host community-string* **hsrp**<br>**Example:**<br>`Device(config)# snmp-server host myhost.comp.com public hsrp` | Specifies the recipient of an SNMP notification operation, and that HSRP notifications be sent to the host. |

# Configuring BFD Session Parameters on an Interface

Perform this task to configure Bidirectional Forwarding Detection (BFD) on an interface by setting the baseline BFD session parameters on the interface. Repeat the steps in this task for each interface on which you want to run BFD sessions to BFD neighbors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface FastEthernet 6/0` | Enters interface configuration mode. |
| **Step 4** | **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*<br>**Example:**<br>`Device(config-if)# bfd interval 50 min_rx 50 multiplier 5` | Enables BFD on the interface. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode. |

# Configuring HSRP BFD Peering

Perform this task to enable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering. Repeat the steps in this task for each interface over which you want to run BFD sessions to HSRP peers.

HSRP supports BFD peering by default. If HSRP BFD peering is disabled, you can reenable it at the device level to enable BFD support globally for all interfaces or you can reenable it on a per-interface basis at the interface level.

### Before You Begin

Before you proceed with this task:

- HSRP must be running on all participating devices.
- Cisco Express Forwarding must be enabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby** [**neighbors**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip cef** [**distributed**]<br>**Example:**<br>`Device(config)# ip cef` | Enables Cisco Express Forwarding or distributed Cisco Express Forwarding. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface FastEthernet 6/0` | Enters interface configuration mode. |
| **Step 5** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.11 255.255.255.0` | Configures an IP address for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.11` | Activates HSRP. |
| **Step 7** | **standby bfd**<br>**Example:**<br>`Device(config-if)# standby bfd` | (Optional) Enables HSRP support for BFD on the interface. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 9** | **standby bfd all-interfaces**<br>**Example:**<br>`Device(config)# standby bfd all-interfaces` | (Optional) Enables HSRP support for BFD on all interfaces. |
| **Step 10** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits global configuration mode. |
| **Step 11** | **show standby** [**neighbors**]<br>**Example:**<br>`Device# show standby neighbors` | (Optional) Displays information about HSRP support for BFD. |

# Verifying HSRP BFD Peering

To verify Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering, use any of the following optional commands.

## SUMMARY STEPS

1. **show standby**
2. **show standby brief**
3. **show standby neighbors** [*type number*]
4. **show bfd neighbors**
5. **show bfd neighbors details**

## DETAILED STEPS

**Step 1** **show standby**

Use the **show standby** command to display HSRP information.

**Example:**

```
Device# show standby

FastEthernet2/0 - Group 1
  State is Active
    2 state changes, last state change 00:08:06
  Virtual IP address is 10.0.0.11
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.772 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 90 (expires in 8.268 sec)
    BFD enabled !
  Priority 110 (configured 110)
    Group name is "hsrp-Fa2/0-1" (default)
```

**Step 2** **show standby brief**

Use the **show standby brief** command to display HSRP standby device information in brief.

**Example:**

```
Device# show standby brief

Interface   Grp  Pri P State   Active  Standby                     Virtual IP

Et0/0       4    120 P Active  local   172.24.1.2                  172.24.1.254
Et1/0       6    120 P Active  local   FE80::A8BB:CCFF:FE00:3401   FE80::5:73FF:FEA0:6
```

**Step 3** **show standby neighbors** [*type number*]

Use the **show standby neighbors** command to display information about HSRP peer devices on an interface.

**Example:**

```
Device1# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
```

```
Device2# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

**Step 4** **show bfd neighbors**

Use the **show bfd neighbors** command to display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies.

**Example:**

```
Device# show bfd neighbors

IPv6 Sessions

NeighAddr                              LD/RD         RH/RS     State     Int

FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
```

**Step 5** **show bfd neighbors details**

Use the **details** keyword to display BFD protocol parameters and timers for each neighbor.

**Example:**

```
Device# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
10.0.0.2      10.0.0.1       5/0    Down      0    (0 )   Down      Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1            - Diagnostic: 0
             State bit: AdminDown  - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 0         - Length: 0
             My Discr.: 0          - Your Discr.: 0
             Min tx interval: 0    - Min rx interval: 0
             Min Echo interval: 0
```

# Configuration Examples for HSRP

## Example: Configuring HSRP Priority and Preemption

In the following example, Device A is configured to be the active device for group 1 because it has the higher priority and standby device for group 2. Device B is configured to be the active device for group 2 and standby device for group 1.

### Device A Configuration

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 95
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

### Device B Configuration

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 110
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

## Example: Configuring HSRP Object Tracking

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Gigabit Ethernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IP-routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on serial interface 1/0 in Device A fails, the HSRP group priority will be reduced and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Device A Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

### Device B Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

## Example: Configuring HSRP Group Shutdown

In the following example, the tracking process is configured to track the IP-routing capability of Gigabit Ethernet interface 0/0/0. HSRP on Gigabit Ethernet interface 0/0/1 then registers with the tracking process to be informed of any changes to the IP-routing state of Gigabit Ethernet interface 0/0/0. If the IP state on Gigabit Ethernet interface 0/0/0 goes down, the HSRP group is disabled.

If both Gigabit Ethernet interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Device A fails, the HSRP group will be disabled and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Device A Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

### Device B Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 shutdown
```

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

## Example: Configuring HSRP MD5 Authentication Using Key Strings

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring HSRP MD5 Authentication Using Key Chains

In the following example, HSRP queries the key chain “hsrp1” to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

### Device 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

### Device 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

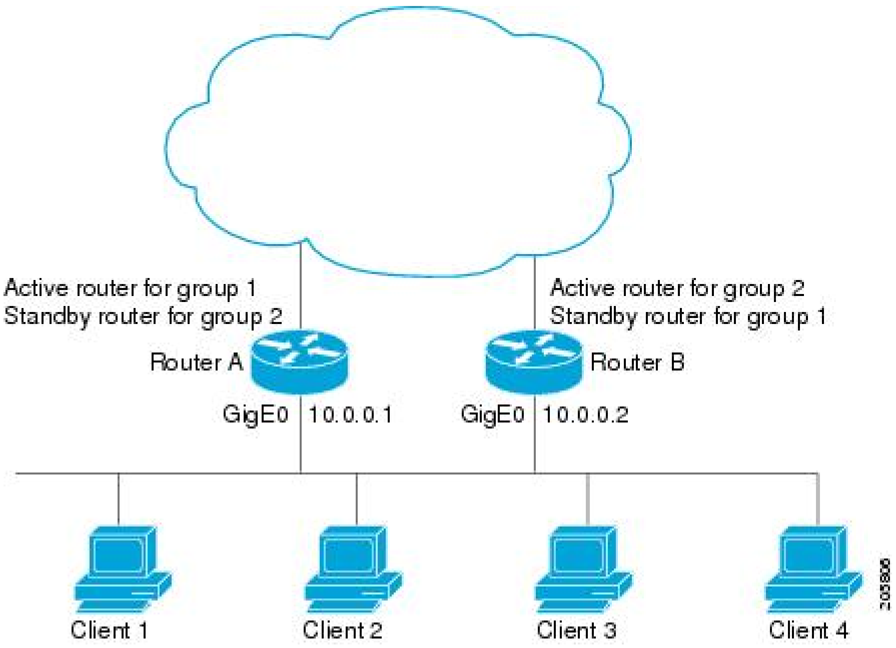
## Example: Configuring HSRP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring Multiple HSRP Groups for Load Balancing

You can use HSRP or multiple HSRP groups when you configure load sharing. In the figure below, half of the clients are configured for Router A, and half of the clients are configured for Router B. Together, the configuration for Routers A and B establish two Hot Standby groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable. The **standby preempt** interface configuration command is necessary so that if a router goes down and then comes back up, preemption occurs and restores load sharing.

*Figure 5: HSRP Load Sharing Example*


Active router for group 1
Standby router for group 2
Router A
GigE0
10.0.0.1
Active router for group 2
Standby router for group 1
Router B
GigE0
10.0.0.2
Client 1
Client 2
Client 3
Client 4
205806

The following example shows Router A configured as the active router for group 1 with a priority of 110 and Router B configured as the active router for group 2 with a priority of 110. The default priority level is 100. Group 1 uses a virtual IP address of 10.0.0.3 and Group 2 uses a virtual IP address of 10.0.0.4.

### Router A Configuration

```
Router(config)# hostname RouterA
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

### Router B Configuration

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

# Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization

The following example shows how to configure an HSRP client and master group:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
```

# Example: Configuring HSRP Support for ICMP Redirect Messages

### Device A Configuration—Active for Group 1 and Standby for Group 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.10 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

### Device B Configuration—Standby for Group 1 and Active for Group 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.11 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 120
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

# Example: Configuring HSRP Virtual MAC Addresses and BIA MAC Address

In an Advanced Peer-to-Peer Networking (APPN) network, an end node is typically configured with the MAC address of the adjacent network node. In the following example, if the end nodes are configured to use 4000.1000.1060, HSRP group 1 is configured to use the same MAC address:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1
Device(config-if)# standby 1 mac-address 4000.1000.1060
Device(config-if)# standby 1 ip 10.0.0.11
```

In the following example, the burned-in address of Token Ring interface 3/0 will be the virtual MAC address mapped to the virtual IP address:

```
Device(config)# interface token 3/0
Device(config-if)# standby use-bia
```

**Note** You cannot use the **standby use-bia** command and the **standby mac-address** command in the same configuration.

# Example: Linking IP Redundancy Clients to HSRP Groups

The following example shows HSRP support for a static Network Address Translation (NAT) configuration. The NAT client application is linked to HSRP via the correlation between the name specified by the **standby name** command. Two devices are acting as HSRP active and standby, and the NAT inside interfaces are HSRP enabled and configured to belong to the group named “group1.”

### Active Device Configuration

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.54 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 priority 110
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 track Ethernet 2/1
!
!
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 2/1
Device(config)# ip route 172.22.33.0 255.255.255.0 Ethernet 2/1
Device(config)# no ip http server
```

### Standby Device Configuration

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.56 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 priority 95
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 track Ethernet 3/1
Device(config-if)# exit
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 3.3.3.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.0.32.231 255.255.255 Ethernet 3/1
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 3/1
Device(config)# no ip http server
```

## Example: Configuring HSRP Version 2

The following example shows how to configure HSRP version 2 on an interface with a group number of 350:

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

## Example: Enabling SSO-Aware HSRP

The following example shows how to set the redundancy mode to SSO. HSRP is automatically SSO-aware when this mode is enabled.

```
Device(config)# redundancy
Device(config-red)# mode sso
```

If SSO HSRP is disabled using the **no standby sso** command, you can reenable it as shown in the following example:

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso
```

## Example: Enabling HSRP MIB Traps

The following examples show how to configure HSRP on two devices and enable the HSRP MIB trap support functionality. As in many environments, one device is preferred as the active one. To configure a device’s preference as the active device, configure the device at a higher priority level and enable preemption. In the following example, the active device is referred to as the primary device. The second device is referred to as the backup device:

### Device A

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host yourhost.cisco.com public hsrp
```

### Device B

```
Device(config)#interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.2 255.255.0.0
Device(config-if)#  standby priority 101
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host myhost.cisco.com public hsrp
```

# Example: HSRP BFD Peering

Hot Standby Router Protocol (HSRP) supports Bidirectional Forwarding Detection (BFD) as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with millisecond hello and hold timers. BFD runs as a pseudo-preemptive process and can therefore, be guaranteed to run when required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

In the following example, the **standby bfd** and the **standby bfd all-interfaces** commands are not displayed. HSRP support for BFD is enabled by default when BFD is configured on a device or an interface by using the **bfd interval** command. The **standby bfd** and **standby bfd all-interfaces** commands are needed only if BFD has been manually disabled on a device or an interface.

### Device A

```
DeviceA(config)# ip cef
DeviceA(config)# interface FastEthernet2/0
DeviceA(config-if)#  no shutdown
DeviceA(config-if)# ip address 10.0.0.2 255.0.0.0
DeviceA(config-if)# ip router-cache cef
DeviceA(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceA(config-if)# standby 1 ip 10.0.0.11
DeviceA(config-if)# standby 1 preempt
DeviceA(config-if)# standby 1 priority 110
DeviceA(config-if)# standby 2 ip 10.0.0.12
DeviceA(config-if)# standby 2 preempt
DeviceA(config-if)# standby 2 priority 110
```

### Device B

```
DeviceB(config)# interface FastEthernet2/0
DeviceB(config-if)# ip address 10.1.0.22 255.255.0.0
DeviceB(config-if)# no shutdown
DeviceB(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceB(config-if)# standby 1 ip 10.0.0.11
DeviceB(config-if)# standby 1 preempt
DeviceB(config-if)# standby 1 priority 90
DeviceB(config-if)# standby 2 ip 10.0.0.12
DeviceB(config-if)# standby 2 preempt
DeviceB(config-if)# standby 2 priority 80
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |

| RFCs | Title |
|---|---|
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 3: Feature Information for HSRP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP—HSRP BFD Peering | 15.2(1)S | The FHRP—HSRP BFD Peering feature introduces BFD in the HSRP group member health monitoring system. Previously, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory to produce and check. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers sub second health monitoring (failure detection in milliseconds) at a relatively low CPU impact.<br>The following commands were introduced or modified by this feature: **debug standby events neighbor**,**show standby**,**show standby neighbors**,**standby bfd**, **standby bfd all-interfaces**. |
| FHRP—HSRP Group Shutdown | 15.2(1)S | The FHRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down.<br>The following commands were modified by this feature:**standby track**, **show standby**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP—HSRP Multiple Group Optimization | 15.2(1)S | FHRP—HSRP Multiple Group Optimization feature improves the negotiation and maintenance of multiple HSRP groups configured on a subinterface. Only one HSRP group is required on a physical interface for the purposes of electing active and standby routers. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups.<br>The following commands were introduced or modified by this feature: **standby follow**, **show standby**. |
| FHRP—HSRP Support for IPv6 | 15.2(1)S | Support for IPv6 was added.<br>For more information see the "Configuring First Hop Redundancy Protocols in IPv6" module of the *Cisco IOS IPv6 Configuration Guide.* |

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP—ISSU | 15.2(1)S | The HSRP--ISSU feature enables support for ISSU in HSRP.<br>The In Service Software Upgrade (ISSU) process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.<br>For more information about this feature, see the "Cisco IOS In Service Software Upgrade Process" module in the *Cisco IOS High Availability Configuration Guide*. There are no new or modified commands for this feature. |
| HSRP MD5 Authentication | 15.2(1)S | Prior to the introduction of the HSRP MD5 Authentication feature, HSRP authenticated protocol packets with a simple plain text string. The HSRP MD5 Authentication feature is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This feature provides added security and protects against the threat from HSRP-spoofing software.<br>The following commands were introduced or modified by this feature: **show standby**, **standby authentication**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP Support for ICMP Redirects | 15.2(1)S | The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP.<br>The following commands were introduced or modified by this feature:<br>**debug standby event** , **debug standby events icmp**,**show standby**,**standby redirects** |
| HSRP Support for MPLS VPNs | 15.2(1)S | HSRP support for a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) interface is useful when an Ethernet LAN is connected between two provider edge (PE) routers with either of the following conditions:<br>There are no new or modified commands for this feature. |
| HSRP Version 2 | 15.2(1)S | HSRP Version 2 feature was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.<br>The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**. |
| SSO—HSRP | 15.2(1)S | The SSO—HSRP feature alters the behavior of HSRP when a router with redundant RPs is configured for SSO. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.<br>The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**. |

# Glossary

**ARP—**Address Resolution Protocol (ARP). ARP performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses. ARP is part of all Cisco IOS systems running IP.

**active device—**The primary device in an HSRP group that is currently forwarding packets for the virtual device.

**active RP—**The active RP that controls the system, provides network services, runs the routing protocols, and presents the system management interface.

**client group—**An HSRP group that is created on a subinterface and linked to the master group via the group name.

**HSRP—**Hot Standby Router Protocol. Protocol that provides high network availability and transparent network-topology changes. HSRP creates a router group with a lead device that services all packets sent to the HSRP address. The lead device is monitored by other devices in the group, and if it fails, one of these standby HSRP devices inherits the lead position and the HSRP group address.

**ISSU—**In Service Software Upgrade. A process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

**master group—**An HSRP group that is required on a physical interface for the purposes of electing active and standby devices.

**RF—**Redundancy Facility. A structured, functional interface used to notify its clients of active and standby state progressions and events.

**RP—**Route Processor. A generic term for the centralized control unit in a chassis.

**RPR—**Route Processor Redundancy. RPR provides an alternative to the High System Availability (HSA) feature. HSA enables a system to reset and use a standby Route Processor (RP) if the active RP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RP if the active RP experiences a fatal error.

**RPR+—**An enhancement to RPR in which the standby RP is fully initialized.

**standby group—**The set of devices participating in HSRP that jointly emulate a virtual device.

**standby device—**The backup device in an HSRP group.

**standby RP—**The backup RP.

**switchover—**An event in which system control and routing protocol execution are transferred from the active RP to the standby RP. Switchover may be a manual operation or may be induced by a hardware or software fault. Switchover may include transfer of the packet forwarding function in systems that combine system control and packet forwarding in an indivisible unit.

**virtual IP address—**The default gateway IP address configured for an HSRP group.

**virtual MAC address—**For Ethernet and FDDI, the automatically generated MAC address when HSRP is configured. The standard virtual MAC address used is: 0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. The functional address is used for Token Ring. The virtual MAC address is different for HSRP version 2.

CHAPTER 4

# HSRP: Global IPv6 Address

IPv6 routing protocols ensure device-to-device resilience and failover. However, in situations in which the path between a host and the first-hop device fails, or the first-hop device itself fails, first hop redundancy protocols (FHRPs) ensure host-to-device resilience and failover.

The Hot Standby Router Protocol (HSRP) protects data traffic in case of a gateway failure.

[other]

**A note on link local addresses**
The HSRP protocol uses a link local address as part of the protocol and this is not changed by the global address feature. Consider the global address feature as exchanging global addresses within the protocol for use, but the protocol itself still uses link locals for its protocol operation. If you only configure a global address, then there is a link-local address that is automatically allocated using the Extended Unique Identifier (EUI-64) method. You can use the **show standby** command to see the allocated link local address. You can still configure an IPv6 link local address by manual configuration if you require it. Manual configuration takes the group out of the 'implicit link-local' mode and replaces the automatic link local address with the configured one. If the configured one is later removed, but there is still a global address, then another implicit link local address is recalculated and applied.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

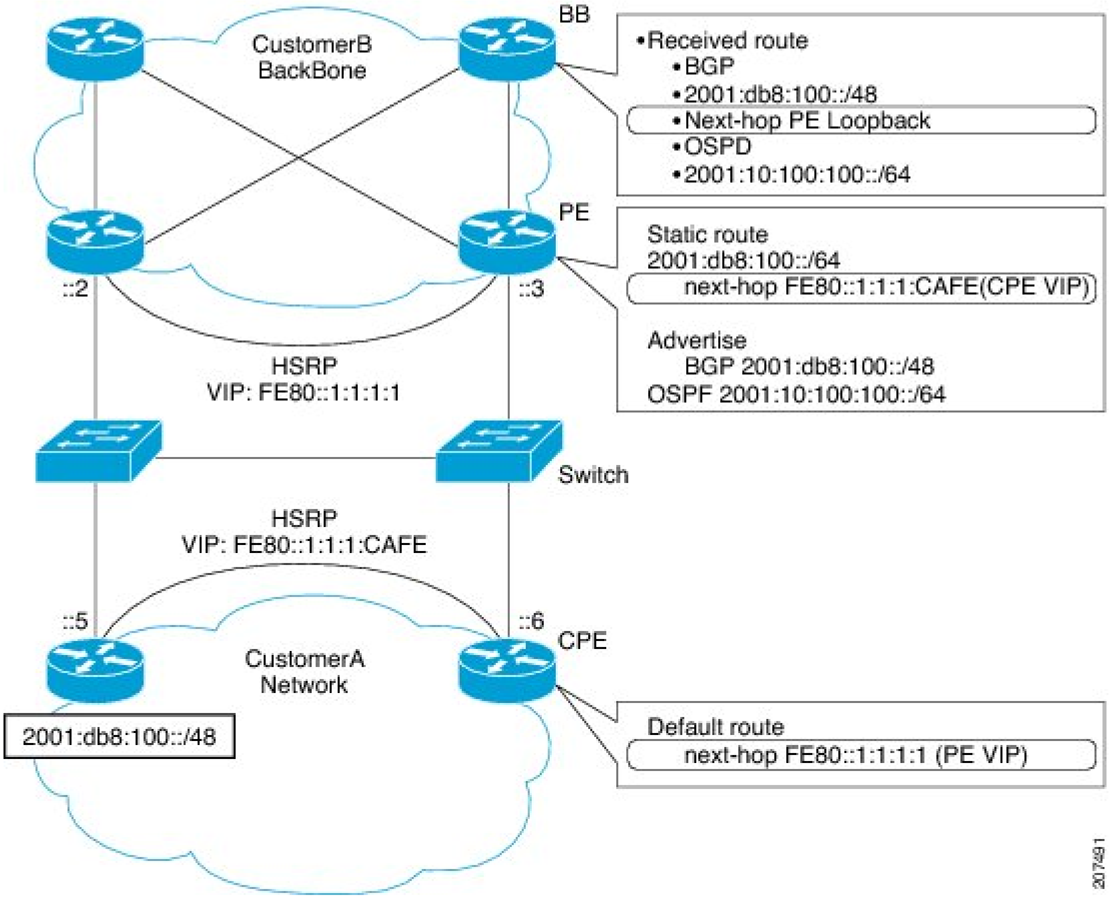
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About HSRP Global IPv6 Address

## HSRP: Global IPv6 Address

The HSRP global IPv6 address feature allows users to configure multiple nonlink local addresses as virtual addresses, and it allows for the storage and management of multiple global IPv6 virtual addresses in addition to the existing primary link-local address. If an IPv6 address is used, it must include an IPv6 prefix length. If a link-local address is used, it must not have a prefix.

The figure below depicts a deployment scenario that uses an HSRP IPv6 global virtual interface:



In the figure above, the provider equipment (PE) devices need to inject a route to reach the customer premises equipment (CPE) from the backbone devices. Because there are two CPEs, HSRP is convenient to use. The static route will be set with a link-local next hop (FE80::1:1:1:CAFE). If this address is injected in the backbone, this route is useless with a link-local next hop, as link-local addresses only have scope within the Layer 2 local LAN space. To address this issue, the next hop of the static route toward the virtual address must be set to a non link-local address, so backbone devices can route packets to the PE devices. At the next-hop address resolution, the active HSRP group member will reply to neighbor solicitation (NS) messages sent to the non link-local address.

### Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

# How to Enable HSRP Global IPv6 Address

## Enabling and Verifying an HSRP Group for IPv6 Operation

In this task, when you enter the **standby ipv6** command, a modified EUI-64 format interface identifier is generated in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address

In IPv6, a device on the link advertises in RA messages any site-local and global prefixes, and its willingness to function as a default device for the link. RA messages are sent periodically and in response to device solicitation messages, which are sent by hosts at system startup

A node on the link can automatically configure site-local and global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detec tion to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Device solicitation messages, which have a value of 133 in the Type field of the ICMPv6 packet header, are sent by hosts at system startup so that the host can immediately auto-configure without needing to wait for the next scheduled RA message.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **standby** [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address/prefix-length* | *ipv6-prefix/prefix-length* | *link-local-address* | **autoconfig**}
6. **standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*]
7. **standby** [*group-number*] **priority** *priority*
8. **exit**
9. **show standby** [*type number* [*group*]] [**all** | **brief**]
10. **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ipv6 unicast-routing**<br>**Example:**<br>`Device(config)# ipv6 unicast-routing` | Enables the forwarding of IPv6 unicast datagrams.<br>• The **ipv6 unicast-routing** command must be enabled for HSRP for IPv6 to work. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface ethernet 0/0` | Specifies an interface type and number, and places the device in interface configuration mode. |
| **Step 5** | **standby** [*group-number*] **ipv6** {*ipv6-global-address* \| *ipv6-address/prefix-length* \| *ipv6-prefix/prefix-length* \| *link-local-address* \| **autoconfig**}<br>**Example:**<br>`Device(config-if)# standby 1 ipv6 autoconfig` | Activates the HSRP in IPv6.<br>If an IPv6 address is used, it must include an IPv6 prefix length. If a link-local address is used, it must not have a prefix. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay minimum** *seconds* \| **reload** *seconds* \| **sync** *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption and preemption delay. |
| **Step 7** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **show standby** [*type number* [*group*]] [**all** \| **brief**]<br>**Example:**<br>`Device# show standby` | Displays HSRP information. |
| **Step 10** | **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]<br>**Example:**<br>`Device# show ipv6 interface ethernet 0/0` | Displays the usability status of interfaces configured for IPv6. |

# Configuration Example for HSRP Global IPv6 Address

## Example: Configuring HSRP Global IPv6 Addresses

This example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
Device(config)# interface ethernet 0/0
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001::DB8:1/64
Device(config-if)# standby 1 ipv6 FE80::1:CAFE
Device(config-if)# standby 1 ipv6 2001::DB8:2/64
Device(config-if)# standby 1 ipv6 2001:DB8::3/64
Device(config-if)# standby 1 ipv6 2001:DB8::4/64
Device(config-if)# exit
```

# Additional References for HSRP Global IPv6 Address

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| HSRP commands | *Cisco IOS First Hop Redundancy Protocols Command Reference* |
| Troubleshooting HSRP | *Hot Standby Router Protocol: Frequently Asked Questions* |
| IPv6 addressing and connectivity | *IPv6 Configuration Guide* |

| Related Topic | Document Title |
|---|---|
| IPv6 commands | *Cisco IOS IPv6 Command Reference* |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |

### RFCs

| RFCs | Title |
|---|---|
| RFCs for IPv6 | *IPv6 RFCs* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP: Global IPv6 Address

*Table 4: Feature Information for HSRP: Global IPv6 Address*

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP: Global IPv6 Address | 15.4(3)S | The HSRP global IPv6 address feature allows users to configure multiple non-link local addresses as virtual addresses.<br>The following commands were introduced or modified: **standby ipv6**. |

CHAPTER 5

# FHRP—HSRP BFD Peering

The FHRP—HSRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the Hot Standby Router Protocol (HSRP) group member health monitoring system. Before the introduction of this feature, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers second health monitoring (failure detection in milliseconds) at a relatively low CPU impact.

IPv6 and IPv4 HSRP groups support BFD. If BFD is configured on an interface, all IPv4 and IPv6 HSRP groups will automatically support BFD.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for FHRP—HSRP BFD Peering

Hot Standby Router Protocol (HSRP) support for Bidirectional Forwarding Detection (BFD) is not available for all platforms and interfaces.

# Information About FHRP—HSRP BFD Peering

## HSRP BFD Peering

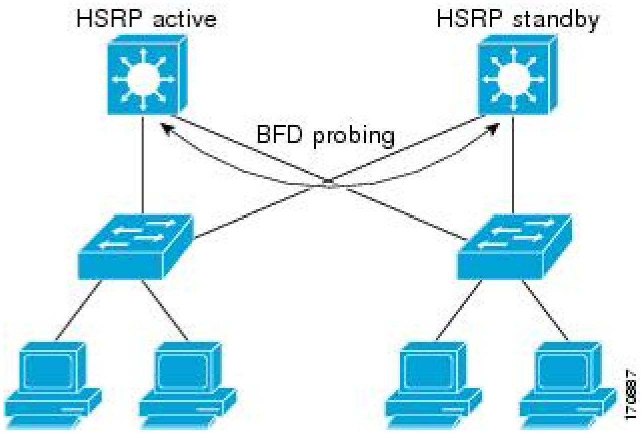
The HSRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the Hot Standby Router Protocol (HSRP) group member health monitoring system. HSRP supports BFD as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with hello and hold timers, in milliseconds. BFD runs as a pseudopreemptive process and can therefore be guaranteed to run when required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

This feature is enabled by default. The HSRP standby device learns the real IP address of the HSRP active device from the HSRP hello messages. The standby device registers as a BFD client and asks to be notified if the active device becomes unavailable. When BFD determines that the connections between standby and active devices has failed, it will notify HSRP on the standby device which will immediately take over as the active device.

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent devices, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between devices. Therefore, to create a BFD session, you must configure BFD on both systems (or BFD peers). When BFD is enabled on the interfaces and at the device level for HSRP, a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols such as, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Hot Standby Router Protocol (HSRP), Intermediate System To Intermediate System (IS-IS), and Open Shortest Path First (OSPF). By sending rapid failure detection notices to the routing protocols in the local device to initiate the routing table recalculation process, BFD contributes to greatly reduce overall network convergence time. The figure below shows a simple network with two devices running HSRP and BFD.

*Figure 6: HSRP BFD Peering*



For more information about BFD, see the *IP Routing: BFD Configuration Guide*.

# How to Configure FHRP—HSRP BFD Peering

## Configuring BFD Session Parameters on an Interface

Perform this task to configure Bidirectional Forwarding Detection (BFD) on an interface by setting the baseline BFD session parameters on the interface. Repeat the steps in this task for each interface on which you want to run BFD sessions to BFD neighbors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface FastEthernet 6/0` | Enters interface configuration mode. |
| **Step 4** | **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*<br>**Example:**<br>`Device(config-if)# bfd interval 50 min_rx 50 multiplier 5` | Enables BFD on the interface. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode. |

# Configuring HSRP BFD Peering

Perform this task to enable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering. Repeat the steps in this task for each interface over which you want to run BFD sessions to HSRP peers.

HSRP supports BFD peering by default. If HSRP BFD peering is disabled, you can reenable it at the device level to enable BFD support globally for all interfaces or you can reenable it on a per-interface basis at the interface level.

## Before You Begin

Before you proceed with this task:

- HSRP must be running on all participating devices.
- Cisco Express Forwarding must be enabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby** [**neighbors**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip cef** [**distributed**]<br>**Example:**<br>`Device(config)# ip cef` | Enables Cisco Express Forwarding or distributed Cisco Express Forwarding. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface FastEthernet 6/0` | Enters interface configuration mode. |
| **Step 5** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.11 255.255.255.0` | Configures an IP address for the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.11` | Activates HSRP. |
| **Step 7** | **standby bfd**<br>**Example:**<br>`Device(config-if)# standby bfd` | (Optional) Enables HSRP support for BFD on the interface. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode. |
| **Step 9** | **standby bfd all-interfaces**<br>**Example:**<br>`Device(config)# standby bfd all-interfaces` | (Optional) Enables HSRP support for BFD on all interfaces. |
| **Step 10** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits global configuration mode. |
| **Step 11** | **show standby** [**neighbors**]<br>**Example:**<br>`Device# show standby neighbors` | (Optional) Displays information about HSRP support for BFD. |

# Verifying HSRP BFD Peering

To verify Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering, use any of the following optional commands.

## SUMMARY STEPS

1. **show standby**
2. **show standby brief**
3. **show standby neighbors** [*type number*]
4. **show bfd neighbors**
5. **show bfd neighbors details**

## DETAILED STEPS

**Step 1** **show standby**

Use the **show standby** command to display HSRP information.

**Example:**

```
Device# show standby

FastEthernet2/0 - Group 1
  State is Active
    2 state changes, last state change 00:08:06
  Virtual IP address is 10.0.0.11
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.772 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 90 (expires in 8.268 sec)
    BFD enabled !
  Priority 110 (configured 110)
    Group name is "hsrp-Fa2/0-1" (default)
```

**Step 2** **show standby brief**

Use the **show standby brief** command to display HSRP standby device information in brief.

**Example:**

```
Device# show standby brief

Interface   Grp  Pri P State   Active  Standby                     Virtual IP

Et0/0       4    120 P Active  local   172.24.1.2                  172.24.1.254
Et1/0       6    120 P Active  local   FE80::A8BB:CCFF:FE00:3401   FE80::5:73FF:FEA0:6
```

**Step 3** **show standby neighbors** [*type number*]

Use the **show standby neighbors** command to display information about HSRP peer devices on an interface.

**Example:**

```
Device1# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
```

```
Device2# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

**Step 4** **show bfd neighbors**

Use the **show bfd neighbors** command to display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies.

**Example:**

```
Device# show bfd neighbors

IPv6 Sessions

NeighAddr                              LD/RD         RH/RS     State     Int

FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
```

**Step 5** **show bfd neighbors details**

Use the **details** keyword to display BFD protocol parameters and timers for each neighbor.

**Example:**

```
Device# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
10.0.0.2      10.0.0.1       5/0    Down      0    (0 )   Down      Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1            - Diagnostic: 0
             State bit: AdminDown  - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 0         - Length: 0
             My Discr.: 0          - Your Discr.: 0
             Min tx interval: 0    - Min rx interval: 0
             Min Echo interval: 0
```

# Configuration Examples for FHRP—HSRP BFD Peering

## Example: HSRP BFD Peering

Hot Standby Router Protocol (HSRP) supports Bidirectional Forwarding Detection (BFD) as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with millisecond hello and hold timers. BFD runs as a pseudo-preemptive process and can therefore, be guaranteed to run when required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

In the following example, the **standby bfd** and the **standby bfd all-interfaces** commands are not displayed. HSRP support for BFD is enabled by default when BFD is configured on a device or an interface by using the **bfd interval** command. The **standby bfd** and **standby bfd all-interfaces** commands are needed only if BFD has been manually disabled on a device or an interface.

### Device A

```
DeviceA(config)# ip cef
DeviceA(config)# interface FastEthernet2/0
DeviceA(config-if)#  no shutdown
DeviceA(config-if)# ip address 10.0.0.2 255.0.0.0
DeviceA(config-if)# ip router-cache cef
DeviceA(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceA(config-if)# standby 1 ip 10.0.0.11
DeviceA(config-if)# standby 1 preempt
DeviceA(config-if)# standby 1 priority 110
DeviceA(config-if)# standby 2 ip 10.0.0.12
DeviceA(config-if)# standby 2 preempt
DeviceA(config-if)# standby 2 priority 110
```

### Device B

```
DeviceB(config)# interface FastEthernet2/0
DeviceB(config-if)# ip address 10.1.0.22 255.255.0.0
DeviceB(config-if)# no shutdown
DeviceB(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceB(config-if)# standby 1 ip 10.0.0.11
DeviceB(config-if)# standby 1 preempt
DeviceB(config-if)# standby 1 priority 90
DeviceB(config-if)# standby 2 ip 10.0.0.12
DeviceB(config-if)# standby 2 preempt
DeviceB(config-if)# standby 2 priority 80
```

# Additional References for FHRP—HSRP BFD Peering

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| BFD | “Bidirectional Forwarding Detection” module in the *IP Routing: BFD Configuration Guide* |
| HSRP commands | *Cisco IOS IP Application Services Command Reference* |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### RFCs

| RFCs | Title |
|---|---|
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

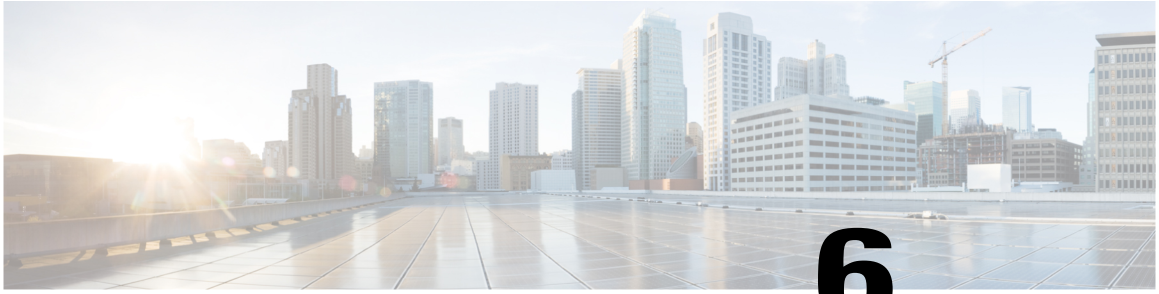
# Feature Information for FHRP—HSRP BFD Peering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 5: Feature Information for FHRP—HSRP BFD Peering*

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP—HSRP BFD Peering | 15.3(1)S | The FHRP-HSRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the Hot Standby Router Protocol (HSRP) group member health monitoring system. Before the introduction of this feature, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers second health monitoring (failure detection in milliseconds) at a relatively low CPU impact.<br>The following commands were introduced or modified by this feature: **debug standby events neighbor, show standby, show standby neighbors, standby bfd, standby bfd all-interfaces.** |
| FHRP—HSRP IPv6 BFD Peering | | The FHRP—HSRP IPv6 BFD Peering feature implements BFD support for IPv6 and IPv4 HSRP groups. |



CHAPTER 6

# HSRP Version 2

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About HSRP Version 2

## HSRP Version 2 Design

HSRP version 2 is designed to address the following restrictions in HSRP version 1:

- In HSRP version 1, millisecond timer values are not advertised or learned. HSRP version 2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
- HSRP version 2 provides improved management and troubleshooting. With HSRP version 1, you cannot use HSRP active hello messages to identify which physical device sent the message because the source

MAC address is the HSRP virtual MAC address. The HSRP version 2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.

- The multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing.

Version 1 is the default version of HSRP.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, used by HSRP version 1. This new multicast address allows CGMP leave processing to be enabled at the same time as HSRP.

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF. The increased group number range does not imply that an interface can, or should, support that many HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

HSRP version 2 has a different packet format than HSRP version 1. The packet format uses a type-length-value (TLV) format. HSRP version 2 packets received by an HSRP version 1 device will have the type field mapped to the version field by HSRP version 1 and subsequently ignored.

The Gateway Load Balancing Protocol (GLBP) also addresses the same restrictions relative to HSRP version 1 that HSRP version 2 does. See the *Configuring GLBP* document for more information on GLBP.

### Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

# How to Configure HSRP Version 2

## Changing to HSRP Version 2

HSRP version 2 was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.

Note

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 will not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same device. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby version** {**1** | **2**}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface vlan 400` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 10.10.28.1 255.255.255.0` | Sets an IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **standby version** {**1** \| **2**}<br>**Example:**<br>`Device(config-if)# standby version 2` | Changes the HSRP version. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 400 ip 10.10.28.5` | Activates HSRP.<br>• The group number range for HSRP version 2 is 0 through 4095. The group number range for HSRP version 1 is 0 through 255. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-if)# end` | Ends the current configuration session and returns to privileged EXEC mode. |
| **Step 8** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• HSRP version 2 information will be displayed if configured. |

# Configuration Examples for HSRP Version 2

## Example: Configuring HSRP Version 2

The following example shows how to configure HSRP version 2 on an interface with a group number of 350:

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

| Related Topic | Document Title |
|---|---|
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

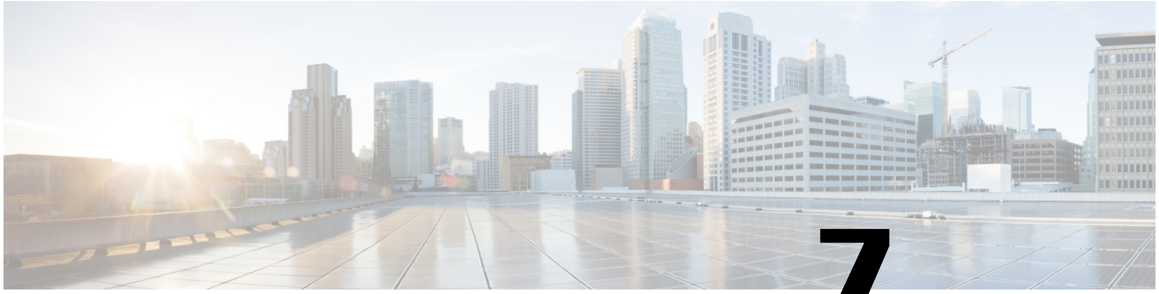
# Feature Information for HSRP Version 2

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 6: Feature Information for HSRP Version 2***

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP Version 2 | 12.2(25)S<br>15.0(1)S | HSRP Version 2 feature was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.<br>In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.<br>The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**. |



CHAPTER 7

# FHRP - HSRP Group Shutdown

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About FHRP - HSRP Group Shutdown

### How Object Tracking Affects the Priority of an HSRP Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to HSRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced. The HSRP device with the higher priority can become the active device if it has the **standby preempt** command configured.

## HSRP Object Tracking

Object tracking separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process as well as HSRP. The priority of a device can change dynamically when it has been configured for object tracking and the object that is being tracked goes down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

A client process such as HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) can register its interest in tracking objects and then be notified when the tracked object changes state.

For more information about object tracking, see the "Configuring Enhanced Object Tracking" document.

## HSRP Group Shutdown

The FHRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down. Use the **standby track** command with the **shutdown** keyword to configure HSRP group shutdown.

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

# How to Configure FHRP - HSRP Group Shutdown

## Configuring HSRP Object Tracking

Perform this task to configure HSRP to track an object and change the HSRP priority based on the state of the object.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes use this number to track a specific object.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** \| **ip routing**}<br>**Example:**<br>`Device(config)# track 100 interface GigabitEthernet 0/0/0 line-protocol` | Configures an interface to be tracked and enters tracking configuration mode. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config-track)# exit` | Returns to global configuration mode. |
| **Step 5** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 6** | **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]<br>**Example:**<br>`Device(config-if)# standby 1 track 100 decrement 20` | Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object.<br>• By default, the priority of the device is decreased by 10 if a tracked object goes down. Use the **decrement** *priority-decrement* keyword and argument combination to change the default behavior.<br>• When multiple tracked objects are down and *priority-decrement* values have been configured, these configured priority decrements are cumulative. If tracked objects are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative.<br>• Use the **shutdown** keyword to disable the HRSP group on the device when the tracked object goes down. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.10.10.0` | Activates HSRP.<br>• The default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show track** [*object-number* \| **brief**] [**interface** [**brief**] \| **ip route** [**brief**] \| **resolution** \| **timers**]<br>**Example:**<br>`Device# show track 100 interface` | Displays tracking information. |

# Configuring HSRP MD5 Authentication Using a Key String

**Note** Text authentication cannot be combined with MD5 authentication for an HSRP group at any one time. When MD5 authentication is configured, the text authentication field in HSRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving device also has MD5 authentication enabled.

**Note** If you are changing a key string in a group of devices, change the active device last to prevent any HSRP state change. The active device should have its key string changed no later than one hold-time period, specified by the **standy timers** interface configuration command, after the nonactive devices. This procedure ensures that the nonactive devices do not time out the active device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **terminal interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*]
8. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **terminal interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **authentication md5 key-string** [**0** \| **7**] *key* [**timeout** *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30` | Configures an authentication string for HSRP MD5 authentication.<br>• The *key* argument can be up to 64 characters in length. We recommended that at least 16 characters be used.<br>• No prefix to the *key* argument or specifying **0** means the key will be unencrypted.<br>• Specifying **7** means the key will be encrypted. The key-string authentication key will automatically be encrypted if the **service password-encryption** global configuration command is enabled.<br>• The **timeout** value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key. |
| **Step 8** | **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 9** | Repeat Steps 1 through 8 on each device that will communicate. | — |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Configuration Examples for FHRP - HSRP Group Shutdown

## Example: Configuring HSRP Object Tracking

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Gigabit Ethernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IP-routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on serial interface 1/0 in Device A fails, the HSRP group priority will be reduced and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Device A Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

### Device B Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

## Example: Configuring HSRP Group Shutdown

In the following example, the tracking process is configured to track the IP-routing capability of Gigabit Ethernet interface 0/0/0. HSRP on Gigabit Ethernet interface 0/0/1 then registers with the tracking process to be informed of any changes to the IP-routing state of Gigabit Ethernet interface 0/0/0. If the IP state on Gigabit Ethernet interface 0/0/0 goes down, the HSRP group is disabled.

If both Gigabit Ethernet interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Device A fails, the HSRP group will be disabled and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Device A Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
```

```
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

### Device B Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 shutdown
```

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | "HSRP for IPv6" module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for FHRP - HSRP Group Shutdown

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 7: Feature Information for FHRP—HSRP Group Shutdown*

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP—HSRP Group Shutdown | 12.4(9)T<br>12.2(33)SRC<br>12.2(33)SXI<br>12.2(50)SY<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1 | The FHRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down.<br>The following commands were modified by this feature:**standby track**, **show standby**. |

CHAPTER 8

# FHRP - HSRP Multiple Group Optimization

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About FHRP - Multiple Group Optimization

## HSRP Multiple Group Optimization

The configuration of many hundreds of subinterfaces on the same physical interface, with each subinterface having its own HSRP group, can cause the processes of negotiation and maintenance of multiple HSRP groups to have a detrimental impact on network traffic and CPU utilization.

Only one HSRP group is required on a physical interface for the purposes of electing active and standby devices. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups.

The HSRP group state of the client groups follows that of the master group. Client groups do not participate in any sort of device election mechanism.

Client groups send periodic messages in order to refresh their virtual MAC addresses in switches and learning bridges. The refresh message may be sent at a much lower frequency compared with the protocol election messages sent by the master group.

# How to configure FHRP - Multiple Group Optimization

## Configuring Multiple HSRP Groups for Load Balancing

Perform this task to configure multiple HSRP groups for load balancing.

Multiple HSRP groups enable redundancy and load-sharing within networks and allow redundant devices to be more fully utilized. A device actively forwarding traffic for one HSRP group can be in standby or in the listen state for another group.

If two devices are used, then Device A would be configured as active for group 1 and standby for group 2. Device B would be standby for group 1 and active for group 2. Fifty percent of the hosts on the LAN would be configured with the virtual IP address of group 1 and the remaining hosts would be configured with the virtual IP address of group 2. See the Example: Configuring Multiple HSRP Groups for Load Balancing for a diagram and configuration example.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.
9. **exit**
10. Repeat Steps 3 through 9 on another device.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *delay*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address*] **secondary**]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 8** | On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups. | For example, Device A can be configured as an active device for group 1 and be configured as an active or standby device for another HSRP group with different priority and preemption values. |
| **Step 9** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits to global configuration mode. |
| **Step 10** | Repeat Steps 3 through 9 on another device. | Configures multiple HSRP and enables load balancing on another device. |

# Improving CPU and Network Performance with HSRP Multiple Group Optimization

Perform this task to configure multiple HSRP client groups.

The **standby follow** command configures an HSRP group to become a slave of another HSRP group.

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

Use the **standby mac-refresh** *seconds* command to directly change the HSRP client group refresh interval. The default interval is 10 seconds and can be configured to as much as 255 seconds.

**Note**

- Client or slave groups must be on the same physical interface as the master group.
- A client group takes its state from the group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
    % Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

### Before You Begin

Configure the HSRP master group using the steps in the Configuring Multiple HSRP Groups for Load Balancing section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby mac-refresh** *seconds*
6. **standby** *group-number* **follow** *group-name*
7. **exit**
8. Repeat Steps 3 through 6 to configure additional HSRP client groups.

## DETAILED STEPS

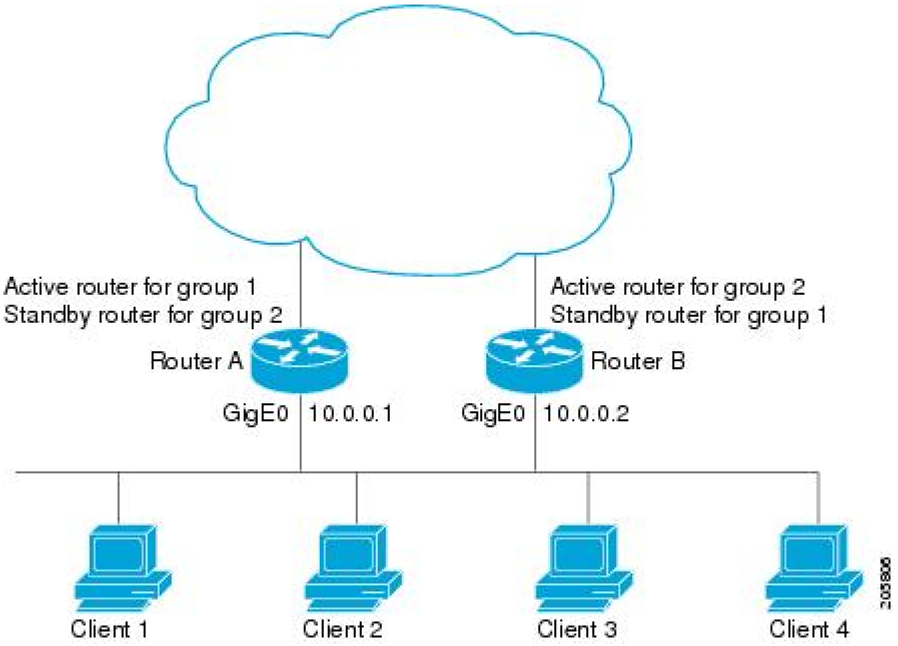
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby mac-refresh** *seconds*<br>**Example:**<br>`Device(config-if)# standby mac-refresh 30` | Configures the HSRP client group refresh interval. |
| **Step 6** | **standby** *group-number* **follow** *group-name*<br>**Example:**<br>`Device(config-if)# standby 1 follow HSRP1` | Configures an HSRP group as a client group. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits to global configuration mode. |
| **Step 8** | Repeat Steps 3 through 6 to configure additional HSRP client groups. | Configures multiple HSRP client groups. |

# Configuration Examples for FHRP - Multiple Group Optimization

## Example: Configuring Multiple HSRP Groups for Load Balancing

You can use HSRP or multiple HSRP groups when you configure load sharing. In the figure below, half of the clients are configured for Router A, and half of the clients are configured for Router B. Together, the configuration for Routers A and B establish two Hot Standby groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable. The **standby preempt** interface configuration command is necessary so that if a router goes down and then comes back up, preemption occurs and restores load sharing.

*Figure 7: HSRP Load Sharing Example*


Active router for group 1
Standby router for group 2
Router A
GigE0
10.0.0.1
Active router for group 2
Standby router for group 1
Router B
GigE0
10.0.0.2
Client 1
Client 2
Client 3
Client 4
205806

The following example shows Router A configured as the active router for group 1 with a priority of 110 and Router B configured as the active router for group 2 with a priority of 110. The default priority level is 100. Group 1 uses a virtual IP address of 10.0.0.3 and Group 2 uses a virtual IP address of 10.0.0.4.

### Router A Configuration

```
Router(config)# hostname RouterA
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

### Router B Configuration

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

## Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization

The following example shows how to configure an HSRP client and master group:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

| Related Topic | Document Title |
|---|---|
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for FHRP - HSRP Multiple Group Optimization

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 8: Feature Information for FHRP—HSRP Multiple Group Optimization*

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP—HSRP Multiple Group Optimization | 12.4(6)T<br>12.2(33)SRB<br>12.2(33)SXI<br>12.2(50)SY<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1 | FHRP—HSRP Multiple Group Optimization feature improves the negotiation and maintenance of multiple HSRP groups configured on a subinterface. Only one HSRP group is required on a physical interface for the purposes of electing active and standby devices. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups.<br>The following commands were introduced or modified by this feature: **standby follow**, **show standby**. |

CHAPTER 9

# HSRP - ISSU

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About HSRP - ISSU

### HSRP—ISSU

The In Service Software Upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* document in the *High Availability Configuration Guide*.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP - ISSU

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 9: Feature Information for HSRP—ISSU*

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP—ISSU | 12.2(31)SGA<br>12.2(33)SRB1<br>15.0(1)S<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE 3.1.0SG | The HSRP—ISSU feature enables support for ISSU in HSRP.<br>The In Service Software Upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.<br>For more information about this feature, see the Cisco IOS In Service Software Upgrade Process module in the *Cisco IOS High Availability Configuration Guide*. There are no new or modified commands for this feature. |

CHAPTER 10

# SSO HSRP

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for SSO HSRP

- Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with HSRP in SSO mode.

# Information About SSO HSRP

## SSO HSRP

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

With this functionality, HSRP SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP device, then the standby HSRP device takes over as the active HSRP device.

The feature is enabled by default when the redundancy mode of operation is set to SSO.

## SSO Dual-Route Processors and Cisco Nonstop Forwarding

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

SSO is generally used with Cisco nonstop forwarding (NSF). Cisco NSF enables forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, users are less likely to experience service outages.

## HSRP and SSO Working Together

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Prior to introduction of the SSO HSRP feature, when the primary RP of the active device failed, it would stop participating in the HSRP group and trigger another switch in the group to take over as the active HSRP switch.

SSO HSRP is required to preserve the forwarding path for traffic destined to the HSRP virtual IP address through an RP switchover.

Configuring SSO on the edge device enables the traffic on the Ethernet links to continue during an RP failover without the Ethernet traffic switching over to an HSRP standby device (and then back, if preemption is enabled).

**Note** You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

# How to Configure SSO HSRP

## Enabling SSO Aware HSRP

The SSO aware HSRP is enabled by default when the redundancy mode is set to SSO. Perform this task to reenable HSRP to be SSO aware if it has been disabled.

**Note** You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **exit**
6. **no standby sso**
7. **standby sso**
8. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **redundancy**<br>**Example:**<br>`Device(config)# redundancy` | Enters redundancy configuration mode. |
| **Step 4** | **mode sso** | Enables the redundancy mode of operation to SSO. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-red)# mode sso` | - HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset. |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-red)# exit` | Exits redundancy configuration mode. |
| **Step 6** | **no standby sso**<br>**Example:**<br>`Device(config)# no standby sso` | Disables HSRP SSO mode for all HSRP groups. |
| **Step 7** | **standby sso**<br>**Example:**<br>`Device(config)# standby sso` | Enables the SSO HSRP feature if you have disabled the functionality. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Ends the current configuration session and returns to privileged EXEC mode. |

# Verifying SSO Aware HSRP

To verify or debug HSRP SSO operation, perform the following steps from the active RP console.

### SUMMARY STEPS

1. **show standby**
2. **debug standby events ha**

### DETAILED STEPS

**Step 1** **show standby**
Use the **show standby** command to display the state of the standby RP, for example:

**Example:**

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
 State is Active (standby RP)
 Virtual IP address is 10.1.0.7
 Active virtual MAC address is unknown
  Local virtual MAC address is 000a.f3fd.5001 (bia)
 Hello time 1 sec, hold time 3 sec
 Authentication text "authword"
 Preemption enabled
 Active router is unknown
 Standby router is unknown
 Priority 110 (configured 120)
  Track object 1 state Down decrement 10
 Group name is "name1" (cfgd)
```

**Step 2** **debug standby events ha**

Use the**debug standby events ha** command to display the active and standby RPs, for example:

**Example:**

```
Device# debug standby events ha

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active
```

# Configuration Examples for SSO HSRP

## Example: Enabling SSO-Aware HSRP

The following example shows how to set the redundancy mode to SSO. HSRP is automatically SSO-aware when this mode is enabled.

```
Device(config)# redundancy
Device(config-red)# mode sso
```

If SSO HSRP is disabled using the **no standby sso** command, you can reenable it as shown in the following example:

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | "HSRP for IPv6" module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for SSO - HSRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 10: Feature Information for SSO—HSRP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| SSO—HSRP | 12.2(25)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.2(50)SY<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE 3.1.0SG | The SSO—HSRP feature alters the behavior of HSRP when a device with redundant RPs is configured for SSO. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.<br>The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**. |

CHAPTER 11

# HSRP MD5 Authentication

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About HSRP MD5 Authentication

## HSRP Text Authentication

HSRP ignores unauthenticated HSRP protocol messages. The default authentication type is text authentication.

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.

- Text authentication strings differ on the device and in the incoming packet.

## HSRP MD5 Authentication

Before the introduction of HSRP MD5 authentication, HSRP authenticated protocol packets with a simple plain text string. HSRP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain.

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device.

HSRP packets will be rejected in any of the following cases:

- The authentication schemes differ on the device and in the incoming packets.
- MD5 digests differ on the device and in the incoming packet.
- Text authentication strings differ on the device and in the incoming packet.

# How to Configure HSRP MD5 Authentication

## Configuring HSRP MD5 Authentication Using a Key Chain

Perform this task to configure HSRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **standby** [*group-number*] **priority** *priority*
11. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
12. **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*
13. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
14. Repeat Steps 1 through 12 on each device that will communicate.
15. **end**
16. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| Step 3 | **key chain** *name-of-chain*<br>**Example:**<br>`Device(config)# key chain hsrp1` | Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode. |
| Step 4 | **key** *key-id*<br>**Example:**<br>`Device(config-keychain)# key 100` | Identifies an authentication key on a key chain and enters key-chain key configuration mode.<br>• The value for the*key-id* argument must be a number. |
| Step 5 | **key-string** *string* | Specifies the authentication string for a key. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config-keychain-key)# key-string mno172` | • The value for the *string* argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-keychain-key)# exit` | Returns to key-chain configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 9** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 10** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 11** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 12** | **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*<br>**Example:**<br>`Device(config-if)# standby 1 authentication md5 key-chain hsrp1` | Configures an authentication MD5 key chain for HSRP MD5 authentication.<br>• The key chain name must match the name specified in Step 3. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.21.8.12` | Activates HSRP. |
| **Step 14** | Repeat Steps 1 through 12 on each device that will communicate. | — |
| **Step 15** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 16** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Troubleshooting HSRP MD5 Authentication

Perform this task if HSRP MD5 authentication is not operating correctly.

### SUMMARY STEPS

1. **enable**
2. **debug standby errors**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug standby errors**<br>**Example:**<br>`Device# debug standby errors` | Displays error messages related to HSRP.<br>• Error messages will be displayed for each packet that fails to authenticate, so use this command with care. |

### Examples

In the following example, Device A has MD5 text string authentication configured, but Device B has the default text authentication:

```
Device# debug standby errors

A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 confgd
 but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth
 failed
```

In the following example, both Device A and Device B have different MD5 authentication strings:

```
Device# debug standby errors

A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth
failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth
failed
```

# Configuring HSRP Text Authentication

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Device(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br>**Example:**<br>`Device(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br>**Example:**<br>`Device(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **authentication text** *string*<br>**Example:**<br>`Device(config-if)# standby 1 authentication text authentication1` | Configures an authentication string for HSRP text authentication.<br>• The default string is cisco. |
| **Step 8** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Device(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 9** | Repeat Steps 1 through 8 on each device that will communicate. | -- |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **show standby**<br>**Example:**<br>`Device# show standby` | (Optional) Displays HSRP information.<br>• Use this command to verify your configuration. The key string or key chain will be displayed if configured. |

# Configuration Examples for HSRP MD5 Authentication

## Example: Configuring HSRP MD5 Authentication Using Key Strings

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring HSRP MD5 Authentication Using Key Chains

In the following example, HSRP queries the key chain “hsrp1” to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

### Device 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

### Device 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

## Example: Configuring HSRP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP MD5 Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 11: Feature Information for HSRP MD5 Authentication*

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP MD5 Authentication | 12.2(25)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.2(50)SY<br>12.3(2)T<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE 3.1.0SG<br>Cisco IOS XE Release 3.9S | Prior to the introduction of the HSRP MD5 Authentication feature, HSRP authenticated protocol packets with a simple plain text string. The HSRP MD5 Authentication feature is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This feature provides added security and protects against the threat from HSRP-spoofing software.<br>The following commands were introduced or modified by this feature: **show standby**, **standby authentication**. |

CHAPTER 12

# HSRP Support for ICMP Redirects

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About HSRP Support for ICMP Redirects

### HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of Internet Control Message Protocol (ICMP) redirect messages is enabled on devices running HSRP.

ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP can send error packets to a host and can send redirect packets to a host.

When HSRP is running, preventing hosts from discovering the interface (or real) IP addresses of devices in the HSRP group is important. If a host is redirected by ICMP to the real IP address of a device, and that device later fails, then packets from the host will be lost.

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.

# ICMP Redirects to Active HSRP Devices

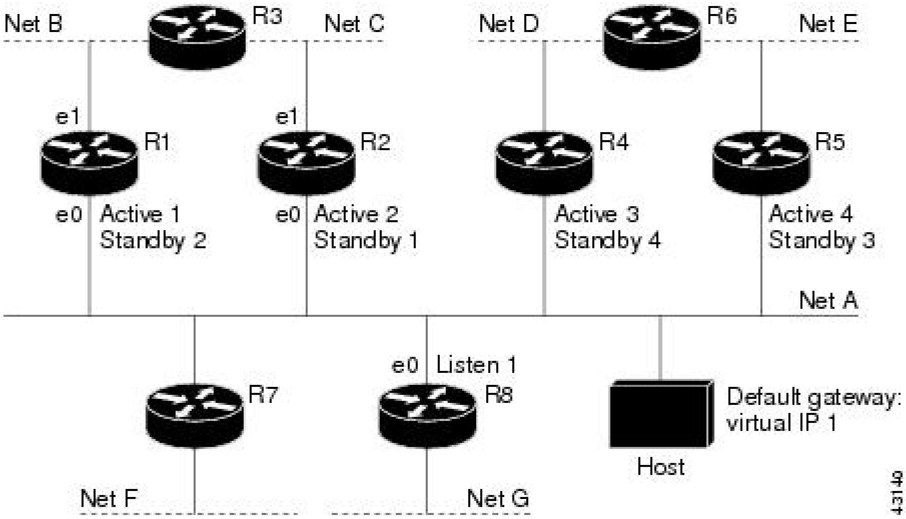
The next-hop IP address is compared to the list of active HSRP devices on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

If no match is found, then the ICMP redirect message is sent only if the device corresponding to the new next hop IP address is not running HSRP. Redirects to passive HSRP devices are not allowed (a passive HSRP device is a device running HSRP, but which contains no active HSRP groups on the interface).

For optimal operation, every device in a network that is running HSRP should contain at least one active HSRP group on an interface to that network. Every HSRP device need not be a member of the same group. Each HSRP device will snoop on all HSRP packets on the network to maintain a list of active devices (virtual IP addresses versus real IP addresses).

Consider the network shown in the figure below, which supports the HSRP ICMP redirection filter.

*Figure 8: Network Supporting the HSRP ICMP Redirection Filter*



If the host wants to send a packet to another host on Net D, then it first sends it to its default gateway, the virtual IP address of HSRP group 1.

The following is the packet received from the host:

```
dest MAC          = HSRP group 1 virtual MAC
source MAC        = Host MAC
dest IP           = host-on-netD IP
source IP         = Host IP
```

Device R1 receives this packet and determines that device R4 can provide a better path to Net D, so it prepares to send a redirect message that will redirect the host to the real IP address of device R4 (because only real IP addresses are in its routing table).

The following is the initial ICMP redirect message sent by device R1:

```
dest MAC         = Host MAC
source MAC       = router R1 MAC
dest IP          = Host IP
source IP        = router R1 IP
gateway to use   = router R4 IP
```

Before this redirect occurs, the HSRP process of device R1 determines that device R4 is the active HSRP device for group 3, so it changes the next hop in the redirect message from the real IP address of device R4 to the virtual IP address of group 3. Furthermore, it determines from the destination MAC address of the packet that triggered the redirect message that the host used the virtual IP address of group 1 as its gateway, so it changes the source IP address of the redirect message to the virtual IP address of group 1.

The modified ICMP redirect message showing the two modified fields (*) is as follows:

```
dest MAC         = Host MAC
source MAC       = router R1 MAC
dest IP          = Host IP
source IP*       = HSRP group 1 virtual IP
gateway to use*  = HSRP group 3 virtual IP
```

This second modification is necessary because hosts compare the source IP address of the ICMP redirect message with their default gateway. If these addresses do not match, the ICMP redirect message is ignored. The routing table of the host now consists of the default gateway, virtual IP address of group 1, and a route to Net D through the virtual IP address of group 3.

# ICMP Redirects to Passive HSRP Devices

ICMP redirects to passive HSRP devices are not permitted. Redundancy may be lost if hosts learn the real IP addresses of HSRP devices.

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R8 is not allowed because R8 is a passive HSRP device. In this case, packets from the host to Net D will first go to device R1 and then be forwarded to device R4; that is, they will traverse the network twice.

A network configuration with passive HSRP devices is considered a misconfiguration. For HSRP ICMP redirection to operate optimally, every device on the network that is running HSRP should contain at least one active HSRP group.

# ICMP Redirects to Non-HSRP Devices

ICMP redirects to devices not running HSRP on their local interface are permitted. No redundancy is lost if hosts learn the real IP address of non-HSRP devices.

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R7 is allowed because R7 is not running HSRP. In this case, the next hop IP address is unchanged. The source IP address is changed dependent upon the destination MAC address of the original packet. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

# Passive HSRP Advertisement Messages

Passive HSRP devices send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP devices can determine the HSRP group state of any HSRP device on the network. These advertisements inform other HSRP devices on the network of the HSRP interface state, as follows:

- Active—Interface has at least one active group. A single advertisement is sent out when the first group becomes active.
- Dormant—Interface has no HSRP groups. A single advertisement is sent once when the last group is removed.
- Passive—Interface has at least one nonactive group and no active groups. Advertisements are sent out periodically.

You can adjust the advertisement interval and hold-down time using the **standby redirect timers** command.

## ICMP Redirects Not Sent

If the HSRP device cannot uniquely determine the IP address used by the host when it sends the packet that caused the redirect, the redirect message will not be sent. The device uses the destination MAC address in the original packet to make this determination. In certain configurations, such as the use of the **standby use-bia** interface configuration command specified on an interface, redirects cannot be sent. In this case, the HSRP groups use the interface MAC address as their virtual MAC address. The device now cannot determine if the default gateway of the host is the real IP address or one of the HSRP virtual IP addresses that are active on the interface.

The IP source address of an ICMP packet must match the gateway address used by the host in the packet that triggered the ICMP packet, otherwise the host will reject the ICMP redirect packet. An HSRP device uses the destination MAC address to determine the gateway IP address of the host. If the HSRP device is using the same MAC address for multiple IP addresses, uniquely determining the gateway IP address of the host is not possible, and the redirect message is not sent.

The following is sample output from the **debug standby events icmp** EXEC command if HSRP could not uniquely determine the gateway used by the host:

```
10:43:08: HSRP: ICMP redirect not sent to 10.0.0.4 for dest 10.0.1.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

# How to Configure HSRP Support for ICMP Redirects

## Enabling HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of ICMP redirect messages is enabled on devices running HSRP. Perform this task to reenable this feature on your device if it is disabled.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby redirect** [**timers** *advertisement holddown*] [**unknown**]
5. **end**
6. **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| Step 4 | **standby redirect** [**timers** *advertisement holddown*] [**unknown**]<br>**Example:**<br>`Device(config-if)# standby redirect` | Enables HSRP filtering of ICMP redirect messages.<br>• You can also use this command in global configuration mode, which enables HSRP filtering of ICMP redirect messages on all interfaces configured for HSRP. |
| Step 5 | **end**<br>**Example:**<br>`Device(config-if)# end` | Returns to privileged EXEC mode. |
| Step 6 | **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]<br>**Example:**<br>`Device# show standby redirect` | (Optional) Displays ICMP redirect information on interfaces configured with HSRP. |

# Configuration Examples for HSRP Support for ICMP Redirects

## Example: Configuring HSRP Support for ICMP Redirect Messages

### Device A Configuration—Active for Group 1 and Standby for Group 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.10 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

### Device B Configuration—Standby for Group 1 and Active for Group 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.11 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 120
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP Support for ICMP Redirects

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 12: Feature Information for HSRP Support for ICMP Redirects***

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP Support for ICMP Redirects | 12.1(3)T<br>12.2(50)SY<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 3.9S | The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP.<br>The following commands were introduced or modified by this feature:<br>**debug standby event** , **debug standby events icmp**,**show standby**,**standby redirects** |

CHAPTER 13

# HSRP Support for MPLS VPNs

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About HSRP Support for MPLS VPNs

## HSRP Support for MPLS VPNs

HSRP support for a Multiprotocol Label Switching (MPLS) VPN interface is useful when an Ethernet LAN is connected between two provider edge (PE) devices with either of the following conditions:

- A customer edge (CE) device with a default route to the HSRP virtual IP address
- One or more hosts with the HSRP virtual IP address configured as the default gateway

Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding table

- Set of interfaces that use the Cisco Express Forwarding forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of routing and Cisco Express Forwarding tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a device within the VPN.

HSRP adds ARP entries and IP hash table entries (aliases) using the default routing table instance. However, a different routing table instance is used when VRF forwarding is configured on an interface, causing ARP and ICMP echo requests for the HSRP virtual IP address to fail.

HSRP support for MPLS VPNs ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop redundancy Protocols Command Reference* |
| HSRP for IPv6 | “HSRP for IPv6” module |
| Troubleshooting HSRP | Hot Standby Router Protocol: Frequently Asked Questions |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 2281 | *Cisco Hot Standby Router Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for HSRP Support for MPLS VPNs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 13: Feature Information for HSRP Support for MPLS VPNs*

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP Support for MPLS VPNs | 12.0(23)S<br>12.0(17)ST<br>12.2(28)SB<br>12.2(17b)SXA<br>12.2(8)T<br>12.2(50)SY<br>15.0(1)S<br>15.0(1)SY<br>Cisco IOS XE Release 2.1 | HSRP support for a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) interface is useful when an Ethernet LAN is connected between two provider edge (PE) devices under certain conditions.<br>There are no new or modified commands for this feature. |

CHAPTER 14

# Configuring IRDP

The ICMP Router Discovery Protocol (IRDP) allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks. For a complete description of the IPv4 addressing commands in this module, refer to the *Cisco IOS IP Application Services Command Reference*. To locate documentation of other commands that appear in this module, use the command reference master index or search online.

This module explains the concepts related to IRDP and describes how to configure IRDP in a network.

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About IRDP

## IRDP Overview

ICMP Router Discovery Protocol (IRDP) allows hosts to locate routers that can be used as a gateway to reach IP-based devices on other networks. When the device running IRDP operates as a router, router discovery packets are generated. When the device running IRDP operates as a host, router discovery packets are received. The Cisco IRDP implementation fully conforms to the router discovery protocol outlined in RFC 1256 (http://www.ietf.org/rfc/rfc1256.txt).

# How to Configure IRDP

## Configuring IRDP

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip routing**
4. **ip gdp irdp** [**multicast**]
5. **interface** *type number*
6. **no shutdown**
7. **ip address** *ip-address mask*
8. **ip irdp**
9. **ip irdp multicast**
10. **ip irdp holdtime** *seconds*
11. **ip irdp maxadvertinterval** *seconds*
12. **ip irdp minadvertinterval** *seconds*
13. **ip irdp preference** *number*
14. **ip irdp address** *address number*
15. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **no ip routing**<br>**Example:**<br>`Router(config)# no ip routing` | Disables IP routing |
| **Step 4** | **ip gdp irdp** [**multicast**]<br>**Example:**<br>`Router(config)# ip gdp irdp` | Configures a gateway to discover routers that transmit IRDP router updates. |
| **Step 5** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface fastethernet 0/0` | Specifies an interface and enters interface configuration mode. |
| **Step 6** | **no shutdown**<br>**Example:**<br>`Router(config-if)# no shutdown` | Activates (enables) the interface. |
| **Step 7** | **ip address** *ip-address mask*<br>**Example:**<br>`Router(config-if)# ip address 172.16.16.1 255.255.240.0` | Configures an IP address on the interface. |
| **Step 8** | **ip irdp**<br>**Example:**<br>`Router(config-if)# ip irdp` | Enables IRDP on the interface |
| **Step 9** | **ip irdp multicast**<br>**Example:**<br>`Router(config-if)# ip irdp multicast` | (Optional) Sends IRDP advertisements to the all-systems multicast address (224.0.0.1) on a specified interface. |
| **Step 10** | **ip irdp holdtime** *seconds*<br>**Example:**<br>`Router(config-if)# ip irdp holdtime 120` | (Optional) Sets the IRDP period for which advertisements are valid. |
| **Step 11** | **ip irdp maxadvertinterval** *seconds*<br>**Example:**<br>`Router(config-if)# ip irdp maxadvertinterval 60` | (Optional) Sets the IRDP maximum interval between advertisements. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **ip irdp minadvertinterval** *seconds*<br>**Example:**<br>`Router(config-if)# ip irdp minadvertinterval 10` | (Optional) Sets the IRDP minimum interval between advertisements. |
| **Step 13** | **ip irdp preference** *number*<br>**Example:**<br>`Router(config-if)# ip irdp preference 900` | (Optional) Sets the IRDP preference level of the device. |
| **Step 14** | **ip irdp address** *address number*<br>**Example:**<br>`Router(config-if)# ip irdp address 192.168.10.2 90` | (Optional) Specifies an IRDP address and preference to proxy-advertise. |
| **Step 15** | **end**<br>**Example:**<br>`Router(config-if)# end` | Exits the current configuration mode and returns to privileged EXEC mode. |

# Configuration Examples for IRDP

## Example: Configuring IRDP

The following example shows how to configure IRDP on a router:

```
Router(config)# no ip routing
Router(config)# ip gdp irdp
Router(config)# interface fastethernet 0/1
Router(config-if)# no shutdown
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# ip irdp
Router(config-if)# ip irdp multicast
Router(config-if)# ip irdp holdtime 120
Router(config-if)# ip irdp maxadvertinterval 60
Router(config-if)# ip irdp minadvertinterval 10
Router(config-if)# ip irdp preference 900
Router(config-if)# ip irdp address 192.168.10.2 90
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IP application services commands | Cisco IOS IP Application Services Command Reference |

### Standards and RFCs

| Standard | Title |
|---|---|
| RFC 1256 | ICMP Router Discovery Messages |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for IRDP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 14: Feature Information for IRDP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| ICMP Router Discovery Protocol | 15.2(1)S | The ICMP Router Discovery Protocol (IRDP) allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (non-local) IP networks.<br>The following command was introduced or modified: **ip irdp**. |

CHAPTER 15

# Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails.

This module explains the concepts related to VRRP and describes how to configure VRRP in a network.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for VRRP

- VRRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. VRRP is not intended as a replacement for existing dynamic protocols.
- VRRP is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must configure the VRRP advertise timer to a value equal to or greater than the forwarding delay on the BVI interface. This setting prevents a VRRP router on a recently initialized BVI interface from unconditionally taking over the master role. Use the **bridge forward-time** command to set the forwarding delay on the BVI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.
- Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with VRRP in SSO mode.

# Information About VRRP

## VRRP Operation

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- ICMP Router Discovery Protocol (IRDP) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

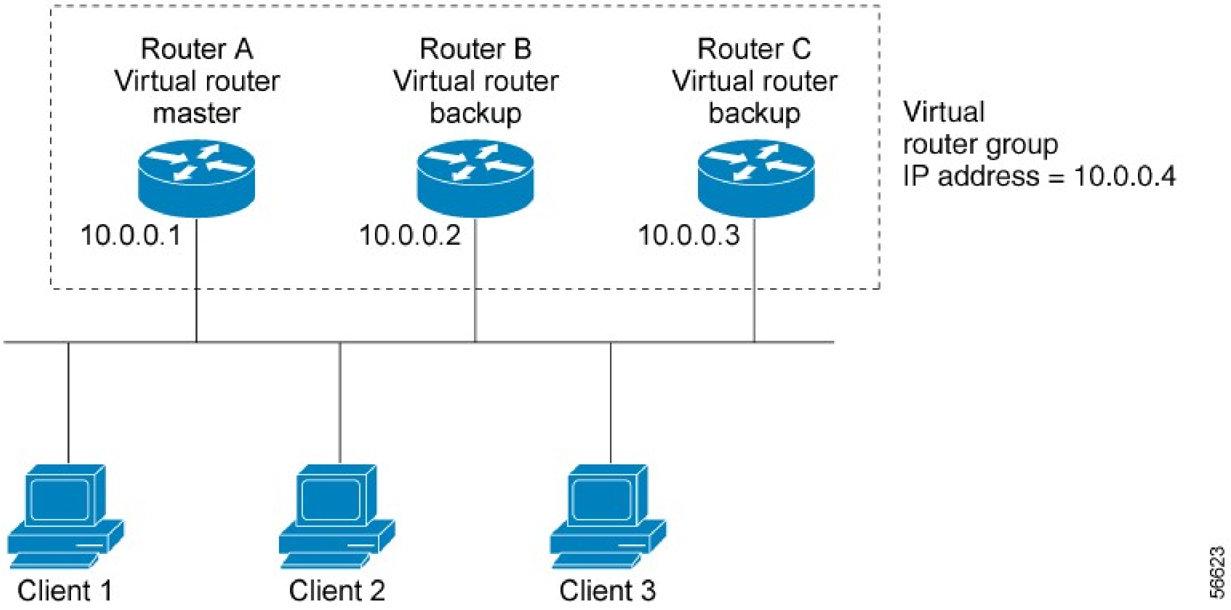
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single *virtual router*. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, and on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

The figure below shows a LAN topology in which VRRP is configured. In this example, Routers A, B, and C are VRRP routers (routers running VRRP) that comprise a virtual router. The IP address of the virtual router is the same as that configured for the Ethernet interface of Router A (10.0.0.1).

*Figure 9: Basic VRRP Topology*

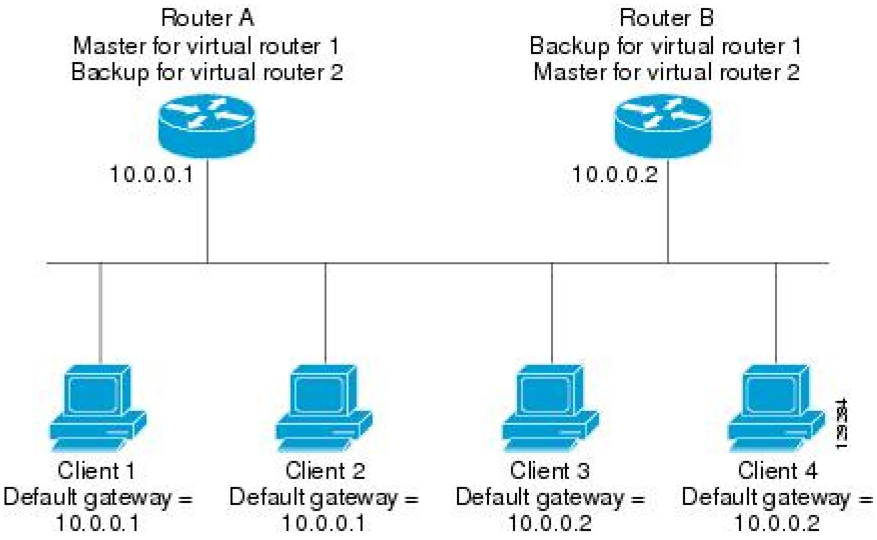


Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual router master and is also known as the IP address owner. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 10.0.0.1.

Routers B and C function as virtual router backups. If the virtual router master fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the VRRP Router Priority and Preemption section.

The figure below shows a LAN topology in which VRRP is configured so that Routers A and B share the traffic to and from clients 1 through 4 and that Routers A and B act as virtual router backups to each other if either router fails.

*Figure 10: Load Sharing and Redundancy VRRP Topology*



In this topology, two virtual routers are configured. (For more information, see the Multiple Virtual Router Support section.) For virtual router 1, Router A is the owner of IP address 10.0.0.1 and virtual router master, and Router B is the virtual router backup to Router A. Clients 1 and 2 are configured with the default gateway IP address of 10.0.0.1.

For virtual router 2, Router B is the owner of IP address 10.0.0.2 and virtual router master, and Router A is the virtual router backup to Router B. Clients 3 and 4 are configured with the default gateway IP address of 10.0.0.2.

# VRRP Benefits

### Redundancy

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

### Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

### Multiple Virtual Routers

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

### Multiple IP Addresses

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

### Preemption

The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

### Authentication

VRRP message digest 5 (MD5) algorithm authentication protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

### Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

### VRRP Object Tracking

VRRP object tracking provides a way to ensure the best VRRP router is the virtual router master for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states.

## Multiple Virtual Router Support

You can configure up to 255 virtual routers on a router physical interface. The actual number of virtual routers that a router interface can support depends on the following factors:

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

In a topology where multiple virtual routers are configured on a router interface, the interface can act as a master for one virtual router and as a backup for one or more virtual routers.

## VRRP Router Priority and Preemption

An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a virtual router master.

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a virtual router master if the virtual router master fails. You can configure the priority of each virtual router backup with a value of 1 through 254 using the **vrrp priority** command.

For example, if Router A, the virtual router master in a LAN topology, fails, an election process takes place to determine if virtual router backups B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become virtual router master because it has the higher priority. If Routers B and C are both configured with the priority of 100, the virtual router backup with the higher IP address is elected to become the virtual router master.

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual router master. You can disable this preemptive scheme using the **no vrrp preempt** command. If preemption is disabled, the virtual router backup that is elected to become virtual router master remains the master until the original virtual router master recovers and becomes master again.

## VRRP Advertisements

The virtual router master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual router master. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco routers allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup routers. The master advertisement value displayed in the **show vrrp** command output on the backup routers is always 1 second because the packets on the backup routers do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only.

## VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process allows you to track individual objects such as a the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP device. You specify the object number to be tracked and VRRP is notified of any change to the object. VRRP increments (or decrements) the priority of the virtual device based on the state of the object being tracked.

# How VRRP Object Tracking Affects the Priority of a Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the VRRP priority is reduced. The VRRP device with the higher priority can now become the virtual device master if it has the **vrrp preempt** command configured. See the "VRRP Object Tracking" section for more information on object tracking.

# In Service Software Upgrade--VRRP

VRRP supports In Service Software Upgrade (ISSU). In Service Software Upgrade (ISSU) allows a high-availability (HA) system to run in stateful switchover (SSO) mode even when different versions of software are running on the active and standby Route Processors (RPs) or line cards.

ISSU provides the ability to upgrade or downgrade from one supported release to another while continuing to forward packets and maintain sessions, thereby reducing planned outage time. The ability to upgrade or downgrade is achieved by running different software versions on the active RP and standby RP for a short period of time to maintain state information between RPs. This feature allows the system to switch over to a secondary RP running upgraded (or downgraded) software and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default.

For detailed information about ISSU, see the In Service Software Upgrade Process document in the *High Availability Configuration Guide*.

# VRRP Support for Stateful Switchover

With the introduction of the VRRP Support for Stateful Switchover feature, VRRP is SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual Route Processors (RPs). SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Prior to being SSO aware, if VRRP was deployed on a router with redundant RPs, a switchover of roles between the active RP and the standby RP would result in the router relinquishing its activity as a VRRP group member and then rejoining the group as if it had been reloaded. The SSO--VRRP feature enables VRRP to continue its activities as a group member during a switchover. VRRP state information between redundant RPs is maintained so that the standby RP can continue the router's activities within the VRRP during and after a switchover.

This feature is enabled by default. To disable this feature, use the **no vrrp sso** command in global configuration mode.

For more information, see the Stateful Switchover document.

# How to Configure VRRP

## Customizing VRRP

Customizing the behavior of VRRP is optional. Be aware that as soon as you enable a VRRP group, that group is operating. It is possible that if you first enable a VRRP group before customizing VRRP, the router could take over control of the group and become the virtual router master before you have finished customizing the feature. Therefore, if you plan to customize VRRP, it is a good idea to do so before enabling VRRP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **description** *text*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **preempt** [**delay minimum** *seconds*]
8. **vrrp** *group* **timers advertise** [**msec**] *interval*
9. **vrrp** *group* **timers learn**
10. **exit**
11. **no vrrp sso**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Router(config-if)# ip address 172.16.6.5 255.255.255.0` | Configures an IP address for an interface. |
| **Step 5** | **vrrp** *group* **description** *text*<br>**Example:**<br>`Router(config-if)# vrrp 10 description working-group` | Assigns a text description to the VRRP group. |
| **Step 6** | **vrrp** *group* **priority** *level*<br>**Example:**<br>`Router(config-if)# vrrp 10 priority 110` | Sets the priority level of the router within a VRRP group.<br>• The default priority is 100. |
| **Step 7** | **vrrp** *group* **preempt** [**delay minimum** *seconds*]<br>**Example:**<br>`Router(config-if)# vrrp 10 preempt delay minimum 380` | Configures the router to take over as virtual router master for a VRRP group if it has a higher priority than the current virtual router master.<br>• The default delay period is 0 seconds.<br>• The router that is IP address owner will preempt, regardless of the setting of this command. |
| **Step 8** | **vrrp** *group* **timers advertise** [**msec**] *interval*<br>**Example:**<br>`Router(config-if)# vrrp 10 timers advertise 110` | Configures the interval between successive advertisements by the virtual router master in a VRRP group.<br>• The unit of the interval is in seconds unless the **msec** keyword is specified. The default *interval* value is 1 second.<br>**Note** All routers in a VRRP group must use the same timer values. If the same timer values are not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master. |
| **Step 9** | **vrrp** *group* **timers learn**<br>**Example:**<br>`Router(config-if)# vrrp 10 timers learn` | Configures the router, when it is acting as virtual router backup for a VRRP group, to learn the advertisement interval used by the virtual router master. |
| **Step 10** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **no vrrp sso**<br>**Example:**<br>`Router(config)# no vrrp sso` | (Optional) Disables VRRP support of SSO.<br>• VRRP support of SSO is enabled by default. |

# Enabling VRRP

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **ip** *ip-address* [**secondary**]
6. **end**
7. **show vrrp** [**brief**] | *group*]
8. **show vrrp interface** *type number* [**brief**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip address** *ip-address mask*<br>**Example:**<br>`Router(config-if)# ip address 172.16.6.5 255.255.255.0` | Configures an IP address for an interface. |
| **Step 5** | **vrrp** *group* **ip** *ip-address* [**secondary**]<br>**Example:**<br>`Router(config-if)# vrrp 10 ip 172.16.6.1` | Enables VRRP on an interface.<br>• After you identify a primary IP address, you can use the **vrrp ip** command again with the **secondary** keyword to indicate additional IP addresses supported by this group.<br>**Note** All routers in the VRRP group must be configured with the same primary address and a matching list of secondary addresses for the virtual router. If different primary or secondary addresses are configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master. |
| **Step 6** | **end**<br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show vrrp** [**brief**] \| *group*]<br>**Example:**<br>`Router# show vrrp 10` | (Optional) Displays a brief or detailed status of one or all VRRP groups on the router. |
| **Step 8** | **show vrrp interface** *type number* [**brief**]<br>**Example:**<br>`Router# show vrrp interface GigabitEthernet 0/0/0` | (Optional) Displays the VRRP groups and their status on a specified interface. |

# Configuring VRRP Object Tracking

**Note** If a VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through object tracking.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **vrrp** *group* **ip** *ip-address*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **track** *object-number* [**decrement** *priority*]
8. **end**
9. **show track** [*object-number*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** \| **ip routing**}<br>**Example:**<br>`Router(config)# track 2 interface serial 6 line-protocol` | Configures an interface to be tracked where changes in the state of the interface affect the priority of a VRRP group.<br>• This command configures the interface and corresponding object number to be used with the **vrrp track** command.<br>• The **line-protocol** keyword tracks whether the interface is up. The **ip routing** keyword also checks that IP routing is enabled and active on the interface.<br>• You can also use the **track ip route** command to track the reachability of an IP route or a metric type object. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface Ethernet 2` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **vrrp** *group* **ip** *ip-address*<br>**Example:**<br>`Router(config-if)# vrrp 1 ip 10.0.1.20` | Enables VRRP on an interface and identifies the IP address of the virtual router. |
| **Step 6** | **vrrp** *group* **priority** *level*<br>**Example:**<br>`Router(config-if)# vrrp 1 priority 120` | Sets the priority level of the router within a VRRP group. |
| **Step 7** | **vrrp** *group* **track** *object-number* [**decrement** *priority*]<br>**Example:**<br>`Router(config-if)# vrrp 1 track 2 decrement 15` | Configures VRRP to track an object. |
| **Step 8** | **end**<br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show track** [*object-number*]<br>**Example:**<br>`Router# show track 1` | Displays tracking information. |

# Configuring VRRP Text Authentication

### Before You Begin

Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.

Text authentication cannot be combined with MD5 authentication for a VRRP group at any one time. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeros on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **terminal interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp** *group* **authentication text** *text-string*
6. **vrrp** *group* **ip** *ip-address*
7. Repeat Steps 1 through 6 on each router that will communicate.
8. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **terminal interface** *type number*<br>**Example:**<br>`Router(config)# interface Ethernet 0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br>**Example:**<br>`Router(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |
| **Step 5** | **vrrp** *group* **authentication text** *text-string*<br>**Example:**<br>`Router(config-if)# vrrp 1 authentication text textstring1` | Authenticates VRRP packets received from other routers in the group.<br>• If you configure authentication, all routers within the VRRP group must use the same authentication string.<br>• The default string is cisco. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master. |
| **Step 6** | **vrrp** *group* **ip** *ip-address*<br>**Example:**<br>`Router(config-if)# vrrp 1 ip 10.0.1.20` | Enables VRRP on an interface and identifies the IP address of the virtual router. |
| **Step 7** | Repeat Steps 1 through 6 on each router that will communicate. | — |
| **Step 8** | **end**<br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |

# Configuration Examples for VRRP

## Example: Configuring VRRP

In the following example, Router A and Router B each belong to three VRRP groups.

In the configuration, each group has the following properties:

- Group 1:
    - Virtual IP address is 10.1.0.10.
    - Router A will become the master for this group with priority 120.
    - Advertising interval is 3 seconds.
    - Preemption is enabled.
- Group 5:
    - Router B will become the master for this group with priority 200.
    - Advertising interval is 30 seconds.
    - Preemption is enabled.
- Group 100:

- Router A will become the master for this group first because it has a higher IP address (10.1.0.2).
- Advertising interval is the default 1 second.
- Preemption is disabled.

### Router A

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 100
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

### Router B

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 200
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

## Example: VRRP Object Tracking

In the following example, the tracking process is configured to track the state of the line protocol on serial interface 0/1. VRRP on Ethernet interface 1/0 then registers with the tracking process to be informed of any changes to the line protocol state of serial interface 0/1. If the line protocol state on serial interface 0/1 goes down, then the priority of the VRRP group is reduced by 15.

```
Router(config)# track 1 interface Serial 0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet 1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.0.0.3
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 track 1 decrement 15
```

## Example: VRRP Object Tracking Verification

The following examples verify the configuration shown in the Example: VRRP Object Tracking section:

```
Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption is enabled
   min delay is 0.000 sec
  Priority is 105
   Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
   1 change, last change 00:06:53
  Tracked by:
   VRRP Ethernet1/0 1
```

## Example: VRRP Text Authentication

The following example shows how to configure VRRP text authentication using a text string:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
```

## Example: VRRP MIB Trap

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host 10.1.1.0 community abc vrrp
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| VRRP commands | *Cisco IOS IP Application Services Command Reference* |
| Object tracking | Configuring Enhanced Object Tracking |

| Related Topic | Document Title |
|---|---|
| Hot Standby Routing Protocol (HSRP) | Configuring HSRP |
| In Service Software Upgrace (ISSU) | "In Service Software Upgrade Process" in the *High Availability Configuration Guide* |
| Gateway Load Balancing Protocol (GLBP) | Configuring GLBP |
| Stateful Switchover | The Stateful Switchover section in the*High Availability Configuration Guide* |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

### MIBs

| MIBs | MIBs Link |
|---|---|
| VRRP MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 2338 | Virtual Router Redundancy Protocol |
| RFC 2787 | Definitions of Managed Objects for the Virtual Router Redundancy Protocol |
| RFC 3768 | Virtual Router Redundancy Protocol (VRRP) |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for VRRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 15: Feature Information for VRRP*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| ISSU—VRRP | 15.2(1)S<br>15.3(1)S | VRRP supports In Service Software Upgrade (ISSU). ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.<br>This feature provides customers with the same level of HA functionality for planned outages due to software upgrades as is available with SSO for unplanned outages. That is, the system can switch over to a secondary RP and continue forwarding packets without session loss and with minimal or no packet loss.<br>This feature is enabled by default.<br>There are no new or modified commands for this feature. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| SSO—VRRP | 15.2(1)S<br>15.3(1)S | VRRP is now SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current VRRP group state.<br>This feature is enabled by default.<br>The following commands were introduced or modified by this feature: **debug vrrp ha**,**vrrp sso**, **show vrrp**. |
| Virtual Router Redundancy Protocol | 15.2(1)S<br>15.3(1)S | VRRP enables a group of routers to form a single virtual router to provide redundancy. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.<br>The following commands were introduced by this feature: **debug vrrp all**, **debug vrrp error**, **debug vrrp events**, **debug vrrp packets**, **debug vrrp state**, **show vrrp**, **show vrrp interface**, **vrrp authentication**, **vrrp description**, **vrrp ip**, **vrrp preempt**, **vrrp priority**, **vrrp timers advertise**, **vrrp timers learn**. |
| VRRP Object Tracking | 15.2(1)S<br>15.3(1)S<br>Cisco IOS XE Release 3.9S | The VRRP Object Tracking feature extends the capabilities of the VRRP to allow tracking of specific objects within the router that can alter the priority level of a virtual router for a VRRP group.<br>The following command was introduced by this feature: **vrrp track**.<br>The following command was modified by this feature: **show track**. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| VRRP MIB—RFC 2787 | Cisco IOS XE Release 3.9S | The VRRP MIB--RFC 2787 feature enables an enhancement to the MIB for use with SNMP-based network management. The feature adds support for configuring, monitoring, and controlling routers that use VRRP.<br>The following command was introduced by this feature: **vrrp shutdown**.<br>The following commands were modified by this feature: **snmp-server enable traps**and**snmp-server host**. |
| FHRP—VRF Aware VRRP | Cisco IOS XE Release 3.9S | The FHRP—VRF Aware VRRP feature enables VRRP support on MPLS VPN.<br>There are no new or modified commands for this feature. |

# Glossary

**virtual IP address owner —**The VRRP router that owns the IP address of the virtual router. The owner is the router that has the virtual router address as its physical interface address.

**virtual router —**One or more VRRP routers that form a group. The virtual router acts as the default gateway router for LAN clients. Also known as a VRRP group.

**virtual router backup —**One or more VRRP routers that are available to assume the role of forwarding packets if the virtual router master fails.

**virtual router master —**The VRRP router that is currently responsible for forwarding packets sent to the IP addresses of the virtual router. Usually the virtual router master also functions as the IP address owner.

**VRRP router** --A router that is running VRRP.

CHAPTER 16

# VRRPv3 Protocol Support

Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. The LAN clients can then be configured with the virtual device as their default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRP version 3 (v3) Protocol Support feature provides the capability to support IPv4 and IPv6 addresses while VRRP version 2 (v2) only supports IPv4 addresses. This module explains concepts related to VRRPv3 and describes how to create and customize a VRRP group in a network. Benefits of using VRRPv3 Protocol Support include the following:

- Interoperability in multi-vendor environments.
- VRRPv3 supports usage of IPv4 and IPv6 addresses while VRRPv2 only supports IPv4 addresses
- Improved scalability through the use of VRRS Pathways.

**Note** In this module, VRRP and VRRPv3 are used interchangeably.

# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for VRRPv3 Protocol Support

- VRRPv3 is not intended as a replacement for existing dynamic protocols. VRRPv3 is designed for use over multi-access, multicast, or broadcast capable Ethernet LANs.
- VRRPv3 is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must not configure the VRRPv3 advertise timer to a value lesser than the forwarding delay on the BVI interface. If you configure the VRRPv3 advertise timer to a value equal to or greater than the forwarding delay on the BVI interface, the setting prevents a VRRP device on a recently initialized BVI interface from unconditionally taking over the master role. Use the **bridge forward-time** command to set the forwarding delay on the BVI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.
- VRRPv3 does not support Stateful Switchover (SSO).
- Full network redundancy can only be achieved if VRRP operates over the same network path as the VRRS Pathway redundant interfaces. For full redundancy, the following restrictions apply:
    - VRRS pathways should not share a different physical interface as the parent VRRP group or be configured on a sub-interface having a different physical interface as the parent VRRP group.
    - VRRS pathways should not be configured on Switch Virtual Interface (SVI) interfaces as long as the associated VLAN does not share the same trunk as the VLAN on which the parent VRRP group is configured.

# Information About VRRPv3 Protocol Support

## VRRPv3 Benefits

### Support for IPv4 and IPv6

VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses.

Note When VRRPv3 is in use, VRRPv2 is unavailable. For VRRPv3 to be configurable, the **fhrp version vrrp v3** command must be used in global configuration mode

### Redundancy

VRRP enables you to configure multiple devices as the default gateway device, which reduces the possibility of a single point of failure in a network.

### Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple devices, thereby sharing the traffic load more equitably between available devices.

### Multiple Virtual Devices

VRRP supports up to 255 virtual devices (VRRP groups) on a device physical interface, subject to restrictions in scaling. Multiple virtual device support enables you to implement redundancy and load sharing in your LAN topology. In scaled environments, VRRS Pathways should be used in combination with VRRP control groups.

### Multiple IP Addresses

The virtual device can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

Note To utilize secondary IP addresses in a VRRP group, a primary address must be configured on the same group.

### Preemption

The redundancy scheme of VRRP enables you to preempt a virtual device backup that has taken over for a failing virtual device master with a higher priority virtual device backup that has become available.

Note Preemption of a lower priority master device is enabled with an optional delay.

### Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address for VRRP advertisements. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:0:12. This addressing scheme minimizes the number of devices that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA has assigned VRRP the IP protocol number 112.

# VRRP Device Priority and Preemption

An important aspect of the VRRP redundancy scheme is VRRP device priority. Priority determines the role that each VRRP device plays and what happens if the virtual device master fails.

If a VRRP device owns the IP address of the virtual device and the IP address of the physical interface, this device will function as a virtual device master.

Priority also determines if a VRRP device functions as a virtual device backup and the order of ascendancy to becoming a virtual device master if the virtual device master fails. You can configure the priority of each virtual device backup with a value of 1 through 254 using the **priority** command (use the **vrrp address-family** command to enter the VRRP configuration mode and access the **priority** option).

For example, if device A, the virtual device master in a LAN topology, fails, an election process takes place to determine if virtual device backups B or C should take over. If devices B and C are configured with the priorities of 101 and 100, respectively, device B is elected to become virtual device master because it has the higher priority. If devices B and C are both configured with the priority of 100, the virtual device backup with the higher IP address is elected to become the virtual device master.

By default, a preemptive scheme is enabled whereby a higher priority virtual device backup that becomes available takes over from the virtual device backup that was elected to become virtual device master. You can disable this preemptive scheme using the **no preempt** command (use the **vrrp address-family** command to enter the VRRP configuration mode, and enter the **no preempt** command). If preemption is disabled, the virtual device backup that is elected to become virtual device master remains the master until the original virtual device master recovers and becomes master again.

**Note** Preemption of a lower priority master device is enabled with an optional delay.

# VRRP Advertisements

The virtual device master sends VRRP advertisements to other VRRP devices in the same group. The advertisements communicate the priority and state of the virtual device master. The VRRP advertisements are encapsulated into either IPv4 or IPv6 packets (based on the VRRP group configuration) and sent to the appropriate multicast address assigned to the VRRP group. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:0:12. The advertisements are sent every second by default and the interval is configurable.

Cisco devices allow you to configure millisecond timers, which is a change from VRRPv2. You need to manually configure the millisecond timer values on both the primary and the backup devices. The master advertisement value displayed in the **show vrrp** command output on the backup devices is always 1 second because the packets on the backup devices do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances. The use of the millisecond timer values is compatible with third party vendors, as long as they also support VRRPv3. You can specify a timer value between 100 milliseconds and 40000 milliseconds.

# How to Configure VRRPv3 Protocol Support

## Enabling VRRPv3 on a Device

To enable VRRPv3 on a device, perform the following task:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables the ability to configure VRRPv3 and VRRS.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

## Creating and Customizing a VRRP Group

To create a VRRP group, perform the following task. Steps 6 to 14 denote customizing options for the group, and they are optional:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay minimum** *seconds*
10. **priority** *priority-level*
11. **timers advertise** *interval*
12. **vrrpv2**
13. **vrrs leader** *vrrs-leader-name*
14. **shutdown**
15. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables the ability to configure VRRPv3 and VRRS.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **vrrp** *group-id* **address-family** {**ipv4** \| **ipv6**}<br>**Example:**<br>`Device(config-if)# vrrp 3 address-family ipv4` | Creates a VRRP group and enters VRRP configuration mode. |
| **Step 6** | **address** *ip-address* [**primary** \| **secondary**]<br>**Example:**<br>`Device(config-if-vrrp)# address 100.0.1.10 primary` | Specifies a primary or secondary address for the VRRP group.<br>**Note** VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses. |
| **Step 7** | **description** *group-description*<br>**Example:**<br>`Device(config-if-vrrp)# description group 3` | (Optional) Specifies a description for the VRRP group. |
| **Step 8** | **match-address**<br>**Example:**<br>`Device(config-if-vrrp)# match-address` | (Optional) Matches secondary address in the advertisement packet against the configured address.<br>• Secondary address matching is enabled by default. |
| **Step 9** | **preempt delay minimum** *seconds*<br>**Example:**<br>`Device(config-if-vrrp)# preempt delay minimum 30` | (Optional) Enables preemption of lower priority master device with an optional delay.<br>• Preemption is enabled by default. |
| **Step 10** | **priority** *priority-level*<br>**Example:**<br>`Device(config-if-vrrp)# priority 3` | (Optional) Specifies the priority value of the VRRP group.<br>• The priority of a VRRP group is 100 by default. |
| **Step 11** | **timers advertise** *interval*<br>**Example:**<br>`Device(config-if-vrrp)# timers advertise 1000` | (Optional) Sets the advertisement timer in milliseconds.<br>• The advertisement timer is set to 1000 milliseconds by default. |
| **Step 12** | **vrrpv2**<br>**Example:**<br>`Device(config-if-vrrp)# vrrpv2` | (Optional) Enables support for VRRPv2 simultaneously, so as to interoperate with devices which only support VRRP v2.<br>• VRRPv2 is disabled by default. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **vrrs leader** *vrrs-leader-name*<br>**Example:**<br>`Device(config-if-vrrp)# vrrs leader leader-1` | (Optional) Specifies a leader's name to be registered with VRRS and to be used by followers.<br>• A registered VRRS name is unavailable by default. |
| **Step 14** | **shutdown**<br>**Example:**<br>`Device(config-if-vrrp)# shutdown` | (Optional) Disables VRRP configuration for the VRRP group.<br>• VRRP configuration is enabled for a VRRP group by default. |
| **Step 15** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Configuring the Delay Period Before FHRP Client Initialization

To configure the delay period before the initialization of all FHRP clients on an interface, perform the following task:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **fhrp delay** {[**minimum**] [**reload**] *seconds*}
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables the ability to configure VRRPv3 and VRRS.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |
| **Step 5** | **fhrp delay** {[**minimum**] [**reload**] *seconds*}<br>**Example:**<br>`Device(config-if)# fhrp delay minimum 5` | Specifies the delay period for the initialization of FHRP clients after an interface comes up.<br>• The range is 0-3600 seconds. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Configuration Examples for VRRPv3 Protocol Support

## Example: Enabling VRRPv3 on a Device

The following example shows how to enable VRRPv3 on a device:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

## Example: Creating and Customizing a VRRP Group

The following example shows how to create and customize a VRRP group:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

**Note** In the above example, the **fhrp version vrrp v3** command is used in the global configuration mode.

## Example: Configuring the Delay Period Before FHRP Client Initialization

The following example shows how to configure the delay period before FHRP client initialization :

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

**Note** In the above example, a five-second delay period is specified for the initialization of FHRP clients after the interface comes up. You can specify a delay period between 0 and 3600 seconds.

## Example: VRRP Status, Configuration, and Statistics Details

The following is a sample output of the status, configuration and statistics details for a VRRP group:

```
Device> enable
Device# show vrrp detail

 Ethernet0/0 - Group 1 - Address-Family IPv4

 State is MASTER
 State duration 3.707 secs
 Virtual IP address is 1.0.0.10
 Virtual MAC address is 0000.5E00.0101
 Advertisement interval is 1000 msec
 Preemption enabled
 Priority is 100
 Master Router is 1.0.0.1 (local), priority is 100
 Master Advertisement interval is 1000 msec (expires in 686 msec)
 Master Down interval is unknown
 State is MASTER
 State duration 3.707 secs
 VRRPv3 Advertisements: sent 5 (errors 0) - rcvd 0
 VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
 Group Discarded Packets: 0
   VRRPv2 incompatibility: 0
   IP Address Owner conflicts: 0
   Invalid address count: 0
   IP address configuration mismatch : 0
   Invalid Advert Interval: 0
   Adverts received in Init state: 0
   Invalid group other reason: 0
 Group State transition:
   Init to master: 0
   Init to backup: 1 (Last change Mon Jul 30 16:42:01.856)
   Backup to master: 1 (Last change Mon Jul 30 16:42:05.469)
   Master to backup: 0
   Master to init: 0
   Backup to init: 0

Device# exit
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Master Commands List, All Releases |
| FHRP commands | First Hop Redundancy Protocols Command Reference |
| Configuring VRRPv2 | *Configuring VRRP* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC5798 | *Virtual Router Redundancy Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for VRRPv3 Protocol Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 16: Feature Information for VRRPv3 Protocol Support*

| Feature Name | Releases | Feature Information |
|---|---|---|
| VRRPv3 Protocol Support | 15.3(1)S | VRRP enables a group of devices to form a single virtual device to provide redundancy. The LAN clients can then be configured with the virtual device as their default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRPv3 Protocol Support feature provides the capability to support IPv4 and IPv6 addresses.<br>The following commands were introduced or modified: **fhrp delay**, **show vrrp**, **vrrp address-family**. |

# Glossary

**Virtual IP address owner—**The VRRP device that owns the IP address of the virtual device. The owner is the device that has the virtual device address as its physical interface address.

**Virtual device—**One or more VRRP devices that form a group. The virtual device acts as the default gateway device for LAN clients. The virtual device is also known as a VRRP group.

**Virtual device backup—**One or more VRRP devices that are available to assume the role of forwarding packets if the virtual device master fails.

**Virtual device master—**The VRRP device that is currently responsible for forwarding packets sent to the IP addresses of the virtual device. Usually, the virtual device master also functions as the IP address owner.

**VRRP device—**A device that is running VRRP.

CHAPTER 17

# VRRPv3: Object Tracking Integration

Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. The LAN clients then can be configured with the virtual device as the default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRPv3: Object Tracking Integration feature allows you to track the behavior of an object and receive notifications of changes. This module explains how object tracking, in particular the tracking of IPv6 objects, is integrated into VRRP version 3 (VRRPv3) and describes how to track an IPv6 object using a VRRPv3 group. See the "VRRP Object Tracking" section for more information on object tracking.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About VRRPv3: Object Tracking Integration

## VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process allows you to track individual objects such as a the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP device. You specify the object number to be tracked and VRRP is notified of any change to the object. VRRP increments (or decrements) the priority of the virtual device based on the state of the object being tracked.

## How VRRP Object Tracking Affects the Priority of a Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the VRRP priority is reduced. The VRRP device with the higher priority can now become the virtual device master if it has the **vrrp preempt** command configured. See the “VRRP Object Tracking” section for more information on object tracking.

# How to Configure VRRPv3: Object Tracking Integration

## Tracking an IPv6 Object using VRRPv3

### SUMMARY STEPS

1. **fhrp version vrrp v3**
2. **interface** *type number*
3. **vrrp** *group-id* **address-family ipv6**
4. **track** *object-number* **decrement** *number*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables you to configure Virtual Router Redundancy Protocol version 3 (VRRPv3) and Virtual Router Redundancy Service (VRRS) on a device.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |
| **Step 2** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Specifies an interface and enters interface configuration mode. |
| **Step 3** | **vrrp** *group-id* **address-family ipv6**<br>**Example:**<br>`Device(config-if)# vrrp 1 address-family ipv6` | Creates a VRRP group for IPv6 and enters VRRP configuration mode. |
| **Step 4** | **track** *object-number* **decrement** *number*<br>**Example:**<br>`Device(config-if-vrrp)# track 1 decrement 20` | Configures the tracking process to track the state of the IPv6 object using the VRRPv3 group. VRRP on Ethernet interface 0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if-vrrp)# end` | Returns to privileged EXEC mode. |

# Configuration Examples for VRRPv3: Object Tracking Integration

## Example: Tracking an IPv6 Object using VRRPv3

In the following example, the tracking process is configured to track the state of the IPv6 object using the VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20:

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

## Example: Verifying VRRP IPv6 Object Tracking

```
Device# show vrrp

Ethernet0/0 - Group 1 - Address-Family IPv4
  State is BACKUP
  State duration 1 mins 41.856 secs
  Virtual IP address is 172.24.1.253
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 80 (configured 100)
    Track object 1 state Down decrement 20
  Master Router is 172.24.1.2, priority is 100
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 3297 msec)

Device# show track ipv6 route brief

Track Type        Instance                   Parameter        State Last Change
601   ipv6 route  3172::1/32                 metric threshold Down  00:08:55
602   ipv6 route  3192:ABCD::1/64            metric threshold Down  00:08:55
603   ipv6 route  3108:ABCD::CDEF:1/96       metric threshold Down  00:08:55
604   ipv6 route  3162::EF01/16              metric threshold Down  00:08:55
605   ipv6 route  3289::2/64                 metric threshold Down  00:08:55
606   ipv6 route  3888::1200/64              metric threshold Down  00:08:55
607   ipv6 route  7001::AAAA/64              metric threshold Down  00:08:55
608   ipv6 route  9999::BBBB/64              metric threshold Down  00:08:55
611   ipv6 route  1111::1111/64              reachability     Down  00:08:55
612   ipv6 route  2222:3333::4444/64         reachability     Down  00:08:55
613   ipv6 route  5555::5555/64              reachability     Down  00:08:55
614   ipv6 route  3192::1/128                reachability     Down  00:08:55
```

# Additional References for VRRPv3: Object Tracking Integration

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS First Hop Redundancy Protocols Command Reference* |
| Troubleshooting HSRP | *Hot Standby Router Protocol: Frequently Asked Questions* |

### RFCs

| RFCs | Title |
|---|---|
| RFC 792 | *Internet Control Message Protocol* |
| RFC 1828 | *IP Authentication Using Keyed MD5* |
| RFC 5798 | *Virtual Router Redundancy Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for VRRPv3: Object Tracking Integration

*Table 17: Feature Information for VRRPv3: Object Tracking Integration*

| Feature Name | Releases | Feature Information |
|---|---|---|
| VRRPv3: Object Tracking Integration | 15.3(3)S | The VRRPv3: Object Tracking Integration feature allows you to use a VRRPv3 group to track an object.<br>The following commands were introduced or modified: **fhrp version vrrp v3**, **show vrrp**, **track (VRRP)**. |

CHAPTER 18

# Virtual Router Redundancy Service

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between the Virtual Router Redundancy Protocol (VRRP), VRRS pathways and optional VRRS clients. The VRRS multiclient service provides a consistent interface with VRRP by abstracting over several First Hop Redundancy Protocols (FHRPs) and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named VRRP groups.

VRRP acts as a server that pushes VRRP status information out to VRRS pathways, and all registered VRRS clients. Pathways and clients obtain status on all essential information provided by VRRP, including current and previous redundancy states, active and inactive Layer 2 and Layer 3 addresses, and, in some cases, information about other redundant gateways in the network. Pathways use this information in order to provide scaled first-hop gateway redundancy across scaled interface environments. VRRS clients will also use this information to provide stateless and stateful redundancy information to clients and protocols.

**Note** In this module, VRRP and VRRPv3 are used interchangeably.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for VRRS

- VRRS plug-ins must be configured on subinterfaces that are not configured with VRRP, but which share a physical interface with a VRRP group it is following.
- VRRP Version 2 (VRRPv2) is configurable only on Gigabit Ethernet interfaces.
- VRRS is currently only available for use with VRRP Version 3 (VRRPv3).

# Information About VRRS

## VRRS Overview

VRRS improves the scalability of VRRP. VRRS provides a stateless redundancy service to VRRS pathways and applications (VRRS clients) by monitoring VRRP. VRRS provides a database of the current VRRP state and provides a “push” data service to the VRRS pathways and clients with which it communicates. VRRP acts as a VRRS server. VRRS clients are other Cisco processes or applications that use VRRP to provide or withhold a service or resource dependent upon the state of the group. VRRS pathways are special VRRS clients that use the VRRS database information in order to provide scaled first–hop gateway redundancy across scaled interface environments.

The VRRS by itself is limited to maintaining its own state. Linking a VRRS client to a VRRP group provides a mechanism that allows VRRS to provide a service to client applications so that they can implement stateless or stateful failover. Stateless failover is failover without syncing of state. Stateful failover requires communication with a nominated backup before failure so that operational data is not lost when failover occurs.

VRRS pathways operate in a similar way to clients, but are integrated with the VRRS architecture. They provide a means to scale first–hop gateway redundancy by allowing the user the opportunity to configure a virtual address across hundreds of interfaces. The “virtual gateway” state of a VRRS pathway follows the state of an FHRP VRRS server.

## Using VRRS with VRRP

VRRP provides server support for VRRS. The VRRP server pushes state and status information to VRRS when an internal update occurs. VRRS updates its internal database upon receiving a server update, and then sends push notifications to each of the VRRS clients associated with the shared name. Clients are interested in the protocol state, virtual MAC (vMAC) address, and virtual IP address information associated with a group. The association name between a client and a VRRP group is a character name string. The information provided by VRRS allows clients to perform various activities that are dependent on the state of the associated VRRP group.

VRRP notifies VRRS of its current state (master, backup, or nonoperational initial state [INIT]). The VRRP state is then passed on to pathways or clients. A VRRP group should be configured with a name to activate VRRS. Pathways or clients should be configured with the same name to bind them with VRRS.

The VRRP group name associates the VRRP group with any clients that are configured as part of VRRS with the same name.

# VRRS Servers and Clients

VRRP acts as the VRRS server. Pathways and clients act on the VRRP server state. When a VRRP group changes state, VRRS pathways and clients act by altering their behaviour (performing tasks such as shutting down interfaces or appending accounting logs) depending on the state received from VRRS.

# VRRS Pathways and Pathway Manager

## VRRS Pathways

A VRRS pathway is defined as an entity that will provide IPv4 or IPv6 traffic forwarding duties using the following features on an Ethernet interface (such as a physical interface, subinterface, or a Switch Virtual Interface [SVI]):

- vMAC address insertion and removal into the hardware driver using MACdb.
- Virtual IP (vIP) insertion and removal using the IPv4 and IPv6 APIs.
- Provision to associate the vIP with the interface burned-in address (BIA) MAC.
- Provision to associate the vMAC address with the interface–owned vIP.
- Maintain the association of a vMAC with a vIP on a LAN using the Address Resolution Protocol (ARP) or Neighbor Discovery Protocol.
- Maintain the switching cache (content-addressable memory or [CAM]) of connected Layer 2 devices on the LAN.
- Checkpoints all data and the pathway state with a High Availability module.

A Pathway will provide some of the above features using its association with either the VRRS Pathway L2 Controller or the VRRS Pathway L3 Controller.

## VRRS Pathway Manager

The VRRS Pathway Manager provides the following features:

- Creates an association between one or more VRRS pathway instances and a single VRRS database name entry.
- Pushes configuration and state information to associated registered pathways in response to a push from VRRS.
- Provides debugging and show output to the user. The output is related to the state and configuration of the VRRS pathway manager.
- Is Online Insertion and Removal (OIR)–aware and manages pathways that may be affected by OIR events.

- Is Virtual Routing and Forwarding (VRF)–aware and manages pathways that may be affected by VRF events.

# How to Configure VRRS

## Configuring VRRPv3 Control Groups

Perform the following task to configure a VRRP control group.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
7. **address** *ip-address* [**primary** | **secondary**]
8. **vrrs leader** *vrrs-leader-name*
9. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables the ability to configure VRRPv3 and VRRS.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface vlan 40` | Enters interface configuration mode. |
| **Step 5** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 209.165.200.230 255.255.255.224` | Configures the IP address on the interface. |
| **Step 6** | **vrrp** *group-id* **address-family** {**ipv4** \| **ipv6**}<br>**Example:**<br>`Device(config-if)# vrrp 1 address-family ipv4` | Creates a VRRP group and enters VRRP configuration mode. |
| **Step 7** | **address** *ip-address* [**primary** \| **secondary**]<br>**Example:**<br>`Device(config-if-vrrp)# address 209.165.202.141` | Specifies a primary or secondary address for the VRRP group. |
| **Step 8** | **vrrs leader** *vrrs-leader-name*<br>**Example:**<br>`Device(config-if-vrrp)# vrrs leader group1` | Specifies a leader's name to be registered with VRRS and enables a VRRP group to control a VRRS pathway.<br>• It is possible for a single VRRP instance to control more than one VRRS group. A registered VRRS name is unavailable by default. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-if-vrrp)# end` | Returns to privileged EXEC mode. |

# Configuring VRRS Pathways

Perform the following task to configure a VRRP pathway.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **vrrs pathway** *vrrs-leader-name*
7. **mac address** *mac-address*
8. **address** *ip-address*
9. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **fhrp version vrrp v3**<br>**Example:**<br>`Device(config)# fhrp version vrrp v3` | Enables the ability to configure VRRPv3 and VRRS.<br>**Note** When VRRPv3 is in use, VRRPv2 is unavailable. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface vlan 42` | Enters interface configuration mode. |
| **Step 5** | **ip address** *ip-address mask*<br>**Example:**<br>`Device(config-if)# ip address 209.165.201.25 255.255.255.224` | Configures the IP address on the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **vrrs pathway** *vrrs-leader-name*<br>**Example:**<br>`Device(config-if)# vrrs pathway group1` | Defines the VRRS pathway for a VRRS group and enters VRRS pathway configuration mode. |
| **Step 7** | **mac address** *mac-address*<br>**Example:**<br>`Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24` | Specifies a MAC address used by a pathway. |
| **Step 8** | **address** *ip-address*<br>**Example:**<br>`Device(config-if-vrrs-pw)# address 209.165.201.10` | Defines the virtual IP for a pathway.<br>• **Note** A VRRP group is capable of controlling more than one pathway. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-if-vrrs-pw)# end` | Returns to privileged EXEC mode.<br>• **Note** Repeat steps 1 to 9 to configure more pathways. |

# Verifying VRRS

Perform this task to verify VRRS functions.

**Note** The **show** commands are not in any specific order. The **show vrrs pathway** command for different pathway states (active, inactive, and "not ready") is displayed below.

### SUMMARY STEPS

1. **enable**
2. **show vrrs pathway**
3. **show vrrs pathway**
4. **show vrrs pathway**
5. **show vrrs server**

## DETAILED STEPS

**Step 1** **enable**

Enables privileged EXEC mode.

**Example:**

```
Device> enable
```

**Step 2** **show vrrs pathway**

Displays VRRS pathway information for an active pathway with the tag name “group1” and VRRP in master state on the VLAN interface.

**Example:**

```
Device# show vrrs pathway

Pathway ["group1"@Vlan42]
State is ACTIVE [VRRS push "ACTIVE"]
Virtual MAC is fe24.fe24.fe24 [Active] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

**Step 3** **show vrrs pathway**

Displays VRRS pathway information for an inactive pathway with the tag name “group1” and VRRP in backup state on the Ethernet 0/1 interface.

**Example:**

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

**Step 4** **show vrrs pathway**

Displays VRRS pathway information for a “not ready” pathway with the tag name “group1” and VRRP in backup state on the Ethernet 0/1 interface.

**Example:**

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is NOT READY [VRRS push "INIT"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
```

```
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

**Step 5** **show vrrs server**

Displays VRRS server information.

**Example:**

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

The table below describes significant fields in the sample output:

| Field | Description |
|---|---|
| State | Current state of VRRS on an interface. The values displayed are “ACTIVE”, “INACTIVE”, “NOT READY”, or “BACKUP”. |
| Virtual MAC | Virtual MAC address that is reserved for an interface. |
| Address-family | IPv4 or IPv6 address family. |
| Default Pathway | Indicates that the pathway has been implicitly created from a VRRP group, if the value is 1. If the value is 0, it indicates that the pathway has been explicitly created using the **vrrs pathway** command. |
| Owner Mode | Indicates that the interface IP address is specified if the value is 1. |
| Accept-Mode | Indicates that traffic to a particular virtual IP address is accepted if the value is 1. |
| Configured vMAC | Indicates that a virtual MAC address is configured if the value is 1. |
| No Shut | Indicates that the interface has been set to no shutdown mode if the value is 1. |
| Connected | Indicates that the VRRS pathway is connected to a VRRS group, if the value is 1. |
| OIR | Indicates online insertion and removal (OIR) of interface line cards on a device is complete if the value is 1. |

| Field | Description |
|---|---|
| L2 Ready | Indicates that the Layer 2 interface is up if the value is 1. |
| L3 Ready | Indicates that the Layer 3 interface is up if the value is 1. |
| vMAC Ready | Indicates that the virtual MAC address has been assigned to an interface if the value is 1. |
| vIP Ready | Indicates that the virtual IP address has been assigned to an interface if the value is 1. |
| Virtual Address List | Address list of the virtual IPv4 or IPv6 addresses. |
| Interface | Name of the interface where the pathway is defined. |
| vMAC | Virtual MAC address that is assigned to an interface. |
| vIP Address | Virtual IP address that is assigned to an interface. |
| Tags Connected | The specific tag name that is currently connected to a pathway on an interface. |

# Configuration Examples for VRRS

## Example: Configuring VRRPv3 Control Groups

The following example shows how to configure a VRRPv3 control group:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 40
Device(config-if)# ip address 209.165.200.230 255.255.255.224
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 209.165.202.141
Device(config-if-vrrp)# vrrs leader group1
Device(config-if-vrrp)# end
```

**Note** In the above example, the **fhrp version vrrp v3** command is used in global configuration mode.

## Example: Configuring VRRS pathways

The following example shows how to configure a VRRS pathway:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 42
Device(config-if)# ip address 209.165.201.25 255.255.255.224
Device(config-if)# vrrs pathway group1
Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24
Device(config-if-vrrs-pw)# address 209.165.201.10
Device(config-if-vrrs-pw)# end
```

**Note** In the above example, the **fhrp version vrrp v3** command is used in global configuration mode.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Master Command List, All Releases |
| FHRP commands | First Hop Redundancy Protocols Command Reference |
| Configuring VRRPv2 | "Configuring VRRP" module in the *First Hop Redundancy Protocols Configuration Guide* |
| VRRPv3 Protocol Support | "VRRPv3 Protocol Support" module in the *First Hop Redundancy Protocols Configuration Guide* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC5798 | *Virtual Router Redundancy Protocol* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Virtual Router Redundancy Service

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 18: Feature Information for Virtual Router Redundancy Service*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Virtual Router Redundancy Service | 15.3(1)S | The VRRS feature provides a multiclient information abstraction and management service between VRRP, VRRS pathways, and optional VRRS clients<br>The following commands were introduced or modified: **debug vrrs all**, **debug vrrs database**, **debug vrrs log**, **debug vrrs pathway**, and **show vrrs**. |