Cisco IOS XE IP Application Services Configuration Guide, Release 2

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 NONINFRINGEMENT 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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

Cisco IOS XE IP Application Services Configuration Guide

Configuring Enhanced Object Tracking

First Published: May 2, 2005
Last Updated: July 1, 2009

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

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Enhanced Object Tracking" section on page 28.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Enhanced Object Tracking

Before you configure the Enhanced Object Tracking feature, you should understand the following concepts:

- Feature Design of Enhanced Object Tracking, page 2
- Enhanced Object Tracking and Embedded Event Manager, page 2
- IP-Routing State of an Interface, page 3
- IP-Routing State of an Interface, page 3
- Tracking IP SLAs Operations, page 4
- IP-Routing State of an Interface, page 3

Feature Design of Enhanced Object Tracking

Enhanced Object Tracking provides complete separation between the objects to be tracked and the action to be taken by a client when a tracked object changes. Thus, several clients such as HSRP, VRRP, or GLPB can register their interest with the tracking process, track the same object, and each take different action when the object changes.

Each tracked object is identified by a unique number that is specified on the tracking command-line interface (CLI). Client processes 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.

You can also configure a combination of tracked objects in a list and a flexible method for combining objects using Boolean logic. This functionality includes the following capabilities:

- Threshold—The tracked list can be configured to use a weight or percentage threshold to measure the state of the list. Each object in a tracked list can be assigned a threshold weight. The state of the tracked list is determined by whether or not the threshold has been met.
- Boolean “and” function—When a tracked list has been assigned a Boolean “and” function, it means that each object defined within a subset must be in an up state so that the tracked object can become up.
- Boolean “or” function—When the tracked list has been assigned a Boolean “or” function, it means that at least one object defined within a subset must be in an up state so that the tracked object can become up.

Enhanced Object Tracking and Embedded Event Manager

Enhanced Object Tracking (EOT) is now integrated with Embedded Event Manager (EEM) to allow EEM to report on status change of a tracked object and to allow EOT to track EEM objects. A new type of tracking object—a stub object—is created. The stub object can be modified by an external process through a defined Application Programming Interface (API). See the "Embedded Event Manager Overview" document in the *Cisco IOS XE Network Management Configuration Guide* for more information on how EOT works with EEM.

IP-Routing State of an Interface

An IP-routing object is considered up when the following criteria exist:

- IP routing is enabled and active on the interface.
- The interface line-protocol state is up.
- The interface IP address is known. The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP routing will go down when one of the following criteria exist:

- IP routing is disabled globally.
- The interface line-protocol state is down.
- The interface IP address is unknown. The IP address is not configured or received through DHCP or IPCP negotiation.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. For example, on a serial interface that uses the Point-to-Point Protocol (PPP), the line protocol could be up (link control protocol [LCP] negotiated successfully), but IP could be down (IPCP negotiation failed).

The **track interface ip routing** command supports the tracking of an interface with an IP address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

Scaled Route Metrics

The **track ip route** command enables tracking of a route in the routing table. If a route exists in the table, the metric value is converted into a number. To provide a common interface to tracking clients, route metric values are normalized to the range from 0 to 255, where 0 is connected and 255 is inaccessible. Scaled metrics can be tracked by setting thresholds. Up and down state notification occurs when the thresholds are crossed. The resulting value is compared against threshold values to determine the tracking state as follows:

- State is up if the scaled metric for that route is less than or equal to the up threshold.
- State is down if the scaled metric for that route is greater than or equal to the down threshold.

Tracking uses a per-protocol configurable resolution value to convert the real metric to the scaled metric. Table 1 shows the default values used for the conversion. You can use the **track resolution** command to change the metric resolution default values.

Table 1 Metric Conversion

Route Type[1]	Metric Resolution
Static	10
Enhanced Interior Gateway Routing Protocol (EIGRP)	2560
Open Shortest Path First (OSPF)	1
Intermediate System-to-Intermediate System (IS-IS)	10

[1] RIP is scaled directly to the range from 0 to 255 because its maximum metric is less than 255.

For example, a change in 10 in an IS-IS metric results in a change of 1 in the scaled metric. The default resolutions are designed so that approximately one 2-Mbps link in the path will give a scaled metric of 255.

Scaling the very large metric ranges of EIGRP and IS-IS to a 0 to 255 range is a compromise. The default resolutions will cause the scaled metric to go above the maximum limit with a 2-Mbps link. However, this scaling allows a distinction between a route consisting of three Fast-Ethernet links and a route consisting of four Fast-Ethernet links.

Tracking IP SLAs Operations

Object tracking of IP SLAs operations allows tracking clients to track the output from IP SLAs objects and use the provided information to trigger an action.

Cisco IOS XE IP SLAs is a network performance measurement and diagnostics tool that uses active monitoring. Active monitoring is the generation of traffic in a reliable and predictable manner to measure network performance. Cisco IOS software uses IP SLAs to collect real-time metrics such as response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss.

These metrics can be used for troubleshooting, for proactive analysis before problems occur, and for designing network topologies.

Every IP SLAs operation maintains an operation return-code value. This return code is interpreted by the tracking process. The return code can return OK, OverThreshold, and several other return codes. Different operations can have different return-code values, so only values common to all operation types are used.

Two aspects of an IP SLAs operation can be tracked: state and reachability. The difference between these aspects relates to the acceptance of the OverThreshold return code. Table 2 shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 2 Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK (all other return codes)	Up Down
Reachability	OK or OverThreshold (all other return codes)	Up Down

Benefits of Enhanced Object Tracking

- Increases the availability and speed of recovery of a network.
- Decreases network outages and their duration.
- Provides a scalable solution that allows other client processes such as VRRP and GLBP the ability to track objects individually or as a list of objects. Prior to the introduction of this functionality, the tracking process was embedded within HSRP.

How to Configure Enhanced Object Tracking

- Tracking the Line-Protocol State of an Interface, page 5 (optional)
- Tracking the IP-Routing State of an Interface, page 7 (optional)
- Tracking IP-Route Reachability, page 8 (optional)
- Tracking the Threshold of IP-Route Metrics, page 10 (optional)
- Tracking the State of an IP SLAs Operation, page 12 (optional)
- Tracking the Reachability of an IP SLAs IP Host, page 13 (optional)
- Configuring a Tracked List and Boolean Expression, page 15 (optional)
- Configuring a Tracked List and Threshold Weight, page 16 (optional)
- Configuring a Tracked List and Threshold Percentage, page 18 (optional)
- Configuring the Track List Defaults, page 19 (optional)

Tracking the Line-Protocol State of an Interface

Perform this task to track the line-protocol state of an interface.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. See the "Tracking the IP-Routing State of an Interface" section for more information.

SUMMARY STEPS

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

3. **track timer interface** *seconds*
4. **track** *object-number* **interface** *type number* **line-protocol**
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **end**
7. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose

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	**`track timer interface`** *`seconds`*
	Example:
	`Router(config)# track timer interface 5`
		(Optional) Specifies the interval in which the tracking process polls the tracked object.
		• The default interval that the tracking process polls interface objects is 1 second.

Step 4	**`track`** *`object-number`* **`interface`** *`type number`* **`line-protocol`**
	Example:
	`Router(config)# track 3 interface GigabitEthernet 1/0/0 line-protocol`
		Tracks the line-protocol state of an interface and enters tracking configuration mode.

Step 5	**`delay`** `{`**`up`** *`seconds`* `[`**`down`** *`seconds`*`]|[`**`up`** *`seconds`*`]` **`down`** *`seconds`*`}`
	Example:
	`Router(config-track)# delay up 30`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

Step 6	**`end`**
	Example:
	`Router(config-track)# end`
		Exits to privileged EXEC mode.

Step 7	**`show track`** *`object-number`*
	Example:
	`Router# show track 3`
		(Optional) Displays tracking information.
		• Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example shows the state of the line protocol on an interface when it is tracked:

```
Router# show track 3
```

```
Track 3
   Interface GigabitEthernet1/0/0 line-protocol
   Line protocol is Up
     1 change, last change 00:00:05
   Tracked by:
     HSRP GigabitEthernet0/0/0 3
```

Tracking the IP-Routing State of an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track timer interface** *seconds*
4. **track** *object-number* **interface** *type number* **ip routing**
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **end**
7. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose
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	**track timer interface** *seconds* **Example:** `Router(config)# track timer interface 5`	(Optional) Specifies the interval in which the tracking process polls the tracked object. - The default interval that the tracking process polls interface objects is 1 second.
Step 4	**track** *object-number* **interface** *type number* **ip routing** **Example:** `Router(config)# track 1 interface GigabitEthernet 1/0/0 ip routing`	Tracks the IP-routing state of an interface and enters tracking configuration mode. - IP-route tracking tracks an IP route in the routing table and the ability of an interface to route IP packets.

Step 5	**delay** {**up** *seconds* [**down** *seconds*]|[**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 30`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

	Command or Action	Purpose

Step 6	`end`
	Example:
	`Router(config-track)# end`
		Returns to privileged EXEC mode.

Step 7	**`show track`** *`object-number`*
	Example:
	`Router# show track 1`
		Displays tracking information.
		- Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example shows the state of IP routing on an interface when it is tracked:

```
Router# show track 1

Track 1
   Interface GigabitEthernet1/0/0 ip routing
   IP routing is Up
     1 change, last change 00:01:08
   Tracked by:
     HSRP GigabitEthernet0/0/0 1
```

Tracking IP-Route Reachability

Perform this task to track the reachability of an IP route. A tracked object is considered up when a routing table entry exists for the route and the route is accessible.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track timer ip route** *seconds*
4. **track** *object-number* **ip route** *ip-address/prefix-length* **reachability**
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **ip vrf** *vrf-name*
7. **end**
8. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose
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	**track timer ip route** *seconds* **Example:** `Router(config)# track timer ip route 20`	(Optional) Specifies the interval in which the tracking process polls the tracked object. - The default interval that the tracking process polls IP-route objects is 15 seconds.
Step 4	**track** *object-number* **ip route** *ip-address/prefix-length* **reachability** **Example:** `Router(config)# track 4 ip route 10.16.0.0/16 reachability`	Tracks the reachability of an IP route and enters tracking configuration mode.

Step 5	**delay** {**up** *seconds* [**down** *seconds*]|[**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 30`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

Step 6	**ip vrf** *vrf-name* **Example:** `Router(config-track)# ip vrf VRF2`	(Optional) Configures a VPN routing and forwarding (VRF) table.

Step 7	**end**
	Example:
	`Router(config-track)# end`
		Returns to privileged EXEC mode.

Step 8	**show track** *object-number* **Example:** `Router# show track 4`	(Optional) Displays tracking information. - Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example shows the state of the reachability of an IP route when it is tracked:

```
Router# show track 4

Track 4
   IP route 10.16.0.0 255.255.0.0 reachability
   Reachability is Up (RIP)
     1 change, last change 00:02:04
```

```
First-hop interface is GigabitEthernet0/1
Tracked by:
  HSRP GigabitEthernet1/0/3 4
```

Tracking the Threshold of IP-Route Metrics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track timer ip route** *seconds*
4. **track resolution ip route** {**eigrp** *resolution-value* | **isis** *resolution-value* | **ospf** *resolution-value* | **static** *resolution-value*}
5. **track** *object-number* **ip route** *ip-address/prefix-length* **metric threshold**
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **ip vrf** *vrf-name*
8. **threshold metric** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}
9. **end**
10. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose

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	**track timer ip route** *seconds* **Example:** `Router(config)# track timer ip route 20`	(Optional) Specifies the interval in which the tracking process polls the tracked object. • The default interval that the tracking process polls IP-route objects is 15 seconds.
Step 4	**track resolution ip route** {**eigrp** *resolution-value* | **isis** *resolution-value* | **ospf** *resolution-value* | **static** *resolution-value*} **Example:** `Router(config)# track resolution ip route eigrp 300`	(Optional) Specifies resolution parameters for a tracked object. • Use this command to change the default metric resolution values.

	Command or Action	Purpose
Step 5	**track** *object-number* **ip route** *ip-address/prefix-length* **metric threshold** **Example:** `Router(config)# track 6 ip route 10.16.0.0/16 metric threshold`	Tracks the scaled metric value of an IP route to determine if it is above or below a threshold. • The default down value is 255, which equates to an inaccessible route. • The default up value is 254.

Step 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 30`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

Step 7	**ip vrf** *vrf-name* **Example:** `Router(config-track)# ip vrf VRF1`	(Optional) Configures a VRF table.

Step 8	**threshold metric** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}
	Example:
	`Router(config-track)# threshold metric up 254 down 255`
		(Optional) Sets a metric threshold other than the default value.

Step 9	**end**
	Example:
	`Router(config-track)# end`
		Exits to privileged EXEC mode.

Step 10	**show track** *object-number* **Example:** `Router# show track 6`	(Optional) Displays tracking information. • Use this command to verify the configuration. See the display output in the "Examples" section.

Examples

The following example shows the metric threshold of an IP route when it is tracked:

```
Router# show track 6

Track 6
   IP route 10.16.0.0 255.255.0.0 metric threshold
   Metric threshold is Up (RIP/6/102)
     1 change, last change 00:00:08
   Metric threshold down 255 up 254
   First-hop interface is GigabitEthernet0/1/1
   Tracked by:
     HSRP GigabitEthernet1/0/0 6
```

Tracking the State of an IP SLAs Operation

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **rtr** *operation-number* **state**
   or
   track *object-number* **ip sla** *operation-number* **state**
4. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
5. **end**
6. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose

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	**Cisco IOS XE Releases Prior to XE2.4**
	track *object-number* **rtr** *operation-number* **state**
	Cisco IOS XE Release 2.4 or Later Releases
	track *object-number* **ip sla** *operation-number* **state**
	Example: Cisco IOS XE Releases Prior to XE2.4
	`Router(config)# track 2 rtr 4 state`
	Example: Cisco IOS XE Release 2.4 Later Releases
	`Router(config)# track 2 ip sla 4 state`
		Tracks the state of an IP SLAs object and enters tracking configuration mode.
		Note Effective with Cisco IOS XE Release 2.4 the **track rtr** command was replaced by the **track ip sla** command. The **track rtr** command will be removed in a future release and is available only to aid the update of existing configurations to the **track ip sla** command.

Step 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 60 down 30`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config-track)# end`
		Exits to privileged EXEC mode.

Step 6	**show track** *object-number* **Example:** `Router# show track 2`	(Optional) Displays tracking information. • Use this command to verify the configuration. See the display output in the "Examples" section of this task.

Examples

The following example shows the state of the IP SLAs tracking:

```
Router# show track 2

Track 2
   IP SLA 1 state
   State is Down
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP GigabitEthernet1/0/0 2
```

Tracking the Reachability of an IP SLAs IP Host

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **rtr** *operation-number* **reachability**

   or

   track *object-number* **ip sla** *operation-number* **reachability**
4. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
5. **end**
6. **show track** *object-number*

DETAILED STEPS

	Command or Action	Purpose
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	**Cisco IOS XE Releases Prior to 2.4:**
	track *object-number* **rtr** *operation-number* **reachability**
	Cisco IOS XE Release 2.4 or Later Releases
	track *object-number* **ip sla** *operation-number* **reachability**
	Example: Cisco IOS XE Releases Prior to 2.4:
	`Router(config)# track 2 rtr 4 reachability`
	Example: Cisco IOS XE Release 2.4 or Later Releases
	`Router(config)# track 2 ip sla 4 reachability`
		Tracks the reachability of an IP SLAs IP host and enters tracking configuration mode.
		Note Effective with Cisco IOS XE Release 2.4 the **track rtr** command was replaced by the **track ip sla** command. The **track rtr** command will be removed in a future release and is available only to aid the update of existing configurations to the **track ip sla** command.

Step 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 30 down 10`
		(Optional) Specifies a period of time (in seconds) to delay communicating state changes of a tracked object.

Step 5	**end**
	Example:
	`Router(config-track)# end`
		Exits to privileged EXEC mode.

Step 6	**show track** *object-number* **Example:** `Router# show track 3`	(Optional) Displays tracking information. - Use this command to verify the configuration. See the display output in the "Examples" section of this task.

Examples

The following example shows whether the route is reachable:

```
Router# show track 3

Track 3
   IP SLA 1 reachability
   Reachability is Up
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
```

```
Tracked by:
  HSRP GigabitEthernet1/0/0 3
```

Configuring a Tracked List and Boolean Expression

Perform this task to configure a tracked list of objects and a Boolean expression to determine the state of the list. A tracked list contains one or more objects. The Boolean expression enables two types of calculations by using either “and” or “or” operators. For example, when tracking two interfaces using the “and” operator, up means that *both* interfaces are up, and down means that *either* interface is down.

You may also configure a tracked list state to be measured using a weight or percentage threshold. See “Configuring a Tracked List and Threshold Weight” section on page 16 and “Configuring a Tracked List and Threshold Percentage” section on page 18.

Prerequisites

An object must exist before it can be added to a tracked list.

Note The “not” operator is specified for one or more objects and negates the state of the object.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list boolean** {**and** | **or**}
4. **object** *object-number* [**not**]
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **end**

DETAILED STEPS

	Command or Action	Purpose

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.

	Command or Action	Purpose

Step 3	**track** *track-number* **list boolean** {**and** | **or**}
	Example:
	`Router(config-track)# track 100 list boolean and`
		Configures a tracked list object and enters tracking configuration mode. The keywords are as follows:
		• **boolean**—Specifies that the state of the tracked list is based on a Boolean calculation. The keywords are as follows:
		– **and**—Specifies that the list is up if all objects are up, or down if one or more objects are down. For example when tracking two interfaces, up means that both interfaces are up, and down means that either interface is down.
		– **or**—Specifies that the list is up if at least one object is up. For example, when tracking two interfaces, up means that either interface is up, and down means that both interfaces are down.

Step 4	**object** *object-number* [**not**] **Example:** `Router(config-track)# object 3 not`	Specifies the object to be tracked. The *object-number* argument has a valid range from 1 to 500. There is no default. The optional **not** keyword negates the state of the object. **Note** The example means that when object 3 is up, the tracked list detects object 3 as down.

Step 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
	Example:
	`Router(config-track)# delay up 3`
		(Optional) Specifies a tracking delay in seconds between up and down states.

Step 6	**end**
	Example:
	`Router(config-track)# end`
		Returns to privileged EXEC mode.

Configuring a Tracked List and Threshold Weight

Perform this task to configure a list of tracked objects, to specify that weight be used as the threshold, and to configure a weight for each of its objects. A tracked list contains one or more objects. Using a threshold weight, the state of each object is determined by comparing the total weight of all objects that are up against a threshold weight for each object.

You can also configure a tracked list state to be measured using a Boolean calculation or threshold percentage. See the "Configuring a Tracked List and Boolean Expression" section on page 15 and the "Configuring a Tracked List and Threshold Percentage" section on page 18.

Prerequisites

An object must exist before it can be added to a tracked list.

Restrictions

You cannot use the Boolean “not” operator in a weight or percentage threshold list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list threshold weight**
4. **object** *object-number* [**weight** *weight-number*]
5. **threshold weight** {**up** *number* **down** *number* | **up** *number* | **down** *number*}
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**

DETAILED STEPS

	Command or Action	Purpose

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	**`track`** *`track-number`* **`list threshold weight`**
	Example:
	`Router(config-track)# track 100 list threshold weight`
		Configures a tracked list object and enters tracking configuration mode. The keywords are as follows:
		• **threshold**—Specifies that the state of the tracked list is based on a threshold.
		• **weight**—Specifies that the threshold is based on a specified weight.

Step 4	**`object`** *`object-number`* `[`**`weight`** *`weight-number`*`]`
	Example:
	`Router(config-track)# object 3 weight 30`
		Specifies the object to be tracked. The *object-number* argument has a valid range from 1 to 500. There is no default. The optional **weight** keyword specifies a threshold weight for each object.

Step 5	**`threshold weight`** `{`**`up`** *`number`* **`down`** *`number`* `|` **`up`** *`number`* `|` **`down`** *`number`*`}`
	Example:
	`Router(config-track)# threshold weight up 30`
		Specifies the threshold weight. The keywords and arguments are as follows:
		• **up** *number*—Valid range is from 1 to 255.
		• **down** *number*—Range depends upon what you select for the **up** keyword. For example, if you configure 25 for up, you will see a range from 0 to 24 for down.

	Command or Action	Purpose

Step 6	`delay {up seconds [down seconds] | [up seconds] down seconds}`
	Example:
	`Router(config-track)# delay up 3`
		(Optional) Specifies a tracking delay in seconds between up and down states.

Step 7	`end`
	Example:
	`Router(config-track)# end`
		Returns to privileged EXEC mode.

Configuring a Tracked List and Threshold Percentage

Perform this task to configure a tracked list of objects, to specify that a percentage will be used as the threshold, and to specify a percentage for each object in the list. A tracked list contains one or more objects. Using the threshold percentage, the state of the list is determined by comparing the assigned percentage of each object to the list.

You may also configure a tracked list state to be measured using a Boolean calculation or threshold weight. See "Configuring a Tracked List and Boolean Expression" section on page 15 and "Configuring a Tracked List and Threshold Weight" section on page 16.

Prerequisites

An object must exist before it can be added to a tracked list.

Restrictions

You cannot use the Boolean "not" operator in a weight or percentage threshold list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list threshold percentage**
4. **object** *object-number*
5. **threshold percentage** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
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	**track** *track-number* **list threshold percentage** **Example:** Router(config-track)# track 100 list threshold percentage	Configures a tracked list object and enters tracking configuration mode. The keywords are as follows: • **threshold**—Specifies that the state of the tracked list is based on a threshold. • **percentage**—Specifies that the threshold is based on a percentage.
Step 4	**object** *object-number* **Example:** Router(config-track)# object 3	Specifies the object to be tracked. The *object-number* argument has a valid range from 1 to 500. There is no default.
Step 5	**threshold percentage** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]} **Example:** Router(config-track)# threshold percentage up 30	Specifies the threshold percentage. The keywords and arguments are as follows: • **up** *number*—Valid range is from 1 to 100. • **down** *number*—Range depends upon what you have selected for the **up** keyword. For example, if you specify 25 as up, a range from 26 to 100 is displayed for the **down** keyword.
Step 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **Example:** Router(config-track)# delay up 3	(Optional) Specifies a tracking delay in seconds between up and down states.
Step 7	**end** **Example:** Router(config-track)# end	Returns to privileged EXEC mode.

Configuring the Track List Defaults

Perform this task to configure a default delay value for a tracked list, a default object, and default threshold parameters for a tracked list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *track-number*
4. **default** {**delay** | **object** *object-number* | **threshold percentage**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose

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	**track** *track-number* **Example:** `Router(config)# track 3`	Enters tracking configuration mode.

Step 4	**default** {**delay** | **object** *object-number* | **threshold percentage**}
	Example:
	`Router(config-track)# default delay`
		Specifies a default delay value for a tracked list, a default object, and default threshold parameters for a tracked list. The keywords and arguments are as follows:
		• **delay**—Reverts to the default delay.
		• **object** *object-number*—Specifies a default object for the track list. The valid range is from 1 to 500.
		• **threshold percentage**—Specifies a default threshold percentage.

Step 5	`end`
	Example:
	`Router(config-track)# end`
		Returns to privileged EXEC mode.

Configuration Examples for Enhanced Object Tracking

- Example: Interface Line Protocol, page 21
- Example: Interface IP Routing, page 21
- Example: IP-Route Reachability, page 22
- Example: IP-Route Threshold Metric, page 23
- Example: IP SLAs IP Host Tracking, page 23

Example: Interface Line Protocol

The following example is very similar to the IP-routing example. Instead, the tracking process is configured to track the line-protocol state of GigabitEthernet interface 1/0/0. HSRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the line-protocol state of GigabitEthernet interface 1/0/0. If the line protocol on GigabitEthernet interface 1/0/0 goes down, the priority of the HSRP group is reduced by 10.

Router A Configuration

```
Router(config)# track 100 interface GigabitEthernet1/0/0 line-protocol
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
```

Router B Configuration

```
Router(config)# track 100 interface GigabitEthernet1/0/0 line-protocol
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
```

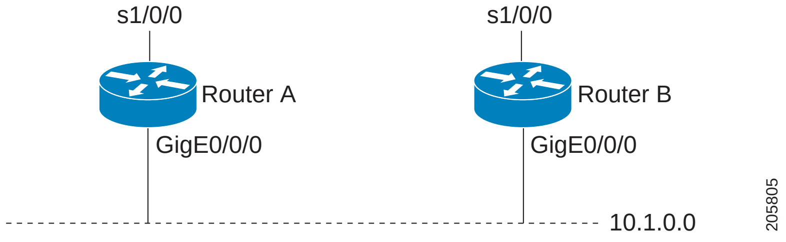
Example: Interface IP Routing

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

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

See Figure 1 for a sample topology.

Figure 1 Topology for IP-Routing Support



Router A Configuration

```
Router(config)# track 100 interface GigabitEthernet1/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
```

Router B Configuration

```
Router(config)# track 100 interface GigabitEthernet1/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
```

Example: IP-Route Reachability

In the following example, the tracking process is configured to track the reachability of IP route 10.2.2.0/24:

Router A Configuration

```
Router(config)# track 100 ip route 10.2.2.0/24 reachability
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.1.21 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.1.1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
```

Router B Configuration

```
Router(config)# track 100 ip route 10.2.2.0/24 reachability
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.1.22 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.1.1
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
```

Example: IP-Route Threshold Metric

In the following example, the tracking process is configured to track the threshold metric of IP route 10.2.2.0/24:

Router A Configuration

```
Router(config)# track 100 ip route 10.2.2.0/24 metric threshold
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.1.21 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.1.1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
```

Router B Configuration

```
Router(config)# track 100 ip route 10.2.2.0/24 metric threshold
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.1.22 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.1.1
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
```

Example: IP SLAs IP Host Tracking

The following example shows how to configure IP host tracking for IP SLAs operation 1 in Cisco IOS XE releases prior to Cisco IOS XE Release 2.4:

```
Router(config)# ip sla 1
Router(config-ip-sla)# icmp-echo 10.51.12.4
Router(config-ip-sla-echo)# timeout 1000
Router(config-ip-sla-echo)# frequency 3
Router(config-ip-sla-echo)# threshold 2
Router(config-ip-sla-echo)# request-data-size 1400
Router(config-ip-sla-echo)# exit
Router(config)# ip sla schedule 1 start-time now life forever
Router(config-ip-sla)# exit
Router(config)# track 2 rtr 1 state
Router(config)# track 3 rtr 1 reachability
Router(config-track)# exit
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# ip address 10.21.0.4 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# standby 3 ip 10.21.0.10d
Router(config-if)# standby 3 priority 120
Router(config-if)# standby 3 preempt
Router(config-if)# standby 3 track 2 decrement 10
Router(config-if)# standby 3 track 3 decrement 10
```

The following example shows how to configure IP host tracking for IP SLAs operation 1 in Cisco IOS XE Release 2.4 and later releases:

```
Router(config)# ip sla 1
Router(config-ip-sla)# icmp-echo 10.51.12.4
Router(config-ip-sla-echo)# timeout 1000
Router(config-ip-sla-echo)# frequency 3
Router(config-ip-sla-echo)# threshold 2
Router(config-ip-sla-echo)# request-data-size 1400
Router(config-ip-sla-echo)# exit
Router(config)# ip sla schedule 1 start-time now life forever
Router(config-ip-sla)# exit
Router(config)# track 2 ip sla 1 state
Router(config)# track 3 ip sla 1 reachability
Router(config-track)# exit
Router(config)# interface gigabitethernet0/1/1
Router(config-if)# ip address 10.21.0.4 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# standby 3 ip 10.21.0.10d
Router(config-if)# standby 3 priority 120
Router(config-if)# standby 3 preempt
Router(config-if)# standby 3 track 2 decrement 10
Router(config-if)# standby 3 track 3 decrement 10
```

Example: Boolean Expression for a Tracked List

In the following example, a track list object is configured to track two GigabitEthernet interfaces when both interfaces are up and when either interface is down:

```
Router(config)# track 1 interface GigabitEthernet2/0/0 line-protocol
Router(config)# track 2 interface GigabitEthernet2/1/0 line-protocol
Router(config-track)# exit
Router(config)# track 100 list boolean and
Router(config-track)# object 1
Router(config-track)# object 2
```

In the following example, a track list object is configured to track two GigabitEthernet interfaces when either interface is up and when both interfaces are down:

```
Router(config)# track 1 interface GigabitEthernet2/0/0 line-protocol
Router(config)# track 2 interface GigabitEthernet2/1/0 line-protocol
Router(config-track)# exit
Router(config)# track 101 list boolean or
Router(config-track)# object 1
Router(config-track)# object 2
```

The following configuration example shows that tracked list 4 has two objects and one object state is negated (if the list is up, the list detects that object 2 is down):

```
Router(config)# track 4 list boolean and
Router(config-track)# object 1
Router(config-track)# object 2 not
```

Example: Threshold Weight for a Tracked List

In the following example, three GigabitEtherent interfaces in tracked list 100 are configured with a threshold weight of 20 each. The down threshold is configured to 0 and the up threshold is configured to 40:

```
Router(config)# track 1 interface GigabitEthernet2/0/0 line-protocol
Router(config)# track 2 interface GigabitEthernet2/1/0 line-protocol
Router(config)# track 3 interface GigabitEthernet2/2/0 line-protocol
Router(config-track)# exit
Router(config)# track 100 list threshold weight
Router(config-track)# object 1 weight 20
Router(config-track)# object 2 weight 20
Router(config-track)# object 3 weight 20
Router(config-track)# threshold weight down 0 up 40
```

The above example means that the track-list object goes down only when all three serial interfaces go down, and only comes up again when at least two interfaces are up (since 20+20 >= 40). The advantage of this configuration is that it prevents the track-list object from coming up if two interfaces are down and the third interface is flapping.

The following configuration example shows that if object 1 and object 2 are down, then track list 4 is up, because object 3 satisfies the up threshold value of up 30. But, if object 3 is down, both objects 1 and 2 need to be up in order to satisfy the threshold weight.

```
Router(config)# track 4 list threshold weight
Router(config-track)# object 1 weight 15
Router(config-track)# object 2 weight 20
Router(config-track)# object 3 weight 30
Router(config-track)# threshold weight up 30 down 10
```

This configuration may be useful to you if you have two small bandwidth connections (represented by object 1 and 2) and one large bandwidth connection (represented by object 3). Also the down 10 value means that once the tracked object is up, it will not go down until the threshold value is lower or equal to 10, which in this example means that all connections are down.

Example: Threshold Percentage for a Tracked List

In the following example, four GigabitEthernet interfaces in track list 100 are configured for an up threshold percentage of 75. The track list is up when 75 percent of the interfaces are up and down when fewer than 75 percent of the interfaces are up.

```
Router(config)# track 1 interface GigabitEthernet2/0/0 line-protocol
Router(config)# track 2 interface GigabitEthernet2/1/0 line-protocol
Router(config)# track 3 interface GigabitEthernet2/2/0 line-protocol
Router(config)# track 4 interface GigabitEthernet2/3/0 line-protocol
Router(config-track)# exit
Router(config)# track 100 list threshold percentage
Router(config-track)# object 1
Router(config-track)# object 2
Router(config-track)# object 3
Router(config-track)# object 4
Router(config-track)# threshold percentage up 75
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Embedded Event Manager	*Embedded Event Manager Overview*
HSRP concepts and configuration tasks	*Configuring HSRP*
GLBP concepts and configuration tasks	*Configuring GLBP*
IP SLAs commands	*Cisco IOS IP SLAs Command Reference*
VRRP concepts and configuration tasks	*Configuring VRRP*
GLBP, HSRP, and VRRP commands	*Cisco IOS IP Application Services Command Reference.*

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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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 Enhanced Object Tracking

Table 3 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 3 Feature Information for Enhanced Object Tracking

Feature Name	Releases	Feature Configuration Information
Enhanced Tracking Support	Cisco IOS XE Release 2.1	The Enhanced Tracking Support feature separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by other Cisco IOS XE processes as well as HSRP. This feature allows tracking of other objects in addition to the interface line-protocol state. The following sections provide information about this feature: • IP-Routing State of an Interface, page 3 • Scaled Route Metrics, page 3 • Tracking the Line-Protocol State of an Interface, page 5 • Tracking the IP-Routing State of an Interface, page 7 • Tracking IP-Route Reachability, page 8 • Tracking the Threshold of IP-Route Metrics, page 10 • Example: Interface Line Protocol, page 21 • Example: Interface IP Routing, page 21 • Example: IP-Route Reachability, page 22 • Example: IP-Route Threshold Metric, page 23 The following commands were introduced or modified by this feature: **debug track**, **delay tracking**, **ip vrf**, **show track**, **standby track**, **threshold metric**, **track interface**, **track ip route**, **track timer**.
FHRP—Enhanced Object Tracking of IP SLAs Operations	Cisco IOS XE Release 2.1	This feature enables First Hop Redundancy Protocols (FHRPs) and other Enhanced Object Tracking (EOT) clients to track the output from IP SLAs objects and use the provided information to trigger an action. The following section provides information about this feature: • Tracking IP SLAs Operations, page 4 • Tracking the State of an IP SLAs Operation, page 12 • Example: IP SLAs IP Host Tracking, page 23 • Example: Boolean Expression for a Tracked List, page 24 The following command was introduced by this feature: **track rtr**.

Table 3 Feature Information for Enhanced Object Tracking (continued)

Feature Name	Releases	Feature Configuration Information
FHRP—Object Tracking List	Cisco IOS XE Release 2.1	This feature enhances the tracking capabilities to enable the configuration of a combination of tracked objects in a list, and a flexible method of combining objects using Boolean logic. The following sections provide information about this feature: • Configuring a Tracked List and Boolean Expression, page 15 • Configuring a Tracked List and Threshold Weight, page 16 • Configuring a Tracked List and Threshold Percentage, page 18 • Configuring the Track List Defaults, page 19 The following commands were introduced or modified by this feature: **show track**, **threshold percentage**, **threshold weight**, **track list**, **track resolution**.
FHRP—EOT Deprecation of **rtr** Keyword	Cisco IOS XE Release 2.4	This feature replaces the **track rtr** command with the **track ip sla** command. The following sections provide information about this feature: • Tracking the State of an IP SLAs Operation, page 12 • Example: IP SLAs IP Host Tracking, page 23 The following command was introduced by this feature: **track ip sla**.
FHRP—Enhanced Object Tracking Integration with Embedded Event Manager	Cisco IOS XE Release 2.1	EOT is now integrated with EEM to allow EEM to report on a status change of a tracked object and to allow EOT to track EEM objects. The following section provides information about this feature: • Enhanced Object Tracking and Embedded Event Manager, page 2 The following commands were introduced or modified by this feature: **action track read**, **action track set**, **default-state**, **event resource**, **event rf**, **event track**, **show track**, **track stub**.

Glossary

DHCP—Dynamic Host Configuration Protocol. DHCP is a protocol that delivers IP addresses and configuration information to network clients.

GLBP—Gateway Load Balancing Protocol. Provides automatic router backup for IP hosts that are configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant (GLBP) routers that will become active if any of the existing forwarding routers fail.

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

IPCP—IP Control Protocol. The protocol used to establish and configure IP over PPP.

LCP—Link Control Protocol. The protocol used to establish, configure, and test data-link connections for use by PPP.

PPP—Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is most commonly used for dial-up Internet access. Its features include address notification, authentication via CHAP or PAP, support for multiple protocols, and link monitoring.

VRF—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge router.

VRRP—Virtual Router Redundancy Protocol. Eliminates the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP addresses associated with a virtual router is called the master, and forwards packets sent to these IP addresses. The election process provides dynamic failover in the forwarding responsibility should the master become unavailable. Any of the virtual router IP addresses on a LAN can then be used as the default first-hop router by end hosts.

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.

Configuring GLBP

First Published: May 2, 2005
Last Updated: March 2, 2009

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for GLBP" section on page 18.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for GLBP

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

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, 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 routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IP address, and all routers in the virtual router 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, User Datagram Protocol (UDP) port 3222 (source and destination).

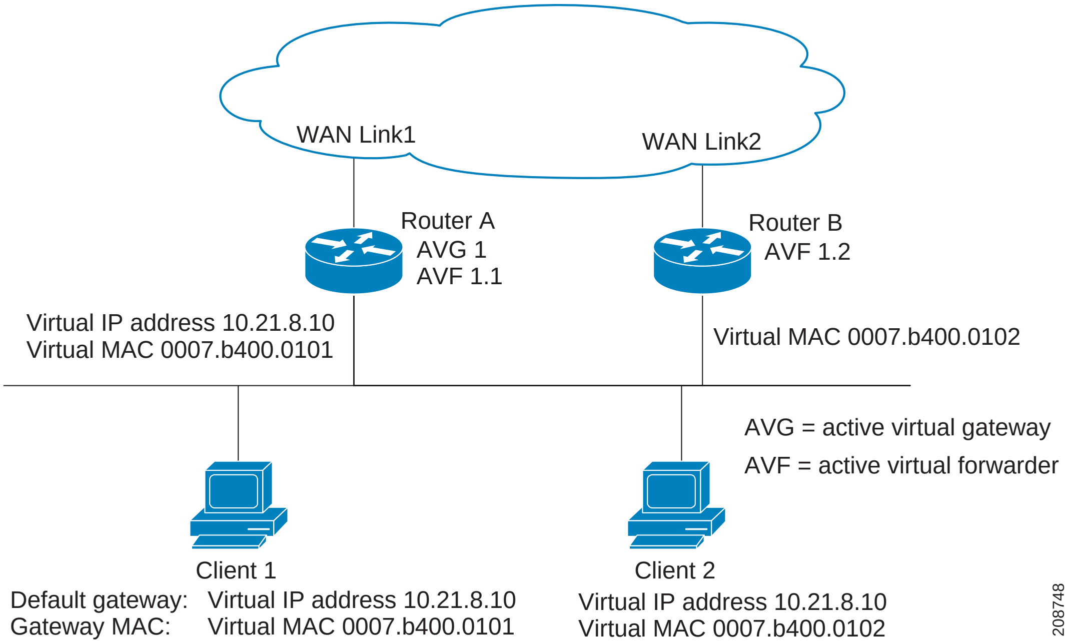
GLBP Active Virtual Gateway

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 in the event that the AVG becomes unavailable. The function of the AVG is that it 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.

In Figure 1, Router 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 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


WAN Link1
WAN Link2
Router A
AVG 1
AVF 1.1
Router B
AVF 1.2
Virtual IP address 10.21.8.10
Virtual MAC 0007.b400.0101
Virtual MAC 0007.b400.0102
AVG = active virtual gateway
AVF = active virtual forwarder
Client 1
Default gateway: Virtual IP address 10.21.8.10
Gateway MAC: Virtual MAC 0007.b400.0101
Client 2
Virtual IP address 10.21.8.10
Virtual MAC 0007.b400.0102
208748

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 router 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 router 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 Figure 1, if Router 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 is the only other member in the group so it will automatically become the new AVG. If another router existed in the same GLBP group with a higher priority, then the router with the higher priority would be elected. If both routers 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 router in the GLBP group. The weighting assigned to a router 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 router. 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.

ISSU—GLBP

GLBP 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 Cisco IOS XE 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 XE 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 XE In Service Software Upgrade Process* document.

GLBP Benefits

Load Sharing

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

Multiple Virtual Routers

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

Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway 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

You can use a simple text password authentication scheme between GLBP group members to detect configuration errors. A router within a GLBP group with a different authentication string than other routers will be ignored by other group members.

How to Configure GLBP

- Enabling and Verifying GLBP, page 6 (required)
- Customizing GLBP, page 8 (optional)
- Configuring GLBP Authentication, page 10 (optional)
- Configuring GLBP Weighting Values and Object Tracking, page 11 (optional)
- Troubleshooting GLBP, page 13 (optional)

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.

Prerequisites

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:
	`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`
		Specifies an interface type and number, and enters interface configuration mode.

Step 4	**`ip address`** *`ip-address mask`* `[`**`secondary`**`]`
	Example:
	`Router(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`* **`ip`** `[`*`ip-address`* `[`**`secondary`**`]]`
	Example:
	`Router(config-if)# glbp 10 ip 10.21.8.10`
		Enables GLBP on an interface and identifies the primary IP address of the virtual gateway.
		- 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:
	`Router(config-if)# exit`
		Exits interface configuration mode, and returns the router to global configuration mode.

Step 7	**`show glbp`** `[`*`interface-type interface-number`*`] [`*`group`*`] [`*`state`*`] [`**`brief`**`]`
	Example:
	`Router(config)# show glbp 10`
		(Optional) Displays information about GLBP groups on a router.
		- Use the optional **brief** keyword to display a single line of information about each virtual gateway or virtual forwarder.
		- See the display output for this command in the "Examples" section of this task.

Examples

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

```
Router# 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

Perform this task to customize your GLBP configuration.

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 router 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. **exit**

DETAILED STEPS

	Command or Action	Purpose
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 GigabitEthernet0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(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**] *hellotime* [**msec**] *holdtime* **Example:** `Router(config-if)# glbp 10 timers 5 18`	Configures the interval between successive hello packets sent by the AVG in a GLBP group. • The *holdtime* 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	**glbp** *group* **timers redirect** *redirect timeout* **Example:** `Router(config-if)# glbp 10 timers redirect 600 7200`	Configures the time interval during which the AVG continues to redirect clients to an AVF. • The *timeout* argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid.
Step 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] **Example:** `Router(config-if)# glbp 10 load-balancing host-dependent`	Specifies the method of load balancing used by the GLBP AVG.
Step 8	**glbp** *group* **priority** *level* **Example:** `Router(config-if)# glbp 10 priority 254`	Sets the priority level of the gateway within a GLBP group. • The default value is 100.

	Command or Action	Purpose
Step 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] **Example:** `Router(config-if)# glbp 10 preempt delay minimum 60`	Configures the router to take over as AVG for a GLBP group if it has a higher priority than the current AVG. • This command is disabled by default. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVG takes place.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.

Configuring GLBP Authentication

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

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

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

Perform this task to configure GLBP text authentication.

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 router that will communicate.
8. **end**
9. **show glbp**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables higher privilege levels, such as 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 GigabitEthernet1/0/0`
		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	**`glbp`** *`group-number`* **`authentication text`** *`string`*
	Example:
	`Router(config-if)# glbp 10 authentication text stringxyz`
		Authenticates GLBP packets received from other routers in the group.
		• If you configure authentication, all routers within the GLBP group must use the same authentication string.

Step 6	**`glbp`** *`group-number`* **`ip`** `[`*`ip-address`* `[`**`secondary`**`]]`
	Example:
	`Router(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 router that will communicate.	—

Step 8	**`end`**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 9	**`show glbp`**
	Example:
	`Router# show glbp`
		(Optional) Displays GLBP information.
		• 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

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
7. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]
8. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
9. **end**
10. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

DETAILED STEPS

	Command or Action	Purpose
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	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
	Example:
	`Router(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.
		• 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:** `Router(config-track)# exit`	Returns to global configuration mode.
Step 5	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Enters interface configuration mode.

	Command or Action	Purpose
Step 6	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] **Example:** `Router(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** *group* **weighting track** *object-number* [**decrement** *value*] **Example:** `Router(config-if)# glbp 10 weighting track 2 decrement 5`	Specifies an object to be tracked that affects the weighting of a GLBP gateway. • The *value* argument specifies a reduction in the weighting of a GLBP gateway when a tracked object fails.
Step 8	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] **Example:** `Router(config-if)# glbp 10 forwarder preempt delay minimum 60`	Configures the router to take over as AVF for a GLBP group if the current AVF for a GLBP group falls below its low weighting threshold. • This command is enabled by default with a delay of 30 seconds. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVF takes place.

Step 9	**end**
	Example:
	`Router(config-if)# exit`
		Returns to privileged EXEC mode.

Step 10	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**] | **resolution** | **timers**] **Example:** `Router# show track 2`	Displays tracking information.

Troubleshooting GLBP

GLBP introduces five privileged EXEC mode commands to enable diagnostic output concerning various events relating to the operation of GLBP to be displayed on a console. 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 router. Perform this task to minimize the impact of using the **debug glbp** commands.

This procedure will minimize the load on the router created by the **debug condition glbp** or **debug glbp** commands 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 router may be unable to respond due to the processor load of generating the debugging output.

Prerequisites

This task requires a router 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 router 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:
	`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	**`no logging console`**
	Example:
	`Router(config)# no logging console`
		Disables all logging to the console terminal.
		• To reenable logging to the console, use the **logging console** command in global configuration mode.

Step 4	Use Telnet to access a router 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:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Step 6	**`terminal monitor`**
	Example:
	`Router# terminal monitor`
		Enables logging output on the virtual terminal.

	Command or Action	Purpose
Step 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] **Example:** `Router# debug condition glbp GigabitEthernet 0/0/0 10 1`	Displays debugging messages about GLBP conditions. • 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:** `Router# terminal no monitor`	Disables logging on the virtual terminal.

Configuration Examples for GLBP

Example: Customizing GLBP Configuration

The following example shows how to configure Router A as shown in Figure 1:

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 timers 5 18
Router(config-if)# glbp 10 timers redirect 600 7200
Router(config-if)# glbp 10 load-balancing host-dependent
Router(config-if)# glbp 10 priority 254
Router(config-if)# glbp 10 preempt delay minimum 60
```

Example: Configuring GLBP Text Authentication

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 authentication text stringxyz
Router(config-if)# glbp 10 ip 10.21.8.10
```

Example: Configuring GLBP Weighting

In the following example, Router A, shown in Figure 1, 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 goes down, the weighting value of the router is reduced.

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

Example: Enabling GLBP Configuration

In the following example, Router A, shown in Figure 1, is configured to enable GLBP, and the virtual IP address of 10.21.8.10 is specified for GLBP group 10:

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 ip 10.21.8.10
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
GLBP commands	*Cisco IOS IP Application Services Command Reference.*
In Service Software Upgrade (ISSU) configuration	*Cisco IOS In Service Software Upgrade Process*
Object tracking	*Configuring Enhanced Object Tracking*
Stateful Switchover	*Stateful Switchover*
VRRP	*Configuring VRRP*
HSRP	*Configuring HSRP*

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
No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for GLBP

Feature Name	Releases	Feature Configuration Information
Gateway Load Balancing Protocol	Cisco IOS XE Release 2.1	GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while allowing packet load sharing between a group of redundant routers. All sections in this configuration module provide information about this feature. The following commands were introduced or modified by this feature: **glbp forwarder preempt, glbp ip, glbp load-balancing, glbp name, glbp preempt, glbp priority, glbp sso, glbp timers, glbp timers redirect, glbp weighting, glbp weighting track, show glbp**.
ISSU—GLBP	Cisco IOS XE Release 2.1	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 XE software are running on the active and standby Route Processors (RPs) or line cards. This feature provides customers with the same level of HA functionality for planned outages due to software upgrades as is available with SSO for unplanned outages. That is, the system can switch over to a secondary RP and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default. The following sections provide information about this feature: • ISSU—GLBP, page 5

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 Cisco IOS XE 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.

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

Configuring HSRP

First Published: May 2, 2005
Last Updated: May 4, 2009

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for HSRP" section on page 49.

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

Contents

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 router 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 router.

HSRP is useful for hosts that do not support a router discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new router when their selected router 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 routers 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 router. The active router receives and routes packets destined for the MAC address of the group. For *n* routers running HSRP, *n* + 1 IP and MAC addresses are assigned.

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

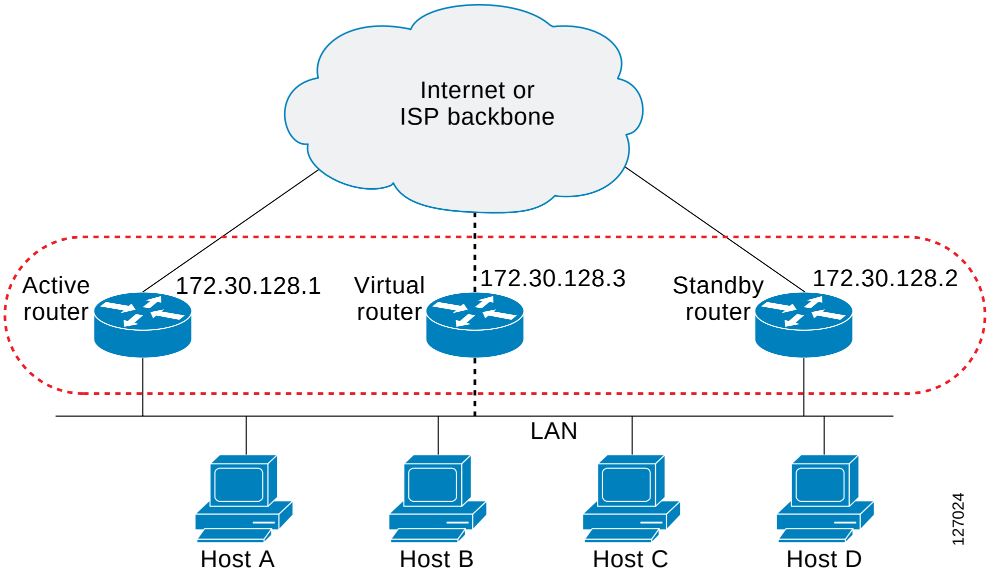
HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure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

Devices that are running HSRP send and receive multicast User Datagram Protocol (UDP)-based hello messages to detect router failure and to designate active and standby routers. When the active router fails to send a hello message within a configurable period of time, the standby router with the highest priority becomes the active router. The transition of packet forwarding functions between routers 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 routers and load sharing.

Figure 1 shows a network configured for HSRP. By sharing a virtual MAC address and IP address, two or more routers can act as a single *virtual router*. The virtual router does not physically exist but represents the common default gateway for routers that are configured to provide backup to each other. You do not need to configure the hosts on the LAN with the IP address of the active router. Instead, you configure them with the IP address (virtual IP address) of the virtual router as their default gateway. If the active router fails to send a hello message within the configurable period of time, the standby router takes over and responds to the virtual addresses and becomes the active router, assuming the active router duties.

Figure 1 HSRP Topology



HSRP Version 2 Design

HSRP version 2 is designed to address the following issues relative to HSRP version 1:

- Previously, 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.
- 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, there is no method to identify from HSRP active hello messages which physical router 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, which is used by 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 router 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 issues relative to HSRP version 1 that HSRP version 2 does. See the "Configuring GLBP" module for more information on GLBP.

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 router.

Preemption

Preemption allows a standby router 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

By using the command-line interface (CLI), group attributes can be applied 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 router becomes HSRP active, and there is already an HSRP active router on the network, it may appear that HSRP preemption is not functioning. This can occur because the new HSRP active router did not receive any hello packets from the current HSRP active router, and the preemption configuration never factored into the new routers decision making.

This can occur on some larger hardware platforms where there can be a delay in an interface receiving packets.

In general, we recommend that all HSRP routers 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 command is separate from 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.

How Object Tracking Affects the Priority of an HSRP Router

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 router with the higher priority can now become the active router if it has the **standby preempt** command configured. See the "Configuring HSRP Object Tracking" section on page 20 for more information on object tracking.

HSRP Addressing

HSRP routers 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 routers) on UDP port 1985. The active router sources hello packets from its configured IP address and the HSRP virtual MAC address while the standby router sources hellos from its configured IP address and the interface MAC address, which may or may not be the Burned-In 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 composed 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.

Virtual MAC Addresses and BIA MAC Addresses

Perform this task to configure an HSRP virtual MAC address or a burned-in address (BIA) MAC address.

A router automatically generates a virtual MAC address for each HSRP router. 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, it is often necessary to be able to specify the virtual MAC address by using the **standby mac-address** command; 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 BIA 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 routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

HSRP Timers

Each HSRP router maintains three timers that are used for timing hello messages: an active timer, a standby timer, and a hello timer. When a timer expires, the router changes to a new HSRP state. Routers or access servers for which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values.

For HSRP version 1, nonactive routers learn timer values from the active router, unless millisecond timer values are being used. If millisecond timer values are being used, all routers 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.

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, Router A has a priority of 120 and is the active router. If a host sends spoof HSRP hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof HSRP hello packets are ignored, Router A will remain the active router.

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

- The authentication schemes differ on the router and in the incoming packets.
- Text authentication strings differ on the router 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, Router A has a priority of 120 and is the active router. If a host sends spoof HSRP hello packets with a priority of 130, then Router A stops being the active router. If Router A has authentication configured such that the spoof HSRP hello packets are ignored, Router A will remain the active router.

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

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

HSRP Messages and States

Routers configured with HSRP exchange three types of multicast messages:

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

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

- Active—The router is performing packet-transfer functions.
- Standby—The router is prepared to assume packet-transfer functions if the active router fails.
- Speak—The router is sending and receiving hello messages.
- Listen—The router is receiving hello messages.
- Init or Disabled—The router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers 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.

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 router with low-priority Level 6 messaging.

HSRP and ARP

HSRP also works when the hosts are configured for proxy ARP. When the active HSRP router receives an ARP request for a host that is not on the local LAN, the router replies with the MAC address of the virtual router. If the active router becomes unavailable or its connection to the remote LAN goes down, the router that becomes the active router receives packets addressed to the virtual router and transfers them accordingly. If the Hot Standby state of the interface is not active, proxy ARP responses are suppressed.

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 now 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" module.

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.

HSRP Support for ICMP Redirects

By default, HSRP filtering of ICMP redirect messages is enabled on routers 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 running HSRP, it is important to prevent hosts from discovering the interface (or real) IP addresses of routers in the HSRP group. If a host is redirected by ICMP to the real IP address of a router, and that router 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 Routers

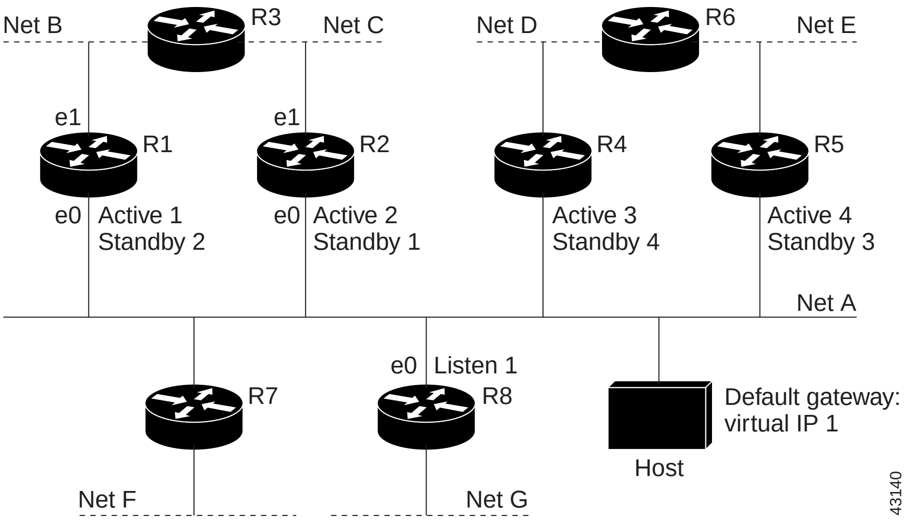
The next-hop IP address is compared to the list of active HSRP routers on that network; if a match is found, then the real next-hop IP address is replaced with a corresponding virtual IP address and the redirect message is allowed to continue.

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

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

Consider the network shown in Figure 2, which supports the HSRP ICMP redirection filter.

Figure 2 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
```

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

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

Redirects to passive HSRP routers are not permitted. Redundancy may be lost if hosts learn the real IP addresses of HSRP routers.

In Figure 2, redirection to router R8 is not allowed because R8 is a passive HSRP router. In this case, packets from the host to Net D will first go to router R1 and then be forwarded to router R4; that is, they will traverse the network twice.

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

ICMP Redirects to Non-HSRP Routers

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

In Figure 2, redirection to router 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 Router Advertisements

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

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

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

You can adjust the advertisement interval and holddown time using the **standby redirect timers** command.

ICMP Redirects Not Sent

If the HSRP router 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 router 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 router 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.

Using HSRP with ICMP redirects is not possible in the Cisco 800 series, Cisco 1000 series, Cisco 1600 series, Cisco 2500 series, Cisco 3000 series, and Cisco 4500 series routers because the Ethernet controller can only support one MAC address.

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 router uses the destination MAC address to determine the gateway IP address of the host. If the HSRP router is using the same MAC address for multiple IP addresses then it is not possible to uniquely determine the gateway IP address of the host 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 20.0.0.4 for dest 30.0.0.2
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) Virtual Private Network (VPN) interface is useful when an Ethernet LAN is connected between two provider edge (PE) routers with either of the following conditions:

- A customer edge (CE) router 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/forwarding (VRF) instances. A VRF consists of the following elements:

- IP routing table
- Cisco Express Forwarding (CEF) table
- Set of interfaces that use the CEF 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 CEF table for each VRF. A separate set of routing and CEF 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 router 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

Increasingly, many hundreds of subinterfaces are being configured on the same physical interface, with each subinterface having its own HSRP group. The negotiation and maintenance of multiple HSRP groups can 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 routers. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups.

The HSRP group state of the client groups follows that of the master group. Client groups do not participate in any sort of router 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 master group.

ISSU—HSRP

The In Service Software Upgrade (ISSU) process 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 Cisco IOS XE software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. This document provides information about ISSU concepts and describes the steps taken to perform ISSU in a system.

For detailed information about ISSU, see the *Cisco IOS XE In Service Software Upgrade Process* document.

SSO HSRP

SSO HSRP alters the behavior of HSRP when a router 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 router, then the standby HSRP router takes over as the active HSRP router.

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

SSO HSRP enables the Cisco IOS XE 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 router.

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

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

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 router 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.

The Cisco IOS XE 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, cHsrpExtSecAddrEntry, and 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, page 15 (required)
- Delaying the Initialization of HSRP on an Interface, page 17 (optional)

- Configuring HSRP Priority and Preemption, page 18 (required)
- Configuring HSRP Object Tracking, page 20 (optional)
- Configuring HSRP MD5 Authentication Using a Key String, page 22 (optional)
- Configuring HSRP MD5 Authentication Using a Key Chain, page 24 (optional)
- Troubleshooting HSRP MD5 Authentication, page 26 (optional)
- Configuring HSRP Text Authentication, page 27 (optional)
- Customizing HSRP, page 29 (optional)
- Configuring Multiple HSRP Groups for Load Balancing, page 30 (optional)
- Enabling HSRP Support for ICMP Redirects, page 32 (optional)
- Improving CPU and Network Performance with HSRP Multiple Group Optimization, page 33 (optional)
- Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses, page 34 (optional)
- Changing to HSRP Version 2, page 36 (optional)
- Enabling SSO Aware HSRP, page 37 (optional)
- Verifying SSO Aware HSRP, page 39 (optional)
- Enabling HSRP MIB Traps, page 40 (optional)

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 router, you must configure the virtual IP address for at least one of the routers in the group; it can be learned on the other routers in the group.

Prerequisites

You can configure many attributes in HSRP such as authentication, timers, priority, and preemption. It is best practice to configure the attributes first 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 configuration is entered.

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:
	`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 GigabitEthernet0/0/0`
		Configures an interface type and 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	`standby [`*`group-number`*`] ip [`*`ip-address`*` [secondary]]`
	Example:
	`Router(config-if)# standby 1 ip 172.16.6.100`
		Activates HSRP.
		• If you do not configure a group number, it defaults to 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
		• The *ip-address* is the virtual IP address of the virtual router. For HSRP to elect a designated router, you must configure the virtual IP address for at least one of the routers in the group; it can be learned on the other routers in the group.

Step 6	`end`
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 7	`show standby [all] [brief]`
	Example:
	`Router# show standby`
		(Optional) Displays HSRP information.
		• This command displays information for each group. The **all** option display 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:
	`Router# show standby GigabitEthernet 0`
		(Optional) Displays HSRP information about specific groups or interfaces.

Delaying the Initialization of HSRP on an Interface

Perform this task to delay 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 router time to settle down after the interface up event and helps prevent HSRP state flapping.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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 GigabitEthernet1/0/0`
		Configures an interface type and enters interface configuration mode.

Step 4	**`ip address`** *`ip-address mask`*
	Example:
	`Router(config-if)# ip address 10.0.0.1 255.255.255.0`
		Specifies an IP address for an interface.

	Command or Action	Purpose
Step 5	**standby delay minimum** *min-delay* **reload** *reload-seconds* **Example:** `Router(config-if)# standby delay minimum 20 reload 25`	(Optional) Configures the delay period before the initialization of HSRP groups. • The *min-delay* 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 *reload-seconds* value is the time period to delay after the router has reloaded. This delay period applies only to the first interface-up event after the router has reloaded.
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	Activates HSRP.

Step 7	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 8	**show standby delay** [*type number*] **Example:** `Router# show standby delay`	(Optional) Displays HSRP information about delay periods.

Troubleshooting Tips

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

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** *delay* | **reload** *delay* | **sync** *delay*}]
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:** `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 GigabitEthernet0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	Specifies an IP address for an interface.
Step 5	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority. • The default priority is 100.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** `Router(config-if)# standby 1 preempt delay minimum 380`	Configures HSRP preemption and preemption delay. • The default delay period is 0 seconds; if the router wants to preempt, it will do so immediately. By default, the router that comes up later becomes the standby.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	Activates HSRP.

Step 8	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 9	**show standby** [**all**] [**brief**] **Example:** `Router# show standby`	(Optional) Displays HSRP information. • This command displays information for each group. The **all** option display groups that are learned or that do not have the **standby ip** command configured.
Step 10	**show standby** *type number* [*group-number* | **all**] [**brief**] **Example:** `Router# show standby GigabitEthernet0/0/0`	(Optional) Displays HSRP information about specific groups or interfaces.

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.

For more information on object tracking, see the "Configuring Enhanced Object Tracking" module.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**`track`** *`object-number`* **`interface`** *`type number`*
	`{`**`line-protocol`**` | `**`ip routing`**`}`
	Example:
	`Router(config)# track 100 interface GigabitEthernet0/0/0 line-protocol`
		Configures an interface to be tracked and enters tracking configuration mode.

Step 4	**`exit`**
	Example:
	`Router(config-track)# exit`
		Returns to global configuration mode.

Step 5	**`interface`** *`type number`*
	Example:
	`Router(config)# interface GigabitEthernet0/0/0`
		Configures an interface type and enters interface configuration mode.

Step 6	**`standby`** `[`*`group-number`*`]` **`track`** *`object-number`*
	`[`**`decrement`** *`priority-decrement`*`] [`**`shutdown`**`]`
	Example:
	`Router(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.
		• By default, the priority of the router 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 *priority-decrement* 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 HRSP group on the router when the tracked object goes down.
		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.

Step 7	**`standby`** `[`*`group-number`*`]` **`ip`** `[`*`ip-address`*
	`[`**`secondary`**`]]`
	Example:
	`Router(config-if)# standby 1 ip 10.10.10.0`
		Activates HSRP.
		• 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

Step 8	`end`
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 9	**`show track`** [*`object-number`* | **`brief`**] [**`interface`** [**`brief`**]| **`ip route`** [**`brief`**]| **`resolution`** | **`timers`**] **Example:** `Router# show track 100 interface`	Displays tracking information.

Configuring HSRP MD5 Authentication Using a Key String

Restrictions

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 router also has MD5 authentication enabled.

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** *delay* | **reload** *delay* | **sync** *delay*}]
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 router that will communicate.
10. **end**
11. **show standby**

DETAILED STEPS

	Command	Purpose
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 GigabitEthernet0/0/0	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	**standby** [*group-number*] **priority** *priority* **Example:** Router(config-if)# standby 1 priority 110	Configures HSRP priority.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** Router(config-if)# standby 1 preempt	Configures HSRP preemption.
Step 7	**standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] **Example:** Router(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30	Configures an authentication string for HSRP MD5 authentication. - The *key* argument can be up to 64 characters in length and it is recommended that at least 16 characters be used. - No prefix to the *key* 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.

	Command	Purpose
Step 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.
Step 9	Repeat Steps 1 through 8 on each router that will communicate.	—

Step 10	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 11	**show standby** **Example:** `Router# show standby`	(Optional) Displays HSRP information. • Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Troubleshooting Tips

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

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** *delay* | **reload** *delay* | **sync** *delay*}]
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 router that will communicate.
15. **end**
16. **show standby**

DETAILED STEPS

	Command	Purpose

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	**`key chain`** *`name-of-chain`*
	Example:
	`Router(config)# key chain hsrp1`
		Enables authentication for routing protocols and identifies a group of authentication keys.

Step 4	**`key`** *`key-id`*
	Example:
	`Router(config-keychain)# key 100`
		Identifies an authentication key on a key chain.
		- The *key-id* must be a number.

Step 5	**`key-string`** *`string`*
	Example:
	`Router(config-keychain-key)# key-string mno172`
		Specifies the authentication string for a key.
		- The *string* can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.

Step 6	**`exit`**
	Example:
	`Router(config-keychain-key)# exit`
		Returns to Keychain configuration mode.

Step 7	**`exit`**
	Example:
	`Router(config-keychain)# exit`
		Returns to global configuration mode.

Step 8	**`interface`** *`type number`*
	Example:
	`Router(config)# interface GigabitEthernet0/0/0`
		Configures an interface type and enters interface configuration mode.

Step 9	**`ip address`** *`ip-address mask`* [**`secondary`**] **Example:** `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	Specifies a primary or secondary IP address for an interface.

	Command	Purpose
Step 10	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 11	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption.
Step 12	**standby** [*group-number*] **authentication md5 key-chain** *key-chain-name* **Example:** `Router(config-if)# standby 1 authentication md5 key-chain hsrp1`	Configures an authentication MD5 key chain for HSRP MD5 authentication. • The key chain name must match the name specified in Step 3.
Step 13	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] **Example:** `Router(config-if)# standby 1 ip 10.21.8.12`	Activates HSRP.
Step 14	Repeat Steps 1 through 12 on each router that will communicate.	—

Step 15	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 16	**show standby** **Example:** `Router# show standby`	(Optional) Displays HSRP information. • 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	Purpose

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

Step 2	**`debug standby errors`**
	Example:
	`Router# debug standby errors`
		Displays error messages related to HSRP.
		• Error messages will be displayed for each packet that fails to authenticate, so use this command with care.
		• See the "Examples" section for an example of the type of error messages displayed when two routers are not authenticating.

Examples

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

```
Router# 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 Router A and Router B have different MD5 authentication strings:

```
Router# 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** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. Repeat Steps 1 through 8 on each router that will communicate.

10. **end**
11. **show standby**

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables higher privilege levels, such as 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 GigabitEthernet0/0/0`
		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	**`standby`** `[`*`group-number`*`]` **`priority`** *`priority`*
	Example:
	`Router(config-if)# standby 1 priority 110`
		Configures HSRP priority.

Step 6	**`standby`** `[`*`group-number`*`]` **`preempt`** `[`**`delay`** `{`**`minimum`** *`delay`* `|` **`reload`** *`delay`* `|` **`sync`** *`delay`*`}]`
	Example:
	`Router(config-if)# standby 1 preempt`
		Configures HSRP preemption.

Step 7	**`standby`** `[`*`group-number`*`]` **`authentication text`** *`string`*
	Example:
	`Router(config-if)# standby 1 authentication text authentication1`
		Configures an authentication string for HSRP text authentication.
		• The default string is cisco.

Step 8	**`standby`** `[`*`group-number`*`]` **`ip`** `[`*`ip-address`* `[`**`secondary`**`]]`
	Example:
	`Router(config-if)# standby 1 ip 10.0.0.3`
		Activates HSRP.

Step 9	Repeat Steps 1 through 8 on each router that will communicate.	—

	Command	Purpose

Step 10	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 11	**show standby** **Example:** `Router# show standby`	(Optional) Displays HSRP information. • Use this command to verify your configuration. The key string or key chain will be displayed if configured.

Customizing HSRP

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:** `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 GigabitEthernet0/0/0`	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.

	Command or Action	Purpose
Step 5	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* **Example:** `Router(config-if)# standby 1 timers 5 15`	Configures the time between hello packets and the time before other routers declare the active Hot Standby router to be down. • Normally, the *holdtime* value is greater than or equal to three times the value of *hellotime*. • See the "SUMMARY STEPS" section for more information.
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.

Troubleshooting Tips

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used. You can use the **standby delay** command to allow the interface to come up completely before HSRP initializes.

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 routers to be more fully utilized. While a router is actively forwarding traffic for one HSRP group, it can be in standby or in the listen state for another group.

If two routers are used, then Router A would be configured as active for group 1 and standby for group 2. Router 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: Multiple HSRP for Load Balancing" section on page 44 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** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. On the same router, repeat Steps 5 through 7 to configure the router attributes for different standby groups.
9. **exit**

10. Repeat Steps 3 through 9 to configure HSRP on another router.

DETAILED STEPS

	Command or Action	Purpose
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 GigabitEthernet0/0/0`	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	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption.
Step 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **Example:** `Router(config-if)# standby 1 ip 10.0.0.3`	Activates HSRP.
Step 8	On the same router, repeat Steps 5 through 7 to configure the router attributes for different standby groups.	For example, Router A can be configured as an active router for group 1 and be configured for active or standby router for another HSRP group with different priority and preemption values.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits to global configuration mode.
Step 10	Repeat Steps 3 through 9 on another router.	Configures multiple HSRP and enables load balancing on another router.

Enabling HSRP Support for ICMP Redirects

By default, HSRP filtering of ICMP redirect messages is enabled on routers running HSRP. Perform this task to reenable this feature on your router 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:** `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 GigabitEthernet0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**standby redirect** [**timers** *advertisement holddown*] [**unknown**] **Example:** `Router(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:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 6	**show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**] **Example:** `Router# show standby redirect`	(Optional) Displays ICMP redirect information on interfaces configured with HSRP.

Improving CPU and Network Performance with HSRP Multiple Group Optimization

Configure the HSRP master group using the steps in the "Configuring Multiple HSRP Groups for Load Balancing" section.

Perform this task to configure multiple HSRP client groups.

The **standby follow** command configures an HSRP group to become a slave 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.

Restrictions

- Client or slave 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:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

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:
	`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 GigabitEthernet0/0/0`
		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	**`standby mac-refresh`** *`seconds`*
	Example:
	`Router(config-if)# standby mac-refresh 30`
		Configures the HSRP client group refresh interval.

Step 6	**`standby`** *`group-number`* **`follow`** *`group-name`*
	Example:
	`Router(config-if)# standby 1 follow HSRP1`
		Configures an HSRP group as a client group.

Step 7	**`exit`**
	Example:
	`Router(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.

Configuring HSRP Virtual MAC Addresses or BIA MAC Addresses

Perform this task to configure an HSRP virtual MAC address or a burned-in address (BIA) MAC address.

Restrictions

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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 GigabitEthernet0/0/0`
		Configures an interface type and enters interface configuration mode.

Step 4	**`ip address`** *`ip-address mask`* `[`**`secondary`**`]`
	Example:
	`Router(config-if)# ip address 172.16.6.5 255.255.255.0`
		Configures an IP address for an interface.

	Command or Action	Purpose

Step 5	`standby [group-number] mac-address mac-address`
	or
	`standby use-bia [scope interface]`
	Example:
	`Router(config-if)# standby 1 mac-address 5000.1000.1060`
	or
	Example:
	`Router(config-if)# standby use-bia`
		Specifies a virtual MAC address for HSRP.
		• 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.
		• 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 [group-number] ip [ip-address [secondary]]`
	Example:
	`Router(config-if)# standby 1 ip 172.16.6.100`
		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.

Restrictions

- 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 router. You cannot change from version 2 to version 1 if you have configured groups above the group number range allowed for version 1 (0 to 255).

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:
	`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 vlan 400`
		Configures an interface type and enters interface configuration mode.

Step 4	**`ip address`** *`ip-address mask`*
	Example:
	`Router(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:
	`Router(config-if)# standby version 2`
		Changes the HSRP version.

Step 6	**`standby`** `[`*`group-number`*`]` **`ip`** `[`*`ip-address`* `[`**`secondary`**`]]`
	Example:
	`Router(config-if)# standby 400 ip 10.10.28.5`
		Activates HSRP.
		• The group number range for HSRP version 2 is expanded to 0 through 4095. The group number range for HSRP version 1 is 0 through 255.

Step 7	**`end`**
	Example:
	`Router(config-if)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

Step 8	**`show standby`**
	Example:
	`Router# show standby`
		(Optional) Displays HSRP information.
		• HSRP version 2 information will be displayed if configured.

Enabling SSO Aware HSRP

The functionality 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:
	`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	`redundancy`
	Example:
	`Router(config)# redundancy`
		Enters redundancy configuration mode.

Step 4	`mode sso`
	Example:
	`Router(config-red)# mode sso`
		Enables the redundancy mode of operation to SSO.
		• After performing this step, HSRP is SSO aware on interfaces that are configured for HSRP and the standby RP is automatically reset.

Step 5	`exit`
	Example:
	`Router(config-red)# exit`
		Exits redundancy configuration mode.

Step 6	`no standby sso`
	Example:
	`Router(config)# no standby sso`
		Disables HSRP SSO mode for all HSRP groups.

	Command or Action	Purpose
Step 7	**standby sso** **Example:** `Router(config)# standby sso`	Enables the SSO HSRP feature if you have disabled the functionality.

Step 8	**end**
	Example:
	`Router(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:

```
Router# 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:

```
Router# 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:** `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	**snmp-server enable traps hsrp** **Example:** `Router(config)# snmp-server enable traps hsrp`	Enables the router to send SNMP traps and informs, and HSRP notifications.
Step 4	**snmp-server host** *host community-string* **hsrp** **Example:** `Router# 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 HSRP

- Example: HSRP Priority and Preemption, page 41

Example: HSRP Priority and Preemption

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

Router A Configuration

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 95
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

Router B Configuration

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

Example: 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, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on serial interface 1/0 in Router A fails, the HSRP group priority will be reduced and Router B will take over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Router A Configuration

```
Router(config)# track 100 interface serial1/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

Router B Configuration

```
Router(config)# track 100 interface serial1/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

Example: 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, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on Gigabit Ethernet interface 0/0/0 in Router A fails, the HSRP group will be disabled and Router B will take over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

Router A Configuration

```
Router(config)# track 100 interface GigabitEthernet0/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/1
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 shutdown
```

Router B Configuration

```
Router(config)# track 100 interface GigabitEthernet0/0/0 ip routing
!
Router(config)# interface GigabitEthernet0/0/1
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(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:

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

Example: HSRP MD5 Authentication Using Key Strings

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Router(config-if)# standby 1 ip 10.21.0.10
```

Example: 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:

```
Router(config)# key chain hsrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

Example: 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:

Router 1

```
Router(config)# key chain hsrp1
Router(config-keychain)# key 0
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

Router 2

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Router(config-if)# standby 1 ip 10.21.0.10
```

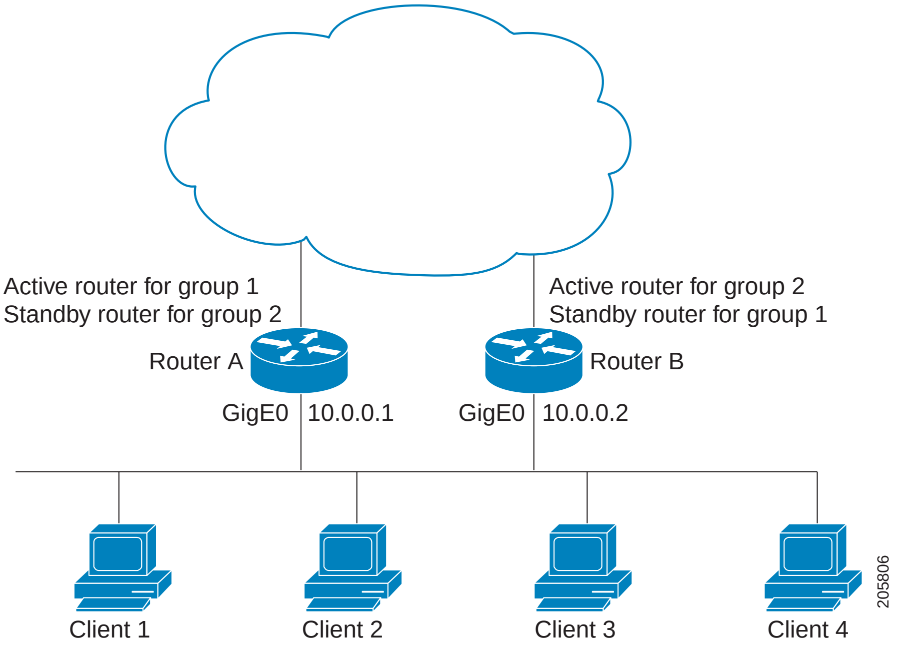
Example: HSRP Text Authentication

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication text company2
Router(config-if)# standby 1 ip 10.21.0.10
```

Example: Multiple HSRP for Load Balancing

You can use HSRP or multiple HSRP groups when you configure load sharing. In Figure 3, 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 3 HSRP Load Sharing Example


Active router for group 1
Standby router for group 2
Router A
GigE0
10.0.0.1
Active router for group 2
Standby router for group 1
Router B
GigE0
10.0.0.2
Client 1
Client 2
Client 3
Client 4
205806

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 master group:

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# no shutdown
Router(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Router(config)# interface GigabitEthernet0/0/1
Router(config-if)# no shutdown
Router(config-if)# ip vrf forwarding VRF2
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 1 ip 10.0.0.254
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 name HSRP1
!Server group
!
Router(config)# interface GigabitEthernet0/0/2
Router(config-if)# no shutdown
Router(config-if)# ip vrf forwarding VRF3
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
!
Router(config)# interface GigabitEthernet0/0/3
Router(config-if)# no shutdown
Router(config-if)# ip vrf forwarding VRF4
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
```

Example: HSRP Support for ICMP Redirect Messages

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

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.10 255.0.0.0
Router(config-if)# standby redirect
Router(config-if)# standby 1 priority 120
Router(config-if)# standby 1 preempt delay minimum 20
Router(config-if)# standby 1 ip 10.0.0.1
Router(config-if)# standby 2 priority 105
Router(config-if)# standby 2 preempt delay minimum 20
Router(config-if)# standby 2 ip 10.0.0.2
```

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

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.11 255.0.0.0
Router(config-if)# standby redirect
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 preempt delay minimum 20
Router(config-if)# standby 1 ip 10.0.0.1
Router(config-if)# standby 2 priority 120
Router(config-if)# standby 2 preempt delay minimum 20
Router(config-if)# standby 2 ip 10.0.0.2
```

Example: HSRP Virtual MAC Addresses and BIA MAC Address

In an 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:

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1
Router(config-if)# standby 1 mac-address 4000.1000.1060
Router(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:

```
Router(config)# interface token3/0
Router(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: HSRP Version 2

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

```
Router(config)# interface vlan350
Router(config-if)# standby version 2
Router(config-if)# standby 350 priority 110
Router(config-if)# standby 350 preempt
Router(config-if)# standby 350 timers 5 15
Router(config-if)# standby 350 ip 172.20.100.10
```

Example: SSO HSRP

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

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

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

```
Router(config)# interface GigabitEthernet1/0/0
Router(config-if)# ip address 10.1.1.1 255.255.0.0
Router(config-if)# standby priority 200
Router(config-if)# standby preempt
Router(config-if)# standby sso
```

Example: HSRP MIB Traps:

The following examples show how to configure HSRP on two routers and enable the HSRP MIB trap support functionality. As in many environments, one router is preferred as the active one. Configuring a router’s preference as the active router is realized by configuring it at a higher priority level and enabling preemption. In the following example, the active router is referred to as the primary router. The second router is referred to as the backup router:

Router A

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.1.1.1 255.255.0.0
Router(config-if)# standby priority 200
Router(config-if)# standby preempt
Router(config-if)# standby ip 10.1.1.3
Router(config-if)# exit
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host yourhost.cisco.com public hsrp
```

Router B

```
Router(config)#interface GigabitEthernet1/0/0
Router(config-if)# ip address 10.1.1.2 255.255.0.0
Router(config-if)#  standby priority 101
Router(config-if)# standby ip 10.1.1.3
Router(config-if)# exit
Router(config)# snmp-server enable traps hsrp
Router(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*
GLBP	“Configuring GLBP” module
HSRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*
ISSU	*Cisco IOS XE In Service Software Upgrade Process* document
Object tracking	“Configuring Enhanced Object Tracking” module
VRRP	“Configuring VRRP” module

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for HSRP

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for HSRP

Feature Name	Releases	Feature Information
FHRP—HSRP-MIB	Cisco IOS XE Release 2.1	The FHRP—HSRP-MIB feature introduces support for the CISCO-HRSP-MIB.
FHRP—HSRP Group Shutdown	Cisco IOS XE Release 2.1	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. The following sections provide information about this feature: • HSRP Group Shutdown, page 9 • Configuring HSRP Object Tracking, page 20 • Example: HSRP Group Shutdown, page 42 The following commands were modified by this feature: **standby track**, **show standby**.

Table 1 Feature Information for HSRP (continued)

Feature Name	Releases	Feature Information
FHRP—HSRP Multiple Group Optimization	Cisco IOS XE Release 2.1	FHRP—HSRP Multiple Group Optimization feature improves the negotiation and maintenance of multiple HSRP groups configured on a subinterface. Only one HSRP group is required on a physical interface for the purposes of electing active and standby routers. This group is known as the *master* group. Other HSRP groups may be created on each subinterface and linked to the master group via the group name. These linked HSRP groups are known as *client* or *slave* groups. The following sections provide information about this feature: • HSRP Multiple Group Optimization, page 13 • Improving CPU and Network Performance with HSRP Multiple Group Optimization, page 33 • Example: Improving CPU and Network Performance with HSRP Multiple Group Optimization, page 45 The following commands were introduced or modified by this feature: **standby follow**, **show standby**.
HSRP—ISSU	Cisco IOS XE Release 2.1	The HSRP—ISSU feature enables support for ISSU in HSRP. The In Service Software Upgrade (ISSU) process 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 Cisco IOS XE software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades. The following section provides information about this feature: • ISSU—HSRP, page 13 For more information about this feature, see the *Cisco IOS XE In Service Software Upgrade Process* document. There are no new or modified command for this feature.

Table 1 Feature Information for HSRP (continued)

Feature Name	Releases	Feature Information
HSRP MD5 Authentication	Cisco IOS XE Release 2.1	Prior to the introduction of the HSRP MD5 Authentication feature, HSRP authenticated protocol packets with a simple plain text string. The HSRP MD5 Authentication feature is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This feature provides added security and protects against the threat from HSRP-spoofing software. The following sections provide information about this feature: • HSRP MD5 Authentication, page 7 • Configuring HSRP MD5 Authentication Using a Key String, page 22 • Configuring HSRP MD5 Authentication Using a Key Chain, page 24 • Troubleshooting HSRP MD5 Authentication, page 26 • Example: HSRP MD5 Authentication Using Key Strings, page 43 • Example: HSRP MD5 Authentication Using Key Chains, page 43 • Example: HSRP MD5 Authentication Using Key Strings and Key Chains, page 43 The following commands were introduced or modified by this feature: **show standby**, **standby authentication**.
HSRP Support for ICMP Redirects	Cisco IOS XE Release 2.1	The HSRP support for ICMP Redirects feature enables ICMP redirection on interfaces configured with HSRP. The following sections provide information about this feature: • HSRP Group Shutdown, page 9 • Configuring HSRP MD5 Authentication Using a Key String, page 22 • Example: HSRP Support for ICMP Redirect Messages, page 45 The following commands were introduced or modified by this feature: **debug standby event**, **debug standby events icmp**, **show standby**, **standby redirects**

Table 1 Feature Information for HSRP (continued)

Feature Name	Releases	Feature Information
HSRP Support for MPLS VPNs	Cisco IOS XE Release 2.1	HSRP support for a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) interface is useful when an Ethernet LAN is connected between two provider edge (PE) routers with either of the following conditions: The following section provides information about this feature: • HSRP Support for MPLS VPNs, page 12 There are no new or modified command for this feature.
HSRP Version 2	Cisco IOS XE Release 2.1	HSRP Version 2 feature 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. The following sections provide information about this feature: • HSRP Version 2 Design, page 4 • Changing to HSRP Version 2, page 36 The following commands were introduced or modified by this feature: **show standby**, **standby ip**, **standby version**.
SSO—HSRP	Cisco IOS XE Release 2.1	The SSO—HSRP feature alters the behavior of HSRP when a router with redundant RPs is configured for SSO. When an RP is active and the other RP is standby, SSO enables the standby RP to take over if the active RP fails. The following sections provide information about this feature: • SSO HSRP, page 13 • SSO Dual-Route Processors and Cisco Nonstop Forwarding, page 14 • HSRP and SSO Working Together, page 14 • Enabling SSO Aware HSRP, page 37 • Verifying SSO Aware HSRP, page 39 The following commands were introduced or modified by this feature: **debug standby events**, **standby sso**.

Glossary

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

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 master 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 router that services all packets sent to the HSRP address. The lead router is monitored by other routers in the group, and if it fails, one of these standby HSRP routers inherits the lead position and the HSRP group address.

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 Cisco IOS XE 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.

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. 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. SSO refers to the implementation of Cisco IOS XE software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. Along with NSF, SSO makes an RP failure undetectable to the network.

standby group—The set of routers participating in HSRP that jointly emulate a virtual router.

standby router—The backup router 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, the automatically generated MAC address when HSRP is configured. The standard virtual MAC address used is: 0000.0C07.ACxy, 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.

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.

Configuring IP Services

First Published: October 23, 2006
Last Updated: June 9, 2010

This module describes how to configure optional IP services. For a complete description of the IP services commands in this chapter, refer to the *Cisco IOS IP Application Services Command Reference.* To locate documentation of other commands that appear in this module, use the command reference master index, or search online.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for IP Services" section on page 15.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About IP Services

IP Source Routing

The Cisco IOS XE software examines IP header options on every packet. It supports the IP header options Strict Source Route, Loose Source Route, Record Route, and Time Stamp, which are defined in RFC 791. If the software finds a packet with one of these options enabled, it performs the appropriate action. If it finds a packet with an invalid option, it sends an Internet Control Message Protocol (ICMP) parameter problem message to the source of the packet and discards the packet.

IP provides a provision known as source routing that allows the source IP host to specify a route through the IP network. Source routing is specified as an option in the IP header. If source routing is specified, the software forwards the packet according to the specified source route. IP source routing is employed when you want to force a packet to take a certain route through the network. The default is to perform source routing. IP source routing is rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash devices running these implementations by sending them datagrams with source routing options. Disable IP source routing whenever possible. Disabling IP source routing will cause a Cisco router to never forward an IP packet that carries a source routing option.

ICMP Overview

Originally created for the TCP/IP suite in RFC 792, the Internet Control Message Protocol (ICMP) was designed to report a small set of error conditions. ICMP also can report a wide variety of error conditions and provide feedback and testing capabilities. Each message uses a common format and is sent and received by using the same protocol rules.

ICMP enables IP to perform addressing, datagram packaging, and routing by allowing encapsulated messages to be sent and received between IP devices. These messages are encapsulated in IP datagrams just like any other IP message. When the message is generated, the original IP header is encapsulated in the ICMP message and these two pieces are encapsulated within a new IP header to be returned as an error report to the sending device.

ICMP messages are sent in several situations: when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. To avoid the infinite regress of messages about messages, no ICMP messages are sent about ICMP messages.

ICMP does not make IP reliable or ensure the delivery of datagrams or the return of a control message. Some datagrams may be dropped without any report of their loss. The higher-level protocols that use IP must implement their own reliability procedures if reliable communication is required.

ICMP Unreachable Error Messages

Type 3 error messages are sent when a message cannot be delivered completely to the application at a destination host. Six codes contained in the ICMP header describe the unreachable condition as follows:

- 0—Network unreachable
- 1—Host unreachable
- 2—Protocol unreachable
- 3—Port unreachable
- 4—Fragmentation needed and the “don’t fragment” (DF) bit is set
- 5—Source route failed

Cisco IOS XE software can suppress the generation of ICMP unreachable destination error messages, which is called rate-limiting. The default is no unreachable messages more often than once every half second. Separate intervals can be configured for code 4 and all other unreachable destination error messages. However, there is no method of displaying how many ICMP messages have not been sent.

The ICMP Unreachable Destination Counters feature provides a method to count and display the unsent Type 3 messages. This feature also provides console logging with error messages when there are periods of excessive rate limiting that would indicate a Denial of Service (DoS) attack against the router.

If the Cisco IOS XE software receives a nonbroadcast packet destined for itself that uses an unknown protocol, it sends an ICMP protocol unreachable message back to the source. Similarly, if the software receives a packet that it is unable to deliver to the final destination because it knows of no route to the destination address, it sends an ICMP host unreachable message to the source. This functionality is enabled by default.

Disable Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. These messages can be used by an attacker to gain network mapping information.

Because the null interface is a packet sink, packets forwarded there will always be discarded and, unless disabled, will generate host unreachable messages. In that case, if the null interface is being used to block a Denial-of-Service attack, these messages flood the local network with these messages. Disabling these messages prevents this situation. In addition, because all blocked packets are forwarded to the null interface, an attacker receiving host unreachable messages could use those messages to determine Access Control List (ACL) configuration. If the “null 0” interface is configured on your router, disable ICMP host unreachable messages for discarded packets or packets routed to the null interface.

ICMP Mask Reply Messages

Occasionally, network devices must know the subnet mask for a particular subnetwork in the internetwork. To obtain this information, such devices can send ICMP mask request messages. ICMP mask reply messages are sent in reply from devices that have the requested information. The Cisco IOS XE software can respond to ICMP mask request messages if this function is enabled.

These messages can be used by an attacker to gain network mapping information.

ICMP Redirect Messages

Routes are sometimes less than optimal. For example, it is possible for the router to be forced to resend a packet through the same interface on which it was received. If the router resends a packet through the same interface on which it was received, the Cisco IOS XE software sends an ICMP redirect message to the originator of the packet telling the originator that the router is on a subnet directly connected to the receiving device, and that it must forward the packet to another system on the same subnet. The software sends an ICMP redirect message to the originator of the packet because the originating host presumably could have sent that packet to the next hop without involving this device at all. The redirect message instructs the sender to remove the receiving device from the route and substitute a specified device representing a more direct path. This functionality is enabled by default.

In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Disabling ICMP redirects will cause no operational impact to the network, and it eliminates this possible method of attack.

Denial of Service Attack

Denial of service has become a growing concern, especially when considering the associated costs of such an attack. DoS attacks can decrease the performance of networked devices, disconnect the devices from the network, and cause system crashes. When network services are unavailable, enterprises and service providers suffer the loss of productivity and sales.

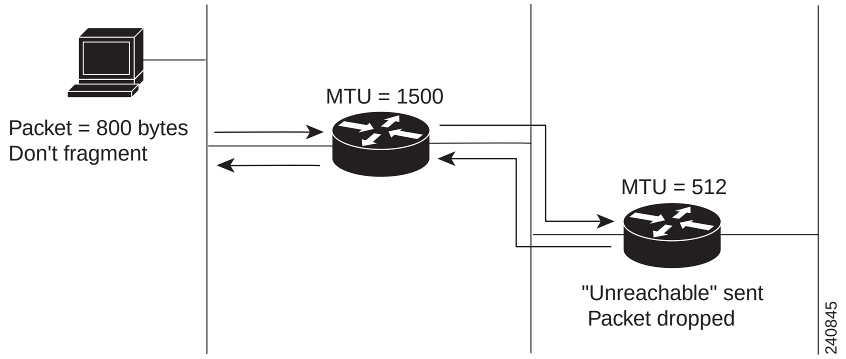
The objective of a DoS attack is to deprive a user or organization access to services or resources. If a Website is compromised by a DoS attack, millions of users could be denied access to the site. DoS attacks do not typically result in intrusion or the illegal theft of information. Instead of providing access to unauthorized users, DoS attacks can cause much aggravation and cost to the target customer by preventing authorized access. Distributed DoS (DDoS) attacks amplify DoS attacks in that a multitude of compromised systems coordinate to flood targets with attack packets, thereby causing denial of service for users of the targeted systems.

A DoS attack occurs when a stream of ICMP echo requests (pings) are broadcast to a destination subnet. The source addresses of these requests are falsified to be the source address of the target. For each request sent by the attacker, many hosts on the subnet will respond flooding the target and wasting bandwidth. The most common DoS attack is called a “smurf” attack, named after an executable program and is in the category of network-level attacks against hosts. DoS attacks can be easily detected when error-message logging of the ICMP Unreachable Destination Counters feature is enabled.

Path MTU Discovery

The Cisco IOS XE software supports the IP Path MTU Discovery mechanism, as defined in RFC 1191. IP Path MTU Discovery allows a host to dynamically discover and cope with differences in the maximum allowable maximum transmission unit (MTU) size of the various links along the path. Sometimes a router is unable to forward a datagram because it requires fragmentation (the packet is larger than the MTU you set for the interface with the **ip mtu** interface configuration command), but the “don’t fragment” (DF) bit is set. The Cisco IOS XE software sends a message to the sending host, alerting it to the problem. The host will need to fragment packets for the destination so that they fit the smallest packet size of all the links along the path. This technique is shown in Figure 1.

Figure 1 IP Path MTU Discovery



IP Path MTU Discovery is useful when a link in a network goes down, forcing the use of another, different MTU-sized link (and different routers). As shown in Figure 1, suppose a router is sending IP packets over a network where the MTU in the first router is set to 1500 bytes, but the second router is set to 512 bytes. If the "don't fragment" bit of the datagram is set, the datagram would be dropped because the 512-byte router is unable to forward it. All packets larger than 512 bytes are dropped in this case. The second router returns an ICMP destination unreachable message to the source of the datagram with its Code field indicating "Fragmentation needed and DF set." To support IP Path MTU Discovery, it would also include the MTU of the next hop network link in the low-order bits of an unused header field.

IP Path MTU Discovery is also useful when a connection is being established and the sender has no information at all about the intervening links. It is always advisable to use the largest MTU that the links will bear; the larger the MTU, the fewer packets the host must send.

Note IP Path MTU Discovery is a process initiated by end hosts. If an end host does not support IP Path MTU Discovery, the receiving device will have no mechanism available to avoid fragmenting datagrams generated by the end host.

If a router that is configured with a small MTU on an outbound interface receives packets from a host that is configured with a large MTU (for example, receiving packets from a Token Ring interface and forwarding them to an outbound Ethernet interface), the router fragments received packets that are larger than the MTU of the outbound interface. Fragmenting packets slows the performance of the router. To keep routers in your network from fragmenting received packets, run IP Path MTU Discovery on all hosts and routers in your network, and always configure the largest possible MTU for each router interface type.

IP MAC Accounting

Cisco IP accounting support provides basic IP accounting functions. By enabling IP accounting, users can see the number of bytes and packets switched through the Cisco IOS XE software on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the software or terminating in the software is not included in the accounting statistics. To maintain accurate accounting totals, the software maintains two accounting databases: an active and a checkpointed database.

Cisco IP accounting support also provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data also indicates that you should verify IP access list configurations. To make this functionality available to users, you must enable IP accounting of access list violations using the **ip accounting access-violations** interface configuration command. Users can then display the number of bytes and packets from a single source that attempted to breach security against the access list for the source destination pair. By default, IP accounting displays the number of packets that have passed access lists and were routed.

The MAC address accounting functionality provides accounting information for IP traffic based on the source and destination MAC addresses on LAN interfaces. MAC accounting calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent. For example, with IP MAC accounting, you can determine how much traffic is being sent to and/or received from various peers at Network Access Profiles (NAPS)/peering points. IP MAC accounting is supported on Ethernet, GigabitEthernet, and FastEthernet interfaces and supports Cisco Express Forwarding (CEF), distributed CEF (dCEF), flow, and optimum switching.

How to Configure IP Services

- Protecting Your Network from DOS Attacks, page 6
- Setting the MTU Packet Size, page 7
- Configuring IP Accounting, page 8
- Monitoring and Maintaining the IP Network, page 10

Protecting Your Network from DOS Attacks

ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP messages can be used by an attacker to gain network mapping information. IP source routing allows the source IP host to specify a route through the IP network and is rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash devices running these implementations by sending them datagrams with source routing options.

Whenever possible, ICMP messages and IP source routing should be disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ip source-route**
4. **interface** *type/number*
5. **no ip unreachables**
6. **no ip redirects**
7. **no ip mask-reply**

DETAILED STEPS

	Command or Action	Purpose

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	**`no ip source-route`**
	Example:
	`Router(config)# no ip source-route`
		Disables IP source routing.

Step 4	**`interface`** *`type/number`*
	Example:
	`Router(config)# interface GigabitEthernet0/0/0`
		Specifies the interface to configure and enters interface configuration mode.

Step 5	**`no ip unreachables`**
	Example:
	`Router(config-if)# no ip unreachables`
		Disables the sending of ICMP protocol unreachable and host unreachable messages. This command is enabled by default.
		Note Disabling the unreachable messages also disables IP Path MTU Discovery because path discovery works by having the Cisco IOS XE software send unreachable messages.

Step 6	**`no ip redirects`**
	Example:
	`Router(config-if)# no ip redirects`
		Disables the sending of ICMP redirect messages to learn routes. This command is enabled by default.

Step 7	**`no ip mask-reply`**
	Example:
	`Router(config-if)# no ip mask-reply`
		Disables the sending of ICMP mask reply messages.

Setting the MTU Packet Size

All interfaces have a default MTU packet size. You can adjust the IP MTU size so that the Cisco software will fragment any IP packet that exceeds the MTU set for an interface.

Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** interface configuration command.

All devices on a physical medium must have the same protocol MTU in order to operate.

Perform this task to set the MTU packet size for a specified interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **ip mtu** *bytes*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

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 GigabitEthernet0/0/0`	Specifies the interface to configure and enters interface configuration mode.
Step 4	`ip mtu` *bytes* **Example:** `Router(config-if)# ip mtu 300`	Sets the IP MTU packet size for an interface.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits to privileged EXEC mode.

Configuring IP Accounting

To enable IP accounting, perform this task for each interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip accounting-threshold** *threshold*
4. **ip accounting-list** *ip-address wildcard*
5. **ip accounting-transits** *count*
6. **interface** *type/number*

7. **ip accounting** [**access-violations**] [**output-packets**]
8. **ip accounting mac-address** {**input** | **output**}

DETAILED STEPS

	Command	Purpose
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	**ip accounting-threshold** *threshold* **Example:** `Router(config)# ip accounting-threshold 500`	(Optional) Sets the maximum number of accounting entries to be created.
Step 4	**ip accounting-list** *ip-address wildcard* **Example:** `Router(config)# ip accounting-list 192.31.0.0 0.0.255.255`	(Optional) Filters accounting information for hosts.
Step 5	**ip accounting-transits** *count* **Example:** `Router(config)# ip accounting-transits 100`	(Optional) Controls the number of transit records that will be stored in the IP accounting database.
Step 6	**interface** *type/number* **Example:** `Router(config)# interface GigabitEthernet1/0/0`	Specifies the interface and enters interface configuration mode.
Step 7	**ip accounting** [**access-violations**] [**output-packets**] **Example:** `Router(config-if)# ip accounting access-violations`	Enables basic IP accounting. • Use the optional **access-violations** keyword to enable IP accounting with the ability to identify IP traffic that fails IP access lists. • Use the optional **output-packets** keyword to enable IP accounting based on the IP packets output on the interface.

Step 8	**ip accounting mac-address** {**input** | **output**}
	Example:
	`Router(config-if)# ip accounting mac-address output`
		(Optional) Configures IP accounting based on the MAC address of received (input) or transmitted (output) packets.

Monitoring and Maintaining the IP Network

You can display specific statistics such as the contents of IP routing tables, caches, databases and socket information. The resulting information can be used to determine resource utilization and to solve network problems.

To monitor and maintain your IP network, perform any of the optional steps in this task.

SUMMARY STEPS

1. **clear ip traffic**
2. **clear ip accounting** [**checkpoint**]
3. **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]
4. **show interface** [*type number*] **mac**
5. **show ip redirects**
6. **show ip sockets**
7. **show ip traffic**

Step 1 **clear ip traffic**

To clear all IP traffic statistical counters on all interfaces, use the following command:

```
Router# clear ip traffic
```

Step 2 **clear ip accounting** [**checkpoint**]

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become or are suspected to be invalid. To clear the active IP accounting database when IP accounting is enabled, use the following command:

```
Router# clear ip accounting
```

To clear the checkpointed IP accounting database when IP accounting is enabled, use the following command:

```
Router# clear ip accounting checkpoint
```

Step 3 **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]

To display access list violations, use the **show ip accounting** command. To use this command, you must first enable IP accounting on a per-interface basis.

Use the **checkpoint** keyword to display the checkpointed database. Use the **output-packets** keyword to indicate that information pertaining to packets that passed access control and were routed should be displayed. Use the **access-violations** keyword to display the number of the access list failed by the last packet for the source and destination pair. The number of packets reveals how aggressive the attack is upon a specific destination. If you do not specify the **access-violations** keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

If neither the **output-packets** nor **access-violations** keyword is specified, output-packets is the default.

The following is sample output from the **show ip accounting** command:

```
Router# show ip accounting

   Source          Destination              Packets              Bytes
 172.16.19.40    192.168.67.20                 7                306
 172.16.13.55    192.168.67.20                 67                2749
 172.16.2.50     192.168.33.51                 17                1111
 172.16.2.50     172.31.2.1                    5                 319
 172.16.2.50     172.31.1.2                    463               30991
 172.16.19.40    172.16.2.1                     4                 262
 172.16.19.40    172.16.1.2                     28                2552
 172.16.20.2     172.16.6.100                   39                2184
 172.16.13.55    172.16.1.2                     35                3020
 172.16.19.40    192.168.33.51                 1986               95091
 172.16.2.50     192.168.67.20                  233               14908
 172.16.13.28    192.168.67.53                  390               24817
 172.16.13.55    192.168.33.51               214669             9806659
 172.16.13.111   172.16.6.23                 27739             1126607
 172.16.13.44    192.168.33.51                35412             1523980
 192.168.7.21    172.163.1.2                     11                 824
 172.16.13.28    192.168.33.2                    21                1762
 172.16.2.166    192.168.7.130                  797              141054
 172.16.3.11     192.168.67.53                    4                 246
 192.168.7.21    192.168.33.51                15696              695635
 192.168.7.24    192.168.67.20                   21                 916
 172.16.13.111   172.16.10.1                    16                1137
 accounting threshold exceeded for 7 packets and 433 bytes
```

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
172.16.19.40    192.168.67.20             7          306         77
172.16.13.55    192.168.67.20            67         2749        185
172.16.2.50     192.168.33.51            17         1111        140
172.16.2.50     172.16.2.1               5          319        140
172.16.19.40    172.16.2.1               4          262         77
Accounting data age is 41
```

Step 4 **show interface** [*type number*] **mac**

To display information for interfaces configured for MAC accounting, use the **show interface mac** command. The following is sample output from the **show interface mac** command:

```
Router# show interface GigabitEthernet 0/0/0 mac

GigabitEthernet0/0/0
Input  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2684ms ago
Total:  4 packets, 456 bytes
Output  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2692ms ago
Total:  4 packets, 456 bytes
```

Step 5 **show ip redirects**

To display the address of the default router and the address of hosts for which an ICMP redirect message has been received, use the **show ip redirects** command.

The following is sample output from the **show ip redirects** command:

```
Router# show ip redirects

Default gateway is 172.16.80.29

Host               Gateway          Last Use    Total Uses  Interface
172.16.1.111      172.16.80.240         0:00            9  Ethernet0
172.16.1.4        172.16.80.240         0:00            4  Ethernet0
```

Step 6 **show ip sockets**

To display IP socket information, and to verify that the socket being used is opening correctly, use the **show ip sockets** command. If there is a local and remote endpoint, a connection is established with the ports indicated.

The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets

Proto    Remote         Port      Local           Port  In Out Stat TTY OutputIF
 17      10.0.0.0         0       172.16.186.193  67    0   0     1   0
 17      172.16.191.135   514     172.16.191.129  1811  0   0     0   0
 17      172.16.135.20    514     172.16.191.1    4125  0   0     0   0
 17      172.16.207.163   49      172.16.186.193  49    0   0     9   0
 17      10.0.0.0         123     172.16.186.193  123   0   0     1   0
 88      10.0.0.0         0       172.16.186.193  202   0   0     0   0
 17      172.16.96.59     32856   172.16.191.1    161   0   0     1   0
 17     --listen--             --any--        496  0    0   1    0
```

Step 7 **show ip traffic**

To display IP protocol statistics, use the **show ip traffic** command. The following example shows that the IP traffic statistics have been cleared by the **clear ip traffic** command:

```
Router# clear ip traffic
Router# show ip traffic

IP statistics:
 Rcvd:  0 total, 0 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options, 0 with options
 Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
        0 timestamp, 0 extended security, 0 record route
        0 stream ID, 0 strict source route, 0 alert, 0 cipso
        0 other
 Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 couldn't fragment
 Bcast: 0 received, 0 sent
 Mcast: 0 received, 0 sent
 Sent: 0 generated, 0 forwarded
 Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 0 unicast RPF, 0 forced drop

ICMP statistics:
 Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
       0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
       0 parameter, 0 timestamp, 0 info request, 0 other
       0 irdp solicitations, 0 irdp advertisements
 Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
       0 mask requests, 0 mask replies, 0 quench, 0 timestamp
       0 info reply, 0 time exceeded, 0 parameter problem
       0 irdp solicitations, 0 irdp advertisements

UDP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total, 0 forwarded broadcasts

TCP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total

Probe statistics:
 Rcvd: 0 address requests, 0 address replies
```

```
       0 proxy name requests, 0 where-is requests, 0 other
 Sent: 0 address requests, 0 address replies (0 proxy)
       0 proxy name replies, 0 where-is replies

EGP statistics:
 Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
 Sent: 0 total

IGRP statistics:
 Rcvd: 0 total, 0 checksum errors
 Sent: 0 total

OSPF statistics:
 Rcvd: 0 total, 0 checksum errors
       0 hello, 0 database desc, 0 link state req
       0 link state updates, 0 link state acks

 Sent: 0 total

IP-IGRP2 statistics:
 Rcvd: 0 total
 Sent: 0 total

PIMv2 statistics: Sent/Received
 Total: 0/0, 0 checksum errors, 0 format errors
 Registers: 0/0, Register Stops: 0/0, Hellos: 0/0
 Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
 Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0

IGMP statistics: Sent/Received
 Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
 Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
 DVMRP: 0/0, PIM: 0/0
```

Configuration Examples for IP Services

- Example: Protecting Your Network from DOS Attacks, page 13
- Example: Setting the MTU Packet Size, page 14
- Example: Configuring IP Accounting, page 14

Example: Protecting Your Network from DOS Attacks

The following example shows how to change some of the ICMP defaults for GigabitEthernet interface 0/0/0 to prevent ICMP from relaying information about paths, routes, and network conditions, which can be used by an attacker to gain network mapping information.

Disabling the unreachable messages will have a secondary effect: it also will disable IP Path MTU Discovery, because path discovery works by having the Cisco IOS XE software send Unreachable messages. If you have a network segment with a small number of devices and an absolutely reliable traffic pattern—which could easily happen on a segment with a small number of rarely used user devices—you would be disabling options that your device would be unlikely to use anyway.

```
Router(config)# no ip source-route
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
```

Example: Setting the MTU Packet Size

The following example shows how to change the default MTU packet size for GigabitEthernet interface 0/0/0:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip mtu 300
```

Example: Configuring IP Accounting

The following example shows how to enable IP accounting based on the source and destination MAC address:

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip accounting mac-address input
Router(config-if)# ip accounting mac-address output
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IP addressing services configuration tasks	*Cisco IOS XE IP Addressing Services Configuration Guide*
IP application services configuration tasks	*Cisco IOS XE IP Application Services Configuration Guide*
IP application services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference.*

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	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

RFC	Title
RFC 791	*Internet Protocol*
RFC 792	*Internet Control Message Protocol*
RFC 1191	*Path MTU discovery*

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 IP Services

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for IP Services

Feature Name	Releases	Feature Information
Clear IP Traffic CLI	Cisco IOS XE Release 2.1	The Clear IP Traffic CLI feature introduced the **clear ip traffic** command to clear all IP traffic statistics on a router instead of reloading the router. For added safety, the user will see a confirmation prompt when entering this command. The following sections provide information about this feature: • Monitoring and Maintaining the IP Network, page 10 The following command was introduced by this feature: **clear ip traffic**.

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

Configuring TCP

First Published: October 23, 2006
Last Updated: September 23, 2010

TCP is a protocol that specifies the format of data and acknowledgments used in data transfer. TCP is a connection-oriented protocol because participants must establish a connection before data can be transferred. By performing flow control and error correction, TCP guarantees reliable, in-sequence delivery of packets. It is considered a reliable protocol because if an IP packet is dropped or received out of order, TCP will request the correct packet until it receives it. This module explains the concepts related to TCP and describes how to configure TCP in a network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for TCP" section on page 16.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for TCP

TCP Time Stamp, TCP Selective Acknowledgment, and TCP Header Compression

Because TCP time stamps are always sent and echoed in both directions and the time-stamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP time-stamp option is disabled. If you want to use TCP header compression over a serial line, TCP time stamp and TCP selective acknowledgment must be disabled. Both features are disabled by default. Use the **no ip tcp selective-ack** command to disable TCP selective acknowledgment once it is enabled.

Information About TCP

TCP Services

TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the Open Systems Interconnection (OSI) reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to handle lost, delayed, duplicate, or misread packets. A timeout mechanism allows devices to detect lost packets and request retransmission.

TCP offers efficient flow control, which means that the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers when sending acknowledgments back to the source.

TCP offers full-duplex operation and TCP processes can both send and receive at the same time.

TCP multiplexing allows numerous simultaneous upper-layer conversations to be multiplexed over a single connection.

TCP Connection Establishment

To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

A three-way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side also is ready to transmit. The three-way handshake is necessary so that packets are not transmitted or retransmitted during session establishment or after session termination.

Each host randomly chooses a sequence number used to track bytes within the stream it is sending. Then, the three-way handshake proceeds in the following manner:

- The first host (Host A) initiates a connection by sending a packet with the initial sequence number (X) and synchronize/start (SYN) bit set to indicate a connection request.
- The second host (Host B) receives the SYN, records the sequence number X, and replies by acknowledging the SYN (with an ACK = X + 1). Host B includes its own initial sequence number (SEQ = Y). An ACK = 20 means the host has received bytes 0 through 19 and expects byte 20 next. This technique is called forward acknowledgment.
- Host A acknowledges all bytes Host B sent with a forward acknowledgment indicating the next byte Host A expects to receive (ACK = Y + 1). Data transfer then can begin.

TCP Connection Attempt Time

You can set the amount of time the Cisco IOS XE software will wait to attempt to establish a TCP connection. Because the connection attempt time is a host parameter, it does not pertain to traffic going through the device, just to traffic originated at the device. To set the TCP connection attempt time, use the **ip tcp synwait-time** command in global configuration mode. The default is 30 seconds.

TCP Selective Acknowledgment

The TCP Selective Acknowledgment feature improves performance in the event that multiple packets are lost from one TCP window of data.

Prior to this feature, with the limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per round-trip time. An aggressive sender could choose to resend packets early, but such re-sent segments might have already been successfully received.

The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that have been received. In other words, the receiver can acknowledge packets received out of order. The sender can then resend only the missing data segments (instead of everything since the first missing packet).

Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would need to be re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 must be re-sent.

TCP selective acknowledgment is used only when multiple packets are dropped within one TCP window. There is no performance impact when the feature is enabled but not used. Use the **ip tcp selective-ack** command in global configuration mode to enable TCP selective acknowledgment.

Refer to RFC 2018 for more detailed information about TCP selective acknowledgment.

TCP Time Stamp

The TCP time-stamp option provides improved TCP round-trip time measurements. Because the time stamps are always sent and echoed in both directions and the time-stamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP time-stamp option is disabled. Use the **ip tcp timestamp** command to enable the TCP time-stamp option.

Refer to RFC 1323 for more detailed information on TCP time stamp.

TCP Maximum Read Size

The maximum number of characters that TCP reads from the input queue for Telnet and rlogin at one time is a very large number (the largest possible 32-bit positive number) by default. To change the TCP maximum read size value, use the **ip tcp chunk-size** command in global configuration mode.

We do not recommend that you change this value.

TCP Path MTU Discovery

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection, which is described in RFC 1191. IP Path MTU Discovery allows a host to dynamically discover and cope with differences in the maximum allowable maximum transmission unit (MTU) size of the various links along the path. Sometimes a router is unable to forward a datagram because it requires fragmentation (the packet is larger than the MTU you set for the interface with the **interface** configuration command), but the “don't fragment” (DF) bit is set. The intermediate gateway sends a “Fragmentation needed and DF bit set” Internet Control Message Protocol (ICMP) message to the sending host, alerting it to the problem. Upon receiving this ICMP message, the host reduces its assumed path MTU and consequently sends a smaller packet that will fit the smallest packet size of all the links along the path.

By default, TCP Path MTU Discovery is disabled. Existing connections are not affected when this feature is enabled or disabled.

Customers using TCP connections to move bulk data between systems on distinct subnets would benefit most by enabling this feature. Customers using remote source-route bridging (RSRB) with TCP encapsulation, serial tunnel (STUN), X.25 Remote Switching (also known as XOT or X.25 over TCP), and some protocol translation configurations might also benefit from enabling this feature.

Use the **ip tcp path-mtu-discovery** global configuration command to enable Path MTU Discovery for connections initiated by the router when it is acting as a host.

For more information about Path MTU Discovery, refer to the "Configuring IP Services" chapter of the *Cisco IOS XE IP Application Services Configuration Guide*.

TCP Window Scaling

The TCP Window Scaling feature adds support for the Window Scaling option in RFC 1323, *TCP Extensions for High Performance*. A larger window size is recommended to improve TCP performance in network paths with large bandwidth-delay product characteristics that are called Long Fat Networks (LFNs). The TCP Window Scaling enhancement provides that support.

The window scaling extension in Cisco IOS XE software expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header. The window size can increase to a scale factor of 14. Typical applications use a scale factor of 3 when deployed in LFNs.

The TCP Window Scaling feature complies with RFC 1323. The maximum window size was increased to 1,073,741,823 bytes. The larger scalable window size will allow TCP to perform better over LFNs. Use the **ip tcp window-size** command in global configuration mode to configure the TCP window size.

TCP Sliding Window

A TCP sliding window provides more efficient use of network bandwidth because it enables hosts to send multiple bytes or packets before waiting for an acknowledgment.

In TCP, the receiver specifies the current window size in every packet. Because TCP provides a byte-stream connection, window sizes are expressed in bytes. A window is the number of data bytes that the sender is allowed to send before waiting for an acknowledgment. Initial window sizes are indicated at connection setup, but might vary throughout the data transfer to provide flow control. A window size of zero means "Send no data." The default TCP window size is 4128 bytes. We recommend you keep the default value unless you know your router is sending large packets (greater than 536 bytes). Use the **ip tcp window-size** command to change the default window size.

In a TCP sliding-window operation, for example, the sender might have a sequence of bytes to send (numbered 1 to 10) to a receiver who has a window size of five. The sender then places a window around the first five bytes and transmits them together. The sender then waits for an acknowledgment.

The receiver responds with an ACK = 6, indicating that it has received bytes 1 to 5 and is expecting byte 6 next. In the same packet, the receiver indicates that its window size is 5. The sender then moves the sliding window five bytes to the right and transmit bytes 6 to 10. The receiver responds with an ACK = 11, indicating that it is expecting sequenced byte 11 next. In this packet, the receiver might indicate that its window size is 0 (because, for example, its internal buffers are full). At this point, the sender cannot send any more bytes until the receiver sends another packet with a window size greater than 0.

TCP Outgoing Queue Size

The default TCP outgoing queue size per connection is 5 segments if the connection has a TTY associated with it (such as a Telnet connection). If no TTY connection is associated with a connection, the default queue size is 20 segments. Use the **ip tcp queuemax** command to change the 5-segment default value.

TCP MSS Adjustment

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

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

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

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

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

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

See the "Configuring the MSS Value and MTU for Transient TCP SYN Packets" section on page 9 for configuration instructions.

TCP Applications Flags Enhancement

The TCP Applications Flags Enhancement feature enables the user to display additional flags with reference to TCP applications. There are two types of flags: status and option. The status flags indicate the status of TCP connections such as retransmission timeouts, application closed, and synchronized (SYNC) handshakes for listen. The additional flags indicate the state of set options such as whether a VRF is set, whether a user is idle, and whether a keepalive timer is running. Use the **show tcp** command to display TCP application flags.

TCP Show Extension

The TCP Show Extension feature introduces the capability to display addresses in IP format instead of hostname format and to display the VRF table associated with the connection. To display the status for all endpoints with the addresses in IP format, use the **show tcp brief numeric** command.

Zero-Field TCP Packets

Prior to Cisco IOS XE Release 2.5, when a zero-field TCP packet is received on the router, the TCP packet counter is incremented.

In Cisco IOS XE Release 2.5 and later releases, when a zero-field TCP packet is received on the router, the TCP packet counter is not incremented.

When a zero-field TCP packet is received, it is displayed as 0 under the TCP statistics field when the **show ip traffic** command is configured. When the **debug ip tcp packet** command is configured, and a zero-field TCP packet is received, a debug message similar to the following is displayed:

```
Jan 19 21:57:28.487: TCP: Alert! Received a segment with cleared flags 10.4.14.49
```

How to Configure TCP

- Configuring TCP Performance Parameters, page 7
- Configuring the MSS Value and MTU for Transient TCP SYN Packets, page 9
- Verifying TCP Performance Parameters, page 10

Configuring TCP Performance Parameters

Prerequisites

Both sides of the link must be configured to support window scaling or the default of 65,535 bytes will apply as the maximum window size.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip tcp synwait-time** *seconds*
4. **ip tcp path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}]
5. **ip tcp selective-ack**
6. **ip tcp timestamp**
7. **ip tcp chunk-size** *characters*
8. **ip tcp window-size** *bytes*
9. **ip tcp queuemax** *packets*

DETAILED STEPS

	Command or Action	Purpose
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	**ip tcp synwait-time** *seconds* **Example:** `Router(config)# ip tcp synwait-time 60`	(Optional) Sets the amount of time the Cisco IOS XE software will wait to attempt to establish a TCP connection. - The default is 30 seconds.
Step 4	**ip tcp path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] **Example:** `Router(config)# ip tcp path-mtu-discovery age-timer 11`	(Optional) Enables Path MTU Discovery. - **age-timer**—Time interval, in minutes, TCP reestimates the path MTU with a larger MSS. The default is 10 minutes. The maximum is 30 minutes. - **infinite**—Disables the age timer.
Step 5	**ip tcp selective-ack** **Example:** `Router(config)# ip tcp selective-ack`	(Optional) Enables TCP selective acknowledgment.
Step 6	**ip tcp timestamp** **Example:** `Router(config)# ip tcp timestamp`	(Optional) Enables the TCP time stamp.
Step 7	**ip tcp chunk-size** *characters* **Example:** `Router(config)# ip tcp chunk-size 64000`	(Optional) Sets the TCP maximum read size for Telnet or rlogin. **Note** We do not recommend that you change this value.
Step 8	**ip tcp window-size** *bytes* **Example:** `Router(config)# ip tcp window-size 75000`	(Optional) Sets the TCP window size. The *bytes* argument can be set to an integer from 0 to 1073741823. - To enable window scaling to support LFNs, the TCP window size must be more than 65535. The default window size is 4128 if window scaling is not configured.
Step 9	**ip tcp queuemax** *packets* **Example:** `Router(config)# ip tcp queuemax 10`	(Optional) Sets the TCP outgoing queue size.

Configuring the MSS Value and MTU for Transient TCP SYN Packets

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

If you are configuring the **ip mtu** command on the same interface as the **ip tcp adjust-mss** command, we recommend that you use the following commands and values:

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip tcp adjust-mss** *max-segment-size*
5. **ip mtu** *bytes*
6. **end**

DETAILED STEPS

	Command or Action	Purpose

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 1/0/0`
		Configures an interface type and enters interface configuration mode.

Step 4	**`ip tcp adjust-mss`** *`max-segment-size`*
	Example:
	`Router(config-if)# ip tcp adjust-mss 1452`
		Adjusts the MSS value of TCP SYN packets going through a router.
		• The *max-segment-size* argument is the maximum segment size, in bytes. The range is from 500 to 1460.

Step 5	**`ip mtu`** *`bytes`*
	Example:
	`Router(config-if)# ip mtu 1492`
		Sets the MTU size of IP packets, in bytes, sent on an interface.

Step 6	**`end`**
	Example:
	`Router(config-if)# end`
		Exits to global configuration mode.

Verifying TCP Performance Parameters

SUMMARY STEPS

1. **show tcp** [*line-number*]
2. **show tcp brief** [**all** | **numeric**]
3. **debug ip tcp transactions**

DETAILED STEPS

Step 1 **show tcp** [*line-number*]

Displays the status of TCP connections. The arguments and keyword are as follows:

- *line-number*—(Optional) Absolute line number of the Telnet connection status.

The following is sample output that displays the status and option flags:

```
Router# show tcp
.
.
.
Status Flags: passive open, active open, retransmission timeout, app closed
Option Flags: vrf id set
IP Precedence value: 6
.
.
.
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
 Status Flags: active open, retransmission timeout
 Option Flags: vrf id set
 IP Precedence value: 6
```

Step 2 **show tcp brief** [**all** | **numeric**]

(Optional) Displays addresses in IP format.

Use the **show tcp brief** command to display a concise description of TCP connection endpoints. Use the optional **all** keyword to display the status for all endpoints with the addresses in a Domain Name System (DNS) hostname format. Without this keyword, endpoints in the LISTEN state are not shown. Use the optional **numeric** keyword to display the status for all endpoints with the addresses in IP format.

The following is sample output from the **show tcp brief** command while a user is connected to the system by using Telnet:

```
Router# show tcp brief

TCB       Local Address           Foreign Address        (state)
609789AC  Router.cisco.com.23     cider.cisco.com.3733   ESTAB
```

The following example shows the IP activity after the **numeric** keyword to display the addresses in IP format:

```
Router# show tcp brief numeric

TCB           Local Address          Foreign Address     (state)
6523A4FC      10.1.25.3.11000        10.1.25.3.23         ESTAB
65239A84      10.1.25.3.23           10.1.25.3.11000      ESTAB
653FCBBC      *.1723 *.* LISTEN
```

Step 3 **debug ip tcp transactions**

Use the **debug ip tcp transactions** command to display information about significant TCP transactions such as state changes, retransmissions, and duplicate packets. This command is particularly useful for debugging a performance problem on a TCP/IP network that you have isolated above the data-link layer.

The following is sample output from the **debug ip tcp transactions** command:

```
Router# debug ip tcp transactions

TCP: sending SYN, seq 168108, ack 88655553
TCP0: Connection to 10.9.0.13:22530, advertising MSS 966
TCP0: state was LISTEN -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: state was SYNSENT -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: Connection to 10.9.0.13:22530, received MSS 956
TCP0: restart retransmission in 5996
TCP0: state was SYNRCVD -> ESTAB [23 -> 10.9.0.13(22530)]
TCP2: restart retransmission in 10689
TCP2: restart retransmission in 10641
TCP2: restart retransmission in 10633
TCP2: restart retransmission in 13384 -> 10.0.0.13(16151)]
TCP0: restart retransmission in 5996 [23 -> 10.0.0.13(16151)]
```

The following line from the **debug ip tcp transactions** command output shows that TCP has entered Fast Recovery mode:

```
fast re-transmit - sndcwnd - 512, snd_last - 33884268765
```

The following lines from the **debug ip tcp transactions** command output show that a duplicate acknowledgment is received when TCP is in Fast Recovery mode (first line) and a partial acknowledgment has been received (second line):

```
TCP0:ignoring second congestion in same window sndcwn - 512, snd_1st - 33884268765
TCP0:partial ACK received sndcwnd:338842495
```

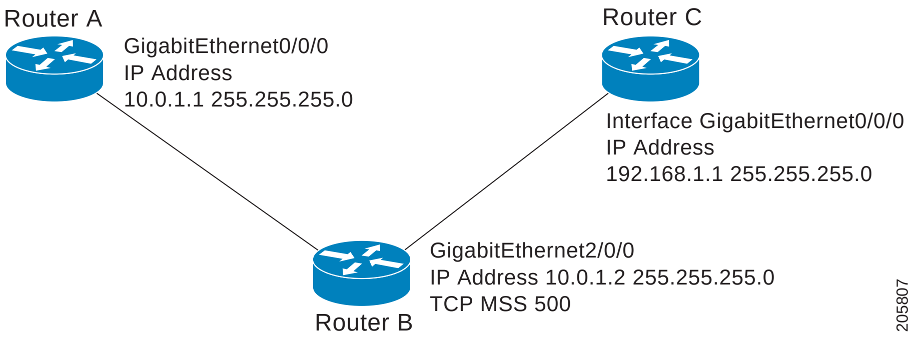
Configuration Examples for TCP

- Example: Configuring the TCP MSS Adjustment, page 11
- Example: Configuring the TCP Application Flags Enhancement, page 13
- Example: Displaying Addresses in IP Format, page 13

Example: Configuring the TCP MSS Adjustment

Figure 1 shows an example topology for the TCP MSS adjustment configuration.

Figure 1 Example Topology for TCP MSS Adjustment



The following example shows how to configure and verify the interface adjustment value for the example topology displayed in Figure 1. Configure the interface adjustment value on router B:

```
Router_B(config)# interface GigabitEthernet2/0/0
Router_B(config-if)# ip tcp adjust-mss 500
```

Telnet from router A to router C, with B having the MSS adjustment configured:

```
Router_A# telnet 192.168.1.1
Trying 192.168.1.1... Open
```

Observe the debug output from router C:

```
Router_C# debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 500, MSS is
500
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 500
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

The MSS gets adjusted to 500 on Router B as configured.

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
Router(config)# vpdn enable
Router(config)# no vpdn logging
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol pppoe
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# exit
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 192.168.100.1.255.255.255.0
Router(config-if)# ip tcp adjust-mss 1452
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface ATM0
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# pvc 8/35
Router(config-if)# pppoe client dial-pool-number 1
Router(config-if)# dsl equipment-type CPE
Router(config-if)# dsl operating-mode GSHDSL symmetric annex B
Router(config-if)# dsl linerate AUTO
Router(config-if)# exit
Router(config)# interface Dialer1
Router(config-if)3 ip address negotiated
Router(config-if)# ip mtu 1492
Router(config-if)# ip nat outside
Router(config-if)# encapsulation ppp
Router(config-if)# dialer pool 1
Router(config-if)# dialer-group 1
Router(config-if)# ppp authentication pap callin
Router(config-if)# ppp pap sent-username sohodyn password 7 141B1309000528
Router(config-if)# ip nat inside source list 101 Dialer1 overload
Router(config-if)# exit
Router(config)# ip route 0.0.0.0.0.0.0.0 Dialer1
Router(config)# access-list permit ip 192.168.100.0.0.0.0.255 any
```

Example: Configuring the TCP Application Flags Enhancement

The following output shows the flags (status and option) displayed using the **show tcp** command:

```
Router# show tcp
.
.
.
Status Flags: passive open, active open, retransmission timeout
 App closed

Option Flags: vrf id set
IP Precedence value: 6
.
.
.
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
```

Example: Displaying Addresses in IP Format

The following example shows the IP activity by using the **numeric** keyword to display the addresses in IP format:

```
Router# show tcp brief numeric

TCB           Local Address           Foreign Address     (state)
6523A4FC      10.1.25.3.11000         10.1.25.3.23         ESTAB
65239A84      10.1.25.3.23            10.1.25.3.11000      ESTAB
653FCBBC      *.1723 *.* LISTEN
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
IP application services configuration tasks	*Cisco IOS XE IP Application Services Configuration Guide*
IP application services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*
Path MTU Discovery	"Configuring IP Services" module

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
CISCO-TCP-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

RFC	Title
RFC 793	*Transmission Control Protocol*
RFC 1191	*Path MTU discovery*
RFC 1323	*TCP Extensions for High Performance*
RFC 2018	*TCP Selective Acknowledgment Options*
RFC 2581	*TCP Congestion Control*
RFC 3782	*The NewReno Modification to TCP's Fast Recovery Algorithm*
RFC 4022	*Management Information Base for the Transmission Control Protocol (TCP)*

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 TCP

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for TCP

Feature Name	Releases	Feature Information
TCP Application Flags Enhancement	Cisco IOS XE Release 2.1	The TCP Applications Flags Enhancement feature enables the user to display additional flags with reference to TCP applications. There are two types of flags: status and option. The status flags indicate the status of TCP connections; for example, retransmission timeouts, application closed, and synchronized (SYNC) handshakes for listen. The additional flags indicate the state of set options; for example, whether a VRF identification is set, whether a user is idle, and whether a keepalive timer is running. The following sections contain information about this feature: • TCP Applications Flags Enhancement, page 6 • Example: Configuring the TCP Application Flags Enhancement, page 13 The following command was modified by this feature: **show tcp**.
TCP MIB for RFC 4022 Support	Cisco IOS XE Release 2.1	The TCP MIB for RFC 4022 Support feature introduces support for RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*. RFC 4022 is an incremental change of the TCP MIB to improve the manageability of TCP. There are no new or modified command for this feature.

Table 1 Feature Information for TCP (continued)

Feature Name	Releases	Feature Information
TCP MSS Adjust	Cisco IOS XE Release 2.1	The TCP MSS Adjust feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse a router, specifically TCP segments in the SYN bit set. The following sections provide information about this feature: • TCP MSS Adjustment, page 6 • Configuring the MSS Value and MTU for Transient TCP SYN Packets, page 9 • Example: Configuring the TCP MSS Adjustment, page 11 The following command was introduced by this feature: **ip tcp adjust-mss**.
TCP Show Extension	Cisco IOS XE Release 2.1	The TCP Show Extension feature introduces the capability to display addresses in IP format instead of hostname format and to display the virtual private network VRF table associated with the connection. The following sections contain information about this feature: • TCP Show Extension, page 6 • Verifying TCP Performance Parameters, page 10 • Example: Displaying Addresses in IP Format, page 13 The following command was modified by this feature: **show tcp brief**.
TCP Window Scaling	Cisco IOS XE Release 2.1	The TCP Window Scaling feature adds support for the Window Scaling option in RFC 1323. A larger window size is recommended to improve TCP performance in network paths with large bandwidth, long-delay characteristics that are called Long Fat Networks (LFNs). This TCP Window Scaling enhancement provides that support. The following sections provide information about this feature: • TCP Window Scaling, page 5 • Configuring TCP Performance Parameters, page 7 • Verifying TCP Performance Parameters, page 10 The following commands were introduced or modified by this feature: **ip tcp window-size**.

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.

Configuring VRRP

First Published: May 2, 2005
Last Updated: February 26, 2010

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 router master, with the other routers acting as backups in case the virtual router master fails.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for VRRP" section on page 17.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for VRRP

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

VRRP is supported on Fast Ethernet, Bridge Group Virtual Interface (BVI), Gigabit Ethernet and TenGigabit interfaces, Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.

The **vrrp shutdown** commnd should not be used on an interface that is configured to share its interface IP address with the VRRP virtual address. This is a misconfiguration and may result in duplicate IP address errors.

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 to 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.

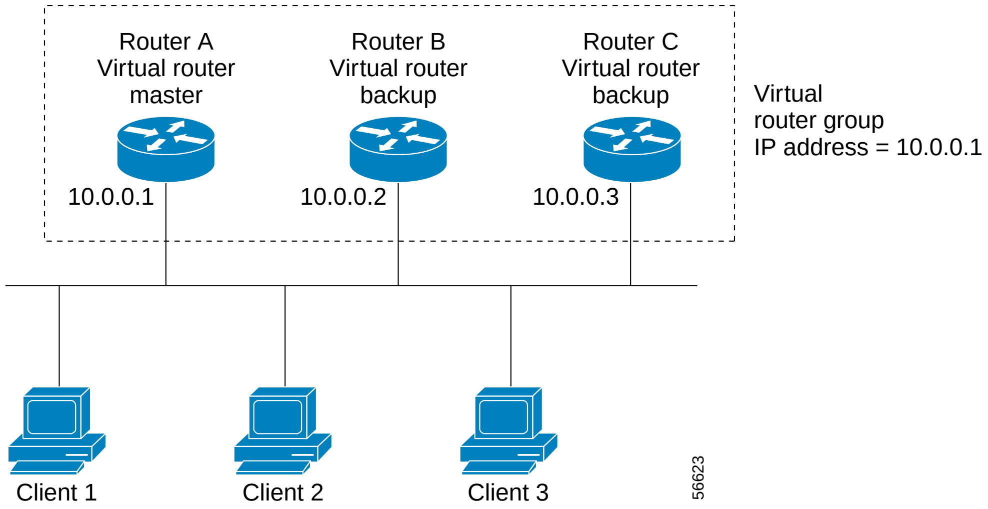
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network 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 Fast Ethernet, BVI, and Gigabit Ethernet interfaces, on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

Figure 1 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 Gigabit Ethernet interface of Router A (10.0.0.1).

Figure 1 Basic VRRP Topology

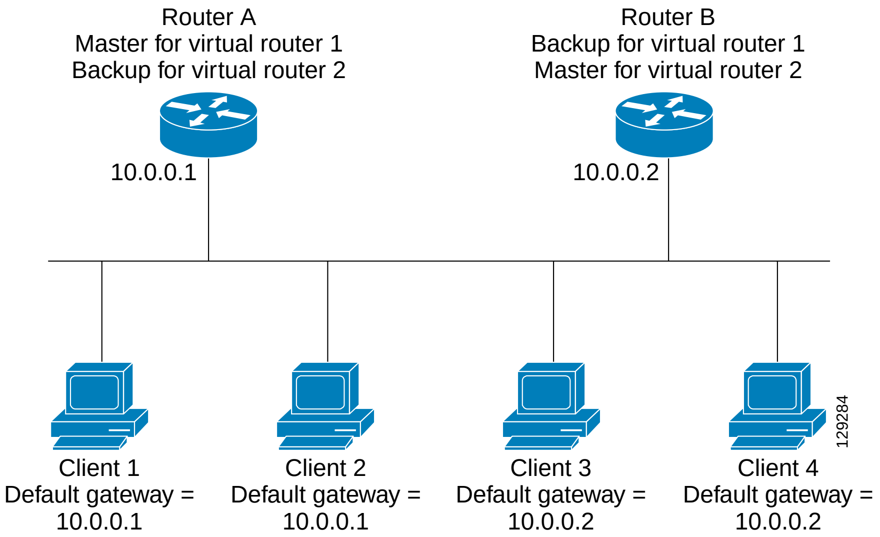


Because the virtual router uses the IP address of the physical Gigabit Ethernet interface of Router A, Router A assumes the role of the *virtual router master* and is also known as the *IP address owner.* As the virtual router master, Router A controls the IP address of the virtual router and is responsible 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 router master fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the "VRRP Router Priority and Preemption" section.

Figure 2 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 2 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 router master, 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 router master, 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

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

Multiple IP Addresses

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on a GigabitEthernet 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 router master with a higher priority virtual router backup that has become available.

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.

Multiple Virtual Router Support

You can configure up to 255 virtual routers on a router physical interface. The actual number of virtual routers that a router interface can support depends on the following factors:

- 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 a master 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 router master 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 router master.

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a virtual router master if the virtual router master 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 router master 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 router master 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 router master.

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 router master. 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 router master remains the master until the original virtual router master recovers and becomes master again.

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 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.

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 Cisco IOS XE 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 XE 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 XE In Service Software Upgrade Process* document.

Stateful Switchover—VRRP

With the introduction of the SSO—VRRP 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 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

- Customizing VRRP, page 7 (optional)
- Enabling VRRP, page 9 (required)
- Disabling a VRRP Group on an Interface, page 10 (optional)

- Configuring VRRP Text Authentication, page 11 (optional)
- Enabling VRRP MIB Trap Support, page 13 (optional)

Customizing VRRP

Perform this task to customize 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 router master 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **description** *text*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **preempt** [**delay minimum** *seconds*]
8. **vrrp** *group* **timers advertise** [**msec**] *interval*
9. **vrrp** *group* **timers learn**
10. **exit**
11. **no vrrp sso**

DETAILED STEPS

	Command or Action	Purpose
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.

	Command or Action	Purpose
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 router master for a VRRP group if it has a higher priority than the current virtual router master. • 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 advertise** [**msec**] *interval* **Example:** `Router(config-if)# vrrp 10 timers advertise 110`	Configures the interval between successive advertisements by the virtual router master in a VRRP group. • The unit of the interval is in seconds unless the **msec** keyword is specified. The default *interval* value is 1 second. **Note** All routers in a VRRP group must use the same timer values. If the same timer values are not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.
Step 9	**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 router master.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 11	**no vrrp sso** **Example:** `Router(config)# no vrrp sso`	(Optional) Disables VRRP support of SSO. • VRRP support of SSO is enabled by default.

Enabling VRRP

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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 master.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 7	**show vrrp** [**brief** | *group*] **Example:** `Router# show vrrp 10`	(Optional) Displays a brief or detailed status of one or all VRRP groups on the router.
Step 8	**show vrrp interface** *type number* [**brief**] **Example:** `Router# show vrrp interface GigabitEthernet 0/0/0`	(Optional) Displays the VRRP groups and their status on a specified interface.

Disabling a VRRP Group on an Interface

Disabling a VRRP group on an interface allows the protocol to be disabled, but the to be configuration retained. This ability was added with the introduction of the VRRP MIB, RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*.

You can use a Simple Network Management Protocol (SNMP) management tool to enable or disable VRRP on an interface. Because of the SNMP management capability, the **vrrp shutdown** command was introduced to represent a method via the command line interface (CLI) for VRRP to show the state that had been configured using SNMP.

When the **show running-config** command is entered, you can see immediately if the VRRP group has been configured and set to enabled or disabled. This is the same functionality that is enabled within the MIB.

The **no** form of the command enables the same operation that is performed within the MIB. If the **vrrp shutdown** command is specified using the SNMP interface, then entering the **no vrrp shutdown** command using the Cisco IOS XE CLI will reenable the VRRP group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **shutdown**

DETAILED STEPS

	Command or Action	Purpose

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 GigabitEthernet0/0/0`
		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`* **`shutdown`**
	Example:
	`Router(config-if)# vrrp 10 shutdown`
		Disables the VRRP group on an interface.
		• The command is now visible on the router.
		Note You can have one VRRP group disabled, while retaining its configuration, and a different VRRP group enabled.

Configuring VRRP Text Authentication

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

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 0/0/1`
		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 master.

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.

Enabling VRRP MIB Trap Support

The VRRP MIB supports SNMP Get operations, which allow network devices to get reports about VRRP groups in a network from the network management station.

Enabling VRRP 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 router becomes a master or backup router. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
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	**snmp-server enable traps vrrp** **Example:** `Router(config)# snmp-server enable traps vrrp`	Enables the router to send SNMP VRRP notifications (traps and informs).
Step 4	**snmp-server host** *host community-string* **vrrp** **Example:** `Router(config)# snmp-server host myhost.comp.com public vrrp`	Specifies the recipient of an SNMP notification operation.

Configuration Examples for VRRP

- Example: Configuring VRRP, page 14
- Example: VRRP Text Authentication, page 15
- Example: Disable a VRRP Group on an Interface, page 15
- Example: VRRP MIB Trap, page 15

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 master for this group with priority 120.
  - Advertising interval is 3 seconds.
  - Preemption is enabled.
- Group 5:
  - Router B will become the master for this group with priority 200.
  - Advertising interval is 30 seconds.
  - Preemption is enabled.
- Group 100:
  - Router A will become the master 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)# 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 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)# interface 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 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 Text Authentication

The following example shows how to configure VRRP text authentication using a text string:

```
Router(config)# interface 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: Disable a VRRP Group on an Interface

The following example shows how to disable one VRRP group on GigabitEthernet interface 0/0/0 while retaining VRRP for group 2 on GigabitEthernet interface 1/0/0:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
Router(config-if)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```

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	*Cisco IOS IP Application Services Command Reference*
Object tracking	*Configuring Enhanced Object Tracking*
Hot Standby Routing Protocol (HSRP)	*Configuring HSRP*
In Service Software Upgrace (ISSU)	*Cisco IOS XE In Service Software Upgrade Process*
Gateway Load Balancing Protocol (GLBP)	*Configuring GLBP*
Stateful Switchover	*Stateful Switchover*

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

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for VRRP

Feature Name	Releases	Feature Information
ISSU—VRRP	Cisco IOS XE Release 2.1	VRRP 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 XE software are running on the active and standby Route Processors (RPs) or line cards. This feature provides customers with the same level of HA functionality for planned outages due to software upgrades as is available with SSO for unplanned outages. That is, the system can switch over to a secondary RP and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default. The following section provides information about this feature: • In Service Software Upgrade—VRRP, page 6 There are no new or modified commands for this feature.
SSO—VRRP	Cisco IOS XE Release 2.1	VRRP is now SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current VRRP group state. This feature is enabled by default. The following sections provide information about this feature: • Stateful Switchover—VRRP, page 6 • Customizing VRRP, page 7 The following commands were introduced or modified by this feature: **debug vrrp ha**, **show vrrp, vrrp sso**.

Table 1 Feature Information for VRRP (continued)

Feature Name	Releases	Feature Information
Virtual Router Redundancy Protocol	Cisco IOS XE Release 2.1	VRRP enables a group of routers to form a single virtual router to provide redundancy. 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. The following commands were introduced by this feature: **debug vrrp all**, **debug vrrp error**, **debug vrrp events**, **debug vrrp packets**, **debug vrrp state**, **show vrrp**, **show vrrp interface**, **vrrp authentication**, **vrrp description**, **vrrp ip**, **vrrp preempt**, **vrrp priority**, **vrrp timers advertise**, **vrrp timers learn**.
VRRP MIB—RFC 2787	Cisco IOS XE Release 2.6	The VRRP MIB—RFC 2787 feature enables an enhancement to the MIB for use with SNMP-based network management. The feature adds support for configuring, monitoring, and controlling routers that use VRRP. The following sections provide information about this feature: • Disabling a VRRP Group on an Interface, page 10 • Enabling VRRP MIB Trap Support, page 13 The following command was introduced by this feature: **vrrp shutdown**. The following commands were modified by this feature: **snmp-server enable traps** and **snmp-server host**.

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 router master fails.

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

VRRP router—A router that is running VRRP.

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

Configuring WCCP

First Published: August 21, 2007
Last Updated: July 30, 2010

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology that intercepts IP packets and redirects those packets to a destination other than that specified in the IP packet. Typically the packets are redirected from their destination web server on the Internet to a content engine that is local to the client. In some WCCP deployment scenarios, redirection of traffic may also be required from the web server to the client. WCCP enables you to integrate content engines into your network infrastructure.

Cisco IOS XE Release 2.2 supports only WCCPv2.

The tasks in this document assume that you have already configured content engines on your network. For specific information on hardware and network planning associated with Cisco Content Engines and WCCP, see the Cisco Content Engines documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/index.htm

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for WCCP" section on page 28.

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for WCCP

- To use WCCP, IP must be configured on the interface connected to the Internet and another interface must be connected to the content engine.
- The interface connected to the content engine must be a Fast Ethernet or Gigabit Ethernet interface.

Restrictions for WCCP

- WCCP works only with IPv4 networks.
- WCCP does not redirect IP multicast packets.
- WCCP packet redirection on outbound interfaces is not supported in XE releases prior to XE Release 3.1S
- There is no SNMP support and no MIB has been implemented for WCCPv2.
- Cisco ASR 1000 Series Routers do not support WCCPv1.
- Cisco ASR 1000 Series Routers do not support inter-VRF redirection.
- Service groups can comprise up to 32 content engines and 32 routers.
- WCCP does not support In-Service Software Upgrade (ISSU), Stateful Switchover (SSO) or Nonstop Forwarding (NSF).
- Transiting packets are lost in the event of a forwarding processor (FP) failover on a 6-rack-unit (6RU) and 13RU chassis.
- All content engines in a cluster must be configured to communicate with all routers servicing the cluster.
- Hash assignment as a load-balancing method for a WCCP service is not supported. As of Cisco IOS XE Release 3.1S, clients that send Hash assignment will not be allowed to come online by the router. On Cisco ASR 1000 Series Routers, the **show ip wccp 61 detail** command displays that Hash is an incompatible assignment method.
- For routers servicing a multicast cluster, the Time To Live (TTL) value must be set at 15 or fewer.
- The **show ip wccp** command displays information about software-based (process, fast and Cisco Express Forwarding [CEF]) forwarding of WCCP packets. The Cisco ASR 1000 Series Routers implement WCCP in hardware, rather than in the CEF or process-switching paths. Implementing WCCP in hardware results in a packet count of 0 when the **show ip wccp** command is entered. Use the **show platform software wccp interface counters** or **show platform software wccp counters** commands to display global statistics related to WCCP on the Cisco ASR 1000 Series Routers.

  In Cisco IOS XE Release 3.1S, the **show ip wccp** command displays redirected WCCP packets.

- When the IP address of an interface that is being used as the router ID (highest IP address of the interfaces) is removed when there is a WCCP cache engine connected via GRE adjacency, the source-IP address of the outer IP packet (of GRE) will continue to use the removed IP address. The traffic will continue to get redirected to the cache engine. This symptom is not visible, as Cisco IOS XE updates the router ID in the protocol messages to the cache engine, and the cache engine uses the new router ID when it sends returns packets to the router.

Configure a loopback address and assign an IP address to it so that it is used as the router ID. It is unlikely that such a loopback IP address will get removed, but when removed, the source IP address of the generic routing encapsulation (GRE) packet from the router to the cache engine will carry the removed IP address. Enter the shutdown command, followed by the no shutdown command on the cache engine interface that has the GRE redirect method configured to stop the interface from using the removed IP address.

The following limitation applies to WCCP Layer 2 Forwarding and Return:

- Layer 2 redirection requires that content engines be directly connected to an interface on each WCCP router. WCCP configuration of the content engine must reference the directly connected interface IP address of the WCCP router and not a loopback IP address or any other IP address configured on the WCCP router.

Information About WCCP

Understanding WCCP

WCCP uses Cisco Content Engines (or other content engines running WCCP) to localize web traffic patterns in the network, enabling content requests to be fulfilled locally. Traffic localization reduces transmission costs and download time.

WCCP enables Cisco IOS XE routing platforms to transparently redirect content requests. The main benefit of transparent redirection is that users need not configure their browsers to use a web proxy. Instead, they can use the target URL to request content, and have their requests automatically redirected to a content engine. The word “transparent” in this case means that the end user does not know that a requested file (such as a web page) came from the content engine instead of from the originally specified server.

When a content engine receives a request, it attempts to service it from its own local cache. If the requested information is not present, the content engine issues its own request to the originally targeted server to get the required information. When the content engine retrieves the requested information, it forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and substantially reducing transmission costs.

WCCP enables a series of content engines, called a content engine cluster, to provide content to a router or multiple routers. Network administrators can easily scale their content engines to handle heavy traffic loads through these clustering capabilities. Cisco clustering technology enables each cluster member to work in parallel, resulting in linear scalability. Clustering content engines greatly improves the scalability, redundancy, and availability of your caching solution. You can cluster up to 32 content engines to scale to your desired capacity.

Layer 2 Forwarding, Redirection and Return

WCCP uses either Generic Routing Encapsulation (GRE) or Layer 2 (L2) to redirect or return IP traffic. When WCCP forwards traffic via GRE, the redirected packets are encapsulated within a GRE header. The packets also have a WCCP redirect header. When WCCP forwards traffic using L2, the original MAC header of the IP packet is overwritten and replaced with the MAC header for the WCCP client.

Using L2 as a forwarding method allows direct forwarding to the content engine without further lookup. Layer 2 redirection requires that the router and content engines are directly connected, that is, on the same IP subnetwork.

When WCCP returns traffic via GRE, the returned packets are encapsulated within a GRE header. The destination IP address is the address of the router and the source address is the address of the WCCP client. When WCCP returns traffic via L2, the original IP packet is returned without any added header information. The router to which the packet is returned will recognize the source of the packet and prevent redirection.

The WCCP redirection method does not have to match the return method.

L2 forwarding, return, or redirection are typically used for hardware accelerated platforms. On Cisco ASR 1000 Series Routers, both the GRE and L2 forward/return methods use the hardware, so there is not any significant performance degradation between them.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp web-cache** command with the **l2-redirect** keyword to configure L2 redirection. For content engines running Cisco Wide Area Application Services (WAAS) software, use the **wccp tcp-promiscuous** command with the **l2-redirect** keyword to configure L2 redirection.

For more information on Cisco ACNS commands used to configure Cisco Content Engines, see the *Cisco ACNS Software Command Reference*, Release 5.5.13, at the following URL:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

For more information on WAAS commands used to configure Cisco Content Engines, see the *Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)* at the following URL:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

WCCP Mask Assignment

The WCCP Mask Assignment feature enables mask assignment as the load-balancing method for a WCCP service.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp web-cache** command with the **mask-assign** keywords to configure mask assignment. For content engines running Cisco Wide Area Application Services (WAAS) software, use the **wccp tcp-promiscuous** command with the **mask-assign** keyword to configure mask assignment.

For more information on Cisco ACNS commands used to configure Cisco Content Engines, see the *Cisco ACNS Software Command Reference*, Release 5.5.13, at the following URL:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

For more information on WAAS commands used to configure Cisco Content Engines, see the *Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)* at the following URL:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

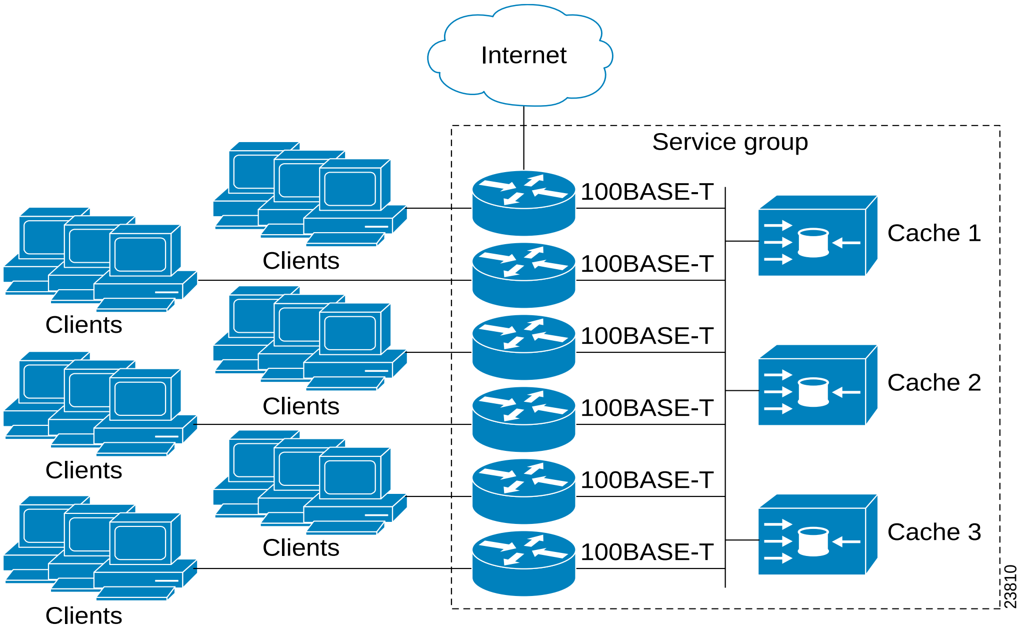
Hardware Acceleration

WCCP implementation on the Cisco ASR 1000 Series Routers is hardware accelerated by default.

WCCPv2 Configuration

Multiple routers can use WCCPv2 to service a content engine cluster. Figure 1 illustrates a sample configuration using multiple routers.

Figure 1 Cisco Content Engine Network Configuration Using WCCPv2



The subset of content engines within a cluster and routers connected to the cluster that are running the same service is known as a *service group*. Available services include TCP and User Datagram Protocol (UDP) redirection.

WCCPv2 requires that each content engine be aware of all the routers in the service group. To specify the addresses of all the routers in a service group, you must choose the following method:

- Unicast—A list of router addresses for each of the routers in the group is configured on each content engine. In this case the address of each router in the group must be explicitly specified for each content engine during configuration.
- Multicast—A single multicast address is configured on each content engine. In the multicast address method, the content engine sends a single-address notification that provides coverage for all routers in the service group. For example, a content engine could indicate that packets should be sent to a multicast address of 224.0.0.100, which would send a multicast packet to all routers in the service group configured for group listening using WCCP (see the **ip wccp group-listen** interface configuration command for details).

The multicast option is easier to configure because you need only specify a single address on each content engine. This option also allows you to add and remove routers from a service group dynamically, without needing to reconfigure the content engines with a different list of addresses each time.

The following sequence of events details how WCCPv2 configuration works:

1. Each content engine is configured with a list of routers.
2. Each content engine announces its presence and a list of all routers with which it has established communications. The routers reply with their view (list) of content engines in the group.
3. When the view is consistent across all content engines in the cluster, one content engine is designated as the lead and sets the policy that the routers need to deploy in redirecting packets.

Support for Services Other Than HTTP

WCCPv2 allows redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic. WCCPv2 supports the redirection of packets intended for other ports, including those used for proxy-web cache handling, File Transfer Protocol (FTP) caching, FTP proxy handling, web caching for ports other than 80, and Real Audio, video, and telephony applications.

To accommodate the various types of services available, WCCPv2 introduces the concept of multiple *service groups*. Service information is specified in the WCCP configuration commands using dynamic services identification numbers (such as 98) or a predefined service keyword (such as **web-cache**). This information is used to validate that service group members are all using or providing the same service.

The content engines in a service group specify traffic to be redirected by protocol (TCP or UDP) and up to eight source or destination ports. Each service group has a priority status assigned to it. The priority of a dynamic service is assigned by the content engine. The priority value is in the range of 0 to 255 where 0 is the lowest priority. The predefined web cache service has an assigned priority of 240.

Support for Multiple Routers

WCCPv2 allows multiple routers to be attached to a cluster of cache engines. The use of multiple routers in a service group allows for redundancy, interface aggregation, and distribution of the redirection load. WCCPv2 supports up to 32 routers per service group. Each service group is established and maintained independently.

MD5 Security

WCCPv2 provides optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard. Shared-secret MD5 one-time authentication (set using the **ip wccp** [**password** [**0** | **7**] *password*] global configuration command) enables messages to be protected against interception, inspection, and replay.

Web Cache Packet Return

If a content engine is unable to provide a requested object it has cached due to error or overload, the content engine will return the request to the router for onward transmission to the originally specified destination server. WCCPv2 provides a check on packets that determines which requests have been returned from the content engine unserviced. Using this information, the router can then forward the request to the originally targeted server (rather than attempting to resend the request to the content engine cluster). This process provides error handling transparency to clients.

Typical reasons why a content engine would reject packets and initiate the packet return feature include the following:

- Instances when the content engine is overloaded and has no room to service the packets
- Instances when the content engine is filtering for certain conditions that make caching packets counterproductive (for example, when IP authentication has been turned on)

WCCP VRF Support

The WCCP VRF Support feature enhances the existing WCCPv2 protocol by implementing support for virtual routing and forwarding (VRF). Inter-VRF redirection is not supported.

The WCCP VRF Support feature allows service groups to be configured on a per VRF basis in addition to those defined globally.

Along with the service identifier, the VRF of WCCP protocol packets arriving at the router is used to associate cache-engines with a configured service group.

The interface on which redirection is applied, the interface which is connected to cache engine, and the interface on which the packet would have left if it had not been redirected must be in the same VRF.

WCCP Bypass Packets

WCCP intercepts IP packets and redirects those packets to a destination other than the destination that is specified in the IP header. Typically the packets are redirected from a web server on the Internet to a web cache that is local to the destination.

Occasionally a web cache decides that it cannot deal with the redirected packets appropriately and returns the packets unchanged to the originating router. These packets are called bypass packets and are returned to the originating router using either Layer 2 forwarding without encapsulation (L2) or encapsulated in generic routing encapsulation (GRE). The router decapsulates and forwards the packets normally.

GRE is a tunneling protocol developed by Cisco that encapsulates packet types from a variety of protocols inside IP tunnels, creating a virtual point-to-point link over an IP network.

WCCP Closed Services and Open Services

In applications where packet flows are intercepted and redirected by a Cisco IOS router to external WCCP client devices, it may be necessary to block the packet flows for the application when a WCCP client device is not available. This blocking is achieved by configuring a WCCP closed service. When a WCCP service is configured as closed, WCCP discards packets that do not have a WCCP client registered to receive the redirected traffic.

By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device.

The **ip wccp service-list** command can only be used for closed-mode services. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When there is a mismatch between the service-list ACL and the definition received from a cache engine, the service is not allowed to start.

WCCP Outbound ACL Check

WCCP operates by intercepting IP packets and redirecting those packets to a destination other than the destination that is specified in the IP header. Typically the packets are redirected from a web server on the Internet to a web cache that is local to the redirecting router.

Access control lists (ACLs) filter network traffic by controlling whether routed packets are forwarded or blocked at the router interface. Each packet is examined to determine whether it will be forwarded or dropped, according to the specified criteria within the ACL. ACL criteria can be the source address of the traffic, the destination address of the traffic, or the upper-layer protocol. An IP ACL is a sequential collection of permit and deny conditions that apply to an IP address. The router tests addresses against the conditions in the ACL one at a time. The first match determines whether the address is accepted or rejected. Because Cisco IOS software stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the router rejects the address, by virtue of an implicit "deny all" clause.

If there is an outbound ACL configured on the interface at which redirection takes place, it is possible, under some circumstances, that hosts whose traffic is redirected will gain access to destinations to which they would otherwise be blocked.

The WCCP Outbound ACL Check feature ensures that the outbound ACL checking is performed at the original interface so that the checking is secure and consistent across all platforms and Cisco IOS switching paths.

WCCP Service Groups

WCCP is a component of Cisco IOS XE software that redirects traffic with defined characteristics from its original destination to an alternative destination. The typical application of WCCP is to redirect traffic bound for a remote web server to a local web cache to improve response time and optimize network resource usage.

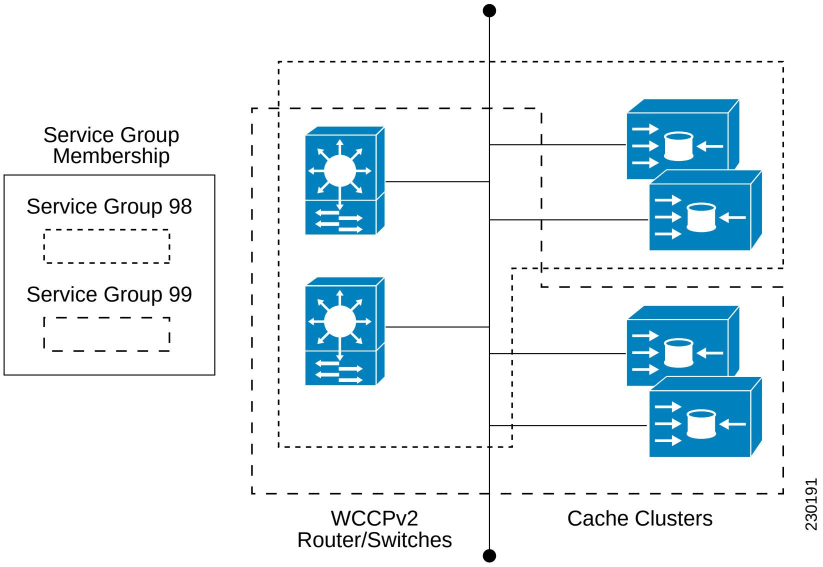
The nature of the selected traffic for redirection is defined by service groups specified on content engines and communicated to routers by using WCCP. The current implementation of WCCP in Cisco IOS XE software allows for a maximum of 256 service groups across all VRFs.

WCCPv2 supports up to 32 routers per service group. Each service group is established and maintained independently.

WCCPv2 uses service groups based on logical redirection services, deployed for intercepting and redirecting traffic. The standard service is web cache, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the content engines. This service is referred to as a *well-known service*, because the characteristics of the web cache service are known by both the router and content engines. A description of a well-known service is not required beyond a service identification. To specify the standard web cache service, use the **ip wccp** command with the **web-cache** keyword.

Note More than one service can run on a router at the same time, and routers and content engines can be part of multiple service groups at the same time.

Figure 2 WCCP Service Groups



The dynamic services are defined by the content engines; the content engine instructs the router which protocol or ports to intercept, and how to distribute the traffic. The router itself does not have information on the characteristics of the dynamic service group's traffic, because this information is provided by the first content engine to join the group. In a dynamic service, up to eight ports can be specified within a single protocol.

Cisco Content Engines, for example, use dynamic service 99 to specify a reverse-proxy service. However, other content engine devices may use this service number for some other service. The configuration information in this document deals with enabling general services on the Cisco ASR 1000 Series Routers.

WCCP: Check Services All

An interface may be configured with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition. When an interface is configured with more than one WCCP service, the precedence of the packets is matched against service groups in priority order.

Note The priority of a WCCP service group cannot be configured via Cisco IOS software.

With the **ip wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL as well as by the service priority.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found that matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check services all** command is configured. When the **ip wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

WCCP Configurable Router ID

WCCP uses a router ID in its control messages and the router ID serves as a means by which a WCCP client can identify a particular WCCP server. The router ID is treated as an IPv4 address and may also be used as the source address of any WCCP-generated GRE frames. Prior to the WCCP Configurable Router ID feature, WCCP selects a router ID using an automatic mechanism; the highest reachable IPv4 address on the system is used as the WCCP router ID. The highest IPv4 address on the system is not always the best choice as the router ID or as the source address of GRE frames. A change in addressing information on the system may cause the WCCP router ID to change unexpectedly. During this changeover period, WCCP clients briefly advertise the existence of two routers (the old router ID and the new Router ID) and GRE frames are sourced from a different address.

The WCCP Configurable Router ID feature enables you to define a WCCP source interface. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, router IDs are not automatically generated when the current router ID is no longer valid and the router ID does not change when another IP address is added to the system. The router ID changes only when a new router ID is manually configured using the **ip wccp source-address** command.

How to Configure WCCP

The following configuration tasks assume that you have already installed and configured the content engines you want to include in your network. You must configure the content engines in the cluster before configuring WCCP functionality on your routers or switches. Refer to the *Cisco Cache Engine User Guide* for content engine configuration and setup tasks.

- Configuring WCCP, page 11 (required)
- Configuring Closed Services, page 13 (optional)
- Registering a Router to a Multicast Address, page 15 (optional)
- Using Access Lists for a WCCP Service Group, page 16 (optional)
- Enabling the WCCP Outbound ACL Check, page 18 (optional)
- Verifying and Monitoring WCCP Configuration Settings, page 19 (optional)

Configuring WCCP

Perform this task to configure WCCP.

Until you configure a WCCP service using the **ip wccp** {**web-cache** | *service-number*} global configuration command, WCCP is disabled on the router. The first use of a form of the **ip wccp** command enables WCCP. By default WCCPv2 is used for services.

Using the **ip wccp web-cache password** command, you can set a password for a router and the content engines in a service group. MD5 password security requires that each router and content engine that wants to join a service group be configured with the service group password. The password can consist of up to eight characters. Each content engine or router in the service group will authenticate the security component in a received WCCP packet immediately after validating the WCCP message header. Packets failing authentication will be discarded.

Restrictions

WCCPv1 is not supported on the Cisco ASR 1000 Series Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp** [**vrf** *vrf-name*] **source-interface** *source-interface*
5. **interface** *type number*
6. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**}
7. **exit**
8. **interface** *type number*
9. **ip wccp redirect exclude in**

DETAILED STEPS

	Command	Purpose

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	**`ip wccp`** `[`**`vrf`** *`vrf-name`*`] {`**`web-cache`** `|` *`service-number`*`} [`**`group-address`** *`group-address`*`] [`**`redirect-list`** *`access-list`*`] [`**`group-list`** *`access-list`*`] [`**`password`** *`password`*`]`
	Example:
	`Router(config)# ip wccp web-cache password password1`
		Specifies a web cache or dynamic service to enable on the router, specifies a VRF name to associate with the service group, specifies the IP multicast address used by the service group, specifies any access lists to use, specifies whether to use MD5 authentication, and enables the WCCP service.

Step 4	**`ip wccp`** `[`**`vrf`** *`vrf-name`*`]` **`source-interface`** *`source-interface`*
	Example:
	`Router (config)# ip wccp source-interface GigabitEthernet0/0/0`
		(Optional) Configures a preferred WCCP router ID.

Step 5	**`interface`** *`type number`*
	Example:
	`Router(config)# interface GigabitEthernet0/1/0`
		Targets an interface number for which the web cache service will run, and enters interface configuration mode.

	Command	Purpose

Step 6	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**}
	Example:
	`Router(config-if)# ip wccp web-cache redirect in`
		Enables packet redirection on an inbound or outbound interface using WCCP.

Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/2/0`	Targets an interface number on which to exclude traffic for redirection, and enters interface configuration mode.
Step 9	**ip wccp redirect exclude in** **Example:** `Router(config-if)# ip wccp redirect exclude in`	(Optional) Excludes traffic on the specified interface from redirection. You can use this command in conjunction with the **ip wccp redirect out** command.

Configuring Closed Services

Perform this task to specify the number of service groups for WCCP, to configure a service group as a closed or open service, and to optionally specify a check of all services.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] [*service-number* **service-list** *service-access-list* **mode** {**open** | **closed**}]

   or

   ip wccp [**vrf** *vrf-name*] **web-cache mode** {**open** | **closed**}
4. **ip wccp check services all**
5. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
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	**ip wccp** [**vrf** *vrf-name*] *service-number* **service-list** *service-access-list* **mode** {**open** | **closed**}
	or
	ip wccp [**vrf** *vrf-name*] **web-cache mode** {**open** | **closed**}
	Example:
	`Router(config)# ip wccp 90 service-list 120 mode closed`
	or
	Example:
	`Router(config)# ip wccp web-cache mode closed`
		Configures a dynamic WCCP service as closed or open.
		or
		Configures a web cache service as closed or open.
		Note When configuring the web cache service as a closed service, you cannot specify a service access list.
		Note When configuring a dynamic WCCP service as a closed service, you must specify a service access list.

Step 4	**ip wccp check services all** **Example:** `Router(config)# ip wccp check services all`	(Optional) Enables a check of all WCCP services. With the **ip wccp check services all** command, WCCP can be configured to check the other configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by the redirect ACL and not just the service description. **Note** The **ip wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Step 5	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*}
	Example:
	`Router(config)# ip wccp 201`
		Specifies the WCCP service identifier. You can specify the standard web cache service or a dynamic service number from 0 to 255.
		The maximum number of services that can be specified is 256.

Step 6	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Registering a Router to a Multicast Address

If you decide to use the multicast address option for your service group, you must configure the router to listen for the multicast broadcasts on an interface.

For network configurations where redirected traffic needs to traverse an intervening router, the router being traversed must be configured to perform IP multicast routing. You must configure the following two components to enable traversal over an intervening router:

- Enable IP multicast routing using the **ip multicast-routing** global configuration command.
- Enable the interfaces to which the cache engines will connect to receive multicast transmissions using the **ip wccp group-listen** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address*
5. **interface** *type number*
6. **ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}]}
7. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen**

DETAILED STEPS

	Command	Purpose
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	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address* **Example:** `Router(config)# ip wccp 99 group-address 239.1.1.1`	Specifies the multicast address for the service group.

	Command	Purpose

Step 5	`interface type number`
	Example:
	`Router(config)# interface ethernet0/0`
		Enables the interfaces to which the content engines will connect to receive multicast transmissions for which the web cache service will run, and enters interface configuration mode.

Step 6	`ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]}`
	Example:
	`Router(config-if)# ip pim dense-mode`
		(Optional) Enables Protocol Independent Multicast (PIM) on an interface.
		Note To ensure correct operation of the **ip wccp group-listen** command on Catalyst 6500 series switches and Cisco 7600 series routers, you must enter the **ip pim** command in addition to the **ip wccp group-listen** command.

Step 7	`ip wccp [vrf vrf-name] {web-cache | service-number} group-listen`
	Example:
	`Router(config-if)# ip wccp 99 group-listen`
		Configures an interface to enable or disable the reception of IP multicast packets for WCCP.

Using Access Lists for a WCCP Service Group

Perform this task to configure the router to use an access list to determine which traffic should be directed to which content engines.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
7. Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.
8. **ip wccp web-cache group-list** *access-list*
9. **ip wccp web-cache redirect-list** *access-list*

DETAILED STEPS

	Command	Purpose

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	**access-list** *access-list-number* **remark** *remark* **Example:** `Router(config)# access-list 1 remark Give access to user1`	(Optional) Adds a user-friendly comment about an access list entry. • A remark of up to 100 characters can precede or follow an access list entry.
Step 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Router(config)# access-list 1 permit 172.16.5.22 0.0.0.0`	Creates an access list that enables or disables traffic redirection to the cache engine. Permits the specified source based on a source address and wildcard mask. • Every access list needs at least one permit statement; it need not be the first entry. • Standard IP access lists are numbered 1 to 99 or 1300 to 1999. • If the *source-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword **any** as a substitute for the *source source-wildcard* to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.5.22 is allowed to pass the access list.
Step 5	**access-list** *access-list-number* **remark** *remark* **Example:** `Router(config)# access-list 1 remark Give access to user1`	(Optional) Adds a user-friendly comment about an access list entry. • A remark of up to 100 characters can precede or follow an access list entry.

	Command	Purpose
Step 6	**access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Router(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	Denies the specified source based on a source address and wildcard mask. • If the *source-wildcard* is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the abbreviation any as a substitute for the *source source-wildcard* to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.7.34 is denied passing the access list.
Step 7	Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit **deny** statement at the end of the access list.
Step 8	**ip wccp web-cache group-list** *access-list* **Example:** `Router(config) ip wccp web-cache group-list 1`	Indicates to the router from which IP addresses of content engines to accept packets.
Step 9	**ip wccp web-cache redirect-list** *access-list* **Example:** `Router(config)# ip wccp web-cache redirect-list 1`	(Optional) Disables caching for certain clients.

Enabling the WCCP Outbound ACL Check

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp check acl outbound**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

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	**`ip wccp`** [**`vrf`** *`vrf-name`*] {**`web-cache`** | *`service-number`*} [**`group-address`** *`multicast-address`*] [**`redirect-list`** *`access-list`*] [**`group-list`** *`access-list`*] [**`password`** *`password`*] **Example:** `Router(config)# ip wccp web-cache`	Enables the support for a Cisco content engine service group or any content engine service group and configures a redirect ACL list or group ACL.

Step 4	**`ip wccp check acl outbound`**
	Example:
	`Router(config)# ip wccp check acl outbound`
		Enables the ACL outbound check on the originating interface.
		Note The **ip wccp outbound-check-acl** command can also be configured.

Step 5	**`exit`**
	Example:
	`Router(config)# exit`
		Exits global configuration.

Verifying and Monitoring WCCP Configuration Settings

The **show ip wccp** command displays information about software-based (process, fast, and Cisco Express Forwarding [CEF]) forwarding of WCCP packets. The Cisco ASR 1000 Series Routers implement WCCP in hardware, rather than in the CEF or process-switching paths. Implementing WCCP in hardware results in a packet count of 0 when the **show ip wccp** command is entered in Cisco IOS XE releases prior to Cisco IOS XE Release 3.1S. To display global statistics related to WCCP in Cisco ASR 1000, use the **show platform software wccp** command. As of Cisco IOS XE Release 3.1S, the **show ip wccp** command displays redirected WCCP packets.

Use the following commands in privileged EXEC mode to verify and monitor the configuration settings for WCCP.

SUMMARY STEPS

1. **enable**
2. **debug ip wccp** {**default** | **vrf** *vrf-name* {**events** | **packets** [**control**]} | **events** | **packets** [**bypass** | **control** | **redirect**] | **platform** | **subblocks**}
3. **debug platform hardware qfp active feature wccp** {{**client** | **lib-client** {**all** | **error** | **info** | **trace** | **warning**}} | **datapath all**}
4. **debug platform software wccp** {**configuration** | **counters** | **detail** | **messages**}

5. **show platform software wccp** [*service-number* **counters** | [*slot* [*service-number* [**access-list**] | **cache-info** | **interface** | **statistics** | **web-cache** [**access-list**]] | [**vrf** *vrf-identifier* {*service-number* [**access-list**] | **web-cache** [**access-list**]}]] | **interface counters** | **statistics | [vrf** *vrf-identifier* {*service-number* **counters** | **web-cache counters**}] | **web-cache counters**]
6. **show platform hardware qfp active feature wccp** [**vrf** *vrf-id*] **service id** *service-id*
7. **show ip wccp global** [**counters**]
8. **show ip interface**
9. **more system:running-config**
10. **configure terminal**
11. **platform trace runtime slot** *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*}

DETAILED STEPS

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

Step 2	**debug ip wccp** {**default** | **vrf** *vrf-name* {**events** | **packets** [**control**]} | **events** | **packets** [**bypass** | **control** | **redirect**] | **platform** | **subblocks**}
	Example:
	`Router# debug ip wccp events`
		Display information about WCCP services.

Step 3	**debug platform hardware qfp active feature wccp** {{**client** | **lib-client** {**all** | **error** | **info** | **trace** | **warning**}} | **datapath all**} **Example:** `Router# debug platform hardware qfp active feature wccp client all`	Enables debug logging for the WCCP client in the Cisco Quantum Flow Processor (QFP).
Step 4	**debug platform software wccp** {**configuration** | **counters** | **detail** | **messages**} **Example:** `Router# debug platform software wccp configuration`	Enables WCCP platform debug messages.

	Command or Action	Purpose
Step 5	**show platform software wccp** [*service-number* **counters** | [*slot* [*service-number* [**access-list**] | **cache-info** | **interface** | **statistics** | **web-cache** [**access-list**]] | [**vrf** *vrf-identifier* {*service-number* [**access-list**] | **web-cache** [**access-list**]}]] | **interface counters** | **statistics** | [**vrf** *vrf-identifier* {*service-number* **counters** | **web-cache counters**}] | **web-cache counters**] **Example:** `Router# show platform software wccp 61 counters`	Displays global statistics related to WCCP on the Cisco ASR 1000 Series Routers.
Step 6	**show platform hardware qfp active feature wccp** [**vrf** *vrf-id*] **service id** *service-id* **Example:** `Router# show platform hardware qfp active feature wccp [vrf vrf-id] service id 1`	Displays WCCP service group information in the active QFP.
Step 7	**show ip wccp global** [**counters**] **Example:** `Router# show ip wccp global counters`	Displays global, nonservice WCCP information.
Step 8	**show ip interface** **Example:** `Router# show ip interface`	Displays status about whether any **ip wccp redirection** commands are configured on an interface. For example, “Web Cache Redirect is enabled / disabled.”
Step 9	**more system:running-config** **Example:** `Router# more system:running-config`	(Optional) Displays contents of the currently running configuration file (equivalent to the **show running-config** command.)
Step 10	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 11	**platform trace runtime slot** *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*} **Example:** `Router(config)# platform trace runtime slot 1 bay 0 process forwarding-manager module wccp level debug`	Enables Forwarding Manager route processor and Embedded Service Processor trace messages for the WCCP process.

Troubleshooting Tips

If the counters suggest that the level of bypass traffic is high, the next step is to examine the bypass counters in the content engine and determine why the content engine is choosing to bypass the traffic. You can log in to the content engine console and use CLI to investigate further. The counters allow you to determine the percent of traffic being bypassed.

Configuration Examples for WCCP

Example: Configuring a General WCCPv2 Session

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100 password password1
Router(config)# ip wccp source-interface GigabitEthernet0/1/0
Router(config)# ip wccp check services all ! Configures a check of all WCCP services.
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/2/0
Router(config-if)# ip wccp redirect exclude in
Router(config-if)# exit
```

Example: Setting a Password for a Router and Content Engines

```
Router# configure terminal
Router(config)# ip wccp web-cache password password1
```

Example: Configuring a Web Cache Service

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router# copy running-config startup-config
```

The following example shows how to configure a session in which redirection of HTTP traffic arriving on Gigabit Ethernet interface 0/1/0 is enabled:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router# show ip interface GigabitEthernet0/1/0
.
.
.
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
```

```
.
.
.
```

Example: Running a Reverse Proxy Service

The following example assumes that you are configuring a service group using Cisco cache engines, which use dynamic service 99 to run a reverse proxy service:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface gigabitethernet0/1/0
Router(config-if)# ip wccp 99 redirect out
```

Example: Registering a Router to a Multicast Address

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface gigabitethernet0/1/0
Router(config-if)# ip wccp web cache group-listen
```

The following example shows a router configured to run a reverse proxy service, using the multicast address of 224.1.1.1. Redirection applies to packets outgoing via GigabitEthernet interface 0/1/0:

```
Router# configure terminal
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface gigabitethernet0/1/0
Router(config-if)# ip wccp 99 redirect out
```

Example: Using Access Lists

To achieve better security, you can use a standard access list to notify the router which IP addresses are valid addresses for a content engine attempting to register with the current router. The following example shows a standard access list configuration session where the access list number is 10 for some sample hosts:

```
Router(config)# access-list 10 permit host 10.1.1.1
Router(config)# access-list 10 permit host 10.1.1.2
Router(config)# access-list 10 permit host 10.1.1.3
Router(config)# ip wccp web-cache group-list 10
```

To disable caching for certain clients, servers, or client/server pairs, you can use WCCP access lists. The following example shows that any requests coming from 10.1.1.1 to 10.3.1.1 will bypass the cache, and that all other requests will be serviced normally:

```
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny tcp host 10.1.1.1 any
Router(config)# access-list 120 deny tcp any host 10.3.1.1
Router(config)# access-list 120 permit ip any any
```

The following example configures a router to redirect web-related packets received via Gigabit Ethernet interface 0/1/0, destined to any host except 209.165.200.224:

```
Router(config)# access-list 100 deny ip any host 209.165.200.224
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface GigabitEthernet0/1/0
Router(config-if)# ip wccp web-cache redirect in
```

Example: WCCP Outbound ACL Check Configuration

The following configuration example shows that the access list prevents traffic from network 10.0.0.0 leaving Gigabit Ethernet interface 0/1/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface gigabitethernet0/1/0
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
Router(config)# ip wccp web-cache redirect-list redirect-out
Router(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config)# access-list 10 permit any
```

If the outbound ACL check is disabled, the HTTP packets from network 10.0.0.0 would be redirected to a web cache. Users with that network address could retrieve web pages even though the network administrator wanted to prevent it.

Example: Verifying WCCP Settings

The following example shows how to verify your configuration changes by using the **more system:running-config** command in privileged EXEC mode. The following example shows that both the web cache service and dynamic service 99 are enabled on the router:

```
Router# more system:running-config

    Building configuration...
    Current configuration:
    !
    version 12.0
    service timestamps debug uptime
    service timestamps log uptime
    no service password-encryption
    service udp-small-servers
    service tcp-small-servers
    !
    hostname router4
    !
    enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
    enable password password1
    !
    ip subnet-zero
    ip wccp web-cache
    ip wccp 99
    ip domain-name cisco.com
    ip name-server 10.1.1.1
    ip name-server 10.1.1.2
    ip name-server 10.1.1.3
    !
    !
    !
    interface GigabitEthernet0/1/1
    ip address 10.3.1.2 255.255.255.0
    no ip directed-broadcast
    ip wccp web-cache redirect in
    ip wccp 99 redirect in
    no ip route-cache
    no ip mroute-cache
    !

    interface GigabitEthernet0/1/0
    ip address 10.4.1.1 255.255.255.0
    no ip directed-broadcast
    ip wccp 99 redirect in
    no ip route-cache
    no ip mroute-cache
    !
    interface Serial0
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    !
    interface Serial1
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    !
    ip default-gateway 10.3.1.1
    ip classless
    ip route 0.0.0.0 0.0.0.0 10.3.1.1
    no ip http server
    !
    !
    !
    line con 0
    transport input none
    line aux 0
    transport input all
    line vty 0 4
    password alaska1
    login
    !
    end
```

The following example shows how to display global statistics related to WCCP:

```
Router# show ip wccp web-cache detail

WCCP Client information:
WCCP Client ID:      10.1.1.2
Protocol Version:    2.0
State:               Usable
Redirection:         L2
Packet Return:       L2
Packets Redirected:  0
Connect Time:        00:20:34
Assignment:          MASK
Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: 0x00000000 0x00001741 0x0000  0x0000
Value SrcAddr    DstAddr   SrcPort DstPort CE-IP
----- -------    -------   ------- ------- -----
0000: 0x00000000 0x00000000 0x0000 0x0000 0x3C010102 (10.1.1.2)
0001: 0x00000000 0x00000001 0x0000 0x0000 0x3C010102 (10.1.1.2)
```

```
0002: 0x00000000 0x00000040 0x0000 0x0000 0x3C010102 (10.1.1.2)
0003: 0x00000000 0x00000041 0x0000 0x0000 0x3C010102 (10.1.1.2)
0004: 0x00000000 0x00000100 0x0000 0x0000 0x3C010102 (10.1.1.2)
0005: 0x00000000 0x00000101 0x0000 0x0000 0x3C010102 (10.1.1.2)
0006: 0x00000000 0x00000140 0x0000 0x0000 0x3C010102 (10.1.1.2)
0007: 0x00000000 0x00000141 0x0000 0x0000 0x3C010102 (60.1.1.2)
0008: 0x00000000 0x00000200 0x0000 0x0000 0x3C010102 (60.1.1.2)
0009: 0x00000000 0x00000201 0x0000 0x0000 0x3C010102 (60.1.1.2)
0010: 0x00000000 0x00000240 0x0000 0x0000 0x3C010102 (60.1.1.2)
0011: 0x00000000 0x00000241 0x0000 0x0000 0x3C010102 (60.1.1.2)
0012: 0x00000000 0x00000300 0x0000 0x0000 0x3C010102 (60.1.1.2)
0013: 0x00000000 0x00000301 0x0000 0x0000 0x3C010102 (60.1.1.2)
```

For more information about the **show ip wccp web-cache** command, see the *Cisco IOS IP Application Services Command Reference*.

Additional References

Related Documents

Related Topic	Document Title
Cisco ACNS software configuration information	• *Cisco ACNS Software Caching Configuration Guide*, Release 4.2 • http://www.cisco.com/en/US/products/sw/conntsw/ps491/products_installation_and_configuration_guides_list.html • Cisco ACNS Software listing page on Cisco.com
Deploying and Troubleshooting WCCP on Cisco ASR 1000 Series Routers	*Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers*
IP Access List overview, configuration tasks, and commands	• *Cisco IOS XE Security Configuration Guide: Securing the Data Plane* • *Cisco IOS Security Command Reference*
IP addressing and services commands and configuration tasks	• *Cisco IOS XE IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*
WCCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*

Standards

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

MIBs

MIB	MIBs Link
None	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

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	

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 WCCP

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for WCCP

Feature Name	Releases	Feature Information
WCCP Bypass Counters	Cisco IOS XE Release 2.2	The WCCP Bypass Counters feature allows you to display a count of packets that have been bypassed by a web cache and returned to the originating router to be forwarded normally. The following sections provide information about this feature: • WCCP Bypass Packets, page 8 • Example: Verifying WCCP Settings, page 24 The following commands were modified or introduced by this feature: **show ip wccp**, **show platform software wccp**.
WCCP: Check Services All	Cisco IOS XE Release 3.1S	The WCCP: Check Services All feature enables you to configure WCCP to search all service groups and redirect ACLs in priority order for a match. The following sections provide information about this feature: • WCCP: Check Services All, page 10 • Configuring Closed Services, page 13 • Example: Configuring a General WCCPv2 Session, page 22 The following command was modified by this feature: **ip wccp check services all**.

Table 1 Feature Information for WCCP (continued)

Feature Name	Releases	Feature Information
WCCP Closed Services	Cisco IOS XE Release 3.1S	The WCCP Closed Services feature permits WCCP services to be configured so that WCCP always intercepts traffic for such services but, if no WCCP client (such as a content engine) has registered to receive this traffic, packets are discarded. This behavior supports AONS (Application-Oriented Network Services) applications, which require traffic to be transparently intercepted using WCCP but do not want the packets to be forwarded to their destination if the WCCP client is unavailable to perform its processing. (This behavior is contrary to the traditional use of WCCP to assist caches where the absence of a cache does not change the behavior as observed by the user.) The following sections provide information about this feature: • WCCP Closed Services and Open Services, page 8 • Configuring Closed Services, page 13 • Example: Configuring a General WCCPv2 Session, page 22 The **ip wccp** command was modified by this feature.
WCCP—Configurable Router ID	Cisco IOS XE Release 3.1S	The WCCP—Configurable Router ID feature permits the router ID which WCCP uses to be configurable, rather than relying on the router's selection mechanism. The following sections provide information about this feature: • WCCP Configurable Router ID, page 11 • Configuring WCCP, page 11 • Example: Configuring a General WCCPv2 Session, page 22 The **ip wccp source-interface** commands was introduced by this feature.
WCCP Egress Redirection Support	Cisco IOS XE Release 3.1S	The WCCP Egress Redirection Support feature enables WCCP based redirection applied to the outbound traffic on the outbound interface. The following section provides information about this feature: • Configuring WCCP, page 11 The **ip wccp redirect** command was modified by this feature.

Table 1 Feature Information for WCCP (continued)

Feature Name	Releases	Feature Information
WCCP Exclude Interface	Cisco IOS XE Release 3.1S	The WCCP Exclude Interface feature enables you to configure an interface to exclude packets received on an interface from being checked for redirection by configuring the **ip wccp redirect exclude in** command in interface configuration mode. The following sections provide information about this feature: • Configuring WCCP, page 11 • Example: Configuring a General WCCPv2 Session, page 22 The following command was introduced by this feature: **ip wccp redirect exclude in**
WCCP Group List	Cisco IOS XE Release 3.1S	The WCCP Group List feature enables you to configure the IP addresses of cache engines from which a router accepts packets. Configuring a group list is used to validate the protocol packets received from the cache engine. Packets matching the address in a configured group-list are processed, others are discarded. The following sections provide information about this feature: • Using Access Lists for a WCCP Service Group, page 16 • Example: Using Access Lists, page 23 The **ip wccp** command was introduced or modified by this feature.
WCCP—Group Listen and Multicast Service Support	Cisco IOS XE Release 3.1S	The WCCP—Group Listen and Multicast Service Support feature adds the ability to configure a multicast address per service group for sending and receiving protocol messages. In the multicast address method, the cache engine sends a single-address notification that provides coverage for all routers in the service group. The following sections provide information about this feature: • WCCPv2 Configuration, page 5 • Registering a Router to a Multicast Address, page 15 • Example: Registering a Router to a Multicast Address, page 23 • The **ip wccp group-listen** command was modified by this feature.

Table 1 Feature Information for WCCP (continued)

Feature Name	Releases	Feature Information
WCCP Increased Services	Cisco IOS XE Release 3.1S	The WCCP Increased Services feature increases the number of services supported by WCCP to a maximum of 256 across all VRFs. The following sections provide information about this feature: • WCCP Service Groups, page 9 • Configuring Closed Services, page 13 • Configuring WCCP, page 11 • Example: Verifying WCCP Settings, page 24 The following commands were modified by this feature: **ip wccp**, **ip wccp check services all**, **ip wccp outbound-acl-check, show ip wccp**.
WCCP Layer 2 Redirection / Forwarding	Cisco IOS XE Release 2.2	The WCCP Layer 2 Redirection/Forwarding feature allows directly connected Cisco content engines to use Layer 2 redirection, which is more efficient than Layer 3 redirection via GRE encapsulation. You can configure a directly connected Cache Engine to negotiate use of the WCCP Layer 2 Redirection/Forwarding feature. The WCCP Layer 2 Redirection/Forwarding feature requires no configuration on the router or switch. The following sections provide information about this feature: • Restrictions for WCCP, page 2 • Layer 2 Forwarding, Redirection and Return, page 4 • Support for Services Other Than HTTP, page 7 There are no new or modified commands associated with this feature.
WCCP L2 Return	Cisco IOS XE Release 2.2	The WCCP L2 Return feature allows content engines to return packets to WCCP routers directly connected at Layer 2 by swapping the source and destination MAC addresses rather than tunneling packets back to the router inside a Layer 3 GRE tunnel. The following sections provide information about this feature: • Layer 2 Forwarding, Redirection and Return, page 4 There are no new or modified commands associated with this feature.

Table 1 Feature Information for WCCP (continued)

Feature Name	Releases	Feature Information
WCCP Mask Assignment	Cisco IOS XE Release 2.2	The WCCP Mask Assignment feature introduces support for ACNS/WAAS devices using mask assignment as a cache engine assignment method. The following section provides information about this feature: • WCCP Mask Assignment, page 5 There are no new or modified commands associated with this feature.
WCCP Outbound ACL Check	Cisco IOS XE Release 3.1S	The WCCP Outbound ACL Check feature enables you to ensure that traffic redirected by WCCP at an input interface is subjected to the outbound ACL checks that may be configured on the output interface prior to redirection. The following sections provide information about this feature: • WCCP Outbound ACL Check, page 8 • Enabling the WCCP Outbound ACL Check, page 18 • Example: Verifying WCCP Settings, page 24 The following commands were introduced or modified by this feature: **ip wccp**, **ip wccp check acl outbound**.
WCCP Redirection on Inbound Interfaces	Cisco IOS XE Release 2.2	The WCCP Redirection on Inbound Interfaces feature enables interfaces to be configured for input redirection for a particular WCCP service. When this feature is enabled on an interface, all packets arriving at that interface are compared against the specified WCCP service. If the packets match, they will be redirected. The following sections provide information about this feature: • Configuring WCCP, page 11 • Example: Configuring a Web Cache Service, page 22 The following commands were introduced or modified by this feature: **ip wccp redirect**.

Table 1 Feature Information for WCCP (continued)

Feature Name	Releases	Feature Information
WCCP Version 2	Cisco IOS XE Release 2.2	The WCCP Version 2 feature provides several enhancements and features to the WCCP protocol, including: • The ability of multiple routers to service a content engine cluster. • Redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic. • Optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard. • A check on packets that determines which requests have been returned from the content engine unserviced. • Load adjustments for individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients. The following sections provide information about this feature: • Restrictions for WCCP, page 2 • WCCPv2 Configuration, page 5 • Support for Services Other Than HTTP, page 7 • Example: Configuring a General WCCPv2 Session, page 22 The following commands were introduced or modified by this feature: **clear ip wccp**, **ip wccp**, **ip wccp group-listen**, **ip wccp redirect**, **ip wccp redirect exclude in**, **ip wccp version**, **show ip wccp**.
WCCP VRF Support	Cisco IOS XE Release 3.1S	The WCCP VRF Support feature provides enhancements to the existing WCCPv2 protocol, which supports VRF awareness. The following sections provide information about this feature: • WCCP VRF Support, page 7 • Configuring WCCP, page 11 The following commands were introduced or modified by this feature: **clear ip wccp**, **debug ip wccp**, **ip wccp**, **ip wccp group-listen**, **ip wccp redirect**, **show ip wccp**.

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.

Virtual Router Redundancy Service

First Published: February 26, 2010
Last Updated: February 26, 2010

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several 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 FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for VRRS" section on page 16.

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

Contents

Restrictions for VRRS

- VRRS plug-ins must be configured on subinterfaces that are not configured with an FHRP, but which share a physical interface with an FHRP it is following.
- VRRPv2 is configurable only on Gigabit Ethernet interfaces.

Information About VRRS

VRRS Overview

VRRS improves the scalability of FHRP. VRRS provides a stateless redundancy service to applications (VRRS clients) by monitoring VRRP. VRRS provides a database of the current VRRP state and operates without maintaining sessions or keeping track of previous states of the clients and servers with which it communicates. VRRP acts as a VRRS server. VRRS clients are other Cisco IOS processes or applications that use VRRP to provide or withhold a service or resource dependent upon the state of the group.

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 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.

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 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 (master, backup, or nonoperational INIT). The VRRP state is then passed on to clients or acted on by a plug-in. A VRRP group should be configured with a name to activate VRRS. 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. Clients act on the VRRP server state. When a VRRP group changes state, VRRS clients act by altering their behavior (perfoming tasks such as shutting down interfaces or appending accounting logs) depending on the state received from VRRS.

The following can be VRRS clients:

- PPP over Ethernet (PPPoE) subinterfaces
- Access Node Control Protocol (ANCP) subinterfaces
- VRRS Interface-state plug-in
- VRRS MAC-Address plug-in
- VRRS Accounting plug-in

VRRS plug-ins extend the failover of VRRP without the need for configuring VRRP groups on all subinterfaces. Configuring a VRRS plug-in on subinterfaces is a substitute for having to configure multiple VRRP groups on many subinterfaces. Plug-ins provide a light-weight version of VRRP and scale better than a fully configured VRRP group. The state of the plug-ins follows the VRRP server state. Client plug-ins are configured on other subinterfaces that share the same physical interface as VRRP.

VRRS MAC-Address Plug-in

The VRRS MAC-Address plug-in provides a mechanism for controlling a virtual MAC address associated with the primary interface IP address. If the VRRS MAC-Address plug-in is configured on an interface, and a VRRP group shares a name association with the plug-in, then a VRRS active state associates a virtual MAC address with the configured primary IP address.

The VRRS MAC-Address plug-in is only interested in the VRRS active state, which is interpreted as up. All other states are interpreted as down. When the state is up and the additional interface criteria listed below have been met, then the VRRS MAC-Address plug-in provides the following services:

- Overwrites the interface IP address ARP table with a virtual MAC address provided by VRRS
- Inserts the virtual MAC address provided by VRRS into the MAC address filter of the interface
- Controls the ARP reply mechanism by substituting a VRRS-provided virtual MAC address
- Broadcasts unsolicited ARP messages that include the VRRS virtual MAC address

When VRRS is in a nonactive state, the virtual MAC address is unassociated from the primary IP address.

When you use the VRRS MAC-Address plug-in, the VRRS Interface-State plug-in must also be used in order to prevent address conflicts with other redundant members.

Additional interface criteria:

- Interfaces must be configured with an interface IP address.
- Interfaces must be in the line-protocol up state.
- Other FHRP protocols cannot be configured on the interface; these include HSRP, VRRP, and GLBP.

The VRRS MAC-Address plug-in is associated with a VRRS group name by configuring the **vrrs follow** *name* command.

VRRS Interface-State Plug-in

The VRRS Interface-State plug-in provides a mechanism for controlling the line-protocol state of a subinterface based on the state of VRRP. The VRRS Interface-State plug-in is an extension of the VRRS, and is directly controlled by the push events associated with the VRRS. If the plug-in is configured on an interface, and a VRRP group shares a name association with the VRRS plug-in, then a VRRS active state allows the lin- protocol state of the interface to be up. A VRRS nonactive state will cause the line protocol of the interface to be down.

Note When first configured, the interface line protocol may immediately change to the down state until the VRRS state is confirmed as up.

The VRRS Interface-State plug-in is associated with a VRRS group name by configuring the **vrrs follow** *name* command.

The Interface-State plug-in restricts the operation of the **no shutdown** command. When an interface is line-protocol down, the interface state will not go up.

VRRS Accounting Plug-in

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the **vrrp name** command in interface configuration mode.

The VRRS Accounting plug-in sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, VRRS
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Time
- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop messages for sessions that are part of that VRRS.

The VRRS accounting type is implemented by AAA to support VRRS accounting.

How to Configure VRRS

- Configuring a VRRS Server, page 5 (required)
- Configuring the Clients That Use VRRS, page 6 (optional)
- Configuring VRRS Accounting, page 7 (optional)
- Monitoring and Maintaining VRRS, page 9 (optional)

Configuring a VRRS Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
5. **vrrp** *group-number* **name** [*vrrp-group-name*]
6. **vrrp** *group* **ip** *ip-address* [**secondary**]
7. **vrrp delay** {**minimum** *seconds* [**reload** *seconds*] | **reload** *seconds*}

DETAILED STEPS

	Command or Action	Purpose

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 gigabitethernet0/0/0`
		Configures an interface type and enters interface configuration mode.

Step 4	**`ip address`** *`ip-address mask`* `[`**`secondary`**
	`[`**`vrf`** *`vrf-name`*`]]`
	Example:
	`Router(config-if)# ip address 10.0.0.1`
	`255.255.255.0`
		Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 5	**vrrp** *group-number* **name** [*vrrp-group-name*] **Example:** `Router(config-if)# vrrp 1 name name1`	Links a VRRS client to a VRRP group.
Step 6	**vrrp** *group* **ip** *ip-address* [**secondary**] **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	**vrrp delay** {**minimum** *seconds* [**reload** *seconds*] | **reload** *seconds*}
	Example:
	`Router(config-if)# vrrp delay minimum 30 reload 60`
		Configures the delay period before the initialization of all VRRP groups on an interface.
		The recommended **minimum** *seconds* value is 30 seconds, and the recommended **reload** *seconds* value is 60 seconds.

Configuring the Clients That Use VRRS

Perform this task to configure the clients, including VRRS plug-ins, that use VRRS. This task is configured on multiple subinterfaces.

1. **enable**
2. **configure terminal**
3. **interface** *type number.subinterface*
4. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
5. **vrrs follow** *name*
6. **vrrs interface-state**
7. **vrrs mac-address** [**arp** [**interval** *seconds*] [**duration** *seconds*]]
8. Repeat Step 3 through Step 7 to configure additional subinterfaces.

DETAILED STEPS

	Command or Action	Purpose
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.

	Command or Action	Purpose

Step 3	**`interface`** *`type number.subinterface`*
	Example:
	`Router(config)# interface gigabitethernet0/0/0.1`
		Configures a subinterface type and enters subinterface configuration mode.

Step 4	**`ip address`** *`ip-address mask`* `[`**`secondary`** `[`**`vrf`** *`vrf-name`*`]]`
	Example:
	`Router(config-subif)# ip address 10.0.0.1 255.255.255.0`
		Sets a primary or secondary IP address for an interface.
		This interface should be a subinterface.

Step 5	**`vrrs follow`** *`name`*
	Example:
	`Router(config-subif)# vrrs follow name1`
		Configures a name association between VRRS plug-ins and the VRRS server.

Step 6	**`vrrs interface-state`**
	Example:
	`Router(config-subif)# vrrs interface-state`
		(Optional) Configures the VRRP shutdown plug-in on an interface.

Step 7	**`vrrs mac-address`** `[`**`arp`** `[`**`interval`** *`seconds`*`] [`**`duration`** *`seconds`*`]]`
	Example:
	`Router(config-subif)# vrrs mac-address`
		(Optional) Configures the VRRS MAC-Address plug-in on an interface.

Step 8	Repeat Steps 3 through 7 to configure additional subinterfaces.	

Configuring VRRS Accounting

Perform this task to configure VRRS to send AAA accounting messages to the AAA server when there is a state-change in VRRS from active to standby or from standby to active.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting vrrs** {**default** | *list-name* **start-stop** [*method1* [*method2...*]]
4. **aaa attribute list** *list-name*
5. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*] [**mandatory**] [**tag** *tag-value*]
6. **exit**
7. **vrrs** *vrrs-group-name* (Optional)
8. **accounting delay** *delay* (Optional)
9. **accounting method** {**default** | *accounting-method-list*} (Optional)
10. **attribute list** *list-name* (Optional)

DETAILED STEPS

	Command or Action	Purpose
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	**aaa accounting vrrs** {**default** | *list-name* **start-stop** [*method1* [*method2...*]] **Example:** `Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
Step 4	**aaa attribute list** *list-name* **Example:** `Router(config)# aaa attribute list vrrp-1-attr`	Defines a AAA attribute list locally on a router.
Step 5	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*][**mandatory**][**tag** *tag-value*] **Example:** `Router(config-attr-list)# attribute type account-delay “10”`	Defines an attribute type that is to be added to an attribute list locally on a router.
Step 6	**exit** **Example:** `Router(config-attr-list)# exit`	Exits attribute list configuration mode and returns to global configuration mode.
Step 7	**vrrs** *vrrs-group-name* **Example:** `Router(config)# vrrs vrrp-name-1`	(Optional) Specifies a distinct AAA accounting method list to use, a nonzero delay time for accounting-off messages, and additional attributes other than the default for a VRRP group.
Step 8	**accounting delay** *delay* **Example:** `Router(config-vrrs)# accounting delay 10`	(Optional) Specifies a delay time for sending accounting-off messages for VRRS.

	Command or Action	Purpose

Step 9	**accounting method** {**default** | *accounting-method-list*}
	Example:
	`Router(config-vrrs)# accounting method METHOD1`
		(Optional) Enables VRRS accounting for a VRRP group.

Step 10	**attribute list** *list-name* **Example:** `Router(config-vrrs)# attribute list vrrp-1-attr`	(Optional) Specifies additional attributes to include in VRRS accounting-on and accounting-off messages.

Monitoring and Maintaining VRRS

SUMMARY STEPS

1. **debug vrrp vrrs**
2. **debug vrrs accounting** {**all** | **errors** | **events**}
3. **debug vrrs infra** {**all** | **client** | **events** | **server**}
4. **debug vrrs plugin** {**all** | **arp-packet** | **client** | **database** | **if-state** | **mac** | **process** | **sublock** | **test**}
5. **show vrrs clients**
6. **show vrrs group** [*group-name*]
7. **show vrrs plugin database**
8. **show vrrs summary**

DETAILED STEPS

Step 1 **debug vrrp vrrs**

This command enables VRRP debugging statements for VRRS interactions.

```
Router# debug vrrp vrrs

VRRP VRRS debugging is on
*Feb  5 09:29:47.005: VRRP: Registered VRRS group "name1"
*Feb  5 09:29:53.237: VRRP: Updated info for VRRS group name1
*Feb  5 09:30:14.153: VRRP: Unregistered VRRS group "name1"
*Feb  5 09:30:14.153: VRRP: Registered VRRS group "name2"
*Feb  5 09:30:22.689: VRRP: Unregistered VRRS group "name2"
```

Step 2 **debug vrrs accounting** {**all** | **errors** |**events**}

This command enables debug messages for VRRS accounting.

```
Router# debug vrrs accounting

00:16:13: VRRS/ACCT/EV: entry create for abc(0x4E8C1F0)
00:16:13: VRRS/ACCT/EV: abc(0x4E8C1F0 12000006) client add ok2(No group)
```

Step 3 **debug vrrs infra** {**all** | **client** | **events** | **server**}

This command enables VRRS infrastructure debug messages.

```
Router# debug vrrs infra

*Sep 9 16:09:53.848: VRRS: Client 21 is not registered
*Sep 9 16:09:53.848: VRRS: Client 21 unregister failed
*Sep 9 16:09:53.848: VRRS: Client VRRS TEST CLIENT registered, id 21
*Sep 9 16:09:53.848: VRRS: Client 21 add, group VRRP-TEST-1 does not exist, allocating...
*Sep 9 16:09:53.848: VRRS: Client 21 add to VRRP-TEST-1. Vrrs handle F7000001, client
handle FE720
*Sep 9 16:09:53.848: VRRS: Server VRRP add, group VRRP-TEST-1, state INIT, vrrs handle
F7000001
```

Step 4 **debug vrrs plugin** {**all** | **arp-packet** | **client** | **database** | **if-state** | **mac** | **process** | **sublock** | **test**}

This command enables VRRS plug-in debug messages.

```
Router# debug vrrs plugin

Feb 17 19:15:38.052: VRRS-P(mac): GigEth0/0/0.1 Add 0000.12ad.0001 to MAC filter, using
(afilter_add)
Feb 17 19:15:38.053: VRRS-P(mac): Active count increase to (2) for MAC : 0000.12ad.0001
```

Step 5 **show vrrs clients**

This command displays a list of VRRS clients.

```
Router# show vrrs clients

ID  Priority  All-groups  Name
------------------------------
1   High      No          VRRS-Plugins
2   Low       Yes         VRRS-Accounting
3   Normal    No          PPPOE-VRRS-CLIENT
```

Step 6 **show vrrs group** [*group-name*]

This command displays information about VRRS groups.

```
Router# show vrrs group DT-CLUSTER-3

DT-CLUSTER-3
Server Not configured, state INIT, old state INIT, reason Protocol
  Address family IPv4, Virtual address 0.0.0.0, Virtual mac 0000.0000.0000
  Active interface address 0.0.0.0, standby interface address 0.0.0.0
Client 5 VRRS TEST CLIENT, priority Low
```

Step 7 **show vrrs plugin database**

This command displays details about the internal VRRS plug-in database.

```
Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Disabled
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                 gige0/0/0.2
                 gige0/0/0.3
```

Step 8 **show vrrs summary**

This command displays a summary of all VRRS groups.

```
Router# show vrrs summary

Group                                             Server State Virtual-address
------------------------------------------------------------------------------
DT-CLUSTER-3                                      UNKNOW INIT   0.0.0.0
DT-CLUSTER-2                                      VRRP   BACKUP 11.1.1.1
DT-CLUSTER-1                                      VRRP   ACTIVE 1.1.1.1
```

Configuration Examples for VRRS

- Example: Configuring a VRRS Server, page 11
- Example: Configuring the Clients that use VRRS, page 11
- Example: Configuring VRRS Accounting, page 11
- Example: Confirming Operation of the VRRS Interface-State Plug-in, page 12
- Example: Confirming Operation of the VRRS MAC-Address plug-in, page 13

Example: Configuring a VRRS Server

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# vrrp 1 name name1
Router(config-if)# vrrp 1 ip 10.0.1.20
Router(config-if)# vrrp delay minimum 30 reload 60
```

Example: Configuring the Clients that use VRRS

The following example shows how to configure the clients, including VRRS plug-ins, that use VRRS.

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0.1
Router(config-subif)# ip address 10.0.0.1 255.255.255.0
Router(config-subif)# vrrs follow name1
Router(config-subif)# vrrs interface-state
Router(config-subif)# vrrs mac-address
```

Example: Configuring VRRS Accounting

The following example shows how to configure VRRS to send AAA accounting messages to the AAA server when there is a state change in VRRS from active to standby or from standby to active.

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay “10”
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-name-1
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# accounting method METHOD1
Router(config-vrrs)# attribute list vrrp-1-attr
```

Example: Confirming Operation of the VRRS Interface-State Plug-in

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# no ip address
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.1
Router(config-if)# encapsulation dot1Q 1 native
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# vrrp 1 name VRRS_NAME_1
Router(config-if)# vrrp 1 ip 172.16.1.254
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.2
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip address 192.168.42.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.3
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip address 192.168.43.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.4
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip address 192.168.44.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_2
Router(config-if)# vrrs interface-state
Router(config-if)# exit
Router# show ip interface brief

Interface                     IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0            unassigned      YES NVRAM  up                    up
GigabitEthernet0/0/0.1          172.24.1.1      YES manual up                    up
GigabitEthernet0/0/0.2          192.168.42.1    YES manual up                    up
GigabitEthernet0/0/0.3          192.168.43.1    YES manual up                    up
GigabitEthernet0/0/0.4          192.168.44.1    YES manual up                    down !
"interface-state" DOWN due to no VRRS server

Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Active
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                 GigE0/0/0.2
                 GigE0/0/0.3
------------------------------------------------
Name = VRRS_NAME_2
Server connection = Disconnected
State = Disabled
MAC addr = 0000.0000.0000
Test Control = False
Client Handle = 603979779
Interface list =
                 GigE0/0/0.4
```

Example: Confirming Operation of the VRRS MAC-Address plug-in

```
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# no ip address
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.1
Router(config-if)# encapsulation dot1Q 1 native
Router(config-if)# ip address 172.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 name VRRS_NAME_1
Router(config-if)# vrrp 1 ip 172.24.1.254
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.2
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip address 192.168.42.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.3
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip address 192.168.43.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_1
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/0/0.4
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip address 192.168.44.1 255.255.255.0
Router(config-if)# vrrs follow VRRS_NAME_2
Router(config-if)# vrrs mac-address arp interval 5 duration 360
Router(config-if)# exit
Router# show ip arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.24.1.1              -   aabb.cc00.fb00  ARPA   GigabitEthernet0/0/0.1
Internet  172.24.1.254            -   0000.5e00.0101  ARPA   GigabitEthernet0/0/0.1
Internet  192.168.42.1            -   0000.5e00.0101  ARPA   GigabitEthernet0/0/0.2 !
"mac-address" enabled interfaces using VRRP MAC via VRRS
Internet  192.168.43.1            -   0000.5e00.0101  ARPA GigabitEthernet0/0/0.3 !
"mac-address" enabled interfaces using VRRP MAC via VRRS
Internet  192.168.44.1            -   aabb.cc00.fb00  ARPA GigabitEthernet0/0/0.4 !
"mac-address" disabled interface using BIA

Router# debug arp

ARP packet debugging is on

*Sep 10 20:02:14.971: IP ARP: sent rep src 192.168.42.1 0000.5e00.0101,
                 dst 192.168.42.1 ffff.ffff.ffff Ethernet0/0.2
*Sep 10 20:02:14.971: IP ARP: sent rep src 192.168.43.1 0000.5e00.0101,
                 dst 192.168.43.1 ffff.ffff.ffff Ethernet0/0.3

*Sep 10 20:02:19.991: IP ARP: sent rep src 192.168.42.1 0000.5e00.0101,
                 dst 192.168.42.1 ffff.ffff.ffff Ethernet0/0.2
*Sep 10 20:02:19.991: IP ARP: sent rep src 192.168.43.1 0000.5e00.0101,
                 dst 192.168.43.1 ffff.ffff.ffff Ethernet0/0.3

Router# show controller gigabitethernet0/0/0
Interface GigabitEthernet0/0/0
Hardware is AMD Unknown
ADDR: 1EC55D8, FASTSEND: FC286088, MCI_INDEX: 0
DIST ROUTE ENABLED: 0
```

```
Route Cache Flag: 11
 amdp2_instance=0x1EC6798, registers=0x1EC5580, ib=0x1EC6D98
 rx ring entries=32, tx ring entries=64
 rxring=0x1EC6DE8, rxr shadow=0x1EC7020, rx_head=0, rx_tail=0
 txring=0x1EC70D8, txr shadow=0x1EC7510, tx_head=0, tx_tail=57, tx_count=57
 running=0, port id=0x5DCF8
 Software MAC address filter(hash:length/addr/mask/hits):
  0x00:  0  ffff.ffff.ffff  0000.0000.0000         0
  0x4C:  0  0100.5e00.0012  0000.0000.0000         0
  0x5F:  0  0000.5e00.0101  0000.0000.0000         0 ! Virtual MAC, note for this
interface, it may be VRRP that added this MAC.
  0xC0:  0  0100.0ccc.cccc  0000.0000.0000         0
  0xC0:  1  0180.c200.0002  0000.0000.0000         0
  0xC5:  0  0180.c200.0007  0000.0000.0000         0
  0xCC:  0  aabb.cc00.fb00  0000.0000.0000         0

Router# show vrrs plugin database

VRRS Plugin Database
------------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Active
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                 GigE0/0/0.2
                 GigE0/0/0.3
------------------------------------------------
Name = VRRS_NAME_2
Server connection = Diconnected
State = Disabled
MAC addr = 0000.0000.0000
Test Control = False
Client Handle = 603979779
Interface list =
                 GigE0/0/0.4
```

Where to Go Next

If you want to configure additional VRRP features, see the "Configuring VRRP" document.

Additional References

Related Documents

Related Topic	Document Title
ANCP	*Access Node Control Protocol*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
VRRP	*Configuring VRRP*
VRRP and VRRS commands	*Cisco IOS IP Application Services Command Reference*

Standards

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

MIBs

MIB	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

RFC	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 VRRS

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for VRRS

Feature Name	Releases	Feature Information
Virtual Router Redundancy Service (VRRS)	Cisco IOS XE Release 2.6	Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP), and a registered client. The following commands were introduced or modified: **aaa accounting vrrs**, **accounting delay** (VRRS), **accounting method** (VRRS), **attribute list** (VRRS), **debug vrrp all**, **debug vrrp vrrs**, **debug vrrs accounting**, **debug vrrs infra**, **debug vrrs plugin**, **show vrrp**, **show vrrs clients**, **show vrrs clients**, **show vrrs group**, **show vrrs plugin database**, **show vrrs summary**, **vrrp delay**, **vrrs follow**, **vrrp ip**, **vrrs mac-address**, **vrrp name**, **vrrs**.

Glossary

AAA—authentication, authorization, and accounting.

RADIUS—Remote Authentication Dial-In User Service.

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.

VRRP—Virtual Router Redundancy Protocol. 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.

VSA—vendor-specific attribute. An attribute that has been implemented by a particular vendor.

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.