Documentation Updates for the Catalyst 2955, 2950, and 2940 Switches, Cisco IOS Release 12.1(22)EA4

March 2005

These documentation updates are for Catalyst 2955, 2950, and 2940 switches, Cisco IOS Release 12.1(22)EA4. Use this document with the information in the *Release Notes for the Catalyst 2955, 2950, and 2940 Switches, Cisco IOS Release 12.1(22)EA4.*

This document provides updates to the 2955, 2950, and 2940 product documentation. These changes will be included in the next revision of the documentation.

For more information about the Catalyst 2955, 2950, and 2940 switches, see the "Related Documentation" section on page 19.

Contents

This information is in the release notes:

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

Documentation Updates for Cisco IOS Release 12.1(22)EA4

These are the updates to the product documentation that occurred in Cisco IOS Release 12.1(22)EA4.

Updates to the Software Configurations Guides

These are the updates to the software guides:

Supported MIBs

In Appendix A, "Supported MIBs," the "Using FTP to Access the MIB Files" section is incorrect. This is the correct procedure.

You can get each MIB file by using this procedure:

1. Make sure that your FTP client is in passive mode.

Note Some FTP clients do not support passive mode.

2. Use FTP to access the server ftp.cisco.com.
3. Log in with the username *anonymous*.
4. Enter your e-mail username when prompted for the password.
5. At the **ftp>** prompt, change directories to /pub/mibs/v1 and /pub/mibs/v2.
6. Use the get MIB_filename command to obtain a copy of the MIB file.

Configuring Loopback Detection

This information was added to the "Configuring Interface Characteristics" chapter of the software configuration guides:

This feature is used to detect a loopback on a 10/100 interface at the physical layer. If you configure the **down-when-looped** interface command, the system checks if the link-up is due to a loopback condition at the physical layer. If the link-up is due to a loopback condition, the system does not let the Ethernet link come up. The system can detect the loopback only on links that are directly connected to that interface and not on links that are indirectly connected. The loopback detection works when the interfaces are configured to autonegotiate.

For complete syntax and usage information for the **down-when-looped** interface command, see the *Cisco IOS Interface Command Reference, Release 12.1*.

Note The **down-when-looped** interface command is not supported on the Catalyst 2950G switches.

IEEE 802.1x Accounting Attribute-Value Pairs

This information was added to the "Configuring IEEE 802.1x" chapter of the software configuration guides:

The information sent to the RADIUS server is represented in the form of Attribute-Value (AV) pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is contained in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a switch that is configured for IEEE 802.1x accounting. Three types of RADIUS accounting packets are sent by a switch:

- START–sent when a new user session starts
- INTERIM–sent during an existing session for updates
- STOP–sent when a session terminates

Table 1 lists the AV pairs and when they are sent are sent by the switch:

Table 1 Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes[1]	Sometimes[1]
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Never	Always
Attribute[43]	Acct-Output-Octets	Never	Never	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Never	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

1. The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

You can view the AV pairs that are being sent by the switch by entering the **debug radius** privileged EXEC command. For more information about these commands, see the *Cisco IOS Debug Command Reference, Release 12.1* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121sup/121debug/index.htm

See RFC 3580, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines," for more information about AV pairs.

Updates to the Command Reference Guides

This is a correction to the command references for this release.

This note was added to the **show version** user EXEC command in the switch command reference:

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

Documentation Updates for Cisco IOS Release 12.1(22)EA3

These are the updates to the product documentation that occurred in Cisco IOS Release 12.1(22)EA3.

Note There have been no changes to the Catalyst 2955 hardware documentation in this release.

Corrections to the Software Configuration Guides

These are the corrections to the software guide:

- The "Configuring a System Name and Prompt" section and the "Configuring a System Prompt" section of the "Administering the Switch" chapter incorrectly state that you can manually configure the **prompt** global configuration command. The switches do not support this command. You should ignore this information in printed and online copies of the software configuration guides.
- In the "Configuring VLANs" chapter of the Catalyst 2950 and 2940 software configuration guides for Cisco IOS Release 12.1(19)EA1 and earlier, the examples that use the **spanning-tree vlan** *vlan-id* **priority** *priority* global configuration command are incorrect because they have a priority value that is not a multiple of 16. In these examples, the correct value for the priority parameter is a multiple of 16. The information in the Figure13-3 of the Catalyst 2940 software guide and Figure 17-3 of the Catalyst 2950 software guide is also incorrect. The correct value for the port priority is a multiple of 16. This information was corrected in the Catalyst 2950 and 2940 software configuration guides for Cisco IOS Release 12.1(20)EA1 and later.

Additions to the Software Configuration Guides

These sections were added to the "Configuring IGMP" chapter:

These sections were added to the "Configuring DHCP" chapter:

Understanding the IGMP Configurable-Leave Timer

In Cisco IOS Release 12.1(22)EA2 and earlier, the IGMP snooping leave time was fixed at 5 seconds. If membership reports were not received by the switch before the query response time of the query expired, a port was removed from the multicast group membership. However, some applications require a leave latency of less than 5 seconds.

In Cisco IOS Release 12.1(22)EA3 and later, you can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be set from 100 to 5000 milliseconds. The timer can be set either globally or on a per-VLAN basis. The VLAN configuration of the leave time overrides the global configuration.

IGMP Leave Timer Guidelines

Follows these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or on a per-VLAN basis.
- Configuring the leave time on a VLAN overrides the global setting.
- The default leave time is 1000 milliseconds.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2.
- The actual leave latency in the network is usually the configured leave time. However, the leave time *might* vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

Configuring the IGMP Leave Timer

Beginning in privileged EXEC mode, follow these steps to configure the IGMP leave timer:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping last-member-query-interval** *time*	Configure the IGMP leave timer globally. The range is from 100 to 5000 miliseconds.
Step 3	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	(Optional) Configure the IGMP leaver time on the VLAN interface. The range is from 100 to 5000 milliseconds. **Note** Configuring the leave time on a VLAN overrides the globally configured timer.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show ip igmp snooping**	(Optional) Display the configured IGMP leave time.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no ip igmp snooping last-member-query-interval** global configuration command to globally reset the IGMP leave timer to the default setting (1000 milliseconds).

Use the **no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** global configuration command to remove the configured IGMP leave-time setting from the specified VLAN.

For more information about commands that support the IGMP configurable leave time, see these sections:

- "ip igmp snooping last-member-query interval" section on page 13
- "show ip igmp snooping" section on page 14

Understanding the IGMP Snooping Querier (Catalyst 2955 Switches Only)

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed. For more information about the IGMP snooping querier, see the "Configuring the IGMP Snooping Querier (Catalyst 2955 Switches Only)" section on page 7.

IGMP Snooping Querier Configuration Guidelines and Restrictions (Catalyst 2955 Switches Only)

Follow these guidelines and restrictions when configuring the IGMP snooping querier:

- The IGMP snooping querier is disabled by default.
- Configure the VLAN in global configuration mode.
- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN switch virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the switch uses the first available IP address configured on the switch. The first IP address available can be seen in the output of the **show ip interface** privileged EXEC command. The IGMP snooping querier does not generate a IGMP general query if it cannot find an available IP address on the switch.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the non querier state if it detects the presence of a multicast router in the network.
- When it is administratively enabled, the IGMP snooping querier moves to the operationally-disabled state under these conditions:
  - IGMP snooping is disabled in the VLAN.
  - PIM is enabled on the SVI of the corresponding VLAN.

Configuring the IGMP Snooping Querier (Catalyst 2955 Switches Only)

To enable the IGMP snooping querier feature in a VLAN, follow these steps:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping querier**	Enable the IGMP snooping querier.
Step 3	**ip igmp snooping querier** *ip_address*	(Optional) Specify an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. **Note** The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch.
Step 4	**ip igmp snooping querier query-interval** *interval-count*	(Optional) Set the interval between IGMP queriers. The interval range is from 1 to 18000 seconds.
Step 5	**ip igmp snooping querier tcn query [count** *count* **| interval** *interval***]**	(Optional) Set the time (in seconds) between Topology Change Notification (TCN) queries. The count range is from 1 to 10. The interval range is from 1 to 255 seconds.
Step 6	**ip igmp snooping querier timer expiry** *timeout*	(Optional) Set the length of time (in seconds) until the IGMP querier expires.The range is from 60 to 300 seconds.”
Step 7	**ip igmp snooping querier version** *version*	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show ip igmp snooping vlan** *vlan-id*	(Optional) Verify that the IGMP snooping querier is enabled on the VLAN interface.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set the IGMP snooping querier source address to 10.0.0.64 and to verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds and to verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds and to verify the configuration:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end
```

This example shows how to set the IGMP snooping querier feature to version 2 and to verify the configuration:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end
```

For more information about commands that support the IGMP querier feature, see these sections:

- "ip igmp snooping querier (Catalyst 2955 Switches Only)" section on page 11
- "show ip igmp snooping querier detail (Catalyst 2955 Switches Only)" section on page 17

DHCP Snooping Enhancement

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When option-82 information is inserted by an edge switch in software releases earlier than Cisco IOS Release 12.2(25)SEA, you cannot configure DHCP snooping on an aggregation switch because the DHCP snooping bindings database will not be properly populated. You also cannot configure IP source guard and dynamic Address Resolution Protocol (ARP) inspection on the switch unless you use static bindings or ARP access control lists (ACLs).

In Cisco IOS Release 12.1(22)EA3 or later, when an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the **ip dhcp snooping information option allowed-trust** global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as DHCP snooping or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on ingress untrusted interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Note Do not enter the **ip dhcp snooping information option allowed-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

Enabling DHCP Snooping and Option 82

Beginning in privileged EXEC mode, follow these steps to enable DHCP snooping on the switch.

Note Step 5 was added in Cisco IOS Release 12.1(22)EA3 or later.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp snooping**	Enable DHCP snooping globally.

	Command	Purpose
Step 3	**ip dhcp snooping vlan** *vlan-range*	Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Step 4	**ip dhcp snooping information option**	Enable the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. The default is enabled.
Step 5	**ip dhcp snooping information option allowed-untrusted**	(Optional) If the switch is an aggregation switch connected to an edge switch, enable the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default is disabled. **Note** You must enter this command only on aggregation switches that are connected to trusted devices.
Step 6	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to be configured.
Step 7	**ip dhcp snooping trust**	(Optional) Configure the interface as trusted or untrusted. You can use the **no** keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.
Step 8	**ip dhcp snooping limit rate** *rate*	(Optional) Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 2048. The default is no rate limit configured. **Note** We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN on which DHCP snooping is enabled.
Step 9	**exit**	Return to global configuration mode.
Step 10	**ip dhcp snooping verify mac-address**	(Optional) Configure the switch to verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show running-config**	Verify your entries.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable DHCP snooping, use the **no ip dhcp snooping** global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the **no ip dhcp snooping vlan** *vlan-range* global configuration command. To disable the insertion and removal of the option-82 field, use the **no ip dhcp snooping information option** global configuration command. To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the **no ip dhcp snooping information option allowed-untrusted** global configuration command.

Updates to the Command References

These commands were added or modified for the command references in this release:

ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information from an edge switch. Use the **no** form of this command to configure the switch to drop these packets from the edge switch.

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Note Do not enter the **ip dhcp snooping information option allowed-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

Syntax Description

This command has no arguments or keywords.

Defaults

The switch drops DHCP packets with option-82 information from an edge switch.

Command Modes

Global configuration

Command History

Release	Modification
12.1(22)EA3	This command was introduced.

Usage Guidelines

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted interface and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the **ip dhcp snooping information option allowed-untrusted** command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted interface. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted interface.

Examples

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch(config)# ip dhcp snooping information option allowed-untrusted
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding information.

ip igmp snooping querier (Catalyst 2955 Switches Only)

Use the **ip igmp snooping querier** global configuration command to globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. Use the **no** form of this command to disable the IGMP querier feature or to reset the parameters to the default settings.

ip igmp snooping querier [**address** {*ip-address*} | **max-response-time** *response-time* | **query-interval** | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

no ip igmp snooping querier [**address** | **max-response-time** | **query-interval** | **tcn query { count** *count* | **interval** *interval}* | **timer expiry** | **version**]

Syntax Description

address	(Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
ip-address	Source IP address for the querier.
max-response-time *response-time*	(Optional) Set the maximum time to wait for an IGMP querier report. You can set a response time from 1 to 25 seconds.
query-interval *interval-count*	(Optional) Set the interval between IGMP queriers. You can set a count from 1 to 18000 seconds.
tcn query	(Optional) Set the time (in seconds) between Topology Change Notification (TCN) queries.
count *count*	(Optional) Set the number of TCN queries to be executed during the TCN interval time. You can set a count from 1 to 10.
interval *interval*	(Optional) Set the TCN query interval time. You can set a time (in seconds) from 1 to 255.

timer expiry	(Optional) Set the length of time until the IGMP querier expires.
version *version*	(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.

Defaults

The IGMP snooping querier feature is globally disabled on the switch.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast-enabled device.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a *querier.*

By default, the IGMP snooping querier is configured to detect devices that use IGMP *Version 2* (IGMPv2) but does not detect clients that are using IGMP *Version 1* (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the **max-response-time w**hen devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC-compliant devices running IGMPv1 might reject IGMP general query messages that have a nonzero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Switch(config)# ip igmp snooping querier
```

This example shows how to globally disable the IGMP snooping querier feature:

```
Switch(config)# no ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Switch(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Switch(config)# no ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(config)# no ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the IGMP snooping configuration.
show ip igmp snooping groups	Displays the IGMP snooping router ports.
show ip igmp snooping groups	Displays IGMP snooping multicast information.

ip igmp snooping last-member-query interval

Use the **ip igmp snooping last-member-query-interval** global configuration command to enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis. Use the **no** form of this command to return the IGMP configurable-leave timer to the default setting.

ip igmp snooping vlan *vlan-id* **last-member-query-interval** *time*

no ip igmp snooping vlan *vlan-id* **last-member-query-interval**

Syntax Descriptiont

vlan-id	VLAN ID value. The range is 1 to 1005 when the standard software image (SI) is installed and 1 to 4094 when the enhanced software image (EI) is installed.
time	Interval time out in seconds. The range is 100 to 5000 milliseconds.

Defaults

The default timeout setting is 1000 milliseconds.

Command History

Release	Modification
12.1(22)EA3	This command was introduced.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch# configure terminal
Switch(config)# ip igmp snooping last-member-query-interval 2000
Switch(config)# end
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
Switch(config)# end
```

This example shows how to globally reset the IGMP leave timer to the default setting:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping last-member-query-interval
Switch(config)# end
```

This example shows how to remove the configured IGMP leave timer on VLAN 1. The globally configured leave timer will then be applied to VLAN 1:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 1 last-member-query-interval
Switch(config)# end
```

To verify your settings, enter the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping vlan	Enables IGMP snooping on a VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

show ip igmp snooping

Note Beginning with Cisco IOS Release 12.2(22)EA3, the value of the IGMP configurable-leave timer is displayed in the output of the **show ip igmp snooping** command.

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN. Use the **mrouter** keyword to display the dynamically learned and manually configured multicast router ports.

show ip igmp snooping [**group** | **mrouter** | **querier**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

group	(Optional) Display information about the IGMP multicast groups, the compatibility mode, and the ports that are associated with each group.
mrouter	(Optional) Display the IGMP snooping dynamically learned and manually configured multicast router ports.
querier	(Optional) Display information about the IGMP version that an interface supports.

vlan *vlan-id*	(Optional) Keyword and variable to specify a VLAN. On Catalyst 2940 switches, the range is 1 to 4094. On Catalyst 2950, 2950-LRE, and 2955 switches, the range is and 1 to 1005 when the standard software image (SI) is installed and 1 to 4094 when the enhanced software image (EI) is installed. This keyword is available only in privileged EXEC mode.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.1(13)AY	This command was introduced.
12.1(19)EA1	The **group** and **querier** keywords were added.

Usage Guidelines

Use this command to display snooping characteristics for the switch or for a specific VLAN.

You can also use the **show mac address-table multicast** privileged EXEC command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

When multicast VLAN registration (MVR) is enabled, use the **show ip igmp snooping mrouter** command to display the IGMP snooping dynamically learned and manually configured multicast router ports.

Use the **group** keyword to display the multicast groups, the compatibility mode, and the ports that are associated with each group.

Use the **show ip igmp snooping querier** command to display the IGMP version and IP address of a detected device that sends IGMP query messages, also called a *querier.* A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch. The command output also shows the VLAN and interface on which the querier was detected. If the querier is a multicast router, the output shows the *Port* field as *Router.*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping** command:

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
```

```
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
Last member query interval           :100
CGMP interoperability mode           :IGMP_ONLY

Vlan 2:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval           : 333
<output truncated>
```

This is an example of output from the **show ip igmp snooping vlan 1** command:

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
Last member query interval  : 100
CGMP interoperability mode           :IGMP_ONLY
```

This is an example of output from the **show ip igmp snooping mrouter vlan 1** command:

Note In this example, `Fa0/3` is a dynamically learned router port, and `Fa0/2` is a configured static router port.

```
Switch# show ip igmp snooping mrouter vlan 1
Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

This is an example of output from the **show ip igmp snooping group vlan 1** command:

```
Switch# show ip igmp snooping group vlan 1
Vlan      Group          Version     Port List
------------------------------------------------------------
1         229.2.3.4      v3          fa0/1 fa0/3
1         224.1.1.1      v2          fa0/8
```

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
```

```
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  fa0/1
2         172.20.40.20   v2                  Router
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping report-suppression	Enables IGMP report suppression.
ip igmp snooping source-only-learning	Enables IP multicast-source-only learning on the switch.
ip igmp snooping source-only-learning age-timer	Enables and configures the aging time of the forwarding-table entries that the switch learns by using the source-only learning method.
ip igmp snooping vlan *vlan-id*	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping querier detail (Catalyst 2955 Switches Only)

Use the **show ip igmp snooping querier detail** user EXEC command to display the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping querier detail

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.

Usage Guidelines

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** only displays the IP address of the most recent device detected by the switch querier.

The **show ip igmp snooping querier command detail** displays the IP address of the most recent device detected by the switch querier along with this additional information:

- the elected IGMP querier in the VLAN
- the configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail
Vlan      IP Address     IGMP Version   Port
------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1

Global IGMP switch querier status
------------------------------------------------------
admin state                   : Enabled
admin version                 : 2
source IP address             : 0.0.0.0
query-interval (sec)          : 60
max-response-time (sec)       : 10
querier-timeout (sec)         : 120
tcn query count               : 2
tcn query interval (sec)      : 10

Vlan 1:   IGMP switch querier status

------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
------------------------------------------------------
admin state                   : Enabled
admin version                 : 2
source IP address             : 10.1.1.65
query-interval (sec)          : 60
max-response-time (sec)       : 10
querier-timeout (sec)         : 120
tcn query count               : 2
tcn query interval (sec)      : 10
operational state             : Non-Querier
operational version           : 2
tcn query pending count       : 0
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping	Displays IGMP snooping multicast information for the switch or for the specified parameter.

Related Documentation

These documents provide complete information about the Catalyst 2955, 2950, and 2940 switches and are available at Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2940/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 20.

These publications provide more information about the Catalyst 2955 and Catalyst 2950 switches:

- *Catalyst 2950 and Catalyst 2955 Desktop Switch Software Configuration Guide* (order number DOC-7811380=)
- *Catalyst 2950 and Catalyst 2955 Desktop Switch Command Reference* (order number DOC-7811381=)
- *Catalyst 2950 and Catalyst 2955 Desktop Switch System Message Guide* (order number DOC-7814233=)
- Device manager online help (available on the switch)
- *Catalyst 2950 Desktop Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2950 Switch Getting Started Guide (*order number DOC-1786521=)
- *Regulatory Compliance and Safety Information for the Catalyst 2950 Switch* (order number DOC-7816625=)
- *Catalyst 2955 Hardware Installation Guide* (order number DOC-7814944=)

These publications provide more information about the Catalyst 2940 switches:

- *Catalyst 2940 Switch Software Configuration Guide* (order number DOC-7815507=)
- *Catalyst 2940 Switch Command Reference* (order number DOC-7815505=)
- *Catalyst 2940 Switch System Message Guide* (order number DOC-7815524=)
- Device manager online help (available on the switch)
- *Catalyst 2940 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2940 Switch Getting Started Guide (*order number DOC-7816576=)
- *Regulatory Compliance and Safety Information for the Catalyst 2940 Switch* (order number DOC-7816656=)

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *1000BASE-T Gigabit Interface Converter Installation Notes* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)
- *Cisco LRE CPE Hardware Installation Guide* (order number DOC-7811469=)
- *CWDM Passive Optical System Installation Note* (not orderable but is available on Cisco.com)

- *Installation Notes for the Catalyst Family Small-Form-Factor Pluggable Modules* (order number DOC-7815160=)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- *Installation and Warranty Notes for the Cisco LRE 48 POTS Splitter* (order number DOC-7812250=)

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.