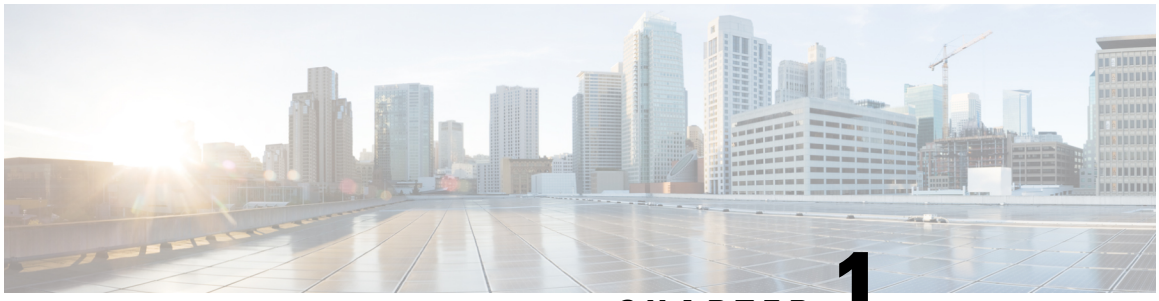
First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE 16 (Cisco ASR 920 Series)

First Published: 2019-07-31

Last Modified: 2020-05-07

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

CONTENTS



CHAPTER 1

Configuring VRRP

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

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

Restrictions for VRRP

- VRRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. VRRP is not intended as a replacement for existing dynamic protocols.
- VRRP is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must configure the VRRP advertise timer to a value equal to or greater than the forwarding delay on the BVI interface. This setting prevents a VRRP router on a recently initialized BVI interface from unconditionally taking over the primary role. Use the **bridge forward-time** command to set the forwarding delay on the BVI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.

Restrictions for VRRP on Cisco Routers

- Stateful Switchover (SSO) with VRRP is supported from Cisco IOS XE Bengaluru 17.5.1 release.

Information About VRRP

VRRP MAC Address

ASIC will be able to receive packets with the IPV4 Virtual MAC address

VRRP is supported on this MAC address: **00:00:5E:00:xx**

VRRP Operation

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

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

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

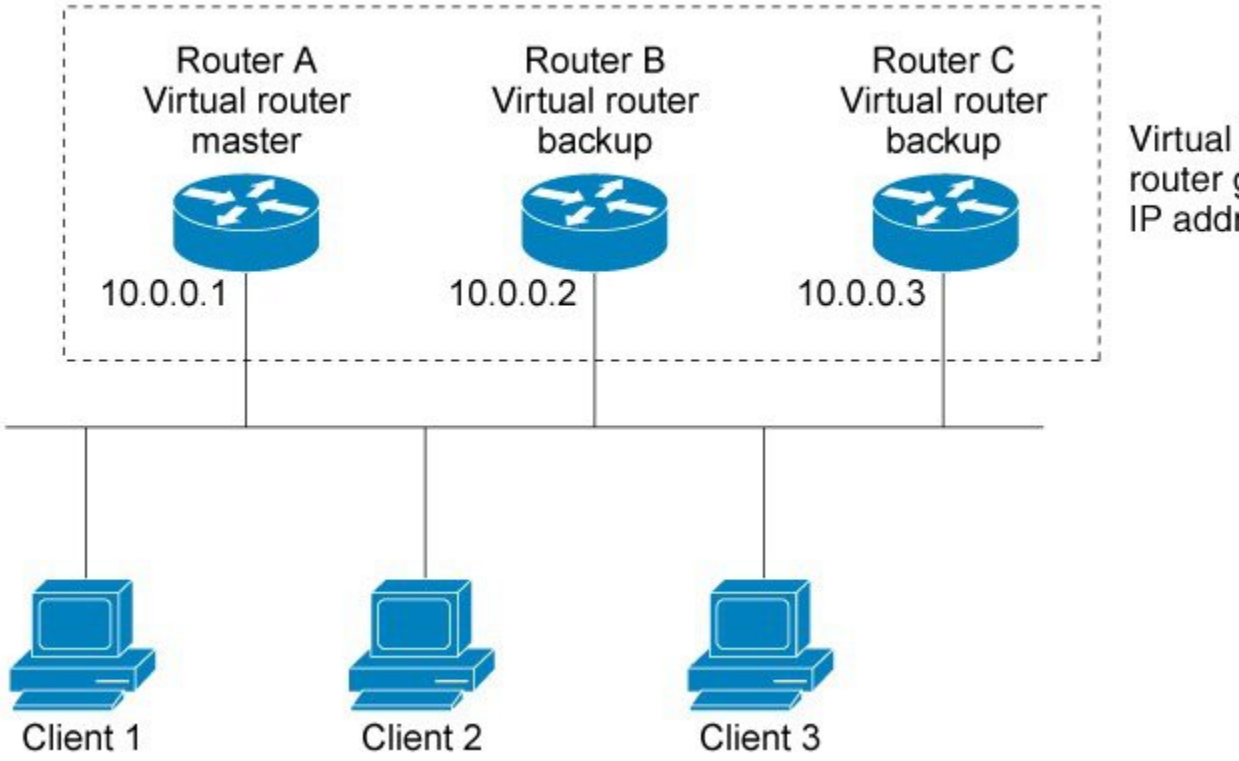
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network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

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

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

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

Figure 1: Basic VRRP Topology

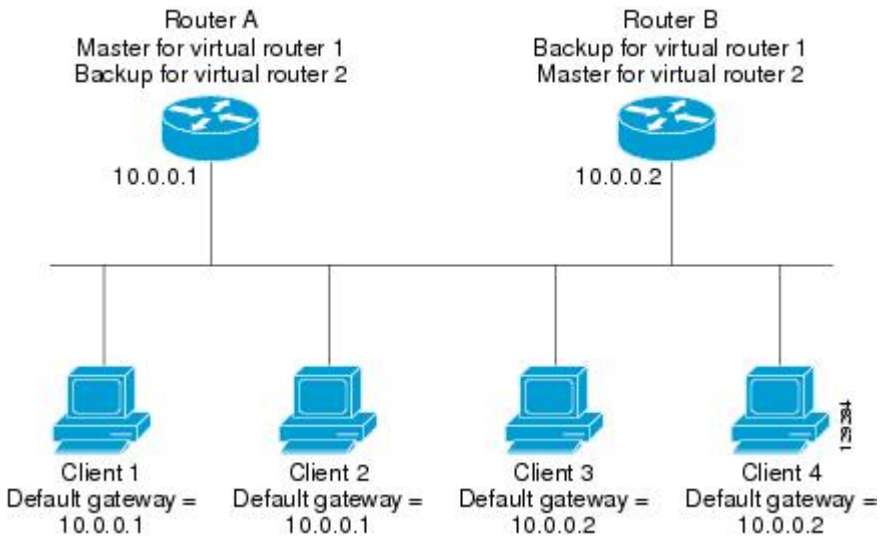


Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual router master and is also known as the IP address owner. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for 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.

The figure below shows a LAN topology in which VRRP is configured so that Routers A and B share the traffic to and from clients 1 through 4 and that Routers A and B act as virtual router backups to each other if either router fails.

Figure 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

Multiple IP Addresses

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

Preemption

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

Authentication

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

Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

VRRP Object Tracking

VRRP object tracking provides a way to ensure the best VRRP router is the virtual primary router for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states.

Multiple Virtual Router Support

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

In a topology where multiple virtual routers are configured on a router interface, the interface can act as primary for one virtual router and as a backup for one or more virtual routers.

VRRP Router Priority and Preemption

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

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

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming virtual primary router if the virtual primary router fails. You can configure the priority of each virtual router backup with a value of 1 through 254 using the **vrrp priority** command.

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

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual primary router. You can disable this preemptive scheme using the **no vrrp preempt** command. If preemption is disabled, the virtual router backup that is elected to become virtual primary router remains as the primary until the original virtual primary router recovers and becomes the primary again.

VRRP Advertisements

The virtual primary router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual primary router. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco routers allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup routers. The primary advertisement value displayed in the **show vrrp** command output on the backup routers is always 1 second because the packets on the backup routers do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only.

In Service Software Upgrade--VRRP

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

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

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

How to Configure VRRP

VRRP

Customizing the behavior of VRRP is optional. Be aware that as soon as you enable a VRRP group, that group is operating. It is possible that if you first enable a VRRP group before customizing VRRP, the router could take over control of the group and become the virtual primary router before you have finished customizing the feature. Therefore, if you plan to customize VRRP, it is a good idea to do so before enabling VRRP.

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *type number*

Example:

```
Router(config)#GigabitEthernet 0/0/0
```

Enters interface configuration mode.

Step 4 **ip address** *ip-address mask*

Example:

```
Router(config-if)# ip address 172.16.6.5 255.255.255.0
```

Configures an IP address for an interface.

Step 5 **vrrp** *group* **description** *text*

Example:

```
Router(config-if)# vrrp 10 description working-group
```

Assigns a text description to the VRRP group.

Step 6 **vrrp** *group* **priority** *level*

Example:

```
Router(config-if)# vrrp 10 priority 110
```

Sets the priority level of the router within a VRRP group.

- The default priority is 100.

Step 7 **vrrp** *group* **preempt** [**delay minimum** *seconds*]

Example:

```
Router(config-if)# vrrp 10 preempt delay minimum 380
```

Configures the router to take over as virtual primary router for a VRRP group if it has a higher priority than the current virtual primary router.

- The default delay period is 0 seconds.
- The router that is IP address owner will preempt, regardless of the setting of this command.

Step 8 **vrrp** *group* **timers learn**

Example:

```
Router(config-if)# vrrp 10 timers learn
```

Configures the router, when it is acting as virtual router backup for a VRRP group, to learn the advertisement interval used by the virtual primary router.

Step 9 **exit**

Example:

```
Router(config-if)# exit
```

Exits interface configuration mode.

Step 10 **no vrrp sso**

Example:

```
Router(config)# no vrrp sso
```

(Optional) Disables VRRP support of SSO.

- VRRP support of SSO is enabled by default.

EnablingVerifying VRRP

Procedure

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)# interfaceGigabitEthernet 0/0/0
```

Enters interface configuration mode.

Step 4 **ip address** *ip-address mask*

Example:

```
Router(config-if)# ip address 172.16.6.5 255.255.255.0
```

Configures an IP address for an interface.

Step 5 **vrrp** *group* **ip** *ip-address* [**secondary**]

Example:

```
Router(config-if)# vrrp 10 ip 172.16.6.1
```

Enables VRRP on an interface.

- After you identify a primary IP address, you can use the **vrrp ip** command again with the **secondary** keyword to indicate additional IP addresses supported by this group.

Note All routers in the VRRP group must be configured with the same primary address and a matching list of secondary addresses for the virtual router. If different primary or secondary addresses are configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to primary.

Step 6 **show vrrp** [**brief all**] | interface]

Example:

```
Router(config-if)#show vrrp brief
Interface Grp Pri Time Own Pre State Master addr Group addr
BD10 1 100 9609 Y Backup 10.1.0.2 10.1.0.10
BD10 5 200 90218 Y Master 10.1.0.1 10.1.0.50
BD10 100 100 3609 Backup 10.1.0.2 10.1.0.100
```

(Optional) Displays a brief or detailed status of one or all VRRP groups on the router.

Step 7 **show vrrp interface** *type number* [**brief**]

Example:

```
Router(config)# interfaceGigabitEthernet 0/0/0
Router)config-if)#show vrrp interface bdi10
BDI10 - Group 10
G1
State is Master
Virtual IP address is 10.0.0.5
Virtual MAC address is 0000.5e00.010a
Advertisement interval is 10.000 sec
Preemption enabled, delay min 380 secs
Priority is 110
Master Router is 10.0.0.2 (local), priority is 110
Master Advertisement interval is 10.000 sec
Master Down interval is 30.570 sec
FLAGS: 1/1
```

(Optional) Displays the VRRP groups and their status on a specified interface.

Step 8 **end**

Example:

```
Router(config-if)# end
```

Returns to privileged EXEC mode.

Disabling a VRRP Group on an Interface

Disabling a VRRP group on an interface allows the protocol to be disabled, but the configuration to be 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 reenables the VRRP group.

Procedure

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)# interfaceGigabitEthernet 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* **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

Before you begin

Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.

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

Procedure

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Router# configure terminal
```

Enters global configuration mode.

Step 3 **terminal interface** *type number*

Example:

```
Router(config)# interfaceGigabitEthernet 0/0/0 Ethernet 0/1
```

Configures an interface type and enters interface configuration mode.

Step 4 **ip address** *ip-address mask* [**secondary**]

Example:

```
Router(config-if)# ip address 10.0.0.1 255.255.255.0
```

Specifies a primary or secondary IP address for an interface.

Step 5 **vrrp** *group* **authentication text** *text-string*

Example:

```
Router(config-if)# vrrp 1 authentication text textstring1
```

Authenticates VRRP packets received from other routers in the group.

- If you configure authentication, all routers within the VRRP group must use the same authentication string.
- The default string is cisco.

Note All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to primary.

Step 6 **vrrp** *group* **ip** *ip-address*

Example:

```
Router(config-if)# vrrp 1 ip 10.0.1.20
```

Enables VRRP on an interface and identifies the IP address of the virtual router.

Step 7 Repeat Steps 1 through 6 on each router that will communicate.

—

Step 8 **end**

Example:

```
Router(config-if)# end
```

Returns to privileged EXEC mode.

Enabling the Router to Send SNMP VRRP Notifications

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.

Procedure

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.

Configuring VRRP v3 for IPV4

```
Fhrp version vrrp v3
Int bdi< >
Vrrp 1 address-family ipv4
Priority 190
Preempt delay minimum 10
Address <ipv4-address> primary
```

BFD on VRRPv3

Table 1: Feature History

Feature Name	Release	Description
Support for BFD, sub-second fast hello for VRRPv3 convergence and re-convergence	Cisco IOS XE Bengaluru 17.6.1	This feature supports VRRP failover such that the fault is detected by the VRRP-BFD client within the configured value – when the connection to the remote interface IP address fails.

The VRRP BFD Peering feature introduces Bidirectional Forwarding Detection (BFD) in the VRRP group. Only one BFD session is created per IP using the **bfd peer** <*IP*> command. The VRRP groups that are configured with the same bfd peer IP, becomes as a client to a common BFD session. You can enable BFD support for VRRP using the **fhrp bfd** command configuration and it is not enabled by default. The VRRP standby device learns the real IP address of the VRRP active device from the VRRP hello messages. The standby device registers as a BFD client and asks to be notified if the active device becomes unavailable. When BFD determines that the connections between standby and active devices has failed, it notifies VRRP on the standby device which immediately takes over as the active device. BFD provides fast peer failure detection independently.

Use the following commands:

- To enable BFD on VRRPv3, use the **fhrp bfd** command.
- To synchronize VRRP or BFD state between the primary and standby RSPs, use the **fhrp sso** command.

Restrictions

- BFD on VRRP is supported only on VRRPv3 groups. For VRRP groups with multiple backup devices, the configuration of BFD peer on each backup device does not create a mesh of peers automatically.
- The VRRP BFD is designed only for one Primary and one Standby topology.
-
- We recommend you to use the BFD template for attaching the BFD timers.
- While using BFD intervals under interfaces, **No bfd echo** must be added explicitly.
- To improve the convergence in multiple ways, use the following commands in your configuration:
  - **arp priority-packet enable**
  - **fhrp delay reload**

Configuration Examples for VRRPv2

Example: Configuring VRRP

In the following example, Router A and Router B each belong to three VRRP groups.

In the configuration, each group has the following properties:

- Group 1:
  - Virtual IP address is 10.1.0.10.
  - Router A will become the primary for this group with priority 120.
  - Advertising interval is 3 seconds.
  - Preemption is enabled.
- Group 5:
  - Router B will become the primary for this group with priority 200.
  - Advertising interval is 30 seconds.
  - Preemption is enabled.
- Group 100:
  - Router A will become the primary for this group first because it has a higher IP address (10.1.0.2).
  - Advertising interval is the default 1 second.
  - Preemption is disabled.

Router A

```
Router(config)#
Router(config)# interfaceGigabitEthernet 0/0/0interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 authentication text cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 100
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

Router B

```
Router(config)#GigabitEthernet 0/0/0interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication text cisco
Router(config-if)# vrrp 1 timers advertise 3
```

```
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 200
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

Example: VRRP Text Authentication

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

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

Example: Disabling 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 the on GigabitEthernet interface 1/0/0:

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

Example: Configuring VRRP BFD Peer

The following example shows how to configure VRRP BFD peer.

```
Router#config terminal
/* Enter configuration commands, one per line. End with CNTL/Z. */
Router(config)#int bdi 101
Router(config-if)#ip add 99.97.5.2 255.255.255.0
Router(config-if)#bfd template 100ms
Router(config-if)#vrrp 105 address-family ipv4
Router(config-if-vrrp)#address 99.97.5.200 primary
Router(config-if-vrrp)#priority 200
Router(config-if-vrrp)#bfd ?
  peer  BFD peer configuration
Router(config-if-vrrp)#bfd peer ?
```

```
  A.B.C.D  IP address
Router(config-if-vrrp)#bfd peer 99.97.5.1
Router(config-if-vrrp)#end
```

Verifying VRRP BFD Peer

To verify the BFD peering information, use the following command in EXEC mode. Also, you can use the **show vrrp neighbor** command to list the number of sessions per neighbor basis.

```
Router#show vrrp bfd
  Interface          Grp  A-F Handle Reference       Peer address        State
  BD51               103 IPv4   1        1                99.97.3.1       UP
  BD76               104 IPv4   2        1                99.97.4.1       UP
  BD101              105 IPv4   3        1                99.97.5.1       UP
  BD126              106 IPv4   4        1                99.97.6.1       UP

Router#show vrrp bfd bdi101
  Interface          Grp  A-F Handle Reference       Peer address        State
  BD101              105 IPv4   3        1                99.97.5.1       UP
```

Example: Configuring VRRP IPv6 Link Local Groups

The following example shows how to configure VRRP IPv6 link local groups.

```
Router(config)#interface bdi 2
Router(config)# bfd template 100ms
Router(config-if)#vrrp 1 address-family ipv6
Router(config-if-vrrp)#address fe80::100 primary
Router(config-if-vrrp)# priority 200
Router(config-if-vrrp)#bfd peer ?
  X:X:X:X::X          IPv6 link-local address
  X:X:X:X::X/<0-128>  IPv6 address and prefix

Router(config-if-vrrp)#bfd peer fe80::4
```

Verifying VRRP IPv6 Link Local Groups

To verify the IPv6 link local group information, use the following command in EXEC mode:

```
Router#show vrrp brief
  Interface          Grp  A-F Pri  Time Own Pre State   Master addr/Group            addr
  BD2                 1 IPv6 200     0  N   Y     MASTER    FE80::3(local)         FE80::100

Router#show vrrp bfd
  Interface          Grp  A-F Handle Reference      Peer address        State
    BD2                1 IPv6         2        1    FE80::4               UP
```

Example: Configuring VRRP for Global IPv6 Groups

The following example shows how to configure VRRP for global IPv6 groups.

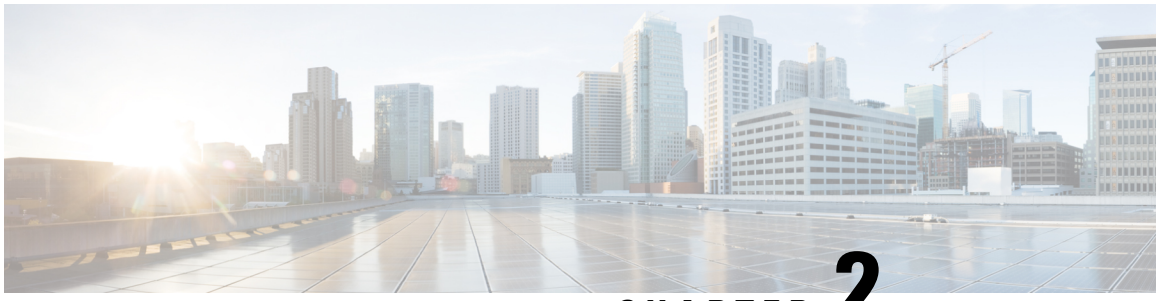
```
Router(config)#interface bdi 3
Router(config)#bfd template 100ms
Router(config-if)#no sh
Router(config-if)#ipv6 address 27::2/64
```

```
Router(config-if)#ipv6 address fe80::1:2 link-local
Router(config-if)#vrrp 1 address-family ipv6
Router(config-if-vrrp)#address fe80::1:100 primary
Router(config-if-vrrp)#address 27::100/64
Router(config-if-vrrp)#bfd peer ?
  X:X:X:X::X          IPv6 link-local address
  X:X:X:X::X/<0-128>  IPv6 address and prefix

Router(config-if-vrrp)#bfd peer 27::3/64
```

Verifying VRRP for Gloabal IPv6 Groups

To verify the global IPv6 information, use the following command in EXEC mode:

```
Router#show vrrp brief
Interface       Grp  A-F Pri  Time Own Pre State   Master addr/Group addr
BD3               1  IPv6 100   0  N   Y  MASTER  FE80::1:2(local) FE80::1:100


Router#show vrrp bfd
  Interface          Grp  A-F Handle Reference       Peer address        State
    BD3                1IPv6   4        1               27::3           UP
```



CHAPTER 2

VRRPv3 Protocol Support

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

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

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

Prerequisites for VRRPv3 Protocol Support

- To enable VRRPv3 on your device, use the **fhrp version vrrp v3** in global configuration mode.

Note By default, the VRRP version is set to version 2.

Restrictions for VRRPv3 Protocol Support

- VRRPv3 is not intended as a replacement for existing dynamic protocols. VRRPv3 is designed for use over multi-access, multicast, or broadcast capable Ethernet LANs.
- VRRPv3 is supported on Ethernet, Fast Ethernet, Bridge Domain Interface (BDI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BDI interface, you must not configure the VRRPv3 advertise timer to a value lesser than the forwarding delay on the BDI interface. If you configure the VRRPv3 advertise timer to a value equal to or greater than the forwarding delay on the BDI interface, the setting prevents a VRRP device on a recently initialized BDI interface from unconditionally taking over the master role. Use the **bridge forward-time** command to set the forwarding delay on the BDI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.
- VRRPv3 does not support Stateful Switchover (SSO).
- Full network redundancy can only be achieved if VRRP operates over the same network path as the VRRS Pathway redundant interfaces. For full redundancy, the following restrictions apply:
  - VRRS pathways should not share a different physical interface as the parent VRRP group or be configured on a sub-interface having a different physical interface as the parent VRRP group.
  - VRRS pathways should not be configured on BDI as long as the associated VLAN does not share the same trunk as the VLAN on which the parent VRRP group is configured.
- No more than two variations of the both VRRP and HSRP protocols are supported when configuring VRRPv3. For example, if both VRRP for IPv4 and VRRP for IPv6 are configured, HSRP cannot be configured.
- Maximum number of VRRPv3 groups supported is 255. It includes both IPv4 and IPv6 groups. Even if the same group is configured with IPv4 and IPv6, they are considered as two different entries.
- Maximum number of VRRPv3 group entries in an interface is four. This is irrespective of whether IPv6 is configured in the same VRRPv3 group as IPv4.
- When enabling 510 VRRPv3 groups, the following restrictions apply:

  Note Use the **platform scale vrrp** command to increase the scale of VRRPv3 groups. For more information, see the *Enabling 510 VRRPv3 Instances* section.

  - HSRP is not supported.
  - IPv6 VRRP is not supported.
  - Only one VRRP group can be configured on an interface.
  - There is no restriction in the number of instances of the same group; only on the maximum number of VRRP group instances, which is 510.

- VRRP scale cannot be enabled or disabled if there is an existing VRRP or HSRP group.

Information About VRRPv3 Protocol Support

VRRPv3 Benefits

Support for IPv4 and IPv6

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

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

Redundancy

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

Load Sharing

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

Multiple Virtual Devices

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

Multiple IP Addresses

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

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

Preemption

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

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

Advertisement Protocol

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

VRRP Device Priority and Preemption

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

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

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

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

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

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

VRRP Advertisements

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

Cisco routers allow you to configure millisecond timers, which is a change from VRRPv2. You need to manually configure the millisecond timer values on both the primary and the backup routers. The master advertisement value displayed in the **show vrrp** command output on the backup routers is always 1 second.

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

How to Configure VRRPv3 Protocol Support

IPv6 VRRP Link Local Address

VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.

Enabling VRRPv3 on a Device

To enable VRRPv3 on a device, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS. **Note** When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Creating and Customizing a VRRP Group

To create a VRRP group, perform the following task. Steps 7 to 14 denote customizing options for the group, and they are optional:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS. **Note** When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Enters interface configuration mode.

Step 5	**vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
	Example:
	`Device(config-if)# vrrp 3 address-family ipv4`
	`Device(config-if)# vrrp 3 address-family ipv6`
		Creates a VRRP group and enters VRRP configuration mode.

Step 6	**address** *ip-address* [**primary** | **secondary**]
	Example:
	`Device(config-if-vrrp)# address 100.0.1.10 primary`
	`Device(config-if-vrrp)# address fe80::10 primary`
		Specifies a primary or secondary address for the VRRP group.
		Note VRRPv3 for IPv6 requires that a primary virtual link-local IPv6 address is configured to allow the group to operate. After the primary link-local IPv6 address is established on the group, you can add the secondary global addresses.

Step 7	**description** *group-description* **Example:**	(Optional) Specifies a description for the VRRP group.

	Command or Action	Purpose
	`Device(config-if-vrrp)# description group 3`	
Step 8	**match-address** **Example:** `Device(config-if-vrrp)# match-address`	(Optional) Matches secondary address in the advertisement packet against the configured address. • Secondary address matching is enabled by default.
Step 9	**preempt delay minimum** *seconds* **Example:** `Device(config-if-vrrp)# preempt delay minimum 30`	(Optional) Enables preemption of lower priority master device with an optional delay. • Preemption is enabled by default.
Step 10	**priority** *priority-level* **Example:** `Device(config-if-vrrp)# priority 3`	(Optional) Specifies the priority value of the VRRP group. • The priority of a VRRP group is 100 by default.
Step 11	**timers advertise** *interval* **Example:** `Device(config-if-vrrp)# timers advertise 1000`	(Optional) Sets the advertisement timer in milliseconds. • The advertisement timer is set to 1000 milliseconds by default.
Step 12	**vrrpv2** **Example:** `Device(config-if-vrrp)# vrrpv2`	(Optional) Enables support for VRRPv2 simultaneously, so as to interoperate with devices which only support VRRP v2. • VRRPv2 is disabled by default.
Step 13	**vrrs leader** *vrrs-leader-name* **Example:** `Device(config-if-vrrp)# vrrs leader leader-1`	(Optional) Specifies a leader's name to be registered with VRRS and to be used by followers. • A registered VRRS name is unavailable by default.
Step 14	**shutdown** **Example:** `Device(config-if-vrrp)# shutdown`	(Optional) Disables VRRP configuration for the VRRP group. • VRRP configuration is enabled for a VRRP group by default.
Step 15	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	

Example: Creating a VRRS Leader and Follower

A VRRS leader **leader-1** is created on interface BDI 201:

```
interface BDI201
ip address 201.0.0.2 255.255.255.0
vrrp 1 address-family ipv4
  vrrs leader leader-1
  address 201.0.0.10 primary
  exit-vrrp
end
```

A VRRS follower is created on interface BDI 200 using the **vrrs pathway** command:

```
interface BDI200
ip address 200.0.0.2 255.255.255.0
vrrs pathway leader-1
  address 200.0.0.10
  exit-vrrs-pw
end
```

Enabling 510 VRRPv3 Instances

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS. **Note** When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	**platform scale vrrp** **Example:** `Device(config)# platform scale vrrp`	Enables the configuration of 510 VRRPv3 group instances.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring the Delay Period Before FHRP Client Initialization

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp v3** **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS. **Note** When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Enters interface configuration mode.
Step 5	**fhrp delay** {[**minimum**] [**reload**] *seconds*} **Example:** `Device(config-if)# fhrp delay minimum 5`	Specifies the delay period for the initialization of FHRP clients after an interface comes up. • The range is 0-3600 seconds.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuration Examples for VRRPv3 Protocol Support

Example: Enabling VRRPv3 on a Device

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

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

Example: Creating and Customizing a VRRP Group

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

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

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

Example: Configuring the Delay Period Before FHRP Client Initialization

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

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

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

Example: VRRP Status, Configuration, and Statistics Details

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

```
Device> enable
Device# show vrrp detail

 Ethernet0/0 - Group 1 - Address-Family IPv4

 State is MASTER
 State duration 3.707 secs
 Virtual IP address is 1.0.0.10
 Virtual MAC address is 0000.5E00.0101
 Advertisement interval is 1000 msec
 Preemption enabled
 Priority is 100
 Master Router is 1.0.0.1 (local), priority is 100
 Master Advertisement interval is 1000 msec (expires in 686 msec)
 Master Down interval is unknown
 State is MASTER
 State duration 3.707 secs
 VRRPv3 Advertisements: sent 5 (errors 0) - rcvd 0
 VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
 Group Discarded Packets: 0
   VRRPv2 incompatibility: 0
   IP Address Owner conflicts: 0
   Invalid address count: 0
   IP address configuration mismatch : 0
   Invalid Advert Interval: 0
   Adverts received in Init state: 0
   Invalid group other reason: 0
 Group State transition:
   Init to master: 0
   Init to backup: 1 (Last change Mon Jul 30 16:42:01.856)
   Backup to master: 1 (Last change Mon Jul 30 16:42:05.469)
   Master to backup: 0
   Master to init: 0
   Backup to init: 0

Device# exit
```

Configuring Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. You can deploy HSRP in a group of routers to select an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met).

Each router uses only three timers in HSRP. The timers time the hello messages. When a failure occurs, the HSRP converges depend on how the HSRP hello and hold timers are configured. By default, these timers are set to three and ten seconds respectively, which means that a hello packet is sent between the HSRP standby group devices every three seconds. The standby device becomes active when a hello packet is not received for ten seconds. You can lower these timer settings to speed up the failover or preemption, but, to avoid increased CPU usage and unnecessary standby state flapping, do not set the hello timer below one second or the hold timer below four seconds.

HSRP is enabled on an interface by entering the **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] command. The standby command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see to the HSRP section of the Cisco IP Configuration Guide publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 0/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

```
Router(config)# interface GigabitEthernet 0/1/0
Router(config-if)# standby 2 ip 120.12.1.200
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
```

Verifying HSRP

To verify the HSRP information, use the **show standby** command in EXEC mode:

```
Router# show standby

Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

SNMP MIBs Supported for VRRPv3

- VRRPv3 operations OID 1.3.6.1.2.1.207.1.1.1
- VRRPv3 statistics OID 1.3.6.1.2.1.207.1.2
- VRRPv3 traps for vrrpv3NewMaster (1.3.6.1.2.1.207.0.1) and vrrpv3ProtoError (1.3.6.1.2.1.207.0.2)

Additional References for VRRPv3 Protocol Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
FHRP commands	First Hop Redundancy Protocols Command Reference
Configuring VRRPv2	*Configuring VRRP*

Standards and RFCs

Standard/RFC	Title
RFC5798	*Virtual Router Redundancy Protocol*
RFC 6527	*Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)*

MIBs

MIB	MIBs Link
VRRPv3 MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Glossary

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

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

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

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

VRRP router—A router that is running VRRP.