



IP Configuration Guide, Cisco IOS XE Fuji 16.9.x (Catalyst 9200 Switches)

First Published: 2018-07-31

Last Modified: 2019-03-17

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Configuring HSRP 1

Configuring HSRP 1

Finding Feature Information 1

Information About Configuring HSRP 1

HSRP Overview 1

HSRP Versions 3

Multiple HSRP 4

HSRP and Switch Stacks 4

Configuring HSRP for IPv6 4

How to Configure HSRP 5

Default HSRP Configuration 5

HSRP Configuration Guidelines 5

Enabling HSRP 6

Configuring HSRP Priority 7

Configuring MHSRP 9

Configuring HSRP Authentication and Timers 16

Enabling HSRP Support for ICMP Redirect Messages 17

Configuring HSRP Groups and Clustering 17

Verifying HSRP 18

Verifying HSRP Configurations 18

Configuration Examples for Configuring HSRP 18

Enabling HSRP: Example 18

Configuring HSRP Priority: Example 19

Configuring MHSRP: Example 19

Configuring HSRP Authentication and Timer: Example 19

Configuring HSRP Groups and Clustering: Example 20

Additional References for Configuring HSRP	20
Feature Information for Configuring HSRP	21

CHAPTER 2**VRRPv3 Protocol Support 23**

VRRPv3 Protocol Support	23
Restrictions for VRRPv3 Protocol Support	23
Information About VRRPv3 Protocol Support	24
VRRPv3 Benefits	24
VRRP Device Priority and Preemption	25
VRRP Advertisements	26
How to Configure VRRPv3 Protocol Support	26
Creating and Customizing a VRRP Group	26
Configuring the Delay Period Before FHRP Client Initialization	28
Configuration Examples for VRRPv3 Protocol Support	29
Example: Enabling VRRPv3 on a Device	29
Example: Creating and Customizing a VRRP Group	29
Example: Configuring the Delay Period Before FHRP Client Initialization	30
Example: VRRP Status, Configuration, and Statistics Details	30
Additional References	31
Feature Information for VRRPv3 Protocol Support	31
Glossary	32

CHAPTER 3**Configuring Enhanced Object Tracking 33**

Finding Feature Information	33
Information About Enhanced Object Tracking	33
Enhanced Object Tracking Overview	33
Tracking Interface Line-Protocol or IP Routing State	34
Tracked Lists	34
Tracking Other Characteristics	34
IP SLAs Object Tracking	35
Static Route Object Tracking	35
How to Configure Enhanced Object Tracking	35
Configuring Tracking for Line State Protocol or IP Routing State on an Interface	35
Configuring Tracked Lists	36

Configuring a Tracked List with a Weight Threshold	36
Configuring a Tracked List with a Percentage Threshold	38
Configuring HSRP Object Tracking	39
Configuring IP SLAs Object Tracking	41
Configuring Static Route Object Tracking	42
Configuring a Primary Interface for Static Routing	42
Configuring a Primary Interface for DHCP	43
Configuring IP SLAs Monitoring Agent	44
Configuring a Routing Policy and a Default Route	45
Monitoring Enhanced Object Tracking	46
Additional References	47
Feature Information for Enhanced Object Tracking	47

CHAPTER 4
Configuring TCP MSS Adjustment 49

Restrictions for TCP MSS Adjustment	49
Information about TCP MSS Adjustment	49
Configuring the MSS Value for Transient TCP SYN Packets	50
Configuring the MSS Value for IPv6 Traffic	51
Example: Configuring the TCP MSS Adjustment for IPv6 traffic	51
Feature History for TCP MSS Adjustment	51

CHAPTER 5
Enhanced IPv6 Neighbor Discovery Cache Management 53

Enhanced IPv6 Neighbor Discovery Cache Management	53
Customizing the Parameters for IPv6 Neighbor Discovery	54
Examples: Customizing Parameters for IPv6 Neighbor Discovery	55
Additional References	55
Feature Information for IPv6 Neighbor Discovery	55



CHAPTER 1

Configuring HSRP

- [Configuring HSRP](#) , on page 1

Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) to provide routing redundancy for routing IP traffic without being dependent on the availability of any single router.

You can also use a version of HSRP in Layer 2 mode to configure a redundant command switch to take over cluster management if the cluster command switch fails.

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 at the end of this module.

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

Information About Configuring HSRP

HSRP Overview

HSRP is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.



Note Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and switch virtual interfaces (SVIs).

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. 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 the routing duties when an active router fails or when preset conditions are met.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group's MAC address. For n routers running HSRP, there are $n + 1$ IP and MAC addresses assigned.

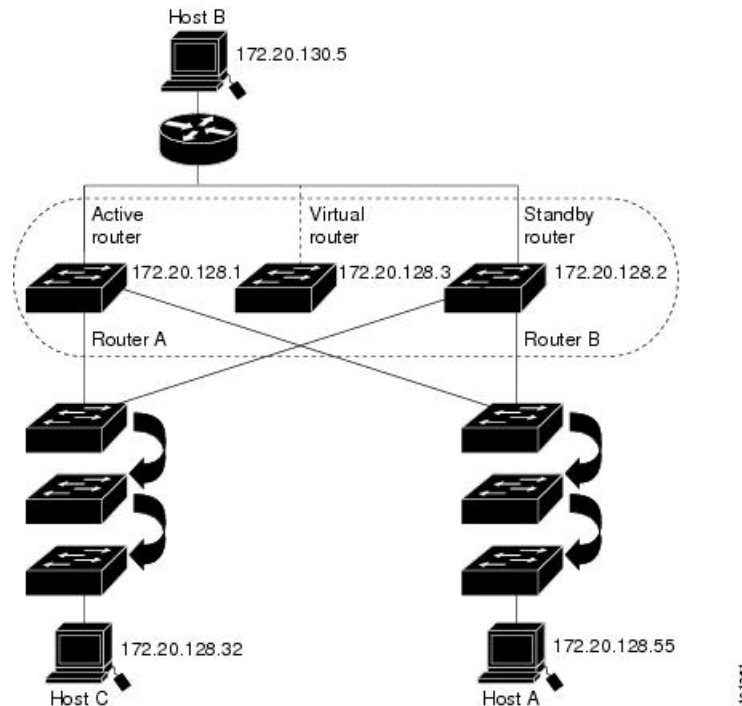
HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group's MAC and IP addresses. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

You can configure multiple Hot Standby groups among switches and switch stacks that are operating in Layer 3 to make more use of the redundant routers.

To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

The following figure shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C's segment that need to communicate with users on Host B's segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.

Figure 1: Typical HSRP Configuration



HSRP Versions

Cisco IOS XE Fuji 16.9.x and later support these Hot Standby Router Protocol (HSRP) versions:

The switch supports these HSRP versions:

- HSRPv1- Version 1 of the HSRP, the default version of HSRP. It has these features:
 - The HSRP group number can be from 0 to 255.
 - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.
- HSRPv2- Version 2 of the HSRP has these features:
 - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.
 - HSRPv2 has a different packet format than HSRPv1.

A switch running HSRPv1 cannot identify the physical router that sent a hello packet because the source MAC address of the router is the virtual MAC address.

HSRPv2 has a different packet format than HSRPv1. A HSRPv2 packet uses the type-length-value (TLV) format and has a 6-byte identifier field with the MAC address of the physical router that sent the packet.

If an interface running HSRPv1 gets an HSRPv2 packet, the type field is ignored.

Multiple HSRP

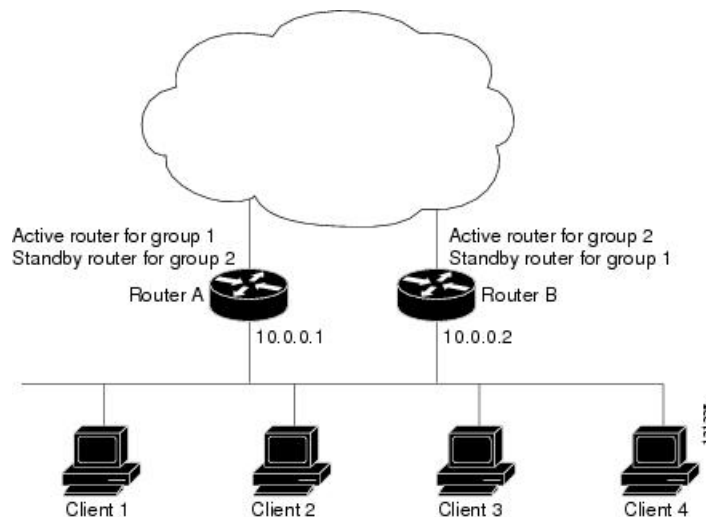
The switch supports Multiple HSRP (MHSRP), an extension of HSRP that allows load sharing between two or more HSRP groups. You can configure MHSRP to achieve load-balancing and to use two or more standby groups (and paths) from a host network to a server network.

In the figure below, half the clients are configured for Router A, and half the clients are configured for Router B. Together, the configuration for Routers A and B establishes two HSRP 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.



Note For MHSRP, you need to enter the **standby preempt** interface configuration command on the HSRP interfaces so that if a router fails and then comes back up, preemption restores load sharing.

Figure 2: MHSRP Load Sharing



HSRP and Switch Stacks

HSRP hello messages are generated by the active switch. If HSRP fails on the active switch, a flap in the HSRP active state might occur. This is because HSRP hello messages are not generated while a new active switch is elected and initialized, and the standby switch might become active after the active switch fails.

Configuring HSRP for IPv6

Switches running the support the Hot Standby Router Protocol (HSRP) for IPv6. HSRP provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router. IPv6 hosts learn of available routers through IPv6 neighbor discovery router advertisement messages. These messages are multicast periodically or are solicited by hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address.

Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These messages stop after a final one is sent when the group leaves the active state.



Note When configuring HSRP for IPv6, you must enable HSRP version 2 (HSRPv2) on the interface.

How to Configure HSRP

Default HSRP Configuration

Table 1: Default HSRP Configuration

Feature	Default Setting
HSRP version	Version 1
HSRP groups	None configured
Standby group number	0
Standby MAC address	System assigned as: 0000.0c07.acXX, where XX is the HSRP group number
Standby priority	100
Standby delay	0 (no delay)
Standby track interface priority	10
Standby hello time	3 seconds
Standby holdtime	10 seconds

HSRP Configuration Guidelines

- HSRPv2 and HSRPv1 are mutually exclusive. HSRPv2 is not interoperable with HSRPv1 on an interface and the reverse.
- In the procedures, the specified interface must be one of these Layer 3 interfaces:
 - Routed port: A physical port configured as a Layer 3 port by entering the **no switchport** command in interface configuration mode.
 - SVI: A VLAN interface created by using the **interface vlan** *vlan_id* in global configuration mode, and by default a Layer 3 interface.
 - Etherchannel port channel in Layer 3 mode: A port-channel logical interface created by using the **interface port-channel** *port-channel-number* in global configuration mode, and binding the Ethernet interface into the channel group.
- All Layer 3 interfaces must have IP addresses assigned to them.



Note HSRP millisecond timers are not supported.

Enabling 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 designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.

When the **standby ip** command is enabled on an interface and proxy ARP is enabled, if the interface's Hot Standby state is active, proxy ARP requests are answered using the Hot Standby group MAC address. If the interface is in a different state, proxy ARP responses are suppressed.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>Switch(config)# configure terminal</code>	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: <code>Switch(config)# interface gigabitethernet1/0/1</code>	Enters interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.
Step 3	standby version { 1 2 } Example: <code>Switch(config-if)# standby version 1</code>	(Optional) Configures the HSRP version on the interface. <ul style="list-style-type: none"> • 1- Selects HSRPv1. • 2- Selects HSRPv2. <p>If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1.</p>
Step 4	standby [<i>group-number</i>] ip [<i>ip-address</i> [<i>secondary</i>]] Example: <code>Switch(config-if)# standby 1 ip</code>	Creates (or enable) the HSRP group using its number and virtual IP address. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) <i>ip-address</i>- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one

	Command or Action	Purpose
		<p>of the interfaces; it can be learned on the other interfaces.</p> <ul style="list-style-type: none"> • (Optional) secondary- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 5	<p>end</p> <p>Example:</p> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode
Step 6	<p>show standby [<i>interface-id</i> [<i>group</i>]]</p> <p>Example:</p> <pre>Switch # show standby</pre>	Verifies the configuration of the standby groups.
Step 7	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring HSRP Priority

The **standby priority**, **standby preempt**, and **standby track** interface configuration commands are all used to set characteristics for finding active and standby routers and behavior regarding when a new active router takes over.

When configuring HSRP priority, follow these guidelines:

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.
- The highest number (1 to 255) represents the highest priority (most likely to become the active router).
- When setting the priority, preempt, or both, you must specify at least one keyword (**priority**, **preempt**, or both)
- The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.
- The **standby track** interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked

- The **standby track interface-priority** interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.
- When multiple tracked interfaces are down and *interface-priority* values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.
- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP priority characteristics on an interface:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Switch # configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Switch(config)# interface gigabitethernet1/0/1	Enters interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	standby [group-number] prioritypriority Example: Switch(config-if)# standby 120 priority 50	Sets a priority value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. <ul style="list-style-type: none"> • (Optional) group-number—The group number to which the command applies. <p>Use the no form of the command to restore the default values.</p>
Step 4	standby [group-number] preempt [delay [minimumseconds] [reloadseconds] [syncseconds]] Example: Switch(config-if)# standby 1 preempt delay 300	Configures the router to preempt , which means that when the local router has a higher priority than the active router, it becomes the active router. <ul style="list-style-type: none"> • (Optional) group-number—The group number to which the command applies. • (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of

	Command or Action	Purpose
		<p>seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload).</p> <ul style="list-style-type: none"> (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). <p>Use the no form of the command to restore the default values.</p>
Step 5	<p>standby [<i>group-number</i>] track <i>type number</i> [<i>interface-priority</i>]</p> <p>Example:</p> <pre>Switch(config-if)# standby track interface gigabitethernet1/1/1</pre>	<p>Configures an interface to track other interfaces so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered.</p> <ul style="list-style-type: none"> (Optional) <i>group-number</i>- The group number to which the command applies. <i>type</i>- Enter the interface type (combined with interface number) that is tracked. <i>number</i>- Enter the interface number (combined with interface type) that is tracked. (Optional) <i>interface-priority</i>- Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.
Step 6	<p>end</p> <p>Example:</p> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 7	show running-config	Verifies the configuration of the standby groups.
Step 8	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring MHSRP

To enable MHSRP and load-balancing, you configure two routers as active routers for their groups, with virtual routers as standby routers as shown in the *MHSRP Load Sharing* figure in the Multiple HSRP section. You need to enter the **standby preempt** interface configuration command on each HSRP interface so that if a router fails and comes back up, the preemption occurs and restores load-balancing.

Router A is configured as the active router for group 1, and Router B is configured as the active router for group 2. The HSRP interface for Router A has an IP address of 10.0.0.1 with a group 1 standby priority of

110 (the default is 100). The HSRP interface for Router B has an IP address of 10.0.0.2 with a group 2 standby priority of 110.

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.

Configuring Router A

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Switch # configure terminal	Enters global configuration mode.
Step 2	interface type number Example: Switch (config)# interface gigabitethernet1/0/1	Configures an interface type and enters interface configuration mode.
Step 3	no switchport Example: Switch (config)# no switchport	Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.
Step 4	ip address ip-address mask Example: Switch (config-if)# ip address 10.0.0.1 255.255.255.0	Specifies an IP address for an interface.
Step 5	standby [group-number] ip [ip-address [secondary]] Example: Switch (config-if)# standby 1 ip 10.0.0.3	Creates the HSRP group using its number and virtual IP address. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) <i>ip-address</i>- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) secondary- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address

	Command or Action	Purpose
		is the active router, with the next highest as the standby router.
Step 6	<p>standby [<i>group-number</i>] priority <i>priority</i></p> <p>Example:</p> <pre>Switch(config-if)# standby 1 priority 110</pre>	<p>Sets a priority value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority.</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number to which the command applies. <p>Use the no form of the command to restore the default values.</p>
Step 7	<p>standby [<i>group-number</i>] preempt [delay [<i>minimum seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]]</p> <p>Example:</p> <pre>Switch(config-if)# standby 1 preempt delay 300</pre>	<p>Configures the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number to which the command applies. • (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). <p>Use the no form of the command to restore the default values.</p>
Step 8	<p>standby [<i>group-number</i>] ip [<i>ip-address</i>] [secondary]]</p> <p>Example:</p> <pre>Switch (config-if)# standby 2 ip 10.0.0.4</pre>	<p>Creates the HSRP group using its number and virtual IP address.</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP

	Command or Action	Purpose
		<p>group, you do not need to enter a group number.</p> <ul style="list-style-type: none"> • (Optional on all but one interface) <i>ip-address</i>- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) secondary- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 9	<p>standby [<i>group-number</i>] preempt [delay [minimum <i>seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]]</p> <p>Example:</p> <pre>Switch(config-if)# standby 2 preempt delay 300</pre>	<p>Configures the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.</p> <ul style="list-style-type: none"> • (Optional) group-number-The group number to which the command applies. • (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). <p>Use the no form of the command to restore the default values.</p>
Step 10	<p>end</p> <p>Example:</p>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	<code>Switch(config-if)# end</code>	
Step 11	show running-config	Verifies the configuration of the standby groups.
Step 12	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Router B

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <code>Switch # configure terminal</code>	Enters global configuration mode.
Step 2	interface <i>type number</i> Example: <code>Switch (config)# interface gigabitethernet1/0/1</code>	Configures an interface type and enters interface configuration mode.
Step 3	no switchport Example: <code>Switch (config)# no switchport</code>	Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.
Step 4	ip address <i>ip-address mask</i> Example: <code>Switch (config-if)# ip address 10.0.0.2 255.255.255.0</code>	Specifies an IP address for an interface.
Step 5	standby [<i>group-number</i>] ip [<i>ip-address</i> [<i>secondary</i>]] Example: <code>Switch (config-if)# standby 1 ip 10.0.0.3</code>	Creates the HSRP group using its number and virtual IP address. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) <i>ip-address</i>- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) secondary- The IP address is a secondary hot standby router interface.

	Command or Action	Purpose
		If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 6	standby [<i>group-number</i>] priority <i>priority</i> Example: Switch(config-if)# standby 2 priority 110	Sets a priority value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number to which the command applies. Use the no form of the command to restore the default values.
Step 7	standby [<i>group-number</i>] preempt [delay [<i>minimum seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]] Example: Switch(config-if)# standby 1 preempt delay 300	Configures the router to preempt , which means that when the local router has a higher priority than the active router, it becomes the active router. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number to which the command applies. • (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the no form of the command to restore the default values.

	Command or Action	Purpose
Step 8	<p>standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]]</p> <p>Example:</p> <pre>Switch (config-if)# standby 2 ip 10.0.0.4</pre>	<p>Creates the HSRP group using its number and virtual IP address.</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>- The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) <i>ip-address</i>- The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. • (Optional) secondary- The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 9	<p>standby [<i>group-number</i>] preempt [delay [<i>minimum seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]]</p> <p>Example:</p> <pre>Switch(config-if)# standby 2 preempt delay 300</pre>	<p>Configures the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.</p> <ul style="list-style-type: none"> • (Optional) <i>group-number</i>-The group number to which the command applies. • (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The

	Command or Action	Purpose
		range is 0 to 3600 seconds (1 hour); the default is 0 (no delay before taking over). Use the no form of the command to restore the default values.
Step 10	end Example: Switch(config-if) # end	Returns to privileged EXEC mode.
Step 11	show running-config	Verifies the configuration of the standby groups.
Step 12	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring HSRP Authentication and Timers

You can optionally configure an HSRP authentication string or change the hello-time interval and hold-time.

When configuring these attributes, follow these guidelines:

- The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperability. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and timer values from other routers configured with HSRP.
- Routers or access servers on which standby timer values are not configured can learn timer values from the active or standby router. The timers configured on an active router always override any other timer settings.
- All routers in a Hot Standby group should use the same timer values. Normally, the *holdtime* is greater than or equal to 3 times the *hellotime*.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP authentication and timers on an interface:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Switch # configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Switch(config) # interface gigabitethernet1/0/1	Enters interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	standby [group-number] authentication string	(Optional) authentication string —Enter a string to be carried in all HSRP messages. The

	Command or Action	Purpose
	Example: <pre>Switch(config-if) # standby 1 authentication word</pre>	authentication string can be up to eight characters in length; the default string is cisco . (Optional) <i>group-number</i> —The group number to which the command applies.
Step 4	standby [<i>group-number</i>] timers <i>hellotime</i> <i>holdtime</i> Example: <pre>Switch(config-if) # standby 1 timers 5 15</pre>	(Optional) Configure the time interval to send and receive hello packets. <ul style="list-style-type: none"> • <i>group-number</i>—The group number to which the command applies. • <i>hellotime</i> —Set the interval between successive hello packets in seconds. The range is 1 to 255 seconds. The default is 3. • <i>holdtime</i>—Set the interval to wait for a hello packet from a neighbor device before declaring the neighbor device as inactive. The range is 1 to 255 seconds. The default is 10.
Step 5	end Example: <pre>Switch(config-if) # end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config	Verifies the configuration of the standby groups.
Step 7	copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Enabling HSRP Support for ICMP Redirect Messages

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host. This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address. For more information, see the Cisco IOS IP Configuration Guide, Release 12.4.

Configuring HSRP Groups and Clustering

When a device is participating in an HSRP standby routing and clustering is enabled, you can use the same standby group for command switch redundancy and HSRP redundancy. Use the **cluster standby-group** *HSRP-group-name* [**routing-redundancy**] global configuration command to enable the same HSRP standby group to be used for command switch and routing redundancy. If you create a cluster with the same HSRP standby group name without entering the **routing-redundancy** keyword, HSRP standby routing is disabled for the group.

Verifying HSRP

Verifying HSRP Configurations

From privileged EXEC mode, use this command to display HSRP settings:

```
show standby [interface-id [group]] [brief] [detail]
```

You can display HSRP information for the whole switch, for a specific interface, for an HSRP group, or for an HSRP group on an interface. You can also specify whether to display a concise overview of HSRP information or detailed HSRP information. The default display is **detail**. If there are a large number of HSRP groups, using the **show standby** command without qualifiers can result in an unwieldy display.

Example

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hello time 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hello time 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

Configuration Examples for Configuring HSRP

Enabling HSRP: Example

This example shows how to activate HSRP for group 1 on an interface. The IP address used by the hot standby group is learned by using HSRP.



Note This procedure is the minimum number of steps required to enable HSRP. Other configurations are optional.

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # standby 1 ip
Switch(config-if) # end
Switch # show standby
```


Configuring HSRP Priority: Example

This example activates a port, sets an IP address and a priority of 120 (higher than the default value), and waits for 300 seconds (5 minutes) before attempting to become the active router:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # standby ip 172.20.128.3
Switch(config-if) # standby priority 120 preempt delay 300
Switch(config-if) # end
Switch # show standby
```

Configuring MHSRP: Example

This example shows how to enable the MHSRP configuration shown in the figure *MHSRP Load Sharing*

Router A Configuration

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # ip address 10.0.0.1 255.255.255.0
Switch(config-if) # standby ip 10.0.0.3
Switch(config-if) # standby 1 priority 110
Switch(config-if) # standby 1 preempt
Switch(config-if) # standby 2 ip 10.0.0.4
Switch(config-if) # standby 2 preempt
Switch(config-if) # end
```

Router B Configuration

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # ip address 10.0.0.2 255.255.255.0
Switch(config-if) # standby ip 10.0.0.3
Switch(config-if) # standby 1 preempt
Switch(config-if) # standby 2 ip 10.0.0.4
Switch(config-if) # standby 2 priority 110
Switch(config-if) # standby 2 preempt
Switch(config-if) # end
```

Configuring HSRP Authentication and Timer: Example

This example shows how to configure word as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # standby 1 authentication word
Switch(config-if) # end
```

This example shows how to set the timers on standby group 1 with the time between hello packets at 5 seconds and the time after which a router is considered down to be 15 seconds:

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if) # no switchport
Switch(config-if) # standby 1 ip
Switch(config-if) # standby 1 timers 5 15
Switch(config-if) # end
```

Configuring HSRP Groups and Clustering: Example

This example shows how to bind standby group my_hsrp to the cluster and enable the same HSRP group to be used for command switch redundancy and router redundancy. The command can only be executed on the cluster command switch. If the standby group name or number does not exist, or if the switch is a cluster member switch, an error message appears.

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if) # end
```

Additional References for Configuring HSRP

Standards and RFCs

Standard/RFC	Title
<i>RFC 2281</i>	Cisco Hot Standby Router Protocol

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for Configuring HSRP

Table 2: Feature Information for Configuring HSRP

Release	Feature Information
Cisco IOS XE Fuji 16.9.1	This feature was introduced.



CHAPTER 2

VRRPv3 Protocol Support

- [VRRPv3 Protocol Support, on page 23](#)

VRRPv3 Protocol Support

Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. The LAN clients can then be configured with the virtual device as their default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRP version 3 (v3) Protocol Support feature provides the capability to support IPv4 and IPv6 addresses while VRRP version 2 (v2) only supports IPv4 addresses. This module explains concepts related to VRRPv3 and describes how to create and customize a VRRP group in a network. Benefits of using VRRPv3 Protocol Support include the following:

- Interoperability in multi-vendor environments.
- VRRPv3 supports usage of IPv4 and IPv6 addresses while VRRPv2 only supports IPv4 addresses
- Improved scalability through the use of VRRS Pathways.



Note In this module, VRRP and VRRPv3 are used interchangeably.

Restrictions for VRRPv3 Protocol Support

- VRRPv3 is not intended as a replacement for existing dynamic protocols. VRRPv3 is designed for use over multi-access, multicast, or broadcast capable Ethernet LANs.
- VRRPv3 is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must not configure the VRRPv3 advertise timer to a value lesser than the forwarding delay on the BVI interface. If you configure the VRRPv3 advertise timer to a value equal to or greater than the forwarding delay on the BVI interface, the setting prevents a VRRP device on a recently initialized BVI interface from unconditionally taking over the primary role. Use the **bridge forward-time** command to set the forwarding

delay on the BVI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.

- VRRPv3 does not support Stateful Switchover (SSO).
- Full network redundancy can only be achieved if VRRP operates over the same network path as the VRRS Pathway redundant interfaces. For full redundancy, the following restrictions apply:
 - VRRS pathways should not share a different physical interface as the parent VRRP group or be configured on a sub-interface having a different physical interface as the parent VRRP group.
 - VRRS pathways should not be configured on Switch Virtual Interface (SVI) interfaces as long as the associated VLAN does not share the same trunk as the VLAN on which the parent VRRP group is configured.

Information About VRRPv3 Protocol Support

VRRPv3 Benefits

Support for IPv4 and IPv6

VRRPv3 supports IPv4 and IPv6 address families while VRRPv2 only supports IPv4 addresses.



Note When VRRPv3 is in use, VRRPv2 is unavailable. For VRRPv3 to be configurable, the **fhrrp version vrrp v3** command must be used in global configuration mode

Redundancy

VRRP enables you to configure multiple devices as the default gateway device, which reduces the possibility of a single point of failure in a network.

Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple devices, thereby sharing the traffic load more equitably between available devices.

Multiple Virtual Devices

VRRP supports up to 255 virtual devices (VRRP groups) on a device physical interface, subject to restrictions in scaling. Multiple virtual device support enables you to implement redundancy and load sharing in your LAN topology. In scaled environments, VRRS Pathways should be used in combination with VRRP control groups.

Multiple IP Addresses

The virtual device can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.



Note To utilize secondary IP addresses in a VRRP group, a primary address must be configured on the same group.

Preemption

The redundancy scheme of VRRP enables you to preempt a virtual device backup that has taken over for a failing virtual primary device with a higher priority virtual device backup that has become available.



Note Preemption of a lower priority primary device is enabled with an optional delay.

Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address for VRRP advertisements. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:12. This addressing scheme minimizes the number of devices that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA has assigned VRRP the IP protocol number 112.

VRRP Device Priority and Preemption

An important aspect of the VRRP redundancy scheme is VRRP device priority. Priority determines the role that each VRRP device plays and what happens if the virtual primary device fails.

If a VRRP device owns the IP address of the virtual device and the IP address of the physical interface, this device will function as a virtual primary device.

Priority also determines if a VRRP device functions as a virtual device backup and the order of ascendancy to becoming a virtual primary device if the virtual primary device fails. You can configure the priority of each virtual device backup with a value of 1 through 254 using the **priority** command (use the **vrrp address-family** command to enter the VRRP configuration mode and access the **priority** option).

For example, if device A, the virtual primary device in a LAN topology, fails, an election process takes place to determine if virtual device backups B or C should take over. If devices B and C are configured with the priorities of 101 and 100, respectively, device B is elected to become virtual primary device because it has the higher priority. If devices B and C are both configured with the priority of 100, the virtual device backup with the higher IP address is elected to become the virtual primary device.

By default, a preemptive scheme is enabled whereby a higher priority virtual device backup that becomes available takes over from the virtual device backup that was elected to become virtual primary device. You can disable this preemptive scheme using the **no preempt** command (use the **vrrp address-family** command to enter the VRRP configuration mode, and enter the **no preempt** command). If preemption is disabled, the virtual device backup that is elected to become virtual primary device remains the primary until the original virtual primary device recovers and becomes primary again.



Note Preemption of a lower priority primary device is enabled with an optional delay.

VRRP Advertisements

The virtual primary device sends VRRP advertisements to other VRRP devices in the same group. The advertisements communicate the priority and state of the virtual primary device. The VRRP advertisements are encapsulated into either IPv4 or IPv6 packets (based on the VRRP group configuration) and sent to the appropriate multicast address assigned to the VRRP group. For IPv4, the multicast address is 224.0.0.18. For IPv6, the multicast address is FF02:0:0:0:0:0:0:12. The advertisements are sent every second by default and the interval is configurable.

Cisco devices allow you to configure millisecond timers, which is a change from VRRPv2. You need to manually configure the millisecond timer values on both the primary and the backup devices. The primary advertisement value displayed in the **show vrrp** command output on the backup devices is always 1 second because the packets on the backup devices do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances. The use of the millisecond timer values is compatible with third party vendors, as long as they also support VRRPv3. You can specify a timer value between 100 milliseconds and 40000 milliseconds.

How to Configure VRRPv3 Protocol Support

Creating and Customizing a VRRP Group

To create a VRRP group, perform the following task. Steps 6 to 14 denote customizing options for the group, and they are optional:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	fhrp version vrrp v3 Example: Device(config)# fhrp version vrrp v3	Enables the ability to configure VRRPv3 and VRRS. <p>Note When VRRPv3 is in use, VRRPv2 is unavailable.</p> <p>The command fhrp version vrrp v2 is not supported though it is configurable.</p>
Step 4	interface <i>type number</i> Example:	Enters interface configuration mode.

	Command or Action	Purpose
	Device(config)# interface GigabitEthernet 0/0/0	
Step 5	vrrp group-id address-family {ipv4 ipv6} Example: Device(config-if)# vrrp 3 address-family ipv4	Creates a VRRP group and enters VRRP configuration mode.
Step 6	address ip-address [primary secondary] Example: Device(config-if-vrrp)# address 100.0.1.10 primary	Specifies a primary or secondary address for the VRRP group. Note VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.
Step 7	description group-description Example: Device(config-if-vrrp)# description group 3	(Optional) Specifies a description for the VRRP group.
Step 8	match-address Example: Device(config-if-vrrp)# match-address	(Optional) Matches secondary address in the advertisement packet against the configured address. • Secondary address matching is enabled by default.
Step 9	preempt delay minimum seconds Example: Device(config-if-vrrp)# preempt delay minimum 30	(Optional) Enables preemption of lower priority primary device with an optional delay. • Preemption is enabled by default.
Step 10	priority priority-level Example: Device(config-if-vrrp)# priority 3	(Optional) Specifies the priority value of the VRRP group. • The priority of a VRRP group is 100 by default.
Step 11	timers advertise interval Example:	(Optional) Sets the advertisement timer in milliseconds. • The advertisement timer is set to 1000 milliseconds by default.

	Command or Action	Purpose
	Device(config-if-vrrp)# timers advertise 1000	
Step 12	vrrpv2 Example: Device(config-if-vrrp)# vrrpv2	(Optional) Enables support for VRRPv2 configured devices in compatibility mode. <ul style="list-style-type: none"> • VRRPv2 is not supported.
Step 13	vrrs leader vrrs-leader-name Example: Device(config-if-vrrp)# vrrs leader leader-1	(Optional) Specifies a leader's name to be registered with VRRS and to be used by followers. <ul style="list-style-type: none"> • A registered VRRS name is unavailable by default.
Step 14	shutdown Example: Device(config-if-vrrp)# shutdown	(Optional) Disables VRRP configuration for the VRRP group. <ul style="list-style-type: none"> • VRRP configuration is enabled for a VRRP group by default.
Step 15	end Example: Device(config)# end	Returns to privileged EXEC mode.

Configuring the Delay Period Before FHRP Client Initialization

To configure the delay period before the initialization of all FHRP clients on an interface, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	fhrp version vrrp v3 Example:	Enables the ability to configure VRRPv3 and VRRS.

	Command or Action	Purpose
	Device(config)# fhrp version vrrp v3	Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Enters interface configuration mode.
Step 5	fhrp delay {[minimum] [reload] seconds} Example: Device(config-if)# fhrp delay minimum 5	Specifies the delay period for the initialization of FHRP clients after an interface comes up. <ul style="list-style-type: none"> • The range is 0-3600 seconds.
Step 6	end Example: Device(config)# end	Returns to privileged EXEC mode.

Configuration Examples for VRRPv3 Protocol Support

Example: Enabling VRRPv3 on a Device

The following example shows how to enable VRRPv3 on a device:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

Example: Creating and Customizing a VRRP Group

The following example shows how to create and customize a VRRP group:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```



Note In the above example, the **fhrp version vrrp v3** command is used in the global configuration mode.

Example: Configuring the Delay Period Before FHRP Client Initialization

The following example shows how to configure the delay period before FHRP client initialization :

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```



Note In the above example, a five-second delay period is specified for the initialization of FHRP clients after the interface comes up. You can specify a delay period between 0 and 3600 seconds.

Example: VRRP Status, Configuration, and Statistics Details

The following is a sample output of the status, configuration and statistics details for a VRRP group:

```
Device> enable
Device# show vrrp detail

GigabitEthernet1/0/1 - Group 3 - Address-Family IPv4
Description is "group 3"
State is MASTER
State duration 53.901 secs
Virtual IP address is 100.0.1.10
Virtual MAC address is 0000.5E00.0103
Advertisement interval is 1000 msec
Preemption enabled, delay min 30 secs (0 msec remaining)
Priority is 100
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1000 msec (expires in 832 msec)
Master Down interval is unknown
VRRPv3 Advertisements: sent 61 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 0
  VRRPv2 incompatibility: 0
  IP Address Owner conflicts: 0
  Invalid address count: 0
  IP address configuration mismatch : 0
  Invalid Advert Interval: 0
  Advert received in Init state: 0
  Invalid group other reason: 0
Group State transition:
  Init to master: 0
  Init to backup: 1 (Last change Sun Mar 13 19:52:56.874)
  Backup to master: 1 (Last change Sun Mar 13 19:53:00.484)
  Master to backup: 0
  Master to init: 0
  Backup to init: 0
```

Device# **exit**

Additional References

Related Documents

Related Topic	Document Title
FHRP commands	First Hop Redundancy Protocols Command Reference
Configuring VRRPv2	<i>Configuring VRRP</i>
VRRPv3 Commands	For complete syntax and usage information for the commands used in this chapter. <i>Command Reference (Catalyst 9200 Series Switches)</i>

Standards and RFCs

Standard/RFC	Title
RFC5798	<i>Virtual Router Redundancy Protocol</i>

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 VRRPv3 Protocol Support

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 3: Feature Information for VRRPv3 Protocol Support

Feature Name	Releases	Feature Information
VRRPv3 Protocol Support	Cisco IOS XE Fuji 16.9.1	VRRP enables a group of devices to form a single virtual device to provide redundancy. The LAN clients can then be configured with the virtual device as their default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRPv3 Protocol Support feature provides the capability to support IPv4 and IPv6 addresses. This feature was introduced.

Glossary

Virtual IP address owner—The VRRP device that owns the IP address of the virtual device. The owner is the device that has the virtual device address as its physical interface address.

Virtual device—One or more VRRP devices that form a group. The virtual device acts as the default gateway device for LAN clients. The virtual device is also known as a VRRP group.

Virtual device backup—One or more VRRP devices that are available to assume the role of forwarding packets if the virtual primary device fails.

Virtual primary device—The VRRP device that is currently responsible for forwarding packets sent to the IP addresses of the virtual device. Usually, the virtual primary device also functions as the IP address owner.

VRRP device—A device that is running VRRP.



CHAPTER 3

Configuring Enhanced Object Tracking

- [Finding Feature Information, on page 33](#)
- [Information About Enhanced Object Tracking, on page 33](#)
- [How to Configure Enhanced Object Tracking, on page 35](#)
- [Monitoring Enhanced Object Tracking, on page 46](#)
- [Additional References, on page 47](#)
- [Feature Information for Enhanced Object Tracking, on page 47](#)

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 at the end of this module.

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

Information About Enhanced Object Tracking

Enhanced Object Tracking Overview

Before the introduction of the Enhanced Object Tracking feature, Hot Standby Router Protocol (HSRP) had a simple tracking mechanism that allowed you to track the interface line-protocol state only. If the line-protocol state of the interface went down, the HSRP priority of the router was reduced, allowing another HSRP router with a higher priority to become active.

The Enhanced Object Tracking feature separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by processes other than HSRP. This feature allows the tracking of other objects in addition to the interface line-protocol state.

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

Each tracked object has a unique number that is specified in the tracking command-line interface (CLI). Client processes use this number to track a specific object. The tracking process periodically polls the tracked object for value changes and sends any changes (as up or down values) to interested client processes, either immediately or after a specified delay. Several clients can track the same object, and can take different actions when the object changes state.

You can also track a combination of objects in a list by using either a weight threshold or a percentage threshold to measure the state of the list. You can combine objects using Boolean logic. A tracked list with a Boolean “AND” function requires that each object in the list be in an up state for the tracked object to be up. A tracked list with a Boolean “OR” function needs only one object in the list to be in the up state for the tracked object to be up.

Tracking Interface Line-Protocol or IP Routing State

You can track either the interface line protocol state or the interface IP routing state. When you track the IP routing state, these three conditions are required for the object to be up:

- IP routing must be enabled and active on the interface.
- The interface line-protocol state must be up.
- The interface IP address must be known.

If all three of these conditions are not met, the IP routing state is down.

Tracked Lists

You can configure a tracked list of objects with a Boolean expression, a weight threshold, or a percentage threshold. A tracked list contains one or more objects. An object must exist before it can be added to the tracked list.

- You configure a Boolean expression to specify calculation by using either “AND” or “OR” operators.
- When you measure the tracked list state by a weight threshold, you assign a weight number to each object in the tracked list. The state of the tracked list is determined by whether or not the threshold was met. The state of each object is determined by comparing the total weight of all objects against a threshold weight for each object.
- When you measure the tracked list by a percentage threshold, you assign a percentage threshold to all objects in the tracked list. The state of each object is determined by comparing the assigned percentages of each object to the list.

Tracking Other Characteristics

You can also use the enhanced object tracking for tracking other characteristics.

- You can track the reachability of an IP route by using the **track ip route reachability** global configuration command.
- You can use the **track ip route metric threshold** global configuration command to determine if a route is above or below threshold.

- You can use the **track resolution** global configuration command to change the metric resolution default values for routing protocols.
- You can use the **track timer tracking** configuration command to configure the tracking process to periodically poll tracked objects.

Use the **show track** privileged EXEC command to verify enhanced object tracking configuration.

IP SLAs Object Tracking

Cisco IOS IP Service Level Agreements (IP SLAs) is a network performance measurement and diagnostics tool that uses active monitoring by generating traffic to measure network performance. Cisco IP SLAs operations collects real-time metrics that you can use for network troubleshooting, design, and analysis.

Object tracking of IP SLAs operations allows clients to track the output from IP SLAs objects and use this information to trigger an action. Every IP SLAs operation maintains an SNMP operation return-code value, such as OK or OverThreshold, that can be interpreted by the tracking process. You can track two aspects of IP SLAs operation: state and reachability. For state, if the return code is OK, the track state is up; if the return code is not OK, the track state is down. For reachability, if the return code is OK or OverThreshold, reachability is up; if not OK, reachability is down.

Static Route Object Tracking

Static routing support using enhanced object tracking provides the ability for the device to use ICMP pings to identify when a pre-configured static route or a DHCP route goes down. When tracking is enabled, the system tracks the state of the route and informs the client when that state changes. Static route object tracking uses Cisco IP SLAs to generate ICMP pings to monitor the state of the connection to the primary gateway.

How to Configure Enhanced Object Tracking

Configuring Tracking for Line State Protocol or IP Routing State on an Interface

Follow these steps to track the line-protocol state or IP routing state of an interface:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Device# <code>configure terminal</code>	
Step 3	track <i>object-number</i> interface <i>interface-id</i> line-protocol Example: Device(config)# track 33 interface gigabitethernet 1/0/1 line-protocol	(Optional) Creates a tracking list to track the line-protocol state of an interface and enter tracking configuration mode. <ul style="list-style-type: none"> • The object-number identifies the tracked object and can be from 1 to 500. • The interface interface-id is the interface being tracked.
Step 4	delay { <i>object-number</i> upseconds [downseconds][upseconds] downseconds ; 	(Optional) Specifies a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.
Step 5	exit	Returns to global configuration mode.
Step 6	track <i>object-number</i> interface <i>interface-id</i> ip routing Example: Device(config)# track 33 interface gigabitethernet 1/0/1 ip routing	(Optional) Creates a tracking list to track the IP routing state of an interface and enter tracking configuration mode. IP route tracking tracks an IP route in the routing table and the ability of an interface to route IP packets. <ul style="list-style-type: none"> • The object-number identifies the tracked object and can be from 1 to 500. • The interface interface-id is the interface being tracked.
Step 7	delay { <i>object-number</i> upseconds [downseconds][upseconds] downseconds ; 	(Optional) Specifies a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.
Step 8	end	Returns to privileged EXEC mode.
Step 9	show track <i>object-number</i>	Verifies that the specified objects are being tracked.

Configuring Tracked Lists

Configuring a Tracked List with a Weight Threshold

To track by weight threshold, configure a tracked list of objects, specify that weight is used as the threshold, and configure a weight for each of its objects. The state of each object is determined by comparing the total weight of all objects that are up against a threshold weight for each object.

You cannot use the Boolean “NOT” operator in a weight threshold list.

Follow these steps to configure a tracked list of objects by using a weight threshold and to configure a weight for each object:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	track track-numberlist threshold {weight} Example: Device(config)# track 4 list threshold weight	Configures a tracked list object, and enters tracking configuration mode. The track-number can be from 1 to 500. <ul style="list-style-type: none"> • threshold—Specifies the state of the tracked list based on a threshold. • weight— Specifies that the threshold is based on weight.
Step 4	object object-number[weightweight-number] Example: Device(config)# object 2 weight 15	Specifies the object to be tracked. The range is from 1 to 500. The optional weightweight-number specifies the threshold weight for the object. The range is from 1 to 255. <p>Note An object must exist before you can add it to a tracked list.</p>
Step 5	threshold weight {upnumber[[downnumber]]} Example: Device(config-track)# threshold weight up 30 down 10	(Optional) Specifies the threshold weight. <ul style="list-style-type: none"> • upnumber—The range is from 1 to 255. • downnumber—(Optional)The range depends on the number selected for the upnumber. If you configure the upnumber as 25, the range shown for the down number is 0 to 24.
Step 6	delay {upseconds[downseconds][upseconds]downseconds}	(Optional) Specifies a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.

	Command or Action	Purpose
Step 7	end	Returns to privileged EXEC mode.
Step 8	show trackobject-number	Verify that the specified objects are being tracked.
Step 9	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Tracked List with a Percentage Threshold

To track by percentage threshold, configure a tracked list of objects, specify that a percentage will be used as the threshold, and specify a percentage for all objects in the list. The state of the list is determined by comparing the assigned percentage of each object to the list.

You cannot use the Boolean “NOT” operator in a percentage threshold list.

Follow these steps to configure a tracked list of objects by using a percentage threshold:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	track track-numberlist threshold {percentage} Example: <pre>Device(config)# track 4 list threshold percentage</pre>	Configures a tracked list object, and enters tracking configuration mode. The track-number can be from 1 to 500. <ul style="list-style-type: none"> • threshold—Specifies the state of the tracked list based on a threshold. • percentage— Specifies that the threshold is based on percentage.

	Command or Action	Purpose
Step 4	object <i>object-number</i> Example: Device(config)# object 1	Specifies the object to be tracked. The range is from 1 to 500. Note An object must exist before you can add it to a tracked list.
Step 5	threshold percentage { upnumber [[downnumber]} Example: Device(config)# threshold percentage up 51 down 10	(Optional) Specifies the threshold percentage. <ul style="list-style-type: none"> • upnumber—The range is from 1 to 100. • downnumber—(Optional)The range depends on the number selected for the upnumber. If you configure the upnumber as 25, the range shown for the down number is 0 to 24.
Step 6	delay { upseconds [[downseconds]][upseconds] downseconds }	(Optional) Specifies a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.
Step 7	end	Returns to privileged EXEC mode.
Step 8	show track <i>object-number</i>	Verify that the specified objects are being tracked.
Step 9	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring HSRP Object Tracking

Follow these steps to configure a standby HSRP group to track an object and change the HSRP priority based on the object state:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	track object-number { interface interface-id { line-protocol ip routing } ip route <i>ip address/prefix-length</i> { metric threshold reachability list } list { <i>weight</i> } }	(Optional) Create a tracking list to track the configured state and enter tracking configuration mode. <ul style="list-style-type: none"> • The object-number identifies the tracked object and can be from 1 to 500. • Enter interface interface-id to select an interface to track. • Enter line-protocol to track the interface line protocol state or enter ip routing to track the interface IP routing state . • Enter ip route<i>ip-address/prefix-length</i> to track the state of an IP route. • Enter metric threshold to track the threshold metric or enter reachability to track if the route is reachable. The default up threshold is 254 and the default down threshold is 255. • Enter list to track objects grouped in a list. <p>Note Repeat this step for each interface to be tracked.</p>
Step 4	exit	Return to global configuration mode.
Step 5	interface { <i>interface-id</i>	Enter interface configuration mode.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i>] secondary]]	Creates (or enables) the HSRP group by using its number and virtual IP address. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—Enters a group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) <i>ip-address</i>—Specifies the virtual IP address of the hot standby router

	Command or Action	Purpose
		<p>interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.</p> <ul style="list-style-type: none"> (Optional) secondary—Specifies that the IP address is a secondary hot standby router interface. If this keyword is omitted, the configured address is the primary IP address.
Step 7	standby [<i>group-number</i>] track [<i>object-number</i>] decrement [<i>priority-decrement</i>]	<p>Configures HSRP to track an object and change the hot standby priority based on the state of the object.</p> <ul style="list-style-type: none"> (Optional) <i>group-number</i>—Enters the group number to which the tracking applies. <i>object-number</i>—Enters a number representing the object to be tracked. The range is from 1 to 500; the default is 1. (Optional) secondary—Specifies that the IP address is a secondary hot standby router interface. If this keyword is omitted, the configured address is the primary IP address. (Optional)decrement<i>priority-decrement</i>—Specifies the amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The range is from 1 to 255; the default is 10.
Step 8	end	Returns to privileged EXEC mode.
Step 9	show standby	Verifies the standby router IP address and tracking states.
Step 10	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring IP SLAs Object Tracking

Follow these steps to track the state of an IP SLAs operation or the reachability of an IP SLAs IP host:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	track <i>object-number</i> ip sla <i>operation-number</i> {state reachability} Example: Device (config)# track 2 ip sla 123 state	Enters tracking configuration mode to track the state of an IP SLAs operation. <ul style="list-style-type: none"> • <i>object-number</i> range is from 1 to 500. • <i>operation-number</i> range is from 1 to 2147483647.
Step 4	delay { upseconds[downseconds][upseconds]downseconds }	(Optional) Specifies a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds.
Step 5	end	Returns to privileged EXEC mode.
Step 6	show track<i>object-number</i>	Verifies that the specified objects are being tracked.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring Static Route Object Tracking

Configuring a Primary Interface for Static Routing

Follow these steps to configure a primary interface for static routing:

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i>	Selects a primary or secondary interface and enters interface configuration mode.
Step 4	description <i>string</i>	Adds a description to the interface.
Step 5	ip address <i>ip-address mask</i> [secondary]	Sets the primary or secondary IP address for the interface.
Step 6	exit	Returns to global configuration mode.

Configuring a Primary Interface for DHCP

Follow these steps to configure a primary interface for DHCP:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i>	Selects a primary or secondary interface and enters interface configuration mode.
Step 4	description <i>string</i>	Adds a description to the interface.
Step 5	ip dhcp client route track <i>number</i>	Configures the DHCP client to associate any added routes with the specified track number. Valid numbers are from 1 to 500.
Step 6	exit	Returns to global configuration mode.

Configuring IP SLAs Monitoring Agent

You can configure an IP SLAs agent to ping an IP address using a primary interface and a track object to monitor the state of the agent.

Follow these steps to configure network monitoring with Cisco IP SLAs:

Procedure

	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	ip sla operation number	Begins configuring a Cisco IP SLAs operation and enters IP SLA configuration mode.
Step 4	icmp-echo { destination ip-address destination hostname}[source - ipaddr {ip-address hostname} source-interface interface-id]	Configures a Cisco IP SLAs end-to-end ICMP echo response time operation and enter IP SLAs ICMP echo configuration mode.
Step 5	timeout milliseconds	Sets the amount of time for which the operation waits for a response from its request packet.
Step 6	frequency seconds	Sets the rate at which the operation is sent into the network.
Step 7	threshold milliseconds	Sets the rising threshold (hysteresis) that generates a reaction event and stores history information for the operation.
Step 8	exit	Exits IP SLAs ICMP echo configuration mode.
Step 9	ip sla schedule operation-number [life {seconds} state {ping power http icmp icmp-echo icmp-jitter icmp-rtt icmp-rtt-jitter icmp-rtt-jitter-avg} time {interval interval interval} [time] [days]	Configures the scheduling parameters for a single IP SLAs operation. • <i>object-number</i> range is from 1 to 500. • <i>operation-number</i> range is from 1 to 2147483647.
Step 10	track object-number rtr operation-number state reachability	Tracks the state of a Cisco IOS IP SLAs operation and enter tracking configuration mode.

	Command or Action	Purpose
Step 11	end	Returns to privileged EXEC mode.
Step 12	show track <i>object-number</i>	Verifies that the specified objects are being tracked.
Step 13	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Routing Policy and a Default Route

Follow these steps to configure a routing policy for backup static routing by using object tracking.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i>	Defines an extended IP access list. Configure any optional characteristics.
Step 4	route-map <i>map tag</i> [permit deny][<i>sequence-number</i>]	Enters route-map configuration mode and define conditions for redistributing routes from one routing protocol to another.
Step 5	match ip address { <i>access-list number</i> [permit deny][<i>sequence-number</i>]	Distribute any routes that have a destination network number address that is permitted by a standard or extended access list or performs policy routing on packets. You can enter multiple numbers or names.
Step 6	set ip next-hop dynamic dhcp	For DHCP networks only. Sets the next hop to the gateway that was most recently learned by the DHCP client.

	Command or Action	Purpose
Step 7	<code>set interface</code> <i>interface-id</i>	For static routing networks only. Indicates where to send output packets that pass a match clause of a route map for policy routing.
Step 8	<code>exit</code>	Returns to global configuration mode.
Step 9	<code>ip local policy route-map</code> <i>map tag</i>	Identifies a route map to use for local policy routing.
Step 10	<code>ip route</code> <i>prefix mask {ip address interface-id [ip address]} [distance] [name] [permanent] [track track-number] [tag tag]</i>	For static routing networks only. Establishes static routes. Entering track <i>track-number</i> specifies that the static route is installed only if the configured track object is up.
Step 11	<code>end</code>	Returns to privileged EXEC mode.
Step 12	<code>show ip route track table</code>	Displays information about the IP route track table.
Step 13	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring Enhanced Object Tracking

Use the privileged EXEC or user EXEC commands in the table below, to display enhanced object tracking information.

Table 4: Commands for Displaying Tracking Information

Command	Purpose
<code>show ip route track table</code>	Displays information about the IP route track table.
<code>show track [object-number]</code>	Displays information about the all tracking objects.
<code>show track brief</code>	Displays VTP status and configuration for tracked interfaces.
<code>show track interface [brief]</code>	Displays information about tracked interfaces.
<code>show track ip [object-number] [brief] route</code>	Displays information about tracked IP routes.
<code>show track resolution</code>	Displays the resolution of tracked parameters.
<code>show track timer</code>	Displays tracked polling interval timers.

Additional References

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for Enhanced Object Tracking

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 5: Feature Information for Enhanced Object Tracking

Feature Name	Releases	Feature Information
Enhanced Object Tracking	Cisco IOS XE Fuji 16.9.1	This feature was introduced.



CHAPTER 4

Configuring TCP MSS Adjustment

- [Restrictions for TCP MSS Adjustment, on page 49](#)
- [Information about TCP MSS Adjustment, on page 49](#)
- [Configuring the MSS Value for Transient TCP SYN Packets, on page 50](#)
- [Configuring the MSS Value for IPv6 Traffic, on page 51](#)
- [Example: Configuring the TCP MSS Adjustment for IPv6 traffic, on page 51](#)
- [Feature History for TCP MSS Adjustment, on page 51](#)

Restrictions for TCP MSS Adjustment

- Subinterfaces do not support TCP MSS Adjust.
- TCP MSS adjustment works only on the ingress packet capture and not on the egress packet capture of a TCP stream on a Layer 3 GRE tunnel.

Information about TCP MSS Adjustment

The Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment feature enables the configuration of the maximum segment size for transient packets that traverse a router, specifically TCP segments with the SYN bit set. Use the `ip tcp adjust-mss` command in interface configuration mode to specify the MSS value on the intermediate router of the SYN packets to avoid truncation.

When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the MTU configuration on the host. The default MSS value for a PC is 1500 bytes.

The PPP over Ethernet (PPPoE) standard supports an MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the ICMP error messages that must be relayed from the host in order for path MTU to work.

The `ip tcp adjust-mss` command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The `ip tcp adjust-mss` command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the max-segment-size argument of the `ip tcp adjust-mss` command is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

Supported Interfaces

TCP MSS Adjust is supported only on the following interfaces:

- Physical Layer 3 interface
- SVI
- Layer 3 port channel
- Layer 3 GRE tunnel

Configuring the MSS Value for Transient TCP SYN Packets

Before you begin

Perform this task to configure the MSS for transient packets that traverse a router, specifically TCP segments with the SYN bit set.

We recommend that you use the `ip tcp adjust-mss 1452` command.

Procedure

	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# config terminal	Enters the global configuration mode.
Step 3	interface <i>type number</i> Example: Device (config) # interface GigabitEthernet 1/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip tcp adjust-mss <i>max-segment-size</i> Example: Device (config-if) # ip tcp adjust-mss 1452	Adjusts the MSS value of TCP SYN packets going through a router. The max-segment-size argument is the maximum segment size, in bytes. The range is from 500 to 1460.
Step 5	end Example:	Exits to global configuration mode.

	Command or Action	Purpose
	Device (config-if) #end	

Configuring the MSS Value for IPv6 Traffic

Procedure

	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#config terminal	Enters the global configuration mode.
Step 3	interface <i>type number</i> Example: Device (config) #interface GigabitEthernet 1/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ipv6 tcp adjust-mss <i>max-segment-size</i> Example: Device (config-if) #ipv6 tcp adjust-mss 1440	Adjusts the MSS value of TCP DF packets going through a device. The max-segment-size argument is the maximum segment size, in bytes. The range is from 40 to 1440.
Step 5	end Example: Device (config-if) #end	Exits interface configuration mode and returns to privileged EXEC mode.

Example: Configuring the TCP MSS Adjustment for IPv6 traffic

```
Device>enable
Device#configure terminal
Device (config) #interface GigabitEthernet 0/0/0
Device (config) #ipv6 tcp adjust-mss 1440
Device (config) #end
```

Feature History for TCP MSS Adjustment

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.2	Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment	The TCP MSS Adjustment feature enables the configuration of the maximum segment size for transient packets that traverse a router, specifically TCP segments with the SYN bitset. This feature helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



CHAPTER 5

Enhanced IPv6 Neighbor Discovery Cache Management

- [Enhanced IPv6 Neighbor Discovery Cache Management](#) , on page 53
- [Customizing the Parameters for IPv6 Neighbor Discovery](#) , on page 54
- [Examples: Customizing Parameters for IPv6 Neighbor Discovery](#), on page 55
- [Additional References](#), on page 55
- [Feature Information for IPv6 Neighbor Discovery](#), on page 55

Enhanced IPv6 Neighbor Discovery Cache Management

Neighbor discovery protocol enforces the neighbor unreachability detection process to detect failing nodes, or devices, and changes to link-layer addresses. Neighbor unreachability detection process maintains the reachability information for all paths between hosts and neighboring nodes, including host-to-host, host-to-device, and device-to-host communication.

The neighbor cache maintains mapping information about the IPv6 link-local or global address to the link-layer address. The neighbor cache also maintains the reachability state of the neighbor using the neighbor unreachability detection process. Neighbors can be in one of the following five possible states:

- DELAY—Neighbor is pending re-resolution with a limited flow of traffic to this neighbor.
- INCOMPLETE—Address resolution is in progress, and the link-layer address is not yet known.
- PROBE—Neighbor re-resolution is in progress with a limited flow of traffic to this neighbor.
- REACHABLE—Neighbor detected within the last reachable time interval.
- STALE—Neighbor requires re-resolution with a limited flow of traffic to this neighbor.

Use the **ipv6 nd na glean** command to configure the neighbor discovery protocol to glean an entry from an unsolicited neighbor advertisement.

Use the **ipv6 nd nud retry** command to configure the neighbor discovery protocol to maintain a neighbor discovery cache entry for a neighbor during a network disruption.

Use the **ipv6 nd cache expire refresh** command to configure the neighbor discovery protocol maintain a neighbor discovery cache entry even when no traffic flows to the neighbor.

Customizing the Parameters for IPv6 Neighbor Discovery

To customize the parameters for IPv6 neighbor discovery, perform this procedure:

Procedure

	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 1/1/4	Specifies an interface type and identifier. Enters the interface configuration mode.
Step 4	ipv6 nd nud retry base interval max-attempts [final-wait-time] Example: Device(config-if)# ipv6 nd nud retry 1 1000 3	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
Step 5	ipv6 nd cache expire expire-time-in-seconds [refresh] Example: Device(config-if)# ipv6 nd cache expire 7200	Configures the length of time before an IPv6 neighbor discovery cache entry expires.
Step 6	ipv6 nd na glean Example: Device(config-if)# ipv6 nd na glean	Configures the length of time before an IPv6 neighbor discovery cache entry expires.
Step 7	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.
Step 8	show ipv6 interface Example: Device# show ipv6 interface	(Optional) Displays the usability status of interfaces that are configured for IPv6 along with neighbor discovery cache management.

Examples: Customizing Parameters for IPv6 Neighbor Discovery

The following example shows that IPv6 neighbor advertisement gleaning is enabled and the IPv6 neighbor discovery cache expiry is set to 7200 seconds (2 hours):

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel 189
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:BD8::/64
Device(config-if)# ipv6 nd reachable-time 2700000
Device(config-if)# ipv6 nd na glean
Device(config-if)# ipv6 nd cache expire 7200
Device(config-if)# no ipv6 redirects
Device(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	See the <i>IP Addressing Services</i> section of <i>Command Reference (Catalyst 9200 Series Switches)</i>
For information on IPv6 Neighbor Discovery Inspection	See the <i>Security</i> section of <i>Software Configuration Guide (Catalyst 9200 Switches)</i>

Feature Information for IPv6 Neighbor Discovery

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.

Table 6: Feature Information for IPv6 Neighbor Discovery

Feature Name	Releases	Feature Information
Enhanced IPv6 Neighbor Discovery Cache Management	Cisco IOS XE Fuji 16.9.2	Neighbor discovery protocol enforces neighbor unreachability detection, which can detect failing nodes or routers, and changes to link-layer addresses.

