



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, on page 1](#)
- [Restrictions for VRRPv3 Protocol Support, on page 2](#)
- [Information About VRRPv3 Protocol Support, on page 3](#)
- [How to Configure VRRPv3 Protocol Support, on page 5](#)
- [Configuration Examples for VRRPv3 Protocol Support, on page 11](#)
- [Configuring Hot Standby Router Protocol, on page 12](#)
- [SNMP MIBs Supported for VRRPv3, on page 13](#)
- [Additional References for VRRPv3 Protocol Support, on page 13](#)

Prerequisites for VRRPv3 Protocol Support

- To enable VRRPv3 on your device, use the **hrnp 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

Increase in VRRPv3 Scale Support on RSP3 Module

- The supported VRRP group scale is increased to 256 VRRPv3 groups (both IPv4 and IPv6) based on VRRP virtual MAC address.

The group numbers for either IPv4 or IPv6 can be configured only from 1 to 255. VRRPv3 groups can be scaled up to 255, only if either IPv4 or IPv6 configured individually. If both IPv4 and IPv6 groups are scaled together, up to 256 groups can be scaled in any combination (for example, 128 IPv4 + 128 IPv6 groups).

- VRRPv3 group numbers can be reused multiple times.
- If VRRPv3 groups are repeated, the virtual MAC address scale should not exceed 256. If the assigned virtual MAC address crosses 256, then unpredictable behavior may be expected.

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 **hrp 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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	fhrp version vrrp v3 Example: Device(config)# fhrp version vrrp v3	Enables the ability to configure VRRPv3 and VRRS. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay** **minimum** *seconds*
10. **priority** *priority-level*
11. **timers** **advertise** *interval*
12. **vrrpv2**
13. **vrrs** **leader** *vrrs-leader-name*
14. **shutdown**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	fhrp version vrrp v3 Example: Device(config)# fhrp version vrrp v3	Enables the ability to configure VRRPv3 and VRRS. Note When VRRPv3 is in use, VRRPv2 is unavailable.
Step 4	interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0	Enters interface configuration mode.
Step 5	vrrp <i>group-id</i> 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 <i>ip-address</i> [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 <i>group-description</i> Example: Device(config-if-vrrp)# description group 3	(Optional) Specifies a description for the VRRP group.
Step 8	match-address Example: Device(config-if-vrrp)# match-address	(Optional) Matches secondary address in the advertisement packet against the configured address. <ul style="list-style-type: none"> Secondary address matching is enabled by default.
Step 9	preempt delay minimum <i>seconds</i> Example:	(Optional) Enables preemption of lower priority master device with an optional delay. <ul style="list-style-type: none"> Preemption is enabled by default.

	Command or Action	Purpose
	<code>Device(config-if-vrrp)# preempt delay minimum 30</code>	
Step 10	<p>priority <i>priority-level</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# priority 3</pre>	<p>(Optional) Specifies the priority value of the VRRP group.</p> <ul style="list-style-type: none"> The priority of a VRRP group is 100 by default.
Step 11	<p>timers advertise <i>interval</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# timers advertise 1000</pre>	<p>(Optional) Sets the advertisement timer in milliseconds.</p> <ul style="list-style-type: none"> The advertisement timer is set to 1000 milliseconds by default.
Step 12	<p>vrrpv2</p> <p>Example:</p> <pre>Device(config-if-vrrp)# vrrpv2</pre>	<p>(Optional) Enables support for VRRPv2 simultaneously, so as to interoperate with devices which only support VRRP v2.</p> <ul style="list-style-type: none"> VRRPv2 is disabled by default.
Step 13	<p>vrrs leader <i>vrrs-leader-name</i></p> <p>Example:</p> <pre>Device(config-if-vrrp)# vrrs leader leader-1</pre>	<p>(Optional) Specifies a leader's name to be registered with VRRS and to be used by followers.</p> <ul style="list-style-type: none"> A registered VRRS name is unavailable by default.
Step 14	<p>shutdown</p> <p>Example:</p> <pre>Device(config-if-vrrp)# shutdown</pre>	<p>(Optional) Disables VRRP configuration for the VRRP group.</p> <ul style="list-style-type: none"> VRRP configuration is enabled for a VRRP group by default.
Step 15	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	<p>Returns to privileged EXEC mode.</p>

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

SUMMARY STEPS

1. enable
2. configure terminal
3. fhrp version vrrp v3
4. platform scale vrrp
5. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	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.
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:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **fhrp delay** {[**minimum**] [**reload**] *seconds*}
6. **end**

DETAILED STEPS

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

Configuration Examples for VRRPv3 Protocol Support

Example: Enabling VRRPv3 on a Device

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

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

Example: Creating and Customizing a VRRP Group

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

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



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

Example: Configuring the Delay Period Before FHRP Client Initialization

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

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



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

Example: VRRP Status, Configuration, and Statistics Details

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

```
Device> enable
Device# show vrrp detail

Ethernet0/0 - Group 1 - Address-Family IPv4

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

Device# exit
```

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	<i>Configuring VRRP</i>

Standards and RFCs

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

MIBs

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

Technical Assistance

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