



CHAPTER 40

Configuring HSRP, VRRP, and GLBP

This chapter describes how to use Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and the Gateway Load Balancing Protocol (GLBP) on the Catalyst 3750 Metro switch. HSRP provides routing redundancy for routing IP traffic without being dependent on the availability of any single router. GLBP provides routing redundancy similar to HSRP and also provides load balancing over multiple routers by using a single virtual IP address and multiple virtual MAC addresses. Cisco IOS Release 12.2(58)SE adds support for GLBP and VRRP for IPv4 and IPv6.

For complete syntax and usage information for the commands used in this chapter and more information on configuring HSRP and GLBP, see these documents:

- Switch command reference for this release
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2:*
http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
- *Hot Standby Router Protocol Version 2* feature module:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthsrvp2.html
- *Configuring GLBP* feature module:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glbp.html
- *Configuring VRRP* feature module:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp.html
- *Configuring First Hop Redundancy Protocols in IPv6*
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-fhrp.html>

This chapter consists of these sections:

- [Understanding HSRP, page 40-1](#)
- [Configuring HSRP, page 40-4](#)
- [Displaying HSRP Configurations, page 40-10](#)
- [Configuring VRRP, page 40-11](#)
- [Configuring GLBP, page 40-11](#)

Understanding HSRP

HSRP is the Cisco standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a

LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

**Note**

Routers in an HSRP group can be any router interface that supports HSRP, including Catalyst 3750 Metro switch routed ports and switch virtual interfaces (SVIs).

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

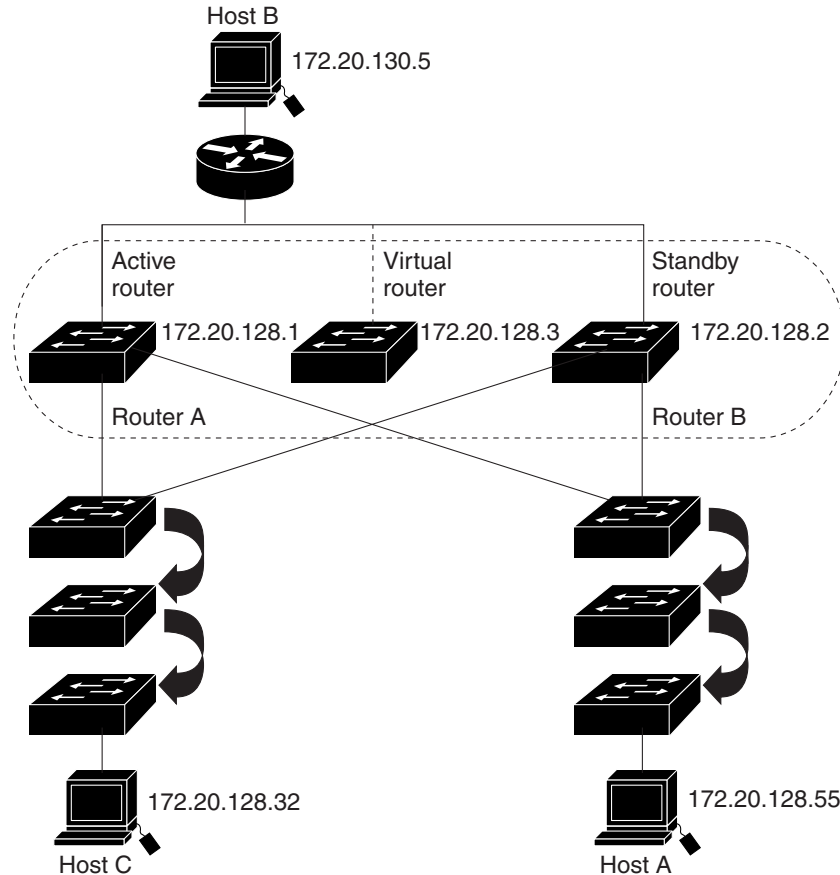
HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group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

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

You can configure multiple Hot Standby groups among switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

Figure 40-1 shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C's segment that need to communicate with users on Host B's segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.

Figure 40-1 Typical HSRP Configuration



HSRP Versions

The switch supports these HSRP versions:

- HSRPv1—Version 1 of the HSRP, the default version of HSRP. It has these features:
 - The HSRP group number can be from 0 to 255.
 - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.
- HSRPv2—Version 2 of the HSRP has these features:
 - To match the HSRP group number to the VLAN ID of a subinterface, HSRPv2 can use a group number from 0 to 4095 and a MAC address from 0000.0C9F.F000 to 0000.0C9F.FFFF.
 - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.
 - HSRPv2 has a different packet format than HSRPv1.

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

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

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

HSRPv2 and HSRPv1 are mutually exclusive. HSRPv2 is not interoperable with HSRPv1 on an interface and the reverse.

Configuring HSRP

- [Default HSRP Configuration, page 40-4](#)
- [HSRP Configuration Guidelines, page 40-4](#)
- [Enabling HSRP, page 40-5](#)
- [Configuring HSRP Group Attributes, page 40-6](#)
- [Enabling HSRP Support for ICMP Redirect Messages, page 40-10](#)

Default HSRP Configuration

Table 40-1 shows the default HSRP configuration.

Table 40-1 Default HSRP Configuration

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

HSRP Configuration Guidelines

- HSRP can be configured on a maximum of 32 VLAN or routing interfaces.
- In the following procedures, the specified interface must be one of these Layer 3 interfaces:
 - Routed port: a physical port configured as a Layer 3 port by entering the **no switchport** interface configuration command.
 - SVI: a VLAN interface created by using the **interface vlan** *vlan_id* global configuration command and by default a Layer 3 interface.

- Etherchannel port channel in Layer 3 mode: a port-channel logical interface created by using the **interface port-channel** *port-channel-number* global configuration command and binding the Ethernet interface into the channel group. For more information, see the “[Configuring Layer 3 EtherChannels](#)” section on page 35-13.
- All Layer 3 interfaces must have IP addresses assigned to them. See the “[Configuring Layer 3 Interfaces](#)” section on page 9-17.
- HSRPv2 and HSRPv1 can be configured on the same switch if HSRPv2 is configured on different interfaces than those on which HSRPv1 is configured.
- The version of an HSRP group can be changed from HSRPv2 to HSRPv1 only if the group number is less than 256.
- If you change the HSRP version on an interface, each HSRP group resets because it now has a new virtual MAC address.

Enabling HSRP

The **standby ip** interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.

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



Note

When multi-VRF CE is configured, you cannot assign the same HSRP standby address to two different VPNs.

Beginning in privileged EXEC mode, follow these steps to create or enable HSRP on a Layer 3 interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.
Step 3	standby version {1 2}	(Optional) Configure the HSRP version on the interface. <ul style="list-style-type: none"> • 1— Select HSRPv1. • 2— Select HSRPv2. <p>If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1.</p>

	Command	Purpose
Step 4	<code>standby [group-number] ip [ip-address [secondary]]</code>	<p>Create (or enable) the HSRP group using its number and virtual IP address.</p> <ul style="list-style-type: none"> (Optional) <i>group-number</i>—The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. (Optional on all but one interface) <i>ip-address</i>—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. (Optional) secondary—The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>show standby [interface-id [group]]</code>	Verify the configuration.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the `no standby [group-number] ip [ip-address]` interface configuration command to disable HSRP.

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



Note

This procedure is the minimum number of steps required to enable HSRP.

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

Configuring HSRP Group Attributes

Although HSRP can run with no other configuration required, you can configure attributes for the HSRP group, including authentication, priority, preemption and preemption delay, timers, or MAC address.

Configuring HSRP Priority

The `standby priority`, `standby preempt`, and `standby track` interface configuration commands are all used to set characteristics for determining active and standby routers and behavior regarding when a new active router takes over. When configuring priority, follow these guidelines:

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.

- The highest number (1 to 255) represents the highest priority (most likely to become the active router).
- When setting the priority, preempt, or both, you must specify at least one keyword (**priority**, **preempt**, or both).
- The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.
- The **standby track** interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.
- The **standby track interface-priority** interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.
- When multiple tracked interfaces are down and *interface-priority* values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.
- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	standby [<i>group-number</i>] priority <i>priority</i>	Set a priority value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. <ul style="list-style-type: none"> • (Optional) <i>group-number</i>—The group number to which the command applies. Use the no form of the command to restore the default values.

	Command	Purpose
Step 4	standby [<i>group-number</i>] preempt [delay [<i>minimum seconds</i>] [reload <i>seconds</i>] [sync <i>seconds</i>]]	<p>Configure the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.</p> <ul style="list-style-type: none"> (Optional) <i>group-number</i>—The group number to which the command applies. (Optional) delay minimum—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over). (Optional) delay reload—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over after a reload). (Optional) delay sync—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an <i>ok</i> or <i>wait</i> reply) for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over). <p>Use the no form of the command to restore the default values.</p>
Step 5	standby [<i>group-number</i>] track <i>type number</i> [<i>interface-priority</i>]	<p>Configure an interface to track other interfaces so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered.</p> <ul style="list-style-type: none"> (Optional) <i>group-number</i>—The group number to which the command applies. <i>type</i>—Enter the interface type (combined with interface number) that is tracked. <i>number</i>—Enter the interface number (combined with interface type) that is tracked. (Optional) <i>interface-priority</i>—Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.
Step 6	end	Return to privileged EXEC mode.
Step 7	show running-config	Verify the configuration of the standby groups.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no standby** [*group-number*] **priority** *priority* [**preempt** [**delay** *delay*]] and **no standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** *delay*] interface configuration commands to restore default priority, preempt, and delay values.

Use the **no standby** [*group-number*] **track** *type number* [*interface-priority*] interface configuration command to remove the tracking.

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.19.108.254
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch#
```


Configuring HSRP Authentication and Timers

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

When configuring these attributes, follow these guidelines:

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

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the HSRP interface on which you want to set authentication.
Step 3	standby [<i>group-number</i>] authentication string	(Optional) authentication string —Enter a string to be carried in all HSRP messages. The authentication string can be up to eight characters in length; the default string is cisco . (Optional) <i>group-number</i> —The group number to which the command applies.
Step 4	standby [<i>group-number</i>] timers <i>hellotime holdtime</i>	(Optional) Configure the time between hello packets and the time before other routers declare the active router to be down. <ul style="list-style-type: none"> • <i>group-number</i>—The group number to which the command applies. • <i>hellotime</i>—The hello interval in seconds. The range is from 1 to 255; the default is 3 seconds. • <i>holdtime</i>—The time in seconds before the active or standby router is declared to be down. The range is from 1 to 255; the default is 10 seconds.
Step 5	end	Return to privileged EXEC mode.
Step 6	show running-config	Verify the configuration of the standby groups.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no standby** [*group-number*] **authentication string** interface configuration command to delete an authentication string. Use the **no standby** [*group-number*] **timers** *hellotime holdtime* interface configuration command to restore timers to their default values.

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

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

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

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

Enabling HSRP Support for ICMP Redirect Messages

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

When the switch is running HSRP, make sure hosts do not discover the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router and that router later fails, packets from the host are lost.

For more information, see the *Cisco IOS IP Configuration Guide, Release 12.2*.

Displaying HSRP Configurations

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

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

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

This is an example of output from the **show standby** privileged EXEC command, displaying HSRP information for two standby groups (group 1 and group 100):

```
Switch# show standby
VLAN1 - Group 1
  Local state is Standby, priority 105, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.182
  Hot standby IP address is 10.0.0.1 configured
  Active router is 172.20.138.35 expires in 00:00:09
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac01
  Name is bbb
```

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

Configuring VRRP

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 multi-access link to use the same virtual IP address. A VRRP router is configured to run VRRP 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, and the other routers act as backups in case it fails.

VRRP Limitations

- You can configure either HSRP or VRRP, but not both, on a switch.
- The VRRP implementation on the switch does not support the MIB specified in RFC 2787.
- The VRRP implementation on the switch supports only text-based authentication.
- The switch supports VRRP only for IPv4.

For more VRRP information and configuration instructions, see [Configuring VRRP](#).

Configuring GLBP

GLBP provides automatic router backup for IP hosts configured with a single default gateway on a 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 act as redundant GLBP routers that become active if any of the existing forwarding routers fail.

GLBP provides load balancing over multiple routers by using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group forward packets.

HSRP, GLBP, and VRRP are First Hop Redundancy Protocols (FHRP).

**Note**

The switch supports only one FHRP at a time. If you enable one FHRP on the switch and try to enable a second one, the command fails.

GLBP is VPN Routing and Forwarding (VRF) aware, supporting multiple routing instances. You can use VRF-aware services to ping for hosts or to display ARP entries for a specific VRF. You can configure GLBP so that traffic from LAN clients can be shared by multiple routers, thereby sharing the traffic load among available routers.

- You can configure only one GLBP group.
- You can configure GLBP group addresses on a maximum of 8 VLANs or routing interfaces.

For more information about GLBP and how to configure it, see:

Configuring First Hop Redundancy Protocols in IPv6

<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-fhrp.html>

The switch supports GLBP IPv4 and GLBP IPv6, and you can configure both at the same time on the switch. Both implementations support identical features and are configured as described in the referenced document with this difference:

- To configure an IPv4 GLBP group, use the command:
glbp group-number ip [ip-address [secondary]]
- To configure an IPv6 GLBP group, use the command:
glbp group-number ipv6 [ipv6-address | autoconfig]

GLBP operates in a mixed IPv4 and IPv6 environment and services both IPv4 and IPv6 VRFs at the same time.

