About HSRP

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

Restrictions for HSRP

- For supporting HSRP, ASIC should be able to receive packets destined with below IPv4 VMAC.

  HSRP is supported on this MAC address: **00:00:0C:07:xx**

- HSRP version 2 is not supported on the NCS520 router.
- HSRP and VRRP are both supported on Bridge Domain Interfaces (BDI) only.
- Timer supported values for the HSRP are: 0.3 seconds for Hello Interval and 1 second for Dead Interval.

Information about HSRP

HSRP Operation

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

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

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

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

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

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

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

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

HSRP Benefits

- Redundancy:

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

- Fast Failover:

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

- Preemption:

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

- Authentication:

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

HSRP Groups and Group Attributes

You can use the CLI to apply group attributes to:

- A single HSRP group—performed in interface configuration mode and applies to a group.

- All groups on the interface—performed in interface configuration mode and applies to all groups on the interface.
- All groups on all interfaces—performed in global configuration mode and applies to all groups on all interfaces.

HSRP Preemption

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

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

In general, we recommend that all HSRP devices have the following configuration: **standby delay minimum 30 reload 60**

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

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

HSRP Priority and Preemption

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

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

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

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

How Object Tracking Affects the Priority of an HSRP Device

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

HSRP Addressing

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

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

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

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

HSRP Virtual MAC Addresses and BIA MAC Addresses

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

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

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

HSRP MAC Address

ASIC will be able to receive packets with the IPV4 Virtual MAC address

HSRP is supported on this MAC address: **00:00:0C:07:xx**

HSRP MAC Refresh Interval

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

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

HSRP Text Authentication

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

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

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

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

HSRP MD5 Authentication

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

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

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

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

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

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

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

How to Configure HSRP

To configure HSRP on the Cisco NCS 520 router, use the following commands:

Configuring HSRP

```
interface GigabitEthernet0/1
  service instance 1 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100

int bdi 100
  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 1 authentication text auth_1

interface GigabitEthernet0/1
  service instance 1 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100
int bdi 100
  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 1 authentication text auth_1
```

Displaying HSRP Information

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**show standby brief all**
	Example:
	`Router# show standby brief all`
	`P indicates configured to preempt.`
	`|`
	`Interface Grp Pri P State Active Standby Virtual IP`
	`BD101 1 190 P Standby 100.100.1.2 local 100.100.1.10`
	`BD101 2 200 P Active local`	

	Command or Action	Purpose
	100.100.1.2 100.100.1.20 Router#	
Step 3	**show standby** **Example:** BDI101 - Group 1 State is Standby 4 state changes, last state change 00:04:24 Virtual IP address is 100.100.1.10 Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac01 (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.616 secs Authentication text, string "auth" Preemption enabled Active router is 100.100.1.2, priority 200 (expires in 9.472 sec) Standby router is local Priority 190 (configured 190) Group name is "hsrp-BD101-1" (default) FLAGS: 0/1 BDI101 - Group 2 State is Active 2 state changes, last state change 00:04:55 Virtual IP address is 100.100.1.20 Active virtual MAC address is 0000.0c07.ac02 (MAC In Use) Local virtual MAC address is 0000.0c07.ac02 (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.256 secs Authentication text, string "auth1" Preemption enabled Active router is local Standby router is 100.100.1.2, priority 190 (expires in 8.960 sec) Priority 200 (configured 200) Group name is "hsrp-BD101-2" (default) FLAGS: 1/1 Router#	
Step 4	**exit** **Example:** Router# end	Returns to privileged EXEC mode.