



Configuring VRRP

Last Updated: December 20, 2011

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 router master, with the other routers acting as backups in case the virtual router master fails.

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

- [Finding Feature Information, page 1](#)
- [Restrictions for VRRP, page 1](#)
- [Information About VRRP, page 2](#)
- [How to Configure VRRP, page 8](#)
- [Configuration Examples for VRRP, page 24](#)
- [Additional References, page 27](#)
- [Feature Information for VRRP, page 28](#)
- [Glossary, page 31](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for VRRP

- VRRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. VRRP is not intended as a replacement for existing dynamic protocols.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- VRRP is supported on Ethernet, Fast Ethernet, Bridge Group Virtual Interface (BVI), and Gigabit Ethernet interfaces, and on Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs), VRF-aware MPLS VPNs, and VLANs.
- Because of the forwarding delay that is associated with the initialization of a BVI interface, you must configure the VRRP advertise timer to a value equal to or greater than the forwarding delay on the BVI interface. This setting prevents a VRRP router on a recently initialized BVI interface from unconditionally taking over the master role. Use the **bridge forward-time** command to set the forwarding delay on the BVI interface. Use the **vrrp timers advertise** command to set the VRRP advertisement timer.
- Enhanced Object Tracking (EOT) is not stateful switchover (SSO)-aware and cannot be used with VRRP in SSO mode.

Information About VRRP

- [VRRP Operation, page 2](#)
- [VRRP Benefits, page 4](#)
- [Multiple Virtual Router Support, page 5](#)
- [VRRP Router Priority and Preemption, page 5](#)
- [VRRP Advertisements, page 6](#)
- [VRRP Object Tracking, page 6](#)
- [How Object Tracking Affects the Priority of a VRRP Router, page 6](#)
- [VRRP Authentication, page 7](#)
- [In Service Software Upgrade--VRRP, page 7](#)
- [VRRP Support for Stateful Switchover, page 7](#)

VRRP Operation

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

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

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

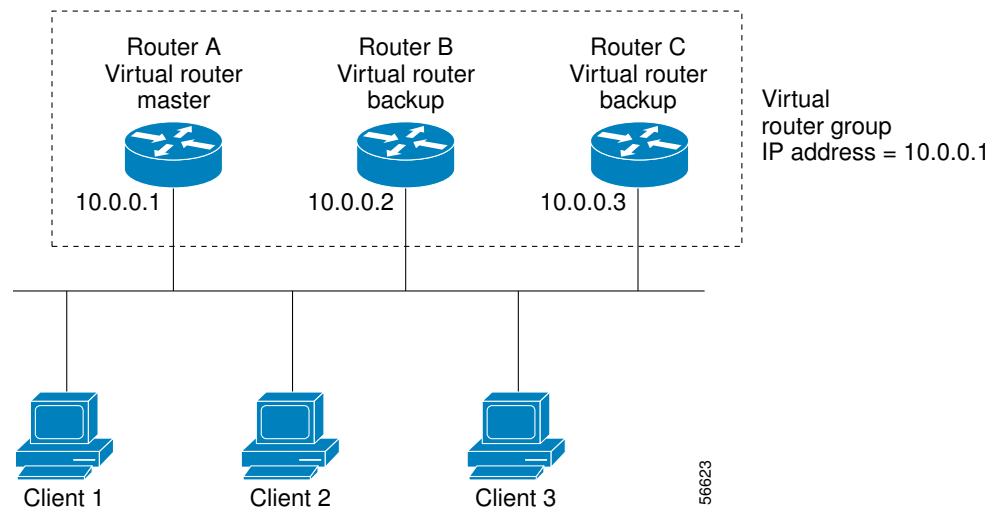
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network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

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

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

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

Figure 1 Basic VRRP Topology

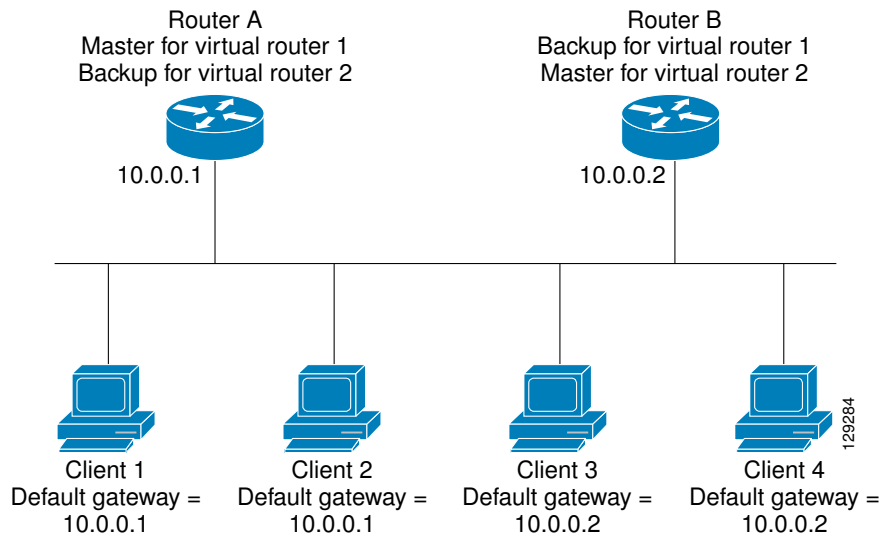


Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual router master and is also known as the IP address owner. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 10.0.0.1.

Routers B and C function as virtual router backups. If the virtual router master fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the [VRRP Router Priority and Preemption, page 5](#) 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, page 5](#) 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

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

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 router master 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 router master 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

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

- 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 a master 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 router master 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 router master.

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

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 router master. 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 router master remains the master until the original virtual router master recovers and becomes master again.

VRRP Advertisements

The virtual router master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual router master. The VRRP advertisements are encapsulated 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 master 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.

VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process provides the ability to track individual objects such as a the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP router. You specify the object number to be tracked and VRRP will be notified of any change to the object. VRRP increments (or decrements) the priority of the virtual router based on the state of the object being tracked.

How Object Tracking Affects the Priority of a VRRP Router

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 VRRP, 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 VRRP priority is reduced. The VRRP router with the higher priority can now become the

virtual router master if it has the **vrrp preempt** command configured. See the [VRRP Object Tracking, page 6](#) section for more information on object tracking.

VRRP Authentication

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

You can configure VRRP text authentication, authentication using a simple MD5 key string, or MD5 key chains for authentication.

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

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

A router will ignore incoming VRRP packets from routers that do not have the same authentication configuration for a VRRP group. VRRP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

VRRP packets will be rejected 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.

In Service Software Upgrade--VRRP

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

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

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

VRRP Support for Stateful Switchover

With the introduction of the VRRP Support for Stateful Switchover feature, VRRP is SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual Route Processors (RPs). SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the

standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Prior to being SSO aware, if VRRP was deployed on a router with redundant RPs, a switchover of roles between the active RP and the standby RP would result in the router relinquishing its activity as a VRRP group member and then rejoining the group as if it had been reloaded. The SSO--VRRP feature enables VRRP to continue its activities as a group member during a switchover. VRRP state information between redundant RPs is maintained so that the standby RP can continue the router's activities within the VRRP during and after a switchover.

This feature is enabled by default. To disable this feature, use the **no vrrp sso** command in global configuration mode.

For more information, see the Stateful Switchover document.

How to Configure VRRP

- [Customizing VRRP, page 8](#)
- [Enabling VRRP, page 10](#)
- [Disabling a VRRP Group on an Interface, page 12](#)
- [Configuring VRRP Object Tracking, page 13](#)
- [Configuring VRRP MD5 Authentication Using a Key String, page 15](#)
- [Configuring VRRP MD5 Authentication Using a Key Chain, page 17](#)
- [Verifying the VRRP MD5 Authentication Configuration, page 20](#)
- [Configuring VRRP Text Authentication, page 21](#)
- [Enabling the Router to Send SNMP VRRP Notifications, page 23](#)

Customizing 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 router master 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp group description** *text*
6. **vrrp group priority** *level*
7. **vrrp group preempt** [*delay minimum seconds*]
8. **vrrp group timers advertise** [*msec*] *interval*
9. **vrrp group timers learn**
10. **exit**
11. **no vrrp sso**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface GigabitEthernet 0/0/0	Enters interface configuration mode.
Step 4	ip address <i>ip-address mask</i> 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 <i>text</i> Example: Router(config-if)# vrrp 10 description working-group	Assigns a text description to the VRRP group.
Step 6	vrrp group priority <i>level</i> Example: Router(config-if)# vrrp 10 priority 110	Sets the priority level of the router within a VRRP group. <ul style="list-style-type: none"> The default priority is 100.
Step 7	vrrp group preempt [<i>delay minimum seconds</i>] Example: Router(config-if)# vrrp 10 preempt delay minimum 380	Configures the router to take over as virtual router master for a VRRP group if it has a higher priority than the current virtual router master. <ul style="list-style-type: none"> The default delay period is 0 seconds. The router that is IP address owner will preempt, regardless of the setting of this command.

	Command or Action	Purpose
Step 8	vrrp group timers advertise [msec] interval Example: Router(config-if)# vrrp 10 timers advertise 110	Configures the interval between successive advertisements by the virtual router master in a VRRP group. <ul style="list-style-type: none"> The unit of the interval is in seconds unless the msec keyword is specified. The default <i>interval</i> value is 1 second. Note All routers in a VRRP group must use the same timer values. If the same timer values are not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.
Step 9	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 router master.
Step 10	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 11	no vrrp sso Example: Router(config)# no vrrp sso	(Optional) Disables VRRP support of SSO. <ul style="list-style-type: none"> VRRP support of SSO is enabled by default.

Enabling VRRP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp group ip** *ip-address* [**secondary**]
6. **end**
7. **show vrrp** [**brief**] | *group*
8. **show vrrp interface** *type number* [**brief**]

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>interface type number</code> Example: <pre>Router(config)# interface GigabitEthernet 0/0/0</pre>	Enters interface configuration mode.
Step 4 <code>ip address ip-address mask</code> Example: <pre>Router(config-if)# ip address 172.16.6.5 255.255.255.0</pre>	Configures an IP address for an interface.
Step 5 <code>vrrp group ip ip-address [secondary]</code> Example: <pre>Router(config-if)# vrrp 10 ip 172.16.6.1</pre>	Enables VRRP on an interface. <ul style="list-style-type: none"> 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. <p>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 master.</p>
Step 6 <code>end</code> Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Command or Action	Purpose
Step 7 <code>show vrrp [brief] group</code> Example: Router# <code>show vrrp 10</code>	(Optional) Displays a brief or detailed status of one or all VRRP groups on the router.
Step 8 <code>show vrrp interface type number [brief]</code> Example: Router# <code>show vrrp interface GigabitEthernet 0/0/0</code>	(Optional) Displays the VRRP groups and their status on a specified interface.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask**
5. **vrrp group shutdown**

DETAILED STEPS

Command or Action	Purpose
Step 1 <code>enable</code> Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>interface type number</code> Example: <pre>Router(config)# interface GigabitEthernet0/0/0</pre>	Enters interface configuration mode.
Step 4 <code>ip address ip-address mask</code> Example: <pre>Router(config-if)# ip address 172.16.6.5 255.255.255.0</pre>	Configures an IP address for an interface.
Step 5 <code>vrrp group shutdown</code> Example: <pre>Router(config-if)# vrrp 10 shutdown</pre>	Disables the VRRP group on an interface. <ul style="list-style-type: none"> 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 Object Tracking

**Note**

If a VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through object tracking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **vrrp group ip** *ip-address*
6. **vrrp group priority** *level*
7. **vrrp group track** *object-number* [**decrement** *priority*]
8. **end**
9. **show track** [*object-number*]

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 track <i>object-number</i> interface <i>type number</i> { line-protocol ip routing } Example: Router(config)# track 2 interface serial 6 line-protocol	Configures an interface to be tracked where changes in the state of the interface affect the priority of a VRRP group. <ul style="list-style-type: none"> This command configures the interface and corresponding object number to be used with the vrrp track command. The line-protocol keyword tracks whether the interface is up. The ip routing keyword also checks that IP routing is enabled and active on the interface. You can also use the track ip route command to track the reachability of an IP route or a metric type object.
Step 4 interface <i>type number</i> Example: Router(config)# interface Ethernet 2	Enters interface configuration mode.

Command or Action	Purpose
Step 5 <code>vrrp group ip ip-address</code> 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 6 <code>vrrp group priority level</code> Example: Router(config-if)# vrrp 1 priority 120	Sets the priority level of the router within a VRRP group.
Step 7 <code>vrrp group track object-number [decrement priority]</code> Example: Router(config-if)# vrrp 1 track 2 decrement 15	Configures VRRP to track an object.
Step 8 <code>end</code> Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 9 <code>show track [object-number]</code> Example: Router# show track 1	Displays tracking information.

Configuring VRRP MD5 Authentication Using a Key String



Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp group priority** *priority*
6. **vrrp group authentication md5 key-string** [**0 | 7**] *key-string* [**timeout seconds**]
7. **vrrp group ip** [*ip-address*[**secondary**]]
8. Repeat Steps 1 through 7 on each router that will communicate.
9. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 interface <i>type number</i> Example: Router(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 4 ip address <i>ip-address mask</i> [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 priority <i>priority</i> Example: Router(config-if)# vrrp 1 priority 110	Configures VRRP priority.

Command or Action	Purpose
Step 6 <code>vrrp group authentication md5 key-string [0 7] key-string [timeout seconds]</code> Example: <pre>Router(config-if)# vrrp 1 authentication md5 key-string d00b4r987654321a timeout 30</pre>	<p>Configures an authentication string for VRRP MD5 authentication.</p> <ul style="list-style-type: none"> The <i>key</i> argument can be up to 64 characters in length and it is recommended that at least 16 characters be used. No prefix to the <i>key</i> argument or specifying 0 means the key will be unencrypted. Specifying 7 means the key will be encrypted. The key-string authentication key will automatically be encrypted if the service password-encryption global configuration command is enabled. The timeout value is the period of time that the old key string will be accepted to allow configuration of all routers in a group with a new key. <p>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 master.</p>
Step 7 <code>vrrp group ip [ip-address[secondary]]</code> Example: <pre>Router(config-if)# vrrp 1 ip 10.0.0.3</pre>	<p>Enables VRRP on an interface and identifies the IP address of the virtual router.</p>
Step 8 Repeat Steps 1 through 7 on each router that will communicate.	--
Step 9 <code>end</code> Example: <pre>Router(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>

Configuring VRRP MD5 Authentication Using a Key Chain

Perform this task to configure VRRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. VRRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.



Note

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **vrrp group** *priority priority*
10. **vrrp group authentication md5 key-chain** *key-chain*
11. **vrrp group ip** [*ip-address*[**secondary**]]
12. Repeat Steps 1 through 11 on each router that will communicate.
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	key chain <i>name-of-chain</i>	Enables authentication for routing protocols and identifies a group of authentication keys.
	Example: Router(config)# key chain vrrp1	
Step 4	key <i>key-id</i>	Identifies an authentication key on a key chain.
	Example: Router(config-keychain)# key 100	<ul style="list-style-type: none"> The <i>key-id</i> must be a number.

	Command or Action	Purpose
Step 5	key-string <i>string</i> Example: Router(config-keychain-key)# key-string mno172	Specifies the authentication string for a key. <ul style="list-style-type: none"> The <i>string</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.
Step 6	exit Example: Router(config-keychain-key)# exit	Returns to global configuration mode.
Step 7	interface <i>type number</i> Example: Router(config)# interface Ethernet0/1	Configures an interface type and enters interface configuration mode.
Step 8	ip address <i>ip-address mask</i> [secondary] Example: Router(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
Step 9	vrrp group priority <i>priority</i> Example: Router(config-if)# vrrp 1 priority 110	Configures VRRP priority.
Step 10	vrrp group authentication md5 key-chain <i>key-chain</i> Example: Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1	Configures an authentication MD5 key chain for VRRP MD5 authentication. <ul style="list-style-type: none"> The key chain name must match the name specified in Step 3. <p>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 master.</p>

Command or Action	Purpose
Step 11 <code>vrrp group ip [ip-address[secondary]]</code> Example: <pre>Router(config-if)# vrrp 1 ip 10.21.8.12</pre>	Enables VRRP on an interface and identifies the IP address of the virtual router.
Step 12 Repeat Steps 1 through 11 on each router that will communicate.	--
Step 13 <code>end</code> Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Verifying the VRRP MD5 Authentication Configuration

SUMMARY STEPS

1. `show vrrp`
2. `debug vrrp authentication`

DETAILED STEPS

Step 1 `show vrrp`

Use this command to verify that the authentication is configured correctly:

Example:

```
Router# show vrrp
Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority is 100
  Authentication MD5, key-string, timeout 30 secs
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

This output shows that MD5 authentication is configured and the f00d4s key string is used. The timeout value is set at 30 seconds.

Step 2 `debug vrrp authentication`

Use this command to verify that both routers have authentication configured, that the MD5 key ID is the same on each router, and that the MD5 key strings are the same on each router:

Example:

```

Router1#: debug vrrp authentication
VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: HshR: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth
Router2#: debug vrrp authentication
VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: HshR: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth

```

Configuring VRRP Text Authentication

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **terminal interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp group authentication text** *text-string*
6. **vrrp group ip** *ip-address*
7. Repeat Steps 1 through 6 on each router that will communicate.
8. **end**

DETAILED STEPS

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

Command or Action	Purpose
Step 2 configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 terminal interface <i>type number</i> Example: <pre>Router(config)# interface Ethernet 0/1</pre>	Configures an interface type and enters interface configuration mode.
Step 4 ip address <i>ip-address mask</i> [secondary] Example: <pre>Router(config-if)# ip address 10.0.0.1 255.255.255.0</pre>	Specifies a primary or secondary IP address for an interface.
Step 5 vrrp group authentication text <i>text-string</i> Example: <pre>Router(config-if)# vrrp 1 authentication text textstring1</pre>	<p>Authenticates VRRP packets received from other routers in the group.</p> <ul style="list-style-type: none"> If you configure authentication, all routers within the VRRP group must use the same authentication string. The default string is cisco. <p>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 master.</p>
Step 6 vrrp group ip <i>ip-address</i> Example: <pre>Router(config-if)# vrrp 1 ip 10.0.1.20</pre>	Enables VRRP on an interface and identifies the IP address of the virtual router.
Step 7 Repeat Steps 1 through 6 on each router that will communicate.	—
Step 8 end Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Enabling the Router to Send SNMP VRRP Notifications

The VRRP MIB supports SNMP Get operations, which allow network devices to get reports about VRRP groups in a network from the network management station.

Enabling VRRP MIB trap support is performed through the CLI, and the MIB is used for getting the reports. A trap notifies the network management station when a router becomes a Master or backup router. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps vrrp**
4. **snmp-server host *host community-string* vrrp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	snmp-server enable traps vrrp Example: <pre>Router(config)# snmp-server enable traps vrrp</pre>	Enables the router to send SNMP VRRP notifications (traps and informs).
Step 4	snmp-server host <i>host community-string</i> vrrp Example: <pre>Router(config)# snmp-server host myhost.comp.com public vrrp</pre>	Specifies the recipient of an SNMP notification operation.

Configuration Examples for VRRP

- [Example: Configuring VRRP, page 24](#)
- [Example: VRRP Object Tracking, page 25](#)
- [Example: VRRP Object Tracking Verification, page 25](#)
- [Example: VRRP MD5 Authentication Configuration Using a Key String, page 26](#)
- [Example: VRRP MD5 Authentication Configuration Using a Key Chain, page 26](#)
- [Example: VRRP Text Authentication, page 26](#)
- [Example: Disabling a VRRP Group on an Interface, page 26](#)
- [Example: VRRP MIB Trap, page 26](#)

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 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

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 authentication 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)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication 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 Object Tracking

In the following example, the tracking process is configured to track the state of the line protocol on serial interface 0/1. VRRP on Ethernet interface 1/0 then registers with the tracking process to be informed of any changes to the line protocol state of serial interface 0/1. If the line protocol state on serial interface 0/1 goes down, then the priority of the VRRP group is reduced by 15.

```

Router(config)# track 1 interface Serial 0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet 1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.0.0.3
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 track 1 decrement 15

```

Example: VRRP Object Tracking Verification

The following examples verify the configuration shown in the [Example: VRRP Object Tracking, page 25](#) section:

```

Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption is enabled
    min delay is 0.000 sec
  Priority is 105
    Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:06:53
  Tracked by:
    VRRP Ethernet1/0 1

```

Example: VRRP MD5 Authentication Configuration Using a Key String

The following example shows how to configure MD5 authentication using a key string and timeout of 30 seconds:

```
Router(config)# interface Ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 ip 10.21.0.10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-string f00c4s timeout 30
Router(config-if)# exit
```

Example: VRRP MD5 Authentication Configuration Using a Key Chain

The following example shows how to configure MD5 authentication using a key chain:

```
Router(config)# key chain vrrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string f00c4s
Router(config-keychain-key)# exit
Router(config)# interface ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1
Router(config-if)# vrrp 1 ip 10.21.0.10
```

In this example, VRRP queries the key chain to obtain the current live key and key ID for the specified key chain.

Example: VRRP Text Authentication

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

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

Example: Disabling a VRRP Group on an Interface

The following example shows how to disable one VRRP group on GigabitEthernet interface 0/0/0 while retaining VRRP for group 2 on GigabitEthernet interface 1/0/0:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
Router(config-if)# exit
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```

Example: VRRP MIB Trap

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host 10.1.1.0 community abc vrrp
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
VRRP commands	<i>Cisco IOS IP Application Services Command Reference</i>
Object tracking	Configuring Enhanced Object Tracking
Hot Standby Routing Protocol (HSRP)	Configuring HSRP
In Service Software Upgrace (ISSU)	"Cisco IOS In Service Software Upgrade Process" in the <i>Cisco IOS High Availability Configuration Guide</i>
Gateway Load Balancing Protocol (GLBP)	Configuring GLBP
Stateful Switchover	The Stateful Switchover section in the <i>Cisco IOS High Availability Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

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

RFCs

RFCs	Title
RFC 2338	Virtual Router Redundancy Protocol
RFC 2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol

RFCs	Title
RFC 3768	Virtual Router Redundancy Protocol (VRRP)

Technical Assistance

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

Feature Information for VRRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 **Feature Information for VRRP**

Feature Name	Releases	Feature Configuration Information
FHRP—VRRP Support for BVI	12.3(14)T	The FHRP—VRRP Support for BVI feature adds the capability to configure VRRP on Bridged Virtual Interfaces (BVIs). This functionality is similar to the existing HSRP support for BVIs.

Feature Name	Releases	Feature Configuration Information
ISSU—VRRP	12.2(33)SRC	<p>VRRP supports In Service Software Upgrade (ISSU). ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.</p> <p>This feature provides customers with the same level of HA functionality for planned outages due to software upgrades as is available with SSO for unplanned outages. That is, the system can switch over to a secondary RP and continue forwarding packets without session loss and with minimal or no packet loss.</p> <p>This feature is enabled by default.</p> <p>There are no new or modified commands for this feature.</p>
SSO—VRRP	12.2(33)SRC 12.2(33)SXI	<p>VRRP is now SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current VRRP group state.</p> <p>This feature is enabled by default.</p> <p>The following commands were introduced or modified by this feature: debug vrrp ha,vrrp sso, show vrrp.</p>

Feature Name	Releases	Feature Configuration Information
Virtual Router Redundancy Protocol	Cisco IOS XE 3.1.0SG 12.2(13)T 12.2(14)S 15.0(1)S	<p>VRRP enables a group of routers to form a single virtual router to provide redundancy. 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.</p> <p>The following commands were introduced by this feature: debug vrrp all, debug vrrp error, debug vrrp events, debug vrrp packets, debug vrrp state, show vrrp, show vrrp interface, vrrp authentication, vrrp description, vrrp ip, vrrp preempt, vrrp priority, vrrp timers advertise, vrrp timers learn.</p>
VRRP MD5 Authentication	12.3(14)T	<p>The VRRP MD5 Authentication feature provides a method of authenticating peers using a more simple method than the method in RFC 2338.</p> <p>The following command was introduced by this feature: debug vrrp authentication.</p> <p>The following commands were modified by this feature: vrrp authentication and show vrrp.</p>

Feature Name	Releases	Feature Configuration Information
VRRP MIB—RFC 2787	12.3(11)T	<p>The VRRP MIB--RFC 2787 feature enables an enhancement to the MIB for use with SNMP-based network management. The feature adds support for configuring, monitoring, and controlling routers that use VRRP.</p> <p>The following command was introduced by this feature: vrrp shutdown.</p> <p>The following commands were modified by this feature: snmp-server enable traps and snmp-server host.</p>
VRRP Object Tracking	12.3(2)T 12.2(25)S	<p>The VRRP Object Tracking feature extends the capabilities of the VRRP to allow tracking of specific objects within the router that can alter the priority level of a virtual router for a VRRP group.</p> <p>The following command was introduced by this feature: vrrp track.</p> <p>The following command was modified by this feature: show track.</p>

Glossary

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

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

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

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

VRRP router --A router that is running VRRP.

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: www.cisco.com/go/trademarks. 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. (1110R)

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.

© 2011 Cisco Systems, Inc. All rights reserved.