



First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Gibraltar 16.10.x

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Read Me First 1

Short Description 2

CHAPTER 2

Configuring GLBP 3

Finding Feature Information 3

Restrictions for GLBP 3

Prerequisites for GLBP 3

Information About GLBP 4

GLBP Overview 4

GLBP Active Virtual Gateway 4

GLBP Virtual MAC Address Assignment 5

GLBP Virtual Gateway Redundancy 5

GLBP Virtual Forwarder Redundancy 6

GLBP Gateway Priority 6

GLBP Gateway Weighting and Tracking 6

GLBP MD5 Authentication 7

ISSU-GLBP 7

GLBP SSO 8

GLBP Benefits 8

How to Configure GLBP 9

Enabling and Verifying GLBP 9

Customizing GLBP 11

Configuring GLBP MD5 Authentication Using a Key String 13

Configuring GLBP MD5 Authentication Using a Key Chain 14

Configuring GLBP Text Authentication 17

Configuring GLBP Weighting Values and Object Tracking 18

Troubleshooting GLBP	20
Configuration Examples for GLBP	22
Example: Customizing GLBP Configuration	22
Example: Configuring GLBP MD5 Authentication Using Key Strings	22
Example: Configuring GLBP MD5 Authentication Using Key Chains	22
Example: Configuring GLBP Text Authentication	22
Example: Configuring GLBP Weighting	23
Example: Enabling GLBP Configuration	23
Additional References for GLBP	23
Feature Information for GLBP	24
Glossary	24

CHAPTER 3
HSRP for IPv6 27

Finding Feature Information	27
Prerequisites for HSRP for IPv6	27
Information About HSRP for IPv6	28
HSRP for IPv6 Overview	28
HSRP IPv6 Virtual MAC Address Range	28
HSRP IPv6 UDP Port Number	28
How to Enable HSRP for IPv6	28
Enabling an HSRP Group for IPv6 Operation	28
Enabling HSRP Version 2	29
Enabling and Verifying an HSRP Group for IPv6 Operation	29
Configuration Examples for HSRP for IPv6	31
Example: Configuration and Verification for an HSRP Group	31
Additional References	33
Feature Information for HSRP for IPv6	34
Glossary	34

CHAPTER 4
Configuring HSRP 35

Finding Feature Information	35
Restrictions for HSRP	35
Information About HSRP	36
HSRP Operation	36

HSRP Version 2 Design	37
HSRP Configuration Changes	38
HSRP Benefits	38
HSRP Groups and Group Attributes	39
HSRP Preemption	39
HSRP Priority and Preemption	39
How Object Tracking Affects the Priority of an HSRP Device	40
HSRP Addressing	40
HSRP Virtual MAC Addresses and BIA MAC Addresses	40
HSRP Timers	41
HSRP MAC Refresh Interval	41
HSRP Text Authentication	41
HSRP MD5 Authentication	41
HSRP Support for IPv6	42
HSRP Messages and States	43
HSRP Group Linking to IP Redundancy Clients	43
HSRP Object Tracking	43
HSRP Group Shutdown	44
HSRP Support for ICMP Redirect Messages	44
ICMP Redirects to Active HSRP Devices	44
ICMP Redirects to Passive HSRP Devices	46
ICMP Redirects to Non-HSRP Devices	46
Passive HSRP Advertisement Messages	46
ICMP Redirects Not Sent	46
HSRP Support for MPLS VPNs	47
HSRP Multiple Group Optimization	47
HSRP—ISSU	48
SSO HSRP	48
SSO Dual-Route Processors and Cisco Nonstop Forwarding	48
HSRP and SSO Working Together	48
HSRP BFD Peering	49
HSRP MIB Traps	50
How to Configure HSRP	50
Enabling HSRP	50

Delaying the Initialization of HSRP on an Interface	52
Configuring HSRP Priority and Preemption	54
Configuring HSRP Object Tracking	55
Configuring HSRP MD5 Authentication Using a Key String	57
Configuring HSRP MD5 Authentication Using a Key Chain	59
Troubleshooting HSRP MD5 Authentication	62
Configuring HSRP Text Authentication	62
Configuring HSRP Timers	64
Configuring an HSRP MAC Refresh Interval	65
Configuring Multiple HSRP Groups for Load Balancing	66
Improving CPU and Network Performance with HSRP Multiple Group Optimization	68
Enabling HSRP Support for ICMP Redirect Messages	70
Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses	71
Linking IP Redundancy Clients to HSRP Groups	72
Changing to HSRP Version 2	73
Enabling SSO Aware HSRP	75
Verifying SSO Aware HSRP	76
Enabling HSRP MIB Traps	77
Configuring BFD Session Parameters on an Interface	78
Configuring HSRP BFD Peering	79
Verifying HSRP BFD Peering	81
Configuration Examples for HSRP	83
Example: Configuring HSRP Priority and Preemption	83
Example: Configuring HSRP Object Tracking	83
Example: Configuring HSRP Group Shutdown	84
Example: Configuring HSRP MD5 Authentication Using Key Strings	85
Example: Configuring HSRP MD5 Authentication Using Key Chains	85
Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains	85
Example: Configuring HSRP Text Authentication	86
Example: Configuring Multiple HSRP Groups for Load Balancing	86
Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization	87
Example: Configuring HSRP Support for ICMP Redirect Messages	88
Example: Configuring HSRP Virtual MAC Addresses and BIA MAC Address	88
Example: Linking IP Redundancy Clients to HSRP Groups	89

Example: Configuring HSRP Version 2	89
Example: Enabling SSO-Aware HSRP	90
Example: Enabling HSRP MIB Traps	90
Example: HSRP BFD Peering	90
Additional References	91
Feature Information for HSRP	92
Glossary	93

CHAPTER 5**HSRP Version 2 95**

Finding Feature Information	95
Information About HSRP Version 2	95
HSRP Version 2 Design	95
How to Configure HSRP Version 2	96
Changing to HSRP Version 2	96
Configuration Examples for HSRP Version 2	98
Example: Configuring HSRP Version 2	98
Additional References	98
Feature Information for HSRP Version 2	99

CHAPTER 6**HSRP MD5 Authentication 101**

Finding Feature Information	101
Information About HSRP MD5 Authentication	101
HSRP Text Authentication	101
HSRP MD5 Authentication	102
How to Configure HSRP MD5 Authentication	102
Configuring HSRP MD5 Authentication Using a Key Chain	102
Troubleshooting HSRP MD5 Authentication	105
Configuring HSRP Text Authentication	105
Configuration Examples for HSRP MD5 Authentication	107
Example: Configuring HSRP MD5 Authentication Using Key Strings	107
Example: Configuring HSRP MD5 Authentication Using Key Chains	107
Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains	108
Example: Configuring HSRP Text Authentication	108
Additional References	108

Feature Information for HSRP MD5 Authentication 109

CHAPTER 7

HSRP Support for ICMP Redirects 111

Finding Feature Information 111

Information About HSRP Support for ICMP Redirects 111

HSRP Support for ICMP Redirect Messages 111

ICMP Redirects to Active HSRP Devices 112

ICMP Redirects to Passive HSRP Devices 113

ICMP Redirects to Non-HSRP Devices 113

Passive HSRP Advertisement Messages 113

ICMP Redirects Not Sent 114

How to Configure HSRP Support for ICMP Redirects 114

Enabling HSRP Support for ICMP Redirect Messages 114

Configuration Examples for HSRP Support for ICMP Redirects 115

Example: Configuring HSRP Support for ICMP Redirect Messages 115

Additional References 116

Feature Information for HSRP Support for ICMP Redirects 117

CHAPTER 8

FHRP - HSRP Multiple Group Optimization 119

Finding Feature Information 119

Information About FHRP - Multiple Group Optimization 119

HSRP Multiple Group Optimization 119

How to configure FHRP - Multiple Group Optimization 120

Configuring Multiple HSRP Groups for Load Balancing 120

Improving CPU and Network Performance with HSRP Multiple Group Optimization 121

Configuration Examples for FHRP - Multiple Group Optimization 123

Example: Configuring Multiple HSRP Groups for Load Balancing 123

Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization 125

Additional References 125

Feature Information for FHRP - HSRP Multiple Group Optimization 126

CHAPTER 9

FHRP - HSRP Group Shutdown 127

Finding Feature Information 127

Information About FHRP - HSRP Group Shutdown 127

How Object Tracking Affects the Priority of an HSRP Device	127
HSRP Object Tracking	127
HSRP Group Shutdown	128
How to Configure FHRP - HSRP Group Shutdown	128
Configuring HSRP Object Tracking	128
Configuring HSRP MD5 Authentication Using a Key String	130
Configuration Examples for FHRP - HSRP Group Shutdown	132
Example: Configuring HSRP Object Tracking	132
Example: Configuring HSRP Group Shutdown	133
Additional References	134
Feature Information for FHRP - HSRP Group Shutdown	135

CHAPTER 10
SSO HSRP 137

Finding Feature Information	137
Restrictions for SSO HSRP	137
Information About SSO HSRP	137
SSO HSRP	137
SSO Dual-Route Processors and Cisco Nonstop Forwarding	138
HSRP and SSO Working Together	138
How to Configure SSO HSRP	138
Enabling SSO Aware HSRP	138
Verifying SSO Aware HSRP	140
Configuration Examples for SSO HSRP	141
Example: Enabling SSO-Aware HSRP	141
Additional References	141
Feature Information for SSO - HSRP	143

CHAPTER 11
HSRP - ISSU 145

Finding Feature Information	145
Information About HSRP - ISSU	145
HSRP—ISSU	145
Additional References	146
Feature Information for HSRP - ISSU	147

CHAPTER 12	FHRP - HSRP MIB	149
	Finding Feature Information	149
	Information About FHRP - HSRP MIB	149
	HSRP MIB Traps	149
	How to Configure FHRP - HSRP MIB	150
	Enabling HSRP MIB Traps	150
	Configuration Examples for FHRP - HSRP MIB	151
	Example: Enabling HSRP MIB Traps	151
	Additional References	151
	Feature Information for FHRP - HSRP-MIB	152

CHAPTER 13	HSRP Support for MPLS VPNs	153
	Finding Feature Information	153
	Information About HSRP Support for MPLS VPNs	153
	HSRP Support for MPLS VPNs	153
	Additional References	154
	Feature Information for HSRP Support for MPLS VPNs	155

CHAPTER 14	Configuring VRRP	157
	Finding Feature Information	157
	Restrictions for VRRP	157
	Information About VRRP	158
	VRRP Operation	158
	VRRP Benefits	160
	Multiple Virtual Router Support	161
	VRRP Router Priority and Preemption	161
	VRRP Advertisements	162
	VRRP Object Tracking	162
	How VRRP Object Tracking Affects the Priority of a Device	162
	In Service Software Upgrade--VRRP	163
	VRRP Support for Stateful Switchover	163
	How to Configure VRRP	163
	VRRP	163

Enabling/Verifying VRRP	165
Configuring VRRP Object Tracking	167
Configuring VRRP Text Authentication	168
Configuration Examples for VRRPv2	170
Example: Configuring VRRP	170
Example: VRRP Object Tracking	171
Example: VRRP Object Tracking Verification	171
Example: VRRP Text Authentication	172
Example: VRRP MIB Trap	172
Additional References	172
Feature Information for VRRP	173
Glossary	173

CHAPTER 15**VRRPv3 Protocol Support 175**

Finding Feature Information	175
Restrictions for VRRPv3 Protocol Support	176
Information About VRRPv3 Protocol Support	176
VRRPv3 Benefits	176
VRRP Device Priority and Preemption	177
VRRP Advertisements	178
How to Configure VRRPv3 Protocol Support	178
IPv6 VRRP Link Local Address	178
Enabling VRRPv3 on a Device	178
Creating and Customizing a VRRP Group	179
Configuring the Delay Period Before FHRP Client Initialization	181
Configuration Examples for VRRPv3 Protocol Support	182
Example: Enabling VRRPv3 on a Device	182
Example: Creating and Customizing a VRRP Group	183
Example: Configuring the Delay Period Before FHRP Client Initialization	183
Example: VRRP Status, Configuration, and Statistics Details	183
Additional References for VRRPv3 Protocol Support	184
Feature Information for VRRPv3 Protocol Support	185
Glossary	185

CHAPTER 16	VRRPv3: Object Tracking Integration	187
	Finding Feature Information	187
	Information About VRRPv3: Object Tracking Integration	187
	VRRP Object Tracking	187
	How VRRP Object Tracking Affects the Priority of a Device	188
	How to Configure VRRPv3: Object Tracking Integration	188
	Tracking an IPv6 Object using VRRPv3	188
	Configuration Examples for VRRPv3: Object Tracking Integration	189
	Example: Tracking an IPv6 Object using VRRPv3	189
	Example: Verifying VRRP IPv6 Object Tracking	189
	Additional References for VRRPv3: Object Tracking Integration	190
	Feature Information for VRRPv3: Object Tracking Integration	191

CHAPTER 17	Virtual Router Redundancy Service	193
	Finding Feature Information	193
	Restrictions for VRRS	194
	Information About VRRS	194
	VRRS Overview	194
	Using VRRS with VRRP	194
	VRRS Servers and Clients	195
	VRRS Pathways and Pathway Manager	195
	VRRS Pathways	195
	VRRS Pathway Manager	195
	How to Configure VRRS	196
	Configuring VRRPv3 Control Groups	196
	Configuring VRRS Pathways	197
	Verifying VRRS	199
	Configuration Examples for VRRS	202
	Example: Configuring VRRPv3 Control Groups	202
	Example: Configuring VRRS pathways	202
	Additional References	202
	Feature Information for Virtual Router Redundancy Service	203



CHAPTER 1

Read Me First

Important Information



Note For CUBE feature support information in Cisco IOS XE Bengaluru 17.6.1a and later releases, see [Cisco Unified Border Element IOS-XE Configuration Guide](#).



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

- [Short Description, on page 2](#)

Short Description

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



CHAPTER 2

Configuring GLBP

Gateway Load Balancing Protocol (GLBP) protects data traffic from a failed device or circuit, like Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP), while allowing packet load sharing between a group of redundant devices.

- [Finding Feature Information, on page 3](#)
- [Restrictions for GLBP, on page 3](#)
- [Prerequisites for GLBP, on page 3](#)
- [Information About GLBP, on page 4](#)
- [How to Configure GLBP, on page 9](#)
- [Configuration Examples for GLBP, on page 22](#)
- [Additional References for GLBP, on page 23](#)
- [Feature Information for GLBP, on page 24](#)
- [Glossary, on page 24](#)

Finding Feature Information

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

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

Restrictions for GLBP

Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with GLBP in SSO mode.

Prerequisites for GLBP

Before configuring GLBP, ensure that the devices can support multiple MAC addresses on the physical interfaces. For each GLBP forwarder to be configured, an additional MAC address is used.

Information About GLBP

GLBP Overview

GLBP provides automatic device backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop devices on the LAN combine to offer a single virtual first-hop IP device while sharing the IP packet forwarding load. Other devices on the LAN act as redundant GLBP devices that will become active if any of the existing forwarding devices fail.

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple devices to participate in a virtual device group configured with a virtual IP address. One member is elected to be the active device to forward packets sent to the virtual IP address for the group. The other devices in the group are redundant until the active device fails. These standby devices have unused bandwidth that the protocol is not using. Although multiple virtual device groups can be configured for the same set of devices, the hosts must be configured for different default gateways, which results in an extra administrative burden. The advantage of GLBP is that it additionally provides load balancing over multiple devices (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all devices in a GLBP group rather than being handled by a single device while the other devices stand idle. Each host is configured with the same virtual IP address, and all devices in the virtual device group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, UDP port 3222 (source and destination).

GLBP Packet Types

GLBP uses 3 different packet types to operate. The packet types are Hello, Request, and Reply. The Hello packet is used to advertise protocol information. Hello packets are multicast, and are sent when any virtual gateway or virtual forwarder is in Speak, Standby or Active state. Request and Reply packets are used for virtual MAC assignment. They are both unicast messages to and from the active virtual gateway (AVG).

GLBP Active Virtual Gateway

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG if the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

The AVG is also responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

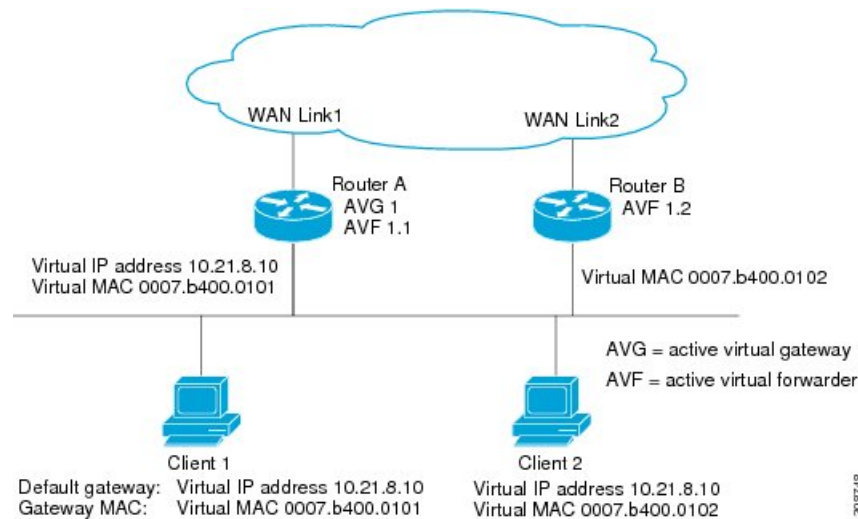
Prior to Cisco IOS Release 15.0(1)M1 and 12.4(24)T2, when the **no glbp load-balancing** command is configured, the AVG always responds to ARP requests with the MAC address of its AVF.

In Cisco IOS Release 15.0(1)M1 and 12.4(24)T2, and later releases, when the **no glbp load-balancing** command is configured, if the AVG does not have an AVF, it preferentially responds to ARP requests with the MAC address of the first listening virtual forwarder (VF), which will cause traffic to route via another gateway until that VF migrates back to being the current AVG.

In the figure below, Router A (or Device A) is the AVG for a GLBP group, and is responsible for the virtual IP address 10.21.8.10. Router A is also an AVF for the virtual MAC address 0007.b400.0101. Router B (or

Device B) is a member of the same GLBP group and is designated as the AVF for the virtual MAC address 0007.b400.0102. Client 1 has a default gateway IP address of 10.21.8.10 and a gateway MAC address of 0007.b400.0101. Client 2 shares the same default gateway IP address but receives the gateway MAC address 0007.b400.0102 because Router B is sharing the traffic load with Router A.

Figure 1: GLBP Topology



If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for the entire GLBP group. Communication for the GLBP members continues despite the failure of a device in the GLBP group.

GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

GLBP Virtual Gateway Redundancy

GLBP operates virtual gateway redundancy in the same way as HSRP. One gateway is elected as the AVG, another gateway is elected as the standby virtual gateway, and the remaining gateways are placed in a listen state.

If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IP address. A new standby virtual gateway is then elected from the gateways in the listen state.

GLBP Virtual Forwarder Redundancy

Virtual forwarder redundancy is similar to virtual gateway redundancy with an AVF. If the AVF fails, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

The new AVF is also a primary virtual forwarder for a different forwarder number. GLBP migrates hosts away from the old forwarder number using two timers that start as soon as the gateway changes to the active virtual forwarder state. GLBP uses the hello messages to communicate the current state of the timers.

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When the redirect time expires, the AVG stops using the old virtual forwarder MAC address in ARP replies, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

The secondary holdtime is the interval during which the virtual forwarder is valid. When the secondary holdtime expires, the virtual forwarder is removed from all gateways in the GLBP group. The expired virtual forwarder number becomes eligible for reassignment by the AVG.

GLBP Gateway Priority

GLBP gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails.

Priority also determines if a GLBP device functions as a backup virtual gateway and the order of ascendancy to becoming an AVG if the current AVG fails. You can configure the priority of each backup virtual gateway with a value of 1 through 255 using the **glbp priority** command.

In the "GLBP Topology" figure, if Router A (or Device A)—the AVG in a LAN topology—fails, an election process takes place to determine which backup virtual gateway should take over. In this example, Router B (or Device B) is the only other member in the group so it will automatically become the new AVG. If another device existed in the same GLBP group with a higher priority, then the device with the higher priority would be elected. If both devices have the same priority, the backup virtual gateway with the higher IP address would be elected to become the active virtual gateway.

By default, the GLBP virtual gateway preemptive scheme is disabled. A backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. You can enable the GLBP virtual gateway preemptive scheme using the **glbp preempt** command. Preemption allows a backup virtual gateway to become the AVG, if the backup virtual gateway is assigned a higher priority than the current AVG.

GLBP Gateway Weighting and Tracking

GLBP uses a weighting scheme to determine the forwarding capacity of each device in the GLBP group. The weighting assigned to a device in the GLBP group can be used to determine whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets. Thresholds can be set to disable forwarding when the weighting for a GLBP group falls below a certain value, and when it rises above another threshold, forwarding is automatically reenabled.

The GLBP group weighting can be automatically adjusted by tracking the state of an interface within the device. If a tracked interface goes down, the GLBP group weighting is reduced by a specified value. Different interfaces can be tracked to decrement the GLBP weighting by varying amounts.

By default, the GLBP virtual forwarder preemptive scheme is enabled with a delay of 30 seconds. A backup virtual forwarder can become the AVF if the current AVF weighting falls below the low weighting threshold

for 30 seconds. You can disable the GLBP forwarder preemptive scheme using the **no glbp forwarder preempt** command or change the delay using the **glbp forwarder preempt delay minimum** command.

GLBP MD5 Authentication

GLBP MD5 authentication uses the industry-standard MD5 algorithm for improved reliability and security. MD5 authentication provides greater security than the alternative plain text authentication scheme and protects against spoofing software.

MD5 authentication allows each GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and, if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can either be given directly in the configuration using a key string or supplied indirectly through a key chain. The key string cannot exceed 100 characters in length.

A device will ignore incoming GLBP packets from devices that do not have the same authentication configuration for a GLBP group. GLBP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

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

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

ISSU-GLBP

GLBP supports In Service Software Upgrade (ISSU). ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.

ISSU provides the ability to upgrade or downgrade from one supported Cisco IOS release to another while continuing to forward packets and maintain sessions, thereby reducing planned outage time. The ability to upgrade or downgrade is achieved by running different software versions on the active RP and standby RP for a short period of time to maintain state information between RPs. This feature allows the system to switch over to a secondary RP running upgraded (or downgraded) software and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* in the *Cisco IOS High Availability Configuration Guide*

For detailed information about ISSU on the 7600 series devices, see the *ISSU and eFSU on Cisco 7600 Series Routers* document.

GLBP SSO

With the introduction of the GLBP SSO functionality, GLBP is stateful switchover (SSO) aware. GLBP can detect when a device is failing over to the secondary router processor (RP) and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Without SSO-awareness, if GLBP is deployed on a device with redundant RPs, a switchover of roles between the active RP and the standby RP results in the device relinquishing its activity as a GLBP group member and then rejoining the group as if it had been reloaded. The GLBP SSO feature enables GLBP to continue its activities as a group member during a switchover. GLBP state information between redundant RPs is maintained so that the standby RP can continue the device's activities within the GLBP during and after a switchover.

This feature is enabled by default. To disable this feature, use the **no glbp sso** command in global configuration mode.

For more information, see the *Stateful Switchover* document in the *Cisco IOS High Availability Configuration Guide*.

GLBP Benefits

Load Sharing

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

Multiple Virtual Devices

GLBP supports up to 1024 virtual devices (GLBP groups) on each physical interface of a device and up to four virtual forwarders per group.

Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway (AVG) with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.

Authentication

GLBP supports the industry-standard message digest 5 (MD5) algorithm for improved reliability, security, and protection against GLBP-spoofing software. A device within a GLBP group with a different authentication string than other devices will be ignored by other group members. You can alternatively use a simple text password authentication scheme between GLBP group members to detect configuration errors.

How to Configure GLBP

Enabling and Verifying GLBP

Perform this task to enable GLBP on an interface and verify its configuration and operation. GLBP is designed to be easy to configure. Each gateway in a GLBP group must be configured with the same group number, and at least one gateway in the GLBP group must be configured with the virtual IP address to be used by the group. All other required parameters can be learned.

Before you begin

If VLANs are in use on an interface, the GLBP group number must be different for each VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp group ip** [*ip-address* [**secondary**]]
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example:	Specifies an interface type and number, and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 5	glbp group ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# glbp 10 ip 10.21.8.10	Enables GLBP on an interface and identifies the primary IP address of the virtual gateway. <ul style="list-style-type: none"> • After you identify a primary IP address, you can use the glbp group ip command again with the secondary keyword to indicate additional IP addresses supported by this group.
Step 6	exit Example: Device(config-if)# exit	Exits interface configuration mode, and returns the device to global configuration mode.
Step 7	show glbp [<i>interface-type interface-number</i>] [<i>group</i>] [<i>state</i>] [brief] Example: Device(config)# show glbp 10	(Optional) Displays information about GLBP groups on a device. <ul style="list-style-type: none"> • Use the optional brief keyword to display a single line of information about each virtual gateway or virtual forwarder.

Example

In the following example, sample output is displayed about the status of the GLBP group, named 10, on the device:

```
Device# show glbp 10

GigabitEthernet0/0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication text "stringabc"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105
```

Customizing GLBP

Customizing the behavior of GLBP is optional. Be aware that as soon as you enable a GLBP group, that group is operating. It is possible that if you first enable a GLBP group before customizing GLBP, the device could take over control of the group and become the AVG before you have finished customizing the feature.

Therefore, if you plan to customize GLBP, it is a good idea to do so before enabling GLBP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp group timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp group timers redirect** *redirect timeout*
7. **glbp group load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp group priority** *level*
9. **glbp group preempt** [**delay minimum** *seconds*]
10. **glbp group name** *redundancy-name*
11. **exit**
12. **no glbp sso**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface fastethernet 0/0	Specifies an interface type and number, and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	glbp group timers [msec] <i>hellotime</i> [msec] <i>holdtime</i> Example:	Configures the interval between successive hello packets sent by the AVG in a GLBP group.

	Command or Action	Purpose
	Device(config-if)# glbp 10 timers 5 18	<ul style="list-style-type: none"> The <i>holdtime</i> argument specifies the interval in seconds before the virtual gateway and virtual forwarder information in the hello packet is considered invalid. The optional msec keyword specifies that the following argument will be expressed in milliseconds, instead of the default seconds.
Step 6	<p>glbp group timers redirect <i>redirect timeout</i></p> <p>Example:</p> <pre>Device(config-if)# glbp 10 timers redirect 1800 28800</pre>	<p>Configures the time interval during which the AVG continues to redirect clients to an AVF. The default is 600 seconds (10 minutes).</p> <ul style="list-style-type: none"> The <i>timeout</i> argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid. The default is 14,400 seconds (4 hours). <p>Note The zero value for the <i>redirect</i> argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, and the device fails, new hosts continue to be assigned to the failed device instead of being redirected to the backup.</p>
Step 7	<p>glbp group load-balancing [host-dependent round-robin weighted]</p> <p>Example:</p> <pre>Device(config-if)# glbp 10 load-balancing host-dependent</pre>	Specifies the method of load balancing used by the GLBP AVG.
Step 8	<p>glbp group priority <i>level</i></p> <p>Example:</p> <pre>Device(config-if)# glbp 10 priority 254</pre>	<p>Sets the priority level of the gateway within a GLBP group.</p> <ul style="list-style-type: none"> The default value is 100.
Step 9	<p>glbp group preempt [delay minimum <i>seconds</i>]</p> <p>Example:</p> <pre>Device(config-if)# glbp 10 preempt delay minimum 60</pre>	<p>Configures the device to take over as AVG for a GLBP group if it has a higher priority than the current AVG.</p> <ul style="list-style-type: none"> This command is disabled by default. Use the optional delay and minimum keywords and the <i>seconds</i> argument to specify a minimum delay interval in seconds before preemption of the AVG takes place.

	Command or Action	Purpose
Step 10	glbp group name <i>redundancy-name</i> Example: Device(config-if)# glbp 10 name abc123	Enables IP redundancy by assigning a name to the GLBP group. <ul style="list-style-type: none"> The GLBP redundancy client must be configured with the same GLBP group name so the redundancy client and the GLBP group can be connected.
Step 11	exit Example: Device(config-if)# exit	Exits interface configuration mode, and returns the device to global configuration mode.
Step 12	no glbp sso Example: Device(config)# no glbp sso	(Optional) Disables GLBP support of SSO.

Configuring GLBP MD5 Authentication Using a Key String

SUMMARY STEPS

- enable
- configure terminal
- interface *type number*
- ip address *ip-address mask* [secondary]
- glbp *group-number authentication md5 key-string* [0 | 7] *key*
- glbp *group-number ip* [*ip-address* [secondary]]
- Repeat Steps 1 through 6 on each device that will communicate.
- end
- show glbp

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	glbp <i>group-number authentication md5 key-string</i> [0 7] <i>key</i> Example: Device(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a	Configures an authentication key for GLBP MD5 authentication. <ul style="list-style-type: none"> • The key string cannot exceed 100 characters in length. • No prefix to the <i>key</i> argument or specifying 0 means the key is unencrypted. • Specifying 7 means the key is encrypted. The key-string authentication key will automatically be encrypted if the service password-encryption global configuration command is enabled.
Step 6	glbp <i>group-number ip</i> [<i>ip-address</i> [secondary]] Example: Device(config-if)# glbp 1 ip 10.0.0.10	Enables GLBP on an interface and identifies the primary IP address of the virtual gateway.
Step 7	Repeat Steps 1 through 6 on each device that will communicate.	—
Step 8	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 9	show glbp Example: Device# show glbp	(Optional) Displays GLBP information. <ul style="list-style-type: none"> • Use this command to verify your configuration. The key string and authentication type will be displayed if configured.

Configuring GLBP MD5 Authentication Using a Key Chain

Perform this task to configure GLBP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. GLBP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **glbp** *group-number authentication md5 key-chain name-of-chain*
11. **glbp** *group-number ip* [*ip-address* [**secondary**]]
12. Repeat Steps 1 through 10 on each device that will communicate.
13. **end**
14. **show glbp**
15. **show key chain**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	key chain <i>name-of-chain</i> Example: Device(config)# key chain glbp2	Enables authentication for routing protocols and identifies a group of authentication keys and enters key-chain configuration mode.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 100	Identifies an authentication key on a key chain. • The value for the <i>key-id</i> argument must be a number.
Step 5	key-string <i>string</i> Example: Device(config-keychain-key)# key-string abc123	Specifies the authentication string for a key and enters key-chain key configuration mode. • The value for the <i>string</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral.

	Command or Action	Purpose
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to key-chain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.
Step 8	interface <i>type number</i> Example: Device(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 9	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.21.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 10	glbp <i>group-number authentication md5 key-chain name-of-chain</i> Example: Device(config-if)# glbp 1 authentication md5 key-chain glbp2	Configures an authentication MD5 key chain for GLBP MD5 authentication. <ul style="list-style-type: none"> • The key chain name must match the name specified in Step 3.
Step 11	glbp <i>group-number ip [ip-address [secondary]]</i> Example: Device(config-if)# glbp 1 ip 10.21.0.12	Enables GLBP on an interface and identifies the primary IP address of the virtual gateway.
Step 12	Repeat Steps 1 through 10 on each device that will communicate.	—
Step 13	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 14	show glbp Example: Device# show glbp	(Optional) Displays GLBP information. <ul style="list-style-type: none"> • Use this command to verify your configuration. The key chain and authentication type will be displayed if configured.

	Command or Action	Purpose
Step 15	show key chain Example: Device# show key chain	(Optional) Displays authentication key information.

Configuring GLBP Text Authentication

Text authentication provides minimal security. Use MD5 authentication if security is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number authentication text string*
6. **glbp** *group-number ip* [*ip-address* [**secondary**]]
7. Repeat Steps 1 through 6 on each device that will communicate.
8. **end**
9. **show glbp**

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 5	glbp group-number authentication text string Example: Device(config-if)# glbp 10 authentication text stringxyz	Authenticates GLBP packets received from other devices in the group. <ul style="list-style-type: none"> If you configure authentication, all devices within the GLBP group must use the same authentication string.
Step 6	glbp group-number ip [ip-address [secondary]] Example: Device(config-if)# glbp 1 ip 10.0.0.10	Enables GLBP on an interface and identifies the primary IP address of the virtual gateway.
Step 7	Repeat Steps 1 through 6 on each device that will communicate.	—
Step 8	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 9	show glbp Example: Device# show glbp	(Optional) Displays GLBP information. <ul style="list-style-type: none"> Use this command to verify your configuration.

Configuring GLBP Weighting Values and Object Tracking

GLBP weighting is used to determine whether a GLBP group can act as a virtual forwarder. Initial weighting values can be set and optional thresholds specified. Interface states can be tracked and a decrement value set to reduce the weighting value if the interface goes down. When the GLBP group weighting drops below a specified value, the group will no longer be an active virtual forwarder. When the weighting rises above a specified value, the group can resume its role as an active virtual forwarder.

SUMMARY STEPS

- enable**
- configure terminal**
- track object-number interface type number {line-protocol | ip routing}**
- exit**
- interface type number**
- glbp group weighting maximum [lower lower] [upper upper]**
- glbp group weighting track object-number [decrement value]**
- glbp group forwarder preempt [delay minimum seconds]**
- exit**
- show track [object-number | brief] [interface [brief] | ip route [brief] | resolution | timers]**

DETAILED STEPS

	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> interface <i>type number</i> {line-protocol ip routing} Example: Device(config)# track 2 interface POS 6/0/0 ip routing	Configures an interface to be tracked where changes in the state of the interface affect the weighting of a GLBP gateway, and enters tracking configuration mode. <ul style="list-style-type: none"> • This command configures the interface and corresponding object number to be used with the glbp weighting track command. • The line-protocol keyword tracks whether the interface is up. The ip routing keywords also check that IP routing is enabled on the interface, and an IP address is configured.
Step 4	exit Example: Device(config-track)# exit	Returns to global configuration mode.
Step 5	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Enters interface configuration mode.
Step 6	glbp <i>group</i> weighting <i>maximum</i> [lower <i>lower</i>] [upper <i>upper</i>] Example: Device(config-if)# glbp 10 weighting 110 lower 95 upper 105	Specifies the initial weighting value, and the upper and lower thresholds, for a GLBP gateway.
Step 7	glbp <i>group</i> weighting track <i>object-number</i> [decrement <i>value</i>] Example: Device(config-if)# glbp 10 weighting track 2 decrement 5	Specifies an object to be tracked that affects the weighting of a GLBP gateway. <ul style="list-style-type: none"> • The <i>value</i> argument specifies a reduction in the weighting of a GLBP gateway when a tracked object fails.

	Command or Action	Purpose
Step 8	<p>glbp group forwarder preempt [delay minimum seconds]</p> <p>Example:</p> <pre>Device(config-if)# glbp 10 forwarder preempt delay minimum 60</pre>	<p>Configures the device to take over as AVF for a GLBP group if the current AVF for a GLBP group falls below its low weighting threshold.</p> <ul style="list-style-type: none"> • This command is enabled by default with a delay of 30 seconds. • Use the optional delay and minimum keywords and the <i>seconds</i> argument to specify a minimum delay interval in seconds before preemption of the AVF takes place.
Step 9	<p>exit</p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	Returns to privileged EXEC mode.
Step 10	<p>show track [object-number brief] [interface [brief] ip route [brief] resolution timers]</p> <p>Example:</p> <pre>Device# show track 2</pre>	Displays tracking information.

Troubleshooting GLBP

GLBP introduces five privileged EXEC mode commands to enable display of diagnostic output concerning various events relating to the operation of GLBP. The **debug condition glbp**, **debug glbp errors**, **debug glbp events**, **debug glbp packets**, and **debug glbp terse** commands are intended only for troubleshooting purposes because the volume of output generated by the software can result in severe performance degradation on the device. Perform this task to minimize the impact of using the **debug glbp** commands.

This procedure will minimize the load on the device created by the **debug condition glbp** or **debug glbp** command because the console port is no longer generating character-by-character processor interrupts. If you cannot connect to a console directly, you can run this procedure via a terminal server. If you must break the Telnet connection, however, you may not be able to reconnect because the device may be unable to respond due to the processor load of generating the debugging output.

Before you begin

This task requires a device running GLBP to be attached directly to a console.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Use Telnet to access a device port and repeat Steps 1 and 2.
5. **end**
6. **terminal monitor**

7. **debug condition glbp** *interface-type interface-number group [forwarder]*
8. **terminal no monitor**

DETAILED STEPS

	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	no logging console Example: Device(config)# no logging console	Disables all logging to the console terminal. <ul style="list-style-type: none"> • To reenble logging to the console, use the logging console command in global configuration mode.
Step 4	Use Telnet to access a device port and repeat Steps 1 and 2.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 5	end Example: Device(config)# end	Exits to privileged EXEC mode.
Step 6	terminal monitor Example: Device# terminal monitor	Enables logging output on the virtual terminal.
Step 7	debug condition glbp <i>interface-type interface-number group [forwarder]</i> Example: Device# debug condition glbp GigabitEthernet0/0/0 1	Displays debugging messages about GLBP conditions. <ul style="list-style-type: none"> • Try to enter only specific debug condition glbp or debug glbp commands to isolate the output to a certain subcomponent and minimize the load on the processor. Use appropriate arguments and keywords to generate more detailed debug information on specified subcomponents. • Enter the specific no debug condition glbp or no debug glbp command when you are finished.
Step 8	terminal no monitor Example:	Disables logging on the virtual terminal.

	Command or Action	Purpose
	Device# terminal no monitor	

Configuration Examples for GLBP

Example: Customizing GLBP Configuration

```

Device(config)# interface fastethernet 0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 timers 5 18
Device(config-if)# glbp 10 timers redirect 1800 28800
Device(config-if)# glbp 10 load-balancing host-dependent
Device(config-if)# glbp 10 priority 254
Device(config-if)# glbp 10 preempt delay minimum 60

Device(config-if)# glbp 10 client-cache maximum 1200 timeout 245

```

Example: Configuring GLBP MD5 Authentication Using Key Strings

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

```

Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Device(config-if)# glbp 2 ip 10.0.0.10

```

Example: Configuring GLBP MD5 Authentication Using Key Chains

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

```

Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Device(config-if)# glbp 2 ip 10.0.0.10

```

Example: Configuring GLBP Text Authentication

```

Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 authentication text stringxyz
Device(config-if)# glbp 10 ip 10.21.8.10

```

Example: Configuring GLBP Weighting

In the following example, the device is configured to track the IP routing state of the POS interface 5/0/0 and 6/0/0, an initial GLBP weighting with upper and lower thresholds is set, and a weighting decrement value of 10 is set. If POS interface 5/0/0 and 6/0/0 go down, the weighting value of the device is reduced.

```
Device(config)# track 1 interface POS 5/0/0 ip routing
Device(config)# track 2 interface POS 6/0/0 ip routing
Device(config)# interface fastethernet 0/0/0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1 decrement 10
Device(config-if)# glbp 10 weighting track 2 decrement 10
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

Example: Enabling GLBP Configuration

In the following example, the device is configured to enable GLBP, and the virtual IP address of 10.21.8.10 is specified for GLBP group 10:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

Additional References for GLBP

Related Documents

Related Topic	Document Title
GLBP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS IP Application Services Command Reference
In Service Software Upgrade (ISSU) configuration	"In Service Software Upgrade" process module in the <i>Cisco IOS High Availability Configuration Guide</i>
Key chains and key management commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Routing Protocol-Independent Command Reference</i>
Object tracking	"Configuring Enhanced Object Tracking" module
Stateful Switchover	The "Stateful Switchover" module in the <i>Cisco IOS High Availability Configuration Guide</i>
VRRP	"Configuring VRRP" module
HSRP	"Configuring HSRP" module
GLBP Support for IPv6	"FHRP - GLBP Support for IPv6" module

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 GLBP

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.

Glossary

active RP—The Route Processor (RP) controls the system, provides network services, runs routing protocols and presents the system management interface.

AVF—active virtual forwarder. One virtual forwarder within a GLBP group is elected as active virtual forwarder for a specified virtual MAC address, and it is responsible for forwarding packets sent to that MAC address. Multiple active virtual forwarders can exist for each GLBP group.

AVG—active virtual gateway. One virtual gateway within a GLBP group is elected as the active virtual gateway, and is responsible for the operation of the protocol.

GLBP gateway—Gateway Load Balancing Protocol gateway. A router or gateway running GLBP. Each GLBP gateway may participate in one or more GLBP groups.

GLBP group—Gateway Load Balancing Protocol group. One or more GLBP gateways configured with the same GLBP group number on connected Ethernet interfaces.

ISSU—In Service Software Upgrade. A process that allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

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

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

RPR—Route Processor Redundancy. RPR provides an alternative to the High System Availability (HSA) feature. HSA enables a system to reset and use a standby Route Processor (RP) if the active RP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RP if the active RP experiences a fatal error.

RPR+—An enhancement to RPR in which the standby RP is fully initialized.

SSO—Stateful Switchover. Enables applications and features to maintain state information between an active and standby unit.

standby RP—An RP that has been fully initialized and is ready to assume control from the active RP should a manual or fault-induced switchover occur.

switchover—An event in which system control and routing protocol execution are transferred from the active RP to the standby RP. Switchover may be a manual operation or may be induced by a hardware or software fault. Switchover may include transfer of the packet forwarding function in systems that combine system control and packet forwarding in an indivisible unit.

vIP—virtual IP address. An IPv4 address. There must be only one virtual IP address for each configured GLBP group. The virtual IP address must be configured on at least one GLBP group member. Other GLBP group members can learn the virtual IP address from hello messages.



CHAPTER 3

HSRP for IPv6

IPv6 routing protocols ensure device-to-device resilience and failover. However, in situations in which the path between a host and the first-hop device fails, or the first-hop device itself fails, first hop redundancy protocols (FHRPs) ensure host-to-device resilience and failover.

The Hot Standby Router Protocol (HSRP) protects data traffic in case of a gateway failure.

- [Finding Feature Information, on page 27](#)
- [Prerequisites for HSRP for IPv6, on page 27](#)
- [Information About HSRP for IPv6, on page 28](#)
- [How to Enable HSRP for IPv6, on page 28](#)
- [Configuration Examples for HSRP for IPv6, on page 31](#)
- [Additional References, on page 33](#)
- [Feature Information for HSRP for IPv6, on page 34](#)
- [Glossary, on page 34](#)

Finding Feature Information

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

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

Prerequisites for HSRP for IPv6

HSRP version 2 must be enabled on an interface before HSRP for IPv6 can be configured.

Information About HSRP for IPv6

HSRP for IPv6 Overview

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

IPv6 hosts learn of available IPv6 devices through IPv6 neighbor discovery RA messages. These are multicast periodically, or may be solicited by hosts. HSRP is designed to provide only a virtual first hop for IPv6 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 RAs are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent when the group leaves the active state.

Periodic RAs for the interface link-local address stop after a final RA is sent while at least one virtual IPv6 link-local address is configured on the interface. No restrictions occur for the interface IPv6 link-local address other than that mentioned for the RAs. Other protocols continue to receive and send packets to this address.

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

HSRP IPv6 Virtual MAC Address Range

HSRP IPv6 uses a different virtual MAC address block than does HSRP for IP:

0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses)

HSRP IPv6 UDP Port Number

Port number 2029 has been assigned to HSRP IPv6.

How to Enable HSRP for IPv6

Enabling an HSRP Group for IPv6 Operation

HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

Enabling HSRP Version 2

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby version** {1 | 2}

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	standby version {1 2} Example: Device(config-if)# standby version 2	Changes the version of the HSRP. <ul style="list-style-type: none"> • Version 1 is the default.

Enabling and Verifying an HSRP Group for IPv6 Operation

In this task, when you enter the **standby ipv6** command, a link-local address is generated from the link-local prefix, and a modified EUI-64 format interface identifier is generated in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are used in the stateless autoconfiguration process. Nodes on a local link can use link-local addresses to communicate; the nodes do not need site-local or globally unique addresses to communicate.

In IPv6, a device on the link advertises in RA messages any site-local and global prefixes, and its willingness to function as a default device for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure site-local and global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the

link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}
6. **standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*]
7. **standby** [*group-number*] **priority** *priority*
8. **exit**
9. **show standby** [*type number* [*group*]] [**all** | **brief**]
10. **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 unicast-routing Example: Device(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams. • The ipv6 unicast-routing command must be enabled for HSRP for IPv6 to work.
Step 4	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	standby [<i>group-number</i>] ipv6 { <i>link-local-address</i> autoconfig }	Activates the HSRP in IPv6.
	Example: Device(config-if)# standby 1 ipv6 autoconfig	

	Command or Action	Purpose
Step 6	standby [<i>group-number</i>] preempt [delay minimum <i>seconds</i> reload <i>seconds</i> sync <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption and preemption delay.
Step 7	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 8	exit Example: Device(config-if)# exit	Returns the device to privileged EXEC mode.
Step 9	show standby [<i>type number</i> [<i>group</i>]] [all brief] Example: Device# show standby	Displays HSRP information.
Step 10	show ipv6 interface [brief] [<i>interface-type</i> <i>interface-number</i>] [prefix] Example: Device# show ipv6 interface GigabitEthernet 0/0/0	Displays the usability status of interfaces configured for IPv6.

Configuration Examples for HSRP for IPv6

Example: Configuration and Verification for an HSRP Group

The following example shows configuration and verification for an HSRP group for IPv6 that consists of Device1 and Device2. The **show standby** command is issued for each device to verify the device's configuration:

Device 1 configuration

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
```

```

standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Device1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)

```

Device 2 configuration

```

interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese
Device2# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)

```

```

Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VRRP commands	<i>Cisco IOS IP Application Services Command Reference</i>
Object tracking	Configuring Enhanced Object Tracking
Hot Standby Routing Protocol (HSRP)	Configuring HSRP
In Service Software Upgrade (ISSU)	"In Service Software Upgrade Process" in the <i>High Availability Configuration Guide</i>
Gateway Load Balancing Protocol (GLBP)	Configuring GLBP
Stateful Switchover	The Stateful Switchover section in the <i>High Availability Configuration Guide</i>

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 2338	Virtual Router Redundancy Protocol
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768	Virtual Router Redundancy Protocol (VRRP)

Technical Assistance

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

Feature Information for HSRP for IPv6

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.

Glossary

- **CPE** --Customer premises equipment
- **FHRP** --First hop redundancy protocol
- **GLBP** --Gateway load balancing protocol
- **HSRP** --Hot standby routing protocol
- **NA** --Neighbor advertisement
- **ND** --Neighbor Discovery
- **NS** --Neighbor solicitation
- **PE** --Provider equipment
- **RA** --Router advertisement
- **RS** --Router solicitation



CHAPTER 4

Configuring HSRP

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

- [Finding Feature Information, on page 35](#)
- [Restrictions for HSRP, on page 35](#)
- [Information About HSRP, on page 36](#)
- [How to Configure HSRP, on page 50](#)
- [Configuration Examples for HSRP, on page 83](#)
- [Additional References, on page 91](#)
- [Feature Information for HSRP, on page 92](#)
- [Glossary, on page 93](#)

Finding Feature Information

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

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

Restrictions for HSRP

- HSRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. HSRP is not intended as a replacement for existing dynamic protocols.

Information About HSRP

HSRP Operation

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

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

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

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

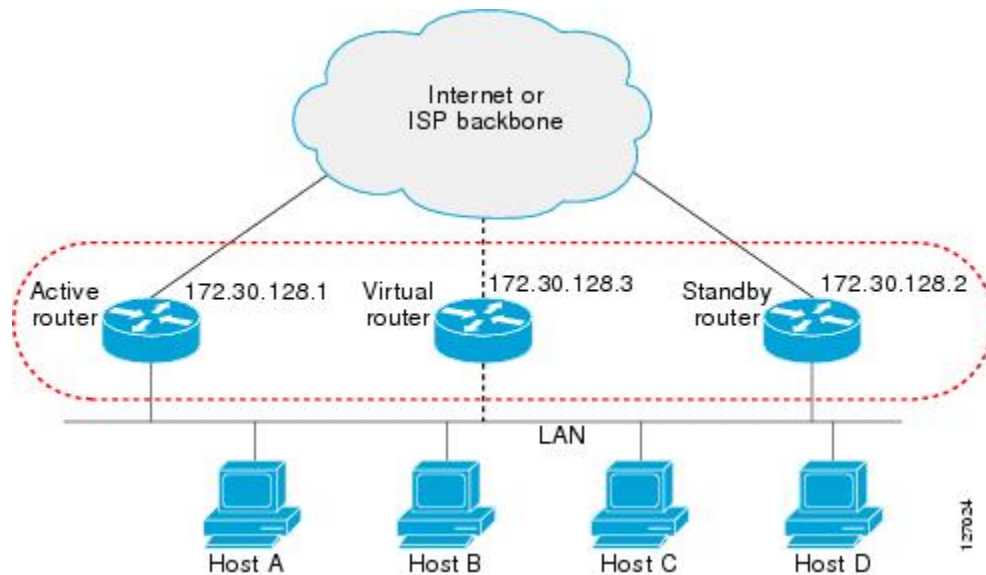
HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure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

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

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

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

Figure 2: HSRP Topology



HSRP Version 2 Design

HSRP version 2 is designed to address the following restrictions in HSRP version 1:

- In HSRP version 1, millisecond timer values are not advertised or learned. HSRP version 2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
- HSRP version 2 provides improved management and troubleshooting. With HSRP version 1, you cannot use HSRP active hello messages to identify which physical device sent the message because the source MAC address is the HSRP virtual MAC address. The HSRP version 2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.
- The multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing.

Version 1 is the default version of HSRP.

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

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF. The increased group number range does not imply that an interface can, or should, support that many HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

HSRP version 2 has a different packet format than HSRP version 1. The packet format uses a type-length-value (TLV) format. HSRP version 2 packets received by an HSRP version 1 device will have the type field mapped to the version field by HSRP version 1 and subsequently ignored.

The Gateway Load Balancing Protocol (GLBP) also addresses the same restrictions relative to HSRP version 1 that HSRP version 2 does. See the *Configuring GLBP* document for more information on GLBP.

Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

HSRP Configuration Changes

With CSCsv12265, an HSRP group may be configured with a virtual IP address that matches the subnet of an IP address of a secondary interface.

When the virtual IP address of an HSRP group is configured with the same network ID as a secondary interface IP address, the source address of HSRP messages is automatically set to the most appropriate interface address. This configuration change allows the following configuration:

```
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 secondary
 standby 1 ip 192.168.1.254
 standby 1 priority 105
 standby 1 preempt
 standby 2 ip 192.168.2.254 !Same network ID as secondary interface
```

Prior to CSCsv12265, an HSRP group remained in INIT state unless the HSRP virtual IP address had the same network ID as the primary interface address.

In addition, the following warning message is displayed if an HSRP group address is configured when no interface addresses are configured:

```
% Warning: address is not within a subnet on this interface
```

HSRP Benefits

Redundancy

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

Fast Failover

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

Preemption

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

Authentication

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

HSRP Groups and Group Attributes

You can use the CLI to apply group attributes to:

- A single HSRP group—performed in interface configuration mode and applies to a group.
- All groups on the interface—performed in interface configuration mode and applies to all groups on the interface.
- All groups on all interfaces—performed in global configuration mode and applies to all groups on all interfaces.

HSRP Preemption

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

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

In general, we recommend that all HSRP devices have the following configuration:

standby delay minimum 30 reload 60

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

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

HSRP Priority and Preemption

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

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

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

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

How Object Tracking Affects the Priority of an HSRP Device

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

HSRP Addressing

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

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

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

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

HSRP Virtual MAC Addresses and BIA MAC Addresses

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

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

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

HSRP Timers

For HSRP version 1, nonactive devices learn timer values from the active device, unless millisecond timer values are being used. If millisecond timer values are being used, all devices must be configured with the millisecond timer values. This rule applies if either the hello time or the hold time is specified in milliseconds. This configuration is necessary because the HSRP hello packets advertise the timer values in seconds. HSRP version 2 does not have this limitation; it advertises the timer values in milliseconds.

Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

HSRP MAC Refresh Interval

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

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

HSRP Text Authentication

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

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

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

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

HSRP MD5 Authentication

Before the introduction of HSRP MD5 authentication, HSRP authenticated protocol packets with a simple plain text string. HSRP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP

portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

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

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

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

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

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

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

HSRP Support for IPv6

Most IPv4 hosts have a single router's IP address configured as the default gateway. When HSRP is used, then the HSRP virtual IP address is configured as the host's default gateway instead of the router's IP address. Simple load sharing may be achieved by using two HSRP groups and configuring half the hosts with one virtual IP address and half the hosts with the other virtual IP address.

In contrast, IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery Router Advertisement (RA) messages. These are multicast periodically, or may be solicited by hosts. HSRP is designed to provide only a virtual first hop for IPv6 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. HSRP IPv6 uses the MAC address range 0005.73A0.0000 to 0005.73A0.0FFF. Periodic RAs are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent when the group leaves the active state.

Periodic RAs for the interface link-local address stop after a final RA is sent while at least one virtual IPv6 link-local address is configured on the interface. No restrictions occur for the interface IPv6 link-local address other than that mentioned for the RAs. Other protocols continue to receive and send packets to this address.

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

For more information see the "Configuring First Hop Redundancy Protocols in IPv6" chapter of the *Cisco IOS IPv6 Configuration Guide*.

HSRP Messages and States

Devices configured with HSRP exchange three types of multicast messages:

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

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

- **Active**—The device is performing packet-transfer functions.
- **Init or Disabled**—The device is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other devices on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state.
- **Learn**—The device has not determined the virtual IP address and has not yet seen an authenticated hello message from the active device. In this state, the device still waits to hear from the active device.
- **Listen**—The device is receiving hello messages.
- **Speak**—The device is sending and receiving hello messages.
- **Standby**—The device is prepared to assume packet-transfer functions if the active device fails.

HSRP uses logging Level 5 for syslog messages related to HSRP state changes to allow logging of an event without filling up the syslog buffer on the device with low-priority Level 6 messaging.

HSRP Group Linking to IP Redundancy Clients

HSRP provides stateless redundancy for IP routing. HSRP by itself is limited to maintaining its own state. Linking an IP redundancy client to an HSRP group provides a mechanism that allows HSRP to provide a service to client applications so they can implement stateful failover.

IP redundancy clients are other Cisco IOS processes or applications that use HSRP to provide or withhold a service or resource dependent upon the state of the group.

HSRP groups have a default name of **hsrp-interface-group** so specifying a group name is optional. For example, Group 1 on Ethernet0/0 has a default group name of "hsrp-Et0/0-1."

HSRP Object Tracking

Object tracking separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process as well as HSRP. The priority of a device can change dynamically when it has been configured for object tracking and the object that is being tracked goes down. Examples of

objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

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

For more information about object tracking, see the "Configuring Enhanced Object Tracking" document.

HSRP Group Shutdown

The HSRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down. Use the **standby track** command with the **shutdown** keyword to configure HSRP group shutdown.

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

HSRP Support for ICMP Redirect Messages

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

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

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

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.

ICMP Redirects to Active HSRP Devices

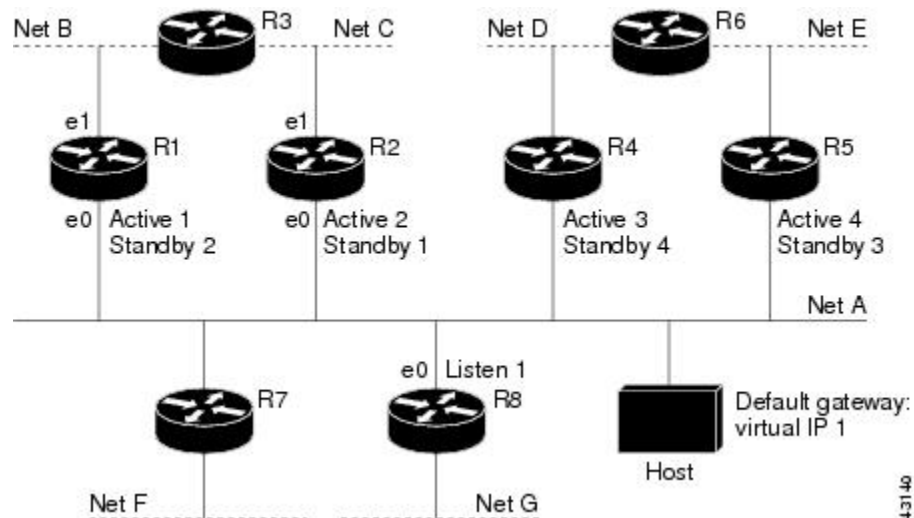
The next-hop IP address is compared to the list of active HSRP devices on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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

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

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

Figure 3: Network Supporting the HSRP ICMP Redirection Filter



If the host wants to send a packet to another host on Net D, then it first sends it to its default gateway, the virtual IP address of HSRP group 1.

The following is the packet received from the host:

```
dest MAC      = HSRP group 1 virtual MAC
source MAC    = Host MAC
dest IP       = host-on-netD IP
source IP     = Host IP
```

Device R1 receives this packet and determines that device R4 can provide a better path to Net D, so it prepares to send a redirect message that will redirect the host to the real IP address of device R4 (because only real IP addresses are in its routing table).

The following is the initial ICMP redirect message sent by device R1:

```
dest MAC      = Host MAC
source MAC    = router R1 MAC
dest IP       = Host IP
source IP     = router R1 IP
gateway to use = router R4 IP
```

Before this redirect occurs, the HSRP process of device R1 determines that device R4 is the active HSRP device for group 3, so it changes the next hop in the redirect message from the real IP address of device R4 to the virtual IP address of group 3. Furthermore, it determines from the destination MAC address of the packet that triggered the redirect message that the host used the virtual IP address of group 1 as its gateway, so it changes the source IP address of the redirect message to the virtual IP address of group 1.

The modified ICMP redirect message showing the two modified fields (*) is as follows:

```
dest MAC      = Host MAC
source MAC    = router R1 MAC
dest IP       = Host IP
source IP*    = HSRP group 1 virtual IP
gateway to use* = HSRP group 3 virtual IP
```

This second modification is necessary because hosts compare the source IP address of the ICMP redirect message with their default gateway. If these addresses do not match, the ICMP redirect message is ignored.

The routing table of the host now consists of the default gateway, virtual IP address of group 1, and a route to Net D through the virtual IP address of group 3.

ICMP Redirects to Passive HSRP Devices

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

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

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

ICMP Redirects to Non-HSRP Devices

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

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R7 is allowed because R7 is not running HSRP. In this case, the next hop IP address is unchanged. The source IP address is changed dependent upon the destination MAC address of the original packet. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

Passive HSRP Advertisement Messages

Passive HSRP devices send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP devices can determine the HSRP group state of any HSRP device on the network. These advertisements inform other HSRP devices on the network of the HSRP interface state, as follows:

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

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

ICMP Redirects Not Sent

If the HSRP device cannot uniquely determine the IP address used by the host when it sends the packet that caused the redirect, the redirect message will not be sent. The device uses the destination MAC address in the original packet to make this determination. In certain configurations, such as the use of the **standby use-bia** interface configuration command specified on an interface, redirects cannot be sent. In this case, the HSRP groups use the interface MAC address as their virtual MAC address. The device now cannot determine if the

default gateway of the host is the real IP address or one of the HSRP virtual IP addresses that are active on the interface.

The IP source address of an ICMP packet must match the gateway address used by the host in the packet that triggered the ICMP packet, otherwise the host will reject the ICMP redirect packet. An HSRP device uses the destination MAC address to determine the gateway IP address of the host. If the HSRP device is using the same MAC address for multiple IP addresses, uniquely determining the gateway IP address of the host is not possible, and the redirect message is not sent.

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

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

HSRP Support for MPLS VPNs

HSRP support for a Multiprotocol Label Switching (MPLS) VPN interface is useful when an Ethernet LAN is connected between two provider edge (PE) devices with either of the following conditions:

- A customer edge (CE) device with a default route to the HSRP virtual IP address
- One or more hosts with the HSRP virtual IP address configured as the default gateway

Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding table
- Set of interfaces that use the Cisco Express Forwarding forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of routing and Cisco Express Forwarding tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a device within the VPN.

HSRP adds ARP entries and IP hash table entries (aliases) using the default routing table instance. However, a different routing table instance is used when VRF forwarding is configured on an interface, causing ARP and ICMP echo requests for the HSRP virtual IP address to fail.

HSRP support for MPLS VPNs ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table.

HSRP Multiple Group Optimization

The configuration of many hundreds of subinterfaces on the same physical interface, with each subinterface having its own HSRP group, can cause the processes of negotiation and maintenance of multiple HSRP groups to have a detrimental impact on network traffic and CPU utilization.

Only one HSRP group is required on a physical interface for the purposes of electing active and standby devices. This group is known as the *primary* group. Other HSRP groups may be created on each subinterface

and linked to the primary group via the group name. These linked HSRP groups are known as *client* or *subordinate* groups.

The HSRP group state of the client groups follows that of the primary group. Client groups do not participate in any sort of device election mechanism.

Client groups send periodic messages in order to refresh their virtual MAC addresses in switches and learning bridges. The refresh message may be sent at a much lower frequency compared with the protocol election messages sent by the primary group.

HSRP—ISSU

The In Service Software Upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* document in the *High Availability Configuration Guide*.

SSO HSRP

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

With this functionality, HSRP SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP device, then the standby HSRP device takes over as the active HSRP device.

The feature is enabled by default when the redundancy mode of operation is set to SSO.

SSO Dual-Route Processors and Cisco Nonstop Forwarding

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

SSO is generally used with Cisco nonstop forwarding (NSF). Cisco NSF enables forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, users are less likely to experience service outages.

HSRP and SSO Working Together

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Prior to introduction of the SSO HSRP feature, when the primary RP of the active device failed, it would stop participating in the HSRP group and trigger another switch in the group to take over as the active HSRP switch.

SSO HSRP is required to preserve the forwarding path for traffic destined to the HSRP virtual IP address through an RP switchover.

Configuring SSO on the edge device enables the traffic on the Ethernet links to continue during an RP failover without the Ethernet traffic switching over to an HSRP standby device (and then back, if preemption is enabled).



Note You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

HSRP BFD Peering

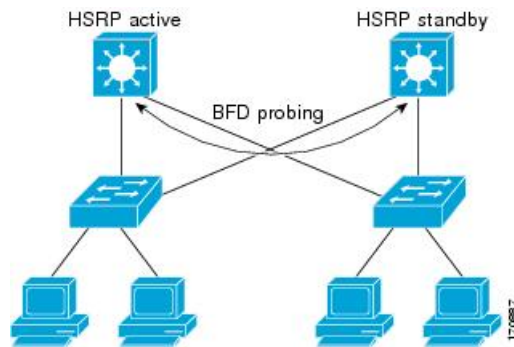
The HSRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the Hot Standby Router Protocol (HSRP) group member health monitoring system. HSRP supports BFD as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with hello and hold timers, in milliseconds. BFD runs as a pseudopreemptive process and can therefore be guaranteed to run when required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

This feature is enabled by default. The HSRP standby device learns the real IP address of the HSRP active device from the HSRP hello messages. The standby device registers as a BFD client and asks to be notified if the active device becomes unavailable. When BFD determines that the connections between standby and active devices has failed, it will notify HSRP on the standby device which will immediately take over as the active device.

BFD provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent devices, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, which depends on the sending of BFD control packets between two systems to activate and maintain BFD neighbor sessions between devices. Therefore, to create a BFD session, you must configure BFD on both systems (or BFD peers). When BFD is enabled on the interfaces and at the device level for HSRP, a BFD session is created, BFD timers are negotiated, and the BFD peers will begin to send BFD control packets to each other at the negotiated interval.

BFD provides fast BFD peer failure detection times independently of all media types, encapsulations, topologies, and routing protocols such as, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Hot Standby Router Protocol (HSRP), Intermediate System To Intermediate System (IS-IS), and Open Shortest Path First (OSPF). By sending rapid failure detection notices to the routing protocols in the local device to initiate the routing table recalculation process, BFD contributes to greatly reduce overall network convergence time. The figure below shows a simple network with two devices running HSRP and BFD.

Figure 4: HSRP BFD Peering



For more information about BFD, see the *IP Routing: BFD Configuration Guide*.

HSRP MIB Traps

HSRP MIB supports Simple Network Management Protocol (SNMP) Get operations, to allow network devices to get reports about HSRP groups in a network from the network management station.

Enabling HSRP MIB trap support is performed through the CLI, and the MIB is used for getting the reports. A trap notifies the network management station when a device leaves or enters the active or standby state. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

Cisco software supports a read-only version of the MIB, and set operations are not supported.

This functionality supports four MIB tables, as follows:

- cHsrpGrpEntry table defined in CISCO-HSRP-MIB.my
- cHsrpExtIfTrackedEntry, defined in CISCO-HSRP-EXT-MIB.my
- cHsrpExtSecAddrEntry, defined in CISCO-HSRP-EXT-MIB.my
- cHsrpExtIfEntry defined in CISCO-HSRP-EXT-MIB.my

The cHsrpGrpEntry table consists of all the group information defined in RFC 2281, *Cisco Hot Standby Router Protocol*; the other tables consist of the Cisco extensions to RFC 2281, which are defined in CISCO-HSRP-EXT-MIB.my.

How to Configure HSRP

Enabling HSRP

Perform this task to enable HSRP.

The **standby ip** interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the virtual IP address for the Hot Standby group. For HSRP to elect a designated device, you must configure the virtual IP address for at least one of the devices in the group; it can be learned on the other devices in the group.

Before you begin

You can configure many attributes in HSRP such as authentication, timers, priority, and preemption. You should configure the attributes before enabling the HSRP group. This practice avoids authentication error messages and unexpected state changes in other routers that can occur if the group is enabled first and then there is a long enough delay (one or two hold times) before the other attributes are configured.

We recommend that you always specify an HSRP IP address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **end**
7. **show standby** [**all**] [**brief**]
8. **show standby** *type number* [*group-number* | **all**] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 172.16.6.5 255.255.255.0	Configures an IP address for an interface.
Step 5	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 1 ip 172.16.6.100	Activates HSRP. <ul style="list-style-type: none"> • If you do not configure a group number, the default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.

	Command or Action	Purpose
		<ul style="list-style-type: none"> The value for the <i>ip-address</i> argument is the virtual IP address of the virtual device. For HSRP to elect a designated device, you must configure the virtual IP address for at least one of the devices in the group; it can be learned on the other devices in the group.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show standby [all] [brief] Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> This command displays information for each group. The all option displays groups that are learned or that do not have the standby ip command configured.
Step 8	show standby type number [group-number all] [brief] Example: Device# show standby GigabitEthernet 0	(Optional) Displays HSRP information about specific groups or interfaces.

Delaying the Initialization of HSRP on an Interface

The **standby delay** command is used to delay HSRP initialization either after a reload and/or after an interface comes up. This configuration allows the interface and device time to settle down after the interface up event and helps prevent HSRP state flapping.

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

SUMMARY STEPS

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

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 1/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies an IP address for an interface.
Step 5	standby delay minimum <i>min-seconds</i> reload <i>reload-seconds</i> Example: Device(config-if)# standby delay minimum 30 reload 60	(Optional) Configures the delay period before the initialization of HSRP groups. <ul style="list-style-type: none"> The <i>min-seconds</i> value is the minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events. The <i>reload-seconds</i> value is the time period to delay after the device has reloaded. This delay period applies only to the first interface-up event after the device has reloaded. <p>Note The recommended <i>min-seconds</i> value is 30 and the recommended <i>reload-seconds</i> value is 60.</p>
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [<i>secondary</i>]] Example: Device(config-if)# standby 1 ip 10.0.0.3 255.255.255.0	Activates HSRP.
Step 7	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 8	show standby delay [<i>typenumber</i>] Example:	(Optional) Displays HSRP information about delay periods.

	Command or Action	Purpose
	Device# show standby delay	

Configuring HSRP Priority and Preemption

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **ip** *ip-address* [**secondary**]
8. **end**
9. **show standby** [**all**] [**brief**]
10. **show standby** *type number* [*group-number* | **all**] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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>type number</i> Example: Device(config)# interface GigabitEthernet0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies an IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority. <ul style="list-style-type: none">• The default priority is 100.

	Command or Action	Purpose
Step 6	<p>standby [<i>group-number</i>] preempt [delay {minimum reload sync} <i>seconds</i>]</p> <p>Example:</p> <pre>Device(config-if)# standby 1 preempt delay minimum 380</pre>	<p>Configures HSRP preemption and preemption delay.</p> <ul style="list-style-type: none"> The default delay period is 0 seconds; if the device wants to preempt, it will do so immediately. By default, the device that comes up later becomes the standby.
Step 7	<p>standby [<i>group-number</i>] ip <i>ip-address</i> [secondary]</p> <p>Example:</p> <pre>Device(config-if)# standby 1 ip 10.0.0.3 255.255.255.0</pre>	<p>Activates HSRP.</p>
Step 8	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 9	<p>show standby [all] [brief]</p> <p>Example:</p> <pre>Device# show standby</pre>	<p>(Optional) Displays HSRP information.</p> <ul style="list-style-type: none"> This command displays information for each group. The all option displays groups that are learned or that do not have the standby ip command configured.
Step 10	<p>show standby <i>type number</i> [<i>group-number</i> all] [brief]</p> <p>Example:</p> <pre>Device# show standby GigabitEthernet 0/0/0</pre>	<p>(Optional) Displays HSRP information about specific groups or interfaces.</p>

Configuring HSRP Object Tracking

Perform this task to configure HSRP to track an object and change the HSRP priority based on the state of the object.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes use this number to track a specific object.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]
8. **end**

9. show track [object-number | brief] [interface [brief] | ip route [brief] | resolution | timers]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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 object-number interface type number {line-protocol ip routing} Example: Device(config)# track 100 interface GigabitEthernet 0/0/0 line-protocol	Configures an interface to be tracked and enters tracking configuration mode.
Step 4	exit Example: Device(config-track)# exit	Returns to global configuration mode.
Step 5	interface type number Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 6	standby [group-number] track object-number [decrement priority-decrement] [shutdown] Example: Device(config-if)# standby 1 track 100 decrement 20	Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object. <ul style="list-style-type: none"> • By default, the priority of the device is decreased by 10 if a tracked object goes down. Use the decrement priority-decrement keyword and argument combination to change the default behavior. • When multiple tracked objects are down and <i>priority-decrement</i> values have been configured, these configured priority decrements are cumulative. If tracked objects are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative. • Use the shutdown keyword to disable the HSRP group on the device when the tracked object goes down.

	Command or Action	Purpose
		<p>Note If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the no standby track command and then reconfigure it using the standby track command with the shutdown keyword.</p>
Step 7	<p>standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]]</p> <p>Example:</p> <pre>Device(config-if)# standby 1 ip 10.10.10.0</pre>	<p>Activates HSRP.</p> <ul style="list-style-type: none"> The default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
Step 8	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>
Step 9	<p>show track [<i>object-number</i> brief] [interface [brief] ip route [brief] resolution timers]</p> <p>Example:</p> <pre>Device# show track 100 interface</pre>	<p>Displays tracking information.</p>

Configuring HSRP MD5 Authentication Using a Key String



Note Text authentication cannot be combined with MD5 authentication for an HSRP group at any one time. When MD5 authentication is configured, the text authentication field in HSRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving device also has MD5 authentication enabled.



Note If you are changing a key string in a group of devices, change the active device last to prevent any HSRP state change. The active device should have its key string changed no later than one hold-time period, specified by the **standby timers** interface configuration command, after the nonactive devices. This procedure ensures that the nonactive devices do not time out the active device.

SUMMARY STEPS

- enable**
- configure terminal**
- terminal interface** *type number*
- ip address** *ip-address mask* [**secondary**]

5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication md5** **key-string** [**0** | **7**] *key* [**timeout** *seconds*]
8. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	terminal interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] authentication md5 key-string [0 7] <i>key</i> [timeout <i>seconds</i>] Example:	Configures an authentication string for HSRP MD5 authentication. • The <i>key</i> argument can be up to 64 characters in length. We recommended that at least 16 characters be used.

	Command or Action	Purpose
	<pre>Device(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30</pre>	<ul style="list-style-type: none"> No prefix to the <i>key</i> argument or specifying 0 means the key will be unencrypted. Specifying 7 means the key will be encrypted. The key-string authentication key will automatically be encrypted if the service password-encryption global configuration command is enabled. The timeout value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key.
Step 8	<p>standby [<i>group-number</i>] ip [<i>ip-address</i>] [secondary]]</p> <p>Example:</p> <pre>Device(config-if)# standby 1 ip 10.0.0.3</pre>	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each device that will communicate.	—
Step 10	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 11	<p>show standby</p> <p>Example:</p> <pre>Device# show standby</pre>	<p>(Optional) Displays HSRP information.</p> <ul style="list-style-type: none"> Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Configuring HSRP MD5 Authentication Using a Key Chain

Perform this task to configure HSRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

SUMMARY STEPS

- enable**
- configure terminal**
- key chain** *name-of-chain*
- key** *key-id*
- key-string** *string*
- exit**
- exit**
- interface** *type number*
- ip address** *ip-address mask* [**secondary**]

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	key chain <i>name-of-chain</i> Example: Device(config)# key chain hsrp1	Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 100	Identifies an authentication key on a key chain and enters key-chain key configuration mode. • The value for the <i>key-id</i> argument must be a number.
Step 5	key-string <i>string</i> Example: Device(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. • The value for the <i>string</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to key-chain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 9	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 10	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 11	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 12	standby [<i>group-number</i>] authentication md5 key-chain <i>key-chain-name</i> Example: Device(config-if)# standby 1 authentication md5 key-chain hsrpl	Configures an authentication MD5 key chain for HSRP MD5 authentication. <ul style="list-style-type: none"> The key chain name must match the name specified in Step 3.
Step 13	standby [<i>group-number</i>] ip [<i>ip-address [secondary]</i>] Example: Device(config-if)# standby 1 ip 10.21.8.12	Activates HSRP.
Step 14	Repeat Steps 1 through 12 on each device that will communicate.	—
Step 15	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 16	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Troubleshooting HSRP MD5 Authentication

Perform this task if HSRP MD5 authentication is not operating correctly.

SUMMARY STEPS

1. **enable**
2. **debug standby errors**

DETAILED STEPS

	Command 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	debug standby errors Example: Device# debug standby errors	Displays error messages related to HSRP. <ul style="list-style-type: none"> • Error messages will be displayed for each packet that fails to authenticate, so use this command with care.

Examples

In the following example, Device A has MD5 text string authentication configured, but Device B has the default text authentication:

```
Device# debug standby errors
```

```
A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 confgd
  but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth
  failed
```

In the following example, both Device A and Device B have different MD5 authentication strings:

```
Device# debug standby errors
```

```
A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth
  failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth
  failed
```

Configuring HSRP Text Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ip address** *ip-address mask [secondary]*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address [secondary]*]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] authentication text <i>string</i> Example:	Configures an authentication string for HSRP text authentication. <ul style="list-style-type: none"> • The default string is cisco.

	Command or Action	Purpose
	Device(config-if)# standby 1 authentication text authentication1	
Step 8	standby [group-number] ip [ip-address [secondary]] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each device that will communicate.	--
Step 10	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 11	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none">• Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Configuring HSRP Timers



Note We recommend configuring a minimum hello-time value of 250 milliseconds and a minimum hold-time value of 800 milliseconds.

You can use the **standby delay** command to allow the interface to come up completely before HSRP initializes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask [secondary]*
5. **standby** [group-number] **timers** [msec] *hellotime* [msec] *holdtime*
6. **standby** [group-number] **ip** [ip-address [secondary]]

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface type number Example: Device(config)# interface Gigabit Ethernet 0/0/1	Configures an interface type and enters interface configuration mode.
Step 4	ip address ip-address mask [secondary]] Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [group-number] timers [msec] hellotime [msec] holdtime Example: Device(config-if)# standby 1 timers 5 15	Configures the time between hello packets and the time before other devices declare the active Hot Standby or standby device to be down.
Step 6	standby [group-number] ip [ip-address [secondary]] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.

Configuring an HSRP MAC Refresh Interval

SUMMARY STEPS

1. enable
2. configure terminal
3. interface *type number*
4. ip address *ip-address mask [secondary]*
5. standby mac-refresh *seconds*
6. standby [*group-number*] ip [*ip-address [secondary]*]

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/1	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> [secondary] Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby mac-refresh <i>seconds</i> Example: Device(config-if)# standby mac-refresh 100	Changes the interval at which packets are sent to refresh the MAC cache when HSRP is running over FDDI. <ul style="list-style-type: none"> • This command applies to HSRP running over FDDI only.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.

Configuring Multiple HSRP Groups for Load Balancing

Perform this task to configure multiple HSRP groups for load balancing.

Multiple HSRP groups enable redundancy and load-sharing within networks and allow redundant devices to be more fully utilized. A device actively forwarding traffic for one HSRP group can be in standby or in the listen state for another group.

If two devices are used, then Device A would be configured as active for group 1 and standby for group 2. Device B would be standby for group 1 and active for group 2. Fifty percent of the hosts on the LAN would be configured with the virtual IP address of group 1 and the remaining hosts would be configured with the virtual IP address of group 2. See the [Example: Configuring Multiple HSRP Groups for Load Balancing](#) for a diagram and configuration example.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **ip address** *ip-address mask [secondary]*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.
9. **exit**
10. Repeat Steps 3 through 9 on another device.

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>delay</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] ip [<i>ip-address</i>] secondary] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.

	Command or Action	Purpose
Step 8	On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.	For example, Device A can be configured as an active device for group 1 and be configured as an active or standby device for another HSRP group with different priority and preemption values.
Step 9	exit Example: Device(config-if)# exit	Exits to global configuration mode.
Step 10	Repeat Steps 3 through 9 on another device.	Configures multiple HSRP and enables load balancing on another device.

Improving CPU and Network Performance with HSRP Multiple Group Optimization

Perform this task to configure multiple HSRP client groups.

The **standby follow** command configures an HSRP group to become a subordinate of another HSRP group.

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

Use the **standby mac-refresh *seconds*** command to directly change the HSRP client group refresh interval. The default interval is 10 seconds and can be configured to as much as 255 seconds.



Note

- Client or subordinate groups must be on the same physical interface as the master group.
- A client group takes its state from the group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

Before you begin

Configure the HSRP master group using the steps in the [Configuring Multiple HSRP Groups for Load Balancing](#) section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***

4. **ip address** *ip-address mask [secondary]*
5. **standby mac-refresh** *seconds*
6. **standby group-number follow** *group-name*
7. **exit**
8. Repeat Steps 3 through 6 to configure additional HSRP client groups.

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby mac-refresh <i>seconds</i> Example: Device(config-if)# standby mac-refresh 30	Configures the HSRP client group refresh interval.
Step 6	standby group-number follow <i>group-name</i> Example: Device(config-if)# standby 1 follow HSRP1	Configures an HSRP group as a client group.
Step 7	exit Example: Device(config-if)# exit	Exits to global configuration mode.
Step 8	Repeat Steps 3 through 6 to configure additional HSRP client groups.	Configures multiple HSRP client groups.

Enabling HSRP Support for ICMP Redirect Messages

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses



Note You cannot use the **standby use-bia** and **standby mac-address** commands in the same configuration; they are mutually exclusive.

The **standby use-bia** command has the following disadvantages:

- When a device becomes active the virtual IP address is moved to a different MAC address. The newly active device sends a gratuitous ARP response, but not all host implementations handle the gratuitous ARP correctly.
- Proxy ARP does not function when the **standby use-bia** command is configured. A standby device cannot cover for the lost proxy ARP database of the failed device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. Enter one of the following commands:
 - **standby** [*group-number*] **mac-address** *mac-address*
 - or
 - **standby use-bia** [*scope interface*]
 - or
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	ip address <i>ip-address mask</i> [secondary] Example: <pre>Device(config-if)# ip address 172.16.6.5 255.255.255.0</pre>	Configures an IP address for an interface.
Step 5	Enter one of the following commands: <ul style="list-style-type: none"> • standby [<i>group-number</i>] mac-address <i>mac-address</i> • or • standby use-bia [scope interface] • or Example: <pre>Device(config-if)# standby 1 mac-address 5000.1000.1060</pre> Example: <pre>Device(config-if)# standby use-bia</pre>	Specifies a virtual MAC address for HSRP. <ul style="list-style-type: none"> • This command cannot be used on a Token Ring interface. or Configures HSRP to use the burned-in address of the interface as its virtual MAC address. <ul style="list-style-type: none"> • The scope interface keywords specify that the command is configured just for the subinterface on which it was entered, instead of the major interface.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: <pre>Device(config-if)# standby 1 ip 172.16.6.100</pre>	Activates HSRP.

Linking IP Redundancy Clients to HSRP Groups

Before you begin

Within the client application, you must first specify the same name as configured in the **standby name** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **name** [*redundancy-name*]
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	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>type number</i> Example: Device(config)# interface Ethernet 0/1	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies an IP address for an interface.
Step 5	standby [<i>group-number</i>] name [<i>redundancy-name</i>] Example: Device(config-if)# standby 1 name HSRP-1	Configures the name of the standby group. <ul style="list-style-type: none"> HSRP groups have a default name of hsrp-interface-group so specifying a group name is optional.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 1 ip 10.0.0.11	Activates HSRP.

Changing to HSRP Version 2

HSRP version 2 was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.



Note

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 will not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same device. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).

SUMMARY STEPS

1. enable
2. configure terminal

3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby version** { 1 | 2 }
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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>type number</i> Example: Device(config)# interface vlan 400	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.10.28.1 255.255.255.0	Sets an IP address for an interface.
Step 5	standby version { 1 2 } Example: Device(config-if)# standby version 2	Changes the HSRP version.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 400 ip 10.10.28.5	Activates HSRP. <ul style="list-style-type: none"> • The group number range for HSRP version 2 is 0 through 4095. The group number range for HSRP version 1 is 0 through 255.
Step 7	end Example: Device(config-if)# end	Ends the current configuration session and returns to privileged EXEC mode.
Step 8	show standby	(Optional) Displays HSRP information.

	Command or Action	Purpose
	Example: Device# show standby	<ul style="list-style-type: none"> • HSRP version 2 information will be displayed if configured.

Enabling SSO Aware HSRP

The SSO aware HSRP is enabled by default when the redundancy mode is set to SSO. Perform this task to reenable HSRP to be SSO aware if it has been disabled.



Note You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

SUMMARY STEPS

1. enable
2. configure terminal
3. redundancy
4. mode sso
5. exit
6. no standby sso
7. standby sso
8. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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	redundancy Example: Device(config)# redundancy	Enters redundancy configuration mode.
Step 4	mode sso Example:	Enables the redundancy mode of operation to SSO. <ul style="list-style-type: none"> • HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset.

	Command or Action	Purpose
	Device(config-red)# mode sso	
Step 5	exit Example: Device(config-red)# exit	Exits redundancy configuration mode.
Step 6	no standby sso Example: Device(config)# no standby sso	Disables HSRP SSO mode for all HSRP groups.
Step 7	standby sso Example: Device(config)# standby sso	Enables the SSO HSRP feature if you have disabled the functionality.
Step 8	end Example: Device(config)# end	Ends the current configuration session and returns to privileged EXEC mode.

Verifying SSO Aware HSRP

To verify or debug HSRP SSO operation, perform the following steps from the active RP console.

SUMMARY STEPS

1. **show standby**
2. **debug standby events ha**

DETAILED STEPS

Step 1 show standby

Use the **show standby** command to display the state of the standby RP, for example:

Example:

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
  State is Active (standby RP)
  Virtual IP address is 10.1.0.7
  Active virtual MAC address is unknown
  Local virtual MAC address is 000a.f3fd.5001 (bia)
  Hello time 1 sec, hold time 3 sec
  Authentication text "authword"
  Preemption enabled
```



```

Active router is unknown
Standby router is unknown
Priority 110 (configured 120)
Track object 1 state Down decrement 10
Group name is "name1" (cfgd)

```

Step 2 debug standby events ha

Use the `debug standby events ha` command to display the active and standby RPs, for example:

Example:

```

Device# debug standby events ha

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active

```

Enabling HSRP MIB Traps

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server enable traps hsrp
4. snmp-server host *host community-string* hsrp

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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# configure terminal	
Step 3	snmp-server enable traps hsrp Example: Device(config)# snmp-server enable traps hsrp	Enables the device to send SNMP traps and informs, and HSRP notifications.
Step 4	snmp-server host <i>host community-string</i> hsrp Example: Device(config)# snmp-server host myhost.comp.com public hsrp	Specifies the recipient of an SNMP notification operation, and that HSRP notifications be sent to the host.

Configuring BFD Session Parameters on an Interface

Perform this task to configure Bidirectional Forwarding Detection (BFD) on an interface by setting the baseline BFD session parameters on the interface. Repeat the steps in this task for each interface on which you want to run BFD sessions to BFD neighbors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **bfd interval *milliseconds* min_rx *milliseconds* multiplier *interval-multiplier***
5. **end**

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface FastEthernet 6/0	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	bfd interval <i>milliseconds</i> min_rx <i>milliseconds</i> multiplier <i>interval-multiplier</i> Example: <pre>Device(config-if)# bfd interval 50 min_rx 50 multiplier 5</pre>	Enables BFD on the interface.
Step 5	end Example: <pre>Device(config-if)# end</pre>	Exits interface configuration mode.

Configuring HSRP BFD Peering

Perform this task to enable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering. Repeat the steps in this task for each interface over which you want to run BFD sessions to HSRP peers.

HSRP supports BFD peering by default. If HSRP BFD peering is disabled, you can reenabling it at the device level to enable BFD support globally for all interfaces or you can reenabling it on a per-interface basis at the interface level.

Before you begin

Before you proceed with this task:

- HSRP must be running on all participating devices.
- Cisco Express Forwarding must be enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby** [**neighbors**]

DETAILED STEPS

	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	ip cef [distributed] Example: Device(config)# ip cef	Enables Cisco Express Forwarding or distributed Cisco Express Forwarding.
Step 4	interface <i>type number</i> Example: Device(config)# interface FastEthernet 6/0	Enters interface configuration mode.
Step 5	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.0.0.11 255.255.255.0	Configures an IP address for the interface.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address [secondary]</i>] Example: Device(config-if)# standby 1 ip 10.0.0.11	Activates HSRP.
Step 7	standby bfd Example: Device(config-if)# standby bfd	(Optional) Enables HSRP support for BFD on the interface.
Step 8	exit Example: Device(config-if)# exit	Exits interface configuration mode.
Step 9	standby bfd all-interfaces Example: Device(config)# standby bfd all-interfaces	(Optional) Enables HSRP support for BFD on all interfaces.

	Command or Action	Purpose
Step 10	exit Example: Device(config)# exit	Exits global configuration mode.
Step 11	show standby [neighbors] Example: Device# show standby neighbors	(Optional) Displays information about HSRP support for BFD.

Verifying HSRP BFD Peering

To verify Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering, use any of the following optional commands.

SUMMARY STEPS

1. **show standby**
2. **show standby brief**
3. **show standby neighbors** *[type number]*
4. **show bfd neighbors**
5. **show bfd neighbors details**

DETAILED STEPS

Step 1 **show standby**

Use the **show standby** command to display HSRP information.

Example:

```
Device# show standby

FastEthernet2/0 - Group 1
  State is Active
    2 state changes, last state change 00:08:06
  Virtual IP address is 10.0.0.11
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.772 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 90 (expires in 8.268 sec)
  BFD enabled !
  Priority 110 (configured 110)
  Group name is "hsrp-Fa2/0-1" (default)
```

Step 2 **show standby brief**

Use the **show standby brief** command to display HSRP standby device information in brief.

Example:

```
Device# show standby brief

Interface   Grp  Pri P State   Active   Standby           Virtual IP
Et0/0      4    120 P Active local    172.24.1.2       172.24.1.254
Et1/0      6    120 P Active local    FE80::A8BB:CCFF:FE00:3401 FE80::5:73FF:FEA0:6
```

Step 3 **show standby neighbors** [*type number*]

Use the **show standby neighbors** command to display information about HSRP peer devices on an interface.

Example:

```
Device1# show standby neighbors

HSRP neighbors on FastEthernet2/0
 10.1.0.22
No active groups
Standby groups: 1
BFD enabled !

Device2# show standby neighbors

HSRP neighbors on FastEthernet2/0
 10.0.0.2
Active groups: 1
No standby groups
BFD enabled !
```

Step 4 **show bfd neighbors**

Use the **show bfd neighbors** command to display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies.

Example:

```
Device# show bfd neighbors

IPv6 Sessions

NeighAddr                               LD/RD           RH/RS           State           Int
FE80::A8BB:CCFF:FE00:3401              4/3             Up              Up              Et1/0
FE80::A8BB:CCFF:FE00:3401              4/3             Up              Up              Et1/0
```

Step 5 **show bfd neighbors details**

Use the **details** keyword to display BFD protocol parameters and timers for each neighbor.

Example:

```
Device# show bfd neighbors details

OurAddr      NeighAddr      LD/RD  RH/RS  Holdown(mult)  State  Int
10.0.0.2     10.0.0.1       5/0    Down   0 (0)          Down   Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
```

```
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1          - Diagnostic: 0
                State bit: AdminDown - Demand bit: 0
                Poll bit: 0         - Final bit: 0
                Multiplier: 0       - Length: 0
                My Discr.: 0        - Your Discr.: 0
                Min tx interval: 0   - Min rx interval: 0
                Min Echo interval: 0
```

Configuration Examples for HSRP

Example: Configuring HSRP Priority and Preemption

In the following example, Device A is configured to be the active device for group 1 because it has the higher priority and standby device for group 2. Device B is configured to be the active device for group 2 and standby device for group 1.

Device A Configuration

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 95
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

Device B Configuration

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 110
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

Example: Configuring HSRP Object Tracking

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Gigabit Ethernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IP-routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on serial interface 1/0 in Device A fails, the HSRP group priority will be reduced and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Device A Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

Device B Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

Example: Configuring HSRP Group Shutdown

In the following example, the tracking process is configured to track the IP-routing capability of Gigabit Ethernet interface 0/0/0. HSRP on Gigabit Ethernet interface 0/0/1 then registers with the tracking process to be informed of any changes to the IP-routing state of Gigabit Ethernet interface 0/0/0. If the IP state on Gigabit Ethernet interface 0/0/0 goes down, the HSRP group is disabled.

If both Gigabit Ethernet interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Device A fails, the HSRP group will be disabled and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Device A Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

Device B Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 shutdown
```


If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

Example: Configuring HSRP MD5 Authentication Using Key Strings

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Chains

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

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

Device 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Device 2

```
Device(config)# interface GigabitEthernet 0/0/0
```

```
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

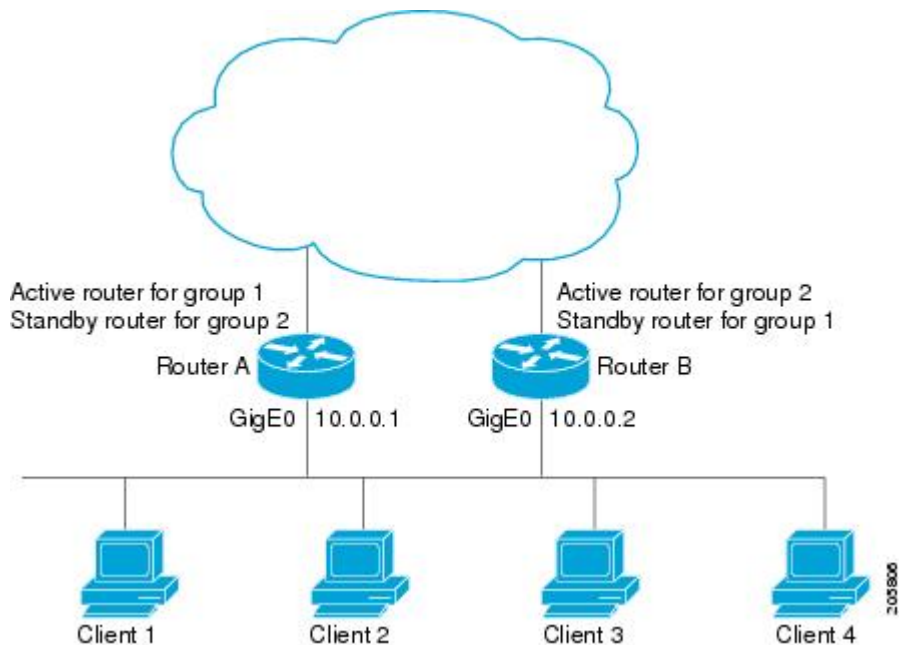
Example: Configuring HSRP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring Multiple HSRP Groups for Load Balancing

You can use HSRP or multiple HSRP groups when you configure load sharing. In the figure below, half of the clients are configured for Router A, and half of the clients are configured for Router B. Together, the configuration for Routers A and B establish two Hot Standby groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable. The **standby preempt** interface configuration command is necessary so that if a router goes down and then comes back up, preemption occurs and restores load sharing.

Figure 5: HSRP Load Sharing Example



The following example shows Router A configured as the active router for group 1 with a priority of 110 and Router B configured as the active router for group 2 with a priority of 110. The default priority level is 100. Group 1 uses a virtual IP address of 10.0.0.3 and Group 2 uses a virtual IP address of 10.0.0.4.

Router A Configuration

```
Router(config)# hostname RouterA
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

Router B Configuration

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization

The following example shows how to configure an HSRP client and primary group:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
```

```
Device(config-if)# standby 2 follow HSRP1
! Client group
```

Example: Configuring HSRP Support for ICMP Redirect Messages

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

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

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

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

Example: Configuring HSRP Virtual MAC Addresses and BIA MAC Address

In an Advanced Peer-to-Peer Networking (APPN) network, an end node is typically configured with the MAC address of the adjacent network node. In the following example, if the end nodes are configured to use 4000.1000.1060, HSRP group 1 is configured to use the same MAC address:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1
Device(config-if)# standby 1 mac-address 4000.1000.1060
Device(config-if)# standby 1 ip 10.0.0.11
```

In the following example, the burned-in address of Token Ring interface 3/0 will be the virtual MAC address mapped to the virtual IP address:

```
Device(config)# interface token 3/0
Device(config-if)# standby use-bia
```



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

Example: Linking IP Redundancy Clients to HSRP Groups

The following example shows HSRP support for a static Network Address Translation (NAT) configuration. The NAT client application is linked to HSRP via the correlation between the name specified by the **standby name** command. Two devices are acting as HSRP active and standby, and the NAT inside interfaces are HSRP enabled and configured to belong to the group named “group1.”

Active Device Configuration

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.54 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 priority 110
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 track Ethernet 2/1
!
!
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 2/1
Device(config)# ip route 172.22.33.0 255.255.255.0 Ethernet 2/1
Device(config)# no ip http server
```

Standby Device Configuration

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.56 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 priority 95
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 track Ethernet 3/1
Device(config-if)# exit
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 3.3.3.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.0.32.231 255.255.255.0 Ethernet 3/1
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 3/1
Device(config)# no ip http server
```

Example: Configuring HSRP Version 2

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

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

Example: Enabling SSO-Aware HSRP

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

```
Device(config)# redundancy
Device(config-red)# mode sso
```

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

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso
```

Example: Enabling HSRP MIB Traps

The following examples show how to configure HSRP on two devices and enable the HSRP MIB trap support functionality. As in many environments, one device is preferred as the active one. To configure a device's preference as the active device, configure the device at a higher priority level and enable preemption. In the following example, the active device is referred to as the primary device. The second device is referred to as the backup device:

Device A

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host yourhost.cisco.com public hsrp
```

Device B

```
Device(config)#interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.2 255.255.0.0
Device(config-if)# standby priority 101
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host myhost.cisco.com public hsrp
```

Example: HSRP BFD Peering

Hot Standby Router Protocol (HSRP) supports Bidirectional Forwarding Detection (BFD) as a part of the HSRP group member health monitoring system. Without BFD, HSRP runs as a process in a multiprocess system and cannot be guaranteed to be scheduled in time to service large numbers of groups with millisecond hello and hold timers. BFD runs as a pseudo-preemptive process and can therefore, be guaranteed to run when

required. Only one BFD session between two devices can provide early failover notification for multiple HSRP groups.

In the following example, the **standby bfd** and the **standby bfd all-interfaces** commands are not displayed. HSRP support for BFD is enabled by default when BFD is configured on a device or an interface by using the **bfd interval** command. The **standby bfd** and **standby bfd all-interfaces** commands are needed only if BFD has been manually disabled on a device or an interface.

Device A

```
DeviceA(config)# ip cef
DeviceA(config)# interface FastEthernet2/0
DeviceA(config-if)# no shutdown
DeviceA(config-if)# ip address 10.0.0.2 255.0.0.0
DeviceA(config-if)# ip router-cache cef
DeviceA(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceA(config-if)# standby 1 ip 10.0.0.11
DeviceA(config-if)# standby 1 preempt
DeviceA(config-if)# standby 1 priority 110
DeviceA(config-if)# standby 2 ip 10.0.0.12
DeviceA(config-if)# standby 2 preempt
DeviceA(config-if)# standby 2 priority 110
```

Device B

```
DeviceB(config)# interface FastEthernet2/0
DeviceB(config-if)# ip address 10.1.0.22 255.255.0.0
DeviceB(config-if)# no shutdown
DeviceB(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceB(config-if)# standby 1 ip 10.0.0.11
DeviceB(config-if)# standby 1 preempt
DeviceB(config-if)# standby 1 priority 90
DeviceB(config-if)# standby 2 ip 10.0.0.12
DeviceB(config-if)# standby 2 preempt
DeviceB(config-if)# standby 2 priority 80
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP

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

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

Table 1: Feature Information for HSRP

Feature Name	Releases	Feature Information
HSRP	Cisco IOS XE 17.3.2	This feature was introduced for the Catalyst 8000 Series platforms.

Glossary

ARP—Address Resolution Protocol (ARP). ARP performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses. ARP is part of all Cisco IOS systems running IP.

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

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

client group—An HSRP group that is created on a subinterface and linked to the primary group via the group name.

HSRP—Hot Standby Router Protocol. Protocol that provides high network availability and transparent network-topology changes. HSRP creates a router group with a lead device that services all packets sent to the HSRP address. The lead device is monitored by other devices in the group, and if it fails, one of these standby HSRP devices inherits the lead position and the HSRP group address.

ISSU—In Service Software Upgrade. A process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

primary group—An HSRP group that is required on a physical interface for the purposes of electing active and standby devices.

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

RP—Route Processor. A generic term for the centralized control unit in a chassis.

RPR—Route Processor Redundancy. RPR provides an alternative to the High System Availability (HSA) feature. HSA enables a system to reset and use a standby Route Processor (RP) if the active RP fails. Using RPR, you can reduce unplanned downtime because RPR enables a quicker switchover between an active and standby RP if the active RP experiences a fatal error.

RPR+—An enhancement to RPR in which the standby RP is fully initialized.

standby group—The set of devices participating in HSRP that jointly emulate a virtual device.

standby device—The backup device in an HSRP group.

standby RP—The backup RP.

switchover—An event in which system control and routing protocol execution are transferred from the active RP to the standby RP. Switchover may be a manual operation or may be induced by a hardware or software

fault. Switchover may include transfer of the packet forwarding function in systems that combine system control and packet forwarding in an indivisible unit.

virtual IP address—The default gateway IP address configured for an HSRP group.

virtual MAC address—For Ethernet and FDDI, the automatically generated MAC address when HSRP is configured. The standard virtual MAC address used is: 0000.0C07.AC xy , where xy is the group number in hexadecimal. The functional address is used for Token Ring. The virtual MAC address is different for HSRP version 2.



CHAPTER 5

HSRP Version 2

- [Finding Feature Information, on page 95](#)
- [Information About HSRP Version 2, on page 95](#)
- [How to Configure HSRP Version 2, on page 96](#)
- [Configuration Examples for HSRP Version 2, on page 98](#)
- [Additional References, on page 98](#)
- [Feature Information for HSRP Version 2, on page 99](#)

Finding Feature Information

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

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

Information About HSRP Version 2

HSRP Version 2 Design

HSRP version 2 is designed to address the following restrictions in HSRP version 1:

- In HSRP version 1, millisecond timer values are not advertised or learned. HSRP version 2 advertises and learns millisecond timer values. This change ensures stability of the HSRP groups in all cases.
- In HSRP version 1, group numbers are restricted to the range from 0 to 255. HSRP version 2 expands the group number range from 0 to 4095.
- HSRP version 2 provides improved management and troubleshooting. With HSRP version 1, you cannot use HSRP active hello messages to identify which physical device sent the message because the source MAC address is the HSRP virtual MAC address. The HSRP version 2 packet format includes a 6-byte identifier field that is used to uniquely identify the sender of the message. Typically, this field is populated with the interface MAC address.

- The multicast address 224.0.0.2 is used to send HSRP hello messages. This address can conflict with Cisco Group Management Protocol (CGMP) leave processing.

Version 1 is the default version of HSRP.

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

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF. The increased group number range does not imply that an interface can, or should, support that many HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

When the HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

HSRP version 2 has a different packet format than HSRP version 1. The packet format uses a type-length-value (TLV) format. HSRP version 2 packets received by an HSRP version 1 device will have the type field mapped to the version field by HSRP version 1 and subsequently ignored.

The Gateway Load Balancing Protocol (GLBP) also addresses the same restrictions relative to HSRP version 1 that HSRP version 2 does. See the *Configuring GLBP* document for more information on GLBP.

Jitter timers

Jitter timers are used in HSRP. They are recommended for timers running on services that work realtime and scale. Jitter timers are intended to significantly improve the reliability of HSRP, and other FHRP protocols, by reducing the chance of bunching of HSRP groups operations, and thus help reduce CPU and network traffic spikes. In the case of HSRP, a given device may have up to 4000 operational groups configured. In order to distribute the load on the device and network, the HSRP timers use a jitter. A given timer instance may take up to 20% more than the configured value. For example, for a hold time set to 15 seconds, the actual hold time may take 18 seconds.

In HSRP, the Hello timer (which sends the Hello Packet) has a negative Jitter, while the Holddown timer (which checks for failure of a peer) has a positive jitter.

How to Configure HSRP Version 2

Changing to HSRP Version 2

HSRP version 2 was introduced to prepare for further enhancements and to expand the capabilities beyond what is possible with HSRP version 1. HSRP version 2 has a different packet format than HSRP version 1.



Note

- HSRP version 2 is not available for ATM interfaces running LAN emulation.
- HSRP version 2 will not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same device. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby version** {1 | 2}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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>type number</i> Example: Device(config)# interface vlan 400	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.10.28.1 255.255.255.0	Sets an IP address for an interface.
Step 5	standby version {1 2} Example: Device(config-if)# standby version 2	Changes the HSRP version.
Step 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 400 ip 10.10.28.5	Activates HSRP. <ul style="list-style-type: none"> • The group number range for HSRP version 2 is 0 through 4095. The group number range for HSRP version 1 is 0 through 255.
Step 7	end Example:	Ends the current configuration session and returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config-if)# end	
Step 8	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> • HSRP version 2 information will be displayed if configured.

Configuration Examples for HSRP Version 2

Example: Configuring HSRP Version 2

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

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP Version 2

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.



CHAPTER 6

HSRP MD5 Authentication

- [Finding Feature Information, on page 101](#)
- [Information About HSRP MD5 Authentication, on page 101](#)
- [How to Configure HSRP MD5 Authentication, on page 102](#)
- [Configuration Examples for HSRP MD5 Authentication, on page 107](#)
- [Additional References, on page 108](#)
- [Feature Information for HSRP MD5 Authentication, on page 109](#)

Finding Feature Information

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

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

Information About HSRP MD5 Authentication

HSRP Text Authentication

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

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

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

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

HSRP MD5 Authentication

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

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

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

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

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

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

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

How to Configure HSRP MD5 Authentication

Configuring HSRP MD5 Authentication Using a Key Chain

Perform this task to configure HSRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. HSRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**

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

DETAILED STEPS

	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	key chain <i>name-of-chain</i> Example: Device(config)# key chain hsrp1	Enables authentication for routing protocols, identifies a group of authentication keys, and enters key-chain configuration mode.
Step 4	key <i>key-id</i> Example: Device(config-keychain)# key 100	Identifies an authentication key on a key chain and enters key-chain key configuration mode. <ul style="list-style-type: none"> • The value for the <i>key-id</i> argument must be a number.
Step 5	key-string <i>string</i> Example: Device(config-keychain-key)# key-string mnol72	Specifies the authentication string for a key. <ul style="list-style-type: none"> • The value for the <i>string</i> argument can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral
Step 6	exit Example: Device(config-keychain-key)# exit	Returns to key-chain configuration mode.
Step 7	exit Example: Device(config-keychain)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 8	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 9	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 10	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 11	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 12	standby [<i>group-number</i>] authentication md5 key-chain <i>key-chain-name</i> Example: Device(config-if)# standby 1 authentication md5 key-chain hsrp1	Configures an authentication MD5 key chain for HSRP MD5 authentication. <ul style="list-style-type: none"> The key chain name must match the name specified in Step 3.
Step 13	standby [<i>group-number</i>] ip [<i>ip-address [secondary]</i>] Example: Device(config-if)# standby 1 ip 10.21.8.12	Activates HSRP.
Step 14	Repeat Steps 1 through 12 on each device that will communicate.	—
Step 15	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 16	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Troubleshooting HSRP MD5 Authentication

Perform this task if HSRP MD5 authentication is not operating correctly.

SUMMARY STEPS

1. `enable`
2. `debug standby errors`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug standby errors Example: Device# <code>debug standby errors</code>	Displays error messages related to HSRP. <ul style="list-style-type: none"> • Error messages will be displayed for each packet that fails to authenticate, so use this command with care.

Examples

In the following example, Device A has MD5 text string authentication configured, but Device B has the default text authentication:

```
Device# debug standby errors
```

```
A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 confgd
  but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth
  failed
```

In the following example, both Device A and Device B have different MD5 authentication strings:

```
Device# debug standby errors
```

```
A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth
  failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth
  failed
```

Configuring HSRP Text Authentication

SUMMARY STEPS

1. `enable`
2. `configure terminal`

3. **interface** *type number*
4. **ip address** *ip-address mask [secondary]*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address [secondary]*]
9. Repeat Steps 1 through 8 on each device that will communicate.
10. **end**
11. **show standby**

DETAILED STEPS

	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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] authentication text <i>string</i> Example:	Configures an authentication string for HSRP text authentication. <ul style="list-style-type: none"> • The default string is cisco.

	Command or Action	Purpose
	Device(config-if)# standby 1 authentication text authentication1	
Step 8	standby [group-number] ip [ip-address [secondary]] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each device that will communicate.	--
Step 10	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 11	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> • Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Configuration Examples for HSRP MD5 Authentication

Example: Configuring HSRP MD5 Authentication Using Key Strings

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Chains

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

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP MD5 Authentication Using Key Strings and Key Chains

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

Device 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

Device 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

Example: Configuring HSRP Text Authentication

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP MD5 Authentication

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.



CHAPTER 7

HSRP Support for ICMP Redirects

- [Finding Feature Information, on page 111](#)
- [Information About HSRP Support for ICMP Redirects, on page 111](#)
- [How to Configure HSRP Support for ICMP Redirects, on page 114](#)
- [Configuration Examples for HSRP Support for ICMP Redirects, on page 115](#)
- [Additional References, on page 116](#)
- [Feature Information for HSRP Support for ICMP Redirects, on page 117](#)

Finding Feature Information

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

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

Information About HSRP Support for ICMP Redirects

HSRP Support for ICMP Redirect Messages

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

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

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

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This functionality works by filtering outgoing ICMP redirect messages through HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.

ICMP Redirects to Active HSRP Devices

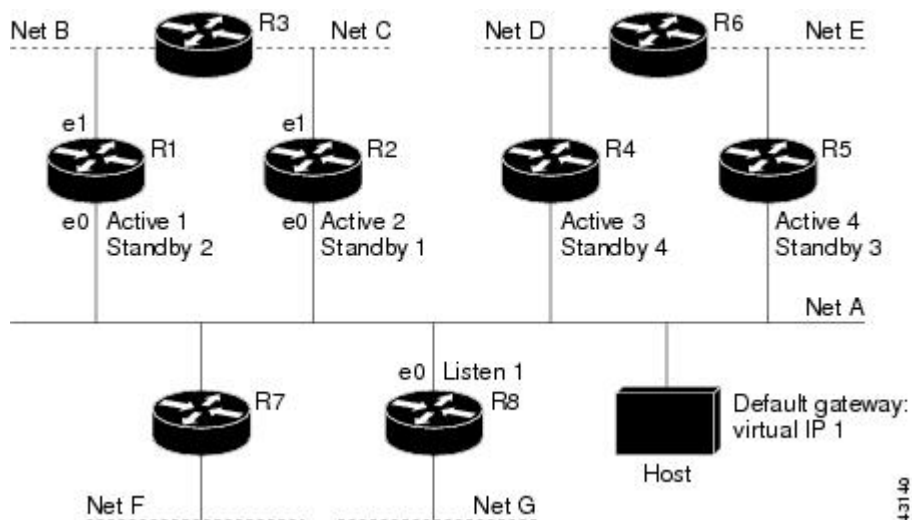
The next-hop IP address is compared to the list of active HSRP devices on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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

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

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

Figure 6: Network Supporting the HSRP ICMP Redirection Filter



If the host wants to send a packet to another host on Net D, then it first sends it to its default gateway, the virtual IP address of HSRP group 1.

The following is the packet received from the host:

```

dest MAC      = HSRP group 1 virtual MAC
source MAC    = Host MAC
dest IP       = host-on-netD IP
source IP     = Host IP

```

Device R1 receives this packet and determines that device R4 can provide a better path to Net D, so it prepares to send a redirect message that will redirect the host to the real IP address of device R4 (because only real IP addresses are in its routing table).

The following is the initial ICMP redirect message sent by device R1:

```

dest MAC      = Host MAC
source MAC    = router R1 MAC
dest IP       = Host IP

```

```
source IP          = router R1 IP
gateway to use    = router R4 IP
```

Before this redirect occurs, the HSRP process of device R1 determines that device R4 is the active HSRP device for group 3, so it changes the next hop in the redirect message from the real IP address of device R4 to the virtual IP address of group 3. Furthermore, it determines from the destination MAC address of the packet that triggered the redirect message that the host used the virtual IP address of group 1 as its gateway, so it changes the source IP address of the redirect message to the virtual IP address of group 1.

The modified ICMP redirect message showing the two modified fields (*) is as follows:

```
dest MAC          = Host MAC
source MAC        = router R1 MAC
dest IP           = Host IP
source IP*        = HSRP group 1 virtual IP
gateway to use*   = HSRP group 3 virtual IP
```

This second modification is necessary because hosts compare the source IP address of the ICMP redirect message with their default gateway. If these addresses do not match, the ICMP redirect message is ignored. The routing table of the host now consists of the default gateway, virtual IP address of group 1, and a route to Net D through the virtual IP address of group 3.

ICMP Redirects to Passive HSRP Devices

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

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

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

ICMP Redirects to Non-HSRP Devices

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

In the "Network Supporting the HSRP ICMP Redirection Filter" figure, redirection to device R7 is allowed because R7 is not running HSRP. In this case, the next hop IP address is unchanged. The source IP address is changed dependent upon the destination MAC address of the original packet. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

Passive HSRP Advertisement Messages

Passive HSRP devices send out HSRP advertisement messages both periodically and when entering or leaving the passive state. Thus, all HSRP devices can determine the HSRP group state of any HSRP device on the network. These advertisements inform other HSRP devices on the network of the HSRP interface state, as follows:

- Active—Interface has at least one active group. A single advertisement is sent out when the first group becomes active.

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

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

ICMP Redirects Not Sent

If the HSRP device cannot uniquely determine the IP address used by the host when it sends the packet that caused the redirect, the redirect message will not be sent. The device uses the destination MAC address in the original packet to make this determination. In certain configurations, such as the use of the **standby use-bia** interface configuration command specified on an interface, redirects cannot be sent. In this case, the HSRP groups use the interface MAC address as their virtual MAC address. The device now cannot determine if the default gateway of the host is the real IP address or one of the HSRP virtual IP addresses that are active on the interface.

The IP source address of an ICMP packet must match the gateway address used by the host in the packet that triggered the ICMP packet, otherwise the host will reject the ICMP redirect packet. An HSRP device uses the destination MAC address to determine the gateway IP address of the host. If the HSRP device is using the same MAC address for multiple IP addresses, uniquely determining the gateway IP address of the host is not possible, and the redirect message is not sent.

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

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

How to Configure HSRP Support for ICMP Redirects

Enabling HSRP Support for ICMP Redirect Messages

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <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>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	standby redirect [<i>timers advertisement holddown</i>] [<i>unknown</i>] Example: Device(config-if)# standby redirect	Enables HSRP filtering of ICMP redirect messages. <ul style="list-style-type: none"> • You can also use this command in global configuration mode, which enables HSRP filtering of ICMP redirect messages on all interfaces configured for HSRP.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	show standby redirect [<i>ip-address</i>] [<i>interface-type interface-number</i>] [<i>active</i>] [<i>passive</i>] [<i>timers</i>] Example: Device# show standby redirect	(Optional) Displays ICMP redirect information on interfaces configured with HSRP.

Configuration Examples for HSRP Support for ICMP Redirects

Example: Configuring HSRP Support for ICMP Redirect Messages

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

```

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

```

```

Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2

```

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

```

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

```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP Support for ICMP Redirects

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

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



CHAPTER 8

FHRP - HSRP Multiple Group Optimization

- [Finding Feature Information, on page 119](#)
- [Information About FHRP - Multiple Group Optimization, on page 119](#)
- [How to configure FHRP - Multiple Group Optimization, on page 120](#)
- [Configuration Examples for FHRP - Multiple Group Optimization, on page 123](#)
- [Additional References, on page 125](#)
- [Feature Information for FHRP - HSRP Multiple Group Optimization, on page 126](#)

Finding Feature Information

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

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

Information About FHRP - Multiple Group Optimization

HSRP Multiple Group Optimization

The configuration of many hundreds of subinterfaces on the same physical interface, with each subinterface having its own HSRP group, can cause the processes of negotiation and maintenance of multiple HSRP groups to have a detrimental impact on network traffic and CPU utilization.

Only one HSRP group is required on a physical interface for the purposes of electing active and standby devices. This group is known as the *primary* group. Other HSRP groups may be created on each subinterface and linked to the primary group via the group name. These linked HSRP groups are known as *client* or *subordinate* groups.

The HSRP group state of the client groups follows that of the primary group. Client groups do not participate in any sort of device election mechanism.

Client groups send periodic messages in order to refresh their virtual MAC addresses in switches and learning bridges. The refresh message may be sent at a much lower frequency compared with the protocol election messages sent by the primary group.

How to configure FHRP - Multiple Group Optimization

Configuring Multiple HSRP Groups for Load Balancing

Perform this task to configure multiple HSRP groups for load balancing.

Multiple HSRP groups enable redundancy and load-sharing within networks and allow redundant devices to be more fully utilized. A device actively forwarding traffic for one HSRP group can be in standby or in the listen state for another group.

If two devices are used, then Device A would be configured as active for group 1 and standby for group 2. Device B would be standby for group 1 and active for group 2. Fifty percent of the hosts on the LAN would be configured with the virtual IP address of group 1 and the remaining hosts would be configured with the virtual IP address of group 2. See the [Example: Configuring Multiple HSRP Groups for Load Balancing](#) for a diagram and configuration example.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.
9. **exit**
10. Repeat Steps 3 through 9 on another device.

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>delay</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] ip [<i>ip-address</i>] secondary] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.
Step 8	On the same device, repeat Steps 5 through 7 to configure the device attributes for different standby groups.	For example, Device A can be configured as an active device for group 1 and be configured as an active or standby device for another HSRP group with different priority and preemption values.
Step 9	exit Example: Device(config-if)# exit	Exits to global configuration mode.
Step 10	Repeat Steps 3 through 9 on another device.	Configures multiple HSRP and enables load balancing on another device.

Improving CPU and Network Performance with HSRP Multiple Group Optimization

Perform this task to configure multiple HSRP client groups.

The **standby follow** command configures an HSRP group to become a subordinate of another HSRP group.

HSRP client groups follow the primary HSRP with a slight, random delay so that all client groups do not change at the same time.

Use the **standby mac-refresh** *seconds* command to directly change the HSRP client group refresh interval. The default interval is 10 seconds and can be configured to as much as 255 seconds.

**Note**

- Client or subordinate groups must be on the same physical interface as the primary group.
- A client group takes its state from the group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
    % Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

Before you begin

Configure the HSRP primary group using the steps in the [Configuring Multiple HSRP Groups for Load Balancing](#) section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby mac-refresh** *seconds*
6. **standby** *group-number follow group-name*
7. **exit**
8. Repeat Steps 3 through 6 to configure additional HSRP client groups.

DETAILED STEPS

	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.

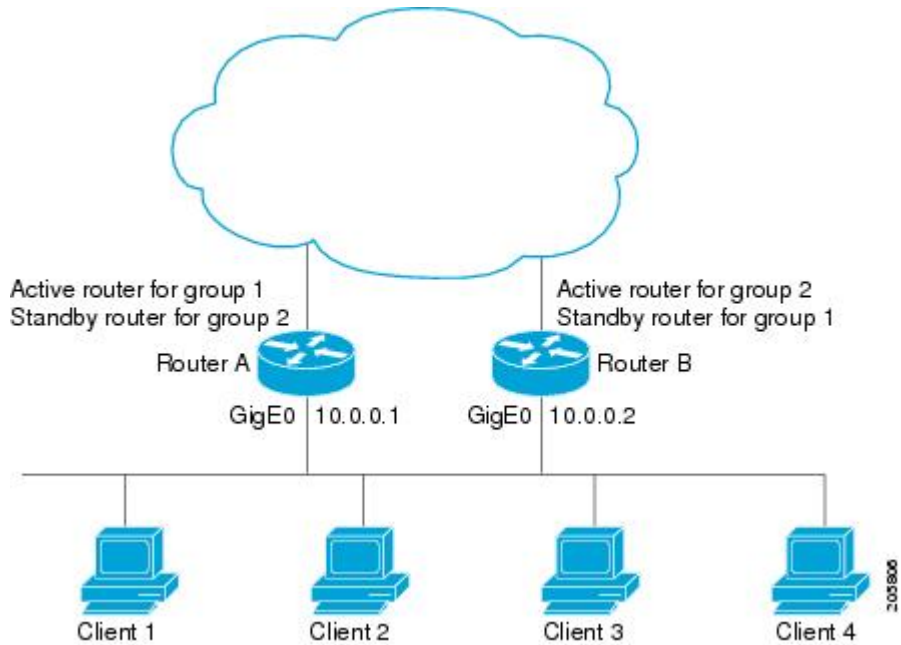
	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby mac-refresh <i>seconds</i> Example: Device(config-if)# standby mac-refresh 30	Configures the HSRP client group refresh interval.
Step 6	standby group-number follow <i>group-name</i> Example: Device(config-if)# standby 1 follow HSRP1	Configures an HSRP group as a client group.
Step 7	exit Example: Device(config-if)# exit	Exits to global configuration mode.
Step 8	Repeat Steps 3 through 6 to configure additional HSRP client groups.	Configures multiple HSRP client groups.

Configuration Examples for FHRP - Multiple Group Optimization

Example: Configuring Multiple HSRP Groups for Load Balancing

You can use HSRP or multiple HSRP groups when you configure load sharing. In the figure below, half of the clients are configured for Router A, and half of the clients are configured for Router B. Together, the configuration for Routers A and B establish two Hot Standby groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable. The **standby preempt** interface configuration command is necessary so that if a router goes down and then comes back up, preemption occurs and restores load sharing.

Figure 7: HSRP Load Sharing Example



The following example shows Router A configured as the active router for group 1 with a priority of 110 and Router B configured as the active router for group 2 with a priority of 110. The default priority level is 100. Group 1 uses a virtual IP address of 10.0.0.3 and Group 2 uses a virtual IP address of 10.0.0.4.

Router A Configuration

```
Router(config)# hostname RouterA
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

Router B Configuration

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```


Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization

The following example shows how to configure an HSRP client and primary group:

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 FHRP - HSRP Multiple Group Optimization

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.



CHAPTER 9

FHRP - HSRP Group Shutdown

- [Finding Feature Information, on page 127](#)
- [Information About FHRP - HSRP Group Shutdown, on page 127](#)
- [How to Configure FHRP - HSRP Group Shutdown, on page 128](#)
- [Configuration Examples for FHRP - HSRP Group Shutdown, on page 132](#)
- [Additional References, on page 134](#)
- [Feature Information for FHRP - HSRP Group Shutdown, on page 135](#)

Finding Feature Information

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

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

Information About FHRP - HSRP Group Shutdown

How Object Tracking Affects the Priority of an HSRP Device

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

HSRP Object Tracking

Object tracking separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process as well as HSRP. The priority of a device can change dynamically

when it has been configured for object tracking and the object that is being tracked goes down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced.

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

For more information about object tracking, see the "Configuring Enhanced Object Tracking" document.

HSRP Group Shutdown

The FHRP—HSRP Group Shutdown feature enables you to configure an HSRP group to become disabled (its state changed to Init) instead of having its priority decremented when a tracked object goes down. Use the **standby track** command with the **shutdown** keyword to configure HSRP group shutdown.

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

How to Configure FHRP - HSRP Group Shutdown

Configuring HSRP Object Tracking

Perform this task to configure HSRP to track an object and change the HSRP priority based on the state of the object.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes use this number to track a specific object.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]
8. **end**
9. **show track** [*object-number*] [**brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	track <i>object-number</i> interface <i>type number</i> {line-protocol ip routing} Example: Device(config)# track 100 interface GigabitEthernet 0/0/0 line-protocol	Configures an interface to be tracked and enters tracking configuration mode.
Step 4	exit Example: Device(config-track)# exit	Returns to global configuration mode.
Step 5	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 6	standby [<i>group-number</i>] track <i>object-number</i> [decrement <i>priority-decrement</i>] [shutdown] Example: Device(config-if)# standby 1 track 100 decrement 20	<p>Configures HSRP to track an object and change the Hot Standby priority on the basis of the state of the object.</p> <ul style="list-style-type: none"> • By default, the priority of the device is decreased by 10 if a tracked object goes down. Use the decrement <i>priority-decrement</i> keyword and argument combination to change the default behavior. • When multiple tracked objects are down and <i>priority-decrement</i> values have been configured, these configured priority decrements are cumulative. If tracked objects are down, but none of them were configured with priority decrements, the default decrement is 10 and it is cumulative. • Use the shutdown keyword to disable the HSRP group on the device when the tracked object goes down. <p>Note If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the no standby track command and then reconfigure it using the standby track command with the shutdown keyword.</p>

	Command or Action	Purpose
Step 7	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] Example: Device(config-if)# standby 1 ip 10.10.10.0	Activates HSRP. <ul style="list-style-type: none"> The default group number is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
Step 8	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 9	show track [<i>object-number</i> brief] [interface [brief] ip route [brief] resolution timers] Example: Device# show track 100 interface	Displays tracking information.

Configuring HSRP MD5 Authentication Using a Key String



Note Text authentication cannot be combined with MD5 authentication for an HSRP group at any one time. When MD5 authentication is configured, the text authentication field in HSRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving device also has MD5 authentication enabled.



Note If you are changing a key string in a group of devices, change the active device last to prevent any HSRP state change. The active device should have its key string changed no later than one hold-time period, specified by the **standby timers** interface configuration command, after the nonactive devices. This procedure ensures that the nonactive devices do not time out the active device.

SUMMARY STEPS

- enable**
- configure terminal**
- terminal interface** *type number*
- ip address** *ip-address mask* [**secondary**]
- standby** [*group-number*] **priority** *priority*
- standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
- standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*]
- standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]
- Repeat Steps 1 through 8 on each device that will communicate.
- end**
- show standby**

DETAILED STEPS

	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	terminal interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip address <i>ip-address mask [secondary]</i> Example: Device(config-if)# ip address 10.0.0.1 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 5	standby [<i>group-number</i>] priority <i>priority</i> Example: Device(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	standby [<i>group-number</i>] preempt [delay { minimum reload sync } <i>seconds</i>] Example: Device(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	standby [<i>group-number</i>] authentication md5 key-string [0 7] <i>key</i> [timeout <i>seconds</i>] Example: Device(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30	Configures an authentication string for HSRP MD5 authentication. <ul style="list-style-type: none"> • The <i>key</i> argument can be up to 64 characters in length. We recommended that at least 16 characters be used. • No prefix to the <i>key</i> argument or specifying 0 means the key will be unencrypted. • Specifying 7 means the key will be encrypted. The key-string authentication key will automatically be encrypted if the service password-encryption global configuration command is enabled.

	Command or Action	Purpose
		<ul style="list-style-type: none"> The timeout value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key.
Step 8	standby [group-number] ip [ip-address] [secondary] Example: Device(config-if)# standby 1 ip 10.0.0.3	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each device that will communicate.	—
Step 10	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 11	show standby Example: Device# show standby	(Optional) Displays HSRP information. <ul style="list-style-type: none"> Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Configuration Examples for FHRP - HSRP Group Shutdown

Example: Configuring HSRP Object Tracking

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Gigabit Ethernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IP-routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on serial interface 1/0 in Device A fails, the HSRP group priority will be reduced and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Device A Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```


Device B Configuration

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

Example: Configuring HSRP Group Shutdown

In the following example, the tracking process is configured to track the IP-routing capability of Gigabit Ethernet interface 0/0/0. HSRP on Gigabit Ethernet interface 0/0/1 then registers with the tracking process to be informed of any changes to the IP-routing state of Gigabit Ethernet interface 0/0/0. If the IP state on Gigabit Ethernet interface 0/0/0 goes down, the HSRP group is disabled.

If both Gigabit Ethernet interfaces are operational, Device A will be the HSRP active device because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Device A fails, the HSRP group will be disabled and Device B will take over as the active device, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Device A Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

Device B Configuration

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 shutdown
```

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 FHRP - HSRP Group Shutdown

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.



CHAPTER 10

SSO HSRP

- [Finding Feature Information, on page 137](#)
- [Restrictions for SSO HSRP, on page 137](#)
- [Information About SSO HSRP, on page 137](#)
- [How to Configure SSO HSRP, on page 138](#)
- [Configuration Examples for SSO HSRP, on page 141](#)
- [Additional References, on page 141](#)
- [Feature Information for SSO - HSRP, on page 143](#)

Finding Feature Information

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

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

Restrictions for SSO HSRP

- Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with HSRP in SSO mode.

Information About SSO HSRP

SSO HSRP

SSO HSRP alters the behavior of HSRP when a device with redundant Route Processors (RPs) is configured for stateful switchover (SSO) redundancy mode. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails.

With this functionality, HSRP SSO information is synchronized to the standby RP, allowing traffic that is sent using the HSRP virtual IP address to be continuously forwarded during a switchover without a loss of data or a path change. Additionally, if both RPs fail on the active HSRP device, then the standby HSRP device takes over as the active HSRP device.

The feature is enabled by default when the redundancy mode of operation is set to SSO.

SSO Dual-Route Processors and Cisco Nonstop Forwarding

SSO functions in networking devices (usually edge devices) that support dual RPs. SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

SSO is generally used with Cisco nonstop forwarding (NSF). Cisco NSF enables forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, users are less likely to experience service outages.

HSRP and SSO Working Together

The SSO HSRP feature enables the Cisco IOS HSRP subsystem software to detect that a standby RP is installed and the system is configured in SSO redundancy mode. Further, if the active RP fails, no change occurs to the HSRP group itself and traffic continues to be forwarded through the current active gateway device.

Prior to introduction of the SSO HSRP feature, when the primary RP of the active device failed, it would stop participating in the HSRP group and trigger another switch in the group to take over as the active HSRP switch.

SSO HSRP is required to preserve the forwarding path for traffic destined to the HSRP virtual IP address through an RP switchover.

Configuring SSO on the edge device enables the traffic on the Ethernet links to continue during an RP failover without the Ethernet traffic switching over to an HSRP standby device (and then back, if preemption is enabled).



Note You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

How to Configure SSO HSRP

Enabling SSO Aware HSRP

The SSO aware HSRP is enabled by default when the redundancy mode is set to SSO. Perform this task to reenable HSRP to be SSO aware if it has been disabled.



Note You may want to disable SSO HSRP by using the **no standby sso** command if you have LAN segments that should switch HSRP traffic to a redundant device while SSO maintains traffic flow for other connections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **exit**
6. **no standby sso**
7. **standby sso**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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	redundancy Example: Device(config)# redundancy	Enters redundancy configuration mode.
Step 4	mode sso Example: Device(config-red)# mode sso	Enables the redundancy mode of operation to SSO. <ul style="list-style-type: none"> • HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset.
Step 5	exit Example: Device(config-red)# exit	Exits redundancy configuration mode.
Step 6	no standby sso Example:	Disables HSRP SSO mode for all HSRP groups.

	Command or Action	Purpose
	Device(config)# no standby sso	
Step 7	standby sso Example: Device(config)# standby sso	Enables the SSO HSRP feature if you have disabled the functionality.
Step 8	end Example: Device(config)# end	Ends the current configuration session and returns to privileged EXEC mode.

Verifying SSO Aware HSRP

To verify or debug HSRP SSO operation, perform the following steps from the active RP console.

SUMMARY STEPS

1. **show standby**
2. **debug standby events ha**

DETAILED STEPS

Step 1 **show standby**

Use the **show standby** command to display the state of the standby RP, for example:

Example:

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
State is Active (standby RP)
Virtual IP address is 10.1.0.7
Active virtual MAC address is unknown
Local virtual MAC address is 000a.f3fd.5001 (bia)
Hello time 1 sec, hold time 3 sec
Authentication text "authword"
Preemption enabled
Active router is unknown
Standby router is unknown
Priority 110 (configured 120)
Track object 1 state Down decrement 10
Group name is "name1" (cfgd)
```

Step 2 **debug standby events ha**

Use the **debug standby events ha** command to display the active and standby RPs, for example:

Example:

```
Device# debug standby events ha
```



```

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active

```

Configuration Examples for SSO HSRP

Example: Enabling SSO-Aware HSRP

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

```

Device(config)# redundancy
Device(config-red)# mode sso

```

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

```

Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS First Hop redundancy Protocols Command Reference</i>

Related Topic	Document Title
HSRP for IPv6	“HSRP for IPv6” module
Troubleshooting HSRP	Hot Standby Router Protocol: Frequently Asked Questions

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 SSO - HSRP

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.



CHAPTER 11

HSRP - ISSU

- [Finding Feature Information](#), on page 145
- [Information About HSRP - ISSU](#), on page 145
- [Additional References](#), on page 146
- [Feature Information for HSRP - ISSU](#), on page 147

Finding Feature Information

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

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

Information About HSRP - ISSU

HSRP—ISSU

The In Service Software Upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

For detailed information about ISSU, see the *Cisco IOS In Service Software Upgrade Process* document in the *High Availability Configuration Guide*.

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP - ISSU

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.



CHAPTER 12

FHRP - HSRP MIB

- [Finding Feature Information, on page 149](#)
- [Information About FHRP - HSRP MIB, on page 149](#)
- [How to Configure FHRP - HSRP MIB, on page 150](#)
- [Configuration Examples for FHRP - HSRP MIB, on page 151](#)
- [Additional References, on page 151](#)
- [Feature Information for FHRP - HSRP-MIB, on page 152](#)

Finding Feature Information

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

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

Information About FHRP - HSRP MIB

HSRP MIB Traps

HSRP MIB supports Simple Network Management Protocol (SNMP) Get operations, to allow network devices to get reports about HSRP groups in a network from the network management station.

Enabling HSRP MIB trap support is performed through the CLI, and the MIB is used for getting the reports. A trap notifies the network management station when a device leaves or enters the active or standby state. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

Cisco software supports a read-only version of the MIB, and set operations are not supported.

This functionality supports four MIB tables, as follows:

- cHsrpGrpEntry table defined in CISCO-HSRP-MIB.my
- cHsrpExtIfTrackedEntry, defined in CISCO-HSRP-EXT-MIB.my

- cHsrpExtSecAddrEntry, defined in CISCO-HSRP-EXT-MIB.my
- cHsrpExtIfEntry defined in CISCO-HSRP-EXT-MIB.my

The cHsrpGrpEntry table consists of all the group information defined in RFC 2281, *Cisco Hot Standby Router Protocol*; the other tables consist of the Cisco extensions to RFC 2281, which are defined in CISCO-HSRP-EXT-MIB.my.

How to Configure FHRP - HSRP MIB

Enabling HSRP MIB Traps

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server enable traps hsrp
4. snmp-server host *host community-string* hsrp

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: 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	snmp-server enable traps hsrp Example: Device(config)# snmp-server enable traps hsrp	Enables the device to send SNMP traps and informs, and HSRP notifications.
Step 4	snmp-server host <i>host community-string</i> hsrp Example: Device(config)# snmp-server host myhost.comp.com public hsrp	Specifies the recipient of an SNMP notification operation, and that HSRP notifications be sent to the host.

Configuration Examples for FHRP - HSRP MIB

Example: Enabling HSRP MIB Traps

The following examples show how to configure HSRP on two devices and enable the HSRP MIB trap support functionality. As in many environments, one device is preferred as the active one. To configure a device's preference as the active device, configure the device at a higher priority level and enable preemption. In the following example, the active device is referred to as the primary device. The second device is referred to as the backup device:

Device A

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host yourhost.cisco.com public hsrp
```

Device B

```
Device(config)#interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.2 255.255.0.0
Device(config-if)# standby priority 101
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host myhost.cisco.com public hsrp
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 FHRP - HSRP-MIB

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.



CHAPTER 13

HSRP Support for MPLS VPNs

- [Finding Feature Information, on page 153](#)
- [Information About HSRP Support for MPLS VPNs, on page 153](#)
- [Additional References, on page 154](#)
- [Feature Information for HSRP Support for MPLS VPNs, on page 155](#)

Finding Feature Information

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

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

Information About HSRP Support for MPLS VPNs

HSRP Support for MPLS VPNs

HSRP support for a Multiprotocol Label Switching (MPLS) VPN interface is useful when an Ethernet LAN is connected between two provider edge (PE) devices with either of the following conditions:

- A customer edge (CE) device with a default route to the HSRP virtual IP address
- One or more hosts with the HSRP virtual IP address configured as the default gateway

Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding table
- Set of interfaces that use the Cisco Express Forwarding forwarding table
- Set of rules and routing protocol parameters to control the information in the routing tables

VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of routing and Cisco Express Forwarding tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that are outside a VPN from being forwarded to a device within the VPN.

HSRP adds ARP entries and IP hash table entries (aliases) using the default routing table instance. However, a different routing table instance is used when VRF forwarding is configured on an interface, causing ARP and ICMP echo requests for the HSRP virtual IP address to fail.

HSRP support for MPLS VPNs ensures that the HSRP virtual IP address is added to the correct IP routing table and not to the default routing table.

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>

RFCs	Title
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 2281	<i>Cisco Hot Standby Router 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 HSRP Support for MPLS VPNs

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.



CHAPTER 14

Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual primary router, with the other routers acting as backups in case the virtual primary router fails.

This module explains the concepts related to VRRP and describes how to configure VRRP in a network.

- [Finding Feature Information, on page 157](#)
- [Restrictions for VRRP, on page 157](#)
- [Information About VRRP, on page 158](#)
- [How to Configure VRRP, on page 163](#)
- [Configuration Examples for VRRPv2, on page 170](#)
- [Additional References, on page 172](#)
- [Feature Information for VRRP, on page 173](#)
- [Glossary, on page 173](#)

Finding Feature Information

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

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

Restrictions for VRRP

- VRRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. VRRP is not intended as a replacement for existing dynamic protocols.
- VRRP is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.

- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must configure the VRRP advertise timer to a value equal to or greater than the forwarding delay on the BVI interface. This setting prevents a VRRP router 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.

Information About VRRP

VRRP Operation

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- ICMP Router Discovery Protocol (IRDP) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

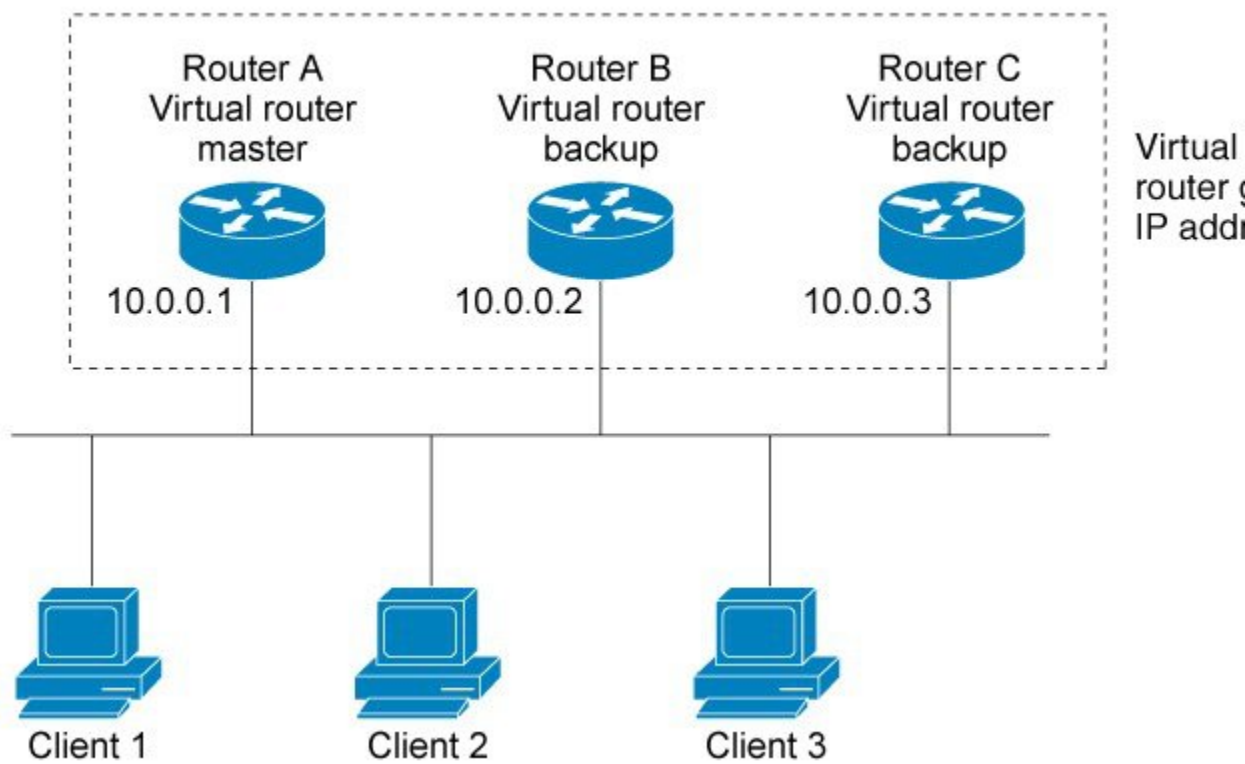
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single *virtual router*. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, and on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

The figure below shows a LAN topology in which VRRP is configured. In this example, Routers A, B, and C are VRRP routers (routers running VRRP) that comprise a virtual router. The IP address of the virtual router is the same as that configured for the Ethernet interface of Router A (10.0.0.1).

Figure 8: Basic VRRP Topology

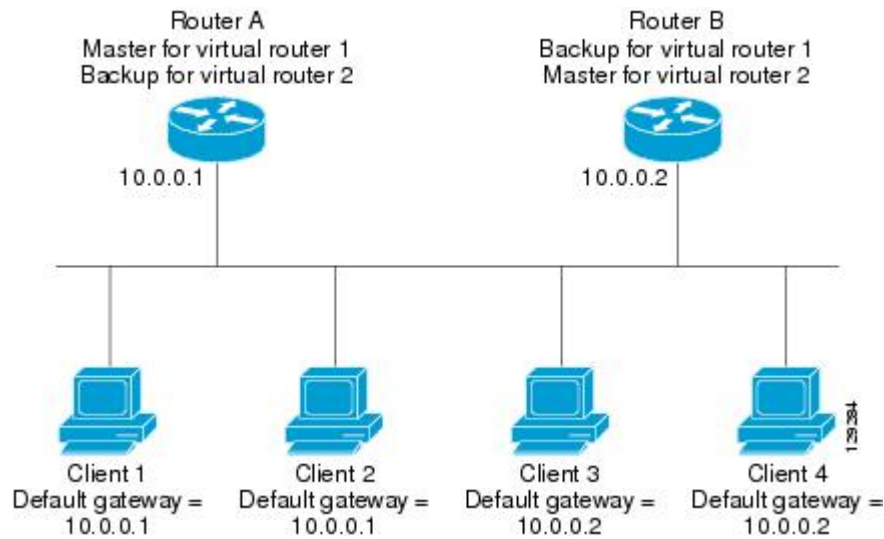


Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual primary router and is also known as the IP address owner. As the virtual primary router, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 10.0.0.1.

Routers B and C function as virtual router backups. If the virtual primary router fails, the router configured with the higher priority will become the virtual primary router and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual primary router again. For more detail on the roles that VRRP routers play and what happens if the virtual primary router fails, see the [VRRP Router Priority and Preemption](#) section.

The figure below shows a LAN topology in which VRRP is configured so that Routers A and B share the traffic to and from clients 1 through 4 and that Routers A and B act as virtual router backups to each other if either router fails.

Figure 9: Load Sharing and Redundancy VRRP Topology



In this topology, two virtual routers are configured. (For more information, see the [Multiple Virtual Router Support](#) section.) For virtual router 1, Router A is the owner of IP address 10.0.0.1 and virtual primary router, and Router B is the virtual router backup to Router A. Clients 1 and 2 are configured with the default gateway IP address of 10.0.0.1.

For virtual router 2, Router B is the owner of IP address 10.0.0.2 and virtual primary router, and Router A is the virtual router backup to Router B. Clients 3 and 4 are configured with the default gateway IP address of 10.0.0.2.

VRRP Benefits

Redundancy

VRRP enables you to configure multiple routers as the default gateway router, 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 routers, thereby sharing the traffic load more equitably among available routers.

Multiple Virtual Routers

Multiple IP Addresses

The virtual router 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.

Preemption

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

Authentication

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

Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

VRRP Object Tracking

VRRP object tracking provides a way to ensure the best VRRP router is the virtual primary router for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states.

Multiple Virtual Router Support

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

In a topology where multiple virtual routers are configured on a router interface, the interface can act as primary for one virtual router and as a backup for one or more virtual routers.

VRRP Router Priority and Preemption

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

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

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming virtual primary router if the virtual primary router fails. You can configure the priority of each virtual router backup with a value of 1 through 254 using the **vrrp priority** command.

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

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual primary router. You can disable this preemptive scheme using the **no vrrp preempt** command. If preemption is disabled, the virtual router backup that is elected to become virtual primary router remains as the primary until the original virtual primary router recovers and becomes the primary again.

VRRP Advertisements

The virtual primary router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual primary router. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco routers allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup routers. The primary advertisement value displayed in the **show vrrp** command output on the backup routers is always 1 second because the packets on the backup routers 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, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only.

VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process allows you to track individual objects such as the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP device. You specify the object number to be tracked and VRRP is notified of any change to the object. VRRP increments (or decrements) the priority of the virtual device based on the state of the object being tracked.

How VRRP Object Tracking Affects the Priority of a Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the VRRP priority is reduced. The VRRP device with the higher priority can now become the virtual primary device if it has the **vrrp preempt** command configured. See the “VRRP Object Tracking” section for more information on object tracking.

In Service Software Upgrade--VRRP

VRRP supports In Service Software Upgrade (ISSU). In Service Software Upgrade (ISSU) allows a high-availability (HA) system to run in stateful switchover (SSO) mode even when different versions of software are running on the active and standby Route Processors (RPs) or line cards.

ISSU provides the ability to upgrade or downgrade from one supported release to another while continuing to forward packets and maintain sessions, thereby reducing planned outage time. The ability to upgrade or downgrade is achieved by running different software versions on the active RP and standby RP for a short period of time to maintain state information between RPs. This feature allows the system to switch over to a secondary RP running upgraded (or downgraded) software and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default.

For detailed information about ISSU, see the In Service Software Upgrade Process document in the *High Availability Configuration Guide*.

VRRP Support for Stateful Switchover

With the introduction of the VRRP Support for Stateful Switchover feature, VRRP is SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual Route Processors (RPs). SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Prior to being SSO aware, if VRRP was deployed on a router with redundant RPs, a switchover of roles between the active RP and the standby RP would result in the router relinquishing its activity as a VRRP group member and then rejoining the group as if it had been reloaded. The SSO--VRRP feature enables VRRP to continue its activities as a group member during a switchover. VRRP state information between redundant RPs is maintained so that the standby RP can continue the router's activities within the VRRP during and after a switchover.

This feature is enabled by default. To disable this feature, use the **no vrrp sso** command in global configuration mode.

For more information, see the Stateful Switchover document.

How to Configure VRRP

VRRP

Customizing the behavior of VRRP is optional. Be aware that as soon as you enable a VRRP group, that group is operating. It is possible that if you first enable a VRRP group before customizing VRRP, the router could take over control of the group and become the virtual primary router before you have finished customizing the feature. Therefore, if you plan to customize VRRP, it is a good idea to do so before enabling VRRP.

Step 1 **enable**
Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **interface *type number***

Example:

```
Router(config)#GigabitEthernet 0/0/0
```

Enters interface configuration mode.

Step 4 **ip address *ip-address mask***

Example:

```
Router(config-if)# ip address 172.16.6.5 255.255.255.0
```

Configures an IP address for an interface.

Step 5 **vrrp group *description text***

Example:

```
Router(config-if)# vrrp 10 description working-group
```

Assigns a text description to the VRRP group.

Step 6 **vrrp group *priority level***

Example:

```
Router(config-if)# vrrp 10 priority 110
```

Sets the priority level of the router within a VRRP group.

- The default priority is 100.

Step 7 **vrrp group preempt [**delay minimum *seconds***]**

Example:

```
Router(config-if)# vrrp 10 preempt delay minimum 380
```

Configures the router to take over as virtual primary router for a VRRP group if it has a higher priority than the current virtual primary router.

- The default delay period is 0 seconds.
- The router that is IP address owner will preempt, regardless of the setting of this command.

Step 8 **vrrp group timers learn****Example:**

```
Router(config-if)# vrrp 10 timers learn
```

Configures the router, when it is acting as virtual router backup for a VRRP group, to learn the advertisement interval used by the virtual primary router.

Step 9 **exit****Example:**

```
Router(config-if)# exit
```

Exits interface configuration mode.

Step 10 **no vrrp sso****Example:**

```
Router(config)# no vrrp sso
```

(Optional) Disables VRRP support of SSO.

- VRRP support of SSO is enabled by default.

Enabling/Verifying VRRP

Step 1 **enable****Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal****Example:**

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **interface type number****Example:**

```
Router(config)# interface GigabitEthernet 0/0/0
```

Enters interface configuration mode.

Step 4 `ip address ip-address mask`**Example:**

```
Router(config-if)# ip address 172.16.6.5 255.255.255.0
```

Configures an IP address for an interface.

Step 5 `vrrp group ip ip-address [secondary]`**Example:**

```
Router(config-if)# vrrp 10 ip 172.16.6.1
```

Enables VRRP on an interface.

- After you identify a primary IP address, you can use the **vrrp ip** command again with the **secondary** keyword to indicate additional IP addresses supported by this group.

Note All routers in the VRRP group must be configured with the same primary address and a matching list of secondary addresses for the virtual router. If different primary or secondary addresses are configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to primary.

Step 6 `show vrrp [brief all] [interface]`**Example:**

```
Router(config-if)#show vrrp brief
Interface Grp Pri Time Own Pre State Master addr Group addr
BD10 1 100 9609 Y Backup 10.1.0.2 10.1.0.10
BD10 5 200 90218 Y Master 10.1.0.1 10.1.0.50
BD10 100 100 3609 Backup 10.1.0.2 10.1.0.100
```

(Optional) Displays a brief or detailed status of one or all VRRP groups on the router.

Step 7 `show vrrp interface type number [brief]`**Example:**

```
Router(config)# interfaceGigabitEthernet 0/0/0
Router)config-if)#show vrrp interface bdi10
BDI10 - Group 10
G1
State is Master
Virtual IP address is 10.0.0.5
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 10.000 sec
Preemption enabled, delay min 380 secs
Priority is 110
Master Router is 10.0.0.2 (local), priority is 110
Master Advertisement interval is 10.000 sec
Master Down interval is 30.570 sec
FLAGS: 1/1
```

(Optional) Displays the VRRP groups and their status on a specified interface.

Step 8 `end`**Example:**

```
Router(config-if)# end
```

Returns to privileged EXEC mode.

Configuring VRRP Object Tracking



Note If a VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through object tracking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **vrrp group ip** *ip-address*
6. **vrrp group priority** *level*
7. **vrrp group track** *object-number* [**decrement** *priority*]
8. **end**
9. **show track** [*object-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	track <i>object-number</i> interface <i>type number</i> { line-protocol ip routing }	Configures an interface to be tracked where changes in the state of the interface affect the priority of a VRRP group. <ul style="list-style-type: none"> • This command configures the interface and corresponding object number to be used with the vrrp track command. • The line-protocol keyword tracks whether the interface is up. The ip routing keyword also checks that IP routing is enabled and active on the interface.

	Command or Action	Purpose
		<ul style="list-style-type: none"> You can also use the track ip route command to track the reachability of an IP route or a metric type object.
Step 4	interface <i>type number</i> Example: Router(config)# interface Ethernet 2	Enters interface configuration mode.
Step 5	vrrp group ip <i>ip-address</i> Example: Router(config-if)# vrrp 1 ip 10.0.1.20	Enables VRRP on an interface and identifies the IP address of the virtual router.
Step 6	vrrp group priority <i>level</i> Example: Router(config-if)# vrrp 1 priority 120	Sets the priority level of the router within a VRRP group.
Step 7	vrrp group track <i>object-number</i> [decrement <i>priority</i>] Example: Router(config-if)# vrrp 1 track 2 decrement 15	Configures VRRP to track an object.
Step 8	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 9	show track [<i>object-number</i>] Example: Router# show track 1	Displays tracking information.

Configuring VRRP Text Authentication

Before you begin

Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.

Text authentication cannot be combined with MD5 authentication for a VRRP group at any one time. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeros on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

Step 1 **enable**
Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **terminal interface** *type number*

Example:

```
Router(config)# interfaceGigabitEthernet 0/0/0 Ethernet 0/1
```

Configures an interface type and enters interface configuration mode.

Step 4 **ip address** *ip-address mask* [**secondary**]

Example:

```
Router(config-if)# ip address 10.0.0.1 255.255.255.0
```

Specifies a primary or secondary IP address for an interface.

Step 5 **vrrp group authentication text** *text-string*

Example:

```
Router(config-if)# vrrp 1 authentication text textstring1
```

Authenticates VRRP packets received from other routers in the group.

- If you configure authentication, all routers within the VRRP group must use the same authentication string.
- The default string is cisco.

Note All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to primary.

Step 6 **vrrp group ip** *ip-address*

Example:

```
Router(config-if)# vrrp 1 ip 10.0.1.20
```

Enables VRRP on an interface and identifies the IP address of the virtual router.

Step 7 Repeat Steps 1 through 6 on each router that will communicate.

—

Step 8 **end**

Example:

```
Router(config-if)# end
```

Returns to privileged EXEC mode.

Configuration Examples for VRRPv2

Example: Configuring VRRP

In the following example, Router A and Router B each belong to three VRRP groups.

In the configuration, each group has the following properties:

- Group 1:
 - Virtual IP address is 10.1.0.10.
 - Router A will become the primary for this group with priority 120.
 - Advertising interval is 3 seconds.
 - Preemption is enabled.
- Group 5:
 - Router B will become the primary for this group with priority 200.
 - Advertising interval is 30 seconds.
 - Preemption is enabled.
- Group 100:
 - Router A will become the primary for this group first because it has a higher IP address (10.1.0.2).
 - Advertising interval is the default 1 second.
 - Preemption is disabled.

Router A

```
Router(config)#
Router(config)# interface GigabitEthernet 0/0/0 interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 authentication text cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 100
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

Router B

```

Router(config)#GigabitEthernet 0/0/0interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication text cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 200
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown

```

Example: VRRP Object Tracking

In the following example, the tracking process is configured to track the state of the line protocol on serial interface 0/1. VRRP on Ethernet interface 1/0 then registers with the tracking process to be informed of any changes to the line protocol state of serial interface 0/1. If the line protocol state on serial interface 0/1 goes down, then the priority of the VRRP group is reduced by 15.

```

Router(config)# track 1 interface Serial 0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet 1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.0.0.3
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 track 1 decrement 15

```

Example: VRRP Object Tracking Verification

The following examples verify the configuration shown in the [Example: VRRP Object Tracking](#) section:

```

Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption is enabled
    min delay is 0.000 sec
  Priority is 105
    Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
    1 change, last change 00:06:53

```

```
Tracked by:
  VRRP Ethernet1/0 1
```

Example: VRRP Text Authentication

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

```
Router(config)#GigabitEthernet 0/0/0interface GigabitEthernet 0/0/0
Router(config)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
```

Example: VRRP MIB Trap

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host 10.1.1.0 community abc vrrp
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VRRP commands	<i>Cisco IOS IP Application Services Command Reference</i>
Object tracking	Configuring Enhanced Object Tracking
Hot Standby Routing Protocol (HSRP)	Configuring HSRP
In Service Software Upgrade (ISSU)	"In Service Software Upgrade Process" in the <i>High Availability Configuration Guide</i>
Gateway Load Balancing Protocol (GLBP)	Configuring GLBP
Stateful Switchover	The Stateful Switchover section in the <i>High Availability Configuration Guide</i>

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 2338	Virtual Router Redundancy Protocol
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768	Virtual Router Redundancy Protocol (VRRP)

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 VRRP

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.

Glossary

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

virtual router —One or more VRRP routers that form a group. The virtual router acts as the default gateway router for LAN clients. Also known as a VRRP group.

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

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

VRRP router --A router that is running VRRP.



CHAPTER 15

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.

- [Finding Feature Information, on page 175](#)
- [Restrictions for VRRPv3 Protocol Support, on page 176](#)
- [Information About VRRPv3 Protocol Support, on page 176](#)
- [How to Configure VRRPv3 Protocol Support, on page 178](#)
- [Configuration Examples for VRRPv3 Protocol Support, on page 182](#)
- [Additional References for VRRPv3 Protocol Support, on page 184](#)
- [Feature Information for VRRPv3 Protocol Support, on page 185](#)
- [Glossary, on page 185](#)

Finding Feature Information

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

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

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 Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and 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).
- VRRPv3 protocol does not support authentication.
- 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 router master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual router master. 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 routers 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 routers. The master advertisement value displayed in the **show vrrp** command output on the backup routers is always 1 second because the packets on the backup routers 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

IPv6 VRRP Link Local Address

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.

Enabling VRRPv3 on a Device

To enable VRRPv3 on a device, perform the following task:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **fhrp version vrrp v3**
4. **end**

DETAILED STEPS

	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. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.

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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {*ipv4* | *ipv6*}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay** **minimum** *seconds*
10. **priority** *priority-level*
11. **timers** **advertise** *interval*
12. **vrrpv2**
13. **vrrs** **leader** *vrrs-leader-name*

14. shutdown
15. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	fhrp version vrrp v3 Example: Device(config)# fhrp version vrrp v3	Enables the ability to configure VRRPv3 and VRRS. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	interface type number Example: Device(config)# interface GigabitEthernet 0/0/0	Enters interface configuration mode.
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:	(Optional) Matches secondary address in the advertisement packet against the configured address. • Secondary address matching is enabled by default.

	Command or Action	Purpose
	Device(config-if-vrrp)# match-address	
Step 9	<p>preempt delay minimum <i>seconds</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# preempt delay minimum 30</pre>	<p>(Optional) Enables preemption of lower priority primary device with an optional delay.</p> <ul style="list-style-type: none"> • Preemption is enabled by default.
Step 10	<p>priority <i>priority-level</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# priority 3</pre>	<p>(Optional) Specifies the priority value of the VRRP group.</p> <ul style="list-style-type: none"> • The priority of a VRRP group is 100 by default.
Step 11	<p>timers advertise <i>interval</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# timers advertise 1000</pre>	<p>(Optional) Sets the advertisement timer in milliseconds.</p> <ul style="list-style-type: none"> • The advertisement timer is set to 1000 milliseconds by default.
Step 12	<p>vrrpv2</p> <p>Example:</p> <pre>Device(config-if-vrrp)# vrrpv2</pre>	<p>(Optional) Enables support for VRRPv2 simultaneously, so as to interoperate with devices which only support VRRP v2.</p> <ul style="list-style-type: none"> • VRRPv2 is disabled by default.
Step 13	<p>vrrs leader <i>vrrs-leader-name</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# vrrs leader leader-1</pre>	<p>(Optional) Specifies a leader's name to be registered with VRRS and to be used by followers.</p> <ul style="list-style-type: none"> • A registered VRRS name is unavailable by default.
Step 14	<p>shutdown</p> <p>Example:</p> <pre>Device(config-if-vrrp)# shutdown</pre>	<p>(Optional) Disables VRRP configuration for the VRRP group.</p> <ul style="list-style-type: none"> • VRRP configuration is enabled for a VRRP group by default.
Step 15	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>

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:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface *type number***
5. **fhrp delay {[minimum] [reload] *seconds*}**
6. **end**

DETAILED STEPS

	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. 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] <i>seconds</i>} 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 gigabitethernet0/0
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 gigabitethernet0/0
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

Ethernet0/0 - Group 1 - Address-Family IPv4

State is MASTER
```

```

State duration 3.707 secs
Virtual IP address is 1.0.0.10
Virtual MAC address is 0000.5E00.0101
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
Master Router is 1.0.0.1 (local), priority is 100
Master Advertisement interval is 1000 msec (expires in 686 msec)
Master Down interval is unknown
State is MASTER
State duration 3.707 secs
VRRPv3 Advertisements: sent 5 (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 Mon Jul 30 16:42:01.856)
  Backup to master: 1 (Last change Mon Jul 30 16:42:05.469)
  Master to backup: 0
  Master to init: 0
  Backup to init: 0

```

Device# **exit**

Additional References for VRRPv3 Protocol Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
FHRP commands	First Hop Redundancy Protocols Command Reference
Configuring VRRPv2	<i>Configuring VRRP</i>

Standards and RFCs

Standard/RFC	Title
RFC5798	<i>Virtual Router Redundancy Protocol</i>
RFC 6527	<i>Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)</i>

MIBs

MIB	MIBs Link
VRRPv3 MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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.

Glossary

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

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

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

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

VRRP router—A router that is running VRRP.



CHAPTER 16

VRRPv3: Object Tracking Integration

Virtual Router Redundancy Protocol (VRRP) enables a group of devices to form a single virtual device to provide redundancy. The LAN clients then can be configured with the virtual device as the default gateway. The virtual device, representing a group of devices, is also known as a VRRP group. The VRRPv3: Object Tracking Integration feature allows you to track the behavior of an object and receive notifications of changes. This module explains how object tracking, in particular the tracking of IPv6 objects, is integrated into VRRP version 3 (VRRPv3) and describes how to track an IPv6 object using a VRRPv3 group. See the “VRRP Object Tracking” section for more information on object tracking.

- [Finding Feature Information, on page 187](#)
- [Information About VRRPv3: Object Tracking Integration, on page 187](#)
- [How to Configure VRRPv3: Object Tracking Integration, on page 188](#)
- [Configuration Examples for VRRPv3: Object Tracking Integration, on page 189](#)
- [Additional References for VRRPv3: Object Tracking Integration, on page 190](#)
- [Feature Information for VRRPv3: Object Tracking Integration, on page 191](#)

Finding Feature Information

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

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

Information About VRRPv3: Object Tracking Integration

VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process allows you to track individual objects such as the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP device. You specify the object number to be tracked and VRRP is notified of any change to the object. VRRP increments (or decrements) the priority of the virtual device based on the state of the object being tracked.

How VRRP Object Tracking Affects the Priority of a Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the VRRP priority is reduced. The VRRP device with the higher priority can now become the virtual primary device if it has the **vrrp preempt** command configured. See the “VRRP Object Tracking” section for more information on object tracking.

How to Configure VRRPv3: Object Tracking Integration

Tracking an IPv6 Object using VRRPv3

SUMMARY STEPS

1. **fhrp version vrrp v3**
2. **interface** *type number*
3. **vrrp group-id address-family ipv6**
4. **track object-number decrement number**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	fhrp version vrrp v3 Example: Device(config)# fhrp version vrrp v3	Enables you to configure Virtual Router Redundancy Protocol version 3 (VRRPv3) and Virtual Router Redundancy Service (VRRS) on a device. Note When VRRPv3 is in use, VRRPv2 is unavailable.

	Command or Action	Purpose
Step 2	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 3	vrrp <i>group-id address-family ipv6</i> Example: Device(config-if)# vrrp 1 address-family ipv6	Creates a VRRP group for IPv6 and enters VRRP configuration mode.
Step 4	track <i>object-number decrement number</i> Example: Device(config-if-vrrp)# track 1 decrement 20	Configures the tracking process to track the state of the IPv6 object using the VRRPv3 group. VRRP on Ethernet interface 0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20.
Step 5	end Example: Device(config-if-vrrp)# end	Returns to privileged EXEC mode.

Configuration Examples for VRRPv3: Object Tracking Integration

Example: Tracking an IPv6 Object using VRRPv3

In the following example, the tracking process is configured to track the state of the IPv6 object using the VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20:

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

Example: Verifying VRRP IPv6 Object Tracking

```
Device# show vrrp

Ethernet0/0 - Group 1 - Address-Family IPv4
  State is BACKUP
  State duration 1 mins 41.856 secs
  Virtual IP address is 172.24.1.253
```

```

Virtual MAC address is 0000.5E00.0101
Advertisement interval is 1000 msec
Preemption enabled
Priority is 80 (configured 100)
  Track object 1 state Down decrement 20
Master Router is 172.24.1.2, priority is 100
Master Advertisement interval is 1000 msec (learned)
Master Down interval is 3609 msec (expires in 3297 msec)

```

Device# **show track ipv6 route brief**

Track	Type	Instance	Parameter	State	Last Change
601	ipv6 route	3172::1/32	metric threshold	Down	00:08:55
602	ipv6 route	3192:ABCD::1/64	metric threshold	Down	00:08:55
603	ipv6 route	3108:ABCD::CDEF:1/96	metric threshold	Down	00:08:55
604	ipv6 route	3162::EF01/16	metric threshold	Down	00:08:55
605	ipv6 route	3289::2/64	metric threshold	Down	00:08:55
606	ipv6 route	3888::1200/64	metric threshold	Down	00:08:55
607	ipv6 route	7001::AAAA/64	metric threshold	Down	00:08:55
608	ipv6 route	9999::BBBB/64	metric threshold	Down	00:08:55
611	ipv6 route	1111::1111/64	reachability	Down	00:08:55
612	ipv6 route	2222:3333::4444/64	reachability	Down	00:08:55
613	ipv6 route	5555::5555/64	reachability	Down	00:08:55
614	ipv6 route	3192::1/128	reachability	Down	00:08:55

Additional References for VRRPv3: Object Tracking Integration

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS First Hop Redundancy Protocols Command Reference</i>
Troubleshooting HSRP	<i>Hot Standby Router Protocol: Frequently Asked Questions</i>

RFCs

RFCs	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 1828	<i>IP Authentication Using Keyed MD5</i>
RFC 5798	<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: Object Tracking Integration



CHAPTER 17

Virtual Router Redundancy Service

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between the Virtual Router Redundancy Protocol (VRRP), VRRS pathways and optional VRRS clients. The VRRS multiclient service provides a consistent interface with VRRP by abstracting over several First Hop Redundancy Protocols (FHRPs) and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named VRRP groups.

VRRP acts as a server that pushes VRRP status information out to VRRS pathways, and all registered VRRS clients. Pathways and clients obtain status on all essential information provided by VRRP, including current and previous redundancy states, active and inactive Layer 2 and Layer 3 addresses, and, in some cases, information about other redundant gateways in the network. Pathways use this information in order to provide scaled first-hop gateway redundancy across scaled interface environments. VRRS clients will also use this information to provide stateless and stateful redundancy information to clients and protocols.



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

- [Finding Feature Information, on page 193](#)
- [Restrictions for VRRS, on page 194](#)
- [Information About VRRS, on page 194](#)
- [How to Configure VRRS, on page 196](#)
- [Configuration Examples for VRRS, on page 202](#)
- [Additional References, on page 202](#)
- [Feature Information for Virtual Router Redundancy Service , on page 203](#)

Finding Feature Information

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

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

Restrictions for VRRS

- VRRS plug-ins must be configured on subinterfaces that are not configured with VRRP, but which share a physical interface with a VRRP group it is following.
- VRRP Version 2 (VRRPv2) is configurable only on Gigabit Ethernet interfaces.
- VRRS is currently only available for use with VRRP Version 3 (VRRPv3).

Information About VRRS

VRRS Overview

VRRS improves the scalability of VRRP. VRRS provides a stateless redundancy service to VRRS pathways and applications (VRRS clients) by monitoring VRRP. VRRS provides a database of the current VRRP state and provides a “push” data service to the VRRS pathways and clients with which it communicates. VRRP acts as a VRRS server. VRRS clients are other Cisco processes or applications that use VRRP to provide or withhold a service or resource dependent upon the state of the group. VRRS pathways are special VRRS clients that use the VRRS database information in order to provide scaled first-hop gateway redundancy across scaled interface environments.

The VRRS by itself is limited to maintaining its own state. Linking a VRRS client to a VRRP group provides a mechanism that allows VRRS to provide a service to client applications so that they can implement stateless or stateful failover. Stateless failover is failover without syncing of state. Stateful failover requires communication with a nominated backup before failure so that operational data is not lost when failover occurs.

VRRS pathways operate in a similar way to clients, but are integrated with the VRRS architecture. They provide a means to scale first-hop gateway redundancy by allowing the user the opportunity to configure a virtual address across hundreds of interfaces. The “virtual gateway” state of a VRRS pathway follows the state of an FHRP VRRS server.

Using VRRS with VRRP

VRRP provides server support for VRRS. The VRRP server pushes state and status information to VRRS when an internal update occurs. VRRS updates its internal database upon receiving a server update, and then sends push notifications to each of the VRRS clients associated with the shared name. Clients are interested in the protocol state, virtual MAC (vMAC) address, and virtual IP address information associated with a group. The association name between a client and a VRRP group is a character name string. The information provided by VRRS allows clients to perform various activities that are dependent on the state of the associated VRRP group.

VRRP notifies VRRS of its current state (primary, backup, or nonoperational initial state [INIT]). The VRRP state is then passed on to pathways or clients. A VRRP group should be configured with a name to activate VRRS. Pathways or clients should be configured with the same name to bind them with VRRS.

The VRRP group name associates the VRRP group with any clients that are configured as part of VRRS with the same name.

VRRS Servers and Clients

VRRP acts as the VRRS server. Pathways and clients act on the VRRP server state. When a VRRP group changes state, VRRS pathways and clients act by altering their behaviour (performing tasks such as shutting down interfaces or appending accounting logs) depending on the state received from VRRS.

VRRS Pathways and Pathway Manager

VRRS Pathways

A VRRS pathway is defined as an entity that will provide IPv4 or IPv6 traffic forwarding duties using the following features on an Ethernet interface (such as a physical interface, subinterface, or a Switch Virtual Interface [SVI]):

- vMAC address insertion and removal into the hardware driver using MACdb.
- Virtual IP (vIP) insertion and removal using the IPv4 and IPv6 APIs.
- Provision to associate the vIP with the interface burned-in address (BIA) MAC.
- Provision to associate the vMAC address with the interface-owned vIP.
- Maintain the association of a vMAC with a vIP on a LAN using the Address Resolution Protocol (ARP) or Neighbor Discovery Protocol.
- Maintain the switching cache (content-addressable memory or [CAM]) of connected Layer 2 devices on the LAN.
- Checkpoints all data and the pathway state with a High Availability module.

A Pathway will provide some of the above features using its association with either the VRRS Pathway L2 Controller or the VRRS Pathway L3 Controller.

VRRS Pathway Manager

The VRRS Pathway Manager provides the following features:

- Creates an association between one or more VRRS pathway instances and a single VRRS database name entry.
- Pushes configuration and state information to associated registered pathways in response to a push from VRRS.
- Provides debugging and show output to the user. The output is related to the state and configuration of the VRRS pathway manager.
- Is Online Insertion and Removal (OIR)-aware and manages pathways that may be affected by OIR events.
- Is Virtual Routing and Forwarding (VRF)-aware and manages pathways that may be affected by VRF events.

How to Configure VRRS

Configuring VRRPv3 Control Groups

Perform the following task to configure a VRRP control group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **vrrp group-id address-family** { **ipv4** | **ipv6** }
7. **address** *ip-address* [**primary** | **secondary**]
8. **vrrs leader** *vrrs-leader-name*
9. **end**

DETAILED STEPS

	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. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	interface <i>type number</i> Example: Device(config)# interface vlan 40	Enters interface configuration mode.
Step 5	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 209.165.200.230	Configures the IP address on the interface.

	Command or Action	Purpose
	255.255.255.224	
Step 6	vrrp <i>group-id</i> address-family { ipv4 ipv6 } Example: Device(config-if)# vrrp 1 address-family ipv4	Creates a VRRP group and enters VRRP configuration mode.
Step 7	address <i>ip-address</i> [primary secondary] Example: Device(config-if-vrrp)# address 209.165.202.141	Specifies a primary or secondary address for the VRRP group.
Step 8	vrrs leader <i>vrrs-leader-name</i> Example: Device(config-if-vrrp)# vrrs leader group1	Specifies a leader's name to be registered with VRRS and enables a VRRP group to control a VRRS pathway. <ul style="list-style-type: none"> It is possible for a single VRRP instance to control more than one VRRS group. A registered VRRS name is unavailable by default.
Step 9	end Example: Device(config-if-vrrp)# end	Returns to privileged EXEC mode.

Configuring VRRS Pathways

Perform the following task to configure a VRRP pathway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **vrrs pathway** *vrrs-leader-name*
7. **mac address** *mac-address*
8. **address** *ip-address*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
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. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	interface type number Example: Device(config)# interface vlan 42	Enters interface configuration mode.
Step 5	ip address ip-address mask Example: Device(config-if)# ip address 209.165.201.25 255.255.255.224	Configures the IP address on the interface.
Step 6	vrrs pathway vrrs-leader-name Example: Device(config-if)# vrrs pathway group1	Defines the VRRS pathway for a VRRS group and enters VRRS pathway configuration mode.
Step 7	mac address mac-address Example: Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24	Specifies a MAC address used by a pathway.
Step 8	address ip-address Example: Device(config-if-vrrs-pw)# address 209.165.201.10	Defines the virtual IP for a pathway. • Note A VRRP group is capable of controlling more than one pathway.
Step 9	end Example: Device(config-if-vrrs-pw)# end	Returns to privileged EXEC mode. • Note Repeat steps 1 to 9 to configure more pathways.

Verifying VRRS

Perform this task to verify VRRS functions.



Note The **show** commands are not in any specific order. The **show vrrs pathway** command for different pathway states (active, inactive, and “not ready”) is displayed below.

SUMMARY STEPS

1. **enable**
2. **show vrrs pathway**
3. **show vrrs pathway**
4. **show vrrs pathway**
5. **show vrrs server**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show vrrs pathway

Displays VRRS pathway information for an active pathway with the tag name “group1” and VRRP in primary state on the VLAN interface.

Example:

```
Device# show vrrs pathway

Pathway ["group1"@Vlan42]
State is ACTIVE [VRRS push "ACTIVE"]
Virtual MAC is fe24.fe24.fe24 [Active] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

Step 3 show vrrs pathway

Displays VRRS pathway information for an inactive pathway with the tag name “group1” and VRRP in backup state on the Ethernet 0/1 interface.

Example:

```
Device# show vrrs pathway
```

```

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10

```

Step 4 show vrrs pathway

Displays VRRS pathway information for a “not ready” pathway with the tag name “group1” and VRRP in backup state on the Ethernet 0/1 interface.

Example:

```

Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is NOT READY [VRRS push "INIT"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10

```

Step 5 show vrrs server

Displays VRRS server information.

Example:

```

Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10

```

The table below describes significant fields in the sample output:

Field	Description
State	Current state of VRRS on an interface. The values displayed are “ACTIVE”, “INACTIVE”, “NOT READY”, or “BACKUP”.
Virtual MAC	Virtual MAC address that is reserved for an interface.
Address-family	IPv4 or IPv6 address family.

Field	Description
Default Pathway	Indicates that the pathway has been implicitly created from a VRRP group, if the value is 1. If the value is 0, it indicates that the pathway has been explicitly created using the vrrs pathway command.
Owner Mode	Indicates that the interface IP address is specified if the value is 1.
Accept-Mode	Indicates that traffic to a particular virtual IP address is accepted if the value is 1.
Configured vMAC	Indicates that a virtual MAC address is configured if the value is 1.
No Shut	Indicates that the interface has been set to no shutdown mode if the value is 1.
Connected	Indicates that the VRRS pathway is connected to a VRRS group, if the value is 1.
OIR	Indicates online insertion and removal (OIR) of interface line cards on a device is complete if the value is 1.
L2 Ready	Indicates that the Layer 2 interface is up if the value is 1.
L3 Ready	Indicates that the Layer 3 interface is up if the value is 1.
vMAC Ready	Indicates that the virtual MAC address has been assigned to an interface if the value is 1.
vIP Ready	Indicates that the virtual IP address has been assigned to an interface if the value is 1.
Virtual Address List	Address list of the virtual IPv4 or IPv6 addresses.
Interface	Name of the interface where the pathway is defined.
vMAC	Virtual MAC address that is assigned to an interface.
vIP Address	Virtual IP address that is assigned to an interface.
Tags Connected	The specific tag name that is currently connected to a pathway on an interface.

Configuration Examples for VRRS

Example: Configuring VRRPv3 Control Groups

The following example shows how to configure a VRRPv3 control group:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 40
Device(config-if)# ip address 209.165.200.230 255.255.255.224
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 209.165.202.141
Device(config-if-vrrp)# vrrs leader group1
Device(config-if-vrrp)# end
```



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

Example: Configuring VRRS pathways

The following example shows how to configure a VRRS pathway:

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 42
Device(config-if)# ip address 209.165.201.25 255.255.255.224
Device(config-if)# vrrs pathway group1
Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24
Device(config-if-vrrs-pw)# address 209.165.201.10
Device(config-if-vrrs-pw)# end
```



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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases

Related Topic	Document Title
FHRP commands	First Hop Redundancy Protocols Command Reference
Configuring VRRPv2	“Configuring VRRP” module in the <i>First Hop Redundancy Protocols Configuration Guide</i>
VRRPv3 Protocol Support	“VRRPv3 Protocol Support” module in the <i>First Hop Redundancy Protocols Configuration Guide</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 Virtual Router Redundancy Service

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.



INDEX

S

show standby command [29](#)

