



Configuring Ethernet Switch Ports

This chapter gives an overview of configuration tasks for the Gigabit Ethernet (GE) switch on the Cisco 800M Series ISR.

This chapter contains the following sections:

- [Configuring VLANs, page 51](#)
- [Configuring VTP, page 52](#)
- [Configuring 802.1x Authentication, page 53](#)
- [Configuring Spanning Tree Protocol, page 54](#)
- [Configuring MAC Address Table Manipulation, page 56](#)
- [Configuring MAC Address Notification Traps, page 57](#)
- [Configuring the Switched Port Analyzer, page 57](#)
- [Configuring IGMP Snooping, page 58](#)
- [Configuring Per-Port Storm Control, page 59](#)
- [Configuring HSRP, page 60](#)
- [Configuring VRRP, page 61](#)

Configuring VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

For detailed information on VLANs, see the following web link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swvlan.html

For a sample VLAN configuration, see “[Example: VLAN configuration](#)”.

Example: VLAN configuration

The following example shows how to configure inter-VLAN routing:

```
Router# configure terminal
Router(config)# vlan 1
Router(config)# vlan 2
Router(config)# interface vlan 1
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 2
Router(config-if)# ip address 2.2.2.2 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface gigabitethernet 0/1
Router(config-if)# switchport access vlan 1
Router(config-if)# interface gigabitethernet 0/2
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

Configuring VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches. VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

You should understand the following concepts for configuring VTP.

- **VTP domain:** A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.
- **VTP server:** In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode.
- **VTP client:** A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode.
- **VTP transparent:** VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.

For detailed information on VTP, see the following web link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swvtp.html

For a sample VTP configuration, see “[Example: Configuring VTP](#)”.

Example: Configuring VTP

The following example shows how to configure the switch as a VTP server:

```
Router# configure terminal
Router(config)# vtp mode server
Router(config)# vtp domain Lab_Network
Router(config)# vtp password WATER
Router(config)# exit
```

The following example shows how to configure the switch as a VTP client:

```
Router# configure terminal
Router(config)# vtp mode client
Router(config)# exit
```

The following example shows how to configure the switch as VTP transparent:

```
Router# configure terminal
Router(config)# vtp mode transparent
Router# exit
```

Configuring 802.1x Authentication

IEEE 802.1x port-based authentication defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before allowing access to any switch or LAN services. Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

With IEEE 802.1x authentication, the devices in the network have specific roles:

- **Supplicant**—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The supplicant is sometimes called the client.)
- **Authentication server**—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device (or Cisco ISR router in this instance) transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- Authenticator—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

For detailed information on how to configure 802.1x port-based authentication, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

For a sample 802.1x authentication configuration see “[Example: Enabling IEEE 802.1x and AAA on a Switch Port](#)”.

Example: Enabling IEEE 802.1x and AAA on a Switch Port

This example shows how to configure Cisco 800M series ISR as 802.1x authenticator.

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface gigabitethernet 0/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# end
```

Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch. Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including

switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

For detailed configuration information on STP see the following link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swstp.html

For configuration examples, see “[Example: Spanning Tree Protocol Configuration](#)”.

Example: Spanning Tree Protocol Configuration

The following example shows configuring spanning-tree port priority of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses the port priority when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

The following example shows how to change the spanning-tree port cost of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state.

```
Router#configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

The following example shows configuring the bridge priority of VLAN 10 to 33792:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

The following example shows configuring the hello time for VLAN 10 being configured to 7 seconds. The hello time is the interval between the generation of configuration messages by the root switch.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 4
Router(config)# end
```

The following example shows configuring forward delay time. The forward delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

The following example shows configuring maximum age interval for the spanning tree. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

Configuring MAC Address Table Manipulation

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- **Dynamic address:** a source MAC address that the switch learns and then drops when it is not in use. You can use the aging time setting to define how long the switch retains unseen addresses in the table.
- **Static address:** a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

See the “[Example: MAC Address Table Manipulation](#)” for sample configurations for enabling secure MAC address, creating a static entry, set the maximum number of secure MAC addresses and set the aging time.

For detailed configuration information on MAC address table manipulation see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

Example: MAC Address Table Manipulation

The following example shows configuration for enabling secure MAC address option on the port.

```
Router# configure terminal
Router(config)# mac-address-table secure 0004.0005.0006 GigabitEthernet 0/1 vlan 5
Router(config)# end
```

The following example shows creating a static entry in the MAC address table.

```
Router# configure terminal
Router(config)# mac-address-table static 0002.0003.0004 interface GigabitEthernet 0/2 vlan 3
Router(config)# end
```

The following example sets the maximum number of secure MAC addresses to 10.

```
Router# configure terminal
Router(config)# mac-address-table secure maximum 10 GigabitEthernet 0/1
Router(config)# end
```

The following example shows setting the aging timer.

```
Router# configure terminal
Router(config)# mac-address-table aging-time 300
```

```
Router(config)# end
```

Configuring MAC Address Notification Traps

MAC address notification enables you to track users on a network by storing the MAC address activity on the switch. Whenever the switch learns or removes a MAC address, an SNMP notification can be generated and sent to the network management system (NMS). If you have many users coming and going from the network, you can set a trap interval time to bundle the notification traps and reduce network traffic. The MAC notification history table stores the MAC address activity for each hardware port for which the trap is enabled. MAC address notifications are generated for dynamic and secure MAC addresses; events are not generated for self addresses, multicast addresses, or other static addresses.

For configuration examples, see “[Example: Configuring MAC Address Notification Traps](#)”.

Example: Configuring MAC Address Notification Traps

This example shows how to enable the MAC notification trap when a MAC address is added to the interface:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# snmp trap mac-notification added
Router(config-if)# end
```

This example shows how to enable the MAC notification trap when a MAC address is removed from this interface.

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# snmp trap mac-notification removed
Router(config-if)# end
```

Configuring the Switched Port Analyzer

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

See [Example: SPAN Configuration, page 58](#) for SPAN configuration examples.

For detailed information on how to configure a switched port analyzer (SPAN) session, see the following web link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

Example: SPAN Configuration

The following example shows how to configure a SPAN session to monitor bidirectional traffic from a Gigabit Ethernet source interface:

```
Router# configure terminal
Router(config)# monitor session 1 source gigabitethernet 0/1
Router(config)# end
```

The following example shows how to configure a gigabit ethernet interface as the destination for a SPAN session:

```
Router# configure terminal
Router(config)# monitor session 1 destination gigabitethernet 0/2
Router(config)# end
```

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:

```
Router# configure terminal
Router(config)# no monitor session 1 source gigabitethernet 0/1
Router(config)# end
```

Configuring IGMP Snooping

IGMP snooping constrains the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

By default, IGMP snooping is globally enabled. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis. Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

See the [“Example: Configuring IGMP Snooping”](#) for a sample configuration on IGMP snooping.

Example: Configuring IGMP Snooping

The following example shows how to enable IGMP snooping on a VLAN interface.

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1
Router# end
```

The following example shows how to enable a static connection to a multicast router.

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/1
Router# end
```


The following example shows how to add a port as a member of a multicast group. Ports normally join multicast groups through the IGMP report message, but you can also statically configure a port as a member of a multicast group.

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet
0/1
Router# end
```

Configuring Per-Port Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, a multicast, or a unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in the network configuration, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received

With either method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold (if one is specified) and then resumes normal forwarding. If the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. In general, the higher the level, the less effective the protection against broadcast storms.



Note

In C800M platform, when you configure the **storm-control action shutdown** command, the state of the port changes to administratively down. Use the **no shutdown** command to manually revert the state of the port.

See the “[Example: Per-Port Storm-Control](#)” for a sample configuration on per-port storm control.

Example: Per-Port Storm-Control

The following example shows bandwidth-based multicast storm control being enabled at 70 percent on Gigabit Ethernet interface.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# storm-control multicast level 70.0 30.0
Router(config-if)# end
Router# show storm-control multicast
```

| Interface | Filter State | Upper | Lower | Current |
|-----------|--------------|---------|---------|---------|
| Gi0/0 | inactive | 100.00% | 100.00% | N/A |
| Gi0/1 | inactive | 100.00% | 100.00% | N/A |
| Gi0/2 | Forwarding | 70.00% | 30.00% | 0.00% |

Configuring HSRP

The Hot Standby Router Protocol (HSRP) is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. If you do not use the standby preempt interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

For more information about configuring HSRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp.html

For a sample HSRP configuration, see “[Example: Configuring HSRP](#)”

Example: Configuring HSRP

In this example, Router A is configured to be the active device for group 1 and standby device for group 2. Device B is configured as the active device for group 2 and standby device for group 1.

```
RouterA# configure terminal
RouterA(config)# interface GigabitEthernet 0/1
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.3
RouterA(config-if)# standby 2 priority 95
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.1.0.4
RouterA(config-if)# end
```

```
RouterB# configure terminal
RouterB(config)# interface GigabitEthernet 0/1
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.3
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails.

An important aspect of the VRRP 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 using the **vrrp priority** command.

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.

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.

For more information on VRRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html

For a sample VRRP configuration, see “[Example: Configuring VRRP](#)”.

Example: Configuring VRRP

In the following example, Router A and Router B each belong to two VRRP groups, group1 and group 5. In this 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.

```
RouterA(config)# interface GigabitEthernet 0/1
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)# no shutdown

RouterA(config-if)# end

RouterB(config)# interface GigabitEthernet 0/1
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)# no shutdown
RouterB(config-if)# end
```