# First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 2

**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

# Configuring GLBP

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



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 GLBP

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

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, 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 routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IP address, and all routers in the virtual router 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 Active Virtual Gateway

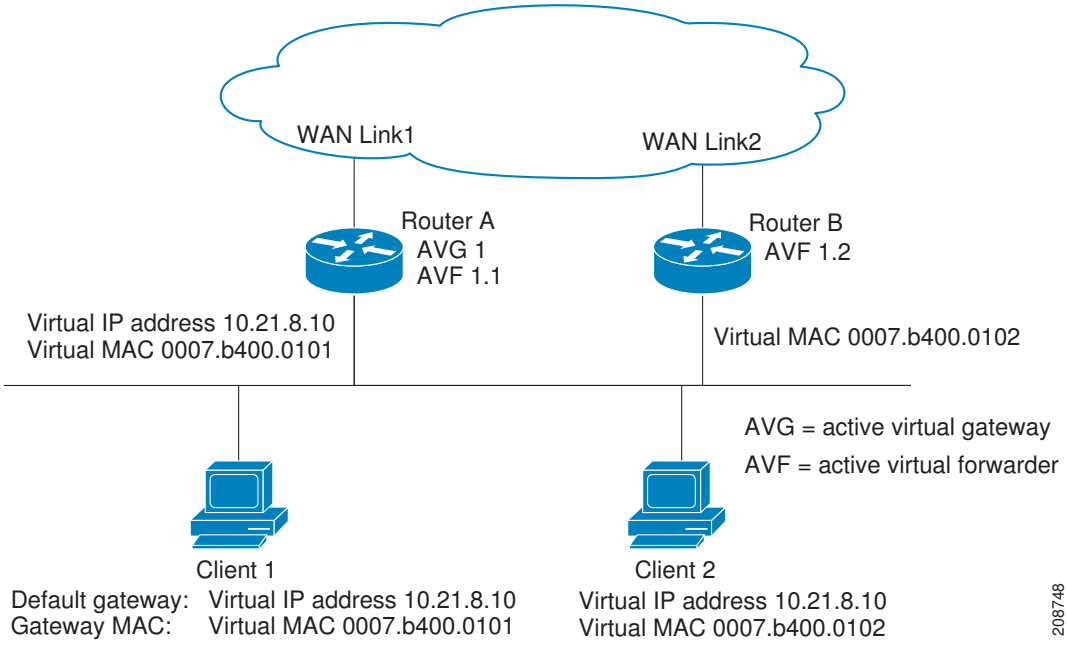
Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The function of the AVG is that it assigns a virtual MAC address to each member of the GLBP group. Each gateway 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.

In the figure below, Router 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 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***




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 router 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 router 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—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 is the only other member in the group so it will automatically become the new AVG. If another router existed in the same GLBP group with a higher priority, then the router with the higher priority would be elected. If both routers 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 router in the GLBP group. The weighting assigned to a router 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 router. 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.

# ISSU--GLBP

GLBP 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 Cisco IOS XE 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 XE 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 XE In Service Software Upgrade Process document in the *Cisco IOS XE 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 routers, thereby sharing the traffic load more equitably among available routers.

### Multiple Virtual Routers

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

### Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway 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

You can use a simple text password authentication scheme between GLBP group members to detect configuration errors. A router within a GLBP group with a different authentication string than other routers will be ignored by other group members.

# 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.

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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **glbp** *group* **ip** [*ip-address* [**secondary**]]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode, and returns the router to global configuration mode. |
| **Step 7** | **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]<br><br>**Example:**<br>`Router(config)# show glbp 10` | (Optional) Displays information about GLBP groups on a router.<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 router:

```
Router# 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

Perform this task to customize your GLBP configuration.

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 router

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. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# ip address 10.21.8.32 255.255.255.0` | Specifies a primary or secondary IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# glbp 10 timers redirect 600 7200` | Configures the time interval during which the AVG continues to redirect clients to an AVF.<br>• The *timeout* argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid. |
| **Step 7** | **glbp** *group* **load-balancing** [**host-dependent** \| **round-robin** \| **weighted**]<br><br>**Example:**<br>`Router(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*<br><br>**Example:**<br>`Router(config-if)# glbp 10 priority 254` | Sets the priority level of the gateway within a GLBP group.<br>• The default value is 100. |
| **Step 9** | **glbp** *group* **preempt** [**delay minimum** [*seconds*]<br><br>**Example:**<br>`Router(config-if)# glbp 10 preempt delay minimum 60` | Configures the router 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** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode, and returns the router to global configuration mode. |

# Configuring GLBP Authentication

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

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

- The authentication schemes differ on the router and in the incoming packet.
- Text authentication strings differ on the router and in the incoming packet.

Perform this task to configure GLBP text authentication.

### 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 router that will communicate.
8. **end**
9. **show glbp**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 1/0/0` | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><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** | **glbp** *group-number* **authentication text** *string*<br><br>**Example:**<br>`Router(config-if)# glbp 10 authentication text stringxyz` | Authenticates GLBP packets received from other routers in the group.<br>• If you configure authentication, all routers within the GLBP group must use the same authentication string. |
| **Step 6** | **glbp** *group-number* **ip** [*ip-address* [**secondary**]]<br><br>**Example:**<br>`Router(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 router that will communicate. | -- |
| **Step 8** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show glbp**<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}<br><br>**Example:**<br>`Router(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. |
| **Step 4** | **exit**<br><br>**Example:**<br>`Router(config-track)# exit` | Returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |
| **Step 6** | **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# glbp 10 forwarder preempt delay minimum 60` | Configures the router 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><br>**Example:**<br>`Router(config-if)# exit` | Returns to privileged EXEC mode. |
| **Step 10** | **show track** [ *object-number* \| **brief**] [**interface** [**brief**] \| **ip route** [ **brief**] \| **resolution** \| **timers**]<br><br>**Example:**<br>`Router# 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 router. Perform this task to minimize the impact of using the **debug glbp** commands.

This procedure will minimize the load on the router 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 router may be unable to respond due to the processor load of generating the debugging output.

This task requires a router 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 router 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no logging console**<br><br>**Example:**<br>`Router(config)# no logging console` | Disables all logging to the console terminal.<br>• To reenable logging to the console, use the**logging console** command in global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Use Telnet to access a router 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><br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |
| **Step 6** | **terminal monitor**<br><br>**Example:**<br>`Router# terminal monitor` | Enables logging output on the virtual terminal. |
| **Step 7** | **debug condition glbp** *interface-type interface-number group* [*forwarder*]<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router# terminal no monitor` | Disables logging on the virtual terminal. |

# Configuration Examples for GLBP



## Example: Customizing GLBP Configuration

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 timers 5 18
Router(config-if)# glbp 10 timers redirect 600 7200
```

```
Router(config-if)# glbp 10 load-balancing host-dependent
Router(config-if)# glbp 10 priority 254
Router(config-if)# glbp 10 preempt delay minimum 60
```

## Example: Configuring GLBP Text Authentication

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

## Example: Configuring GLBP Weighting

In the following example, Router A 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 goes down, the weighting value of the router is reduced.

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

## Example: Enabling GLBP Configuration

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

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

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| GLBP commands | *Cisco IOS IP Application Services Command Reference* |
| In Service Software Upgrade (ISSU) configuration | Cisco IOS In Service Software Upgrade Process in the *Cisco IOS High Availability XE Configuration Guide* |
| Object tracking | Configuring Enhanced Object Tracking |
| Stateful Switchover | Stateful Switchover section in the *Cisco IOS High Availability XE Configuration Guide* |

| Related Topic | Document Title |
|---|---|
| VRRP | Configuring VRRP |
| HSRP | Configuring HSRP |

### 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 |
|---|---|
| No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | 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 |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

### 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 | Cisco IOS XE Release 2.1 | 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><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**. |
| ISSU--GLBP | Cisco IOS XE Release 2.1 | 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 XE software are running on the active and standby Route Processors (RPs) or line cards.<br><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><br>This feature is enabled by default. |

# 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 Cisco IOS XE 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.

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# 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 router. 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 router and a standby router. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router 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 feature information and caveats, see 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 document.

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 router 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 router.

HSRP is useful for hosts that do not support a router discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new router when their selected router 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 routers 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 router. The active router receives and routes packets destined for the MAC address of the group. For *n* routers running HSRP, *n*+ 1 IP and MAC addresses are assigned.

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

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

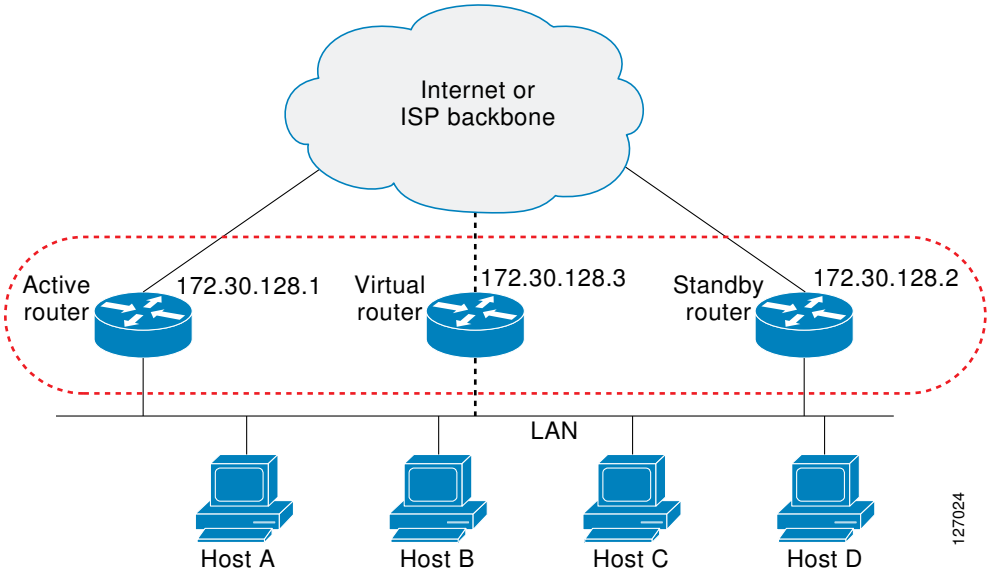
all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

Devices that are running HSRP send and receive multicast User Datagram Protocol (UDP)-based hello messages to detect router failure and to designate active and standby routers. When the active router fails to send a hello message within a configurable period of time, the standby router with the highest priority becomes the active router. The transition of packet forwarding functions between routers 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 routers and load sharing.

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

# 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 router.

### Preemption

Preemption allows a standby router 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 router becomes HSRP active, and there is already an HSRP active router on the network, HSRP preemption may appear to not function. HSRP preemption may appear not function correctly because the new HSRP active router did not receive any hello packets from the current HSRP active router, and the preemption configuration never factored into the new router'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 routers 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 Router

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 router with the higher priority can become the active router if it has the **standby preempt** command configured.

# HSRP Addressing

HSRP routers 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 routers) on UDP port 1985. The active router sources hello packets from its configured IP address and the HSRP virtual MAC address while the standby router 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 composed of 0000.0C07.ACxy, 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 router automatically generates a virtual MAC address for each HSRP router. 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 routers 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 router 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 router changes to a new HSRP state. Routers or access servers for which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values.

For HSRP version 1, nonactive routers learn timer values from the active router, unless millisecond timer values are being used. If millisecond timer values are being used, all routers 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.

# 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, Router A has a priority of 120 and is the active router. If a host sends spoof HSRP hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof HSRP hello packets are ignored, Router A will remain the active router.

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

- The authentication schemes differ on the router and in the incoming packets.
- Text authentication strings differ on the router 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, Router A has a priority of 120 and is the active router. If a host sends spoof HSRP hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof HSRP hello packets are ignored, Router A will remain the active router.

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

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

# HSRP Messages and States

Routers configured with HSRP exchange three types of multicast messages:

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

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

- Active--The router is performing packet-transfer functions.
- Standby--The router is prepared to assume packet-transfer functions if the active router fails.
- Speak--The router is sending and receiving hello messages.
- Listen--The router is receiving hello messages.
- Init or Disabled--The router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers 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.

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 router with low-priority Level 6 messaging.

# HSRP and ARP

HSRP works when the hosts are configured for proxy ARP. When the active HSRP router receives an ARP request for a host that is not on the local LAN, the router replies with the MAC address of the virtual router. If the active router becomes unavailable or its connection to the remote LAN goes down, the router that becomes the active router receives packets addressed to the virtual router and transfers them accordingly. If the Hot Standby state of the interface is not active, proxy ARP responses are suppressed.

# 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 routers 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 routers in the HSRP group is important. If a host is redirected by ICMP to the real IP address of a router, and that router 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 Routers

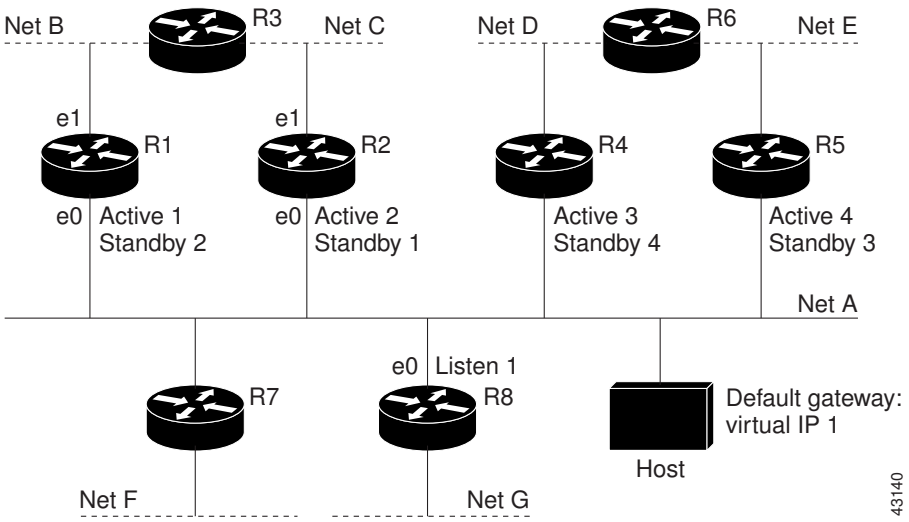
The next-hop IP address is compared to the list of active HSRP routers on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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

For optimal operation, every router in a network that is running HSRP should contain at least one active HSRP group on an interface to that network. Every HSRP router need not be a member of the same group. Each HSRP router will snoop on all HSRP packets on the network to maintain a list of active routers (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
```

Router R1 receives this packet and determines that router 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 router R4 (because only real IP addresses are in its routing table).

The following is the initial ICMP redirect message sent by router 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 router R1 determines that router R4 is the active HSRP router for group 3, so it changes the next hop in the redirect message from the real IP address of router 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 Routers

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

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

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

# ICMP Redirects to Non-HSRP Routers

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

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to router 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 Router Advertisements

Passive HSRP routers send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP routers can determine the HSRP group state of any HSRP router on the network. These advertisements inform other HSRP routers 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 router 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 router 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 router 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.

Using HSRP with ICMP redirects is not possible in the Cisco 800 series, Cisco 1000 series, Cisco 1600 series, Cisco 2500 series, Cisco 3000 series, and Cisco 4500 series routers because the Ethernet controller can support only one MAC address.

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 router uses the destination MAC address to determine the gateway IP address of the host. If the HSRP router 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) routers with either of the following conditions:

- A customer edge (CE) router 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 router 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 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.

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

# ISSU--HSRP

The In Service Software Upgrade (ISSU) process 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 Cisco IOS XE 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.

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

# SSO HSRP

SSO HSRP alters the behavior of HSRP when a router 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 router, then the standby HSRP router takes over as the active HSRP router.

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

- SSO Dual-Route Processors and Cisco Nonstop Forwarding, page 32
- HSRP and SSO Working Together, page 33

## 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

SSO HSRP enables the Cisco IOS XE 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 router.

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

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

## 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 router 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.

The Cisco IOS XE 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, cHsrpExtSecAddrEntry, and 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 router, you must configure the virtual IP address for at least one of the routers in the group; it can be learned on the other routers in the group.

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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><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** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br><br>**Example:**<br>`Router(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 router. For HSRP to elect a designated router, you must configure the virtual IP address for at least one of the routers in the group; it can be learned on the other routers in the group. |
| **Step 6** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show standby** [**all**] [**brief**]<br><br>**Example:**<br>`Router# 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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show standby** *type number* [*group-number* \| **all**] [**brief**]<br><br>**Example:**<br>`Router# 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 router 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 1/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><br>**Example:**<br>`Router(config-if)# ip address 10.0.0.1 255.255.255.0` | Specifies an IP address for an interface. |
| **Step 5** | **standby delay minimum** *min-seconds* **reload** *reload-seconds*<br><br>**Example:**<br>`Router(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 router has reloaded. This delay period applies only to the first interface-up event after the router 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><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0` | Activates HSRP. |
| **Step 7** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show standby delay** [*typenumber*]<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><br>**Example:**<br>`Router(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** [*group-number*] **priority** *priority*<br><br>**Example:**<br>`Router(config-if)# standby 1 priority 110` | Configures HSRP priority.<br>• The default priority is 100. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br><br>**Example:**<br>`Router(config-if)# standby 1 preempt delay minimum 380` | Configures HSRP preemption and preemption delay.<br>• The default delay period is 0 seconds; if the router wants to preempt, it will do so immediately. By default, the router that comes up later becomes the standby. |
| **Step 7** | **standby** [*group-number*] **ip** *ip-address* [**secondary**]]<br><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0` | Activates HSRP. |
| **Step 8** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show standby** [**all**] [**brief**]<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-track)# exit` | Returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **interface** *type number*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(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 router 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 router 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><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **show track** [*object-number* \| **brief**] [**interface** [**brief**] \| **ip route** [**brief**] \| **resolution** \| **timers**]<br><br>**Example:**<br>`Router# 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 router also has MD5 authentication enabled.

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

## 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 router that will communicate.
10. **end**
11. **show standby**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **terminal interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><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** | **standby** [*group-number*] **priority** *priority*<br><br>**Example:**<br>`Router(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br><br>**Example:**<br>`Router(config-if)# standby 1 preempt` | Configures HSRP preemption. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **standby** [*group-number*] **authentication md5 key-string** [**0** \| **7**] *key* [**timeout** *seconds*]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 9** | Repeat Steps 1 through 8 on each router that will communicate. | — |
| **Step 10** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show standby**<br><br>**Example:**<br>`Router# 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 router that will communicate.
15. **end**
16. **show standby**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key chain** *name-of-chain*<br><br>**Example:**<br>`Router(config)# key chain hsrp1` | Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **key** *key-id*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-keychain-key)# exit` | Returns to key-chain configuration mode. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-keychain)# exit` | Returns to global configuration mode. |
| **Step 8** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 9** | **ip address** *ip-address mask* [**secondary**]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# standby 1 priority 110` | Configures HSRP priority. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br><br>**Example:**<br>`Router(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 12** | **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.21.8.12` | Activates HSRP. |
| **Step 14** | Repeat Steps 1 through 12 on each router that will communicate. | — |
| **Step 15** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 16** | **show standby**<br><br>**Example:**<br>`Router# 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><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **debug standby errors**<br><br>**Example:**<br><br>`Router# debug standby errors` | Displays error messages related to HSRP.<br><br>• Error messages will be displayed for each packet that fails to authenticate, so use this command with care. |

### Examples

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

```
Router# 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 Router A and Router B have different MD5 authentication strings:

```
Router# 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 router that will communicate.
10. **end**
11. **show standby**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **standby** [*group-number*] **priority** *priority*<br><br>**Example:**<br>`Router(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *seconds*]<br><br>**Example:**<br>`Router(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **authentication text** *string*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |
| **Step 9** | Repeat Steps 1 through 8 on each router that will communicate. | -- |
| **Step 10** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show standby**<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(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><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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*<br><br>**Example:**<br><br>`Router(config-if)# standby 1 timers 5 15` | Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down. |
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br><br>**Example:**<br><br>`Router(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 routers to be more fully utilized. A router actively forwarding traffic for one HSRP group can be in standby or in the listen state for another group.

If two routers are used, then Router A would be configured as active for group 1 and standby for group 2. Router 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, page 68 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 router, repeat Steps 5 through 7 to configure the router attributes for different standby groups.
9. **exit**
10. Repeat Steps 3 through 9 on another router.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary** ]<br><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** | **standby** [*group-number*] **priority** *priority*<br><br>**Example:**<br>`Router(config-if)# standby 1 priority 110` | Configures HSRP priority. |
| **Step 6** | **standby** [*group-number*] **preempt** [**delay** {**minimum** \| **reload** \| **sync**} *delay*]<br><br>**Example:**<br>`Router(config-if)# standby 1 preempt` | Configures HSRP preemption. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address*] **secondary**]<br><br>**Example:**<br>`Router(config-if)# standby 1 ip 10.0.0.3` | Activates HSRP. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | On the same router, repeat Steps 5 through 7 to configure the router attributes for different standby groups. | For example, Router A can be configured as an active router for group 1 and be configured as an active or standby router for another HSRP group with different priority and preemption values. |
| **Step 9** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits to global configuration mode. |
| **Step 10** | Repeat Steps 3 through 9 on another router. | Configures multiple HSRP and enables load balancing on another router. |

# 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:

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

Configure the HSRP master group using the steps in the Configuring Multiple HSRP Groups for Load Balancing, page 52 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><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** | **standby mac-refresh** *seconds*<br><br>**Example:**<br>`Router(config-if)# standby mac-refresh 30` | Configures the HSRP client group refresh interval. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** *group-number* **follow** *group-name*<br><br>**Example:**<br>`Router(config-if)# standby 1 follow HSRP1` | Configures an HSRP group as a client group. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(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 routers running HSRP. Perform this task to reenable this feature on your router 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **standby redirect** [**timers** *advertisement holddown*] [**unknown**]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]<br><br>**Example:**<br>`Router# 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 router becomes active the virtual IP address is moved to a different MAC address. The newly active router 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 router cannot cover for the lost proxy ARP database of the failed router.

### 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><br>**Example:**<br>`Router(config-if)# ip address 172.16.6.5 255.255.255.0` | Configures an IP address for an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **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>`Router(config-if)# standby 1 mac-address 5000.1000.1060`<br>**Example:**<br>`Router(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>`Router(config-if)# standby 1 ip 172.16.6.100` | 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 router. 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface vlan 400` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# standby version 2` | Changes the HSRP version. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br><br>**Example:**<br>`Router(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><br>**Example:**<br>`Router(config-if)# end` | Ends the current configuration session and returns to privileged EXEC mode. |
| **Step 8** | **show standby**<br><br>**Example:**<br>`Router# 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **redundancy**<br><br>**Example:**<br>`Router(config)# redundancy` | Enters redundancy configuration mode. |
| **Step 4** | **mode sso**<br><br>**Example:**<br>`Router(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. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-red)# exit` | Exits redundancy configuration mode. |
| **Step 6** | **no standby sso**<br><br>**Example:**<br>`Router(config)# no standby sso` | Disables HSRP SSO mode for all HSRP groups. |
| **Step 7** | **standby sso**<br><br>**Example:**<br>`Router(config)# standby sso` | Enables the SSO HSRP feature if you have disabled the functionality. |

| | Command or Action | Purpose |
|---|---|---|
| Step 8 | **end**<br><br>**Example:**<br>`Router(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:**

```
Router# 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:**

```
Router# 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**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server enable traps hsrp**<br><br>**Example:**<br>`Router(config)# snmp-server enable traps hsrp` | Enables the router to send SNMP traps and informs, and HSRP notifications. |
| **Step 4** | **snmp-server host** *host community-string* **hsrp**<br><br>**Example:**<br>`Router(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. |

# Configuration Examples for HSRP



## Example: Configuring HSRP Priority and Preemption

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

### Router A Configuration

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

### Router B Configuration

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(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, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on serial interface 1/0 in Router A fails, the HSRP group priority will be reduced and Router B will take over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Router A Configuration

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

### Router B Configuration

```
Router(config)# track 100 interface serial 1/0/0 ip routing
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
Router(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, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Router A fails, the HSRP group will be disabled and Router B will take over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Router A Configuration

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

### Router B Configuration

```
Router(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
```

```
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(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:

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

# Example: Configuring HSRP MD5 Authentication Using Key Strings

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

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

### Router 1

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

### Router 2

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

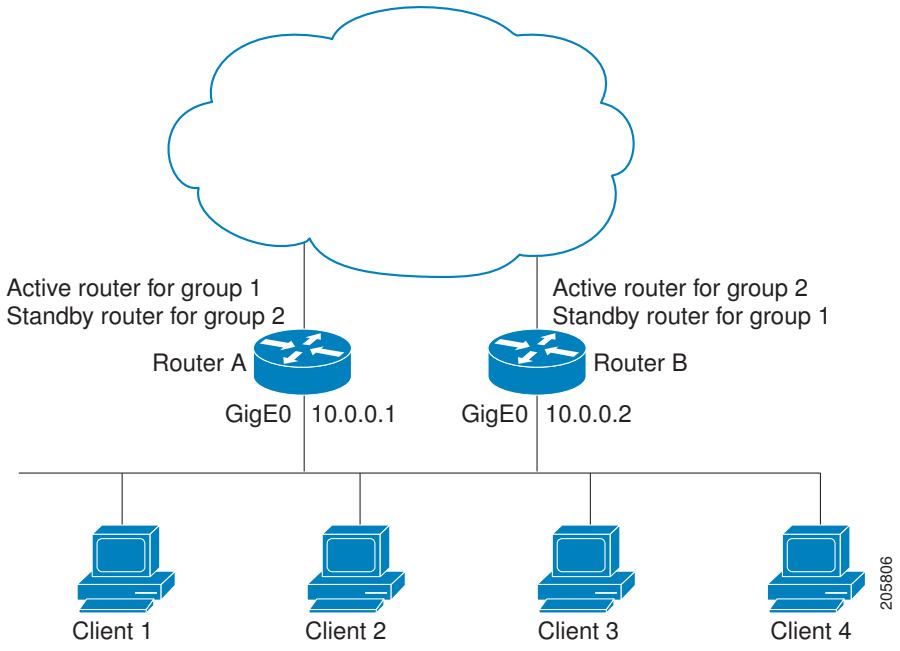
# Example: Configuring HSRP Text Authentication

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication text company2
Router(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 4 HSRP Load Sharing Example***




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:

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

## Example: Configuring HSRP Support for ICMP Redirect Messages

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

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.10 255.0.0.0
Router(config-if)# standby redirect
```

```
Router(config-if)# standby 1 priority 120
Router(config-if)# standby 1 preempt delay minimum 20
Router(config-if)# standby 1 ip 10.0.0.1
Router(config-if)# standby 2 priority 105
Router(config-if)# standby 2 preempt delay minimum 20
Router(config-if)# standby 2 ip 10.0.0.2
```

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

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

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

```
Router(config)# interface token 3/0
Router(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: Configuring HSRP Version 2

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

```
Router(config)# interface vlan 350
Router(config-if)# standby version 2
Router(config-if)# standby 350 priority 110
Router(config-if)# standby 350 preempt
Router(config-if)# standby 350 timers 5 15
Router(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.

```
Router(config)# redundancy
Router(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:

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

# Example: Enabling HSRP MIB Traps

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

### Router A

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

### Router B

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

# Additional References

### Related Documents

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

| Related Topic | Document Title |
|---|---|
| GLBP | Configuring GLBP module |
| HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Application Services Command Reference* |
| ISSU | Cisco IOS XE In Service Software Upgrade Process in the *Cisco IOS XE High Availability Configuration Guide* |
| Object tracking | Configuring Enhanced Object Tracking module |
| VRRP | Configuring VRRP module |

### 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

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*

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP--HSRP-MIB | Cisco IOS XE Release 2.1 | The FHRP--HSRP-MIB feature introduces support for the CISCO-HRSP-MIB. |
| FHRP--HSRP Group Shutdown | 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**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| FHRP--HSRP Multiple Group Optimization | 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 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><br>The following commands were introduced or modified by this feature: **standby follow**, **show standby**. |
| HSRP--ISSU | Cisco IOS XE Release 2.1 | The HSRP--ISSU feature enables support for ISSU in HSRP.<br><br>The In Service Software Upgrade (ISSU) process 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 Cisco IOS XE software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.<br><br>For more information about this feature, see the Cisco IOS XE In Service Software Upgrade Process document in the Cisco IOS XE High Availability Configuration Guide.<br><br>There are no new or modified command for this feature. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP MD5 Authentication | Cisco IOS XE Release 2.1 | 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><br>The following commands were introduced or modified by this feature: **show standby**, **standby authentication**. |
| HSRP Support for ICMP Redirects | Cisco IOS XE Release 2.1 | The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP.<br><br>The following commands were introduced or modified by this feature:<br><br>**debug standby event** , **debug standby events icmp**, **show standby**, **standby redirects** |
| HSRP Support for MPLS VPNs | 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) routers with either of the following conditions:<br><br>There are no new or modified command for this feature. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| HSRP Version 2 | Cisco IOS XE Release 2.1 | 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><br>The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**. |
| SSO--HSRP | Cisco IOS XE Release 2.1 | 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><br>The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**. |

# Glossary

active router--The primary router in an HSRP group that is currently forwarding packets for the virtual router.

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 router that services all packets sent to the HSRP address. The lead router is monitored by other routers in the group, and if it fails, one of these standby HSRP routers inherits the lead position and the HSRP group address.

**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 Cisco IOS XE 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.

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. 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. SSO refers to the implementation of Cisco IOS XE software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. Along with NSF, SSO makes an RP failure undetectable to the network.

standby group--The set of routers participating in HSRP that jointly emulate a virtual router.

standby router--The backup router 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, the automatically generated MAC address when HSRP is configured. The standard virtual MAC address used is: 0000.0C07.ACxy, 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.

# 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 feature information and caveats, see 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 document.

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 LANs. VRRP is not intended as a replacement for existing dynamic protocols.

VRRP is supported on Fast Ethernet, Bridge Group Virtual Interface (BVI), Gigabit Ethernet and TenGigabit interfaces, Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.

The **vrrp shutdown** commnd should not be used on an interface that is configured to share its interface IP address with the VRRP virtual address. This is a misconfiguration and may result in duplicate IP address errors.

# 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 to 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.

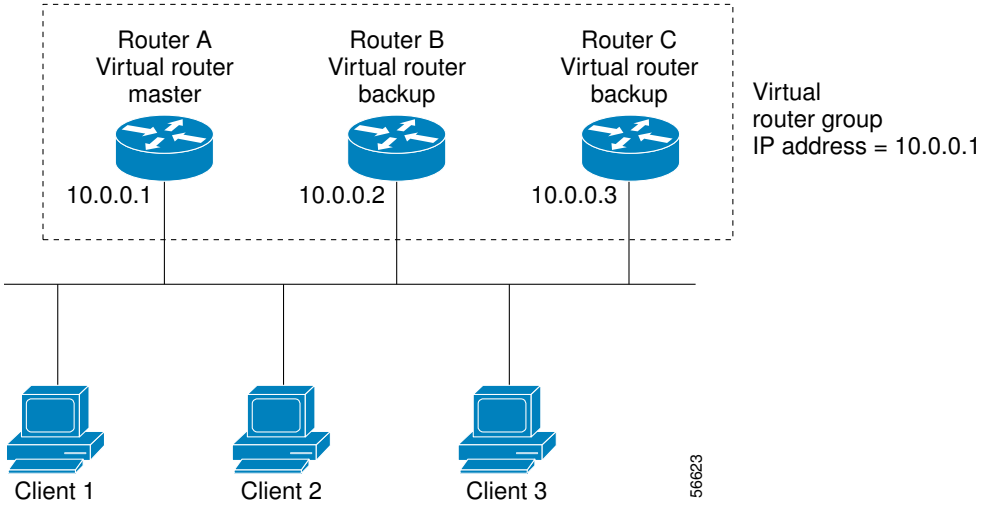
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network 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 Fast Ethernet, BVI, and Gigabit Ethernet interfaces, 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 Gigabit Ethernet interface of Router A (10.0.0.1).

***Figure 5 Basic VRRP Topology***

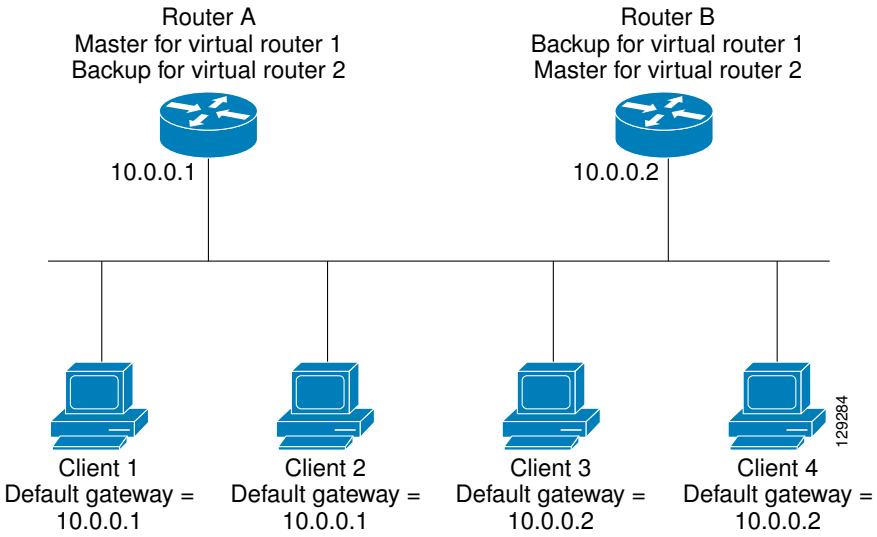



Because the virtual router uses the IP address of the physical Gigabit Ethernet interface of Router A, Router A assumes the role of the *virtual router master* and is also known as the *IP address owner*. As the virtual router master, Router A controls the IP address of the virtual router and is responsible 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, page 83 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 6 Load Sharing and Redundancy VRRP Topology***



In this topology, two virtual routers are configured. (For more information, see the Multiple Virtual Router Support, page 82 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 a GigabitEthernet 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.

### 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.

# 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.

# 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 Cisco IOS XE 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 XErelease 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 theCisco IOS XE In Service Software Upgrade Process document in the *Cisco IOS XE 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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><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><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><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><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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **vrrp** *group* **timers advertise** [**msec**] *interval*<br><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><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><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |
| **Step 11** | **no vrrp sso**<br><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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><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><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><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **show vrrp** [**brief**] \| *group*]<br><br>**Example:**<br><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><br>**Example:**<br><br>`Router# show vrrp interface GigabitEthernet 0/0/0` | (Optional) Displays the VRRP groups and their status on a specified interface. |

# Disabling a VRRP Group on an Interface

Disabling a VRRP group on an interface allows the protocol to be disabled, but the configuration to be retained. This ability was added with the introduction of the VRRP MIB, RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol* .

You can use a Simple Network Management Protocol (SNMP) management tool to enable or disable VRRP on an interface. Because of the SNMP management capability, the **vrrp shutdown** command was introduced to represent a method via the command line interface (CLI) for VRRP to show the state that had been configured using SNMP.

When the **show running-config** command is entered, you can see immediately if the VRRP group has been configured and set to enabled or disabled. This is the same functionality that is enabled within the MIB.

The **no** form of the command enables the same operation that is performed within the MIB. If the **vrrp shutdown** command is specified using the SNMP interface, then entering the **no vrrp shutdown** command reenables the VRRP group.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **shutdown**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | Enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask*<br><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* **shutdown**<br><br>**Example:**<br>`Router(config-if)# vrrp 10 shutdown` | Disables the VRRP group on an interface.<br>• The command is now visible on the router.<br>**Note** You can have one VRRP group disabled, while retaining its configuration, and a different VRRP group enabled. |

# Configuring VRRP Text Authentication

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **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><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/1` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary**]<br><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. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **vrrp** *group* **authentication text** *text-string*<br><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.<br>**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><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><br>**Example:**<br>`Router(config-if)# end` | Returns to privileged EXEC mode. |

# Enabling the Router to Send SNMP VRRP Notifications

The VRRP MIB supports SNMP Get operations, which allow network devices to get reports about VRRP groups in a network from the network management station.

Enabling VRRP 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 router becomes a Master or backup router. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

### SUMMARY STEPS

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

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server enable traps vrrp**<br><br>**Example:**<br>`Router(config)#`<br>`snmp-server enable traps vrrp` | Enables the router to send SNMP VRRP notifications (traps and informs). |
| **Step 4** | **snmp-server host** *host community-string* **vrrp**<br><br>**Example:**<br>`Router(config)#`<br>`snmp-server host myhost.comp.com public vrrp` | Specifies the recipient of an SNMP notification operation. |

# 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 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: Disabling a VRRP Group on an Interface

The following example shows how to disable one VRRP group on GigabitEthernet interface 0/0/0 while retaining VRRP for group 2 on GigabitEthernet interface 1/0/0:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
Router(config-if)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```

## 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 |
| Hot Standby Routing Protocol (HSRP) | Configuring HSRP |
| In Service Software Upgrace (ISSU) | "Cisco IOS XE In Service Software Upgrade Process" in the *Cisco IOS XEHigh Availability Configuration Guide* |
| Gateway Load Balancing Protocol (GLBP) | Configuring GLBP |
| Stateful Switchover | The Stateful Switchover section in the *Cisco IOS XE 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 3 Feature Information for VRRP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| ISSU--VRRP | Cisco IOS XE Release 2.1 | 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 XE 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. |
| SSO--VRRP | Cisco IOS XE Release 2.1 | 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**, **show vrrp, vrrp sso**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| Virtual Router Redundancy Protocol | Cisco IOS XE Release 2.1 | 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><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 MIB--RFC 2787 | Cisco IOS XE Release 2.6 | 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><br>The following command was introduced by this feature: **vrrp shutdown**.<br><br>The following commands were modified by this feature: **snmp-server enable traps**and **snmp-server host**. |

# 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.

# Virtual Router Redundancy Service

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several 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 FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 an FHRP, but which share a physical interface with an FHRP it is following.
- VRRPv2 is configurable only on Gigabit Ethernet interfaces.

# Information About VRRS



## VRRS Overview

VRRS improves the scalability of FHRP. VRRS provides a stateless redundancy service to applications (VRRS clients) by monitoring VRRP. VRRS provides a database of the current VRRP state and operates without maintaining sessions or keeping track of previous states of the clients and servers with which it communicates. VRRP acts as a VRRS server. VRRS clients are other Cisco IOS processes or applications that use VRRP to provide or withhold a service or resource dependent upon the state of the group.

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 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.

## 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 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 INIT). The VRRP state is then passed on to clients or acted on by a plug-in. A VRRP group should be configured with a name to activate VRRS. 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. Clients act on the VRRP server state. When a VRRP group changes state, VRRS clients act by altering their behavior (performing tasks such as shutting down interfaces or appending accounting logs) depending on the state received from VRRS.

The following can be VRRS clients:

- PPP over Ethernet (PPPoE) subinterfaces
- Access Node Control Protocol (ANCP) subinterfaces

- VRRS Interface-state plug-in
- VRRS MAC-Address plug-in
- VRRS Accounting plug-in

VRRS plug-ins extend the failover of VRRP without the need for configuring VRRP groups on all subinterfaces. Configuring a VRRS plug-in on subinterfaces is a substitute for having to configure multiple VRRP groups on many subinterfaces. Plug-ins provide a light-weight version of VRRP and scale better than a fully configured VRRP group. The state of the plug-ins follows the VRRP server state. Client plug-ins are configured on other subinterfaces that share the same physical interface as VRRP.

# VRRS MAC-Address Plug-in

The VRRS MAC-Address plug-in provides a mechanism for controlling a virtual MAC address associated with the primary interface IP address. If the VRRS MAC-Address plug-in is configured on an interface, and a VRRP group shares a name association with the plug-in, then a VRRS active state associates a virtual MAC address with the configured primary IP address.

The VRRS MAC-Address plug-in is only interested in the VRRS active state, which is interpreted as up. All other states are interpreted as down. When the state is up and the additional interface criteria listed below have been met, then the VRRS MAC-Address plug-in provides the following services:

- Overwrites the interface IP address ARP table with a virtual MAC address provided by VRRS
- Inserts the virtual MAC address provided by VRRS into the MAC address filter of the interface
- Controls the ARP reply mechanism by substituting a VRRS-provided virtual MAC address
- Broadcasts unsolicited ARP messages that include the VRRS virtual MAC address

When VRRS is in a nonactive state, the virtual MAC address is unassociated from the primary IP address.

When you use the VRRS MAC-Address plug-in, the VRRS Interface-State plug-in must also be used in order to prevent address conflicts with other redundant members.

Additional interface criteria:

- Interfaces must be configured with an interface IP address.
- Interfaces must be in the line-protocol up state.
- Other FHRP protocols cannot be configured on the interface; these include HSRP, VRRP, and GLBP.

The VRRS MAC-Address plug-in is associated with a VRRS group name by configuring the **vrrs follow** *name* command.

# VRRS Interface-State Plug-in

The VRRS Interface-State plug-in provides a mechanism for controlling the line-protocol state of a subinterface based on the state of VRRP. The VRRS Interface-State plug-in is an extension of the VRRS, and is directly controlled by the push events associated with the VRRS. If the plug-in is configured on an interface, and a VRRP group shares a name association with the VRRS plug-in, then a VRRS active state allows the line- protocol state of the interface to be up. A VRRS nonactive state will cause the line protocol of the interface to be down.

**Note** When first configured, the interface line protocol may immediately change to the down state until the VRRS state is confirmed as up.

The VRRS Interface-State plug-in is associated with a VRRS group name by configuring the **vrrs follow** *name* command.

The Interface-State plug-in restricts the operation of the **no shutdown** command. When an interface is line-protocol down, the interface state will not go up.

# VRRS Accounting Plug-in

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode.

The VRRS Accounting plug-in sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, VRRS
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Time
- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop messages for sessions that are part of that VRRS.

The VRRS accounting type is implemented by AAA to support VRRS accounting.

# How to Configure VRRS

# Configuring a VRRS Server

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
5. **vrrp** *group-number* **name** [*vrrp-group-name*]
6. **vrrp** *group* **ip** *ip-address* [**secondary**]
7. **vrrp delay** {**minimum** *seconds* [**reload** *seconds*] | **reload** *seconds*}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface gigabitethernet 0/0/0` | Configures an interface type and enters interface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]<br><br>**Example:**<br>`Router(config-if)# ip address 10.0.0.1 255.255.255.0` | Sets a primary or secondary IP address for an interface. |
| **Step 5** | **vrrp** *group-number* **name** [*vrrp-group-name*]<br><br>**Example:**<br>`Router(config-if)# vrrp 1 name name1` | Links a VRRS client to a VRRP group. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **vrrp** *group* **ip** *ip-address* [**secondary**]<br><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** | **vrrp delay** {**minimum** *seconds* [**reload** *seconds*] \| **reload** *seconds*}<br><br>**Example:**<br>`Router(config-if)# vrrp delay minimum 30 reload 60` | Configures the delay period before the initialization of all VRRP groups on an interface.<br>The recommended **minimum** *seconds* value is 30 seconds, and the recommended **reload** *seconds* value is 60 seconds. |

# Configuring the Clients That Use VRRS

Perform this task to configure the clients, including VRRS plug-ins, that use VRRS. This task is configured on multiple subinterfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number***.***subinterface*
4. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
5. **vrrs follow** *name*
6. **vrrs interface-state**
7. **vrrs mac-address** [**arp** [**interval** *seconds*] [**duration** *seconds*]]
8. Repeat Steps 3 through 7 to configure additional subinterfaces.

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type number.subinterface*<br><br>**Example:**<br>`Router(config)# interface gigabitethernet0/0/0.1` | Configures a subinterface type and enters subinterface configuration mode. |
| **Step 4** | **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]<br><br>**Example:**<br>`Router(config-subif)# ip address 10.0.0.1 255.255.255.0` | Sets a primary or secondary IP address for an interface.<br>This interface should be a subinterface. |
| **Step 5** | **vrrs follow** *name*<br><br>**Example:**<br>`Router(config-subif)# vrrs follow name1` | Configures a name association between VRRS plug-ins and the VRRS server. |
| **Step 6** | **vrrs interface-state**<br><br>**Example:**<br>`Router(config-subif)# vrrs interface-state` | (Optional) Configures the VRRP shutdown plug-in on an interface. |
| **Step 7** | **vrrs mac-address** [**arp** [**interval** *seconds*] [**duration** *seconds*]]<br><br>**Example:**<br>`Router(config-subif)# vrrs mac-address` | (Optional) Configures the VRRS MAC-Address plug-in on an interface. |
| **Step 8** | Repeat Steps 3 through 7 to configure additional subinterfaces. | |

# Configuring VRRS Accounting

Perform this task to configure VRRS to send AAA accounting messages to the AAA server when there is a state-change in VRRS from active to standby or from standby to active.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting vrrs** { **default** | *list-name* **start-stop** [*method1* [*method2...*]]
4. **aaa attribute list** *list-name*
5. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*] [**mandatory**] [ **tag** *tag-value*]
6. **exit**
7. **vrrs** *vrrs-group-name*
8. **accounting delay** *delay*
9. **accounting method** {**default** | *accounting-method-list*}
10. **attribute list** *list-name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa accounting vrrs** { **default** \| *list-name* **start-stop** [*method1* [*method2...*]]<br><br>**Example:**<br>`Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius` | Enables AAA accounting of requested services for billing or security purposes when you use VRRS. |
| **Step 4** | **aaa attribute list** *list-name*<br><br>**Example:**<br>`Router(config)# aaa attribute list vrrp-1-attr` | Defines a AAA attribute list locally on a router. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **attribute type** *name value* [**service** *service*] [**protocol** *protocol*] [**mandatory**] [ **tag** *tag-value*]<br><br>**Example:**<br>`Router(config-attr-list)# attribute type account-delay “10”` | Defines an attribute type that is to be added to an attribute list locally on a router. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-attr-list)# exit` | Exits attribute list configuration mode and returns to global configuration mode. |
| **Step 7** | **vrrs** *vrrs-group-name*<br><br>**Example:**<br>`Router(config)# vrrs vrrp-name-1` | (Optional) Specifies a distinct AAA accounting method list to use, a nonzero delay time for accounting-off messages, and additional attributes other than the default for a VRRP group. |
| **Step 8** | **accounting delay** *delay*<br><br>**Example:**<br>`Router(config-vrrs)# accounting delay 10` | (Optional) Specifies a delay time for sending accounting-off messages for VRRS. |
| **Step 9** | **accounting method** {**default** \| *accounting-method-list*}<br><br>**Example:**<br>`Router(config-vrrs)# accounting method METHOD1` | (Optional) Enables VRRS accounting for a VRRP group. |
| **Step 10** | **attribute list** *list-name*<br><br>**Example:**<br>`Router(config-vrrs)# attribute list vrrp-1-attr` | (Optional) Specifies additional attributes to include in VRRS accounting-on and accounting-off messages. |

# Monitoring and Maintaining VRRS

### SUMMARY STEPS

1. **debug vrrp vrrs**
2. **debug vrrs accounting** {**all** | **errors** | **events**}
3. **debug vrrs infra** {**all** | **client** | **events** | **server**}
4. **debug vrrs plugin** {**all** | **arp-packet** | **client** | **database** | **if-state** | **mac** | **process** | **sublock** | **test**}
5. **show vrrs clients**
6. **show vrrs group** [*group-name*]
7. **show vrrs plugin database**
8. **show vrrs summary**

### DETAILED STEPS

**Step 1** **debug vrrp vrrs**
This command enables VRRP debugging statements for VRRS interactions.

**Example:**

```
Router# debug vrrp vrrs

VRRP VRRS debugging is on
*Feb  5 09:29:47.005: VRRP: Registered VRRS group "name1"
*Feb  5 09:29:53.237: VRRP: Updated info for VRRS group name1
*Feb  5 09:30:14.153: VRRP: Unregistered VRRS group "name1"
*Feb  5 09:30:14.153: VRRP: Registered VRRS group "name2"
*Feb  5 09:30:22.689: VRRP: Unregistered VRRS group "name2"
```

**Step 2** **debug vrrs accounting** {**all** | **errors** | **events**}
This command enables debug messages for VRRS accounting.

**Example:**

```
Router# debug vrrs accounting

00:16:13: VRRS/ACCT/EV: entry create for abc(0x4E8C1F0)
00:16:13: VRRS/ACCT/EV: abc(0x4E8C1F0 12000006) client add ok2(No group)
```

**Step 3** **debug vrrs infra** {**all** | **client** | **events** | **server**}
This command enables VRRS infrastructure debug messages.

**Example:**

```
Router# debug vrrs infra

*Sep 9 16:09:53.848: VRRS: Client 21 is not registered
*Sep 9 16:09:53.848: VRRS: Client 21 unregister failed
*Sep 9 16:09:53.848: VRRS: Client VRRS TEST CLIENT registered, id 21
*Sep 9 16:09:53.848: VRRS: Client 21 add, group VRRP-TEST-1 does not exist, allocating...
*Sep 9 16:09:53.848: VRRS: Client 21 add to VRRP-TEST-1. Vrrs handle F7000001, client
handle FE720
```

```
*Sep 9 16:09:53.848: VRRS: Server VRRP add, group VRRP-TEST-1, state INIT, vrrs handle
F7000001
```

**Step 4** **debug vrrs plugin** {**all** | **arp-packet** | **client** | **database** | **if-state** | **mac** | **process** | **sublock** | **test**}
This command enables VRRS plug-in debug messages.

**Example:**

```
Router# debug vrrs plugin

Feb 17 19:15:38.052: VRRS-P(mac): GigEth0/0/0.1 Add 0000.12ad.0001 to MAC filter, using
(afilter_add)
Feb 17 19:15:38.053: VRRS-P(mac): Active count increase to (2) for MAC : 0000.12ad.0001
```

**Step 5** **show vrrs clients**
This command displays a list of VRRS clients.

**Example:**

```
Router# show vrrs clients

ID  Priority  All-groups  Name
-----------------------------
1   High      No          VRRS-Plugins
2   Low       Yes         VRRS-Accounting
3   Normal    No          PPPOE-VRRS-CLIENT
```

**Step 6** **show vrrs group** [*group-name*]
This command displays information about VRRS groups.

**Example:**

```
Router# show vrrs group DT-CLUSTER-3

DT-CLUSTER-3
Server Not configured, state INIT, old state INIT, reason Protocol
  Address family IPv4, Virtual address 0.0.0.0, Virtual mac 0000.0000.0000
  Active interface address 0.0.0.0, standby interface address 0.0.0.0
Client 5 VRRS TEST CLIENT, priority Low
```

**Step 7** **show vrrs plugin database**
This command displays details about the internal VRRS plug-in database.

**Example:**

```
Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Disabled
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                 gige0/0/0.2
                 gige0/0/0.3
```

**Step 8** **show vrrs summary**
This command displays a summary of all VRRS groups.

**Example:**

```
Router# show vrrs summary

Group                                                 Server State Virtual-address
-------------------------------------------------------------------------------
DT-CLUSTER-3                                          UNKNOW INIT    0.0.0.0
DT-CLUSTER-2                                          VRRP   BACKUP 11.1.1.1
DT-CLUSTER-1                                          VRRP   ACTIVE  1.1.1.1
```

# Configuration Examples for VRRS



## Example: Configuring a VRRS Server

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# vrrp 1 name name1
Router(config-if)# vrrp 1 ip 10.0.1.20
Router(config-if)# vrrp delay minimum 30 reload 60
```

## Example: Configuring the Clients that use VRRS

The following example shows how to configure the clients, including VRRS plug-ins, that use VRRS.

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0.1
Router(config-subif)# ip address 10.0.0.1 255.255.255.0
Router(config-subif)# vrrs follow name1
Router(config-subif)# vrrs interface-state
Router(config-subif)# vrrs mac-address
```

## Example: Configuring VRRS Accounting

The following example shows how to configure VRRS to send AAA accounting messages to the AAA server when there is a state change in VRRS from active to standby or from standby to active.

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay “10”
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-name-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method METHOD1
Router(config-vrrs)# attribute list vrrp-1-attr
```

# Example: Confirming Operation of the VRRS Interface-State Plug-in

The following example shows how to confirm the VRRS Interface-State plug-in.

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# no ip address
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.1
Router(config-if)# encapsulation dot1Q 1 native
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# vrrp 1 name VRRS_NAME_1
Router(config-if)# vrrp 1 ip 172.16.1.254
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.2
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip address 192.168.42.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.3
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip address 192.168.43.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.4
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip address 192.168.44.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_2
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router# show ip interface brief

Interface                      IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0           unassigned      YES NVRAM  up                    up
GigabitEthernet0/0/0.1         172.24.1.1      YES manual up                    up
GigabitEthernet0/0/0.2         192.168.42.1    YES manual up                    up
GigabitEthernet0/0/0.3         192.168.43.1    YES manual up                    up
GigabitEthernet0/0/0.4         192.168.44.1    YES manual up                    down
! "interface-state" DOWN due to no VRRS server

Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Active
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                GigE0/0/0.2
                GigE0/0/0.3
------------------------------------------------
Name = VRRS_NAME_2
Server connection = Disconnected
State = Disabled
MAC addr = 0000.0000.0000
Test Control = False
Client Handle = 603979779
Interface list =
                GigE0/0/0.4
```

# Example: Confirming Operation of the VRRS MAC-Address plug-in

The following example shows the confirm operation for the VRRS MAC address plug-in.

```
Router(config)# interface GigabitEthernet0/0/0
```

```
Router(config-if)# no ip address
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.1
Router(config-if)# encapsulation dot1Q 1 native
Router(config-if)# ip address 172.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 name VRRS_NAME_1
Router(config-if)# vrrp 1 ip 172.24.1.254
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.2
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip address 192.168.42.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.3
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip address 192.168.43.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.4
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip address 192.168.44.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_2
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router# show ip arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.24.1.1              -   aabb.cc00.fb00  ARPA   GigabitEthernet0/0/0.1
Internet  172.24.1.254            -   0000.5e00.0101  ARPA   GigabitEthernet0/0/0.1
Internet  192.168.42.1            -   0000.5e00.0101  ARPA   GigabitEthernet0/0/0.2
!"mac-address" enabled interfaces using VRRP MAC via VRRS
Internet  192.168.43.1            -   0000.5e00.0101  ARPA   GigabitEthernet0/0/0.3
!"mac-address" enabled interfaces using VRRP MAC via VRRS
Internet  192.168.44.1            -   aabb.cc00.fb00  ARPA   GigabitEthernet0/0/0.4
!"mac-address" disabled interface using BIA
Router# debug arp

ARP packet debugging is on
*Sep 10 20:02:14.971: IP ARP: sent rep src 192.168.42.1 0000.5e00.0101,
                dst 192.168.42.1 ffff.ffff.ffff Ethernet0/0.2
*Sep 10 20:02:14.971: IP ARP: sent rep src 192.168.43.1 0000.5e00.0101,
                dst 192.168.43.1 ffff.ffff.ffff Ethernet0/0.3
*Sep 10 20:02:19.991: IP ARP: sent rep src 192.168.42.1 0000.5e00.0101,
                dst 192.168.42.1 ffff.ffff.ffff Ethernet0/0.2
*Sep 10 20:02:19.991: IP ARP: sent rep src 192.168.43.1 0000.5e00.0101,
                dst 192.168.43.1 ffff.ffff.ffff Ethernet0/0.3
Router# show controller gigabitethernet0/0/0

Interface GigabitEthernet0/0/0
Hardware is AMD Unknown
ADDR: 1EC55D8, FASTSEND: FC286088, MCI_INDEX: 0
DIST ROUTE ENABLED: 0
Route Cache Flag: 11
 amdp2_instance=0x1EC6798, registers=0x1EC5580, ib=0x1EC6D98
 rx ring entries=32, tx ring entries=64
 rxring=0x1EC6DE8, rxr shadow=0x1EC7020, rx_head=0, rx_tail=0
 txring=0x1EC70D8, txr shadow=0x1EC7510, tx_head=0, tx_tail=57, tx_count=57
 running=0, port id=0x5DCF8
 Software MAC address filter(hash:length/addr/mask/hits):
  0x00:  0  ffff.ffff.ffff  0000.0000.0000         0
  0x4C:  0  0100.5e00.0012  0000.0000.0000         0
  0x5F:  0  0000.5e00.0101  0000.0000.0000         0
! Virtual MAC, note for this interface, it may be VRRP that added this MAC.
  0xC0:  0  0100.0ccc.cccc  0000.0000.0000         0
  0xC0:  1  0180.c200.0002  0000.0000.0000         0
  0xC5:  0  0180.c200.0007  0000.0000.0000         0
  0xCC:  0  aabb.cc00.fb00  0000.0000.0000         0
Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
```

```
Name = VRRS_NAME_1
Server connection = Live
State = Active
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                GigE0/0/0.2
                GigE0/0/0.3
-----------------------------------------------
Name = VRRS_NAME_2
Server connection = Diconnected
State = Disabled
MAC addr = 0000.0000.0000
Test Control = False
Client Handle = 603979779
Interface list =
                GigE0/0/0.4
```

# Where to Go Next

If you want to configure additional VRRP features, see the Configuring VRRP document.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| ANCP | *Access Node Control Protocol Configuration Guide* |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| VRRP | Configuring VRRP |
| VRRP and VRRS commands | *Cisco IOS IP Application Services Command Reference* |

### Standards

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

### MIBs

| MIB | 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

| RFC | 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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for VRRS

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 4 Feature Information for VRRS*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Virtual Router Redundancy Service (VRRS) | Cisco IOS XE Release 2.6 | Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP), and a registered client.<br><br>The following commands were introduced or modified:<br><br>**aaa accounting vrrs** , **accounting delay** (VRRS), **accounting method**(VRRS), **attribute list** (VRRS), **debug vrrp all**, **debug vrrp vrrs**, **debug vrrs accounting**, **debug vrrs infra**, **debug vrrs plugin**, **show vrrp**, **show vrrs clients**, **show vrrs clients**, **show vrrs group**, **show vrrs plugin database**, **show vrrs summary**, **vrrp delay**, **vrrs follow**, **vrrp ip**, **vrrs mac-address**, **vrrp name**, **vrrs**. |

# Glossary

**AAA** --authentication, authorization, and accounting.

**RADIUS** --Remote Authentication Dial-In User Service.

**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.

**VRRP** --Virtual Router Redundancy Protocol. 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.

**VSA** --vendor-specific attribute. An attribute that has been implemented by a particular vendor.

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.