



Configuring VRRP

This chapter describes how to configure the Virtual Router Redundancy Protocol (VRRP) on a switch

This chapter includes the following sections:

- [Information About VRRP, page 18-1](#)
- [Licensing Requirements for VRRP, page 18-8](#)
- [Guidelines and Limitations, page 18-8](#)
- [Default Settings, page 18-9](#)
- [Configuring VRRP, page 18-9](#)
- [Enabling VRRPv3 feature, page 18-20](#)
- [Displaying VRRP Statistics, page 18-25](#)
- [Configuration Examples for VRRP, page 18-25](#)
- [Additional References, page 18-26](#)

Information About VRRP

VRRP allows for transparent failover at the first-hop IP router, by configuring a group of routers to share a virtual IP address. VRRP selects a master router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the master router fails.

This section includes the following topics:

- [VRRP Operation, page 18-2](#)
- [VRRP Benefits, page 18-3](#)
- [Multiple VRRP Groups, page 18-3](#)
- [VRRP Router Priority and Preemption, page 18-4](#)
- [BFD, page 18-5](#)
- [vPC and VRRP, page 18-5](#)
- [VRRP Advertisements, page 18-6](#)
- [VRRP Authentication, page 18-6](#)
- [VRRP Tracking, page 18-6](#)
- [Virtualization Support, page 18-7](#)

VRRP Operation

A LAN client can determine which router should be the first hop to a particular remote destination by using 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.

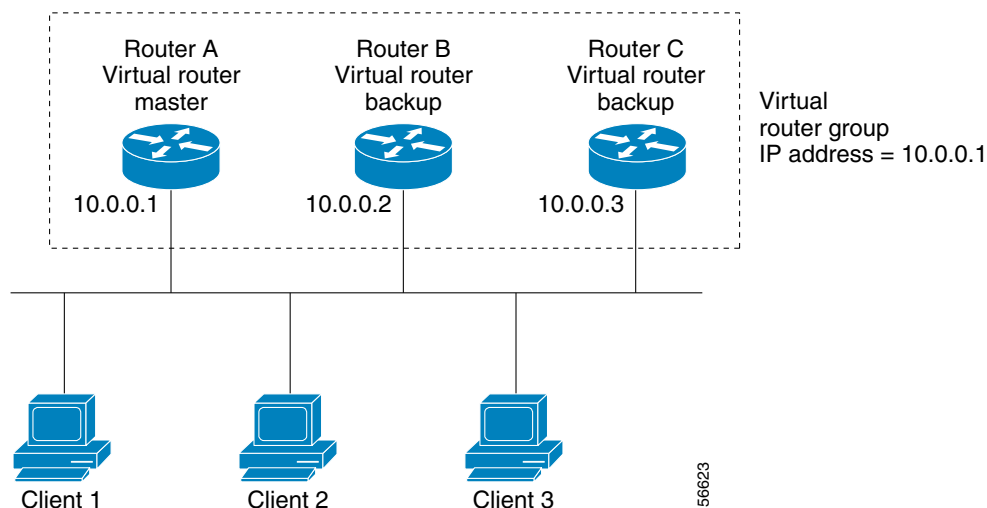
The disadvantage to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. Although, this approach simplifies client configuration and processing, it 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 by enabling a group of routers (a VRRP group) to share a single virtual IP address. You can then configure the LAN clients with the virtual IP address as their default gateway.

Figure 18-1 shows a basic VLAN topology. In this example, Routers A, B, and C form a VRRP group. The IP address of the group is the same address that was configured for the Ethernet interface of Router A (10.0.0.1).

Figure 18-1 Basic VRRP Topology



Because the virtual IP address uses the IP address of the physical Ethernet interface of Router A, Router A is the master (also known as the IP address owner). As the master, Router A owns the virtual IP address of the VRRP group router and forwards 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 backups. If the master fails, the backup router with the highest priority becomes the master and takes over the virtual IP address to provide uninterrupted service for the LAN hosts. When router A recovers, it becomes the router master again. For more information, see the “[VRRP Router Priority and Preemption](#)” section.

**Note**

In Cisco NX-OS Release 4.1(2) and later, pPackets received on a routed port destined for the VRRP virtual IP address will terminate on the local router, regardless of whether that router is the master VRRP router or a backup VRRP router. This includes ping and telnet traffic. Packets received on a Layer 2 (VLAN) interface destined for the VRRP virtual IP address will terminate on the master router.

VRRP Benefits

The benefits of VRRP are as follows:

- **Redundancy**—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**—Allows traffic to and from LAN clients to be shared by multiple routers. The traffic load is shared more equitably among available routers.
- **Multiple VRRP groups**—Supports up to 255 VRRP groups on a router physical interface if the platform supports multiple MAC addresses. Multiple VRRP groups enable you to implement redundancy and load sharing in your LAN topology.
- **Multiple IP Addresses**—Allows you to manage multiple IP addresses, including secondary IP addresses. If you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.
- **Preemption**—Enables you to preempt a backup router that has taken over for a failing master with a higher priority backup router that has become available.
- **Authentication**—Protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.
- **Advertisement Protocol**—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. IANA has assigned the IP protocol number 112 to VRRP.
- **VRRP Tracking**—Ensures that the best VRRP router is the master for the group by altering VRRP priorities based on interface states.

VRRPv3 has the following benefits:

- Interoperability in multi-vendor environments.
- Support for IPv4 and IPv6 address families.
- Improved scalability through the use of VRRS pathways.

Multiple VRRP Groups

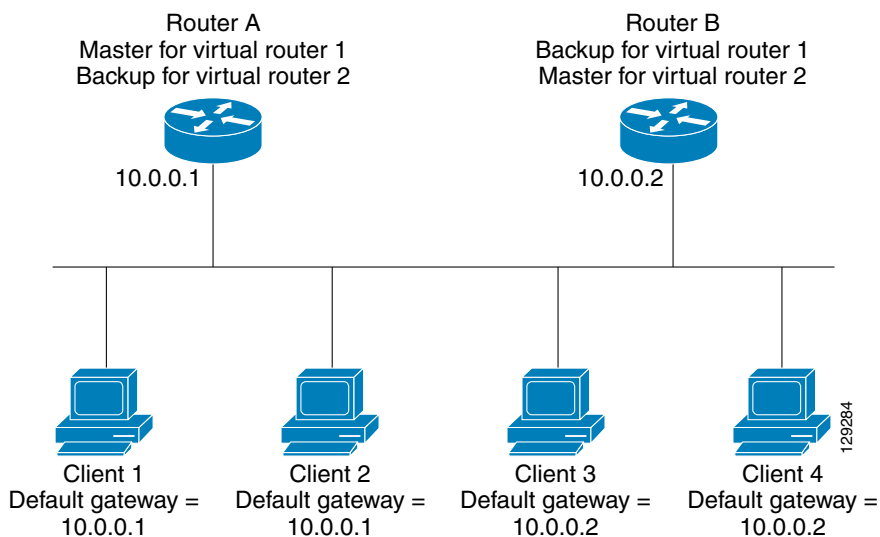
You can configure up to 255 VRRP groups on a physical interface. The actual number of VRRP groups that a router interface can support depends on the following factors:

- Router processing capability
- Router memory capability

In a topology where multiple VRRP groups are configured on a router interface, the interface can act as a master for one VRRP group and as a backup for one or more other VRRP groups.

Figure 18-2 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. Routers A and B act as backups to each other if either router fails.

Figure 18-2 Load Sharing and Redundancy VRRP Topology



This topology contains two virtual IP addresses for two VRRP groups that overlap. For VRRP group 1, Router A is the owner of IP address 10.0.0.1 and is the master. Router B is the backup to router A. Clients 1 and 2 are configured with the default gateway IP address of 10.0.0.1.

For VRRP group 2, Router B is the owner of IP address 10.0.0.2 and is the master. Router A is the backup to router B. Clients 3 and 4 are configured with the default gateway IP address of 10.0.0.2.

VRRP Router Priority and Preemption

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

If a VRRP router owns the virtual IP address and the IP address of the physical interface, this router functions as the master. The priority of the master is 255.

Priority also determines if a VRRP router functions as a backup router and the order of ascendancy to becoming a master if the master fails.

For example, if router A, the master in a LAN topology fails, VRRP must determine if backups B or C should take over. If you configure router B with priority 101 and router C with the default priority of 100, VRRP selects router B to become the master because it has the higher priority. If you configure routers B and C with the default priority of 100, VRRP selects the backup with the higher IP address to become the master.

VRRP uses preemption to determine what happens after a VRRP backup router becomes the master. With preemption enabled by default, VRRP will switch to a backup if that backup comes online with a priority higher than the new master. For example, if Router A is the master and fails, VRRP selects Router B (next in order of priority). If Router C comes online with a higher priority than Router B, VRRP selects Router C as the new master, even though Router B has not failed.

If you disable preemption, VRRP will only switch if the original master recovers or the new master fails.

BFD

VRRP supports Bidirectional forwarding detection (BFD). BFD is a detection protocol that provides fast forwarding-path failure detection times. BFD provides subsecond failure detection between two adjacent devices and can be less CPU-intensive than protocol hello messages because some of the BFD load can be distributed onto the data plane on supported modules. See the *Cisco Nexus 6000 Series NX-OS Interfaces Configuration Guide, Release 7.x* for more information.



Note

Currently, BFD is supported only on VRRPv2. It is not supported on VRRPv3.

vPC and VRRP

VRRP interoperates with virtual port channels (vPCs). vPCs allow links that are physically connected to two different Cisco Nexus 6000 Series switches to appear as a single port channel by a third switch. See the *Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide, Release 7.x*, for more information on vPCs.

A vPC forwards traffic through both the master VRRP router as well as the backup VRRP router. You can configure a threshold on the priority of the backup VRRP router to determine when traffic should failover to the vPC trunk. See the [“Configuring VRRP Priority” section on page 18-12](#).



Note

You should configure VRRP on the primary vPC peer switch as active and VRRP on the vPC secondary switch as standby.

vPC and VRRP

VRRP interoperates with virtual port channels (vPCs). vPCs allow links that are physically connected to two different Cisco Nexus 7000 series devices to appear as a single port channel by a third device. See the *Cisco Nexus 6000 Series NX-OS Layer 2 Switching Configuration Guide, Release 7.x* for more information on vPCs.

vPC forwards traffic through both the master VRRP router as well as the backup VRRP router. You can configure a threshold on the priority of the backup VRRP router to determine when traffic should failover to the vPC trunk. See the [“Configuring VRRP Priority” section on page 18-12](#).



Note

You should configure VRRP on the primary vPC peer device as master and VRRP on the vPC secondary device as backup.

VRRP Advertisements

The VRRP master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the master. Cisco NX-OS encapsulates the VRRP advertisements in IP packets and sends them to the IP multicast address assigned to the VRRP group. Cisco NX-OS sends the advertisements once every second by default, but you can configure a different advertisement interval.

VRRP Authentication

VRRP supports the following authentication mechanisms:

- No authentication
- Plain text authentication
- MD5 authentication

MD5 authentication provides greater security than plain text authentication. MD5 authentication allows each VRRP group member to use a secret key that you configure to generate a keyed MD5 hash of the outgoing packet. Cisco NX-OS generates a keyed hash of an incoming packet and if the generated hash does not match the hash within the incoming packet, Cisco NX-OS ignores the packet.

VRRP rejects packets in any of the following cases:

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

Restrictions

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 zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

VRRP Tracking

VRRP supports the following two options for tracking:

- Native interface tracking—Tracks the state of an interface and uses that state to determine the priority of the VRRP router in a VRRP group. The tracked state is down if the interface is down or if the interface does not have a primary IP address.
- Object tracking—Tracks the state of a configured object and uses that state to determine the priority of the VRRP router in a VRRP group. See [Chapter 19, “Configuring Object Tracking”](#) for more information on object tracking.

If the tracked state (interface or object) goes down, VRRP updates the priority based on what you configure the new priority to be for the tracked state. When the tracked state comes up, VRRP restores the original priority for the virtual router group.

For example, you may want to lower the priority of a VRRP group member if its uplink to the network goes down so another group member can take over as master for the VRRP group. See the [“Configuring VRRP Interface State Tracking” section on page 18-18](#) for more information.

**Note**

Currently, tracking is only supported on VRRPv2 and not on VRRPv3..

VRRPv3 and VRRS

VRRP version 3 (VRRPv3) enables a group of switches to form a single virtual switch in order to provide redundancy and reduce the possibility of a single point of failure in a network. The LAN clients can then be configured with the virtual switch as their default gateway. The virtual switch, representing a group of switches, is also known as a VRRPv3 group.

Virtual router redundancy service (VRRS) improves the scalability of VRRPv3 by providing a stateless redundancy service to VRRS pathways and VRRS clients by monitoring VRRPv3. VRRPv3 acts as a VRRS server that pushes VRRPv3 status information (such as current and previous redundancy states, active and inactive Layer 2 and Layer 3 addresses, and so on) to VRRS pathways and all registered VRRS clients.

VRRS clients are other Cisco processes or applications that use VRRPv3 to provide or withhold a service or resource dependent upon the state of the group. VRRS pathways are special VRRS clients that use the VRRS database information to provide scaled first-hop gateway redundancy across scaled interface environments.

VRRS by itself is limited to maintaining its own state. Linking a VRRS client to a VRRPv3 group provides a mechanism that allows VRRS to provide a service to client applications so that they can implement stateless or stateful failovers. A stateful failover requires communication with a nominated backup before the failure so that operational data is not lost when the failover occurs.

VRRS pathways operate in a similar way to clients but are integrated with the VRRS architecture. They provide a means to scale first-hop gateway redundancy by allowing you to configure a virtual address across hundreds of interfaces. The virtual gateway state of a VRRS pathway follows the state of a First-Hop Redundancy Protocol (FHRP) VRRS server.

VRRPv3 notifies VRRS of its current state (master, backup, or nonoperational initial state [INIT]) and passes that information to pathways or clients. The VRRPv3 group name activates VRRS and associates the VRRPv3 group with any clients or pathways that are configured as part of VRRS with the same name.

Pathways and clients act on the VRRPv3 server state. When a VRRPv3 group changes states, VRRS pathways and clients alter their behavior (performing tasks such as shutting down interfaces or appending accounting logs) depending on the state received from VRRS.

Virtualization Support

VRRP supports Virtual Routing and Forwarding instances (VRFs). VRFs exist within virtual device contexts (VDCs). By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF.

If you change the VRF membership of an interface, Cisco NX-OS removes all Layer 3 configuration, including VRRP.

For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x* and see [Chapter 12, “Configuring Layer 3 Virtualization.”](#)

Licensing Requirements for VRRP

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	VRRP requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the <i>Cisco DCNM Licensing Guide</i> .
Cisco NX-OS	VRRP requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .
	Note Make sure the LAN Base Services license is installed on the switch to enable Layer 3 interfaces.

Guidelines and Limitations

VRRP has the following configuration guidelines and limitations:

- You cannot configure VRRP on the management interface.
- When VRRP is enabled, you should replicate the VRRP configuration across switches in your network.
- We recommend that you do not configure more than one first-hop redundancy protocol on the same interface.
- You must configure an IP address for the interface that you configure VRRP on and enable that interface before VRRP becomes active.
- Cisco NX-OS removes all Layer 3 configurations on an interface when you change the interface VRF membership, port channel membership, or when you change the port mode to Layer 2.
- When you configure VRRP to track a Layer 2 interface, you must shut down the Layer 2 interface and reenabling the interface to update the VRRP priority to reflect the state of the Layer 2 interface.
- If the Layer 3 license is not installed on your Cisco Nexus 6000 device, VRRP can still be configured but will not function and a non-disruptive ISSU is not possible.
- All Layer 3 configuration must be removed from the Cisco Nexus 6000 device before clearing the Layer 3 license, including OSPF, PIM, and **no switchport** configurations. VRRP does not need to be removed before clearing the Layer 3 license but it is recommended that it be unconfigured first.

VRRPv3 has the following configuration guidelines and limitations:

- 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 only on Ethernet and Fast Ethernet interfaces, bridge group virtual interfaces (BVI), and Gigabit Ethernet interfaces as well as on Multiprotocol Label Switching (MPLS) virtual private networks (VPNs), VRF-aware MPLS VPNs, and VLANs.

- When VRRPv3 is in use, VRRPv2 is unavailable. To configure VRRPv3, you must disable any VRRPv2 configuration.
- VRRS is currently available only for use with VRRPv3.
- Use VRRPv3 millisecond timers only where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances. The millisecond timer values are compatible with third-party vendors, as long as they also support VRRPv3.
- Full network redundancy can be achieved only if VRRPv3 operates over the same network path as the VRRS pathway redundant interfaces. For full redundancy, the following restrictions apply:
 - VRRS pathways should use the same physical interface as the parent VRRPv3 group or be configured on a sub-interface with the same physical interface as the parent VRRPv3 group.
- VRRS pathways can be configured on switch virtual interfaces (SVIs) only if the associated VLAN shares the same trunk as the VLAN on which the parent VRRPv3 group is configured.

Default Settings

Table 18-1 lists the default settings for VRRP parameters.

Table 18-1 Default VRRP Parameters

Parameters	Default
advertisement interval	1 seconds
authentication	no authentication
preemption	enabled
priority	100
VRRP feature	disabled
VRRPv3	disabled
VRRS	disabled
VRRPv3 secondary address matching	enabled
Priority of a VRRPv3 group	100
VRRPv3 advertisement timer	1000 milliseconds

Configuring VRRP

This section includes the following topics:

- [Enabling the VRRP Feature, page 18-10](#)
- [Configuring VRRP Groups, page 18-10](#)
- [Configuring VRRP Priority, page 18-12](#)
- [Configuring VRRP Authentication, page 18-14](#)
- [Configuring Time Intervals for Advertisement Packets, page 18-15](#)
- [Disabling Preemption, page 18-17](#)
- [Configuring VRRP Interface State Tracking, page 18-18](#)

**Note**

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Enabling the VRRP Feature

You must globally enable the VRRP feature before you can configure and enable any VRRP groups.

To enable the VRRP feature, use the following command in global configuration mode:

Command	Purpose
feature vrrp	Enables VRRP.
Example: switch(config)# feature vrrp	

To disable the VRRP feature in a VDC and remove all associated configuration, use the following command in global configuration mode:

Command	Purpose
no feature vrrp	Disables the VRRP feature.
Example: switch(config)# no feature vrrp	

Configuring VRRP Groups

You can create a VRRP group, assign the virtual IP address, and enable the group.

You can configure one virtual IPv4 address for a VRRP group. By default, the master VRRP router drops the packets addressed directly to the virtual IP address because the VRRP master is only intended as a next-hop router to forward packets. Some applications require that Cisco NX-OS accept packets addressed to the virtual router IP. Use the secondary option to the virtual IP address to accept these packets when the local router is the VRRP master.

Once you have configured the VRRP group, you must explicitly enable the group before it becomes active.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that you configure an IP address on the interface (see the [“Configuring IPv4 Addressing”](#) section on page 2-8).

SUMMARY STEPS

1. **configure terminal**
2. **interface interface-type slot/port**
3. **no switchport**

4. **vrrp** *number*
5. **address** *ip-address* [**secondary**]
6. **no shutdown**
7. (Optional) **show vrrp**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# switch(config-if)# interface ethernet 2/1	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	vrrp <i>number</i> Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group. The range is from 1 to 255.
Step 5	address <i>ip-address</i> [secondary] Example: switch(config-if-vrrp)# address 192.0.2.8	Configures the virtual IPv4 address for the specified VRRP group. This address should be in the same subnet as the IPv4 address of the interface. Use the secondary option only if applications require that VRRP routers accept the packets sent to the virtual router's IP address and deliver to applications.
Step 6	no shutdown Example: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.

	Command	Purpose
Step 7	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays VRRP information.
Step 8	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring VRRP Priority

The valid priority range for a virtual router is from 1 to 254 (1 is the lowest priority and 254 is the highest). The default priority value for backups is 100. For switches whose interface IP address is the same as the primary virtual IP address (the master), the default value is 255.

If you configure VRRP on a vPC-enabled interface, you can optionally configure the upper and lower threshold values to control when to fail over to the vPC trunk. If the backup router priority falls below the lower threshold, VRRP sends all backup router traffic across the vPC trunk to forward through the master VRRP router. VRRP maintains this scenario until the backup VRRP router priority increases above the upper threshold.

BEFORE YOU BEGIN

Ensure that you have enabled the VRRP feature (see the [“Configuring VRRP” section on page 18-9](#)).

Ensure that you have configured an IP address on the interface (see the [“Configuring IPv4 Addressing” section on page 2-8](#)).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **priority** *level* [**forwarding-threshold** **lower** *lower-value* **upper** *upper-value*]
7. **no shutdown**
8. (Optional) **show vrrp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	vrrp <i>number</i> Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 5	shutdown Example: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 6	priority <i>level</i> [forwarding-threshold lower <i>lower-value</i> upper <i>upper-value</i>] Example: switch(config-if-vrrp)# priority 60 forwarding-threshold lower 40 upper 50	Sets the priority level used to select the active router in an VRRP group. The <i>level</i> range is from 1 to 254. The default is 100 for backups and 255 for a master that has an interface IP address equal to the virtual IP address. Optionally, sets the upper and lower threshold values used by vPC to determine when to fail over to the vPC trunk. The <i>lower-value</i> range is from 1 to 255. The default is 1. The <i>upper-value</i> range is from 1 to 255. The default is 255.
Step 7	no shutdown Example: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 8	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 9	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring VRRP Authentication

You can configure simple text authentication or MDS authentication for a VRRP group. You configure the MD5 authentication using a key string and the security parameter index (SPI). The receiving router uses SPI to identify the security association (SA) to which an incoming packet is bound. VRRP only verifies the MD5 digest.

BEFORE YOU BEGIN

Ensure that the authentication configuration is identical for all VRRP switches in the network.

Ensure that you have enabled the VRRP feature (see the “[Configuring VRRP](#)” section on page 18-9).

Ensure that you have configured an IP address on the interface (see the “[Configuring IPv4 Addressing](#)” section on page 2-8).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **authentication**{**md5** *keyname spi index*| **text** *password*}
7. **no shutdown**
8. (Optional) **show vrrp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.

	Command	Purpose
Step 4	vrrp <i>number</i> Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 5	shutdown Example: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 6	authentication text <i>password</i> Example: switch(config-if-vrrp)# authentication md5 prd555o1n47espn0 spi 0x0	Assigns the simple text authentication option and specifies the keyname password. The keyname range is from 1 to 255 characters. We recommend that you use at least 16 characters. The text password is up to eight alphanumeric characters.
Step 7	no shutdown Example: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 8	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 9	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring Time Intervals for Advertisement Packets

You can configure the time intervals for advertisement packets.

BEFORE YOU BEGIN

Ensure that you have enabled the VRRP feature (see the [“Configuring VRRP” section on page 18-9](#)).

Ensure that you have configured an IP address on the interface (see the [“Configuring IPv4 Addressing” section on page 2-8](#)).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **advertisement-interval** *seconds*

7. **no shutdown**
8. (Optional) **show vrrp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	vrrp number Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 5	shutdown Example: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 6	advertisement-interval <i>seconds</i> Example: switch(config-if-vrrp)# advertisement-interval 15	Sets the interval time in seconds between sending advertisement frames. The range is from 1 to 254. The default is 1 second.
Step 7	no shutdown Example: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 8	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 9	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Disabling Preemption

You can disable preemption for a VRRP group member. If you disable preemption, a higher-priority backup router will not take over for a lower-priority master router. Preemption is enabled by default.

BEFORE YOU BEGIN

Ensure that you have enabled the VRRP feature (see the [“Configuring VRRP” section on page 18-9](#)).

Ensure that you have configured an IP address on the interface (see the [“Configuring IPv4 Addressing” section on page 2-8](#)).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **no preempt**
7. **no shutdown**
8. (Optional) **show vrrp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	vrrp <i>number</i> Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.

	Command	Purpose
Step 5	no shutdown Example: switch(config-if-vrrp)# no shutdown	Enables the VRRP group. Disabled by default.
Step 6	no preempt Example: switch(config-if-vrrp)# no preempt	Disables the preempt option and allows the master to remain when a higher-priority backup appears.
Step 7	no shutdown Example: switch(config-if-vrrp)# no shutdown	Enables the VRRP group. Disabled by default.
Step 8	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 9	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Configuring VRRP Interface State Tracking

Interface state tracking changes the priority of the virtual router based on the state of another interface in the switch. When the tracked interface goes down or the IP address is removed, Cisco NX-OS assigns the tracking priority value to the virtual router. When the tracked interface comes up and an IP address is configured on this interface, Cisco NX-OS restores the configured priority to the virtual router (see the [“Configuring VRRP Priority”](#) section on page 18-12).



Note

For interface state tracking to function, you must enable preemption on the interface.



Note

VRRP does not support Layer 2 interface tracking.

BEFORE YOU BEGIN

- Ensure that you have enabled the VRRP feature (see the [“Configuring VRRP”](#) section on page 18-9).
- Ensure that you have configured an IP address on the interface (see the [“Configuring IPv4 Addressing”](#) section on page 2-8).
- Ensure that you have enabled the virtual router (see the [“Configuring VRRP Groups”](#) section on page 18-10).
- Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **configure terminal**

2. **interface** *interface-type slot/port*
3. **no switchport**
4. **vrrp** *number*
5. **shutdown**
6. **track interface** *type number priority value*
7. **no shutdown**
8. (Optional) **show vrrp**
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters configuration mode.
Step 2	interface <i>interface-type slot/port</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> .
Step 3	no switchport Example: switch(config-if)# no switchport	Configures the interface as a Layer 3 routed interface.
Step 4	vrrp <i>number</i> Example: switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 5	shutdown Example: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 6	track interface <i>type number priority value</i> Example: switch(config-if-vrrp)# track interface ethernet 2/10 priority 254	Enables interface priority tracking for a VRRP group. The priority range is from 1 to 254.
Step 7	no shutdown Example: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.

	Command	Purpose
Step 8	show vrrp Example: switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 9	copy running-config startup-config Example: switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Enabling VRRPv3 feature

BEFORE YOU BEGIN

You must globally enable the VRRPv3 feature before you configure and enable any VRRPv3 group.

The following are the steps to enable VRRPv3 feature:

-
- Step 1** Enter global configuration mode:
- ```
switch# configure terminal
```
- Step 2** Enable VRRP version 3 and Virtual Router Redundancy Service (VRRS). The no form of this command disables VRRPv3 and VRRS in a VDC:
- ```
switch(config)# feature vrrpv3
```

If VRRPv2 is currently configured, use the **no feature vrrp** command in global configuration mode to remove the VRRPv2 configuration and then use the **feature vrrpv3** command to enable VRRPv3.

Configuring VRRPv3 Groups

You can create a VRRPv3 group, assign a virtual IP address and enable the group.

BEFORE YOU BEGIN

- Ensure that VRRPv3 feature is enabled.
- Ensure that you configure an IP address on the interface.

The following are the steps to configure a VRRPv3 group:

-
- Step 1** Enter global configuration mode:
- ```
switch# configure terminal
```
- Step 2** Enter interface configuration mode:
- ```
switch(config)# interface type/number
```

- Step 3** Create VRRPv3 group and enter VRRPv3 group configuration mode. The range is from 1 to 255:
- ```
switch(config-if)# vrrpv3 number address-family [ipv4 | ipv6]
```
- Step 4** (Optional) Specify a primary or secondary IPv4 or IPv6 address for the VRRPv3 group. To utilize secondary IP addresses in a VRRPv3 group, you must first configure a primary IP address on the same group:
- ```
switch(config-if-vrrpv3-group)# address ip-address [primary | secondary]
```
- Step 5** (Optional) Specify a description for the VRRPv3 group. You can enter up to 80 alphanumeric characters:
- ```
switch(config-if-vrrpv3-group)# description description
```
- Step 6** (Optional) Match the secondary address in the advertisement packet against the configured address:
- ```
switch(config-if-vrrpv3-group)# match-address
```
- Step 7** (Optional) Enable the preemption of a lower priority master switch with an optional delay. The range is from 0 to 3600:
- ```
switch(config-if-vrrpv3-group)# preempt [delay minimum seconds]
```
- Step 8** (Optional) Specify the priority of VRRPv3 group. The range is from 1 to 254:
- ```
switch(config-if-vrrpv3-group)# priority level
```
- Step 9** (Optional) Set the advertisement timer in milliseconds. The range is from 100 to 40950. Cisco recommends that you set this timer to a value greater than or equal to 1 second:
- ```
switch(config-if-vrrpv3-group)# timers advertise interval
```
- Step 10** (Optional) Enable support for VRRPv2 simultaneously, to ensure interoperability with devices that support only VRRPv2:
- ```
switch(config-if-vrrpv3-group)# vrrp2
```
- VRRPv2 compatibility mode is provided to allow an upgrade from VRRPv2 to VRRPv3. This is not a full VRRPv2 implementation and should be used only to perform an upgrade.
- Step 11** (Optional) Specify a leader's name to be registered with VRRS:
- ```
switch(config-if-vrrpv3-group)# vrrs leader vrrs-leader-name
```
- Step 12** (Optional) Disable VRRP configuration for VRRPv3 group:
- ```
switch(config-if-vrrpv3-group)# shutdown
```
- Step 13** (Optional) Display First Hop Redundancy Protocol (FHRP) information. Use the verbose keyword to view detailed information:
- ```
switch(config-if-vrrpv3-group)# show fhrp [interface-type interface-number] [verbose]
```
- Step 14** (Optional) Save this configuration change:
- ```
switch(config-if-vrrpv3-group)# copy running-config startup-config
```

The following example shows how to create a VRRPv3 group:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# vrrpv3 5 address-family ipv4
switch(config-if)# hsrp version 2
switch(config-if-vrrpv3-group)# address 100.0.1.10 primary
switch(config-if-vrrpv3-group)# description group3
switch(config-if-vrrpv3-group)# match-address
switch(config-if-vrrpv3-group)# preempt delay minimum 30
switch(config-if-vrrpv3-group)# priority 3
switch(config-if-vrrpv3-group)# timers advertise 1000
switch(config-if-vrrpv3-group)# vrrp2
switch(config-if-vrrpv3-group)# vrrs leader leader1
switch(config-if-vrrpv3-group)# shutdown
switch(config-if-vrrpv3-group)# show fhrp ethernet 1/2 verbose
switch(config-if-vrrpv3-group)# show running-config startup-config
```

Configuring VRRPv3 Control Group

BEFORE YOU BEGIN

- Ensure that the VRRPv3 feature is enabled.
- Ensure that you configure an IP address on the interface.

The following are the steps to configure VRRPv3 control group:

Step 1 Enter global configuration mode:

```
switch# configure terminal
```

Step 2 Enter interface configuration mode:

```
switch(config)# interface type/number
```

Step 3 Configure IP address on the interface. You can use the **secondary** keyword to configure additional IP addresses on the interface:

```
switch(config-if)# ip address ip-address mask [secondary]
```

Step 4 Create a VRRPv3 group and enter VRRPv3 group configuration mode. The range is from 1 to 255:

```
switch(config-if)# vrrpv3 number address-family [ipv4 | ipv6]
```

Step 5 (Optional) Specify a primary or secondary IPv4 or IPv6 address for the VRRPv3 group:

```
switch(config-if-vrrpv3-group)# address ip-address [primary | secondary]
```

Step 6 (Optional) Specify a leader's name to be registered with VRRS:

```
switch(config-if-vrrpv3-group)# vrrs leader vrrs-leader-name
```

Step 7 (Optional) Disable VRRP configuration for VRRPv3 group:

```
switch(config-if-vrrpv3-group)# shutdown
```

- Step 8** (Optional) Display First Hop Redundancy Protocol (FHRP) information. Use the **verbose** keyword to view detailed information:

```
switch(config-if-vrrpv3-group)# show fhrp [interface-type interface-number] [verbose]
```

- Step 9** (Optional) Save this configuration change:

```
switch(config-if-vrrpv3-group)# copy running-config startup-config
```

The following example shows how to configure a VRRPv3 control group:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 209.165.200.230 255.255.255.224
switch(config-if)# vrrpv3 5 address-family ipv4
switch(config-if-vrrpv3-group)# address 209.165.200.227 primary
switch(config-if-vrrpv3-group)# vrrs leader leader1
switch(config-if-vrrpv3-group)# shutdown
switch(config-if-vrrpv3-group)# show fhrp ethernet 1/2 verbose
switch(config-if-vrrpv3-group)# show running-config startup-config
```

Configuring VRRS Pathways

You can configure a Virtual Router Redundancy Service (VRRS) pathway. In scaled environments, VRRS pathways should be used in combination with VRRPv3 control groups.

BEFORE YOU BEGIN

- Ensure that the VRRPv3 feature is enabled.
- Ensure that you configure an IP address on the interface.

The following are the steps to configure VRRS pathways:

- Step 1** Enter global configuration mode:

```
switch# configure terminal
```

- Step 2** Enter interface configuration mode:

```
switch(config)# interface type/number
```

- Step 3** Configure IP address on the interface. You can use the **secondary** keyword to configure additional IP addresses on the interface:

```
switch(config-if)# ip address ip-address mask [secondary]
```

- Step 4** Define VRRS pathway for a VRRS group and enter VRRS pathway configuration mode:

```
switch(config-if)# vrrs pathway vrrs-tag
```

The **vrrs-tag** argument specifies the name of the VRRS tag that is being associated with the pathway.

Step 5 Specify a MAC address for the pathway:

```
switch(config-if-vrrs-pw)# mac address {mac-address | inherit}
```

The **inherit** keyword causes the pathway to inherit the virtual MAC address of the VRRPv3 group with which the pathway is associated.

Step 6 Define the virtual IPv4 or IPv6 address for a pathway:

```
switch(config-if-vrrs-pw)# address ip-address
```

A VRRPv3 group is capable of controlling more than one pathway.

Step 7 (Optional) Display the VRRS pathway information for different pathway states, such as active, inactive, and not ready:

```
switch(config-if-vrrs-pw)# show vrrs pathway interface-type interface-number
```

Step 8 (Optional) Save this configuration change:

```
switch(config-if-vrrs-pw)# copy running-config startup-config
```

The following example shows how to configure a VRRS pathways:

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 209.165.200.230 255.255.255.224
switch(config-if)# vrrpvs pathway path1
switch(cofig-if-vrrs-pw)# mac address fe24.fe24.fe24
switch(cofig-if-vrrs-pw)# address 209.165.201.10
switch(cofig-if-vrrs-pw)# show vrrs pathway ethernet 1/2 verbose
switch(cofig-if-vrrs-pw)# show running-config startup-config
```

Verifying the VRRP Configuration

To display the VRRP configuration information, perform one of the following tasks:

Command	Purpose
show vrrp	Displays the VRRP status for all groups.
show vrrp vr <i>group-number</i>	Displays the VRRP status for a VRRP group.
show vrrp vr <i>number interface interface-type port configuration</i>	Displays the virtual router configuration for an interface.
show vrrp vr <i>number interface interface-type port status</i>	Displays the virtual router status for an interface.

Displaying VRRP Statistics

To display VRRP statistics, use the following commands:

Command	Purpose
show vrrp vr <i>number</i> interface <i>interface-type</i> port statistics	Displays the virtual router information.
show vrrp statistics	Displays the VRRP statistics.

Use the **clear vrrp statistics** command to clear all the VRRP statistics for all interfaces in the switch.

Use the **clear vrrp vr** command to clear the IPv4 VRRP statistics for a specified interface.

Use the **clear vrrp ipv4** command to clear all the statistics for the specified IPv4 virtual router.

Configuration Examples for VRRP

In this 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 master for this group with priority 120.
 - Advertising interval is 3 seconds.
 - Preemption is enabled.
- Group 5:
 - Router B will become the master for this group with priority 200.
 - Advertising interval is 30 seconds.
 - Preemption is enabled.
- Group 100:
 - Router A will become the master 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

```
interface ethernet 1/0
  no switchport
  ip address 10.1.0.2/16
  no shutdown
  vrrp 1
    priority 120
    authentication text cisco
    advertisement-interval 3
    address 10.1.0.10
    no shutdown
  vrrp 5
    priority 100
```

```

    advertisement-interval 30
    address 10.1.0.50
    no shutdown
vrrp 100
    no preempt
    address 10.1.0.100
    no shutdown

```

Router B

```

interface ethernet 1/0
  no switchport
  ip address 10.2.0.1/2
  no shutdown
  vrrp 1
    priority 100
    authentication text cisco
    advertisement-interval 3
    address 10.2.0.10
    no shutdown

  vrrp 5
    priority 200
    advertisement-interval 30
    address 10.2.0.50
    no shutdown
  vrrp 100
    no preempt
    address 10.2.0.100
    no shutdown

```

The following example shows how to enable VRRPv3, and create and customize a VRRPv3 group:

```

configure terminal
feature vrrp
interface ethernet 4/6
  vrrpv3 5 address-family ipv4
  address 209.165.200.255 primary
  description group3
  match-address
  preempt delay minimum 30

```

Additional References

For additional information related to implementing VRRP, see the following sections:

- [Related Documents, page 18-27](#)

Related Documents

Related Topic	Document Title
Configuring the gateway load balancing protocol	Chapter 18, “Configuring GLBP”
Configuring the Hot Standby Routing Protocol	Chapter 17, “Configuring HSRP”
VRRP CLI commands	<i>Cisco Nexus 6000 Series Command Reference, Cisco NX-OS Releases 7.x</i>

