CHAPTER 20

Configuring VRRP

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

This chapter includes the following sections:

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 in the event that the master router fails.

This section includes the following topics:

- Virtualization Support, page 20-6

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.

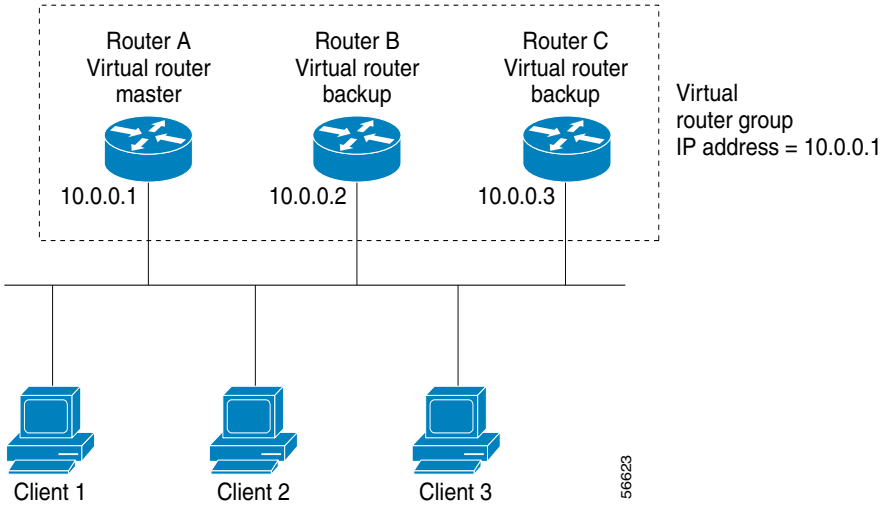
The disadvantage to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

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 20-1 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 20-1 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 r 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 r master again. For more information, see the "VRRP Router Priority and Preemption" section.

Note In Cisco NX-OS Release 4.1(2) and later, packets 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.
- 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.

Multiple VRRP Groups

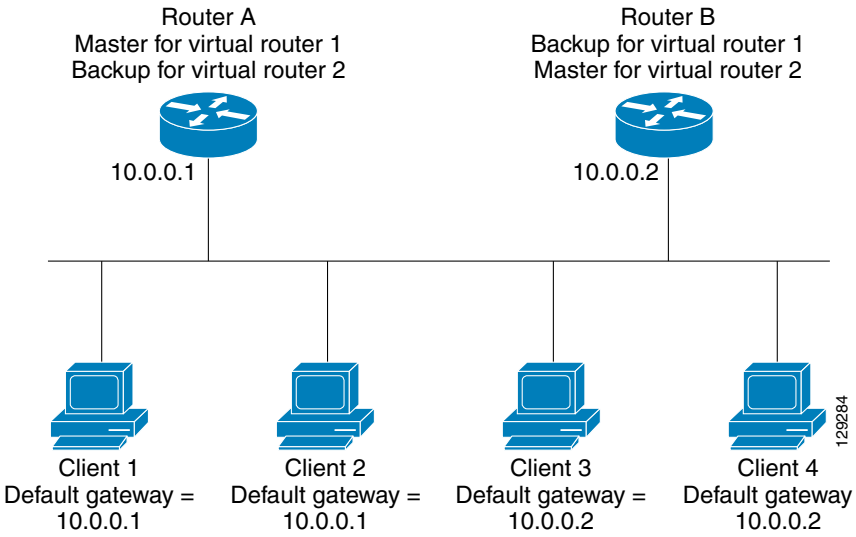
You can configure up to 255 VRRP groups on a physical interface. The actual number of VRRP groups that a router interface can support depends on the following factors:

- 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 20-2 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 20-2 Load Sharing and Redundancy VRRP Topology



In 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.

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 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.x* for more information on vPCs.

vPC forwards traffic through both the master VRRP router as well as the backup VRRP router. See the "Configuring VRRP Priority" section on page 20-9.

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

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

VRRP rejects packets in any of the following cases:

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

VRRP Tracking

VRRP supports the following two options for tracking:

- Native interface tracking— Tracks the state of an interface and use 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 use that state to determine the priority of the VRRP router in a VRRP group. See Chapter 21, "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 20-17 for more information.

Note VRRP does not support Layer 2 interface tracking.

High Availability

VRRP supports stateful restarts and stateful switchover. A stateful restart occurs when the VRRP process fails and is restarted. Stateful switchover occurs when the active supervisor switches to the standby supervisor. Cisco NX-OS applies the run-time configuration after the switchover.

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 4.x* and see Chapter 14, "Configuring Layer 3 Virtualization."

Licensing Requirements for VRRP

The following table shows the licensing requirements for this feature:

Product	License Requirement
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 NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations

VRRP has the following guidelines and limitations:

- You cannot configure VRRP on the management interface.
- When VRRP is enabled, you should replicate the VRRP configuration across devices 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 configuration 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 reenable the interface to update the VRRP priority to reflect the state of the Layer 2 interface.

Configuring VRRP

This section includes the following topics:

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 **Example:** `switch(config)# feature vrrp`	Enables 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 **Example:** `switch(config)# no feature vrrp`	Disables the VRRP feature in a VDC.

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 2-7.

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **vrrp** *number*
4. **address** *ip-address* [**secondary**]
5. **no shutdown**

6. **show vrrp**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# switch(config-if)# interface ethernet 2/1	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group. The range is from 1 to 255.
Step 4	**address** *ip-address* [**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 5	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 6	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	(Optional) Displays VRRP information.
Step 7	**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 devices whose interface IP address is the same as the primary virtual IP address (the master), the default value is 255.

f 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 20-7).

Ensure that you have configured an IP address on the interface (see the "Configuring IPv4 Addressing" section on page 2-7.

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

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 4	**shutdown** **Example**: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 5	**priority** *level* [**forwarding-threshold lower** *lower-value* **upper** *upper-value*] **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 *level* 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 *lower-value* range is from 1 to 255. The default is 1. The *upper-value* range is from 1 to 255. The default is 255.
Step 6	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 7	**show vrrp** ***Example:*** switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of 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 Authentication

You can configure simple text authentication for a VRRP group.

BEFORE YOU BEGIN

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

Ensure that you have enabled the VRRP feature (see the "Configuring VRRP" section on page 20-7).

Ensure that you have configured an IP address on the interface (see the "Configuring IPv4 Addressing" section on page 2-7.

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

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **vrrp** *number*
4. **shutdown**
5. **authentication text** *password*
6. **no shutdown**
7. **show vrrp**
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 4	**shutdown** **Example**: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 5	**authentication text** *password* **Example:** switch(config-if-vrrp)# authentication md5 prd555oln47espn0 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 6	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 7	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of 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 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 20-7).

Ensure that you have configured an IP address on the interface (see the "Configuring IPv4 Addressing" section on page 2-7.

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

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **vrrp** *number*
4. **shutdown**
5. **advertisement-interval** *seconds*
6. **no shutdown**
7. **show vrrp**
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 4	**shutdown** **Example**: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 5	**advertisement-interval** *seconds* **Example:** switch(config-if-vrrp)# advertisement-interval 15	Sets the interval time in seconds between sending advertisement frames. The range is from 1 to 255. The default is 1 second.
Step 6	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 7	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 8	**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 back up 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 20-7).

Ensure that you have configured an IP address on the interface (see the "Configuring IPv4 Addressing" section on page 2-7.

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

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **vrrp** *number*
4. **shutdown**
5. **no preempt**
6. **no shutdown**
7. **show vrrp**
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 4	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown	Enables the VRRP group. Disabled by default.
Step 5	**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 6	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown	Enables the VRRP group. Disabled by default.
Step 7	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of 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 Interface State Tracking

Interface state tracking changes the priority of the virtual router based on the state of another interface in the device. 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 20-9).

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 20-7).

Ensure that you have configured an IP address on the interface (see the "Configuring IPv4 Addressing" section on page 2-7.

Ensure that you have enabled the virtual router (see the "Configuring VRRP Groups" section on page 20-8).

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

SUMMARY STEPS

1. **config t**
2. **interface** *interface-type slot/port*
3. **vrrp** *number*
4. **shutdown**
5. **track interface** *type number* **priority** *value*
6. **no shutdown**
7. **show vrrp**
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters configuration mode.
Step 2	**interface** *interface-type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode.
Step 3	**vrrp** *number* **Example:** switch(config-if)# vrrp 250 switch(config-if-vrrp)#	Creates a virtual router group.
Step 4	**shutdown** **Example**: switch(config-if-vrrp)# shutdown switch(config-if-vrrp)#	Disables the VRRP group. Disabled by default.
Step 5	**track interface** type *number* **priority** *value* **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 6	**no shutdown** **Example**: switch(config-if-vrrp)# no shutdown switch(config-if-vrrp)#	Enables the VRRP group. Disabled by default.
Step 7	**show vrrp** **Example:** switch(config-if-vrrp)# show vrrp	(Optional) Displays a summary of VRRP information.
Step 8	**copy running-config startup-config** **Example:** switch(config-if-vrrp)# copy running-config startup-config	(Optional) Saves this configuration change.

Verifying the VRRP Configuration

To verify VRRP configuration information, use the following commands:

Command	Purpose
show vrrp	Displays the VRRP status for all groups.
show vrrp vr *group-number*	Displays the VRRP status for a VRRP group.

Command	Purpose
show vrrp vr *number* **interface** *interface-type port* **configuration**	Displays the virtual router configuration for an interface.
show vrrp vr *number* **interface** *interface-type port* **status**	Displays the virtual router status for an interface.

Displaying VRRP Statistics

To display VRRP statistics, use the following commands:

Command	Purpose
show vrrp vr *number* **interface** *interface-type 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 device.

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.

VRRP Example Configuration

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
   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
 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
```

Default Settings

Table 20-1 lists the default settings for VRRP parameters.

Table 20-1 Default VRRP Parameters

Parameters	Default
advertisement interval	1 seconds
authentication	no authentication
preemption	enabled
priority	100
VRRP feature	disabled

Additional References

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

- Related Documents, page 20-22

Related Documents

Related Topic	Document Title
Configuring the gateway load balancing protocol	Chapter 18, “Configuring GLBP”
Configuring the hot standby routing protocol	Chapter 19, “Configuring HSRP”
VRRP CLI commands	*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*
Configuring high availability	*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*

Feature History for VRRP

Table 20-2 lists the release history for this feature.

Table 20-2 Feature History for VRRP

Feature Name	Releases	Feature Information
VRRP priority thresholds	4.2(1)	Added support for priority thresholds and vPC.
VRRP object tracking	4.2(1)	Added support for tracking multiple object types in VRRP.
VRRP	4.0(1)	This feature was introduced.