



## **First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE 17 (Cisco NCS 520 Series)**

**First Published:** 2019-11-26

### **Americas Headquarters**

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



# CONTENTS

---

## CHAPTER 1

### About HSRP 1

- Restrictions for HSRP 1
- Information about HSRP 1
  - HSRP Operation 1
  - HSRP Benefits 2
  - HSRP Groups and Group Attributes 2
  - HSRP Preemption 3
  - HSRP Priority and Preemption 3
  - How Object Tracking Affects the Priority of an HSRP Device 3
  - HSRP Addressing 4
  - HSRP Virtual MAC Addresses and BIA MAC Addresses 4
  - HSRP MAC Address 4
  - HSRP MAC Refresh Interval 4
  - HSRP Text Authentication 5
  - HSRP MD5 Authentication 5
- How to Configure HSRP 6
  - Configuring HSRP 6
  - Displaying HSRP Information 6

---

## CHAPTER 2

### Configuring VRRP 9

- Restrictions for VRRP 9
- Restrictions for VRRP for NCS 520 9
- Information About VRRP 10
  - VRRP MAC Address 10
  - VRRP Operation 10
  - VRRP Benefits 12

Multiple Virtual Router Support	13
VRRP Router Priority and Preemption	13
VRRP Advertisements	14
How to Configure VRRP	14
Configuring VRRP	14
Enabling VRRP	16
Disabling a VRRP Group on an Interface	17
Configuring VRRP Text Authentication	19
Configuring VRRP v3 for IPv4	20
BFD on VRRPv3	20
Configuration Examples for VRRPv2	21
Example: Configuring VRRP	21
Example: VRRP Text Authentication	22
Example: Disabling a VRRP Group on an Interface	22
Example: Configuring VRRP BFD Peer	23
Example: Configuring VRRP IPv6 Link Local Groups	23
Example: Configuring VRRP for Global IPv6 Groups	24



# CHAPTER 1

## About HSRP

---

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

- [Restrictions for HSRP, on page 1](#)
- [Information about HSRP, on page 1](#)
- [How to Configure HSRP, on page 6](#)

## Restrictions for HSRP

- For supporting HSRP, ASIC should be able to receive packets destined with below IPv4 VMAC.  
HSRP is supported on this MAC address: **00:00:0C:07:xx**
- HSRP version 2 is not supported on the NCS520 router.
- HSRP and VRRP are both supported on Bridge Domain Interfaces (BDI) only.
- Timer supported values for the HSRP are: 0.3 seconds for Hello Interval and 1 second for Dead Interval.

## Information about HSRP

### HSRP Operation

Most IP hosts have an IP address of a single device configured as the default gateway. When HSRP is used, the HSRP virtual IP address is configured as the host's default gateway instead of the IP address of the device.

HSRP is useful for hosts that do not support a discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new device when their selected device reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of devices running HSRP. The address of this HSRP group is referred to as the virtual IP address. One of these devices is selected by the protocol to be the active device. The active device receives and routes packets destined for the MAC address of the group. For  $n$  devices running HSRP,  $n + 1$  IP and MAC addresses are assigned.

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

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

Devices that are running HSRP send and receive multicast UDP-based hello messages to detect device failure and to designate active and standby devices. When the active device fails to send a hello message within a configurable period of time, the standby device with the highest priority becomes the active device. The transition of packet forwarding functions between devices is completely transparent to all hosts on the network.

You can configure multiple Hot Standby groups on an interface, thereby making fuller use of redundant devices and load sharing.

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

## HSRP Benefits

- **Redundancy:**  
HSRP employs a redundancy scheme that is time proven and deployed extensively in large networks.
- **Fast Failover:**  
HSRP provides transparent fast failover of the first-hop device.
- **Preemption:**  
Preemption allows a standby device to delay becoming active for a configurable amount of time.
- **Authentication:**  
HSRP message digest 5 (MD5) algorithm authentication protects against HSRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

## HSRP Groups and Group Attributes

You can use the CLI to apply group attributes to:

- A single HSRP group—performed in interface configuration mode and applies to a group.

- All groups on the interface—performed in interface configuration mode and applies to all groups on the interface.
- All groups on all interfaces—performed in global configuration mode and applies to all groups on all interfaces.

## HSRP Preemption

When a newly reloaded device becomes HSRP active, and there is already an HSRP active device on the network, HSRP preemption may appear to not function. HSRP preemption may appear not function correctly because the new HSRP active device did not receive any hello packets from the current HSRP active device, and the preemption configuration never factored into the new device's decision making.

HSRP may appear to not function on some larger hardware platforms where there can be a delay in an interface receiving packets.

In general, we recommend that all HSRP devices have the following configuration: **standby delay minimum 30 reload 60**

The **standby delay minimum reload** interface configuration command delays HSRP groups from initializing for the specified time after the interface comes up.

This is a different command than the **standby preempt delay** interface configuration command, which enables HSRP preemption delay.

## HSRP Priority and Preemption

Preemption enables the HSRP router with the highest priority to immediately become the active router. Priority is determined first by the configured priority value, and then by the IP address. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. In each case, a higher value is of greater priority. If you do not use the **standby preempt** interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

A standby router with equal priority but a higher IP address will not preempt the active router.

When a router first comes up, it does not have a complete routing table. You can set a preemption delay that allows preemption to be delayed for a configurable time period. This delay period allows the router to populate its routing table before becoming the active router.

If preemption is not enabled, then a router may appear to preempt the active router if it does not receive any Hello messages from the active router.

## How Object Tracking Affects the Priority of an HSRP Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to HSRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If the specified object goes down, the HSRP priority is reduced. The HSRP device with the higher priority can become the active device if it has the **standby preempt** command configured.

## HSRP Addressing

HSRP devices communicate between each other by exchanging HSRP hello packets. These packets are sent to the destination IP multicast address 224.0.0.2 (reserved multicast address used to communicate to all devices) on UDP port 1985. The active device sources hello packets from its configured IP address and the HSRP virtual MAC address while the standby device sources hellos from its configured IP address and the interface MAC address, which may or may not be the burned-in MAC address (BIA).

Because hosts are configured with their default gateway as the HSRP virtual IP address, hosts must communicate with the MAC address associated with the HSRP virtual IP address. This MAC address will be a virtual MAC address in the format of 0000.0C07.ACxy, where xy is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group one will use the HSRP virtual MAC address of 0000.0C07.AC01. Hosts on the adjoining LAN segment use the normal Address Resolution Protocol (ARP) process to resolve the associated MAC addresses.

HSRP version 2 uses the new IP multicast address 224.0.0.102 to send hello packets instead of the multicast address of 224.0.0.2, which is used by version 1. This new multicast address allows Cisco Group Management Protocol (CGMP) leave processing to be enabled at the same time as HSRP.

HSRP version 2 permits an expanded group number range, 0 to 4095, and consequently uses a new MAC address range 0000.0C9F.F000 to 0000.0C9F.FFFF

## HSRP Virtual MAC Addresses and BIA MAC Addresses

A device automatically generates a virtual MAC address for each HSRP device. However, some network implementations, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, specify the virtual MAC address by using the **standby mac-address** command in the group; the virtual IP address is unimportant for these protocols.

The **standby use-bia** command was implemented to overcome the limitations of using a functional address for the HSRP MAC address on Token Ring interfaces. This command allows HSRP groups to use the burned-in MAC address of an interface instead of the HSRP virtual MAC address. When HSRP runs on a multiple-ring, source-routed bridging environment and the HSRP devices reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

The **standby use-bia** command is used for an interface and the **standby mac-address** command is used for an HSRP group.

## HSRP MAC Address

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

HSRP is supported on this MAC address: **00:00:0C:07:xx**

## HSRP MAC Refresh Interval

When HSRP runs over FDDI, you can change the interval at which a packet is sent to refresh the MAC cache on learning bridges and switches. HSRP hello packets on FDDI interfaces use the burned-in address (BIA) instead of the MAC virtual address. Refresh packets keep the MAC cache on switches and learning bridges current. Refresh packets are also used for HSRP groups configured as multigroup slaves because these do not send regular Hello messages.

You can change the refresh interval on FDDI rings to a longer or shorter interval, thereby using bandwidth more efficiently. You can prevent the sending of any MAC refresh packets if you do not need them (if you have FDDI but do not have a learning bridge or switch).

## HSRP Text Authentication

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

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device.

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

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

## HSRP MD5 Authentication

Before the introduction of HSRP MD5 authentication, HSRP authenticated protocol packets with a simple plain text string. HSRP MD5 authentication is an enhancement to generate an MD5 digest for the HSRP portion of the multicast HSRP protocol packet. This functionality provides added security and protects against the threat from HSRP-spoofing software.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each HSRP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can be either given directly in the configuration using a key string or supplied indirectly through a key chain.

HSRP has two authentication schemes:

- Plain text authentication
- MD5 authentication

HSRP authentication protects against false HSRP hello packets causing a denial-of-service attack. For example, Device A has a priority of 120 and is the active device. If a host sends spoof HSRP hello packets with a priority of 130, then Device A stops being the active device. If Device A has authentication configured such that the spoof HSRP hello packets are ignored, Device A will remain the active device.

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

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



	Command or Action	Purpose
	<pre> 100.100.1.2    100.100.1.20 Router#                     </pre>	
<b>Step 3</b>	<p><b>show standby</b></p> <p><b>Example:</b></p> <pre> BDI101 - Group 1   State is Standby     4 state changes, last state change 00:04:24   Virtual IP address is 100.100.1.10   Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)   Local virtual MAC address is 0000.0c07.ac01 (v1 default)   Hello time 3 sec, hold time 10 sec   Next hello sent in 1.616 secs   Authentication text, string "auth"   Preemption enabled   Active router is 100.100.1.2, priority 200 (expires in 9.472 sec)   Standby router is local   Priority 190 (configured 190)   Group name is "hsrp-BD101-1" (default)    FLAGS: 0/1 BDI101 - Group 2   State is Active     2 state changes, last state change 00:04:55   Virtual IP address is 100.100.1.20   Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)   Local virtual MAC address is 0000.0c07.ac02 (v1 default)   Hello time 3 sec, hold time 10 sec   Next hello sent in 0.256 secs   Authentication text, string "auth1"   Preemption enabled   Active router is local   Standby router is 100.100.1.2, priority 190 (expires in 8.960 sec)   Priority 200 (configured 200)   Group name is "hsrp-BD101-2" (default)    FLAGS: 1/1 Router#                     </pre>	
<b>Step 4</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre> Router# end                     </pre>	Returns to privileged EXEC mode.





## CHAPTER 2

# 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, on page 9](#)
- [Restrictions for VRRP for NCS 520, on page 9](#)
- [Information About VRRP, on page 10](#)
- [How to Configure VRRP, on page 14](#)
- [Configuring VRRP v3 for IPV4, on page 20](#)
- [BFD on VRRPv3, on page 20](#)
- [Configuration Examples for VRRPv2, on page 21](#)

## Restrictions for VRRP

### Restrictions for VRRP for NCS 520

- A maximum of 255 unique FHRP (HSRP and VRRP) groups is supported.
- Bridge Domain Interface (BDI) can have 4 instances of HSRP and VRRP combined.
- HSRP and VRRP are both supported **only** on the Bridge Domain Interface.
- HSRP and VRRP are supported on layer 3 Bridge Domain Interfaces (BDI) with Trunk Ethernet Flow Points EFP/TEFP over layer 2 port and layer 3 BDI with EFP/TEFP over layer 2 port channel.
- IPv6 is not supported on the HSRP and VRRP.

# 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.

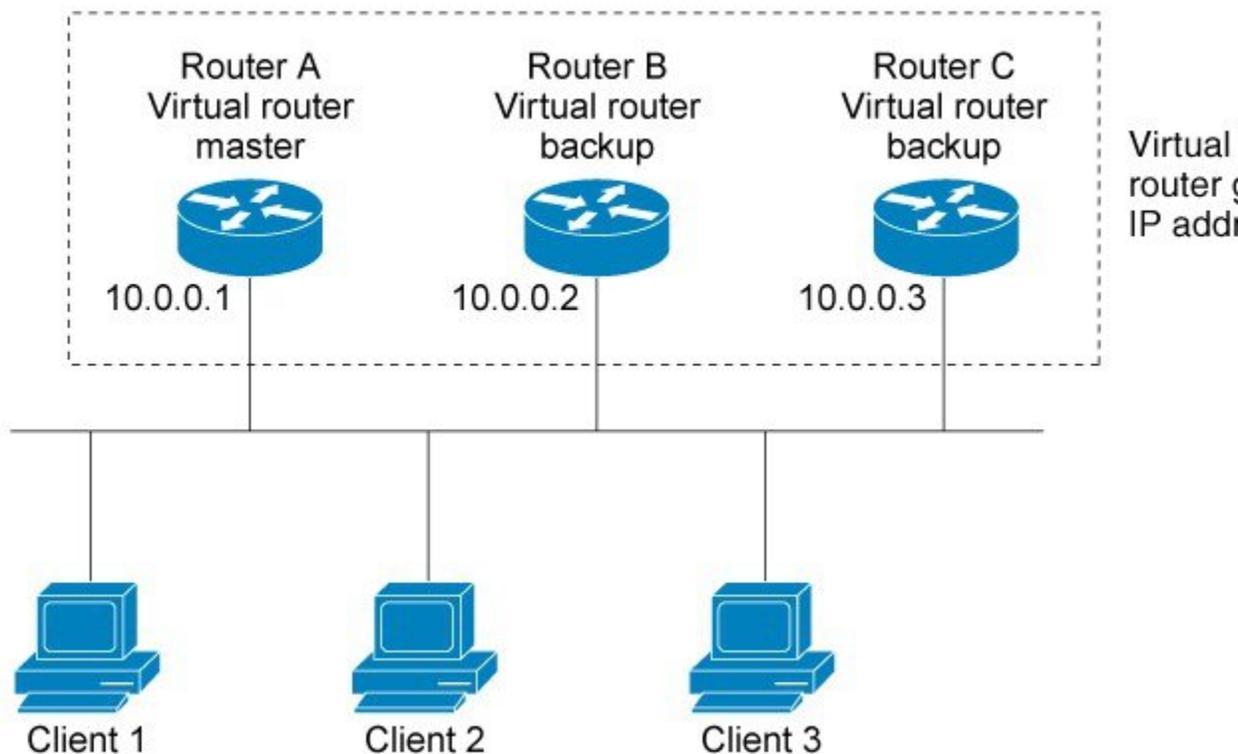
The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

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.

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

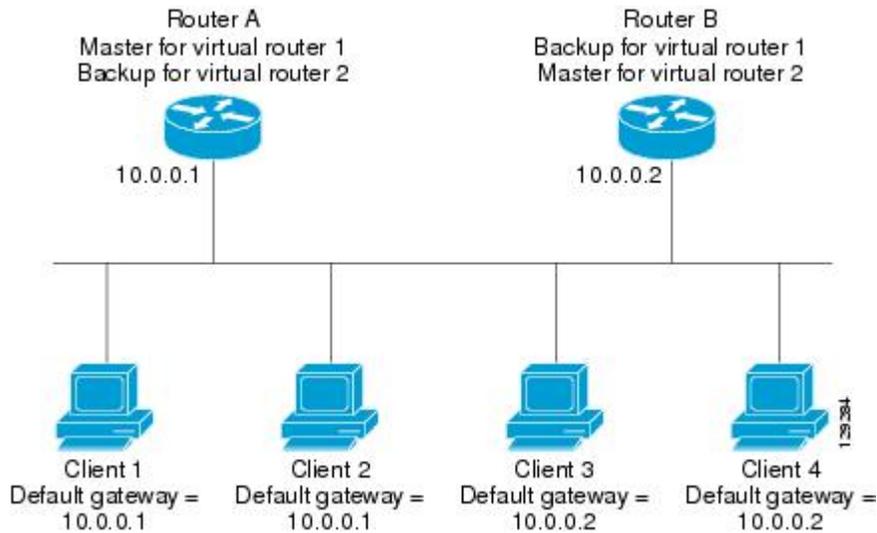


Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual router master and is also known as the IP address owner. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for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

## How to Configure VRRP

### Configuring 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)# BDI <interface number>
```

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.
- 

## 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)# interface BDI <interface number>
```

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)# interface BDI <interface number>
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)# interface BDI <interface number>
```

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)# interface BDI <interface number> 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** `end`

**Example:**

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

Returns to privileged EXEC mode.

## 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)# interface BDI <interface number>
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)# BDI <interface number>
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)# BDI <interface number>
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 BDI Interface while retaining VRRP for group 2 on the BDI interface:

```

Router(config)# BDI <interface number>
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)# BDI <interface number>
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254

```

## 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 Global 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                 1 IPv6          4          1  27::3       UP
```