Configuring HSRP

The Hot Standby Router Protocol (HSRP) is a first-hop redundancy protocol (FHRP) designed to allow for transparent fail-over of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet, Fiber Distributed Data Interface (FDDI), Bridge-Group Virtual Interface (BVI), LAN Emulation (LANE), or Token Ring 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.

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Not all features may be supported in your Cisco IOS software release. Use the "Feature Information for HSRP" section on page 47 to find information about feature support and configuration.

Contents

Restrictions for Configuring 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.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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.

Information About HSRP

To configure HSRP, you should understand the following concepts:

HSRP Operation

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

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

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

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

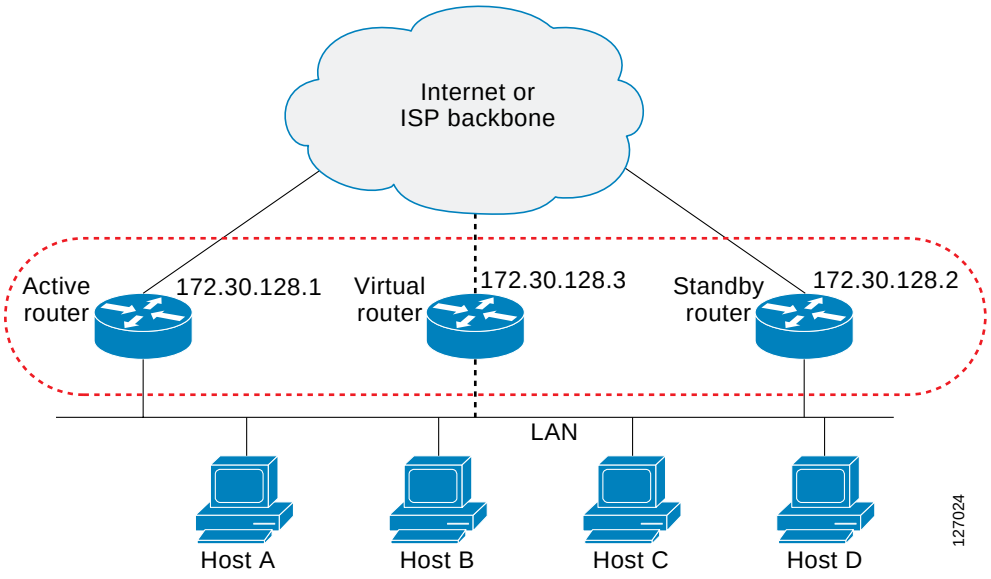
HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure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

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

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

Figure 1 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. Refer to the “Configuring Routing Between VLANs with ISL Encapsulation” chapter in the *Cisco IOS Switching Services Configuration Guide*, Release 12.2.

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 Terminology

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

standby group—The set of routers participating in HSRP that represent a virtual router.

standby router—The primary backup router.

virtual IP address—The IP address assigned to the virtual router that is used as the default gateway by the IP hosts on the LAN.

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.ACxy, where *xy* is the group number in hexadecimal. The functional address is used for Token Ring. The virtual MAC address is different for HSRP version 2.

HSRP Groups and Group Attributes

By using the command-line interface (CLI), group attributes can be applied 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 Addressing

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

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

Token Ring interfaces use functional addresses for the HSRP MAC address. Functional addresses are the only general multicast mechanism available. There are a limited number of Token Ring functional addresses 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 Messages and States

Routers configured with HSRP exchange three types of multicast messages:

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

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

- Active—The router is performing packet-transfer functions.
- Standby—The router is prepared to assume packet-transfer functions if the active router fails.
- Speak—The router is sending and receiving hello messages.
- Listen—The router is receiving hello messages.

HSRP and ARP

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

HSRP Object Tracking

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

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

HSRP Support for MPLS VPNs

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:

- 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/forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding (CEF) table
- Set of interfaces that use the CEF 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 CEF table for each VRF. A separate set of routing and CEF 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.

How to Configure HSRP

This section contains the following procedures:

- Configuring Multiple HSRP Groups for Load Balancing, page 23 (optional)
- Enabling HSRP Support for ICMP Redirects, page 25 (optional)
- Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses, page 29 (optional)
- Linking IP Redundancy Clients to HSRP Groups, page 30 (optional)
- Changing to HSRP Version 2, page 32 (optional)
- Configuring SSO-Aware HSRP (Cisco IOS Release 12.2(25)S), page 34 (optional)
- Enabling HSRP MIB Traps, page 37 (optional)

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.

Prerequisites

You can configure many attributes in HSRP such as authentication, timers, priority, and preemption. It is best practice to configure the attributes first 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 configuration is entered.

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 ethernet 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.
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, it defaults to 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. • The *ip-address* 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 display 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 ethernet 0`	(Optional) Displays HSRP information about specific groups or interfaces.

Delaying the Initialization of HSRP on an Interface

Perform this task to delay 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.

SUMMARY STEPS

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

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 Ethernet0/1`	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 delay minimum** *min-delay* **reload** *reload-delay* **Example:** `Router(config-if)# standby delay minimum 20 reload 25`	(Optional) Configures the delay period before the initialization of HSRP groups. • The *min-delay* 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-delay* 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.

	Command or Action	Purpose
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** [*type number*] **Example:** `Router# show standby delay`	(Optional) Displays HSRP information about delay periods.

Troubleshooting Tips

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

Configuring HSRP Priority and Preemption

Perform this task to configure HSRP priority and preemption.

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.

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 now become the active router if it has the **standby preempt** command configured. See the "Configuring HSRP Object Tracking" section on page 12 for more information on object tracking.

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** *delay* | **reload** *delay* | **sync** *delay*}]
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 Ethernet0/1`	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*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority. • The default priority is 100.

	Command or Action	Purpose
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **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 display 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 ethernet 0/1`	(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.

For more information on object tracking, see the "Configuring Enhanced Object Tracking" configuration module.

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*]
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 serial2/0 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.
Step 5	**interface** *type number* **Example:** `Router(config)# interface ethernet 2`	Configures an interface type and enters interface configuration mode.
Step 6	**standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] **Example:** `Router(config-if)# standby 1 track 100 decrement 20`	Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object. • 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. • 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.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.10.10.0`	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.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**]| **resolution** | **timers**] **Example:** `Router# show track 100 interface`	Displays tracking information.

Configuring HSRP Authentication

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

The following sections describe configuration tasks for HSRP authentication. The task you perform depends on whether you want to use text authentication, a simple MD5 key string, or MD5 key chains for authentication.

- Configuring HSRP MD5 Authentication Using a Key String, page 15
- Configuring HSRP MD5 Authentication Using a Key Chain, page 17
- Troubleshooting HSRP MD5 Authentication, page 19
- Configuring HSRP Text Authentication, page 20

How HSRP MD5 Authentication Works

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.

Benefits of HSRP MD5 Authentication

- Protects against HSRP-spoofing software
- Uses the industry-standard MD5 algorithm for improved reliability and security

Restrictions

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.

Configuring HSRP MD5 Authentication Using a Key String

Perform this task to configure HSRP MD5 authentication using a key string.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
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	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	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet0/1`	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.
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** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption.
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 and it is 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.	—

	Command	Purpose
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.

Troubleshooting Tips

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 holdtime period, specified by the **standby timers** interface configuration command, after the non-active routers. This procedure ensures that the non-active routers do not time out the active router.

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. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **standby** [*group-number*] **priority** *priority*
10. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
11. **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*
12. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
13. Repeat Steps 1 through 12 on each router that will communicate.
14. **end**
15. **show standby**

DETAILED STEPS

	Command	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 and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 100`	Identifies an authentication key on a key chain. • The *key-id* 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 *string* can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface Ethernet0/1`	Configures an interface type and enters interface configuration mode.
Step 8	**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 9	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 10	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption.

	Command	Purpose
Step 11	**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 12	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.21.8.12`	Activates HSRP.
Step 13	Repeat Steps 1 through 12 on each router that will communicate.	—
Step 14	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 15	**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	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. • See the "Examples" section for an example of the type of error messages displayed when two routers are not authenticating.

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

Perform this task to configure 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** *delay* | **reload** *delay* | **sync** *delay*}]
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	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet0/1`	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.
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** *delay* | **reload** *delay* | **sync** *delay*}] **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 sanjose`	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.

Customizing HSRP

Perform this task to customize HSRP parameters.

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 or switches. HSRP hello packets use the burned-in address (BIA) instead of the MAC virtual address. Refresh packets keep the MAC cache on switches and learning bridges current.

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).

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 mac-refresh** *seconds*
7. **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 Ethernet0/1`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
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*] **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 router to be down. • Normally, the *holdtime* value is greater than or equal to three times the value of *hellotime*. • See the "HSRP Timers" concept in this section for more information.
Step 6	**standby mac-refresh** *seconds* **Example:** `Router(config-if)# standby mac-refresh 100`	Changes the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI. • This command applies to HSRP running over FDDI only.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.

Troubleshooting Tips

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used on Cisco 7200 platforms or better, and on Fast-Ethernet or FDDI interfaces or better. You can use the **standby delay** command to allow the interface to come up completely before HSRP initializes.

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. While a router is actively forwarding traffic for one HSRP group, it 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 "Multiple HSRP for Load Balancing: Example" section on page 41 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** *delay* | **reload** *delay* | **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 to configure HSRP 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 Ethernet0/1`	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.
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** *delay* | **reload** *delay* | **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.

	Command or Action	Purpose
Step 8	On the same router, repeat Steps 5 through 7 to configure the router attributes for different standby groups.	For example, Router A can be configured as an active router for group 1 and be configured for 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.

Enabling HSRP Support for ICMP Redirects

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.

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 running HSRP, it is important to prevent hosts from discovering the interface (or real) IP addresses of routers in the HSRP group. 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

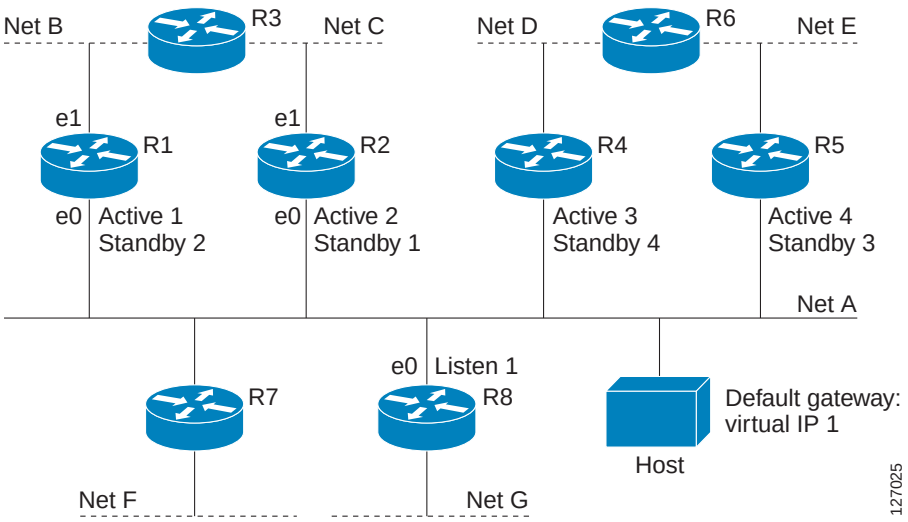
The next-hop IP address is compared to the list of active HSRP routers on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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 Figure 2, 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

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

In Figure 2, 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

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 Figure 2, 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:

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

You can adjust the advertisement interval and holddown 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 only support 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 then it is not possible to uniquely determine the gateway IP address of the host 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: SB: ICMP redirect not sent to 20.0.0.4 for dest 30.0.0.2
10:43:08: SB: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

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 Ethernet0/1`	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.

	Command or Action	Purpose
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

Perform this task to configure an HSRP virtual MAC address or a burned-in address (BIA) MAC address.

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, it is often necessary to be able to specify the virtual MAC address by using the **standby mac-address** command; 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 BIA 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).

Restrictions

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 breaks 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. **standby** [*group-number*] **mac-address** *mac-address*
   or
   standby use-bia [**scope interface**]
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 Ethernet0/1`	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	**standby** [*group-number*] **mac-address** *mac-address*
	or
	standby use-bia [**scope interface**]
	
	Example:
	`Router(config-if)# standby 1 mac-address 5000.1000.1060`
	or
	
	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

Perform this task to link IP redundancy clients to HSRP groups.

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.

Prerequisites

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 Ethernet0/1`	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.

	Command or Action	Purpose
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 so it is not a requirement to specify a name.
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.

HSRP Version 2 Design

HSRP version 2 is designed to address the following issues relative to HSRP version 1:

- Previously, 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.
- 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, there is no method to identify from HSRP active hello messages 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, which is used by 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 issues relative to HSRP version 1 that HSRP version 2 does. See the *Configuring GLBP* configuration module for more information on GLBP.

Restrictions

- 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.
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.

	Command or Action	Purpose
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 expanded to 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.

Configuring SSO-Aware HSRP (Cisco IOS Release 12.2(25)S)

This section contains the following tasks:

- Enabling SSO Aware HSRP, page 35 (required)
- Verifying SSO Aware HSRP, page 36 (optional)

SSO-aware 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

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

SSO-aware 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).

Enabling SSO Aware HSRP

The functionality 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-aware 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.

	Command or Action	Purpose
Step 3	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 4	**mode sso** **Example:** `Router(config-red)# mode sso`	Enables the redundancy mode of operation to SSO. • After performing this step, 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-aware 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:

```
Router# show standby

Ethernet0/0/1 - Group 1
 State is Init (standby RP, peer state is Active)
 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
 IP redundancy 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:

```
Router# debug standby events ha

!Active RP

*Apr 27 04:13:47.755: HSRP: Et0/0/1 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: Et0/0/1 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: Et0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Et0/0/1 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: Et0/0/1 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: Et0/0/1 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: Et0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Et0/0/1 Grp 101 RF sync state Standby -> Active
```

Enabling 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.

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# snmp-server host myhost.comp.com public hsrp`	Specifies the recipient of an SNMP notification operation, and that HSRP notifications be sent to the host.

Configuration Examples for HSRP

This section provides the following configuration examples:

HSRP Priority and Preemption: Example

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

```
interface Ethernet0/0
 ip address 10.1.0.21 255.255.0.0
 standby 1 priority 110
 standby 1 preempt
 standby 1 ip 10.1.0.1
 standby 2 priority 95
 standby 2 preempt
 standby 2 ip 10.1.0.2
```

Router B Configuration

```
interface Ethernet0/0
 ip address 10.1.0.22 255.255.0.0
 standby 1 preempt
 standby 1 priority 105
 standby 1 ip 10.1.0.1
 standby 2 priority 110
 standby 2 preempt
 standby 2 ip 10.1.0.2
```

HSRP Object Tracking: Example

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Ethernet interface 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

```
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
 ip address 10.1.0.21 255.255.0.0
 standby 1 preempt
 standby 1 priority 110
 standby 1 track 100 decrement 10
 standby 1 ip 10.1.0.1
```

Router B Configuration

```
track 100 interface serial1/0 ip routing
!
```

```
interface Ethernet0/0
 ip address 10.1.0.22 255.255.0.0
 standby 1 preempt
 standby 1 priority 105
 standby 1 track 100 decrement 10
 standby 1 ip 10.1.0.1
```

HSRP MD5 Authentication Using Key Strings: Example

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

```
interface Ethernet0/1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 54321098452103ab timeout 30
 standby 1 ip 10.21.0.10
```

HSRP MD5 Authentication Using Key Chains: Example

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

```
key chain hsrp1
 key 1
  key-string 54321098452103ab

interface Ethernet0/1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-chain hsrp1
 standby 1 ip 10.21.0.10
```

HSRP MD5 Authentication Using Key Strings and Key Chains: Example

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

```
key chain hsrp1
 key 0
  key-string 54321098452103ab

interface Ethernet0/1
 standby 1 authentication md5 key-chain hsrp1
 standby 1 ip 10.21.0.10
```

Router 2

```
interface Ethernet0/1
 standby 1 authentication md5 key-string 54321098452103ab
 standby 1 ip 10.21.0.10
```

HSRP Text Authentication: Example

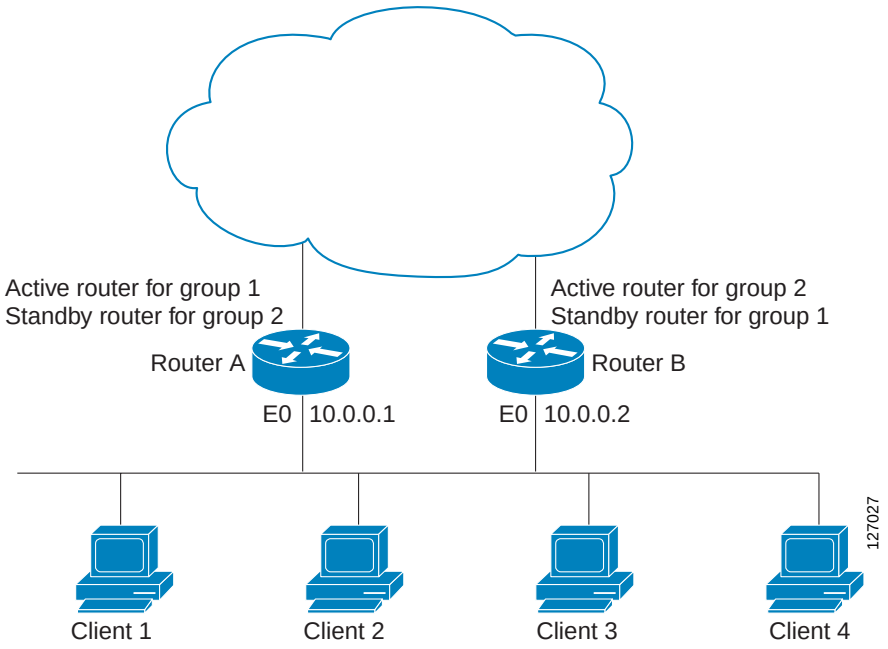
The following example shows how to configure HSRP text authentication using a text string:

```
interface Ethernet0/1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication text company2
 standby 1 ip 10.21.0.10
```

Multiple HSRP for Load Balancing: Example

You can use HSRP or multiple HSRP groups when you configure load sharing. In Figure 3, 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 3 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

```
hostname RouterA
!
interface ethernet 0
  ip address 10.0.0.1 255.255.255.0
  standby 1 priority 110
  standby 1 preempt
  standby 1 ip 10.0.0.3
  standby 2 preempt
  standby 2 ip 10.0.0.4
```

Router B Configuration

```
hostname RouterB
!
interface ethernet 0
  ip address 10.0.0.2 255.255.255.0
  standby 1 preempt
  standby 1 ip 10.0.0.3
  standby 2 priority 110
  standby 2 preempt
  standby 2 ip 10.0.0.4
```

HSRP Support for ICMP Redirect Messages: Example

The following is a configuration example for two HSRP groups that allow the filtering of ICMP redirect messages:

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

```
interface Ethernet1
  ip address 10.0.0.10 255.0.0.0
  standby redirect
  standby 1 priority 120
  standby 1 preempt delay minimum 20
  standby 1 ip 10.0.0.1
  standby 2 priority 105
  standby 2 preempt delay minimum 20
  standby 2 ip 10.0.0.2
```

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

```
interface Ethernet1
  ip address 10.0.0.11 255.0.0.0
  standby redirect
  standby 1 priority 105
  standby 1 preempt delay minimum 20
  standby 1 ip 10.0.0.1
  standby 2 priority 120
  standby 2 preempt delay minimum 20
  standby 2 ip 10.0.0.2
```

HSRP Virtual MAC Addresses and BIA MAC Address: Example

In an 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:

```
interface Ethernet0/2
 ip address 10.0.0.1
 standby 1 mac-address 4000.1000.1060
 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:

```
interface token3/0
 standby use-bia
```

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

Linking IP Redundancy Clients to HSRP Groups: Example

The following example shows HSRP support for a static 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 “sanjose.”

Active Router Configuration

```
interface BVI10
 ip address 192.168.5.54 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 ip 192.168.5.30
 standby 10 priority 110
 standby 10 preempt
 standby 10 name sanjose
 standby 10 track Ethernet2/1
!
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 10.10.10.5 redundancy sanjose
 ip classless
 ip route 10.10.10.0 255.255.255.0 Ethernet2/1
 ip route 172.22.33.0 255.255.255.0 Ethernet2/1
 no ip http server
```

Standby Router Configuration

```
interface BVI10
 ip address 192.168.5.56 255.255.255.255.0
 no ip redirects
 ip nat inside
 standby 10 priority 95
 standby 10 preempt
 standby 10 name sanjose
 standby 10 ip 192.168.5.30
 standby 10 track Ethernet3/1
!
 ip default-gateway 10.0.18.126
 ip nat inside source static 192.168.5.33 3.3.3.5 redundancy sanjose
 ip classless
 ip route 10.0.32.231 255.255.255 Ethernet3/1
 ip route 10.10.10.0 255.255.255.0 Ethernet3/1
 no ip http server
```

HSRP Version 2: Example

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

```
!
interface vlan350
 standby version 2
 standby 350 priority 110
 standby 350 preempt
 standby 350 timers 5 15
 standby 350 ip 172.20.100.10
```

SSO-Aware HSRP (Cisco IOS Release 12.2(25)S): Example

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

```
redundancy
 mode sso
```

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

```
interface Ethernet1
 ip address 10.1.1.1 255.255.0.0
 standby priority 200
 standby preempt
 standby sso
```

HSRP MIB Traps: Example

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. This is realized by configuring it at a higher priority level and enabling 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

```
interface Ethernet1
 ip address 10.1.1.1 255.255.0.0
 standby priority 200
 standby preempt
 standby ip 10.1.1.3
snmp-server enable traps hsrp
snmp-server host yourhost.cisco.com public hsrp
```

Router B

```
interface Ethernet1
 ip address 10.1.1.2 255.255.0.0
 standby priority 101
 standby ip 10.1.1.3
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com public hsrp
```

Additional References

The following sections provide references related to HSRP.

Related Documents

Related Topic	Document Title
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*, Release 12.4
Key chains and key management commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols*, Release 12.4
Object tracking	"Configuring Enhanced Object Tracking" module
VRRP	"Configuring VRRP" module
GLBP	"Configuring GLBP" module
Troubleshooting HSRP	*Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks* document.

Standards

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

MIBs

MIBs	MIBs Link
No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1828	*IP Authentication Using Keyed MD5*
RFC 2281	*Cisco Hot Standby Router Protocol*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Glossary

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

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

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.

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

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

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

RPR+—An enhanced Route Processor Redundancy (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.

Note Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for HSRP

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.2(25)S or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the "FHRP Features Roadmap".

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Table 1 Feature Information for HSRP

Feature Name	Releases	Feature Configuration Information
HSRP MD5 Authentication	12.3(2)T 12.2(25)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 sections provide information about this feature: • Configuring HSRP Authentication, page 14 The following commands were introduced or modified by this feature: **show standby**, **standby authentication**.

Table 1 Feature Information for HSRP (continued)

Feature Name	Releases	Feature Configuration Information
HSRP Version 2	12.3(4)T 12.2(25)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 sections provide information about this feature: • Changing to HSRP Version 2, page 32 The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**
FHRP - SSO-Aware HSRP	12.2(25)S	SSO-aware HSRP 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 sections provide information about this feature: • Configuring SSO-Aware HSRP (Cisco IOS Release 12.2(25)S), page 34 The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**

This module first published May 2, 2005. Last updated May 2, 2005.