



Configuring HSRP

This chapter describes how to configure the Hot Standby Router Protocol (HSRP) on the Cisco NX-OS switch.

This chapter includes the following sections:

- [Information About HSRP, page 16-1](#)
- [Licensing Requirements for HSRP, page 16-8](#)
- [Prerequisites for HSRP, page 16-8](#)
- [Guidelines and Limitations, page 16-8](#)
- [Default Settings, page 16-9](#)
- [Configuring HSRP, page 16-10](#)
- [Enabling DHCP Relay Agent Using VIP, page 16-19](#)
- [Configuration Examples for HSRP, page 16-20](#)
- [Additional References, page 16-21](#)

Information About HSRP

HSRP is a first-hop redundancy protocol (FHRP) that allows a transparent failover of the first-hop IP router. HSRP provides first-hop routing redundancy for IP hosts on Ethernet networks configured with a default router IP address. You use HSRP in a group of routers for selecting an active router and a standby router. In a group of routers, the active router is the router that routes packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

Many host implementations do not support any dynamic router discovery mechanisms but can be configured with a default router. Running a dynamic router discovery mechanism on every host is not feasible for a number of reasons, including administrative overhead, processing overhead, and security issues. HSRP provides failover services to these hosts.

This section includes the following topics:

- [HSRP Overview, page 16-2](#)
- [HSRP for IPv4, page 16-3](#)
- [.HSRP for IPv6, page 16-4](#)
- [HSRP Versions, page 16-5](#)
- [HSRP Authentication, page 16-5](#)

- [HSRP Messages, page 16-5](#)
- [HSRP Load Sharing, page 16-6](#)
- [BFD, page 16-7](#)
- [vPC and HSRP, page 16-7](#)
- [Virtualization Support, page 16-7](#)

HSRP Overview

When you use HSRP, you configure the HSRP virtual IP address as the host's default router (instead of the IP address of the actual router). The virtual IP address is an IPv4 or IPv6 address that is shared among a group of routers that run HSRP.

When you configure HSRP on a network segment, you provide a virtual MAC address and a virtual IP address for the HSRP group. You configure the same virtual address on each HSRP-enabled interface in the group. You also configure a unique IP address and MAC address on each interface that acts as the real address. HSRP selects one of these interfaces to be the active router. The active router receives and routes packets destined for the virtual MAC address of the group.

HSRP detects when the designated active router fails. At that point, a selected standby router assumes control of the virtual MAC and IP addresses of the HSRP group. HSRP also selects a new standby router at that time.

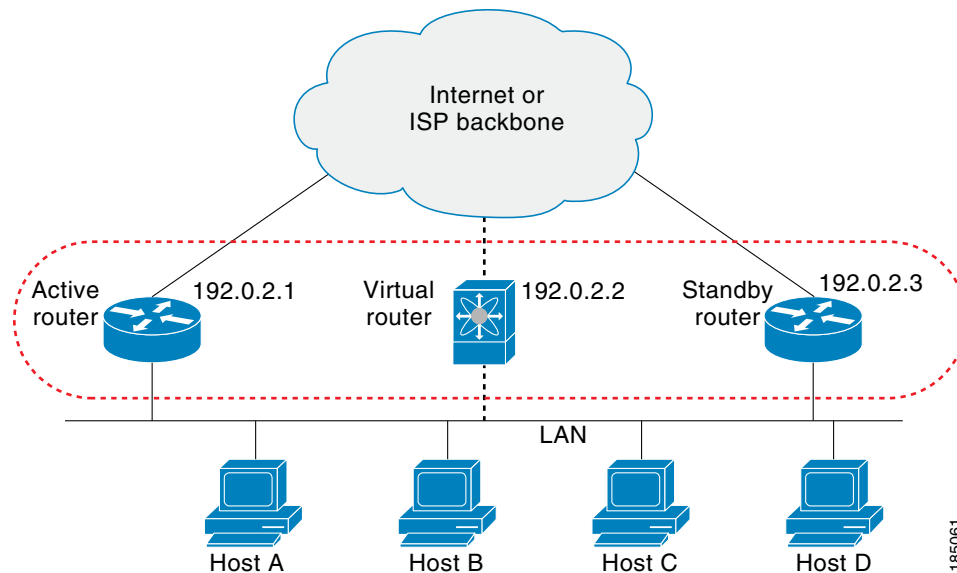
HSRP uses a priority mechanism to determine which HSRP-configured interface becomes the default active router. To configure an interface as the active router, you assign it with a priority that is higher than the priority of all the other HSRP-configured interfaces in the group. The default priority is 100, so if you configure just one interface with a higher priority, that interface becomes the default active router.

Interfaces that run HSRP send and receive multicast User Datagram Protocol (UDP)-based hello messages to detect a 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 the active and standby router is completely transparent to all hosts on the network.

You can configure multiple HSRP groups on an interface.

[Figure 16-1](#) shows a network configured for HSRP. By sharing a virtual MAC address and a virtual IP address, two or more interfaces can act as a single virtual router.

Figure 16-1 HSRP Topology with Two Enabled Routers



The virtual router does not physically exist but represents the common default router for interfaces 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 router. If the active router fails to send a hello message within the configurable period of time, the standby router takes over, responds to the virtual addresses, and becomes the active router, assuming the active router duties. From the host perspective, the virtual router remains the same.



Note

Packets received on a routed port destined for the HSRP virtual IP address will terminate on the local router, regardless of whether that router is the active HSRP router or the standby HSRP router. This includes ping and Telnet traffic. Packets received on a Layer 2 (VLAN) interface destined for the HSRP virtual IP address will terminate on the active router.

HSRP for IPv4

HSRP routers communicate with 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 address (BIA). The BIA is the last six bytes of the MAC address that is assigned by the manufacturer of the network interface card (NIC).

Because hosts are configured with their default router as the HSRP virtual IP address, hosts must communicate with the MAC address associated with the HSRP virtual IP address. This MAC address is a virtual MAC address, 0000.0C07.ACxy, where xy is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group 1 uses the HSRP virtual MAC address of 0000.0C07.AC01. Hosts on the adjoining LAN segment use the normal Address Resolution Protocol (ARP) process to resolve the associated MAC addresses.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, which is used by version 1. HSRP version 2 permits an expanded group number range of 0 to 4095 and uses a new MAC address range of 0000.0C9F.F000 to 0000.0C9F.FFFF.

.HSRP for IPv6

IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery (ND) router advertisement (RA) messages. These messages are multicast periodically, or be solicited by hosts, but the time delay for detecting when a default route is down be 30 seconds or more. HSRP for IPv6 provides a much faster switchover to an alternate default router than the IPv6 ND protocol provides, less than a second if the milliseconds timers are used. HSRP for IPv6 provides a virtual first hop for IPv6 hosts.

When you configure an IPv6 interface for HSRP, the periodic RAs for the interface link-local address stop after IPv6 ND sends a final RA with a router lifetime of zero. No restrictions occur for the interface IPv6 link-local address. Other protocols continue to receive and send packets to this address.

IPv6 ND sends periodic RAs for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent with a router lifetime of 0 when the HSRP group leaves the active state. HSRP uses the virtual MAC address for active HSRP group messages only (hello, coup, and redesign).

HSRP for IPv6 uses the following parameters:

- HSRP version 2
- UDP port 2029
- Virtual MAC address range from 0005.73A0.0000 through 0005.73A0.0FFF
- Multicast link-local IP destination address of FF02::66
- Hop limit set to 255

HSRP IPv6 Addresses

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 derived, by default, from the HSRP virtual MAC address. The default virtual MAC address for an HSRP IPv6 group always used to form the virtual IPv6 link-local address, regardless of the actual virtual MAC address used by the group.

[Table 16-1](#) shows the MAC and IP addresses used for IPv6 neighbor discovery packets and HSRP packets.

Table 16-1 HSRP and IPv6 ND Addresses

Packet	MAC Source Address	IPv6 Source Address	IPv6 Destination Address	Link-layer Address Option
Neighbor solicitation (NS)	Interface MAC address	Interface IPv6 address	—	Interface MAC address
Router solicitation (RS)	Interface MAC address	Interface IPv6 address	—	Interface MAC address
Neighbor advertisement (NA)	Interface MAC address	Interface IPv6 address	Virtual IPv6 address	HSRP virtual MAC address
Route advertisement (RA)	Interface MAC address	Virtual IPv6 address	—	HSRP virtual MAC address
HSRP (inactive)	Interface MAC address	Interface IPv6 address	—	—
HSRP (active)	Virtual MAC address	Interface IPv6 address	—	—

HSRP does not add IPv6 link-local addresses to the Unicast Routing Information Base (URIB). There are also no secondary virtual IP addresses for link-local addresses.

For global unicast addresses, HSRP adds the virtual IPv6 address to the URIB and IPv6 but does not register the virtual IPv6 addresses to ICMPv6. ICMPv6 redirects are not supported for HSRP IPv6 groups.

HSRP Versions

Cisco NX-OS supports HSRP version 1 by default. You can configure an interface to use HSRP version 2.

HSRP version 2 has the following enhancements to HSRP version 1:

- Expands the group number range. HSRP version 1 supports group numbers from 0 to 255. HSRP version 2 supports group numbers from 0 to 4095.
- For IPv4, uses the IPv4 multicast address 224.0.0.102 or the IPv6 multicast address FF02::66 to send hello packets instead of the multicast address of 224.0.0.2, which is used by HSRP version 1.
- Uses the MAC address range from 0000.0C9F.F000 to 0000.0C9F.FFFF for IPv4 and 0005.73A0.0000 through 0005.73A0.0FFF for IPv6 addresses. HSRP version 1 uses the MAC address range 0000.0C07.AC00 to 0000.0C07.ACFE.
- Adds support for MD5 authentication.

When you change the HSRP version, Cisco NX-OS reinitializes the group 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 are ignored.

HSRP 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 includes the IPv4 or IPv6 address in the authentication TLVs .

HSRP Messages

Routers that are configured with HSRP exchange the following three types of multicast messages:

- Hello—The hello message conveys the HSRP priority and state information of the router to other HSRP routers.
- 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.

HSRP Load Sharing

HSRP allows you to configure multiple groups on an interface. You can configure two overlapping IPv4 HSRP groups to load share traffic from the connected hosts while providing the default router redundancy expected from HSRP. Figure 16-2 shows an example of a load-sharing HSRP IPv4 configuration.

Figure 16-2 HSRP Load Sharing

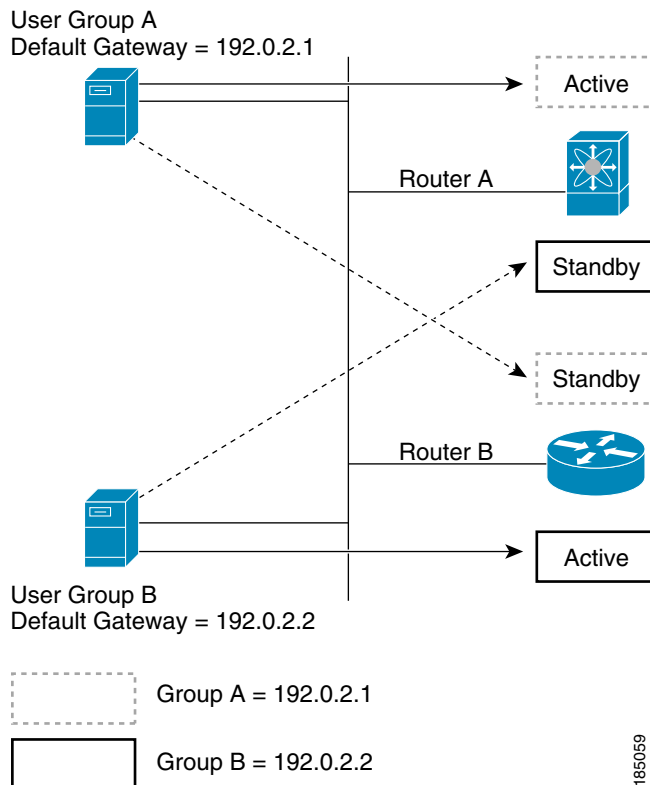


Figure 16-2 shows two routers (A and B) and two HSRP groups. Router A is the active router for group A but is the standby router for group B. Similarly, router B is the active router for group B and the standby router for group A. If both routers remain active, HSRP load balances the traffic from the hosts across both routers. If either router fails, the remaining router continues to process traffic for both hosts.



Note

HSRP for IPv6 load balances by default. If there are two HSRP IPv6 groups on the subnet, hosts learn of both from their router advertisements and choose to use one so that the load is shared between the advertised routers.

BFD

HSRP supports bidirectional forwarding detection (BFD). BFD is a detection protocol that provides fast forwarding-path failure detection times. BFD provides subsecond failure detection between two adjacent devices and can be less CPU-intensive than protocol hello messages because some of the BFD load can be distributed onto the data plane on supported modules. See the *Cisco Nexus 5500 Series NX-OS Interfaces Configuration Guide, Release 6.0* for more information.

vPC and HSRP

HSRP interoperates with virtual port channels (vPCs). vPCs allow links that are physically connected to two different Cisco Nexus 5500 switches to appear as a single port channel by a third switch. See the *Cisco Nexus 5500 Series NX-OS Layer 2 Switching Configuration Guide, Release 6.0*, for more information on vPCs.

vPC forwards traffic through both the active HSRP router and the standby HSRP router. You can configure a threshold on the priority of the standby HSRP router to determine when traffic should fail over to the vPC trunk. See the [“Configuring the HSRP Priority” section on page 16-17](#).

**Note**

You should configure HSRP on the primary vPC peer switch as active and HSRP on the vPC secondary switch as standby.

vPC Peer Gateway and HSRP

Some third-party devices can ignore the HSRP virtual MAC address and instead use the source MAC address of an HSRP router. In a vPC environment, the packets using this source MAC address may be sent across the vPC peer link, causing a potential dropped packet. Configure the vPC peer gateway to enable the HSRP routers to directly handle packets sent to the local vPC peer MAC address and the remote vPC peer MAC address, as well as the HSRP virtual MAC address. See the *Cisco Nexus 5500 Series NX-OS Layer 2 Switching Configuration Guide, Release 6.0*, for more information on the vPC peer gateway.

**Note**

For mixed-chassis configurations where the vPC peer link is configured on an F-series module, configure the vPC peer gateway exclude option to exclude the Layer 3 backup route that traverses the vPC peer link. See the *Cisco Nexus 5500 Series NX-OS Layer 2 Switching Configuration Guide, Release 6.0*, for more information on the vPC peer gateway exclude option.

Virtualization Support

HSRP supports Virtual Routing and Forwarding instances (VRFs).

If you change the VRF membership of an interface, Cisco NX-OS removes all Layer 3 configuration, including HSRP.

VIP HSRP Enhancement

Starting with Cisco NX-OS Release 7.2(0)N1(1), the vIP HSRP enhancement provides support for an HSRP VIP configuration to be in a different subnet than that of the interface subnet. This feature is applicable only for IPv4 and not for IPv6. The following are the enhancements:

- Enhance ARP to source with VIP from SUP for hosts when hosts in VIP subnet are referenced by static route to VLAN configuration.
- Support periodic ARP synchronization to VPC peer if this feature enabled
- Allow use of the VIP address as L3 source address and gateway address for all communications with DHCP server.
- Enhance DHCP relay agent to relay DHCP packets with source as VIP instead of SVI IP when the feature is enabled.

Licensing Requirements for HSRP

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	<p>HSRP requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i>.</p> <p>Note Make sure the Layer 3 Hardware and LAN Base Services licenses that are included with the hardware are installed on the switch to enable Layer 3 interfaces.</p>

Prerequisites for HSRP

HSRP has the following prerequisites:

- You must enable the HSRP feature in a switch before you can configure and enable any HSRP groups.

Guidelines and Limitations

HSRP has the following configuration guidelines and limitations:

- The minimum hello timer value is 250 milliseconds.
- The minimum hold timer value is 750 milliseconds.
- You must configure an IP address for the interface that you configure HSRP on and enable that interface before HSRP becomes active.
- You must configure HSRP version 2 when you configure an IPv6 interface for HSRP.
- For IPv4, the virtual IP address must be in the same subnet as the interface IP address.

- We recommend that you do not configure more than one first-hop redundancy protocol on the same interface. HSRP version 2 does 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).
- Cisco NX-OS removes all Layer 3 configuration on an interface when you change the interface VRF membership, port channel membership, or when you change the port mode to Layer 2.
- If you configure virtual MAC addresses with a virtual port channel (vPC), you must configure the same virtual MAC address on both vPC peers.
- You cannot use the HSRP MAC address burned-in option on a VLAN interface that is a vPC member.
- If you have not configured authentication, the **show hsrp** command displays the following string: Authentication text "cisco".
- This is the default behavior of HSRP as defined in RFC 2281: If no authentication data is configured, the RECOMMENDED default value is 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.
- If you add a third Nexus 5000 router to an HSRP group, which already contains two routers of the same type, then the third one can only be configured as a listener.
- On the Cisco Nexus 5500 Series switches, in a vPC topology with HSRP, partial FabricPath configuration on vPC peers is not supported. Partial FabricPath configuration means that when the FabricPath feature is enabled, but the FabricPath mode is not configured for the Multichassis EtherChannel Trunk (MCT) and Switch Virtual Interface (SVI) VLANs. With Partial FabricPath configuration, ping to the virtual IP address will fail.

The VIP HSRP enhancement has the following guidelines and limitations:

- This feature will work only for HSRP in combination with VPC topologies. In scenarios where HSRP standby is not a VPC pair, this feature will not work, as there will not be periodic adjacency sync support for non-VPC cases.
- This feature is applicable only for IPv4 and not for IPv6.
- Support for this feature is only for Regular HSRP and not for Anycast HSRP, so this feature will not work if Anycast HSRP is enabled.
- SUP generated IP traffic (for example, ping/traceroute/ICMP Error packets) destined for VIP subnets originated from the HSRP Active/Standby box will continue to source with IPv4 SVI interface IP and not the vIP. If you want to explicitly source using the loopback IP for ping/traceroute, you can specify the loopback IP along with the source keyword.
- Static ARP configuration for creating entries in VIP subnets is not supported.
- DHCP relay agent will always use primary VIP address to communicate with DHCP server. DHCP relay agent does not consider use of secondary VIP addresses as long as primary VIP is available
- DHCP relay agent behavior in case inter-vrf is different and requires use of Option-82 information in DHCP packets. DHCP server and clients will be in the same VRF and use of VIP is not supported for inter-vrf relay.

Default Settings

Table 16-2 lists the default settings for HSRP parameters.

Table 16-2 Default HSRP Parameters

Parameters	Default
HSRP	Disabled
Authentication	Enabled as text for version 1, with cisco as the password
HSRP version	Version 1
Preemption	disabled
Priority	100
virtual MAC address	Derived from HSRP group number

Configuring HSRP

This section includes the following topics:

- [Enabling the HSRP Feature, page 16-10](#)
- [Configuring the HSRP Version, page 16-11](#)
- [Configuring an HSRP Group for IPv4, page 16-11](#)
- [Configuring an HSRP Group for IPv6, page 16-13](#)
- [Configuring the HSRP Virtual MAC Address, page 16-15](#)
- [Authenticating HSRP, page 16-15](#)
`switch(config-if-hsrp)# copy running-config startup-config`, page 16-17
- [Configuring the HSRP Priority, page 16-17](#)
- [Customizing HSRP, page 16-18](#)



Note

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling the HSRP Feature

You must globally enable the HSRP feature before you can configure and enable any HSRP groups. **DETAILED STEPS**

To enable the HSRP feature, use the following command in global configuration mode:

Command	Purpose
<code>feature hsrp</code>	Enables HSRP.
Example: <code>switch(config)# feature hsrp</code>	

To disable the HSRP feature and remove all associated configuration, use the following command in global configuration mode:

Configuring the HSRP Version

Command	Purpose
no feature hsrp Example: switch(config)# no feature hsrp	Disables HSRP for all groups.

You can configure the HSRP version. If you change the version for existing groups, Cisco NX-OS reinitializes HSRP for those groups because the virtual MAC address changes. The HSRP version applies to all groups on the interface.



Note

IPv6 HSRP groups must be configured as HSRP version 2.

To configure the HSRP version, use the following command in interface configuration mode:

Command	Purpose
hsrp version {1 2} Example: switch(config-if)# hsrp version 2	Configures the HSRP version. Version 1 is the default.

Configuring an HSRP Group for IPv4

You can configure an HSRP group on an IPv4 interface and configure the virtual IP address and virtual MAC address for the HSRP group.

BEFORE YOU BEGIN

Ensure that you have enabled the HSRP feature (see the [“Enabling the HSRP Feature”](#) section on page 16-10).

Cisco NX-OS enables an HSRP group once you configure the virtual IP address on any member interface in the group. You should configure HSRP attributes such as authentication, timers, and priority before you enable the HSRP group.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip** *ip-address/length*
5. **hsrp group-number** [ipv4]
6. **ip** [*ip-address* [secondary]]
7. **exit**
8. **no shutdown**

9. (Optional) **show hsrp** [group *group-number*] [ipv4]
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>type number</i> Example: switch(config)# interface ethernet 1/2 switch(config-if)#	Enters interface configuration mode.
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	ip <i>ip-address/length</i> Example: switch(config-if)# ip 192.0.2.2/8	Configures the IPv4 address of the interface.
Step 5	hsrp <i>group-number</i> [ipv4] Example: switch(config-if)# hsrp 2 switch(config-if-hsrp)#	Creates an HSRP group and enters hsrp configuration mode. The range for HSRP version 1 is from 0 to 255. The range is for HSRP version 2 is from 0 to 4095. The default value is 0.
Step 6	ip [<i>ip-address</i> [secondary]] Example: switch(config-if-hsrp)# ip 192.0.2.1	Configures the virtual IP address for the HSRP group and enables the group. This address should be in the same subnet as the IPv4 address of the interface.
Step 7	exit Example: switch(config-if-hsrp)# exit	Exits HSRP configuration mode.
Step 8	no shutdown Example: switch(config-if)# no shutdown	Enables the interface.
Step 9	show hsrp [group <i>group-number</i>] [ipv4] Example: switch(config-if)# show hsrp group 2	(Optional) Displays HSRP information.
Step 10	copy running-config startup-config Example: switch(config-if)# copy running-config startup-config	(Optional) Saves this configuration change.



Note

You should use the **no shutdown** command to enable the interface after you finish the configuration.

This example shows how to configure an HSRP group on Ethernet 1/2:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# ip 192.0.2.2/8
switch(config-if)# hsrp 2
switch(config-if-hsrp)# ip 192.0.2.1
switch(config-if-hsrp)# exit
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

Configuring an HSRP Group for IPv6

You can configure an HSRP group on an IPv6 interface and configure the virtual MAC address for the HSRP group.

When you configure an HSRP group for IPv6, HSRP generates a link-local address from the link-local prefix. HSRP also generates a modified EUI-64 format interface identifier in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

There are no HSRP IPv6 secondary addresses.

BEFORE YOU BEGIN

Ensure that you have enabled the HSRP feature (see the [“Enabling the HSRP Feature”](#) section on page 16-10).

Ensure that you have enabled HSRP version 2 on the interface that you want to configure an IPv6 HSRP group on.

Ensure that you have configured HSRP attributes such as authentication, timers, and priority before you enable the HSRP group.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **ipv6** *ipv6-address/length*
4. **hsrp version 2**
5. **hsrp group-number** *ipv6*
6. **ip** *ipv6-address* [**secondary**]
7. **ip autoconfig**
8. **no shutdown**
9. **show hsrp** [**group** *group-number*] [**ipv6**]
10. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface type number Example: switch(config)# interface ethernet 3/2 switch(config-if)#	Enters interface configuration mode.
Step 3	ipv6 ipv6-address/length Example: switch(config-if)# ipv6 2001:0DB8:0001:0001:/64	Configures the IPv6 address of the interface.
Step 4	hsrp version 2 Example: switch(config-if-hsrp)# hsrp version 2	Configures this group for HSRP version 2.
Step 5	hsrp group-number ipv6 Example: switch(config-if)# hsrp 10 ipv6 switch(config-if-hsrp)#	Creates an IPv6 HSRP group and enters hsrp configuration mode. The range for HSRP version 2 is from 0 to 4095. The default value is 0.
Step 6	ip [ipv6-address [secondary]] Example: switch(config-if-hsrp)# ip 2001:DB8::1	Configures the virtual IPv6 address for the HSRP group and enables the group.
Step 7	ip autoconfig Example: switch(config-if-hsrp)# ip autoconfig	Autoconfigures the virtual IPv6 address for the HSRP group from the calculated link-local virtual IPv6 address and enables the group.
Step 8	no shutdown Example: switch(config-if-hsrp)# no shutdown	Enables the interface.
Step 9	show hsrp [group group-number] [ipv6] Example: switch(config-if-hsrp)# show hsrp group 10	(Optional) Displays HSRP information.
Step 10	copy running-config startup-config Example: switch(config-if-hsrp)# copy running-config startup-config	(Optional) Saves this configuration change.

**Note**

You should use the **no shutdown** command to enable the interface after you finish the configuration.

The following example shows how to configure an IPv6 HSRP group on Ethernet 3/2:

```
switch# configure terminal
switch(config)# interface ethernet 3/2
switch(config-if)# ip 12001:0DB8:0001:0001:/64
switch(config-if)# hsrp 2 ipv6
switch(config-if-hsrp)# exit
switch(config-if)# no shutdown
switch(config-if)# copy running-config startup-config
```

Configuring the HSRP Virtual MAC Address

You can override the default virtual MAC address that HSRP derives from the configured group number.



Note

You must configure the same virtual MAC address on both vPC peers of a vPC link.

To manually configure the virtual MAC address for an HSRP group, use the following command in hsrp configuration mode:

Command	Purpose
mac-address <i>string</i> Example: switch(config-if-hsrp)# mac-address 5000.1000.1060	Configures the virtual MAC address for an HSRP group. The string uses the standard MAC address format (xxxx.xxxx.xxxx).

To configure HSRP to use the burned-in MAC address of the interface for the virtual MAC address, use the following command in interface configuration mode:

Command	Purpose
hsrp use-bia [<i>scope interface</i>] Example: switch(config-if)# hsrp use-bia	Configures HSRP to use the burned-in MAC address of the interface for the HSRP virtual MAC address. You can optionally configure HSRP to use the burned-in MAC address for all groups on this interface by using the scope interface keyword.

Authenticating HSRP

You can configure HSRP to authenticate the protocol using cleartext or MD5 digest authentication. MD5 authentication uses a key chain (see the *Cisco Nexus 5500 Series NX-OS Security Configuration Guide, Release 6.0*).

BEFORE YOU BEGIN

Ensure that you have enabled the HSRP feature (see the [“Enabling the HSRP Feature”](#) section on page 16-10).

You must configure the same authentication and keys on all members of the HSRP group.

Ensure that you have created the key chain if you are using MD5 authentication.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **hsrp group-number** [ipv4 | ipv6]
5. **authentication text** *string*
or
authentication md5 {**key-chain** *key-chain* | **key-string** {0 | 7} *text* [**timeout** *seconds*]}
6. (Optional) **show hsrp** [**group** *group-number*]
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 1/2 switch(config-if)#	Enters interface configuration mode. Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	hsrp group-number [ipv4 ipv6] Example: switch(config-if)# hsrp 2 switch(config-if-hsrp)#	Creates an HSRP group and enters HSRP configuration mode.
Step 5	authentication text <i>string</i> Example: switch(config-if-hsrp)# authentication text mypassword	Configures cleartext authentication for HSRP on this interface.
	authentication md5 { key-chain <i>key-chain</i> key-string {0 7} <i>text</i> [timeout <i>seconds</i>]}	Configures MD5 authentication for HSRP on this interface. You can use a key chain or key string. If you use a key string, you can optionally set the timeout for when HSRP will only accept a new key. The range is from 0 to 32767 seconds.
	Example: switch(config-if-hsrp)# authentication md5 key-chain hsrp-keys	

	Command	Purpose
Step 6	show hsrp [<i>group group-number</i>] Example: switch(config-if-hsrp)# show hsrp group 2	(Optional) Displays HSRP information.
Step 7	copy running-config startup-config Example: switch(config-if-hsrp)# copy running-config startup-config	(Optional) Saves this configuration change.

This example shows how to configure MD5 authentication for HSRP on Ethernet 1/2 after creating the key chain:

```
switch# configure terminal
switch(config)# key chain hsrp-keys
switch(config-keychain)# key 0
switch(config-keychain-key)# key-string 7 zqdest
switch(config-keychain-key) accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
switch(config-keychain-key) key 1
switch(config-keychain-key) key-string 7 uaeqdyito
switch(config-keychain-key) accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
switch(config-keychain-key) send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
switch(config-keychain-key)# interface ethernet 1/2
switch(config-if)# no switchport
switch(config-if)# hsrp 2
switch(config-if-hsrp)# authenticate md5 key-chain hsrp-keys
switch(config-if-hsrp)# copy running-config startup-config
```

Configuring the HSRP Priority

You can configure the HSRP priority on an interface. HSRP uses the priority to determine which HSRP group member acts as the active router. If you configure HSRP on a vPC-enabled interface, you can optionally configure the upper and lower threshold values to control when to fail over to the vPC trunk. If the standby router priority falls below the lower threshold, HSRP sends all standby router traffic across the vPC trunk to forward through the active HSRP router. HSRP maintains this scenario until the standby HSRP router priority increases above the upper threshold.

For IPv6 HSRP groups, if all group members have the same priority, HSRP selects the active router based on the IPv6 link-local address.

To configure the HSRP priority, use the following command in interface configuration mode:

Command	Purpose
priority <i>level</i> [forwarding-threshold <i>lower lower-value</i> upper <i>upper-value</i>] Example: switch(config-if-hsrp)# priority 60 forwarding-threshold lower 40 upper 50	Sets the priority level used to select the active router in an HSRP group. The <i>level</i> range is from 0 to 255. The default is 100. Optionally, sets the upper and lower threshold values used by vPC to determine when to fail over to the vPC trunk. The <i>lower-value</i> range is from 1 to 255. The default is 1. The <i>upper-value</i> range is from 1 to 255. The default is 255.

Customizing HSRP

You can optionally customize the behavior of HSRP. Be aware that as soon as you enable an HSRP group by configuring a virtual IP address, that group is now operational. If you first enable an HSRP group before customizing HSRP, the router could take control over the group and become the active router before you finish customizing the feature. If you plan to customize HSRP, you should do so before you enable the HSRP group.

Command	Purpose
<p>name <i>string</i></p> <p>Example: switch(config-if-hsrp)# name HSRP-1</p>	<p>Specifies the IP redundancy name for an HSRP group. The <i>string</i> is from 1 to 255 characters. The default string has the following format:</p> <p>hsrp-<interface-short-name>-<group-id>. For example, hsrp-Eth2/1-1.</p>
<p>preempt [delay [<i>minimum seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]]</p> <p>Example: switch(config-if-hsrp)# preempt delay minimum 60</p>	<p>Configures the router to take over as an active router for an HSRP group if it has a higher priority than the current active router. This command is disabled by default. The range is from 0 to 3600 seconds.</p>
<p>timers [msec] <i>hellotime</i> [msec] <i>holdtime</i></p> <p>Example: switch(config-if-hsrp)# timers 5 18</p>	<p>Configures the hello and hold time for this HSRP member as follows:</p> <ul style="list-style-type: none"> • <i>hellotime</i>—The interval between successive hello packets sent. The range is from 1 to 254 seconds. • <i>holdtime</i>—The interval before the information in the hello packet is considered invalid. The range is from 3 to 255. <p>The optional msec keyword specifies that the argument is expressed in milliseconds, instead of the default seconds. The timer ranges for milliseconds are as follows:</p> <ul style="list-style-type: none"> • <i>hellotime</i>—The interval between successive hello packets sent. The range is from 255 to 999 milliseconds. • <i>holdtime</i>—The interval before the information in the hello packet is considered invalid. The range is from 750 to 3000 milliseconds.

To customize HSRP, use the following commands in interface configuration mode:

Command or Action	Purpose
hsrp delay minimum <i>seconds</i> Example: switch(config-if)# hsrp delay minimum 30	Specifies the minimum amount of time that HSRP waits after a group is enabled before participating in the group. The range is from 0 to 10000 seconds. The default is 0.
hsrp delay reload <i>seconds</i> Example: switch(config-if)# hsrp delay reload 30	Specifies the minimum amount of time that HSRP waits after reload before participating in the group. The range is from 0 to 10000 seconds. The default is 0.

Enabling DHCP Relay Agent Using VIP

Command	Purpose
configure terminal Example: switch(config)# configure terminal	Enters global configuration mode.
[no] ip dhcp relay source-address hsrp Example: switch(config)# [no] ip dhcp relay source-address hsrp	Enables/disables DHCP relay agent to use VIP globally.
interface <i>type number</i> Example: switch(config)# interface vlan 500	Enters interface configuration mode.
[no] ip dhcp relay source-address hsrp Example: switch(config-if)# [no] ip dhcp relay source-address hsrp	Enables/Disables DHCP relay agent to use VIP at L3 interface level.



Note

You can use the **show ip dhcp relay** command to verify the DHCP relay agent configuration.

Verifying the HSRP Configuration

To display the HSRP configuration information, perform one of the following tasks:

Command	Purpose
<code>show hsrp [group group-number]</code>	Displays the HSRP status for all groups or one group.
<code>show hsrp delay [interface interface-type slot/port]</code>	Displays the HSRP delay value for all interfaces or one interface. Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
<code>show hsrp [interface interface-type slot/port]</code>	Displays the HSRP status for an interface. Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
<code>show hsrp [group group-number] [interface interface-type slot/port] [active] [all] [init] [learn] [listen] [speak] [standby]</code>	Displays the HSRP status for a group or interface for virtual forwarders in the active, init, learn, listen, or standby state. Use the all keyword to see all states, including disabled. Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
<code>show hsrp [group group-number] [interface interface-type slot/port] active] [all] [init] [learn] [listen] [speak] [standby] brief</code>	Displays a brief summary of the HSRP status for a group or interface for virtual forwarders in the active, init, learn, listen, or standby state. Use the all keyword to see all states, including disabled. Note If this is a QSFP+ GEM, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .

Configuration Examples for HSRP

This example shows how to enable HSRP on an interface with MD5 authentication and interface tracking:

```
key chain hsrp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
    send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
    send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
feature hsrp
track 2 interface ethernet 2/2 ip
interface ethernet 1/2
  no switchport
  ip address 192.0.2.2/8
  hsrp 1
    authenticate md5 key-chain hsrp-keys
    priority 90
    track 2 decrement 20
```

```
ip-address 192.0.2.10
no shutdown
```

This example shows how to enable DHCP relay agent using VIP address:

```
interface vlan 500
ip address 5.5.5.5/24
ip dhcp relay source-address hsrp
ip dhcp relay address 100.100.100.100
hsrp 10
ip 17.17.17.17/28
ip 15.15.15.20/28 secondary
```

Additional References

For additional information related to implementing HSRP, see the following sections:

- [Related Documents, page 16-21](#)

Related Documents

Related Topic	Document Title
Configuring the Virtual Router Redundancy Protocol	Chapter 18, “Configuring VRRP”
HSRP CLI commands	<i>Cisco Nexus 5000 Series Command Reference, Cisco NX-OS Releases 4.x, 5.x</i>

