4

Multimedia Traffic Control with IP Multicast (IGMP)

Contents

Overview

This chapter describes Multimedia Traffic Control with IP Multicast (IGMP), and explains how to configure IGMP controls to reduce unnecessary bandwidth usage on a per-port basis.

For the latest information on IGMP, see the software release notes posted on the ProCurve Networking support web site at http://www.procurve.com.

For general information on how to use the switch's built-in interfaces, refer to these chapters in the *Management and Configuration Guide* for your switch:

- Chapter 3, "Using the Menu Interface"
- Chapter 4, "Using the Command Line Interface (CLI)"
- Chapter 5, "Using the Web Browser Interface"
- Appendix C, "Switch Memory and Configuration"

General Operation and Features

IGMP Features

Feature	Default	Menu	CLI	Web
view igmp configuration	n/a	—	page 4-6	—
show igmp status for multicast groups used by the selected VLAN	n/a	—	Yes	—
enabling or disabling IGMP (Requires VLAN ID Context)	disabled	—	page 4-8	page 4-11
per-port packet control	auto	—	page 4-9	—
IGMP traffic priority	normal	—	page 4-10	—
querier	enabled	—	page 4-10	—
fast-leave	disabled	—	page 4-14	—

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol controls). In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows detection of IGMP queries and report packets in order to manage IP multicast traffic through the switch. If no other querier is detected, the switch will then also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to "Changing the Querier Configuration Setting" on page 4-10.)

Note

IGMP configuration on the switch operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context.

IGMP Terms

- **IGMP Device:** A switch or router running IGMP traffic control features.
- **IGMP Host:** An end-node device running an IGMP (multipoint, or multicast communication) application.
- **Querier:** A required IGMP device that facilitates the IGMP protocol and traffic flow on a given LAN. This device tracks which ports are connected to devices (IGMP clients) that belong to specific multicast groups, and triggers updates of this information. A querier uses data received from the queries to determine whether to forward or block multicast traffic on specific ports. When the switch has an IP address on a given VLAN, it automatically operates as a Querier for that VLAN if it does not detect a multicast router or another switch functioning as a Querier. When enabled (the default state), the switch's querier function eliminates the need for a multicast router. In most cases, ProCurve recommends that you leave this parameter in the default "enabled" state even if you have a multicast router performing the querier function in your multicast group. For more information, see "How IGMP Operates" on page 4-11.

IGMP Operating Features

Basic Operation

In the factory default configuration, IGMP is disabled. If multiple VLANs are not configured, you must configure IGMP on the default VLAN (DEFAULT_VLAN; VID = 1). If multiple VLANs are configured, you must configure IGMP on a per-VLAN basis for every VLAN where this feature is desired.

Enhancements

With the CLI, you can configure these additional options:

- **Forward with High Priority.** Disabling this parameter (the default) causes the switch or VLAN to process IP multicast traffic, along with other traffic, in the order received (usually, normal priority). Enabling this parameter causes the switch or VLAN to give a higher priority to IP multicast traffic than to other traffic.
- **Auto/Blocked/Forward:** You can use the console to configure individual ports to any of the following states:
  - **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
  - **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
  - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.
- **Operation With or Without IP Addressing:** This feature helps to conserve IP addresses by enabling IGMP to run on VLANs that do not have an IP address. See “Operation With or Without IP Addressing” on page 4-13.
- **Querier Capability:** The switch performs this function for IGMP on VLANs having an IP address when there is no other device in the VLAN acting as querier. See “Querier Operation” on page 4-21.

Notes

Whenever IGMP is enabled, the switch generates an Event Log message indicating whether querier functionality is enabled.

IP multicast traffic groups are identified by IP addresses in the range of 224.0.0.0 to 239.255.255.255. Also, incoming IGMP packets intended for reserved, or "well-known" multicast addresses automatically flood through all ports (except the port on which the packets entered the switch). For more on this topic, see "Excluding Multicast Addresses from IP Multicast Filtering" on page 4-22.

For more information, refer to "How IGMP Operates" on page 4-11.

CLI: Configuring and Displaying IGMP

IGMP Commands Used in This Section

show ip igmp configuration config vid [config] group <ip address>	page 4-7
ip igmp	page 4-8
high-priority-forward	page 4-10
auto <[ethernet] <port-list>	page 4-9
blocked <[ethernet] <port-list>	page 4-9
forward <[ethernet] <port-list>	page 4-9
querier	page 4-10
show ip igmp	See the appendix on monitoring and analyzing switch operation in the *Management and Configuration Guide*.

Viewing the Current IGMP Configuration. This command lists the IGMP configuration for all VLANs configured on the switch or for a specific VLAN.

Syntax: *show ip igmp config*
IGMP configuration for all VLANs on the switch.

show ip igmp < vid > config
IGMP configuration for a specific VLAN on the switch, including per-port data.

show ip igmp group < ip-address >
Lists the ports on which the specified multicast group IP address is registered.

(For IGMP operating status, see the appendix on monitoring and analyzing switch operation in the *Management and Configuration Guide*.)

For example, suppose you have the following VLAN and IGMP configurations on the switch:

VLAN ID	VLAN Name	IGMP Enabled	Forward with High Priority	Querier
1	DEFAULT_VLAN	Yes	No	No
22	VLAN-2	Yes	Yes	Yes
33	VLAN-3	No	No	No

You could use the CLI to display this data as follows:

```
ProCurve> show ip igmp config
 IGMP Service
  VLAN ID      VLAN NAME    IGMP Enabled Forward with High Priority Querier
  ------------ ------------ ------------ -------------------------- -------
  1            DEFAULT_VLAN Yes          No                         No
  22           VLAN-2       Yes          Yes                        Yes
  33           VLAN-3       No           No                         Yes
```

Figure 4-1. Example Listing of IGMP Configuration for All VLANs in the Switch

The following version of the show ip igmp command includes the VLAN ID (*vid*) designation, and combines the above data with the IGMP per-port configuration:

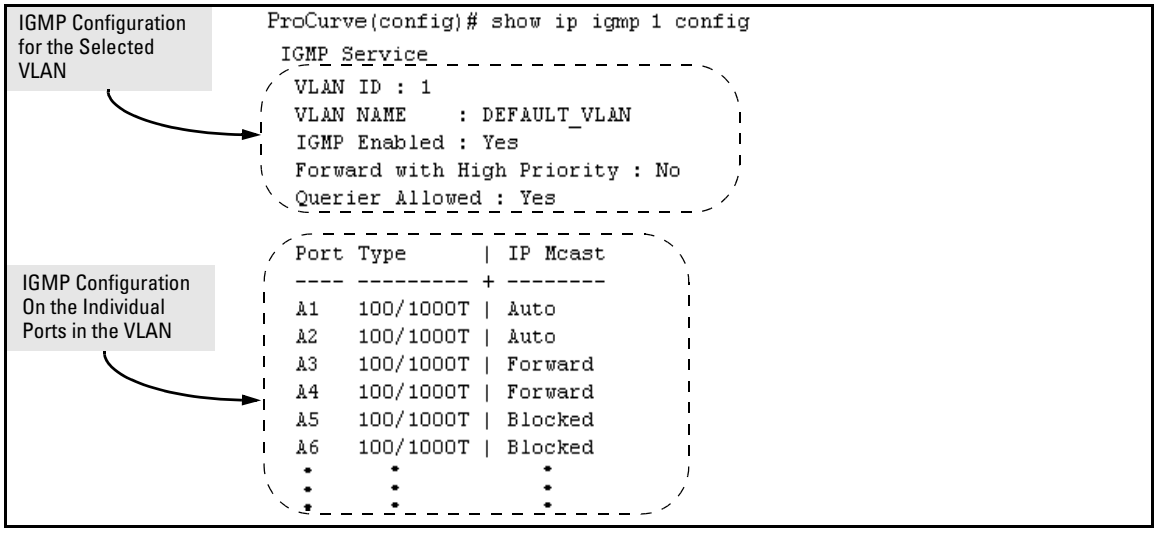

Figure 4-2. Example Listing of IGMP Configuration for A Specific VLAN

Enabling or Disabling IGMP on a VLAN. You can enable IGMP on a VLAN, along with the last-saved or default IGMP configuration (whichever was most recently set), or you can disable IGMP on a selected VLAN. Note that this command must be executed in a VLAN context.

Syntax: [no] ip igmp

For example, here are methods to enable and disable IGMP on the default VLAN (VID = 1).

```
ProCurve(config)# vlan 1 ip igmp
```
Enables IGMP on VLAN 1.

```
ProCurve(vlan-1)# ip igmp
```
Same as above.

```
ProCurve(config)# no vlan 1 ip igmp
```
Disables IGMP on VLAN 1.

Note

If you disable IGMP on a VLAN and then later re-enable IGMP on that VLAN, the switch restores the last-saved IGMP configuration for that VLAN. For more on how switch memory operates, see the chapter on switch memory and configuration in the *Management and Configuration Guide.*

You can also combine the **ip igmp** command with other IGMP-related commands, as described in the following sections.

Configuring Per-Port IGMP Packet Control. Use this command in the VLAN context to specify how each port should handle IGMP traffic.

Syntax: vlan < *vid* > ip igmp
[auto <port-list> | blocked <port-list> | forward <port-list>]

Syntax: vlan < *vid* > ip igmp

Enables IGMP on the specified VLAN. In a VLAN context, use only **ip igmp** *without the VLAN specifier.*

auto < *port-list* > (Default operation)

Filter multicast traffic on the specified ports. Forward IGMP traffic to hosts on the ports that belong to the multicast group for which the traffic is intended. (Also forward any multicast traffic through any of these ports that is connected to a multicast router.) This is the default IGMP port configuration.

blocked < *port-list* >

Drop all multicast traffic received from devices on the specified ports, and prevent any outgoing multicast traffic from moving through these ports.

forward < *port-list* >

Forward all multicast traffic through the specified port.

For example, suppose you wanted to configure IGMP as follows for VLAN 1 on ports A1 - A6:

- Ports A1 - A2: Auto
- Ports A3 - A4: Forward
- Ports A5 - A6: Block

Depending on the privilege level, you could use one of the following commands to configure IGMP on VLAN 1 with the above settings:

```
ProCurve(config)# vlan 1
ProCurve(vlan-1)# ip igmp auto a1,a2
ProCurve(vlan-1)# ip igmp forward a3,a4
ProCurve(vlan-1)# ip igmp blocked a5,a6
```

The following command displays the VLAN and per-port configuration resulting from the above commands.

```
ProCurve> show ip igmp 1 config
```

Configuring IGMP Traffic Priority. This command allows you to prioritize IGMP traffic as either "high" or "normal" (the default).

Syntax:[no] vlan < vid > ip igmp high-priority-forward

*Assigns "high" priority to IGMP traffic. The "***no***" form returns a high-priority setting to (the default) "normal" priority. (The switch services the traffic at its inbound priority.)*

```
ProCurve(config)# vlan 1 ip igmp high-priority-forward
```

This example configures high priority for IGMP traffic on VLAN 1.

```
ProCurve(vlan-1)# ip igmp high-priority-forward
```

Same as above command, but in the VLAN 1 context level.

```
ProCurve(vlan 1)# no ip igmp high-priority-forward
```

Returns IGMP traffic to "normal" priority.

```
ProCurve> show ip igmp config
```

Show command to display results of above high-priority commands.

Configuring the Querier Function. In its default configuration, the switch is capable of operating as an IGMP querier. This command lets you disable or re-enable this function.

Syntax:[no] vlan <vid> ip igmp querier

Disables or re-enables the ability for the switch to become querier, if necessary, on the specified VLAN. The default querier capability is "enabled".

```
ProCurve(config)# no vlan 1 ip igmp querier
```

Disables the querier function on VLAN 1.

```
ProCurve> show ip igmp config
```

This is the show command used to display results of the above querier command.

Web: Enabling or Disabling IGMP

In the web browser interface you can enable or disable IGMP on a per-VLAN basis. To configure other IGMP features, telnet to the switch console and use the CLI.

To Enable or Disable IGMP

1. Click on the **Configuration** tab.
2. Click on the **Device Features** button.
3. If more than one VLAN is configured, use the VLAN pull-down menu to select the VLAN on which you want to enable or disable IGMP.
4. Use the Multicast Filtering (IGMP) menu to enable or disable IGMP.
5. Click on **Apply Changes** button to implement the configuration change.

For web-based help on how to use the web browser interface screen, click on the **?** button provided on the web browser screen.

How IGMP Operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. (In ProCurve's implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the **querier** feature enabled.) A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a *multicast group*, and all devices in the group use the same multicast group address.

Message Types

The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information

from the hosts on the network. (If you need to disable the querier feature, you can do so through the CLI, using the IGMP configuration MIB. See "Configuring the Querier Function" on page 4-10.)

- **Report (Join):** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

IGMP Operating Notes

IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups based on the following process.

- An IP multicast packet includes the multicast group (address) to which the packet belongs.
- When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP report (join request) to the network. (The multicast group specified in the join request is determined by the requesting application running on the IGMP client.)
- When a networking device with IGMP enabled receives the join request for a specific group, it forwards any IP multicast traffic it receives for that group through the port on which the join request was received.
- When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member.
- When the leave request is detected, the appropriate IGMP device will cease transmitting traffic for the designated multicast group through the port on which the leave request was received (as long as there are no other current members of that group on the affected port).

Displaying IGMP Data.

To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see the appendix on monitoring and analyzing switch operation in the *Management and Configuration Guide*.

Supported Standards and RFCs

ProCurve's implementation of IGMP supports the following standards and operating capabilities:

- RFC2236 (IGMP V.2, with backwards support for IGMP V.1)
- IETF draft for IGMP and MLD snooping switches (for IGMP V1, V2 V3)
- Full IGMPv2 support as well as full support for IGMPv1 Joins.
- Ability to operate in IGMPv2 Querier mode on VLANs with an IP address.

The ProCurve implementation is subject to the following restrictions:

- Interoperability with RFC3376 (IGMPv3)
- Interoperability with IGMPv3 Joins. When the switch receives an IGMPv3 Join, it accepts the host request and begins forwarding the IGMP traffic. This means ports that have not joined the group and are not connected to routers or the IGMP Querier will not receive the group's multicast traffic.
- No support for the IGMPv3 "Exclude Source" or "Include Source" options in the Join Reports. Rather, the group is simply joined from all sources.
- No support for becoming a version 3 Querier. The switch will become a version 2 Querier in the absence of any other Querier on the network.

Note IGMP is supported in the HP MIB, rather than the standard IGMP MIBs, as the latter reduce Group Membership detail in switched environments.

Operation With or Without IP Addressing

You can configure IGMP on VLANs that do not have IP addressing. The benefit of IGMP without IP addressing is a reduction in the number of IP addresses you have to use and configure. This can be significant in a network with a large number of VLANs. The limitation on IGMP without IP addressing is that the switch cannot become Querier on any VLANs for which it has no IP address—so the network administrator must ensure that another IGMP device will act as Querier. It is also advisable to have an additional IGMP device available as a backup Querier. See the following table.

Table 4-1.Comparison of IGMP Operation With and Without IP Addressing

IGMP Function Available With IP Addressing Configured on the VLAN	Available *Without* IP Addressing?	Operating Differences Without an IP Address
Forward multicast group traffic to any port on the VLAN that has received a join request for that multicast group.	Yes	None
Forward join requests (reports) to the Querier.	Yes	None
Configure individual ports in the VLAN to **Auto** (the default)/**Blocked**, or **Forward**.	Yes	None
Configure IGMP traffic forwarding to normal or high-priority forwarding.	Yes	None
Age-Out IGMP group addresses when the last IGMP client on a port in the VLAN leaves the group.	Yes	Requires that another IGMP device in the VLAN has an IP address and can operate as Querier. This can be a multicast router or another switch configured for IGMP operation. (ProCurve recommends that the VLAN also include a device operating as a backup Querier in case the device operating as the primary Querier fails for any reason.
Support Fast-Leave IGMP (below) and Forced Fast-Leave IGMP (page 4-14).	Yes	
Support automatic Querier election.	No	Querier operation not available.
Operate as the Querier.	No	Querier operation not available.
Available as a backup Querier.	No	Querier operation not available.

Automatic Fast-Leave IGMP

IGMP Operation Presents a "Delayed Leave" Problem. Where multiple IGMP clients are connected to the same port on an IGMP device (switch or router), if only one IGMP client joins a given multicast group, then later sends a Leave Group message and ceases to belong to that group, the IGMP device retains that IGMP client in its IGMP table and continues forwarding IGMP traffic to the IGMP client until the Querier triggers confirmation that no other group members exist on the same port. This means that the switch continues to transmit unnecessary multicast traffic through the port until the Querier renews the multicast group status.

Fast-Leave IGMP. Depending on the switch model, Fast-Leave is enabled or disabled in the default configuration.

Table 4-3.IGMP: Data-Driven and Non-Data Driven Behavior

Switch Model or Series	Data-Driven IGMP Included?	IGMP Fast-Leave Setting	Default IGMP Behavior
Switch 5300 Switch 2800 Switch 2500	Yes	Always Enabled	Drops unjoined multicast traffic except for always-forwarded traffic toward the Querier or multicast routers, and out of IGMP-forward ports. Selectively forwards joined multicast traffic.
Switch 2600 Switch 2600-PWR Switch 4100 Switch 6108	No	Disabled in the Default Configuration	IGMP Fast-Leave disabled in the default configuration. Floods unjoined multicast traffic to all ports. Selectively forwards joined multicast traffic.

On switches that do not support Data-Driven IGMP, unregistered multicast groups are flooded to the VLAN rather than pruned. In this scenario, Fast-Leave IGMP can actually increase the problem of multicast flooding by removing the IGMP group filter before the Querier has recognized the IGMP Leave. The Querier will continue to transmit the multicast group during this short time, and because the group is no longer registered the switch will then flood the multicast group to all ports.

On ProCurve switches that do support Data-Driven IGMP (“Smart” IGMP), when unregistered multicasts are received the switch automatically filters (drops) them. Thus, the sooner the IGMP Leave is processed, the sooner this multicast traffic stops flowing.

Because of the multicast flooding problem mentioned above, the IGMP FastLeave feature is disabled by default on all ProCurve switches that *do not* support Data-Driven IGMP. (See table 4-3, above.) The feature can be enabled on these switches via an SNMP set of this object:

hpSwitchIgmpPortForceLeaveState.< *vid* >.< *port number* >

However, this is not recommended as this will increase the amount of multicast flooding during the period between the client's IGMP Leave and the Querier's processing of that Leave. For more on this topic, refer to “Forced Fast-Leave IGMP” on page 4-17.

ProCurve recommends that the following settings be used.

- Use Delayed Group Flush on the Series 2600 switches whenever Fast Leave or Forced Fast Leave are set on a port (see page 4-17).
- Forced fast leave can be used when there are multiple devices attached to a port.

Automatic Fast-Leave Operation. If a switch port is:

a. Connected to only one end node
b. The end node currently belongs to a multicast group; i.e. is an IGMP client
c. The end node subsequently leaves the multicast group

Then the switch does not need to wait for the Querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting IGMP traffic to the client. (If the switch detects multiple end nodes on the port, automatic Fast-Leave does not activate—regardless of whether one or more of these end nodes are IGMP clients.)

In the next figure, automatic Fast-Leave operates on the switch ports for IGMP clients "3A" and "5A", but not on the switch port for IGMP clients "7A" and 7B, Server "7C", and printer "7D".

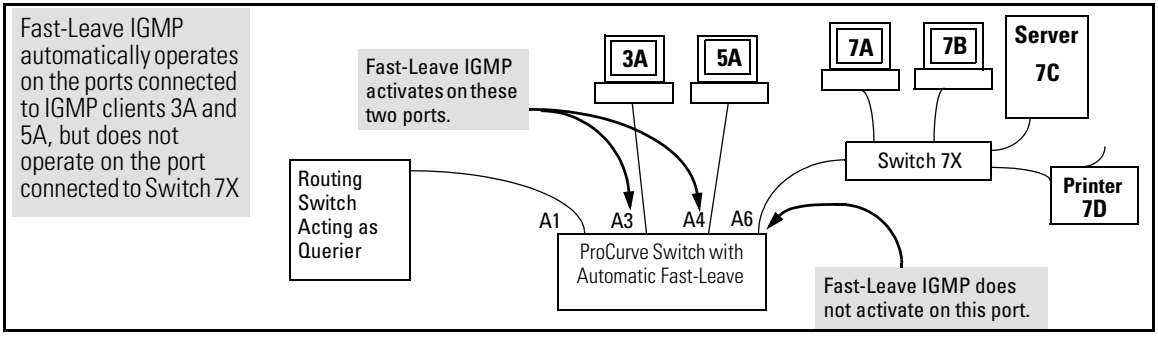

Figure 4-4. Example of Automatic Fast-Leave IGMP Criteria

When client "3A" running IGMP is ready to leave the multicast group, it transmits a Leave Group message. Because the switch knows that there is only one end node on port A3, it removes the client from its IGMP table and halts multicast traffic (for that group) to port A3. If the switch is not the Querier, it does not wait for the actual Querier to verify that there are no other group members on port A3. If the switch itself is the Querier, it does not query port A3 for the presence of other group members.

Note that Fast-Leave operation does not distinguish between end nodes on the same port that belong to different VLANs. Thus, for example, even if all of the devices on port A6 in figure 4-4 belong to different VLANs, Fast-Leave does not operate on port A6.

Using Delayed Group Flush

This feature continues to filter IGMP-Left groups for a specified additional period of time. This is beneficial in switches such as the Series 2600 or 4100gl, where Data-Driven IGMP is not supported. The delay in flushing the group filter prevents stale traffic from being forwarded by the server. Delayed Group Flush is enabled or disabled for the entire switch.

ProCurve recommends that Delayed Group Flush be used whenever Fast Leave or Forced Fast Leave are enabled on the Series 2600 and 2600-PWR Switches. Note that this command must be executed in the configuration context of the CLI.

Syntax: igmp delayedflush *<time period>*

Enables the switch to continue to flush IGMP-Left groups for a specified period of time (0 - 255 seconds). The default setting is **Disabled**. *To disable, reset the time period to zero.*

Syntax: Show igmp delayedflush

Displays the current setting for the switch.

Forced Fast-Leave IGMP

Forced Fast-Leave IGMP speeds up the process of blocking unnecessary IGMP traffic to a switch port that is connected to multiple end nodes. (This feature does not activate on ports where the switch detects only one end node). For example, in figure 4-4, even if you configured Forced Fast-Leave on all ports in the switch, the feature would activate only on port A6 (which has multiple end nodes) when a Leave Group request arrived on that port.

When a port having multiple end nodes receives a Leave Group request from one end node for a given multicast group “X”, Forced Fast-Leave activates and waits a small amount of time to receive a join request from any other group “X” member on that port. If the port does not receive a join request for that group within the forced-leave interval, the switch then blocks any further group “X” traffic to the port.

Setting Fast-Leave and Forced Fast-Leave from the CLI

In previous software versions, Fast-Leave and Forced Fast-Leave options for a port were set exclusively through the MIB. The following commands now allow a port to be configured for Fast-Leave or Forced Fast-leave operation from the CLI. Note that these commands must be executed in a VLAN context

Syntax: [no] ip igmp fastleave <*port-list*>

Enables IGMP Fast-Leaves on the specified ports in the VLAN (the default setting). In the Config context, use the VLAN specifier, for example, **vlan <** *vid* **> ip igmp fastleave <***port-list***>***. The "no" form disables Fast-Leave on the specified ports.*

[no] ip igmp forcedfastleave <*port-list*>

Forces IGMP Fast-Leaves on the specified ports in the VLAN, even if they are cascaded.

To view the IGMP Fast-Leave status of a port use the **show running-config** or **show configuration** commands.

Setting Forced Fast-Leave Using the MIB

Fast-Leave and Forced Fast-Leave options for a port can also be set through the switch's MIB (Management Information Base).

Feature	Default	Settings	Function
Forced Fast-Leave state	**2** (disabled)	**1** (enabled) **2** (disabled)	Uses the **setmib** command to enable or disable Forced Fast-Leave on individual ports. When enabled on a port, Forced Fast-Leave operates only if the switch detects multiple end nodes (and at least one IGMP client) on that port.

Note on VLAN Numbers:

In the ProCurve switches covered in this guide, the **walkmib** and **setmib** commands use an internal VLAN number (and not the VLAN ID, or VID) to display or change many per-vlan features, such as the Forced Fast-Leave state. Because the internal VLAN number for the default VLAN is always 1 (regardless of whether VLANs are enabled on the switch), and because a discussion of internal VLAN numbers for multiple VLANs is beyond the scope of this manual, this section concentrates on examples that use the default VLAN.

Listing the MIB-Enabled Forced Fast-Leave Configuration

The Forced Fast-Leave configuration data is available in the switch's MIB, and includes the state (enabled or disabled) for each port and the Forced-Leave Interval for all ports on the switch.

To List the Forced Fast-Leave State for all Ports in the Switch. In the CLI, use the **walkmib** command, as shown below.

1. Enter either of the following walkmib command options:

   ```
   walkmib hpSwitchIgmpPortForcedLeaveState
   ```

   - OR -

   ```
   walkmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5
   ```

   The resulting display lists the Forced Fast-Leave state for all ports in the switch, by VLAN. (A port belonging to more than one VLAN will be listed once for each VLAN, and if multiple VLANs are *not* configured, all ports will be listed as members of the default VLAN.) The following command produces a listing such as that shown in figure 4-5:

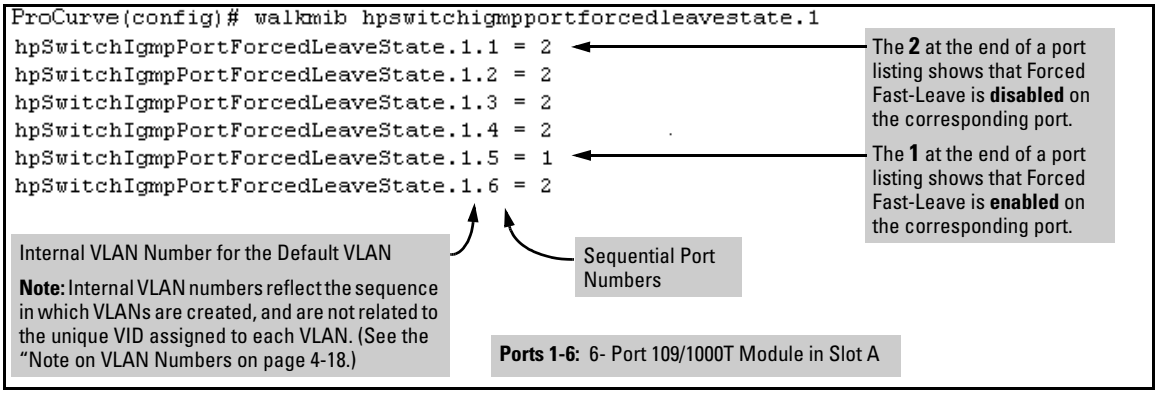

Figure 4-5. Example of a Forced Fast-Leave Listing where all Ports are Members of the Default VLAN

To List the Forced Fast-Leave State for a Single Port. (See the "Note on VLAN Numbers" on page 4-18.)

Go to the switch's command prompt and use the **getmib** command, as shown below.

Syntax:

getmib hpSwitchIgmpPortForcedLeaveState.<vlan number><.port number>

- OR -

getmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.<vlan number><.port number>

For example, the following command to list the state for port A6 (which, in this case, belongs to the default VLAN) produces the indicated listing:

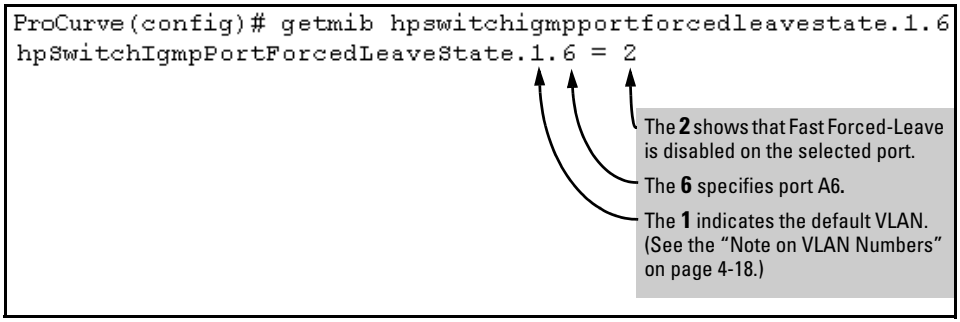

Figure 4-6. Example Listing the Forced Fast-Leave State for a Single Port on the Default VLAN

Configuring Per-Port Forced Fast-Leave IGMP

In the factory-default configuration, Forced Fast-Leave is disabled for all ports on the switch. To enable (or disable) this feature on individual ports, use the switch's **setmib** command, as shown below.

Configuring Per-Port Forced Fast-Leave IGMP on Ports. This procedure enables or disables Forced Fast-Leave on ports in a given VLAN. (See the "Note on VLAN Numbers" on page 4-18.)

Syntax:

setmib hpSwitchIgmpPortForcedLeaveState.< vlan number >< *.port number* > *-i* < 1 | 2 >

- OR -

setmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.< vlan number >< *.port number* > *-i* < 1 | 2 >

where:

1 = Forced Fast-Leave enabled

2 = Forced Fast-Leave disabled

For example, suppose that your switch has a six-port gigabit module in slot A, and port C1 is a member of the default VLAN. In this case, the port number is "49" (In the MIB, slot A = ports 1-24; slot B = ports 25-48; slot C = ports 49-72, and so on.) To enable Forced Fast-Leave on C6 (53), you would execute the following command and see the indicated result:

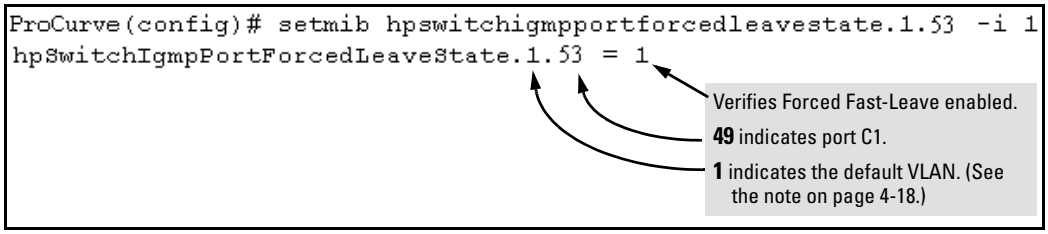

Figure 4-7. Example of Changing the Forced Fast-Leave Configuration on Port 49

Using the Switch as Querier

Querier Operation

The function of the IGMP Querier is to poll other IGMP-enabled devices in an IGMP-enabled VLAN to elicit group membership information. The switch performs this function if there is no other device in the VLAN, such as a multicast router, to act as Querier. Although the switch automatically ceases Querier operation in an IGMP-enabled VLAN if it detects another Querier on the VLAN, you can also use the Command Prompt to disable the Querier capability for that VLAN.

Note

A Querier is required for proper IGMP operation. For this reason, if you disable the Querier function on a switch, ensure that there is an IGMP Querier (and, preferably, a backup Querier) available on the same VLAN.

If the switch becomes the Querier for a particular VLAN (for example, the DEFAULT_VLAN), then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the Querier for that VLAN. If this occurs, the switch Event Log lists a pair of messages similar to these:

```
I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: Other Querier detected

I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: This switch is no longer
Querier
```

In the above scenario, if the other device ceases to operate as a Querier on the default VLAN, then the switch detects this change and can become the Querier as long as it is not pre-empted by some other IGMP Querier on the VLAN. In this case, the switch Event Log lists messages similar to the following to indicate that the switch has become the Querier on the VLAN:

```
I 01/15/01 09:21:55 igmp: DEFAULT_VLAN: Querier Election in
process

I 01/15/01 09:22:00 igmp: DEFAULT_VLAN: This switch has been
elected as Querier
```

Excluding Multicast Addresses from IP Multicast Filtering

Each multicast host group is identified by a single IP address in the range of 224.0.0.0 through 239.255.255.255. Specific groups of consecutive addresses in this range are termed "well-known" addresses and are reserved for predefined host groups. IGMP does not filter these addresses, so any packets the switch receives for such addresses are flooded out all ports assigned to the VLAN on which they were received (except the port on which the packets entered the VLAN).

The following table lists the 32 well-known address groups (8192 total addresses) that IGMP does not filter on the switches covered in this guide, as well as on the 1600M, 2400M, 2424M, 2650M, 4000M, 6108M, 8000M, and Switch 2500 Series devices.

Table 4-2.IP Multicast Address Groups Excluded from IGMP Filtering

Groups of Consecutive Addresses in the Range of 224.0.0.*X* to 239.0.0.*X**		Groups of Consecutive Addresses in the Range of 224.128.0.*X* to 239.128.0.*X**	
224.0.0.x	232.0.0.x	224.128.0.x	232.128.0.x
225.0.0.x	233.0.0.x	225.128.0.x	233.128.0.x
226.0.0.x	234.0.0.x	226.128.0.x	234.128.0.x
227.0.0.x	235.0.0.x	227.128.0.x	235.128.0.x
228.0.0.x	236.0.0.x	228.128.0.x	236.128.0.x
229.0.0.x	237.0.0.x	229.128.0.x	237.128.0.x
230.0.0.x	238.0.0.x	230.128.0.x	238.128.0.x
231.0.0.x	239.0.0.x	231.128.0.x	239.128.0.x

* X is any value from 0 to 255.

Notes:

IP Multicast Filters. *This operation applies to the ProCurve Switch 1600M, 2400M, 2424M, 4000M, and 8000M, but not to the Switch 2500, 2600, 2600-PWR, 2800, 4100, and 5300 Series devices or the Switch 6108 (which do not have static multicast traffic/security filters).*

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Where a switch has a static Traffic/Security filter configured with a "Multicast" filter type and a "Multicast Address" in this range, the switch will use the static filter unless IGMP learns of a multicast group destination in this range. In this case, IGMP dynamically takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the switch returns filtering control to the static filter.

Reserved Addresses Excluded from IP Multicast (IGMP) Filtering. Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are "well known" or "reserved" addresses. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

Number of IP Multicast Addresses Allowed. Multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

— This page is intentionally unused. —