SUPERMICRO®

# L2 / L3 Switches

# IGMP Snooping

# Configuration Guide

**Revision 1.0**

The information in this USER'S MANUAL has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

IN NO EVENT WILL SUPERMICRO BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPERMICRO SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference,  in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. Perchlorate Material-special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate/ for further details.

Manual Revision 1.0

Release Date: February 4, 2013

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

## Contents

# 1 IGMP Snooping Configuration Guide

This document describes the IGMP Snooping feature supported in Supermicro Layer 2 / Layer 3 switch products.

The IGMP Snooping configurations for the below listed Supermicro switch products are covered.

| Top of Rack Switches | Blade Switches |
|---|---|
| • SSE-G24-TG4 | • SBM-GEM-X2C |
| • SSE-G48-TG4 | • SBM-GEM-X2C+ |
| • SSE-X24S | • SBM-GEM-X3S+ |
| • SSE-X3348S | • SBM-XEM-X10SM |
| • SSE-X3348T | |

The majority of this document applies to all the above listed Supermicro switch products. In any particular sub section however, the contents might vary across these switch product models. In those sections the differences are clearly identified with reference to particular switch product models. If any particular switch product model is not referenced, the reader can safely assume that the content is applicable to all the above listed models.

Throughout this document, the common term "switch" refers to any of the above listed Supermicro switch product models unless a particular switch product model is noted.

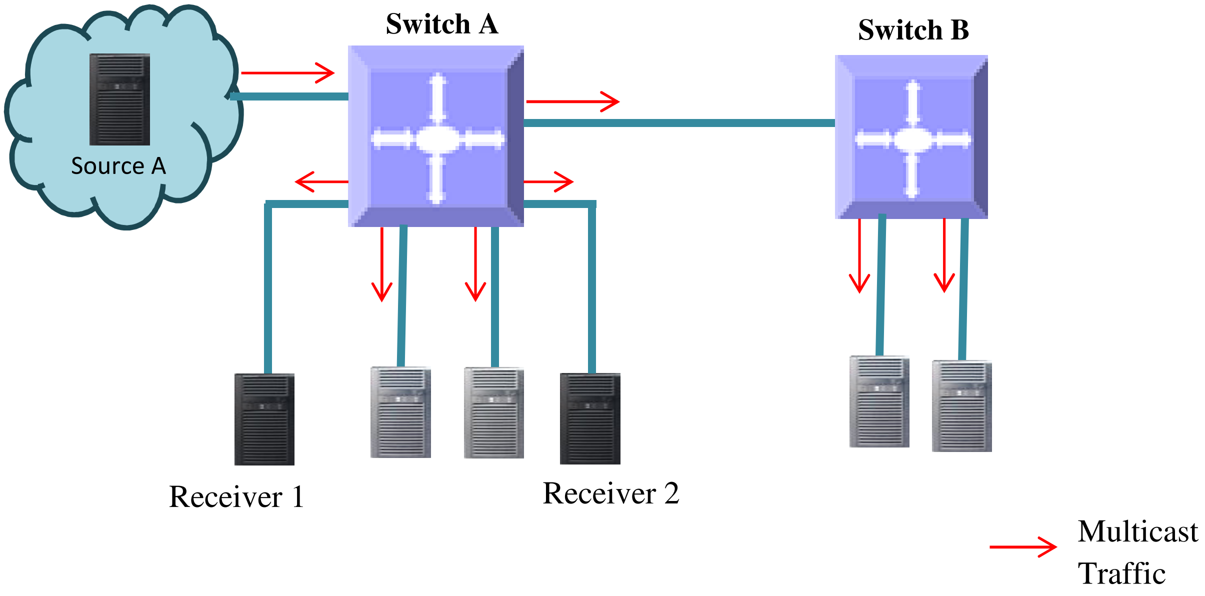
## 1.1 IGMP Snooping Basics

Switches learn the source MAC addresses for unicast traffic and forward the unicast traffic only to the required ports. But for multicast and broadcast traffic, switches forward the traffic to all ports except for the port that received that traffic. This basic multicast switching function helps all hosts connected to the switch to receive the multicast traffic.

In practical deployments, all hosts connected to a switch may not run the same multicast applications. The hosts that do not run multicast applications receive the multicast traffic unnecessarily. Similarly the multicast traffic is forwarded to other switches unnecessarily when there are no hosts connected to the other switches expecting the multicast traffic.

Forwarding multicast traffic to unnecessary hosts and switches wastes network bandwidth and computing resources. In IP TV and other similar multicast intensive deployments, this problem leads to considerable underutilization of network and compute resources.

### Figure IGS-1: Multicast Forwarding without IGMP Snooping

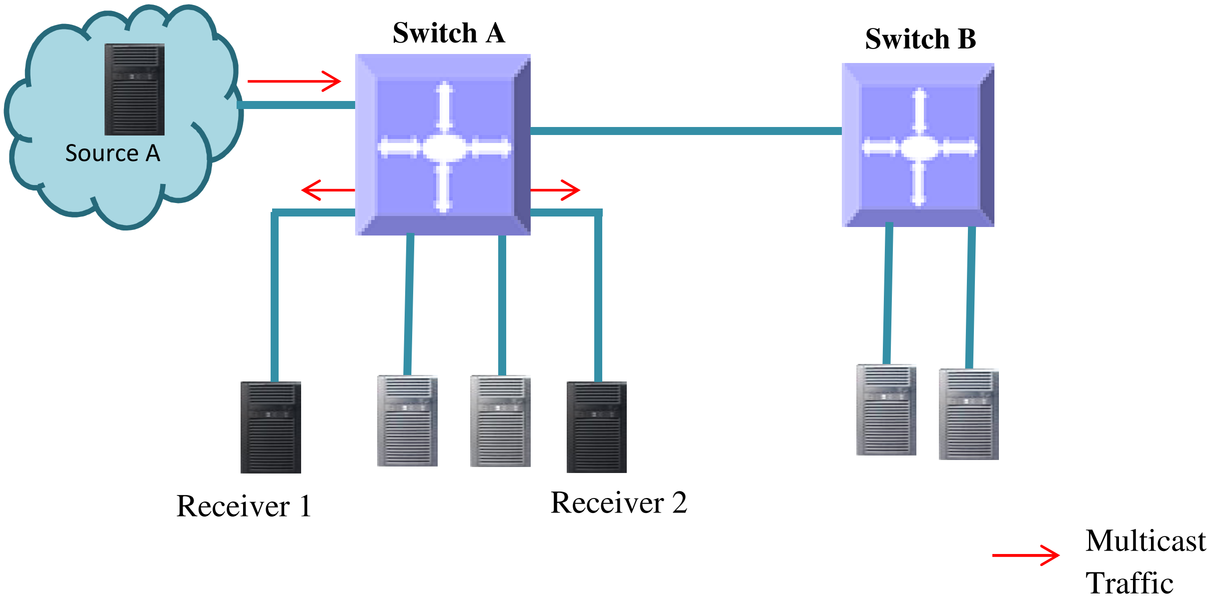


The IGMP snooping function helps the switches to forward IPv4 multicast traffic to only the ports that require IPv4 multicast traffic. This function saves network bandwidth by preventing the unnecessary flooding of IPv4 multicast traffic.

A switch performs the IGMP snooping function by snooping the Layer 3 IGMP packets and recognizes an IGMP host's connected ports by snooping the IGMP join messages sent from hosts.  Similarly, a switch recognizes an IGMP router's connected ports by snooping the IGMP control messages sent by IGMP routers. The switch maintains a multicast forwarding table based on the hosts joined and router connected ports for every multicast group and updates the multicast forwarding table when hosts leave multicast groups.

A switch forwards the multicast traffic based on the information available on the multicast table. It sends the multicast traffic of any group to only the ports that have hosts joined for that multicast group. This mechanism prevents the unnecessary flooding of multicast traffic to all the ports.

Figure IGS-2: Multicast Forwarding with IGMP Snooping



## 1.2 IGMP Snooping Support

Supermicro switches support IGMP snooping for all three IGMP versions (1, 2 and 3).

Supermicro switches support forwarding of multicast traffic based on MAC and IP addresses.

Supermicro switches support up to 255 multicast groups.

## 1.3 IGMP Snooping Defaults

| Parameter | Default Value |
|---|---|
| IGMP snooping global status | Disabled |
| IGMP snooping status in VLAN | Disabled |
| Multicast forwarding mode | MAC Based |
| Send query on topology change | Disabled |
| Proxy report | Enabled |
| Router port purge interval | 125 seconds |
| Port purge interval | 260 seconds |
| Report forward interval | 5 seconds |
| Group specific query interval | 2 seconds |
| Forwarding reports | To only router ports |
| Group specific query retry count | 2 |
| IGMP version | 3 |
| Immediate leave (fast leave) | Disabled |
| Querier | Non-querier |

| | |
|---|---|
| Query interval | 125 seconds |

## 1.4 Enabling IGMP Snooping

IGMP snooping is disabled by default in Supermicro switches.

IGMP snooping needs to be enabled globally and also needs to be enabled in VLANs individually.

Follow the steps below to enable IGMP snooping.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping** | Enables IGMP snooping globally. |
| Step 3 | **vlan <***vlan-list***>** | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.<br>If multiple VLANs are provided, the next step will enable IGMP snooping on all these VLANs. |
| Step 4 | **ip igmp snooping** | Enables IGMP snooping on VLAN. |
| Step 5 | **end** | Exits the configuration mode. |
| Step 6 | **show ip igmp snooping globals**<br>**show ip igmp snooping vlan <***vlan***>** | Displays the IGMP snooping information. |
| Step 7 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The GMRP feature needs to be in the disabled state while enabling IGMP snooping. GMRP is disabled by default in Supermicro switches.
Use the "**set gmrp disable**" command to disable the GMRP feature if needed.

The example below shows the commands to enable IGMP snooping.

**Enable IGMP snooping for VLAN 1, 10 and 20.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping
SMIS(config)# vlan 1,10,20
SMIS(config-vlan)# ip igmp snooping
SMIS(config-vlan)# end
```

# 1.5 IGMP Version

The IGMP protocol standard has three versions: v1, v2 and v3. Supermicro switches support IGMP snooping for all three versions. Supermicro IGMP snooping support interoperates with different IGMP versions as defined in IGMP protocol standard.

The default IGMP snooping version is v3, which works compatible with IGMP versions 1 and 2.

Supermicro switches provide flexibility for user to configure IGMP snooping versions for individual VLANs. User can configure different IGMP version on different VLANs.

Follow the steps below to change IGMP snooping version on any VLAN.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **vlan <*vlan-list*>** | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.<br>If multiple VLANs are provided, the next step will be applied on all these VLANs. |
| Step 3 | **ip igmp snooping version {v1 \| v2 \| v3}** | Configures IGMP snooping version. |
| Step 5 | **end** | Exits the configuration mode. |
| Step 6 | **show ip igmp snooping vlan <*vlan*>** | Displays the IGMP snooping version information for the given VLAN. |
| Step 7 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The example below shows the commands to configure different versions of IGMP snooping.

**Configure IGMP snooping version 3 for VLAN 10 and version 2 for VLAN 20.**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ip igmp snooping version v3
SMIS(config-vlan)# exit
SMIS(config)# vlan 20
SMIS(config-vlan)# ip igmp snooping version v2
SMIS(config-vlan)# end
```

## 1.6 Multicast Router Ports

Supermicro switches monitor the IGMP control messages sent by IGMP routers and recognize the ports that receive IGMP router messages as router ports.

A switch forwards the IGMP member reports from the host computers to only the router ports. If a switch does not recognize any router ports, it forwards the host computers' IGMP reports to all ports except the one that received the host report's message.

### 1.6.1 Router Port Timeouts

After finding the router ports, switches expect to periodically receive IGMP control messages from them. If IGMP receives no control messages are for a period of time from any router port, a switch will stop considering those ports as router ports until IGMP control messages are received again. This period of time is called the router port timeout value.

By default, Supermicro switches have a router port timeout value of 125 seconds. This value can be changed by following the steps below.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping mrouter-time-out** <*timeout*> | Configures the router port timeout value in seconds.<br>*timeout* – may be any value from 60 to 600 seconds.<br>The default value is 125 seconds. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping router port timeout information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping mrouter-time-out"** command resets the router timeout value to its default value of 125 seconds.

The example below shows the commands used to configure the router port timeout value.

**Configure the router port timeout value as 90 seconds.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping mrouter-time-out 90
SMIS(config)# end
```

## 1.6.2 Static Router Ports

Router ports can also be configured statically. Router ports are configured per VLAN basis.

Follow the steps below to configure the static router port for any VLAN.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **vlan <***vlan-list***>** | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.<br>If multiple VLANs are provided, the next step will configure the router ports for all these VLANs. |
| Step 3 | **ip igmp snooping mrouter <***interface-type***> <***interface-id***>** | Configures the router port.<br>*interface-type* – may be any of the following:<br>gigabit ethernet – gi<br>extreme ethernet – ex<br>qx ethernet – qx<br>port channel – po<br>*interface-id* is in *slot/port* format for all physical interfaces. It may be the port channel identifier for port channel interfaces. |
| Step 5 | **end** | Exits the configuration mode. |
| Step 6 | **show ip igmp snooping mrouter [vlan <***vlan***>]** | Displays the IGMP snooping router port information. If a VLAN identifier is provided it displays the router port for the given VLAN. If a VLAN identifier is not provided it displays the router ports |

| | | |
|---|---|---|
| | | for all the VLANs on the switch. |
| Step 7 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping mrouter** <*interface-type*> <*interface-id*>**"** command can be used to remove a statically configured router port from a VLAN.

The example below shows the commands used to configure the router ports.

**Configure port gi 0/1 as the router port for VLAN 10.**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ip igmp snooping mrouter gi 0/1
SMIS(config-vlan)# end
```

## 1.7 Leaving a Multicast Group

Host computers leave multicast groups either silently or by sending IGMP leave messages. Switches monitor the IGMP leave messages sent by host computers. When a switch receives an IGMP leave message for any group on a port, it does not delete the port from the group entry on the multicast table immediately. Instead, the switch sends an IGMP group-specific query message on the port that received the IGMP leave message. If there is any other IGMP host on that port that joined the same multicast group, the switch will receive an IGMP member report as a response. If no hosts respond on that port, the switch will assume no other IGMP hosts are connected on that port for the same group and will delete the corresponding port from the group entry on the multicast table.

Switches follow the above process only for IGMP version 2 leave messages.

The following parameters are used to control the leave message handling procedure in Supermicro switches.

**Group Query Interval** – This configures the amount of time a switch will wait to get response for its group specific queries from IGMP hosts.

**Retry Count** – This configures the number of times a switch sends a group specific query to look for IGMP hosts on the port that received an IGMP leave message.

**Immediate Leave** – This configures the switch to consider the host leave immediately instead of sending group specific query messages to look for other IGMP hosts on the port that received an IGMP leave message.

These parameters can be configured as explained below.

### 1.7.1 Group Query Interval

Switches send a group specific query messages on the port that received an IGMP leave message. Switches wait for the group query interval time to get a response from the hosts for its group specific query messages. If they receive any host member report as a response, they will drop the leave message received earlier on that port. If they do not receive any response from hosts for a group query interval time, the switches will resend a query specific message based on the retry count. When the number of times specified in the retry count is met without a response from any of the hosts, the switches will remove the port from the group entry in the multicast forwarding table.

Users can configure this group query interval. The default group query interval is 2 seconds.

Follow the steps below to configure the group query interval.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping group-query-interval <*timeout*>** | Configures the group query interval timeout.<br>*timeout* – may be any value from 2 to 5 seconds.<br>The default is 2 seconds. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping group query interval information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **“no ip igmp snooping group-query-interval”** command resets the group query interval value to its default value of 2 seconds.

The example below shows the commands used to configure the group query interval time.

**Configure the group query interval time as 5 seconds.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping group-query-interval 5
SMIS(config)# end
```

## 1.7.2 Group Query Retry Count

When no response is received from any host for the group specific query messages, switches will resend a group specific query messages. The number of times a switch retries sending the group specific query messages is configurable. The default retry count is 2.

Follow the steps below to configure the group specific query message retry count.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping retry-count <*count*>** | Configures the group specific query message retry count.<br>*count* – may be any value from 1 to 5 seconds. The default is 2. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping group specific query message retry count information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping retry-count"** command resets the group specific query retry count value to its default value of 2.

The example below shows the commands used to configure the retry count fir group specific query messages.

**Configure the group specific query message retry count as 3.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping retry-count 3
SMIS(config)# end
```

## 1.7.3 Immediate Leave

The switch can be configured to immediately remove the port from the group entry on the multicast table when any port receives an IGMP leave message without sending out group specific query messages. This function is called immediate leave and it is configurable per a VLAN basis. Immediate leave is disabled by default in all VLANs.

Follow the steps below to enable the immediate leave for any VLAN.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **vlan <***vlan-list***>** | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.<br>If multiple VLANs are provided, the next step will enable the immediate leave for all these VLANs. |
| Step 3 | **ip igmp snooping fast-leave** | Enables the IGMP immediate leave. |
| Step 4 | **end** | Exits the configuration mode. |
| Step 5 | **show ip igmp snooping vlan <***vlan***>** | Displays the IGMP snooping immediate leave information for the given VLAN. |
| Step 6 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **“no ip igmp snooping fast-leave”** command can be used to disable the immediate leave function for any VLAN.

The example below shows the commands used to enable the immediate leave function.

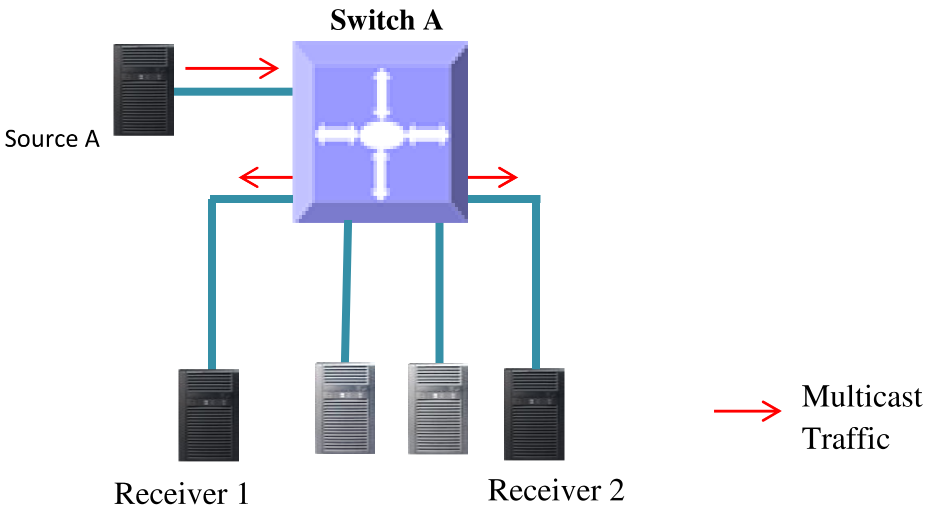
**Enable the immediate leave for the VLANs 10 and 20.**

```
SMIS# configure terminal
SMIS(config)# vlan 10,20
SMIS(config-vlan)# ip igmp snooping fast-leave
SMIS(config-vlan)# end
```

## 1.8 IGMP Snooping Querier

The IGMP snooping function needs an IGMP router on the network. Simple multicast deployments in which multicast traffic is switched and not routed may not have IGMP routers on the network. In these cases switches will have multicast hosts and sources on the same subnet as shown in the figure below.

### Figure IGS-3: Multicast Deployment Without IGMP Routers



In simple multicast networks without IGMP routers, IGMP hosts will not send periodic membership reports since there is no IGMP router to respond. Without periodic membership reports from hosts, a switch will remove all multicast group entries on port purge timeouts. The removal of multicast group entries on a switch will cause flooding of multicast traffic on all ports. To avoid this flooding, a switch can be configured as an IGMP querier.

When a switch is configured as an IGMP querier, it will send periodic queries to hosts, similar to the action of an IGMP router. This will make hosts send periodic IGMP reports and hence the multicast group entries in switches will not time out.

Supermicro switches do not act as an IGMP querier by default. Users can configure the switch to act as an IGMP querier for any required VLANs.

When a Supermicro switch acts as an IGMP querier, it sends queries every 125 seconds. This periodic time interval can be configured for every VLAN.

Follow the steps below to configure a switch as an IGMP querier for any VLAN.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **vlan** <*vlan-list*> | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, |

| | | |
|---|---|---|
| | | such as 5-10.<br>If multiple VLANs are provided, the next step will configure the switch as an IGMP querier for all these VLANs. |
| Step 3 | **ip igmp snooping querier** | Configures the switch to act as an IGMP querier. |
| Step 4 | **ip igmp snooping query-interval <***interval-value***>** | Configures the periodic interval on the switch that will send IGMP queries.<br>*interval-value* – may be any value from 60 to 600 seconds.<br>The default value is 125 seconds. |
| Step 5 | **end** | Exits the configuration mode. |
| Step 6 | **show ip igmp snooping vlan <***vlan***>** | Displays the IGMP snooping querier configuration for the given VLAN. |
| Step 7 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping querier"** command can be used to remove the IGMP querier configuration from a VLAN.

The "**no ip igmp snooping query-interval**" command can be used to set the querier periodic interval to the default value 125 seconds.

The example below shows the commands to configure the switch to act as an IGMP querier.

**Configure the switch to act as an IGMP querier for VLAN 10 and set the querier periodic interval to 300 seconds.**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ip igmp snooping querier
SMIS(config-vlan)# ip igmp snooping query-interval 300
SMIS(config-vlan)# end
```

## 1.9 Report Forward

When IGMP snooping is enabled, Supermicro switches forward IGMP host member reports to IGMP routers. When a switch has not recognized any router ports, it forwards IGMP host member reports to all ports except the port on which the host member report was received. When a switch recognizes a router port, it forwards the IGMP host member reports to only the recognized router port.

The switch behavior can be changed to forward the IGMP host member reports to all the ports except the port on which the host member report was received irrespective of router port learning.

Follow the steps below to configure a switch to forward the IGMP host member reports to all the ports except the port on which the host member report was received.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping report-forward { all-ports \| router-ports }** | Configures the IGMP host member's report forwarding behavior.<br>Use **all-ports** to configure a switch to forward IGMP host member reports to all ports.<br>Use **router-ports** to configure the switch to forward the IGMP host member reports to the router ports only.<br>The default behavior is **router-ports**. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping report-forward"** command configures the switch to the default behavior of forwarding the IGMP host member reports only to the router port.

The example below shows commands to configure the IGMP member report forwarding.

**Configure the switch to forward the IGMP member report to all ports.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping report-forward all-ports
SMIS(config)# end
```

## 1.10 Port Timeout (Port Purge Interval)

A switch recognizes a IGMP host's connected ports by snooping the IGMP join messages sent by the host and maintains a multicast forwarding table based on the host's joined ports for every multicast group.

After recognizing the host's member ports, a switch expects to receive IGMP member reports periodically on the host ports. If IGMP member reports are not received over a time period in any host member port, the switch will remove those ports from the corresponding group entry in the multicast forwarding table. This time period is called the port purge interval value. Once a host port is removed from the multicast forwarding table for any group, it will no longer receive the multicast traffic for that group.

Supermicro switches have a port purge interval value of 260 seconds by default. Users can change this value by following the steps below.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping port-purge-interval <*timeout*>** | Configures the port purge interval value in seconds.<br>*timeout* – may be any value from 130 to 1225 seconds.<br>The default value is 260 seconds. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping port purge interval information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping port-purge-interval"** command resets the port purge interval value to its default value of 260 seconds.

The example below shows commands to configure the port purge interval value.

**Configure the port purge interval value to 900 seconds.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping port-purge-interval 900
SMIS(config)# end
```

## 1.11 Report Suppression Interval

Supermicro switches forward the IGMP member reports sent by the hosts to IGMP multicast routers. To avoid forwarding duplicate reports, Supermicro switches suppress any reports received within a short time period for the same group. This time period is called the report suppression interval. Any reports received for the same group after this interval will be forwarded to multicast routers.

Supermicro switches suppress the IGMP reports for IGMP versions 1 and 2 only. If a IGMP report contains IGMP version 3 reports, switches will forward these reports to multicast routers without suppressing.

Users can configure the report suppression time period. The default value is 5 seconds.

Follow the steps below to configure the report suppression interval.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping report-suppression-interval** <*interval*> | Configures the port purge interval value in seconds.<br>*interval* – may be any value from 1 to 25 seconds.<br>The default value is 5 seconds. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping report suppression interval information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping report-suppression-interval"** command resets the report suppression interval value to its default value of 5 seconds.

The example below shows the commands used to configure the report suppression interval value.

**Configure the port report suppression interval value as 90 seconds.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping report-suppression-interval 90
SMIS(config)# end
```

# 1.12 Proxy Reporting

IGMP snooping switches maintain the states of IGMP host members. This information helps the switches send summarized IGMP reports to IGMP multicast routers. This function of IGMP snooping is called proxy reporting. This proxy reporting feature helps reduce IGMP control message traffic on the network by preventing the forwarding of every host report to the IGMP routers.

Proxy reporting is enabled by default in Supermicro switches. Users can disable or enable the proxy reporting feature by following the steps below.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **ip igmp snooping proxy-reporting** | Enables the proxy reporting feature. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping proxy reporting status information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"no ip igmp snooping proxy-reporting"** command disables the proxy reporting feature.

The example below shows the commands used to enable the proxy reporting feature.

**Enable IGMP snooping proxy reporting.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping proxy-reporting
SMIS(config)# end
```

## 1.13 Sending Queries when Topology Changes

When spanning tree topology changes, multicast traffic is often flooded. To quickly recover from the flood, switches can be configured to send general IGMP queries to all ports when spanning tree topology changes. This helps switches correctly recognize member ports based on the new spanning tree topology.

Supermicro switches do not send general IGMP queries by default when spanning tree topology changes. Users can enable the switch to send general IGMP queries when spanning tree topology change events occur. When enabled in RSTP mode, switches send general IGMP queries to all ports except for router ports. In MSTP mode, switches send general IGMP queries to all ports except for the router ports of the VLANs associated with topology changed MST instance.

Follow the steps below to enable the switch to send general IGMP queries when spanning tree topology changes.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |

| | | |
|---|---|---|
| Step 2 | **ip igmp snooping send-query enable** | Enables the switch to send general IGMP queries when spanning tree topology changes. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping information. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The **"ip igmp snooping send-query disable"** command configures the switch to not send general IGMP queries when spanning tree topology changes

The example below shows the commands used to enable a switch to send general IGMP queries when spanning tree topology changes.

**Enable the switch to send general IGMP queries when spanning tree topology changes.**

```
SMIS# configure terminal
SMIS(config)# ip igmp snooping send-query enable
SMIS(config)# end
```

## 1.14 Multicast Forwarding Mode

Multicast traffic can be forwarded based on either the destination multicast's MAC address or the its IP address. When IGMP snooping is enabled, Supermicro switches forward multicast traffic based on the destination MAC address. Users can change multicast forwarding to use the destination multicast's IP address instead of its MAC address.

Follow the steps below to configure the switch to forward the multicast traffic based on the multicast's group IP address.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **snooping multicast-forwarding-mode ip** | Configures the switch to forward the multicast traffic based on the multicast group IP address. |
| Step 3 | **end** | Exits the configuration mode. |
| Step 4 | **show ip igmp snooping globals** | Displays the IGMP snooping multicast forwarding mode. |
| Step 5 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of |

| | | |
|---|---|---|
| | | the startup configuration. |

The **"snooping multicast-forwarding-mode mac"** command configures the switch to forward the multicast traffic based on the multicast's MAC address.

The example below shows the commands used to configure a switch to forward multicast traffic based on the multicast group's IP address.

**Configure the switch to forward the multicast traffic based on the multicast group's IP address.**

```
SMIS# configure terminal
SMIS(config)# snooping multicast-forwarding-mode ip
SMIS(config)# end
```

## 1.15 Disabling IGMP Snooping

IGMP snooping is disabled by default in Supermicro switches.

After enabling IGMP snooping, it must be disabled globally and also in VLANs individually.

Follow the steps below to disable IGMP snooping.

| Step | Command | Description |
|---|---|---|
| Step 1 | **configure terminal** | Enters the configuration mode. |
| Step 2 | **no ip igmp snooping** | Disables IGMP snooping globally. |
| Step 3 | **vlan <*vlan-list*>** | Enters the VLAN configuration mode.<br>*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.<br>If multiple VLANs are provided, the next step will disable IGMP snooping on all these VLANs. |
| Step 4 | **no ip igmp snooping** | Disables IGMP snooping in VLAN. |
| Step 5 | **end** | Exits the configuration mode. |
| Step 6 | **show ip igmp snooping globals** | Displays the IGMP snooping information. |

| | | |
|---|---|---|
| | **show ip igmp snooping vlan <*vlan*>** | |
| Step 7 | **write startup-config** | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |

The example below shows the commands used to disable IGMP snooping.

**Disable the IGMP snooping function assuming the switch has VLANs 1, 10 and 20.**

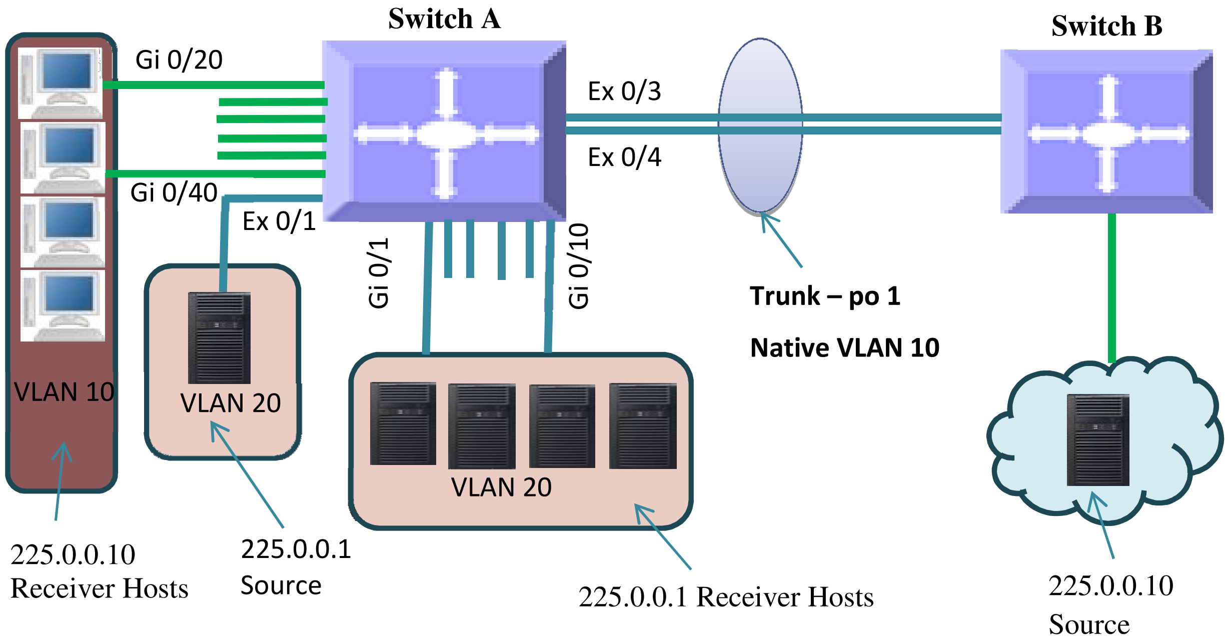
```
SMIS# configure terminal
SMIS(config)# no ip igmp snooping
SMIS(config)# vlan 1,10,20
SMIS(config-vlan)# no ip igmp snooping
SMIS(config-vlan)# end
```

## 1.16 IGMP Snooping Configuration Example

Configure the following requirements on Switch A as shown below in Figure IGS-4.

1. Enable IGMP snooping.
2. There is no multicast router for group 225.0.0.1 so configure the switch as a querier for this group.
3. Use IGMP v2 for group 225.0.0.1 and also enable fast leave since hosts are directly connected to the switch.
4. Disable the proxy reporting.
5. Enable the switch to send general IGMP queries when spanning tree topology changes.

### Figure IGS-4 IGMP Snooping Configuration Example



```
SMIS# configure terminal

# Create all the required VLANs first
SMIS(config)# vlan 10,20
SMIS(config-vlan)# exit

# Add member ports to VLAN 10
SMIS(config)# int range gi 0/20-40
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# exit

# Add member ports to VLAN 20
SMIS(config)# int range ex 0/1 gi 0/1-10
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan 20
SMIS(config-if)# exit

# Create the port channel 1 interface
SMIS(config)# int port-channel 1
SMIS(config-if)# exit

# Add member ports to the port channel 1 interface
SMIS(config)# int range ex 0/3-4
SMIS(config-if)# channel-group 1 mode active
SMIS(config-if)# exit
```

```
# Configure the VLAN requirements for the port channel 1 interface
SMIS(config)# int port-channel 1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk native vlan 10
SMIS(config-if)# exit

# Req.1 Enable IGMP Snooping
SMIS(config)# ip igmp snooping
SMIS(config)# vlan 10,20
SMIS(config-vlan)# ip igmp snooping
SMIS(config-vlan)# exit

# Req.2 Configure the switch as a querier for group 225.0.0.1
SMIS(config)# vlan 20
SMIS(config-vlan)# ip igmp snooping querier
SMIS(config-vlan)# exit

# Req.3 Configure IGMP v2 and fast leave for group 225.0.0.1
SMIS(config)# vlan 20
SMIS(config-vlan)# ip igmp snooping version v2
SMIS(config-vlan)# ip igmp snooping fast-leave
SMIS(config-vlan)# exit

# Req.4 Disable proxy reporting
SMIS(config)# no ip igmp snooping proxy reporting

# Req.5 Enable the switch to send general IGMP queries when spanning tree topology changes
SMIS(config)# ip igmp snooping send-query enable

# Check the running-configuration for accuracy
SMIS# show running-config

Building configuration...
Switch ID     Hardware Version            Firmware Version
0           SSE-G48-TG4   (P2-01)        1.0.13-10

interface port-channel 1
exit

vlan 1
ports gi 0/11-19 untagged
ports gi 0/41-48 untagged
ports ex 0/2 untagged
exit
vlan 10
ports gi 0/20-40 untagged
ports po 1 untagged
exit
```

```
vlan 20
exit

interface Gi 0/1
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/2
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/3
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/4
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/5
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/6
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/7
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/8
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/9
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/10
switchport trunk allowed vlan 20
switchport mode trunk

interface Gi 0/20
switchport access vlan 10
switchport mode access

interface Gi 0/21
```

```
switchport access vlan 10
switchport mode access

interface Gi 0/22
switchport access vlan 10
switchport mode access

interface Gi 0/23
switchport access vlan 10
switchport mode access

interface Gi 0/24
switchport access vlan 10
switchport mode access

interface Gi 0/25
switchport access vlan 10
switchport mode access

interface Gi 0/26
switchport access vlan 10
switchport mode access

interface Gi 0/27
switchport access vlan 10
switchport mode access

interface Gi 0/28
switchport access vlan 10
switchport mode access

interface Gi 0/29
switchport access vlan 10
switchport mode access

interface Gi 0/30
switchport access vlan 10
switchport mode access

interface Gi 0/31
switchport access vlan 10
switchport mode access

interface Gi 0/32
switchport access vlan 10
switchport mode access

interface Gi 0/33
```

```
switchport access vlan 10
switchport mode access

interface Gi 0/34
switchport access vlan 10
switchport mode access

interface Gi 0/35
switchport access vlan 10
switchport mode access

interface Gi 0/36
switchport access vlan 10
switchport mode access

interface Gi 0/37
switchport access vlan 10
switchport mode access

interface Gi 0/38
switchport access vlan 10
switchport mode access

interface Gi 0/39
switchport access vlan 10
switchport mode access

interface Gi 0/40
switchport access vlan 10
switchport mode access

interface Ex 0/1
switchport trunk allowed vlan 20
switchport mode trunk

interface Ex 0/3
channel-group 1 mode active

interface Ex 0/4
channel-group 1 mode active

interface po 1
switchport trunk native vlan 10
switchport mode trunk
exit

ip igmp snooping
no ip igmp snooping proxy-reporting
```

```
vlan 20
ip igmp snooping fast-leave
ip igmp snooping version v2
ip igmp snooping querier
exit
SMIS#

SMIS# sh ip igmp snooping globals
Snooping Configuration
-----------------------------
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
Transmit Query on Topology Change globally enabled
Multicast forwarding mode is MAC based
Proxy reporting globally disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 2 seconds
Reports are forwarded on router ports
Group specific query retry count is 2

SMIS# show ip igmp snooping vlan 10
Snooping VLAN Configuration for the VLAN 10
IGMP Snooping enabled
IGMP Operating version is V3
Fast leave is disabled
Snooping switch is acting as Non-Querier
Query interval is 125 seconds

SMIS# show ip igmp snooping vlan 20
Snooping VLAN Configuration for the VLAN 20
IGMP Snooping enabled
IGMP configured version is V2
IGMP Operating version is V2
Fast leave is enabled
Snooping switch is configured as Querier
Snooping switch is acting as Querier
Query interval is 125 seconds
SMIS#

# Save this port channel configuration.
SMIS# write startup-config
Building configuration, Please wait. May take a few minutes ...
[OK]
SMIS#
```