Configuring HSRP

Last Updated: December 20, 2011

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.
- HSRP is configurable on Ethernet, FDDI, BVI, LANE, or Token Ring interfaces. Token Ring interfaces allow up to three Hot Standby groups each, the group numbers being 0, 1, and 2.

- The Cisco 2500 series, Cisco 3000 series, Cisco 4000 series, and Cisco 4500 routers that use Lance Ethernet hardware do not support multiple Hot Standby groups on a single Ethernet interface. The Cisco 800 series and Cisco 1600 series that use PQUICC Ethernet hardware do not support multiple Hot Standby groups on a single Ethernet interface. You can configure a workaround solution by using the **standby use-bia** interface configuration command, which uses the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address.

- HSRP support for Bidirectional Forwarding Detection (BFD) is not available for all platforms and interfaces.

- The same HSRP group number or HSRP MAC address cannot be configured on different subinterfaces of the same major interface.

> **Note** This restriction was removed in Cisco IOS Release 12.4(14), 12.4(15)T, 12.2(33)SRB, 12.2(33)SXH, and later releases.

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

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 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 1　　　　　*HSRP Topology*
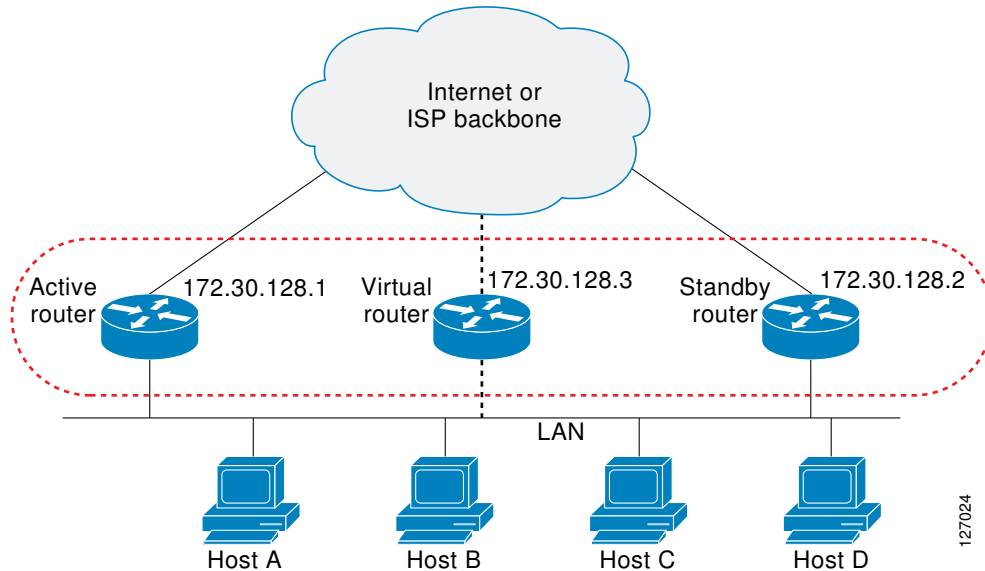
HSRP is supported over Inter-Switch Link (ISL) encapsulation. See the "Virtual LANs" section of the "Configuring Routing Between VLANs " chapter in the *Cisco IOS LAN Switching Configuration Guide.*

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 Configuration Changes

In Cisco IOS Release 12.2(33)SXI, 12.4(24)T, 12.2(33)SRE, and later releases, an HSRP group may be configured with a virtual IP address that matches the subnet of an IP address of a secondary interface.

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

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

Prior to Cisco IOS Release 12.2(33)SXI, 12.4(24)T, or 12.2(33)SRE, an HSRP group remained in INIT state unless the HSRP virtual IP address had the same network ID as the primary interface address.

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

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

HSRP Benefits

Redundancy

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

Fast Failover

HSRP provides transparent fast failover of the first-hop 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.

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

Token Ring interfaces use functional addresses for the HSRP MAC address. Functional addresses are the only general multicast mechanism available. A limited number of Token Ring functional addresses are available, and many of them are reserved for other functions. The following are the only three addresses available for use with HSRP:

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

Thus, only three HSRP groups may be configured on Token Ring interfaces unless the **standby use-bia** interface configuration command is configured.

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 MAC Refresh Interval

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

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

HSRP Text Authentication

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

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, 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 Support for IPv6

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

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

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

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

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

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

HSRP Messages and States

Routers configured with HSRP exchange three types of multicast messages:

- Coup—When a standby router wants to assume the function of the active router, it sends a coup message.
- Hello—The hello message conveys to other HSRP routers the HSRP priority and state information of the router.

- 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.
- 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.
- Learn—The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.
- Listen—The router is receiving hello messages.
- Speak—The router is sending and receiving hello messages.
- Standby—The router is prepared to assume packet-transfer functions if the active router fails.

In Cisco IOS Release 12.2(33)SXH, Cisco IOS Release 12.2(33)SRB, Cisco IOS Release 12.4(8), and later releases, 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.

Cisco IOS software prior to these releases uses logging Level 6 for syslog messages related to HSRP state changes.

HSRP Group Linking to IP Redundancy Clients

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

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

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

HSRP 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 Gratuitous ARP

The HSRP Gratuitous ARP feature configures HSRP to check that the entries in the ARP cache are correct and to send periodic gratuitous ARP packets from one or more HSRP active groups. By default, HSRP sends out three gratuitous ARP packets from an HSRP group when the group state changes to Active. HSRP sends the first gratuitous ARP packet when the group becomes active. The second two gratuitous ARP packets are sent 2 and 4 seconds later.

The HSRP Gratuitous ARP feature enhances the capability of HSRP so that the number and frequency of gratuitous ARP packets sent by an active HSRP group are configurable. Use the **standby arp gratuitous**

command in interface configuration mode to configure a specific number of gratuitous ARP packets to be sent at a specified interval.

Use the **standby send arp** command in EXEC mode to configure HSRP to send a single gratuitous ARP packet for each active group. When the **standby send arp** command is configured, HSRP checks that the entries in the ARP cache are correct prior to sending a gratuitous ARP packet. If an ARP entry is incorrect, HSRP will try to readd it. Static or alias ARP entries cannot be overwritten by HSRP.

Configuring the **standby send arp** command ensures that a host ARP cache is updated prior to heavy CPU-usage processes or configurations are started.

When CPU usage is above 50 percent due to heavy ARP traffic combined with moderate software switched IP traffic, ARP refresh requests could fail, causing some application servers to lose their default gateway ARP entries and fail to communicate with the rest of the network. In some scenarios, operations such as enabling a large access list can cause ARP requests from hosts to be delayed, causing the host to have no default gateway for a short time. A periodic gratuitous ARP packet sent from the HSRP active router refreshes the host ARP cache before it expires.

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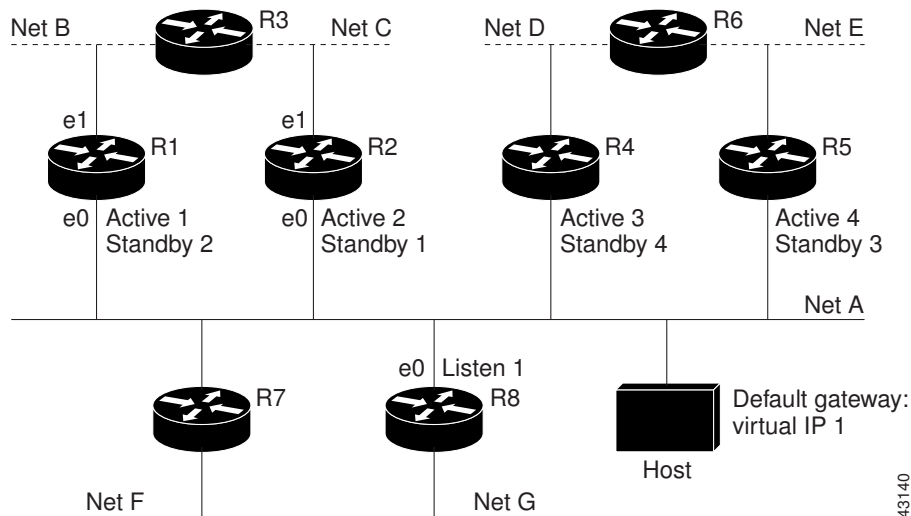
If the host wants to send a packet to another host on Net D, then it first sends it to its default gateway, the virtual IP address of HSRP group 1.

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.

HSRP--ISSU

The In Service Software Upgrade (ISSU) process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.

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

For detailed information about ISSU on the 7600 series routers, see the *ISSU and eFSU on Cisco 7600 Series Routers* document at the following URL:

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/guide/efsuovrw.html

For detailed information about ISSU on Cisco Catalyst 4500 series switches, see the "Configuring the Cisco IOS In Service Software Upgrade Process" chapter of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* , Release 12.2(31)SGA at the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/issu.html

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

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

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

HSRP and SSO Working Together

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

Prior to introduction of the SSO HSRP 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).

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

HSRP BFD Peering

The HSRP BFD Peering feature introduces BFD in the HSRP group member health monitoring system. HSRP supports BFD as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with millisecond hello and hold timers. BFD runs as a pseudo-preemptive process and can therefore be guaranteed to run when required. Only one BFD session between two routers can provide early failover notification for multiple HSRP groups.

This feature is enabled by default. The HSRP standby router learns the real IP address of the HSRP active router from the HSRP Hello messages. The standby router will register as a BFD client and ask to be notified if the active router becomes unavailable.

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

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols BGP, EIGRP, HSRP, IS-IS, and OSPF. By sending rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process, BFD contributes to greatly reduce overall network convergence time. The figure below shows a simple network with two routers running HSRP and BFD.

Figure 3   *HSRP BFD Peering*
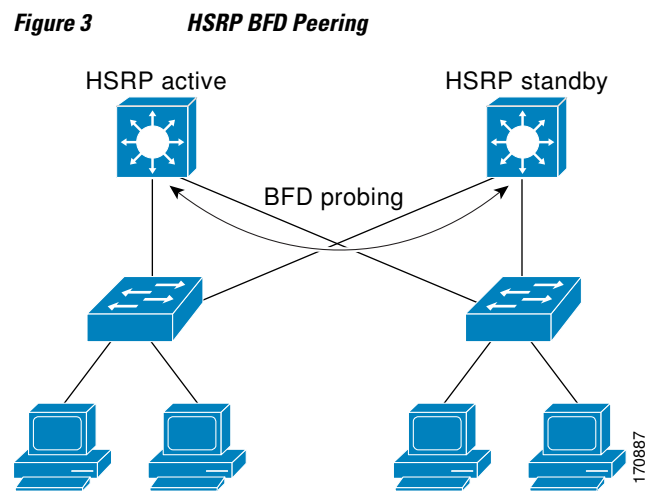
For more information on BFD, see the Bidirectional Forwarding Detection chapter in the *Cisco IOS IP Routing Configuration Guide*

HSRP MIB Traps

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

Enabling HSRP MIB trap support is performed through the CLI, and the MIB is used for getting the reports. A trap notifies the network management station when a 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 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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** 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	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 172.16.6.100`	Activates HSRP. • 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. • 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** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show standby** [**all**] [**brief**] **Example:** `Router# show standby`	(Optional) Displays HSRP information. • This command displays information for each group. The **all** option displays groups that are learned or that do not have the **standby ip** command configured.
Step 8	**show standby** *type number* [*group-number* | **all**] [**brief**] **Example:** `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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 1/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** 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 delay minimum** *min-seconds* **reload** *reload-seconds* **Example:** Router(config-if)# standby delay minimum 30 reload 60	(Optional) Configures the delay period before the initialization of HSRP groups. • 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. • 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. **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**]] **Example:** Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0	Activates HSRP.
Step 7 **end** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 8 **show standby delay** [*typenumber*] **Example:** 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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** 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* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority. • The default priority is 100.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum**	**reload**	**sync**} *seconds*] **Example:** `Router(config-if)# standby 1 preempt delay minimum 380`	Configures HSRP preemption and preemption delay. • 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**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	Activates HSRP.
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show standby** [**all**] [**brief**] **Example:** `Router# show standby`	(Optional) Displays HSRP information. • 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**] **Example:** `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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**track** *object-number* **interface** *type number* {**line-protocol**	**ip routing**} **Example:** 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** **Example:** Router(config-track)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 5	**interface** *type number*	Configures an interface type and enters interface configuration mode.
	Example:	
	Router(config)# interface GigabitEthernet 0/0/0	
Step 6	**standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]	Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object.
		• 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.
	Example:	• 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.
	Router(config-if)# standby 1 track 100 decrement 20	• Use the **shutdown** keyword to disable the HRSP group on the router when the tracked object goes down.
		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**]]	Activates HSRP.
		• 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.
	Example:	
	Router(config-if)# standby 1 ip 10.10.10.0	
Step 8	**end**	Returns to privileged EXEC mode.
	Example:	
	Router(config-if)# end	

Command or Action	Purpose
Step 9 **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]	Displays tracking information.
Example:	
Router# show track 100 interface	

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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**terminal interface** *type number* **Example:** Router(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** 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* **Example:** Router(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] **Example:** 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*] **Example:** Router(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30	Configures an authentication string for HSRP MD5 authentication. • The *key* argument can be up to 64 characters in length. We recommended that at least 16 characters be used. • No prefix to the *key* argument or specifying **0** means the key will be unencrypted. • 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. • 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**]] **Example:** 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** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 11	**show standby** **Example:** Router# show standby	(Optional) Displays HSRP information. • 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `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* **Example:** Router(config-keychain)# key 100	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The value for the *key-id* argument must be a number.
Step 5	**key-string** *string* **Example:** Router(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. • 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** **Example:** Router(config-keychain-key)# exit	Returns to key-chain configuration mode.
Step 7	**exit** **Example:** Router(config-keychain)# exit	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** 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* **Example:** 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*] **Example:** Router(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 12 **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name* **Example:** Router(config-if)# standby 1 authentication md5 key-chain hsrp1	Configures an authentication MD5 key chain for HSRP MD5 authentication. • The key chain name must match the name specified in Step 3.
Step 13 **standby** [*group-number*] **ip** [*ip-address* [*secondary*]] **Example:** 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** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 16 **show standby** **Example:** Router# show standby	(Optional) Displays HSRP information. • 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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug standby errors** **Example:** Router# debug standby errors	Displays error messages related to HSRP. • 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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** 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* **Example:** Router(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6 **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] **Example:** Router(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7 **standby** [*group-number*] **authentication text** *string* **Example:** Router(config-if)# standby 1 authentication text authentication1	Configures an authentication string for HSRP text authentication. • The default string is cisco.
Step 8 **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** 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** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 11 **show standby** **Example:** Router# show standby	(Optional) Displays HSRP information. • 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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** 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**]] **Example:** 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* **Example:** 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**]] **Example:** Router(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.

Configuring an HSRP MAC Refresh Interval

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number*	Configures an interface type and enters interface configuration mode.
	Example:	
	Router(config)# interface GigabitEthernet 0/0/1	
Step 4	**ip address** *ip-address mask* [**secondary**]	Specifies a primary or secondary IP address for an interface.
	Example:	
	Router(config-if)# ip address 10.0.0.1 255.255.255.0	
Step 5	**standby mac-refresh** *seconds*	Changes the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI.
		• This command applies to HSRP running over FDDI only.
	Example:	
	Router(config-if)# standby mac-refresh 100	
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	Activates HSRP.
	Example:	
	Router(config-if)# standby 1 ip 10.0.0.3	

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 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `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* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.

	Command or Action	Purpose
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum**	**reload**	**sync**} *delay*] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption.
Step 7	**standby** [*group-number*] **ip** [*ip-address*] **secondary**] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.
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** **Example:** `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 38 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** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.

Command or Action	Purpose
Step 4 **ip address** *ip-address mask* [**secondary**]	Specifies a primary or secondary IP address for an interface.
Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0	
Step 5 **standby mac-refresh** *seconds*	Configures the HSRP client group refresh interval.
Example: Router(config-if)# standby mac-refresh 30	
Step 6 **standby** *group-number* **follow** *group-name*	Configures an HSRP group as a client group.
Example: Router(config-if)# standby 1 follow HSRP1	
Step 7 **exit**	Exits to global configuration mode.
Example: Router(config-if)# exit	
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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	**standby redirect** [**timers** *advertisement holddown*] [**unknown**] **Example:** Router(config-if)# standby redirect	Enables HSRP filtering of ICMP redirect messages. • 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** **Example:** Router(config-if)# end	Returns to privileged EXEC mode.
Step 6	**show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**] **Example:** 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** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Command or Action	Purpose
Step 3 **interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4 **ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	Configures an IP address for an interface.

Step 5   Enter one of the following commands:
 	
 • **standby** [*group-number*] **mac-address** *mac-address*
 • or
 • **standby use-bia** [**scope interface**]
 	
 • or
 	
 Example:
 	
 `Router(config-if)# standby 1 mac-address 5000.1000.1060`
 	
 Example:
 	
 `Router(config-if)# standby use-bia`
	Specifies a virtual MAC address for HSRP.
	
	 • This command cannot be used on a Token Ring interface.
	
	 or
	
	 Configures HSRP to use the burned-in address of the interface as its virtual MAC address.
	
	 • 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**]] **Example:** `Router(config-if)# standby 1 ip 172.16.6.100`	Activates HSRP.

Linking IP Redundancy Clients to HSRP Groups

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface Ethernet 0/1	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** Router(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies an IP address for an interface.
Step 5	**standby** [*group-number*] **name** [*redundancy-name*] **Example:** Router(config-if)# standby 1 name HSRP-1	Configures the name of the standby group. • HSRP groups have a default name of **hsrp**-*interface-group* so specifying a group name is optional.

Command or Action	Purpose
Step 6 **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.11`	Activates HSRP.

Changing to HSRP Version 2

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

Note

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 will not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same 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** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.

Command or Action	Purpose
Step 2 **configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3 **interface** *type number* **Example:** `Router(config)# interface vlan 400`	Configures an interface type and enters interface configuration mode.

Step 4 **ip address** *ip-address mask*
 	
Example:
`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**} **Example:** `Router(config-if)# standby version 2`	Changes the HSRP version.
Step 6 **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 400 ip 10.10.28.5`	Activates HSRP. • 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** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 8 **show standby** **Example:** `Router# show standby`	(Optional) Displays HSRP information. • 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.

	Command or Action	Purpose
Step 4	**mode sso** **Example:** `Router(config-red)# mode sso`	Enables the redundancy mode of operation to SSO. • HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset.
Step 5	**exit** **Example:** `Router(config-red)# exit`	Exits redundancy configuration mode.
Step 6	**no standby sso** **Example:** `Router(config)# no standby sso`	Disables HSRP SSO mode for all HSRP groups.
Step 7	**standby sso** **Example:** `Router(config)# standby sso`	Enables the SSO HSRP feature if you have disabled the functionality.
Step 8	**end** **Example:** `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** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**snmp-server enable traps hsrp** **Example:** 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** **Example:** 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.

Configuring BFD Session Parameters on the Interface

Perform this task to configure BFD on the interface by setting the baseline BFD session parameters on an interface. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to BFD neighbors.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.
		• Enter your password if prompted.
	Example:	
	Router> enable	
Step 2	**configure terminal**	Enters global configuration mode.
	Example:	
	Router# configure terminal	
Step 3	**interface** *type number*	Enters interface configuration mode.
	Example:	
	Router(config)# interface FastEthernet 6/0	
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*	Enables BFD on the interface.
	Example:	
	Router(config-if)# bfd interval 50 min_rx 50 multiplier 5	
Step 5	**end**	Exits interface configuration mode.
	Example:	
	Router(config-if)# end	

Configuring HSRP BFD Peering

Perform this task to enable HSRP BFD peering. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to HSRP peers.

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

- HSRP must be running on all participating routers.
- Cisco Express Forwarding (CEF) must be enabled.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**ip cef** [**distributed**] **Example:** Router(config)# ip cef	Enables CEF or distributed CEF.
Step 4	**interface** *type number* **Example:** Router(config)# interface FastEthernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 5	**ip address** *ip-address mask* **Example:** Router(config-if)# ip address 10.0.0.11 255.255.255.0	Configures an IP address for the interface.
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** Router(config-if)# standby 1 ip 10.0.0.11	Activates HSRP.
Step 7	**standby bfd** **Example:** Router(config-if)# standby bfd	(Optional) Enables HSRP support for BFD on the interface.
Step 8	**exit** **Example:** Router(config-if)# exit	Exits interface configuration mode.
Step 9	**standby bfd all-interfaces** **Example:** Router(config)# standby bfd all-interfaces	(Optional) Enables HSRP support for BFD on all interfaces.
Step 10	**exit** **Example:** Router(config)# exit	Exits global configuration mode.
Step 11	**show standby** [**neighbors**] **Example:** Router# show standby neighbors	(Optional) Displays information about HSRP support for BFD.

Verifying HSRP BFD Peering

To verify HSRP BFD Peering, use any of the following optional commands.

SUMMARY STEPS

1. **show standby**
2. **show standby neighbors** [*type number*]
3. **show bfd neighborsdetails**

DETAILED STEPS

Step 1 **show standby**
Use the **show standby**command to display HSRP information.

Example:

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

Step 2 **show standby neighbors** [*type number*]
Use the **show standby neighbors** command to display information about HSRP peer routers on an interface.

Example:

```
Router1# show standby neighbors
HSRP neighbors on FastEthernet2/0
    10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !
Router2# show standby neighbors
HSRP neighbors on FastEthernet2/0
    10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

Step 3 **show bfd neighborsdetails**
Use the **show bfd neighbors** command to display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies. The **details** keyword displays BFD protocol parameters and timers for each neighbor.

Example:

```
Router# show bfd neighbors details
OurAddr       NeighAddr     LD/RD  RH/RS  Holdown(mult)  State    Int
10.0.0.2      10.0.0.1      5/0    Down     0   (0 )    Down     Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
```

```
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1          - Diagnostic: 0
             State bit: AdminDown - Demand bit: 0
             Poll bit: 0          - Final bit: 0
             Multiplier: 0        - Length: 0
             My Discr.: 0         - Your Discr.: 0
             Min tx interval: 0   - Min rx interval: 0
             Min Echo interval: 0
```

Configuring HSRP Gratuitous ARP

Perform this task to configure HSRP to check that the entries in the ARP cache are correct and to send periodic gratuitous ARP packets from one or more HSRP active groups. By default, HSRP sends out three gratuitous ARP packets from an HSRP group when the group state changes to Active. HSRP sends the first gratuitous ARP packet when the group becomes active. The second two gratuitous ARP packets are sent 2 and 4 seconds later.

SUMMARY STEPS

1. **enable**
2. **standby send arp** [*interface-type interface-number* [*group-number*]]
3. **configure terminal**
4. **interface** *type number*
5. **standby arp gratuitous** [**count** *number*] [**interval** *seconds*]
6. **end**
7. **show standby arp gratuitous** [*type-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.
	Example:	• Enter your password if prompted.
	Router> enable	
Step 2	**standby send arp** [*interface-type interface-number* [*group-number*]]	(Optional) Configures HSRP to send a single gratuitous ARP packet for each active HSRP group.
	Example:	
	Router# standby send arp Ethernet 1/1 1	

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 4	**interface** *type number* **Example:** Router(config)# interface Ethernet1/1	Configures an interface type and enters interface configuration mode.
Step 5	**standby arp gratuitous** [**count** *number*] [**interval** *seconds*] **Example:** Router(config-if)# standby arp gratuitous count 3 interval 4	Configures the number of gratuitous ARP packets sent by an active HSRP group, and how often they are sent.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Returns to privileged EXEC mode.
Step 7	**show standby arp gratuitous** [*type-number*] **Example:** Router# show standby arp gratuitous ethernet1/1	(Optional) Display the number and configured interval of gratuitous ARP packets sent by HSRP.

Example

The following is sample output from the **show standby arp gratuitous** command:

```
Router# show standby arp gratuitous ethernet 1/1

HSRP Gratuitous ARP
Interface          Interval  Count
Ethernet1/1 4          3
```

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
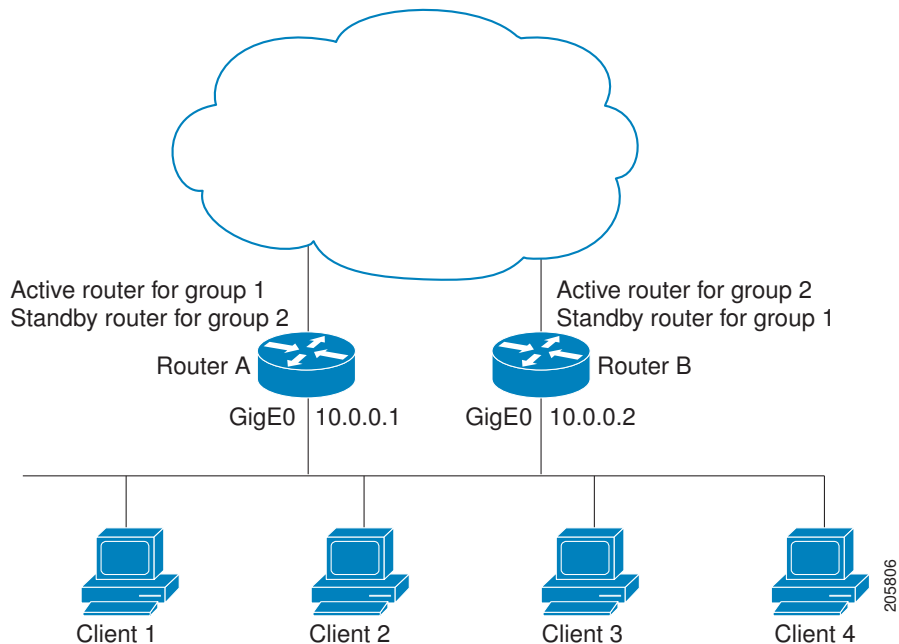```

# 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: Linking IP Redundancy Clients to HSRP Groups

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

Active Router Configuration

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

Standby Router Configuration

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

Example: Configuring HSRP Version 2

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

```
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
```

Example HSRP BFD Peering

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

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

Router A

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

Router B

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

Example: Configuring HSRP Gratuitous ARP

The following example shows how to configure HSRP to check that the entries in the ARP cache are correct and to send three gratuitous ARP packets at 4-second intervals when an HSRP group on the interface changes to active state:

```
Router> enable
Router# standby send arp Ethernet 1/1 1
Router# configure terminal
Router(config)# interface Ethernet 1/1
Router(config-if)# standby arp gratuitous count 3 interval 4
Router(config-if)# end
Router# show standby arp gratuitous ethernet 1/1
HSRP Gratuitous ARP
Interface    Interval    Count
Ethernet1/1 4            3
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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*
HSRP and IPSec	"Hot Standby Routing Protocol and IPSec" section in the "IPSec VPN High Availability Enhancements" module in the *Cisco IOS Security: Secure Connectivity Configuration Guide*
HSRP and IPv6	"Configuring First Hop Redundancy Protocols IPv6" module in the *Cisco IOS IPv6 Configuration Guide*
ISSU	• "Cisco IOS In Service Software Upgrade Process" module of the *Cisco IOS High Availability Configuration Guide* • Configuring the Cisco IOS In Service Software Upgrade Process module of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*, Release 12.2(31)SGA.
Object tracking	"Configuring Enhanced Object Tracking" module
Troubleshooting HSRP	Hot Standby Router Protocol: Frequently Asked Questions

Related Topic	Document Title
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: 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 1　　*Feature Information for HSRP*

Feature Name	Releases	Feature Information
FHRP--HSRP BFD Peering	12.4(11)T	The FHRP--HSRP BFD Peering feature introduces BFD in the HSRP group member health monitoring system. Previously, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory to produce and check. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers sub second health monitoring (failure detection in milliseconds) at a relatively low CPU impact. The following commands were introduced or modified by this feature: **debug standby events neighbor**,**show standby**,**show standby neighbors**,**standby bfd**, **standby bfd all-interfaces**.
FHRP--HSRP Group Shutdown	12.4(9)T 12.2(33)SRC 12.2(33)SXI 15.0(1)S	The FHRP--HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down. The following commands were modified by this feature:**standby track**, **show standby**.
FHRP--HSRP-MIB	12.0(3)T 12.0(12)S	The FHRP--HSRP-MIB feature introduces support for the CISCO-HRSP-MIB.

Feature Name	Releases	Feature Information
FHRP--HSRP Multiple Group Optimization	12.4(6)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S	FHRP--HSRP Multiple Group Optimization feature improves the negotiation and maintenance of multiple HSRP groups configured on a subinterface. Only one HSRP group is required on a physical interface for the purposes of electing active and standby routers. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups. The following commands were introduced or modified by this feature: **standby follow**, **show standby**.
FHRP--HSRP Support for IPv6	12.4(4)T 12.2(33)SRB 12.2(33)SXI	Support for IPv6 was added. For more information see the Configuring First Hop Redundancy Protocols in IPv6 module of the *Cisco IOS IPv6 Configuration Guide.*
HSRP: Global IPv6 Address	12.2(33)SXI4	HSRP Support for Global IPv6 addresses was added. For more information see the Configuring First Hop Redundancy Protocols in IPv6 module of the *Cisco IOS IPv6 Configuration Guide.*

Feature Name	Releases	Feature Information
HSRP Gratuitous ARP	12.2(33)SXI	The HSRP Gratuitous ARP feature configures HSRP to check that the entries in the ARP cache are correct and to send periodic gratuitous ARP packets from one or more HSRP active groups.
		The following commands were introduced by this feature: **show standby arp gratuitous**, **standby arp gratuitous**, **standby send arp**.
		The following commands were modified by this feature: **show standby**, **debug standby events**.
HSRP--ISSU	Cisco IOS XE 3.1.0SG 12.2(31)SGA 12.2(33)SRB1 15.0(1)S	The HSRP--ISSU feature enables support for ISSU in HSRP.
		The In Service Software Upgrade (ISSU) process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.
		For more information about this feature, see the Cisco IOS In Service Software Upgrade Process module in the *Cisco IOS High Availability Configuration Guide*. There are no new or modified commands for this feature.

Feature Name	Releases	Feature Information
HSRP MD5 Authentication	Cisco IOS XE 3.1.0SG 12.3(2)T 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	Prior to the introduction of the HSRP MD5 Authentication feature, HSRP authenticated protocol packets with a simple plain text string. The HSRP MD5 Authentication feature is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This feature provides added security and protects against the threat from HSRP-spoofing software. The following commands were introduced or modified by this feature: **show standby**, **standby authentication**.
HSRP Support for ICMP Redirects	12.1(3)T 15.0(1)S	The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP. The following commands were introduced or modified by this feature: **debug standby event** , **debug standby events icmp**,**show standby**,**standby redirects**
HSRP Support for MPLS VPNs	12.0(23)S, 12.0(17)ST, 12.2(28)SB, 12.2(17b)SXA, 12.2(8)T 15.0(1)S	HSRP support for a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) interface is useful when an Ethernet LAN is connected between two provider edge (PE) routers with either of the following conditions: There are no new or modified commands for this feature.

Feature Name	Releases	Feature Information
HSRP Version 2	Cisco IOS XE 3.1.0SG 12.3(4)T 12.2(25)S 15.0(1)S	HSRP Version 2 feature was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1. The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**.
SSO--HSRP	Cisco IOS XE 3.1.0SG 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	The SSO--HSRP feature alters the behavior of HSRP when a router with redundant RPs is configured for SSO. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails. The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**.

Glossary

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

active 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.

BFD—Bidirectional Forwarding Detection. A detection protocol designed to provide fast forwarding path failure detection encapsulations, topologies, and routing protocols. In addition to fast forwarding, BFD provides a consistent failure detection method for network administrators.

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

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

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

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.