Configuring Virtual Router Redundancy Protocol

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 multi-access 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 chapter includes the following topics:

- Information About VRRP, page 31-1
- Configuring VRRP, page 31-7
- Configuration Examples for VRRP, page 31-16

Information About VRRP

- VRRP Operation, page 31-1
- Benefits of VRRP, page 31-3
- Multiple Virtual Router Support, page 31-4
- VRRP Router Priority and Preemption, page 31-4
- VRRP Advertisements, page 31-5
- VRRP Object Tracking, page 31-5
- How Object Tracking Affects the Priority of a VRRP Router, page 31-5
- VRRP Authentication, page 31-6
- ISSU—VRRP, page 31-6
- SSO—VRRP, page 31-7

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 responds to the ARP request with its own MAC address.
Information About VRRP

- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- IRDP (ICMP Router Discovery Protocol) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The dynamic discovery protocols incur some configuration and processing overhead on the LAN client. This could be detrimental 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 detached 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, on MPLS VPNs, VRF-aware MPLS VPNs and VLANs.

Figure 31-1 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).

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 master virtual router fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the “VRRP Router Priority and Preemption” section later in this document.
Figure 31-2 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 and that Routers A and B act as virtual router backups to each other if either router fails.

In this topology, two virtual routers are configured. (For more information, see the “Multiple Virtual Router Support” section later in this document.) 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.

**Benefits of VRRP**

**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 virtual router master for the group by altering VRRP priorities to the status of tracked objects such as interface or IP route states.

Multiple Virtual Router Support
You can configure up to 255 virtual routers on a 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 IPv4 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 now 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 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. 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” 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 ignores 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 are 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.

### ISSU—VRRP

VRRP supports In Service Software Upgrade (ISSU). An 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 at the following URL:


For detailed information about ISSU on the 7600 series routers, see the ISSU and eFSU on Cisco 7600 Series Routers document at the following URL:

**SSO—VRRP**

With the introduction of the SSO—VRRP 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](http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html) document at the following URL:


**Configuring VRRP**

The following sections outline the steps necessary to configure VRRP:

- Customizing VRRP, page 31-7 (optional)
- Enabling VRRP, page 31-8 (required)
- Disabling VRRP on an Interface, page 31-9 (optional)
- Configuring VRRP Object Tracking, page 31-10 (optional)
- Configuring VRRP MD5 Authentication Using a Key String, page 31-11 (optional)
- Configuring VRRP MD5 Authentication Using a Key Chain, page 31-12 (optional)
- Verifying the VRRP MD5 Authentication Configuration, page 31-13 (optional)
- Configuring VRRP Text Authentication, page 31-14 (optional)
- Enabling the Router to Send SNMP VRRP Notifications, page 31-15 (optional)

**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.

Complete the following steps in privileged EXEC mode to customize VRRP:
### Configuring VRRP

To enable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip-address mask</td>
<td>Configures an IP address for an interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>vrrp group description text</td>
<td>Assigns a text description to the VRRP group.</td>
</tr>
<tr>
<td>Step 6</td>
<td>vrrp group priority level</td>
<td>Sets the priority level of the router within a VRRP group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The default priority is 100.</td>
</tr>
<tr>
<td>Step 7</td>
<td>vrrp group preempt [delay minimum seconds]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The default delay period is 0 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The router that is IP address owner will preempt, regardless of the setting of this command.</td>
</tr>
<tr>
<td>Step 8</td>
<td>vrrp group timers advertise [msec] interval</td>
<td>Configures the interval between successive advertisements by the virtual router master in a VRRP group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The unit of the interval is in seconds unless the msec keyword is specified. The default interval value is 1 second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Step 9</td>
<td>vrrp group timers learn</td>
<td>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.</td>
</tr>
<tr>
<td>Step 10</td>
<td>no vrrp sso</td>
<td>(Optional) Disables VRRP support of SSO. VRRP support of SSO is enabled by default.</td>
</tr>
</tbody>
</table>
### Configuring VRRP

Disabling VRRP on an interface allows the protocol to be disabled, but the configuration 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 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 using the Cisco IOS CLI will reenable the VRRP group.

To disable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

### Disabling VRRP on an Interface

Disabling VRRP on an interface allows the protocol to be disabled, but the configuration 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 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 using the Cisco IOS CLI will reenable the VRRP group.

To disable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip address ip-address mask</code></td>
<td>Configures an IP address for an interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>vrrp group ip ip-address [secondary]</code></td>
<td>Enables VRRP on an interface.</td>
</tr>
<tr>
<td></td>
<td>• After you identify a primary IP address, you can use the <code>vrrp ip</code> command again with the <code>secondary</code> keyword to indicate additional IP addresses supported by this group.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> `Router# show vrrp [brief</td>
<td>Displays a brief or detailed status of one or all VRRP groups on the router.</td>
</tr>
<tr>
<td></td>
<td>group]`</td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>Router# show vrrp interface type number [brief]</code></td>
<td>Displays the VRRP groups and their status on a specified interface.</td>
</tr>
</tbody>
</table>
Configuring VRRP

### Restrictions

The following restriction applies to VRRP object tracking.

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

To configure VRRP object tracking perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> track object-number interface type number (line-protocol</td>
<td>ip routing)</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> vrrp group ip ip-address</td>
<td>Enables VRRP on an interface and identifies the IP address of the virtual router.</td>
</tr>
<tr>
<td><strong>Step 6</strong> vrrp group priority level</td>
<td>Sets the priority level of the router within a VRRP group.</td>
</tr>
<tr>
<td><strong>Step 7</strong> vrrp group track object-number [decrement priority]</td>
<td>Configures VRRP to track an object.</td>
</tr>
</tbody>
</table>
Configuring VRRP MD5 Authentication Using a Key String

Restrictions

The following restrictions apply to configuring VRRP MD5 Authentication using a key string.

- 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.

To configure VRRP MD5 Authentication using a key string perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td><code>show track object-number</code></td>
<td>Displays tracking information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface type number</code></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip address ip-address mask [secondary]</code></td>
<td>Specifies a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>vrrp group priority priority</code></td>
<td>Configures VRRP priority.</td>
</tr>
</tbody>
</table>
Configuring VRRP

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.

Restrictions

The following restrictions apply to configuring VRRP MD5 using a keychain.

- 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.

To configure VRRP MD5 authentication using a key chain perform the following steps.
### Configuring VRRP

#### Verifying the VRRP MD5 Authentication Configuration

To verify the VRRP MD5 authentication configuration perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>key chain name-of-chain</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>key key-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>key-string string</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>interface type number</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ip address ip-address mask [secondary]</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>vrrp group priority priority</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>vrrp group authentication md5 key-chain key-chain</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>vrrp group ip [ip-address [secondary]]</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Repeat Steps 1 through 11 on each router that will communicate.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
Step 1  show vrrp

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

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:

Router1# debug vrrp authentication

VRPP: Sent: 21016401FE050000AC1801FE0000000000000000
VRPP: HshC: B861CBF1B9026130DD34AE0849BEC8A1

VRPP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRPP: HshC: C5E193C684533FDC750F85FCFB051E1
VRPP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth

Router2# debug vrrp authentication

VRPP: Sent: 21016401FE050000AC1801FE0000000000000000
VRPP: HshC: C5E193C684533FDC750F85FCFB051E1

VRPP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRPP: HshC: B861CBF1B9026130DD34AE0849BEC8A1
VRPP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth

Configuring VRRP Text Authentication

Restrictions

The following restrictions apply to 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 zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.
To configure VRRP text authentication perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type number</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address ip-address mask [secondary]</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>vrrp group authentication text text-string</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>vrrp group ip ip-address</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Repeat Steps 1 through 6 on each router that will communicate.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

### 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 collecting 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.

To enable the router to send SNMP VRRP notifications perform the following steps:
**Configuration Examples for VRRP**

- Example: Configuring VRRP, page 31-16
- Example: VRRP Object Tracking, page 31-17
- Example: VRRP Object Tracking Verification, page 31-17
- Example: VRRP MD5 Authentication Configuration Using a Key String, page 31-18
- Example: VRRP MD5 Authentication Configuration Using a Key Chain, page 31-18
- Example: VRRP Text Authentication, page 31-18
- Example: Disabling a VRRP Group on an Interface, page 31-19
- Example: VRRP MIB Trap, page 31-19

**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.

---

**Command or Action** | **Purpose**
--- | ---
Step 1  enable | Enables privileged EXEC mode.
  - Enter your password if prompted.
Step 2  configure terminal | Enters global configuration mode.
Step 3  snmp-server enable traps vrrp | Enables the router to send SNMP VRRP notifications (traps and informs).
Step 4  snmp-server host host community-string vrrp | Specifies the recipient of an SNMP notification operation.
Router A
RouterA(config)# interface ethernet 1/0
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# vrrp 100 timers learn
RouterA(config-if)# no vrrp 100 preempt
RouterA(config-if)# vrrp 100 ip 10.1.0.100
RouterA(config-if)# no shutdown

Router B
RouterB(config)# interface ethernet 1/0
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# vrrp 100 timers learn
RouterB(config-if)# no vrrp 100 preempt
RouterB(config-if)# vrrp 100 ip 10.1.0.100
RouterB(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 Serial0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet1/0
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” 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 fastethernet 0/0
Router(config-if)# 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 Ethernet interface 0/1 while retaining VRRP for group 2 on Ethernet interface 0/2:

```plaintext
Router(config)# interface ethernet0/1
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 ethernet0/2
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

The following example shows how to enable the VRRP MIB trap support functionality:

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