Configuring GLBP

Last Updated: November 16, 2011

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 Table at the end of this document.

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

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, 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 the figure below, 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*
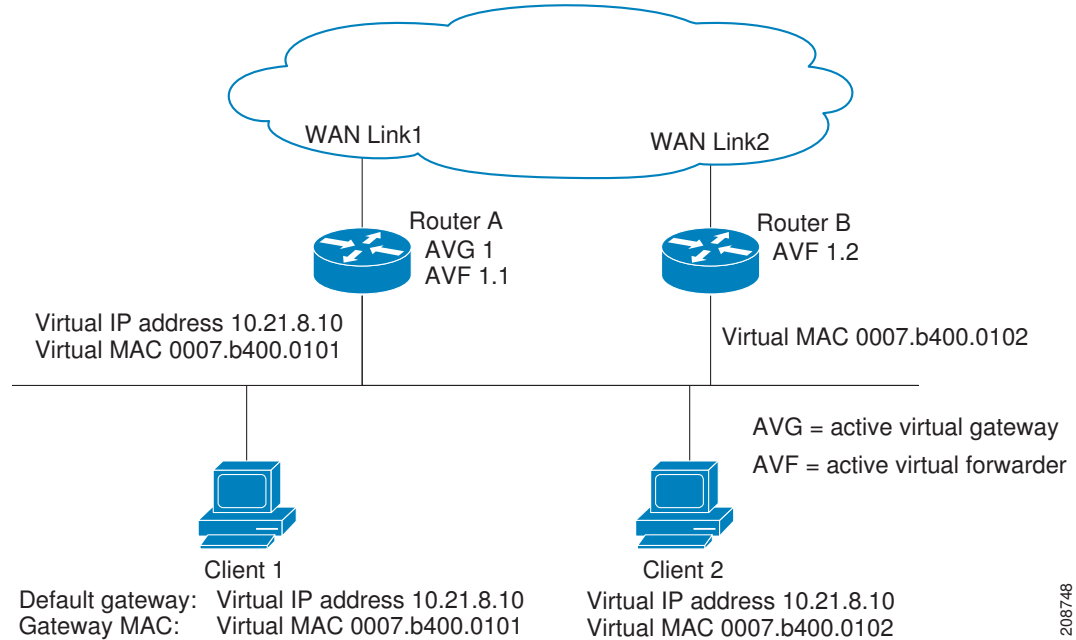
If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for 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 the "GLBP Topology" figure, 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 in the *Cisco IOS XE High Availability Configuration Guide*.

GLBP Benefits

Load Sharing

You can configure GLBP in such a way that traffic from LAN clients can be shared by multiple 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

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.

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.

Command or Action	Purpose
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.

Example

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 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.

	Command or Action	Purpose
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.

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

	Command or Action	Purpose
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. **exit**
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.

Command or Action	Purpose
Step 5 **interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Enters interface configuration mode.
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 **exit** **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 display of diagnostic output concerning various events relating to the operation of GLBP. The **debug condition glbp**,**debug glbp errors**, **debug glbp events**, **debug glbp packets**, and **debug glbp terse** commands are intended only for troubleshooting purposes because the volume of output generated by the software can result in severe performance degradation on the 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** command because the console port is no longer generating character-by-character processor interrupts. If you cannot connect to a console directly, you can run this procedure via a terminal server. If you must break the Telnet connection, however, you may not be able to reconnect because the router may be unable to respond due to the processor load of generating the debugging output.

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.

	Command or Action	Purpose
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.
Step 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] **Example:** `Router# debug condition glbp GigabitEthernet0/0/0 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

```
Router(config)# interface GigabitEthernet 0/0/0
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 GigabitEthernet 0/0/0
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 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 is configured to enable GLBP, and the virtual IP address of 10.21.8.10 is specified for GLBP group 10:

```
Router(config)# interface GigabitEthernet 0/0/0
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 in the *Cisco IOS High Availability XE Configuration Guide*
Object tracking	Configuring Enhanced Object Tracking
Stateful Switchover	Stateful Switchover section in the *Cisco IOS High Availability XE Configuration Guide*

Related Topic	Document Title
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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software

release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1   ***Feature Information for 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.
		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.

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.

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.