HSRP Support for ICMP Redirects

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About HSRP Support for ICMP Redirects

HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of Internet Control Message Protocol (ICMP) redirect messages is enabled on devices running HSRP.

ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP can send error packets to a host and can send redirect packets to a host.

When HSRP is running, preventing hosts from discovering the interface (or real) IP addresses of devices in the HSRP group is important. If a host is redirected by ICMP to the real IP address of a device, and that device 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 Devices

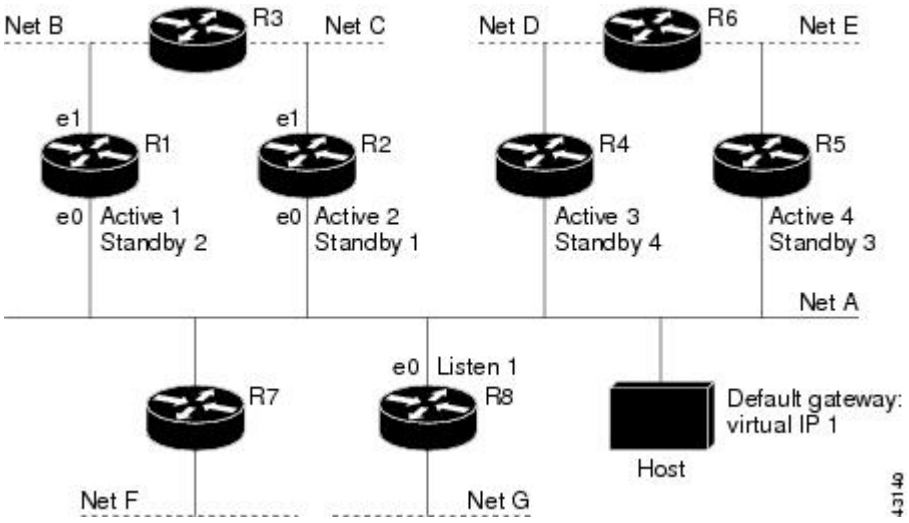
The next-hop IP address is compared to the list of active HSRP devices on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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

For optimal operation, every device in a network that is running HSRP should contain at least one active HSRP group on an interface to that network. Every HSRP device need not be a member of the same group. Each HSRP device will snoop on all HSRP packets on the network to maintain a list of active devices (virtual IP addresses versus real IP addresses).

Consider the network shown in the figure below, which supports the HSRP ICMP redirection filter.

Figure 1: 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
```

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

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

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

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

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

ICMP Redirects to Non-HSRP Devices

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

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device 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 Advertisement Messages

Passive HSRP devices send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP devices can determine the HSRP group state of any HSRP device on the

network. These advertisements inform other HSRP devices on the network of the HSRP interface state, as follows:

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

You can adjust the advertisement interval and hold-down time using the **standby redirect timers** command.

ICMP Redirects Not Sent

If the HSRP device 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 device 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 device 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.

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 device uses the destination MAC address to determine the gateway IP address of the host. If the HSRP device is using the same MAC address for multiple IP addresses, uniquely determining the gateway IP address of the host is not possible, and the redirect message is not sent.

The following is sample output from the **debug standby events icmp** EXEC command if HSRP could not uniquely determine the gateway used by the host:

```
10:43:08: HSRP: ICMP redirect not sent to 10.0.0.4 for dest 10.0.1.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

How to Configure HSRP Support for ICMP Redirects

Enabling HSRP Support for ICMP Redirect Messages

By default, HSRP filtering of ICMP redirect messages is enabled on devices running HSRP. Perform this task to reenable this feature on your device if it is disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby redirect** [**timers** *advertisement holddown*] [**unknown**]
5. **end**
6. **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**standby redirect** [**timers** *advertisement holddown*] [**unknown**] **Example:** `Device(config-if)# standby redirect`	Enables HSRP filtering of ICMP redirect messages. • You can also use this command in global configuration mode, which enables HSRP filtering of ICMP redirect messages on all interfaces configured for HSRP.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**] **Example:** `Device# show standby redirect`	(Optional) Displays ICMP redirect information on interfaces configured with HSRP.

Configuration Examples for HSRP Support for ICMP Redirects

Example: Configuring HSRP Support for ICMP Redirect Messages

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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.10 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.11 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 120
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS First Hop redundancy Protocols Command Reference*
HSRP for IPv6	“HSRP for IPv6” module
Troubleshooting HSRP	Hot Standby Router Protocol: Frequently Asked Questions

Standards

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

MIBs

MIBs	MIBs Link
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 792	*Internet Control Message Protocol*
RFC 1828	*IP Authentication Using Keyed MD5*
RFC 2281	*Cisco Hot Standby Router Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for HSRP Support for ICMP Redirects

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for HSRP Support for ICMP Redirects

Feature Name	Releases	Feature Information
HSRP Support for ICMP Redirects	12.1(3)T 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP. The following commands were introduced or modified by this feature: **debug standby event** , **debug standby events icmp**,**show standby**,**standby redirects**