Switch Configuration User’s Guide

Revision 1.12

The information in this USER’S GUIDE 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.
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.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Manual Revision 1.12
Release Date: 11/12/2019

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.

Copyright © 2019 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America
## Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/27/2018</td>
<td>1.2</td>
<td>Initial document.</td>
</tr>
<tr>
<td>08/24/2018</td>
<td>1.3</td>
<td>Updated SNMP and ACL configuration details.</td>
</tr>
<tr>
<td>10/24/2018</td>
<td>1.4</td>
<td>Removed ACL egress port configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated string length in SNMP targetparams, System contact, System location commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrected typo in ‘lldp tlv-select’ commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added port splitting section.</td>
</tr>
<tr>
<td>02/05/2019</td>
<td>1.5</td>
<td>Added loop protection in System Configuration section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Also added Unknown Multicast Filtering in IGMP Snooping section.</td>
</tr>
<tr>
<td>02/05/2019</td>
<td>1.6</td>
<td>Added IPv4 Layer-3 routing details.</td>
</tr>
<tr>
<td>03/25/2019</td>
<td>1.7</td>
<td>Added section 5.2.5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed Physical L3 Interface.</td>
</tr>
<tr>
<td>04/10/2019</td>
<td>1.8</td>
<td>Removed IGMP configurations on router ports, as we router ports are not supported yet.</td>
</tr>
<tr>
<td>05/31/2019</td>
<td>1.9</td>
<td>Corrected vendor-class in Section 2.8.5</td>
</tr>
<tr>
<td>09/05/2019</td>
<td>1.10</td>
<td>Added DCBX section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated spanning-tree port priority value range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated ip pim message-interval value range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corrected the default ip pim lan-prune-delay value to disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fixed the missing page numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added login authentication fallback commands.</td>
</tr>
<tr>
<td>09/11/2019</td>
<td>1.11</td>
<td>Updated the default IP PIM Hold time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated OSPF configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated the Interface split section.</td>
</tr>
<tr>
<td>11/12/2019</td>
<td>1.12</td>
<td>Updated default unique password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed the configuration IP PIM Hold time.</td>
</tr>
</tbody>
</table>
Contents

1 Introduction .................................................................................................................. 16
  1.1 Features ................................................................................................................. 16
  1.2 Cables .................................................................................................................... 17
  1.3 Management Interface .......................................................................................... 17
    1.3.1 Console Port ................................................................................................... 18
2 System Configuration ................................................................................................... 19
  2.1 Management IP ...................................................................................................... 19
    2.1.1 Static Management IP Address ..................................................................... 19
    2.1.2 DHCP ............................................................................................................ 19
    2.1.3 Default IP Gateway ...................................................................................... 20
  2.2 Management Access ............................................................................................... 20
    2.2.1 User Login .................................................................................................... 21
    2.2.2 Enable ........................................................................................................... 22
    2.2.3 Enable Password ......................................................................................... 22
    2.2.4 IP Authorized Manager ............................................................................... 23
  2.3 Interface Properties ................................................................................................. 24
    2.3.1 Description .................................................................................................... 25
    2.3.2 Negotiation ................................................................................................... 28
    2.3.3 Speed ............................................................................................................. 31
    2.3.4 Duplex Operation ......................................................................................... 34
    2.3.5 MTU ............................................................................................................... 35
    2.3.6 Flow Control .................................................................................................. 37
    2.3.7 Storm Control ............................................................................................... 38
    2.3.8 Forward Error Correction (FEC) Mode ......................................................... 40
    2.3.9 Port Splitting ................................................................................................ 41
  2.4 Time Management .................................................................................................. 42
    2.4.1 NTP Server .................................................................................................... 43
    2.4.2 Enable/Disable NTP ..................................................................................... 44
    2.4.3 NTP Authentication ....................................................................................... 44
    2.4.4 NTP Broadcast ............................................................................................... 45
    2.4.5 System Clock ................................................................................................ 46
    2.4.6 Time Zone ..................................................................................................... 47
  2.5 System Management ............................................................................................... 48
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1</td>
<td>Switch Name</td>
</tr>
<tr>
<td>2.5.2</td>
<td>Switch Contact</td>
</tr>
<tr>
<td>2.5.3</td>
<td>System Location</td>
</tr>
<tr>
<td>2.5.4</td>
<td>System MTU</td>
</tr>
<tr>
<td>2.5.5</td>
<td>Static MAC</td>
</tr>
<tr>
<td>2.5.6</td>
<td>MAC Aging</td>
</tr>
<tr>
<td>2.6</td>
<td>System Logging (Syslog)</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Enable/Disable Syslog</td>
</tr>
<tr>
<td>2.6.2</td>
<td>Syslog Server</td>
</tr>
<tr>
<td>2.6.3</td>
<td>Console Log</td>
</tr>
<tr>
<td>2.6.4</td>
<td>Log File</td>
</tr>
<tr>
<td>2.6.5</td>
<td>Logging Buffer</td>
</tr>
<tr>
<td>2.6.6</td>
<td>Facility</td>
</tr>
<tr>
<td>2.6.7</td>
<td>Traps</td>
</tr>
<tr>
<td>2.6.8</td>
<td>Clear Log Buffer</td>
</tr>
<tr>
<td>2.6.9</td>
<td>Clear Log File</td>
</tr>
<tr>
<td>2.7</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>2.7.1</td>
<td>Save Startup-Config</td>
</tr>
<tr>
<td>2.7.2</td>
<td>Save Running Configuration to File</td>
</tr>
<tr>
<td>2.7.3</td>
<td>Configuring Startup Config File Name</td>
</tr>
<tr>
<td>2.7.4</td>
<td>Copy Startup-config</td>
</tr>
<tr>
<td>2.7.5</td>
<td>Copy File</td>
</tr>
<tr>
<td>2.7.6</td>
<td>Deleting a Saved Configuration</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Firmware Upgrade</td>
</tr>
<tr>
<td>2.7.7</td>
<td>Boot-up Options</td>
</tr>
<tr>
<td>2.7.8</td>
<td>Reset to Factory Defaults</td>
</tr>
<tr>
<td>2.8</td>
<td>Zero Touch Provisioning</td>
</tr>
<tr>
<td>2.8.1</td>
<td>ZTP Config Restore</td>
</tr>
<tr>
<td>2.8.2</td>
<td>ZTP Info</td>
</tr>
<tr>
<td>2.8.3</td>
<td>ZTP Firmware Upgrade</td>
</tr>
<tr>
<td>2.8.4</td>
<td>Disable ZTP</td>
</tr>
<tr>
<td>2.8.5</td>
<td>DHCP Vendor Class</td>
</tr>
<tr>
<td>2.9</td>
<td>Tracking Uplink Failures</td>
</tr>
<tr>
<td>2.10</td>
<td>Loop Protection</td>
</tr>
</tbody>
</table>
Sending Queries When Topology Changes

Proxy Reporting

Port Timeout (Port Purge Interval)

Report Forward

IGMP Snooping Querier

Immediate Leave

Group Query Retry Count

Leaving a Multicast Group

Static Router Ports

Router Port Timeouts

IGMP Version

IGMP Snooping Support

Enabling IGMP Snooping

Auto Edge

Link Type

Spanning Tree Configuration Examples

Link Type

Auto Edge

Port Fast

Topology Change Guard

Root Guard

Transmit Hold Count

Path Cost Long/Short

Group Query Interval

Group Query Retry Count

Immediate Leave

IGMP Snooping Querier

Report Forward

Port Timeout (Port Purge Interval)

Report Suppression Interval

Proxy Reporting

Sending Queries When Topology Changes
8  ACL............................................................................................................................ 223

8.1 Types of ACLs ........................................................................................................ 223

8.1.1 MAC Extended ACL............................................................................................. 224

8.1.2 IP Standard ACL .................................................................................................. 224

8.1.3 IP Extended ACL ................................................................................................. 224

8.2 MAC Extended ACL................................................................................................. 224

8.2.1 Creating MAC Extended ACLs ............................................................................. 225

8.2.2 Modifying MAC Extended ACLs ........................................................................ 227

8.2.3 Removing MAC Extended ACLs ......................................................................... 227

8.2.4 Applying MAC Extended ACLs to Interfaces .................................................... 228

8.2.5 ACL Ingress Port Configuration ......................................................................... 228

8.2.6 Displaying MAC Extended ACLs ...................................................................... 230

8.2.7 MAC Extended ACL Configuration .................................................................. 231

8.3 IP Standard ACL ...................................................................................................... 232

8.3.1 Creating IP Standard ACLs ................................................................................ 233

8.3.2 Modifying IP Standard ACLs ............................................................................. 234

8.3.3 Removing IP Standard ACLs ............................................................................. 235

8.3.4 Applying IP ACLs to Interfaces ......................................................................... 235

8.3.5 ACL Ingress Port Configuration ......................................................................... 235

8.3.6 Displaying IP Standard ACLs ............................................................................ 237

8.3.7 IP Standard ACL Configuration Example 1 ...................................................... 238

8.3.8 IP Extended ACLs .............................................................................................. 239

8.3.9 Creating IP Extended ACLs for IP Traffic ......................................................... 240

8.3.10 Creating IP Extended ACLs for TCP Traffic .................................................. 242

8.3.11 Creating IP Extended ACLs for UDP Traffic .................................................. 244

8.3.12 Creating IP Extended ACLs for ICMP Traffic ................................................ 246

8.3.13 Modifying IP Extended ACLs ........................................................................... 247

8.3.14 Removing IP Extended ACLs .......................................................................... 248

8.3.15 Applying IP Extended ACLs to Interfaces ....................................................... 248

8.3.16 Displaying IP Extended ACLs .......................................................................... 248

8.4 IP Extended ACL Configuration Example 1 .......................................................... 251
18.2.8 Router Id ................................................................. 444
18.2.9 Priority ............................................................... 444
18.2.10 Route Summarization ......................................... 444
18.2.11 Authentication .................................................... 444
18.2.12 Timers .............................................................. 444
18.2.13 Virtual Link ....................................................... 445
18.2.14 Passive Interface ............................................... 445
18.2.15 Demand Circuit .................................................. 445
18.2.16 Network Type .................................................... 445
18.2.17 OSPF Configuration ............................................. 446
18.3 BGP ................................................................. 456
  18.3.1 Router ID .......................................................... 457
  18.3.2 Speaker and Peer .............................................. 457
  18.3.3 Autonomous System (AS) ................................ 457
  18.3.4 Aggregate Addresses ...................................... 457
  18.3.5 Route Reflection ............................................... 457
  18.3.6 Confederation .................................................. 458
  18.3.7 Attributes ........................................................ 458
  18.3.8 Filters ............................................................ 459
  18.3.9 Overlapping Routes .......................................... 459
  18.3.10 Synchronization .............................................. 459
  18.3.11 BGP Path selection ....................................... 460
  18.3.12 Timers .......................................................... 460
  18.3.13 Route dampening ......................................... 460
  18.3.14 BGP Configuration ........................................ 461
19 PIM Configuration ..................................................... 474
  19.1 PIM ................................................................. 475
    19.1.1 PIM-SM Basics .............................................. 475
    19.1.2 PIM-DM Basics ............................................. 476
  19.2 PIM Support ....................................................... 476
  19.3 PIM Defaults ..................................................... 477
  19.4 Enabling PIM ...................................................... 477
  19.5 PIM Component and Interface ................................ 478
  19.6 PIM Mode ........................................................ 481
1 Introduction
This document explains the switch configuration for Supermicro switch model SSE-SSE-F3548S and its companion model, the SSE-F3548SR. The SSE-F3548SR model features a data-center-friendly reverse airflow technique for improved cooling when installed in the rear of a rack.

Regular Airflow (front to back)
SSE-F3548S

Reverse Airflow (back to front)
SSE-F3548SR

The SSE-F3548S and SSE-F3548SR Layer 2+ Ethernet switches both offer 48 25Gb Ethernet (GbE) ports allowing connectivity to 25GbE servers. These 48 ports can also run in 10Gb or 1Gb mode to connect to existing low-speed network devices. The SSE-F3548S/R also offer six ports running at 100Gbps for access to high-speed backbone networks or storage servers. These 100Gbps ports can also operate at 40Gbps or each can be split into four different ports to run at 25Gbps or 10Gbps.

This document explains the configuration for Supermicro switch models SSE-SSE-G3548S/R.

1.1 Features
Other major features of the SSE-F3548S/R include:

- **Layer 2 Features**:
  - 4K VLANS
  - Spanning Tree (802.1D)
  - Rapid Spanning Tree (802.1w)
  - Multiple Spanning Trees (802.1s)
  - IEEE 802.1Q VLANs/ port-based VLANs
  - IEEE 802.3ad with LACP
  - IEEE 802.1AB Link Layer Discovery Protocol (LLDP)

- **Advanced Layer 2 Features**:
  - Storm control
  - Flow control
  - Port mirroring
  - Uplink Failure Detection (UFD)
  - MLAG

- **System Management**:
  - Industry Standard CLI
  - Context Sensitive Help
  - Command Completion
  - SNMP v1/v2/v3
- SSH
- Syslog
- DHCP (Client)
- Web-based management interface
- NTP
- RMON

- **Multicast:**
  - IGMP Snooping

- **Ethernet frame:**
  - Jumbo frames up to 9KB

- **Power:**
  - Redundant Hot-pluggable 500W Power Supplies
  - AC Input: 100-127/200-240 V, 50/60 Hz
  - Power Consumption: 410 Watts

- **Physical/Environmental:**
  - 1U form factor for flexible installation
  - Net weight: 8.9 Kg (19.6 lb) with 2 PSUs
  - Size (W x D x H): 445 x 510 x 44 mm (17.52 x 20.1 x 1.73 inches)
  - Operating Temperature: 0°C to 45°C (32°F to 113°F)
  - Operating Humidity: 0% to 95% RH

Mounting rails are included for ease of installation to a rack.

### 1.2 Cables

The following cables and transceivers are supported:

<table>
<thead>
<tr>
<th>Item</th>
<th>Supermicro Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C05M</td>
<td>0.5m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C10M</td>
<td>1m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C15M</td>
<td>1.5m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C20M</td>
<td>2m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C25M</td>
<td>2.5m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>SFP28 Copper Cable</td>
<td>CBL-NTWK-0944-MS28C30M</td>
<td>3m 25GbE SFP28 to SFP28, Passive</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C05M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 0.5M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C10M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 1M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C15M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 1.5M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C20M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 2M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C25M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 2.5M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0942-QSFP28C30M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 3M</td>
</tr>
<tr>
<td>Ethernet</td>
<td>CBL-NTWK-0943-QSFP28C10M</td>
<td>Ethernet, QSFP28, 100GbE, Passive, 1M</td>
</tr>
<tr>
<td>QSFP28 Transceiver Module</td>
<td>AOM-100GBE-SR4-FT</td>
<td>QSFP28 transceiver module for short rage fiber cables (up to 100m), 100G, 850nm, MMF</td>
</tr>
</tbody>
</table>

### 1.3 Management Interface

The Supermicro switch can be managed in the following methods.

- Command Line Interface
- Web Interface
- SNMP
- RESTCONF – Rest APIs using OPENCONFIG Yang Models
This document discusses mainly the command line interface configuration method. To manage using RESTCONF, refer the RESTCONF user guide.

The Supermicro switch command line interface (CLI) is accessible through an RS232 console port, or via Telnet and SSH connections. The CLI is designed to follow industry standard CLI commands. Standard features including context sensitive “help” and auto-completion-on-tab-key are supported.

Log into the switch with the user ID ‘ADMIN’ and the password can be found on the label stuck on the switch.

After you log into the switch CLI, you are automatically placed in the user EXEC mode. This mode supports “show” commands and minimal configuration commands.

**To enter the configuration mode, use the command “configure terminal”. For example:**

```
SMIS# configure terminal
SMIS(config)#
```

To exit to EXEC mode, use the command *exit* or *end*.

### 1.3.1 Console Port

The SSE-G3548S/R has an RJ45 connector for the RS232 console port.

Use the serial cable provided with the switch to connect the RS232 port to any computer.

The computer COM port settings should be as follows:

- **Baudrate:** 115200
- **Data:** 8 bit
- **Parity:** none
- **Stop:** 1 bit
- **Flow Control:** none

Further information on Management Access can be found in Section 2.2 of this manual.
2 System Configuration

2.1 Management IP
The SSE-G3548S/R comes with DHCP IP settings for default IP management.

2.1.1 Static Management IP Address
The IP address command can be used to manually configure the management interface IP address.

Follow the steps below to manually configure the management interface IP address.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip address [&lt;ip-address&gt;</td>
<td>&lt;ip-address&gt;/prefix-length] [&lt;subnet-mask&gt;]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip-address – A valid IPv4 Address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip-address/prefix-length - A valid IPv4 Address with a prefix length of 1-32.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>subnet-mask – A valid IP subnet mask.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip interface</td>
<td>Displays the management interface IP configuration.</td>
</tr>
</tbody>
</table>

The manual IP address configuration is saved automatically as part of the start-up config.

The “no ip address” command resets the switch IP address to 0.0.0.0.

The example below shows the commands used to configure the management interface IP address manually.

SMIS# configure terminal
SMIS(config)# ip address 192.168.1.10
SMIS(config)# end

2.1.2 DHCP
Supermicro switches can be configured to obtain the management IP address through DHCP protocol. In this case, the switch acts as a DHCP client and obtains an IP address for any DHCP server on the LAN.

DHCP is the default management IP address mode.

Follow the steps below to obtain the management interface IP address dynamically from a DHCP server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
Step 2 | ip address dhcp | Configures the management interface IP address through DHCP server.
---|---|---
Step 3 | End | Exits the configuration mode.
Step 4 | show ip interface | Displays the Management interface IP configuration.

The **IP address dhcp** configuration is saved automatically as part of start-up config.

The “no ip address dhcp” command disables configuring the management interface IP address through DHCP server.

The example below shows the commands used to configure the management interface IP address through DHCP.

SMIS# configure terminal
SMIS(config)#ip address dhcp
SMIS(config)# end

### 2.1.3 Default IP Gateway

To configure default gateway on the switch follow the steps below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | ip gateway <ip-address> | Configure IP gateway.  
*ip-address* – IP address of a directly connected router. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show ip interface | Displays the interface IP configuration. |

The **IP Gateway** configuration is saved automatically as part of start-up config.

The “no ip gateway” command resets the switch IP gateway to its default value of 0.0.0.0.

The example below shows the commands used to configure the IP gateway.

SMIS# configure terminal
SMIS(config)# ip gateway 10.1.1.1
SMIS(config)# end

### 2.2 Management Access

Supermicro switches enable access control of the switch by various mechanisms:
- User name and password
- Enable password
- Authorized Managers

Defaults – Management Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default User Name</td>
<td>ADMIN</td>
</tr>
<tr>
<td>Password</td>
<td>Default password is unique for each switch and it can be found on the label stuck on the switch.</td>
</tr>
<tr>
<td>Privilege for default user ADMIN.</td>
<td>15</td>
</tr>
<tr>
<td>Default privilege for configured users.</td>
<td>1</td>
</tr>
<tr>
<td>IP Authorized Managers</td>
<td>None</td>
</tr>
</tbody>
</table>

2.2.1 User Login

User accounts can be configured for switch access. Each username can be associated with a password and privilege level. Users configured with a password are authenticated while accessing the switch to the configured privilege level.

Users with privilege level 1 or above can execute all “show” commands. To execute configuration commands, access with privilege level 15 is required.

Follow the steps below to configure the username.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | username <user-name> [password <passwd>] [privilege <1-15>] | Configure username and password.  
user-name – Alphanumeric characters of length 1-20  
password – Alphanumeric characters of length 1-20  
privilege - Specify 1-15, any of the privilege levels |
| Step 3 | End                                   | Exits the configuration mode.                                                                     |
| Step 4 | list users                            | Displays the users available in the switch.                                                          |
|       | show users                            | Displays users that are currently logged in.                                                          |

The *username* configuration is saved automatically as part of start-up config. Configured users are not displayed in ‘show running config’ command.

The “no username <user-name>” command deletes the configured user.
The example below shows the commands used to configure users.

SMIS# configure terminal
SMIS(config)# username user1 password pwd1 privilege 15
SMIS(config)# end

SMIS# list users

<table>
<thead>
<tr>
<th>Users</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN</td>
<td>15</td>
</tr>
<tr>
<td>user1</td>
<td>15</td>
</tr>
</tbody>
</table>

SMIS# show users

Line | User | Peer-Address
--- | ---- | ------------|
0 con| user1| Local Peer

2.2.2 Enable

Supermicro switches provide support for configuring access to various CLI commands. This is achieved by *Enable* password and *privilege levels*. Fifteen privilege levels can be specified.

Follow the steps below to enable a privilege level.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>enable [&lt;1-15&gt; Enable Level]</td>
<td>Enable a privilege level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Enable Level</em> – Specify 1-15, any of the privilege levels</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

The example below shows the command used to enable a particular privilege level.

SMIS# enable15

2.2.3 Enable Password

Passwords for different enable levels can be configured by the switch administrator using the *enable password* command.

Follow the steps below to enable password for any privilege level.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>enable password [level (1-15)] &lt;LINE 'enable' password&gt;</td>
<td>Configure password for a particular privilege level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Level</em> – Specify 1-15, any of the privilege levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>LINE enable password</em> – Alphanumeric</td>
</tr>
</tbody>
</table>
Step 3 | End | Exits the configuration mode.

The *enable password* configuration is saved automatically as part of start-up config. Enable password configuration is not displayed in the ‘show running config’ command.

The “no enable password [level (1-15)]” command disables the enable password parameters.

The example below shows the commands used to configure *enable password*.

SMIS# configure terminal
SMIS(config)# enable password level 10 pwd1

### 2.2.4 IP Authorized Manager

Supermicro switches allow configuration of IP authorized managers. This feature enhances security on the switch by using IP addresses to authorize computers are allowed to:

- Access the switch’s web browser interface
- Telnet into the switch’s console interface
- Use SNMP or SSH

Follow the steps below to configure authorized managers for the switch.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>authorized-manager ip-source &lt;ip-address&gt;[[&lt;subnet-mask&gt;</td>
<td>/ &lt;prefix-length(1-32)&gt;]] [interface [&lt;interface-type &lt;0/a-b, 0/c, ...&gt;]] [vlan&lt;a,b or a,b or a,b,c-d&gt;] [service [snmp] [telnet] [http] [http s] [ssh]]</td>
</tr>
</tbody>
</table>
If IP Authorized Managers are configured in a Supermicro switch, access to the switch via telnet, ssh, etc. is possible only by those hosts allowed to access. Other hosts will not be permitted access.

The “no authorized-manager ip-source <ip-address> [/<subnet-mask> | /<prefix-length(1-32)>]]” command deletes the particular authorized manager.

The example below shows the commands used to configure Authorized Managers.

```
SMIS# configure terminal
SMIS(config)#authorized-manager ip-source 200.200.200.10 service telnet
SMIS(config)# authorized-manager ip-source 100.100.100.10 service http
SMIS(config)# end
SMIS# show authorized-managers
Ip Authorized Manager Table
-------------------------
Ip Address: 100.100.100.10
Ip Mask: 255.255.255.255
Services allowed: HTTP
Ip Address: 200.200.200.10
Ip Mask: 255.255.255.255
Services allowed: TELNET
```

### 2.3 Interface Properties

The SSE-F3548S/R supports the following physical interface types.

**25G Fx Ports**

The SSE-F3548S/R has 48 Fx ports by default. The Fx ports operate at 25G speed by default and can be configured to operate at 10G or 1G speed.
100G Cx Ports
The SSE-F3548S/R has six 100G capable Cx ports by default. The Cx ports can also operate at 40G speed. Additionally, each Cx port can be split into four ports that can operate at 25G or 10G speed. Use the speed command in interface mode to split the ports. The below table shows the port names in the split cases.

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Interface Numbers</th>
<th>Speed</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx</td>
<td>1 – 48</td>
<td>25G default Can operate in 10G/1G</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Cx</td>
<td>1 – 6</td>
<td>100G default Can operate in 40G Or can be split into 4 ports</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Fx</td>
<td>49 – 51</td>
<td>25G / 10G</td>
<td>When Cx 0/1 splitted – it becomes Cx 0/1, Fx 49, Fx 50 and Fx 51</td>
</tr>
<tr>
<td>Fx</td>
<td>52 – 54</td>
<td>25G / 10G</td>
<td>When Cx 0/2 splitted – it becomes Cx 0/2, Fx 52, Fx 53 and Fx 54</td>
</tr>
<tr>
<td>Fx</td>
<td>55 – 57</td>
<td>25G / 10G</td>
<td>When Cx 0/3 splitted – it becomes Cx 0/3, Fx 55, Fx 56 and Fx 57</td>
</tr>
<tr>
<td>Fx</td>
<td>58 – 60</td>
<td>25G / 10G</td>
<td>When Cx 0/4 splitted – it becomes Cx 0/4, Fx 58, Fx 59 and Fx 60</td>
</tr>
<tr>
<td>Fx</td>
<td>61 – 63</td>
<td>25G / 10G</td>
<td>When Cx 0/5 splitted – it becomes Cx 0/5, Fx 61, Fx 62 and Fx 63</td>
</tr>
<tr>
<td>Fx</td>
<td>64 – 66</td>
<td>25G / 10G</td>
<td>When Cx 0/6 splitted – it becomes Cx 0/6, Fx 64, Fx 65 and Fx 66</td>
</tr>
</tbody>
</table>

Supermicro switches also support port channel interfaces. Each interface has different characteristics, some of which are configurable.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>1500 bytes</td>
</tr>
<tr>
<td>Negotiation</td>
<td>Enabled</td>
</tr>
<tr>
<td>Storm-control</td>
<td>Disabled</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
</tr>
<tr>
<td>Duplex Operation</td>
<td>Full</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Off</td>
</tr>
<tr>
<td>FEC Mode</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

2.3.1 Description
Supermicro switches allow users to configure a description string to the interfaces. This description string will be useful to identify the interfaces easily.

Follow the steps below to configure interface description string.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;&lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode. Interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx Interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>description <code>&lt;string&gt;</code></td>
<td>Configure the interface description String – alphanumeric characters of length 1-64.</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface description</td>
<td>Displays the interface description configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure interface description.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/22
SMIS(config-if)# description Server_Cluster_0100
SMIS(config-if)# end
SMIS

# sh int description

Interface    Status   Protocol  Description
---------   ------   -------    --------
```
<table>
<thead>
<tr>
<th>Fx0/1</th>
<th>up</th>
<th>down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/2</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/6</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/7</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/8</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/9</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/10</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/11</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/12</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/13</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/14</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/16</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/17</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/18</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/19</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/20</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/21</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/22</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/23</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/24</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/25</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/26</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/27</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/28</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/29</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>Fx0/30</td>
<td>up</td>
<td>down</td>
</tr>
</tbody>
</table>
2.3.2 Negotiation

Interface speed can be negotiated between connected devices, if both ends support negotiation.

Auto negotiation is enabled by default on all the Fx and Cx ports. It can be disabled if needed by using the ‘no negotiation’ command. **Auto negotiation is not supported for 40G speeds.** Turn off auto negotiation to set the Cx port speed to 40G.
Follow the steps below to configure Interface Negotiation.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ….</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type – may be any of the following: cx-ethernet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range cx 0/1-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range cx 0/1-2, cx 0/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Negotiation</td>
<td>Enable Interface Negotiation</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface status</td>
<td>Displays the interface configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no negotiation” command disables interface negotiation.

The example below shows the commands used to configure Interface Negotiation.

SMIS# configure terminal
SMIS(config)# interface Cx 0/2
SMIS(config-if)# no negotiation
SMIS(config-if)# end
SMIS

# sh int status
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Duplex</th>
<th>Speed</th>
<th>Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/2</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/6</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/7</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/8</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/9</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/10</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/11</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/12</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/13</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/14</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/16</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/17</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/18</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/19</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/20</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/21</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/22</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/23</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/24</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/25</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/26</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/27</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/28</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Interface</td>
<td>Connection Status</td>
<td>Speed Status</td>
<td>Speed</td>
<td>Auto-Negotiation Status</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
<td>--------------</td>
<td>-------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Fx0/29</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/30</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/31</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/32</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/33</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/34</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/35</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/36</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/37</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/38</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/39</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/40</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/41</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/42</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/43</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/44</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/45</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/46</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/47</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/48</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Cx0/1</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Cx0/2</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>No-Negotiation</td>
</tr>
<tr>
<td>Cx0/3</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Cx0/4</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Cx0/5</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Cx0/6</td>
<td>not connected</td>
<td>Full</td>
<td>100 Gbps</td>
<td>Auto</td>
</tr>
</tbody>
</table>

### 2.3.3 Speed

Interface speed can be configured for physical interfaces when auto negotiation is disabled.

25G FX ports can be configured to operate at 25G, 10G or 1G speeds.
100G CX ports can be configured to operate at 100G or 40G, or it can be split to operate at 25G/10G. The split can be done using the speed command to set the interface speed to 25G or 10G for the Cx ports.

Follow the steps below to configure the Interface speed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td>or</td>
<td>interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g. int range fx 0/1-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,). E.g. int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>speed { 1000</td>
<td>10000</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface status</td>
<td>Displays the interface configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no speed” command restores the default interface speed.

The example below shows the commands used to configure the interface speed.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/44
SMIS(config-if)# speed 1000
SMIS(config-if)# speed 1000
SMIS(config-if)# end
SMIS# show interface status
```
<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Duplex</th>
<th>Speed</th>
<th>Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/2</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/6</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/7</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/8</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/9</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/10</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/11</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/12</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/13</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/14</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/16</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/17</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/18</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/19</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/20</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/21</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/22</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/23</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/24</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/25</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/26</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
<tr>
<td>Fx0/27</td>
<td>not connected</td>
<td>Full</td>
<td>25 Gbps</td>
<td>Auto</td>
</tr>
</tbody>
</table>
Fx0/28  not connected  Full  25 Gbps  Auto
Fx0/29  not connected  Full  25 Gbps  Auto
Fx0/30  not connected  Full  25 Gbps  Auto
Fx0/31  not connected  Full  25 Gbps  Auto
Fx0/32  not connected  Full  25 Gbps  Auto
Fx0/33  not connected  Full  25 Gbps  Auto
Fx0/34  not connected  Full  25 Gbps  Auto
Fx0/35  not connected  Full  25 Gbps  Auto
Fx0/36  not connected  Full  25 Gbps  Auto
Fx0/37  not connected  Full  25 Gbps  Auto
Fx0/38  not connected  Full  25 Gbps  Auto
Fx0/39  not connected  Full  25 Gbps  Auto
Fx0/40  not connected  Full  25 Gbps  Auto
Fx0/41  not connected  Full  25 Gbps  Auto
Fx0/42  not connected  Full  25 Gbps  Auto
Fx0/43  not connected  Full  25 Gbps  Auto
Fx0/44  not connected  Full  1 Gbps  Auto
Fx0/45  not connected  Full  25 Gbps  Auto
Fx0/46  not connected  Full  25 Gbps  Auto
Fx0/47  not connected  Full  25 Gbps  Auto
Fx0/48  not connected  Full  25 Gbps  Auto
Cx0/1  not connected  Full  100 Gbps  Auto
Cx0/2  not connected  Full  100 Gbps  Auto
Cx0/3  not connected  Full  100 Gbps  Auto
Cx0/4  not connected  Full  100 Gbps  Auto
Cx0/5  not connected  Full  100 Gbps  Auto
Cx0/6  not connected  Full  100 Gbps  Auto

2.3.4 Duplex Operation
The Supermicro F3548 switch doesn’t support half-duplex operation on its physical interfaces.
2.3.5 MTU
The default maximum transmission unit (MTU) size for frames received and transmitted is 1500 bytes. The MTU size can be increased for an interface.

Follow the steps below to configure the interface MTU.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | interface <interface-type><interface-id> or interface range <interface-type><interface-id> .... | Enters the interface configuration mode.  
interface-type – may be any of the following:  
fx-ethernet – fx  
cx-ethernet – cx  
port-channel - po  
interface-id is in slot/port format for all physical interfaces.  
To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10  
To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20  
If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces. |
| Step 3 | mtu<frame-size(1500-9216)> | Configure interface MTU in the range 1500-9216. |
| Step 4 | End | Exits the configuration mode. |
| Step 5 | show interface status | Displays the interface configuration. |
| Step 6 | write startup-config | Optional step – saves this configuration to be part of startup configuration. |

The “no mtu” command restores the interface MTU to its default of 1500 bytes.

To change the MTU for all the interfaces, the “system mtu” command can be used.

The example below shows the commands used to configure the interface MTU.

SMIS# configure terminal  
SMIS(config)# interface fx 0/22  
SMIS(config-if)# mtu 9000
SMIS(config-if)# end
SMIS

# show interface fx 0/22
Fx0/22 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port

Hardware Address is 0c:c4:7a:2c:1f:33
MTU  9000 bytes, Full duplex, 25 Gbps,  FEC is on,  Auto-Negotiation
HOL Block Prevention enabled.
Input flow-control is off, output flow-control is off
DCBX is Disabled
PFC is Disabled

Link Up/Down Trap is enabled

Reception Counters
  Octets: 0
  Unicast Packets: 0
  Unicast Packets Rate: 0/Sec
  Broadcast Packets: 0
  Broadcast Packets Rate: 0/Sec
  Multicast Packets: 0
  Multicast Packets Rate: 0/Sec
  Pause Frames: 0
  Undersize Frames: 0
  Oversize Frames: 0
  CRC Error Frames: 0
  Discarded Packets: 0
  Error Packets: 0
  Unknown Protocol: 0
Transmission Counters

Octets: 0
Unicast Packets: 0
Unicast Packets Rate: 0/Sec
Broadcast Packets: 0
Broadcast Packets Rate: 0/Sec
Multicast Packets: 0
Multicast Packets Rate: 0/Sec
Pause Frames: 0
Discarded Packets: 0
Error Packets: 0

# show interface mtu fx-ethernet 0/22

Fx0/22  MTU size is 9000

2.3.6 Flow Control
Flow control enables Ethernet ports to control traffic during congestion to avoid packet loss.

If a port experiences congestion and cannot receive any more traffic, it notifies other ports by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets to prevent any loss of data packets during the congestion period.

Follow the steps below to configure Flow Control.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10</td>
</tr>
</tbody>
</table>
To provide multiple interfaces or ranges, separate with a comma (,).
E.g.: int range fx 0/1-10, fx 0/20

If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

| Step 3 | flowcontrol { send | receive} { on | off } |
|--------|----------------------------------------|
|        | Configure flow control                 |
|        | Send – The port can send pause frames   |
|        | but cannot receive pause frames from a  |
|        | connected device.                       |
|        | Receive – The port cannot send pause    |
|        | frames but can receive pause frames     |
|        | from a connected device.                |
|        | On – Enable flow control                |
|        | Off - Disable flow control              |

Step 4
End
Exits the configuration mode.

Step 5
show flow-control [ interface <interface-type><interface-id>] Displays the Interface Flow control configuration.

Step 6
write startup-config Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to configure Flow Control.

SMIS# configure terminal
SMIS(config)# interface fx 0/22
SMIS(config-if)# flowcontrol send on
SMIS(config-if)# end
SMIS# show flow-control interface fx 0/22

Port   TxFlowControl  RxFlowControl  Tx Pause  Rx Pause
Fx0/22  on           off          0          0

2.3.7 Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN due to errors or mistakes in network configurations, etc. LAN storms degrade network performance.

Storm Control monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold. The port blocks traffic when the rising threshold is reached and remains blocked until the traffic rate drops below the falling threshold before resuming normal forwarding.

Follow the steps below to configure Storm control.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;</code>&lt;interface-id&gt; or interface range <code>&lt;interface-type&gt;</code>&lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>storm-control { broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Level – Threshold level in kbps, in range 1-10000000.</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interfaces storm-control</td>
<td>Displays the interface Storm control configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no storm-control { broadcast | multicast | dlf } level” command disables Storm Control.

The example below shows the commands used to configure Storm Control.

SMIS# configure terminal
SMIS(config)# interface fx 0/22
SMIS(config-if)#storm-control broadcast level 50000
SMIS(config-if)# end

SMIS# show interfaces fx 0/22 storm-control
Fx0/22

DLF Storm Control : Disabled
Broadcast Storm Control : Enabled

Broadcast Storm Control : 50000
Multicast Storm Control : Disabled

2.3.8 Forward Error Correction (FEC) Mode
Supermicro switches allow users to enable or disable the FEC mode on the interfaces configured for 25G and 100G. FEC is not supported for other speed settings. **It is recommended to turn ON FEC for most cables and peer devices.**

FEC is enabled by default in all Fx and Cx ports. This switch supports RS_FEC, which is equivalent to cl91 FEC in some devices.

Follow the steps below to enable FEC mode on the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Fec-mode</td>
<td>Enable FEC mode on interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface</td>
<td>Displays the fec mode for the interface.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The example below shows the commands used to configure the interface description.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/22
SMIS(config-if)# fec-mode
SMIS(config-if)# end
SMIS
SMIS# sh int Fx 0/22
```

It is recommended to turn ON the FEC for most cables and peer devices. This switch supports FEC type RS (Reed-Solomon). Make sure the same FEC type is configured in peer devices.

### 2.3.9 Port Splitting
Supermicro switches allow users to split each of the Cx-ethernet ports into 4 ports that can operate at speed 25G or 10G. After splitting, the new split interfaces are created with default configuration; i.e. previously configured FEC and auto-negotiation will not be inherited by the newly created split interfaces.

Follow the steps below to split Cx-ethernet ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>Enters the interface configuration mode. interface-type – may be any of the following: cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range cx 0/1-6 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range cx 0/1-2, cx 0/4 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>speed 25000 Or speed 10000</td>
<td>Splits the port into four 25G ports or four 10G ports.</td>
</tr>
</tbody>
</table>
Note: Fec-mode and negotiation have to be turned off for splitting into 4 x 10G ports.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>show interface status</td>
<td>Split ports can be viewed in the output.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to split Cx 0/1 interface in SBM-25G-100 into four 25G ports.

SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# speed 25000
SMIS(config-if)# end

Use show interface command to check that Fx 49, Fx 50 and Fx 51 ports were created. SMIS# show interface status

Use show running-config command to check that Cx 0/1 speed is set to 25G. SMIS# show running-config

The example below shows the commands used to split Cx 0/1 interface in SBM-25G-100 into four 10G ports.

SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config)# no fec-mode
SMIS(config)# no negotiation
SMIS(config-if)# speed 10000
SMIS(config-if)# end

Use show interface command to check that Fx 49, Fx 50 and Fx 51 ports were created. SMIS# show interface status

Use show running-config command to check that Cx 0/1 speed is set to 10G. SMIS# show running-config

2.4 Time Management
The system time and date on Supermicro switches can be managed by Network Time Protocol (NTP) or configured manually.

NTP provides synchronization of network resources by a synchronized network timestamp. Supermicro switches can function as an NTP client over UDP and receive the time from an NTP server in the network.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timezone offset</td>
<td>None</td>
</tr>
<tr>
<td>NTP status</td>
<td>Disabled</td>
</tr>
<tr>
<td>NTP operation</td>
<td>Unicast</td>
</tr>
</tbody>
</table>
2.4.1 NTP Server

Supermicro switches can synchronize their time with that of an NTP server. Follow the below steps to configure NTP server parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | ntp server <ip_address> [key (1-65535)] [prefer] | Configure the NTP server.  
  
ip_addr – IP address of server.  
  
key – Authentication Key for server connectivity in the range 1-65535.  
  
prefer – This option can be used to specify a preferred NTP server when multiple NTP servers are configured in the switch. Only 1 server can be configured ‘prefer’ at a time. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show ntp | Displays the NTP configuration. |
| Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration. |

The “enable agent” command enables the agent. NTP servers can be deleted only when NTP status is disabled.

If a key is configured on Supermicro switches acting as NTP client, ensure the same key is configured on the NTP server(s) as well.

The example below shows the commands used to configure an NTP server.

SMIS# configure terminal
SMIS(config)# ntp server 200.200.200.10 key 100 prefer
SMIS(config)# ntp server 100.100.100.1 key 500
SMIS(config)# end
SMIS# show ntp

[NTP] ntp is disabled
  Server   Key   Prefer
  =========== ====== =====

200.200.200.10   100   YES
100.100.100.1   500

Key #    Key
========  =============================
Time zone offset not set

### 2.4.2 Enable/Disable NTP
NTP is disabled by default in Supermicro switches. Follow the below steps to enable NTP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ntp enable</td>
<td>Enable NTP in switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ntp</td>
<td>Displays the NTP configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “ntp disable” command disables NTP in the switch. NTP can be enabled in Supermicro switches only after configuring at least one NTP server.

The example below shows the commands used to configure NTP.

```
SMIS# configure terminal
SMIS(config)# ntp enable
SMIS(config)# end
SMIS# show ntp

[NTP] ntp running unicast mode

<table>
<thead>
<tr>
<th>Server</th>
<th>Key</th>
<th>Prefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>===============</td>
<td>===</td>
<td>========</td>
</tr>
<tr>
<td>200.200.200.10</td>
<td>100</td>
<td>YES</td>
</tr>
<tr>
<td>100.100.100.1</td>
<td>500</td>
<td></td>
</tr>
</tbody>
</table>
```

Key #    Key
========  =============================
Time zone offset not set

### 2.4.3 NTP Authentication
Supermicro switches support NTP authentication by the NTP server. The authentication data is encrypted by an MD5 algorithm. The NTP authentication key can be configured in the switch and this must be matched with the NTP authentication key in the NTP server. The authentication key is an NTP key number and text pair.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ntp key &lt;key_number (1 - 65535)&gt; &lt;key_text&gt;</td>
<td>Configure NTP authentication key.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ntp</td>
<td>Displays the NTP configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no ntp key” command deletes the NTP authentication key.

The example below shows the commands used to configure NTP.

SMIS(config)# ntp key 200 For-server1
SMIS(config)# show ntp

[NTP] ntp is enabled

<table>
<thead>
<tr>
<th>Server</th>
<th>Key</th>
<th>Prefer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key 

Key 

Key  

200  For-server1

Time zone offset not set

2.4.4 NTP Broadcast
NTP server messages can be broadcast or unicast. By default, Supermicro switches receive unicast NTP messages.

Follow the below steps to configure Supermicro switches to receive NTP broadcast messages from the NTP server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ntp broadcast [authentication]</td>
<td>Configure NTP broadcast.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>authentication</em> – If specified, NTP authentication is enabled for broadcast mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ntp</td>
<td>Displays the NTP configuration.</td>
</tr>
</tbody>
</table>
Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration.

The “no ntp broadcast” command disables NTP Broadcast.

The example below shows the commands used to configure NTP Broadcast.

SMIS(config)# ntp broadcast authentication
SMIS(config)# show ntp
[ntp running broadcast mode
  Server Key Prefer
  ================ =====  ======
  Key # Key
  ========= ===================
  Time zone offset not set

2.4.5 System Clock
The system clock in Supermicro switches run from the time the moment the switch starts up and keeps track of system date and time. The system clock can also be manually configured. The system time configured manually remains accurate until next restart. Manual configuration of system clock is useful when the system time cannot be obtained from any other source, such as NTP associations.

Follow the steps below to set the system clock.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | clock set hh:mm:ss day<1-31>month<january|february|march|april|may|june|july|august|september|october|november|december> year<2000 - 2035> | Configure the system clock.
  
  \textit{hh:mm:ss} – Time in Hours:Minutes:Seconds format.

  \textit{day} – Day in 1-31 format.

  \textit{month} – Month in January-December format.

  \textit{year} – Year in yyyy format.

  |
| Step 2 | show clock                  | Displays the system clock.                                   |

The example below shows the commands used to configure system clock.
SMIS# clock set 09:26:15 31 august 2013

SMIS# show clock

Wed Aug 31 09:26:20 2013

2.4.6 Time Zone

The system clock maintains time based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). The local time zone can be specified as an offset from UTC.

Follow the below steps to configure the time zone.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>tz posix &lt;std&gt;&lt;offset&gt;[&lt;dst&gt;]</td>
<td>Configure the time zone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;std&gt; - Standard time text e.g. PST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;offset&gt; - Time zone offset in [+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;dst&gt; - Day light savings time text e.g. PDT</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the time zone configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure the time zone offset.

SMIS# configure terminal
SMIS(config)# tz posix PST8
SMIS(config)# end

SMIS# show system information

Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
2.5 System Management

Supermicro switches can be administered by configuring various operations.

- Switch Name
- Switch Location
- Switch Contact
- System MTU
- Port mirroring
- MAC aging
- Reload or reset

Defaults – System Management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch name</td>
<td>SMIS</td>
</tr>
<tr>
<td>System contact</td>
<td><a href="http://www.supermicro.com">http://www.supermicro.com</a></td>
</tr>
<tr>
<td>System location</td>
<td>Supermicro</td>
</tr>
<tr>
<td>MAC aging</td>
<td>300 secs</td>
</tr>
<tr>
<td>MAC table static entries</td>
<td>None</td>
</tr>
<tr>
<td>System MTU</td>
<td>1500 bytes</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring direction</td>
<td>Both</td>
</tr>
</tbody>
</table>

2.5.1 Switch Name

Supermicro switches can be assigned a name for identification purpose. The default switch name is SMIS. The switch name is also used as a prompt.

Follow the steps below to configure the Switch Name.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>device name &lt;devname(15)&gt;</td>
<td>Configure Switch Name and prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Devname—Switch name specified as 1-15 alphanumeric characters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the system information configuration.</td>
</tr>
</tbody>
</table>

The device name configuration is automatically stored as part of startup-config file.

The example below shows the commands used to configure the switch name.

SMIS# configure terminal
SMIS(config)# device name switch1
switch1(config)# end

switch1# show system information

Switch Name: switch1
Serial Number: SSC36SR08200014
Switch Management MAC Address: 0c:c4:7a:2c:1f:1d
Switch Base MAC Address: 0c:c4:7a:2c:1f:1e
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
ZTP Config Restore Option: ZTP Enabled
Config Restore Status: Successful
Config Restore Option: Restore
Config Restore ZTP Filename:
Config Restore ZTP TFTP IP Address: 0.0.0.0
Config Restore Local Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 3 hrs 43 mins 6 secs

Boot-up Flash Area: Normal

NTP Broadcast Mode: No

[ntp] ntp is disabled

Server  Key  Prefer
=============== =====  ======

Key #  Key

Time zone offset not set

### 2.5.2 Switch Contact

Supermicro switches provide an option to configure the switch in charge of contact details, usually an email ID.

Follow the steps below to configure the switch contact.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>system contact &lt;string - to use more than one word, provide the string within double quotes&gt;</td>
<td>Configure Switch Contact.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>String – Contact information entered as a String of maximum length 64.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the System information configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The System Contact configuration is automatically stored as part of the startup-config file.

The example below shows the commands used to configure the switch contact.

```
SMIS# configure terminal
SMIS(config)# system contact "User1 at CA"
SMIS(config)# end
SMIS# show system information

Switch Name: SMIS
Serial Number: SSC36SR08200014
Switch Management MAC Address: 0c:c4:7a:2c:1f:1d
Switch Base MAC Address: 0c:c4:7a:2c:1f:1e
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: User1 at CA
```
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
ZTP Config Restore Option: ZTP Enabled
Config Restore Status: Successful
Config Restore Option: Restore
Config Restore ZTP Filename:
Config Restore ZTP TFTP IP Address: 0.0.0.0
Config Restore Local Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 3 hrs 48 mins 33 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled

Server    Key    Prefer
=========== =====  ======

Key #    Key
========== =============
Time zone offset not set

2.5.3 System Location
Supermicro switches provide option to configure the switch location details.

Follow the steps below to configure the system location.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>system location &lt;location name&gt;</td>
<td>Configure System Location.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>location name –Location of the switch specified as a string of maximum size 238.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the System Location configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The System Location configuration is automatically stored as part of the startup-config file.

The example below shows the commands used to configure the system location.

SMIS# configure terminal
SMIS(config)# system location "Santa Clara"
SMIS(config)# end

SMIS# show system information

Switch Name: SMIS
Serial Number: SSC36SR08200014
Switch Management MAC Address: 0c:c4:7a:2c:1f:1d
Switch Base MAC Address: 0c:c4:7a:2c:1f:1e
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Santa Clara
Logging Option: Console Logging
Login Authentication Mode: Local
ZTP Config Restore Option: ZTP Enabled
Config Restore Status: Successful
Config Restore Option: Restore
Config Restore ZTP Filename:
Config Restore ZTP TFTP IP Address: 0.0.0.0
Config Restore Local Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 3 hrs 55 mins 33 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
  Server   Key   Prefer
  =========== =====  ======
  Key #    Key
  =======   ==============
  Time zone offset not set

2.5.4 System MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces of
the switch is 1500 bytes. The MTU size can be increased for all interfaces of the switch at the same time by
using the ‘system MTU’ command.

Follow the steps below to configure the system MTU.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | system mtu <frame-size(1500-9216)> | Configure System MTU.
frame-size – Specify MTU of frame in range 1500-9216. |
| Step 3 | End                         | Exits the configuration mode                                               |
| Step 4 | show interface mtu          | Displays the interface MTU                                                 |
| Step 5 | write startup-config        | Optional step – saves this configuration to be part of startup configuration. |
The “no system mtu” command resets the system MTU to its default value of 1500 bytes.

The example below shows the commands used to configure the system MTU.

SMIS# configure terminal
SMIS(config)# system mtu 9200
SMIS(config)# end

SMIS
# show interface mtu
Fx0/1  MTU size is 9200
Fx0/2  MTU size is 9200
Fx0/3  MTU size is 9200
Fx0/4  MTU size is 9200
Fx0/5  MTU size is 9200
Fx0/6  MTU size is 9200
Fx0/7  MTU size is 9200
Fx0/8  MTU size is 9200
Fx0/9  MTU size is 9200
Fx0/10 MTU size is 9200
Fx0/11 MTU size is 9200
Fx0/12 MTU size is 9200
Fx0/13 MTU size is 9200
Fx0/14 MTU size is 9200
Fx0/15 MTU size is 9200
Fx0/16 MTU size is 9200
Fx0/17 MTU size is 9200
Fx0/18 MTU size is 9200
Fx0/19 MTU size is 9200
Fx0/20  MTU size is 9200
Fx0/21  MTU size is 9200
Fx0/22  MTU size is 9200
Fx0/23  MTU size is 9200
Fx0/24  MTU size is 9200
Fx0/25  MTU size is 9200
Fx0/26  MTU size is 9200
Fx0/27  MTU size is 9200
Fx0/28  MTU size is 9200
Fx0/29  MTU size is 9200
Fx0/30  MTU size is 9200
Fx0/31  MTU size is 9200
Fx0/32  MTU size is 9200
Fx0/33  MTU size is 9200
Fx0/34  MTU size is 9200
Fx0/35  MTU size is 9200
Fx0/36  MTU size is 9200
Fx0/37  MTU size is 9200
Fx0/38  MTU size is 9200
Fx0/39  MTU size is 9200
Fx0/40  MTU size is 9200
Fx0/41  MTU size is 9200
Fx0/42  MTU size is 9200
Fx0/43  MTU size is 9200
Fx0/44  MTU size is 9200
Fx0/45  MTU size is 9200
Fx0/46  MTU size is 9200
Fx0/47  MTU size is 9200
Fx0/48  MTU size is 9200
Cx0/1   MTU size is 9200
Cx0/2   MTU size is 9200
Cx0/3   MTU size is 9200
Cx0/4   MTU size is 9200
Cx0/5   MTU size is 9200
Cx0/6   MTU size is 9200
SMIS#

2.5.5 Static MAC
The MAC address table stores MAC addresses used by the switch to forward traffic between ports. Supermicro switches allow for static configuration of entries in MAC addresses.

Static MAC Characteristics:
- Static MAC addresses do not age and are automatically stored as part of startup-config so they are available after restart.
- Static MAC addresses can be unicast or multicast.

Forwarding Behavior for Static MAC:
- Supermicro switches provide flexibility to configure forwarding behavior for static MAC addresses, i.e. how a port that receives a packet forwards it to another port for transmission.
- A packet with a static address that arrives on a VLAN on which a static MAC address has been configured, is flooded to all ports and not learned.
- A static address is created by specifying the destination MAC unicast address and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the interface-id option.

Follow the steps below to configure static MAC.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mac-address-table static multicast <a href="">aa:aa:aa:aa:aa:aa</a> vlan &lt;vlan-id(1-4069)&gt; interface [{&lt;interface-type&gt;&lt;0/a-b,0/c,...&gt;} [interface-type]&lt;0/a-b,0/c,...&gt; ] [port-channel &lt;a,b,c,d&gt;]]</td>
<td>Configure Multicast or unicast static MAC.</td>
</tr>
<tr>
<td></td>
<td>_vlan -- Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.</td>
<td></td>
</tr>
</tbody>
</table>
### mac-address-table static unicast

```
<aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface <interface-type><iface>
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>End</th>
<th>Exit the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>show mac-address-table static multicast [vlan &lt;vlan-range&gt;] [address <a href="">aa:aa:aa:aa:aa:aa</a>] [[interface &lt;interface-type&gt;&lt;interface-id&gt;]]</td>
<td>Displays the static MAC configuration.</td>
</tr>
<tr>
<td></td>
<td>show mac-address-table static unicast [vlan &lt;vlan-range&gt;] [address <a href="">aa:aa:aa:aa:aa:aa</a>] [[interface &lt;interface-type&gt;&lt;interface-id&gt;]]</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

---

The “no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type><interface-id>]” command deletes the particular static MAC entry.

The “no mac-address-table static multicast <aa:aa:aa:aa:aa:aa> [recv-port <interface-type><interface-id>]” command deletes the particular static multicast MAC entry.

---

The example below shows the commands used to configure a static MAC.

SMIS# configure terminal
SMIS(config)# mac-address-table static unicast 90:4e:e5:0c:03:75 vlan 1 interface fx 0/14 status permanent
SMIS(config)# end

SMIS# show mac-address-table static unicast

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>90:4e:e5:0c:03:75</td>
<td>Permanent</td>
<td>Fx0/14</td>
</tr>
</tbody>
</table>

Total Mac Addresses displayed: 1
2.5.6 MAC Aging

Dynamic MAC address table entries are addresses learned by the switch that age when not in use. The MAC aging time can be configured by users.

Follow the steps below to configure MAC aging.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mac-address-table aging-time &lt;10-1000000 seconds&gt;</td>
<td>Configure MAC Aging time in range 10-1000000 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mac-address-table aging-time</td>
<td>Displays the MAC address table aging time.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no mac-address-table aging-time” command resets MAC aging to its default value of 300 seconds.

The example below shows the commands used to configure MAC Aging.

SMIS# configure terminal
SMIS(config)# mac-address-table aging-time 50000
SMIS(config)# end
SMIS# show mac-address-table aging-time
Mac Address Aging Time: 50000
SMIS# show mac-address-table
Vlan  Mac Address  Type  Ports
    --------  ------  ----  ---
1    90:4c:e5:0b:04:77  Learnt  Fx0/21
1    94:d7:23:94:88:d8  Learnt  Fx0/21
Total Mac Addresses displayed: 2

2.6 System Logging (Syslog)

Supermicro switches send system message output to a klogging process called System Message Logging (Syslog). Logging can be done at various locations:

- Console
- File
- Server

<p>| Parameter | Default Value |</p>
<table>
<thead>
<tr>
<th>Syslog status</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging buffer size</td>
<td>50 entries</td>
</tr>
<tr>
<td>Console logging</td>
<td>Enabled</td>
</tr>
<tr>
<td>File Logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Trap Logging</td>
<td>Critical</td>
</tr>
<tr>
<td>MAC Address table update Logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>Facility</td>
<td>Local0</td>
</tr>
</tbody>
</table>

**2.6.1 Enable/Disable Syslog**

Syslog is enabled by default in Supermicro switches.

Follow the steps below to disable Syslog.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging disable</td>
<td>Disable Syslog.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “logging enable” command enables the Syslog feature.

The example below shows the commands used to disable Syslog.

SMIS# configure terminal
SMIS(config)# logging disable
SMIS(config)# end
SMIS# show logging

System Log Information

-----------------------------
Syslog logging: disabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name: 
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 50 Entries
LogBuffer: (0 Entries)
2.6.2 Syslog Server
In Supermicro switches, Syslog messages can be re-directed to a Syslog server.

Follow the steps below to configure the Syslog server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging &lt;ip-address&gt;</td>
<td>Configure Syslog Server. ip-address – IP address of Syslog server</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration</td>
</tr>
</tbody>
</table>

The “no logging <ip-address>” command deletes the Syslog server.

The example below shows the commands used to configure a Syslog server.

SMIS# configure terminal
SMIS(config)# logging 192.168.1.3
SMIS(config)# end
SMIS# show logging

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: 192.168.1.3
Facility: Default (local0)
Buffered size: 50 Entries

LogBuffer: (0 Entries)
LogFile: (0 Entries)

2.6.3 Console Log
System logging messages can be displayed in switch console.
Follow the steps below to enable the Syslog console.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging console</td>
<td>Enable Syslog Console.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no logging console” command disables console logging.

The example below shows the commands used to enable Syslog console.

```
SMIS# configure terminal
SMIS(config)# logging console
SMIS(config)# end
SMIS# show logging
```

System Log Information

-------------
Syslog logging: enabled(Number of messages 0)
Console logging: enabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 50 Entries
LogBuffer: (0 Entries)
LogFile: (0 Entries)

**2.6.4 Log File**

System logging messages can be stored as a log file in the switch NVRAM.

Follow the steps below to enable storing logs in a file.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging file &lt;filename&gt; max-entries &lt;short (1-8000)&gt;</td>
<td>Enable storing Logs in a File.</td>
</tr>
</tbody>
</table>

_Filename_ – Specify file name of upto 32 characters.

_Short_– Specify entries that can stored in file in range 1-8000.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no logging file” command disables the logging of system message in a file.

The example below shows the commands used to enable storing logs in a file.

```
SMIS# configure terminal
SMIS(config)#logging file log1
SMIS(config)# end
SMIS# show logging file

LogFile(2 Entries)
<129> Apr 29 10:11:30 2013:INTF-1:Interface Fx0/22 status changed to UP
<129> Apr 29 10:11:31 2013:INTF-1:Interface Fx0/22 status changed to UP

SMIS#
SMIS# show logging

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: enabled(Number of messages 2)
Log File Name: log1
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 50 Entries

LogBuffer: (11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7: Exitting DHCPC Task Init
<135> Apr 29 10:11:05 2013:DHC-7: Entered in DhcppIntSelectTaskMain fn
<135> Apr 29 10:11:05 2013:DHC-7: Entered in DhcppSocketOpen fn
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13c32878 type : 1
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13c32890 type : 1
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13c34448 type : 1
<135> Apr 29 10:11:07 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7: Rcvd Msg 13c34908 type : 1
<129> Apr 29 10:11:31 2013:INTF-1: Interface Fx0/22 status changed to UP
```
2.6.5 Logging Buffer
The log messages are stored in a circular internal buffer in which older messages are overwritten once the buffer is full. The Syslog buffer size is configurable in Supermicro switches.

Follow the steps below to configure the Syslog buffer.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging buffered &lt;size (1-200)&gt;</td>
<td>Configure Syslog Buffer with maximum size of 200 entries.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no logging buffered” command resets the logging buffer to its default value of 50 entries.

The example below shows the commands used to configure Syslog Buffer.

```
SMIS# configure terminal
SMIS(config)#logging buffered 200
SMIS(config)# end
SMIS# show logging
```

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 200 Entries

LogBuffer(11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7:Exiting DHCPC Task Init
<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCIntSelectTaskMain fn
2.6.6 Facility
The Syslog facility provides approximate details regarding which part of the system the Syslog message originated from.

Follow the steps below to configure the Syslog facility.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging facility {local0</td>
<td>local1</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “nologging facility” command resets the logging facility to its default value of Local0.

The example below shows the commands used to configure the Syslog facility.

SMIS# configure terminal
SMIS(config)# logging facility local5
SMIS(config)# end
SMIS# show logging

System Log Information

Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: local5
Buffered size: 50 Entries
LogBuffer: (0 Entries)
LogFile: (0 Entries)

**2.6.7 Traps**
Supermicro switches provide an option for specifying the type of traps that are to be logged.

Follow the steps below to configure logging traps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | logging trap [{ <level (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings }] | Configure Logging Traps. There are various levels of traps that can be logged.  
*Level 0 – Emergencies*  
Used for logging messages that are equivalent to a panic condition.  
*Level 1 – Alerts*  
Used for logging messages that require immediate attention.  
*Level 2 – Critical*  
Used for logging critical errors.  
*Level 3 – Errors*  
Used for error messages.  
*Level 4 – Warning*  
Used for logging warning messages.  
*Level 5 – Notification*  
Used for logging messages that require attention but are not errors.  
*Level 6 – Informational*  
Used for logging informational messages.  
*Level 7 – Debugging*  
Used for logging debug messages. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show logging | Displays the Syslog configuration. |
| Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration. |
The “no logging trap” command resets trap logging to its default value of ‘Critical’.

The example below shows the commands used to configure logging traps.

SMIS# configure terminal
SMIS(config)# logging trap 5
SMIS# end
SMIS(config)# show logging

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Notification

Log server IP: None
Facility: Default (local0)
Buffered size: 200 Entries
LogBuffer: (11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7:Exiting DHCP Task Ini
<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpClntSelectTaskMain fn
<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCSocketOpen fn
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cb8128 type : 1
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cb8128 type : 1
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cf4258 type : 1
<135> Apr 29 10:11:08 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:08 2013:DHC-7:Rcvd Msg 13cf4858 type : 1

LogFile(0 Entries)

2.6.8 Clear Log Buffer

The Syslog buffer can be cleared to enable the fresh logging of messages.

Follow the steps below to clear the log buffer.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>clear log buffer</td>
<td>Clear Logging Buffer.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
</tbody>
</table>
Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to clear the log buffer.

SMIS# configure terminal
SMIS(config)# clear log buffer
SMIS(config)# end
SMIS# show logging

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 50 Entries
LogBuffer: (0 Entries)
LogFile: (0 Entries)

2.6.9 Clear Log File
The Syslog file can be cleared to enable the fresh logging of messages.

Follow the steps below to clear the log file.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>clear log file</td>
<td>Clear Logging File.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show logging</td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to clear the log file.

SMIS# configure terminal
SMIS(config)# clear log file
SMIS(config)# end
SMIS# show logging

System Log Information

----------------------
Syslog logging: enabled(Number of messages 0)
2.7 Configuration Management

This section describes the steps to save and manage the configuration files on the switch. It also describes the firmware upgrade and “restore to factory defaults” functions.

2.7.1 Save Startup-Config

Switch configurations can be saved using the command write startup-config. A configuration saved as a startup configuration will be loaded automatically when switch reboots. The default startup configuration file name is iss.conf. This startup configuration file is stored in the flash memory.

Follow the steps below to write existing switch configuration as startup-config.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>write startup-config</td>
<td>Configure Writing of Switch Configuration to a file or startup-config.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show startup-config</td>
<td>Displays the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the command used to write existing switch configuration as startup-config.

SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...
[OK]

To change the default startup config file name, use the “set startup-config” command.

2.7.2 Save Running Configuration to File

Switch configurations can be saved to a file either in local flash memory or to a remote TFTP server.

Follow the steps below to write an existing switch configuration to a file.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 1  write { flash:filename | tftp://ip-address/filename} | Configure Writing of Switch Configuration to a file in the local flash memory or in a remote TFTP server. filename – name of the configuration file.

Step 2  show stored-config<filename> | Displays the stored configuration file from local flash memory. filename – name of the configuration file.

The example below shows the commands used to write an existing switch configuration to a file.

SMIS# write flash: r1sw1.conf
Building configuration, please wait. May take a few minutes ... [OK]

SMIS# writetftp://192.168.1.100/r1sw1.conf
Building configuration, please wait. May take a few minutes ... [OK]

SMIS# show stored-config r1sw1.conf

vlan 1
ports fx 0/1-48 untagged
ports cx 0/1-4 untagged
exit
snmp view restricted 1 excluded nonvolatile
setip igmp enable
setip pim enable
ip pim component 1
exit

2.7.3 Configuring Startup Config File Name
Supermicro switches provide an option to select a file stored in flash memory as the startup configuration file that gets loaded when the switch is powered on or restarted.

Follow the steps below to configure the startup configuration.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set startup-config&lt;filename&gt;</td>
<td>Configure Startup-config file name. filename – name of the configuration file.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
Step 4 | show startup-config | Displays the configured startup configuration file contents.

The example below shows the commands used to configure the switch startup configuration.

SMIS# configure terminal
SMIS(config)# set startup-config config2.conf
SMIS(config)# end
SMIS# show startup-config

vlan 1
ports fx 0/1-48 untagged
ports cx 0/1-4 untagged
exit
snmp view restricted 1 excluded nonvolatile
setip igmp enable
setip pim enable
ip pim component 1
exit

2.7.4 Copy Startup-config
Supermicro switches support copying the switch startup configuration to a file in flash or remote location.

Follow the steps below to copy startup-config to a file in a remote location or flash.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>copy startup-config flash:filename</td>
<td>Copy from startup-config to a file in remote location or flash.</td>
</tr>
<tr>
<td></td>
<td>tftp://ip-address/filename</td>
<td>filename – name of the configuration file.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to copy startup-config to a file in flash.

SMIS# copy startup-config flash:config5.txt
Copied startup-config => flash:/mnt/config5.txt
SMIS#

2.7.5 Copy File
The copy command copies the configuration file from flash memory to a remote TFTP server and vice versa. This command can be used to copy files locally within the flash memory also.
Follow the steps below to copy the configuration file to a remote site/flash.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>copy flash: filename</td>
<td>Copies a local flash file to remote TFTP server.</td>
</tr>
<tr>
<td></td>
<td>copy tftp://ip-address/filename flash: filename</td>
<td>Copies a remote file to local flash.</td>
</tr>
<tr>
<td></td>
<td>copy flash: filename flash: filename</td>
<td>Makes a copy of the file in the flash memory.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to copy a file to another file in remote site/flash.

SMIS# copy flash:config1.txt flash:switch1.conf

Copied flash:/mnt/config1.txt ==> flash:/mnt/switch1.conf

SMIS#

2.7.6 Deleting a Saved Configuration
Supermicro switches allow for the deletion of the switch startup configuration and other stored configuration files.

Follow the steps below to delete the startup-config file or other configuration files.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>erase startup-config</td>
<td>Removes the startup-config.</td>
</tr>
<tr>
<td></td>
<td>erase flash:filename</td>
<td>Deletes the configuration file from local flash.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to erase the startup-config file or another file.

SMIS# erase flash:config1.txt
Do you really want to delete file config1.txt? [y/n]
% Deleted file config1.txt.
SMIS#

SMIS# erase startup-config
Do you really want to delete startup configuration? [y/n]
% Deleted startup configuration file.
SMIS#
1.1.1 Firmware Upgrade
The switch supports upgrading from both the switch CLI and the ONIE shell. To upgrade from the switch CLI, use the file with the ‘swi’ extension. To upgrade from the ONIE console, use the file with the ‘installer’ extension.

This command upgrades only the switch firmware. ONIE will not be upgraded.

1.1.1.1 Firmware Upgrade from Switch CLI
Follow the steps below to update the firmware image from the switch CLI:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>firmware upgrade { tftp://ip-address/filename}</td>
<td>Updates the firmware image from the remote TFTP server.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure the firmware upgrade.

SMIS# firmware upgrade tftp://100.100.100.1/SSE-F3548-fw-1.0.1.4.swi

Use the file with the ‘swi’ extension to upgrade from the switch CLI.

1.1.1.2 Firmware Upgrade from ONIE Shell
Follow the steps below to update the firmware image from the ONIE shell:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Boot the switch</td>
<td>Boot the switch by powering on. If the switch is already on, use the ‘reload’ command to reboot the switch.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the grub menu, choose the ‘ONIE’ option and press enter.</td>
<td>The grub menu remains for only 4 seconds, after 4 seconds the switch will automatically boot from the ‘Supermicro SSE-F3548 Switch’ option, so, use the down arrow quick enough to move the cursor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the ONIE menu, choose the ‘ONIE: Install OS’ option and press enter.</td>
<td>After 4 seconds the switch will automatically boot to the ONIE shell from the ‘ONIE: Install OS’ option.</td>
</tr>
<tr>
<td>Step 4</td>
<td>onie-discovery-stop</td>
<td>This step stops ONIE from discovering installer files from the network. Stopping the discovery helps stop the discovery messages on the console and prevents the switch from installing</td>
</tr>
</tbody>
</table>
Step 5  scp <username>@<hostname>:<path>/SSE-F3548-fw-x.x.x.x.installer ./  
from the random ONIE source connected to the network.

Step 6  Type ‘y’ and press enter to confirm when the switch prompts  
“Do you want to continue connecting? (y/n)”.  
Username is the login user on the remote Linux server.  
Use the firmware file with the extension ‘installer’.

Step 7  onie-nos-install ./SSE-F3548-fw-x.x.x.x.installer  
The switch will install the firmware and reboot with new firmware.

The example below shows the commands used to upgrade the firmware from the ONIE shell.

ONIE:/ # onie-discovery-stop

ONIE:/ # scp admin@10.10.10.10:/home/tftp/SSE-F3548-fw-1.0.1.4.installer ./

ONIE:/ # onie-nos-install ./SSE-F3548-fw-1.0.1.4.installer

Use the file with the ‘installer’ extension to upgrade from ONIE shell.

After booting to the ONIE shell, stop the ONIE discovery as quickly as possible to prevent the switch from initiating an installation from rouge ONIE boot sources. Installation from the wrong source could damage the switch. Entering ‘ONIE: Install OS’ will erase the grub menu, so a new image will need to be installed before rebooting the device.

2.7.7 Boot-up Options
Supermicro switches support dual firmware images ("normal" and "fallback"). The switch boots up from the normal firmware image by default. Users can configure the switch to boot from the fallback firmware image.

Follow the steps below to configure the switch boot-up firmware option.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set boot-up {normal</td>
<td>fallback}</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the system information configuration.</td>
</tr>
</tbody>
</table>
The `boot-up configuration is automatically stored as part of the startup-config file.

The example below shows the commands used to configure the switch boot-up options.

SMIS# configure terminal
SMIS(config)# set boot-up fallback
SMIS(config)# end
SMIS# show system information

Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
ConfigSave IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 0 mins 53 secs
Boot-up Flash Area: Fallback

NTP Broadcast Mode: No
[NTP] ntp is disabled

<table>
<thead>
<tr>
<th>Server</th>
<th>Key</th>
<th>Prefer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key #   Key
========

Time zone offset not set

2.7.8 Reset to Factory Defaults

Supermicro switches can be reset to the factory defaults using a CLI command.

Follow the steps below to reset to the factory defaults.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>reset-to-factory-defaults</td>
<td>Configure Factory Defaults.</td>
</tr>
</tbody>
</table>

Resetting to factory defaults will remove all stored configurations, files on the flash memory, user accounts and the management IP address.
After resetting to factory defaults, the switch can be managed from serial console with the default administrator user ID ADMIN and password can be found on the label stuck on the switch.

The example below shows the command to reset to the factory defaults.

```
SMIS(config)# reset-to-factory-defaults
This command will reset settings to the factory defaults.
After resetting to factory defaults, the switch will be reloaded immediately.
Do you really want to execute this command and reload the switch? [y/n]
```
2.8 Zero Touch Provisioning

Zero Touch Provisioning (ZTP) helps to auto provision Supermicro switches without manual intervention. ZTP also helps to upgrade the switch firmware automatically.

SSE-F3548S/R switches come with the default management IP address set to DHCP mode. When switches boot up, the management IP address is received from the DHCP server. The DHCP server can also be configured to supply the switch configurations and firmware image when assigning IP addresses to Supermicro switches.

ZTP is enabled by default in Supermicro switches.

---

When users prefer to save a configuration locally on the switch using the “write startup-config” command or other similar functionalities, the switch will provide a warning message and disable the ZTP on user confirmation. This helps to restore the locally saved configuration without waiting for DHCP IP availability.

---

2.8.1 ZTP Config Restore

This section explains details on using ZTP to automatically configure Supermicro switches.

2.8.1.1 DHCP Server Configuration

Switches expect the following information from the DHCP server to restore configurations supplied along with DHCP IP.

1. Configuration File Name
2. TFTP Server IP Address

Configuration File Name

The configuration file name is sent to switches from the DHCP server using vendor specific option 43 in sub option 01.

This is a simple text field that carries the configuration file name with the path in respect to the TFTP server root directory. If this file is kept in the TFTP root directory in the TFTP server, this field is a simple file name.

TFTP Server IP Address

The configuration file needs to be available in a TFTP server for a switch to download.

The TFTP server’s IP address is sent to switches from the DHCP server using standard DHCP option 66, \texttt{tftp-server-name}. This field needs to be configured in IP address format (e.g. xxx.xxx.xxx.xxx). Switches cannot accept server names, as domain name resolution is not supported.
These options can be added to dhcpd.conf as shown in the example below.

```plaintext
# Need to add the lines below to define option 43.1 for Supermicro switches.

dooble space smc-op;
dooble smc-op.config-file-name code 1 = text;
dooble smc-op-encapsulation code 43 = encapsulate smc-op;

# network for Supermicro switches

subnet 172.31.0.0 netmask 255.255.0.0 {
  range 172.31.30.10 172.31.30.79;
  # the below lines added for automatic restore of configuration
  dooble smc-op.config-file-name "smcSwitch.conf";
  option tftp-server-name "172.31.43.59";
}
```

The lines in bold are newly required, other lines are shown for clarity.
2.8.1.2 Switch Configuration Restore

A ZTP configuration restore feature is enabled in Supermicro switches by default. The default management IP address configuration is DHCP mode. Hence, when switches boot up with DHCP, it gets the configuration file and applies the configuration.

The diagram below shows how a switch restores the configuration in ZTP and non-ZTP case.

![Switch Configuration Restore Diagram]
2.8.2 ZTP Info

The “show system information” command in CLI displays the ZTP related information, including the following:

ZTP Config Restore Option – Default ZTP Enabled

Config Restore ZTP Filename – The name of the configuration file restored using ZTP. If ZTP restore is not applied, this field will be empty.

Config Restore ZTP TFTP IP Address – The IP address of the TFTP server from where the ZTP config file is downloaded. If ZTP restore is not applied, this field will be empty.

The “Config Restore Option” will also show “ZTP Restore” if a ZTP restore is attempted.

This information can be seen in the web interface on the “system settings” page in the “system management” group.

2.8.3 ZTP Firmware Upgrade

This section explains details on using ZTP to automatically upgrade firmware on Supermicro switches.

2.8.3.1 DHCP Server Configuration

Switches expect the following information from the DHCP server to upgrade the firmware supplied along with DHCP IP.

1. Firmware Image File Name
2. TFTP Server IP Address

Firmware Image File Name

The firmware image name is sent to switches from the DHCP server using vendor specific option 43 in sub option 04.

This simple text field carries the firmware image file name with the path in respect to the TFTP server root directory. If this file is kept in the TFTP root directory in a TFTP server, this field is a simple file name.

TFTP Server IP Address

The configuration file needs to be available on a TFTP server for the switch to download.

TFTP server IP address is sent to switches from the DHCP server using standard DHCP option 66, \texttt{tftp-server-name}. This field needs to be configured in IP address format (e.g. xxx.xxx.xxx.xxx). Switches cannot accept server names, as domain name resolution is not supported.
These options can be added to dhcpd.conf as shown in the below example.

```bash
# Need to add the below lines to define option 43.1 for Supermicro switches.

option space smc-op;
option smc-op.config-file-name code 1 = text;
option smc-op.fw-img-file-name code 4 = text;
option smc-op-encapsulation code 43 = encapsulate smc-op;

subnet 172.31.0.0 netmask 255.255.0.0 {
    range 172.31.30.10 172.31.30.79;
    option smc-op.config-file-name "smcSwitch.conf";
    option tftp-server-name "172.31.43.59";
    option smc-op.fw-img-file-name "SSE-F3548-fw-1.0.1.4.swi";
}
```

### 2.8.3.2 Switch Firmware Upgrade

The ZTP firmware upgrade feature is enabled in Supermicro switches by default. The default management IP address configuration is DHCP mode. Hence, when switches boot up with DHCP, it gets the firmware image file and checks whether an upgrade is needed or not.
The diagram below shows how a switch upgrades the firmware in ZTP.

Switch Boots up

Static IP

Is Static or DHCP IP?

No

No firmware upgrade

Yes

DHCIP IP

Got DHCP?

No

Got ZTP options?

No

Download Firmware

Failed

Yes

Success

Is ZTP firmware different than current running?

No

Upgrade Firmware & Reload Switch

Yes
2.8.4 Disable ZTP
If a customer prefers not to use ZTP and wants to disable ZTP for any reason, it can be done. When ZTP is disabled, a switch always loads the local configuration file. If no local configuration file is available, a switch comes up with a default configuration. Similarly when ZTP is disabled, a switch does not upgrade firmware automatically.

To disable ZTP in CLI, please use the “ztp disable” command in config mode.

To enable ZTP back in CLI, please use the “ztp enable” command in config mode.

This option can be enabled or disabled in the web interface on “system settings” page in the “system management” group.

2.8.5 DHCP Vendor Class
Supermicro switches advertise its vendor class information on DHCP (discover and request) packets. The DHCP vendor class option 60 is used for this purpose.

The SSE-F3548S/R switch advertises the vendor class as “SSE-F3548S”.

This vendor class information can be used in DHCP servers to send ZTP options only to the relevant switch models.

The example below shows a DHCP server configuration that uses vendor class information to send ZTP options for Supermicro switch SSE-F3548S/R.

```
class "vendor-class" {
    match option vendor-class-identifier;
}

option space smc-op;
option smc-op.config-file-name code 1 = text;
option smc-op.fw-img-file-name code 4 = text;
option smc-op-encapsulation code 43 = encapsulate smc-op;
subnet 172.31.0.0 netmask 255.255.0.0 {
    range 172.31.30.10 172.31.30.79;
    subclass "vendor-class" "SSE-F3548S" {
        option smc-op.config-file-name "iss-11.conf";
        option smc-op.fw-img-file-name "SSE-F3548-fw-1.0.1.4.swi";
        option tftp-server-name "172.31.33.5";
    }
}
```
2.9 Tracking Uplink Failures

The Uplink Failure Tracking Feature (ULFT) is useful for Supermicro switches. This helps servers move to downstream Ethernet ports in case any switch uplink fails.

The user can configure one or more groups for ULFT. Each group can have one or more uplinks and one or more downstream ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>link-status-tracking enable</td>
<td>Enabling uplink failure tracking feature</td>
</tr>
<tr>
<td>Step 3</td>
<td>link-status-tracking group &lt;id&gt;</td>
<td>Creating group</td>
</tr>
<tr>
<td>Step 4</td>
<td>link-status-tracking group &lt;id&gt; upstream</td>
<td>Adding uplink to group</td>
</tr>
<tr>
<td>Step 5</td>
<td>link-status-tracking group &lt;id&gt; downstream</td>
<td>Adding downstream ports to group</td>
</tr>
<tr>
<td>Step 6</td>
<td>link-status-tracking disable</td>
<td>Disabling uplink failure tracking feature</td>
</tr>
<tr>
<td>Step 7</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show link-status-tracking</td>
<td>Displays the link-status-tracking configuration.</td>
</tr>
<tr>
<td>Step 9</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

For example, if it is desired to bring down all fourteen ports from fx 0/1 to fx 0/14 when uplink interfaces Cx 0/1 and Cx 0/2 go down:

```
SMIS# configure terminal
SMIS(config)# link-status-tracking enable
SMIS(config)# link-status-tracking group 1
SMIS(config)# interface range Cx 0/1-2
SMIS(config-if)# link-status-tracking group 1 upstream
SMIS(config-if)# exit
SMIS(config)# interface range fx0/1-14
SMIS(config-if)# link-status-tracking group 1 downstream
SMIS(config-if)# exit
SMIS(config)# link-status-tracking disable
SMIS(config)# show link-status-tracking
```

If more than one uplink ports are configured, all downstream ports will be brought down only when all upstream ports are down.
2.10 Loop Protection

Loop protection feature helps to detect and prevent network loops. This loop protection feature is independent of the spanning tree protocol.

This feature can be used when the switches are connected to unmanaged devices where spanning tree cannot prevent network loops.

This feature detects networks loops by transmitting Ethernet control packets.

When the loop detected the switch discards all the packets from the loop detected port. When the loop disappears switch automatically move the port to forwarding without user administration.

2.10.1 Defaults

Loop Protection feature is disabled by default.

2.10.2 Enable Loop Protection

Loop Protection feature need to be enabled both globally and also on the interface level.

It can be enabled on all the interfaces or on selected interfaces.

Use the below commands to enable loop protection feature.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>loop-protect enable</td>
<td>Enabling the loop protection feature globally</td>
</tr>
<tr>
<td>Step 3</td>
<td>Interface &lt;ifname&gt; &lt;ifid&gt;</td>
<td>Enter the interface configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>loop-protect</td>
<td>Enabling the loop protection feature on this interface</td>
</tr>
<tr>
<td>Step 5</td>
<td>End</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 6</td>
<td>show loop protection</td>
<td>Displays the loop protection configuration.</td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

2.10.3 Disable Loop Protection

Loop Protection feature need to be disabled both globally and also on the interface level.

To disable loop protection on particular interface, use the below commands.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;ifname&gt; &lt;ifid&gt;</td>
<td>Enter the interface configuration mode</td>
</tr>
</tbody>
</table>
To disable loop protection on particular interface, use the below commands.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td>no loop-protect</td>
<td>Disabling the loop protection feature on this interface</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show loop protection</td>
<td>Displays the loop protection configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step — saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
3 VLAN

3.1 VLAN Basics

A Virtual LAN (VLAN) is a logical switched LAN formed by segmenting physical Local Area Networks (LANs).

Segmenting a switched LAN as one or more VLANs provides the following advantages:

- Limits multicast and broadcast floods only to the required segments of the LAN to save LAN bandwidth
- Provides secured LAN access by limiting traffic to specific LAN segments
- Eases management by logically grouping ports across multiple switches

Figure VLAN-1: VLANs on a Switched LAN

VLANs work in the same way as physical LANs. The packets from the end stations of a VLAN are switched only to other end stations or network devices inside that VLAN. To reach devices in another VLAN, the packets have to be routed from one VLAN to another. Supermicro L2/L3 switches support such Inter VLAN routing to route packets across different VLANs. Inter VLAN routing is done by creating “Layer 3 Interface VLANs”.

3.2 VLAN Support

Supermicro switches support the three types of VLANs: MAC based VLANs, protocol based VLANs and port based VLANs.
Once a packet is received, a switch tries to identify the VLAN for the received packet. This VLAN identification is done according to the procedure below.

If the incoming packet has a VLAN tag and the VLAN ID in the tag is not equal to zero, then this VLAN ID is used as the VLAN for this packet.

If the incoming packet does not have a VLAN tag (untagged packet) or if the VLAN ID in the VLAN tag is equal to zero (priority tagged packet), the packet is considered as untagged/priority tagged and the below steps are used to identify the VLAN for this untagged/priority tagged packet.

Step 1: Use the source MAC of the incoming packet and check the MAC VLAN mapping. If the VLAN is found for this source MAC, that VLAN ID is used as the VLAN for this packet. If the MAC VLAN is not found, proceed to the next step.

Step 2: Use the protocol field from the incoming packet layer 2 header and check the protocol VLAN table. If a protocol VLAN is found, that VLAN ID is used as the VLAN for this packet. If a protocol VLAN is not found, proceed to the next step.

Step 3: This step identifies the VLAN based on a port based VLAN configuration. If the received port is in access mode, the configured access VLAN (default is VLAN 1) is used as the VLAN for this packet. If the received port is in trunk mode, the configured trunk native VLAN (default is VLAN 1) is used as the VLAN for this packet. If the received port is in hybrid mode, the configured PVID (default is VLAN 1) is used as the VLAN for this packet.

This VLAN identification procedure is shown in Figure VLAN-3: VLAN Identification Procedure.

Once the VLAN is identified for the received packet, the switch checks if the received port is a member of this identifier VLAN. If the received is not member of the identified VLAN, the packet is dropped. If the received port is a member of the identified VLAN, then it will be forwarded to other member ports of this VLAN based on the forwarding logic. If there are no other member ports for this VLAN, the packet will most likely be dropped unless it was routed or sent to the CPU or redirected by an ACL rule.
Figure VLAN-3: VLAN Identification Procedure

- Packet has VLAN tag?
  - No
  - Yes
    - VLAN ID != 0?
      - No
      - Use VLAN ID from VLAN tag
      - Yes
      - Use Protocol VLAN ID
    - Yes
      - Use MAC VLAN ID
  - Use Access VLAN ID
  - Use Trunk Native VLAN ID
  - Use PVID as VLAN ID

- Found Src MAC in MAC VLAN?
  - No
    - Yes
      - Use MAC VLAN ID
    - No
      - Yes
        - Use Protocol VLAN ID
      - No
        - Yes
          - Use Access VLAN ID
          - No
            - Yes
              - Use Trunk Native VLAN ID
              - No
                - Yes
                  - Use PVID as VLAN ID
                  - No
                    - Found VLAN

- Is Access Port?
  - No
    - Yes
      - Use Access VLAN ID
      - No
        - Yes
          - Use Trunk Native VLAN ID
          - No
            - Yes
              - Use PVID as VLAN ID
              - No
                - Found VLAN

- Is Trunk Port?
  - No
    - Yes
      - Use Trunk Native VLAN ID
      - No
        - Yes
          - Use PVID as VLAN ID
          - No
            - Found VLAN

- Is Hybrid Port?
  - No
    - Yes
      - Use PVID as VLAN ID
      - No
        - Found VLAN
### 3.3 VLAN Numbers

SSE-G3548S/R supports 4K static VLANs.

SSE-G3548S/R switches support VLAN identifiers from 1 to 4069 for user created VLANs. VLAN identifiers 4070 to 4094 are reserved for internal use.

The command **`show vlan device info`** displays the maximum VLAN identifiers and total number of VLANs supported by the switch.

SSE-G3548S/R supports 1024 MAC based VLANs.

Supermicro switches support 16 protocol groups for protocol based VLANs. These 16 protocol groups can be mapped to different VLANs in every port. The same protocol group can be associated with different VLANs in different ports.

### 3.4 VLAN Defaults

Supermicro switches boot up with VLAN 1, which is a default Layer 2 VLAN. The switchable ports of all switches are added to this default VLAN 1 as hybrid ports. This default setup helps switch forwarding traffic across all the ports without the need of any user configuration.

Users can modify the port members of this VLAN 1 by adding or removing any ports to this VLAN 1 as either tagged or untagged ports. The easier way is to change the port modes to either “Access” or “Trunk” ports and configure the relevant VLANs. The “Access” and “Trunk” modes are described in detail in later sections.

VLAN 1 cannot be deleted by the user. If user wants to prohibit traffic from/to VLAN 1, then remove all the ports from VLAN 1 by using the **`no ports`** command available in the VLAN configuration mode. After removing all the ports, **“show vlan id 1”** command should display ‘none’ as shown below.

```
SMIS(config)# show vlan id 1

Vlan database
----------
Vlan ID : 1
Member Ports : None
Hybrid Tagged Ports : None
Hybrid Untagged Ports : None
Hybrid Forbidden Ports : None
Access Ports : None
Trunk Ports : None
Name :
Status : Permanent
```

---

---
The port based VLAN identifier (PVID) for all the switch ports is set to 1 by default. The PVID is used to associate incoming untagged packets to port based VLANs for the ports in “Hybrid” mode. Users can modify the PVID for switch ports to any VLAN identifier for “Hybrid” ports.

The switch port mode is set to “hybrid” for all switch ports by default. Users can change the port mode as explained in the Port Based VLAN section.

VLAN 1 is configured as the default native VLAN for all trunk interfaces. Users can change the native VLANs for trunk interfaces as explained in the Native VLAN on Trunk section.

Protocol based VLAN is enabled by default.

Supermicro switches do not create VLANs by default except for VLAN 1. Users need to create all the VLANs used on their network in Supermicro switches. Trunk ports will be able to carry only VLANs created in Supermicro switches.

### 3.5 Creating VLANs

Follow the steps below to create VLANs in Supermicro switches.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan &lt;vlan-list&gt;</td>
<td>Creates a VLAN using vlan command. &lt;vlan-list&gt; – 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. User can configure VLANs with identifiers 1 to 4069.</td>
</tr>
<tr>
<td>Step 3</td>
<td>show vlan</td>
<td>Displays the configured VLANs</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – Save these VLAN configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The examples below show various ways of creating VLANs.

**Create a VLAN with identifier 10**
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# exit

Create VLANs with identifiers 20 to 30, 50 and 100

SMIS# configure terminal
SMIS(config)# vlan 20-30,50,100
SMIS(config-vlan)# exit

3.6 Removing VLANs

Follow the steps below to remove VLANs from Supermicro switches.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no vlan &lt;vlan-list&gt;</td>
<td>Remove VLANs using the no vlan command.</td>
</tr>
</tbody>
</table>

 vlan-list – may be any vlan number or list of vlan numbers. Multiple vlan numbers can be provided as comma separated list. Consecutive vlan numbers can be provided as ranges like 5-10.

| Step 3 | show vlan | To display the configured VLANs |
| Step 4 | write startup-config | Optional step – Save these VLAN configuration to be part of startup configuration. |

The below examples show ways to remove VLANs.

Delete a VLAN with identifier 10

SMIS# configure terminal
SMIS(config)# no vlan 10

Delete VLANs with identifier 20 to 30, 50 and 100

SMIS# configure terminal
SMIS(config)# no vlan 20-30,50,100
SMIS(config-vlan)# exit

3.7 VLAN Name

VLANs can be associated with a label name string for easier configuration and identification.

Follow the steps below to add or modify a name string to any VLAN in Supermicro switches.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | vlan <vlan-list> | Enters the VLAN configuration mode.  
  
  **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.  
  
  If multiple VLANs are provided, the same name string provided in next step will be associated with all these VLANs. |
| Step 3 | name <vlan-name-string> | Associates a name string to this VLAN using the name command.  
  
  **vlan-name-string** is any alphanumeric string up to 32 characters. |
| Step 4 | show vlan | Displays the configured VLANs |
| Step 5 | write startup-config | Optional step – saves this VLAN configuration to be part of startup configuration. |

The example below shows the steps necessary to associate a name string to a VLAN.

**Associate name main_user_vlan to VLAN 50.**

```
SMIS# configure terminal
SMIS(config)# vlan 50
SMIS(config-vlan)# name main_user_vlan
SMIS(config-vlan)# exit
```

Follow the steps below to remove a name string from any VLAN in a Supermicro switch.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | vlan <vlan-list> | Enters the VLAN configuration mode.  
  
  **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.  
  
  If multiple VLANs are provided, the name string of all these VLANs will be removed by the next step. |
The example below shows steps to remove name string from a VLAN.

**Remove name from VLAN 50.**

```
SMIS# configure terminal
SMIS(config)# vlan 50
SMIS(config-vlan)# no name
SMIS(config-vlan)# exit
```

### 3.8 Port Based VLANs

Port based VLANs are the simplest and most useful type of VLAN.

In port based VLAN deployment, switch ports are associated with one or more VLANs as member ports.

The traffic sent on the ports is decided by the VLAN membership and mode of the ports. Usually ports are associated with VLANs as either “access” port members or “trunk” port members. Supermicro switches support an additional port mode called “hybrid”.

---

**Port Channel interfaces also can be configured as VLAN member ports.**

---

**Figure VLAN-4: Port Based VLANs**
3.8.1 Access Ports

Access ports carry the traffic of only one VLAN. Any switch port can be configured as an access port. Usually switch ports connected to end stations (computers / servers) that have only one type of traffic are configured as access ports.

Access ports cannot be configured to be part of more than one VLAN.

Switches will not add VLAN tag headers to all the packets sent out on an access port. Switches expect to receive untagged or priority tagged (VLAN identifier 0) packets only at the access ports. If any tagged packets are received on an access port, the switch will drop them. Follow the below steps to configure any port as the access port of any VLAN.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | interface <interface-type> <interface-id> or interface range <interface-type> <interface-id> | Enters the interface mode. 

interface-type – may be any of the following:
- fx-ethernet – fx
- cx-ethernet – cx
- port-channel – po

interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.

To configure multiple interfaces, use the “interface range ..” command. To provide a range use a hypen (-) between the start and end interface numbers.

E.g.: int range fx 0/1-10
To provide multiple interfaces or ranges, use separate with a comma (,).

E.g.: int range fx 0/1-10, fx 0/20

Step 3 | switchport mode access | Sets the port mode as the access port. |

Step 4 | switchport access vlan <vlan-id> | Configures the access VLAN for this interface. The VLAN identifiers may be any VLAN number from 1 to 4069.

If the given VLAN does not exist, switch will provide a warning message. Only when the VLAN available, the port will operate as an access port for that VLAN.
### Step 5

**show vlan port config port <iftype> <ifnum>**

Displays the configured mode and accesses the VLAN for this interface.

| Step 6 | **write startup-config** | Optional step – saves this VLAN configuration to be part of startup configuration. |

---

The “switchport access vlan” command will be accepted only if the port is in access mode.

The **no switchport mode** command will change the port mode to the default hybrid mode. For more details about hybrid mode, refer to the Hybrid Ports section.

The **no switchport access vlan** command will set the access VLAN as default VLAN 1. The port will continue to be the access port of VLAN 1.

The examples below show various ways to create VLANs with access ports.

**Create a VLAN with identifier 50 and configure ports fx 0/2 to fx 0/10 as access ports to this VLAN.**

```
SMIS# configure terminal
SMIS(config)# vlan 50
SMIS(config-vlan)# exit
SMIS(config)# interface range fx 0/2-10
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 50
SMIS(config-if)# exit
```

**Create a VLAN with identifier 10 and configure port channel 1 as access port to this VLAN.**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# exit
SMIS(config)# interface po 1
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# exit
```

### 3.8.2 Trunk Ports

Trunk ports carry the traffic of one or more VLANs. Any switch port can be configured as a trunk port. Usually switch ports connected between switches are configured as trunk ports to carry multiple VLAN traffic across switches. Switch ports connected to end stations (computers / servers) that have multiple VLANs are also configured as trunk ports.

When a switch port is configured as a trunk port, it will be added to all the VLANs in the switch as a tagged port by default. To restrict the VLANs carried in trunk ports, refer to the Allowed VLANs on a Trunk section.
Trunk ports will not carry traffic for VLANs that are not configured in a switch.
For example, if the user wants to carry traffic for all the VLANs from 1 to 1024 in a trunk port, VLANs 1 to 1024 need to be created in the switch using the “vlan” command.

A switch adds the VLAN tag header to all packets sent out on the trunk port except for native VLAN traffic. Supermicro switches support only IEEE 802.1Q encapsulation for VLAN tag headers.

When a packet is received on a trunk port, the switch identifies the VLAN for the received packet from the packet’s VLAN tag header. If the received packet did not have a VLAN identifier and the packet did not match any MAC or protocol VLAN, the native VLAN is used to determine the VLAN for all untagged and priority tagged packets that are received.

If the user has not configured a native VLAN, the default VLAN 1 will be used as native VLAN for the trunk ports.

Follow the steps below to configure any port as a trunk port.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | interface <interface-type> <interface-id> or interface range <interface-type> <interface-id> | Enters the interface mode.  

**interface-type** – may be any of the following:  
fx-ethernet – fx  
cx-ethernet – cx  
port-channel – po  

**interface-id** is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.  
E.g.: int range fx 0/1-10  
To provide multiple interfaces or ranges, separate with a comma (,).  
E.g.: int range fx 0/1-10, fx 0/20 |
| Step 3 | switchport mode trunk | Sets the port mode as a trunk port. |
| Step 4 | show vlan port config port <iftype> <ifnum> and show running-config | Displays the configured mode for this interface. |
| Step 5 | write startup-config | Optional step – saves this VLAN configuration to be part of startup configuration. |
The “no switchport mode” command will change the port mode to the default hybrid mode. For more details about hybrid mode, refer to the Hybrid Ports section.

The examples below show various ways to configure trunk ports.

**Configure port fx 0/1 and fx 0/2 as trunk ports.**

SMIS# configure terminal
SMIS(config)# interface range fx 0/1-2
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit

Configure port channel 1 as a trunk port.

SMIS# configure terminal
SMIS(config)# interface po 1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit

### 3.8.2.1 Allowed VLANs on a Trunk

By default, all the VLANs configured on a switch are allowed on the trunk interfaces. However, there may be some cases where users would like to limit the number of VLANs carried on the trunk ports. This can be configured by following the steps below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface range &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
</tbody>
</table>

*interface-type* – may be any of the following:
- fx-ethernet – fx
- cx-ethernet – cx
- port-channel – po

*interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.

E.g.: int range fx 0/1-10
To provide multiple interfaces or ranges, separate with a comma (,).
E.g.: `int range fx 0/1-10, fx 0/20`

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>switchport mode trunk</code></td>
<td>Sets the port mode as trunk port.</td>
</tr>
<tr>
<td>4</td>
<td>Use any one of the below steps 4a to 4f based on the need.</td>
<td>The <code>vlan-list</code> parameter used in the below commands could 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.</td>
</tr>
<tr>
<td>4a</td>
<td><code>switchport trunk allowed vlan &lt;vlan-list&gt;</code></td>
<td>This command configures the list of allowed VLANs on this trunk. Only the VLANs provided on the <code>vlan-list</code> will be carried over the trunk.</td>
</tr>
<tr>
<td>4b</td>
<td><code>switchport trunk allowed vlan add &lt;vlan-list&gt;</code></td>
<td>This command adds the given list of VLANs to the existing set of allowed VLANs on this trunk.</td>
</tr>
<tr>
<td>4c</td>
<td><code>switchport trunk allowed vlan remove &lt;vlan-list&gt;</code></td>
<td>This command removes the given list of VLANs from the existing set of allowed VLANs on this trunk.</td>
</tr>
<tr>
<td>4d</td>
<td><code>switchport trunk allowed vlan except &lt;vlan-list&gt;</code></td>
<td>This command makes all the configured VLANs allowed on this trunk except for the given list of VLANs.</td>
</tr>
<tr>
<td>4e</td>
<td><code>switchport trunk allowed vlan all</code></td>
<td>This command sets the default behavior of allowing all VLANs configured in the switch as allowed VLANs on this trunk.</td>
</tr>
<tr>
<td>4f</td>
<td><code>switchport trunk allowed vlan none</code></td>
<td>This command removes all the allowed VLANs from this trunk.</td>
</tr>
<tr>
<td>5</td>
<td><code>show vlan port config port &lt;iftype&gt; &lt;ifnum&gt;</code> and <code>show running-config</code></td>
<td>Displays the configured, allowed VLANs for this trunk interface.</td>
</tr>
<tr>
<td>6</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this VLAN configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The "switchport trunk allowed vlan ..." commands will be accepted only if the port is in trunk mode.

A trunk port will not carry traffic for any VLANs that are not configured in the switch. For example, if a user wants to allow traffic for VLANs 1 to 100, VLANs 1 to 100 need to be created in the switch using the "vlan" command.

The examples below show examples of configurations to allow VLANs on trunk ports.

**Configure to allow only VLANs 2 to 20 on trunk interface fx 0/1.**
SMIS# configure terminal
SMIS(config)# vlan 2-20
SMIS(config-vlan)# exit
SMIS(config)# interface fx 0/1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan 2-20
SMIS(config-if)# exit

Configure to not to allow VLANs 30 to 50 on trunk interface fx 0/1.

SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan except 30-50
SMIS(config-if)# exit

3.8.2.2 Native VLAN on Trunk
All packets sent out on a trunk interface carry the 802.1Q VLAN tag header. There may be cases in which untagged packets need to be carried over a trunk interface. This is achieved by using the native VLAN feature of the trunk interface.

Any VLAN can be configured on any trunk interface as a native VLAN. Trunk interfaces will send native VLAN packets as untagged packets without adding the 802.1Q VLAN tag header. Similarly, any untagged packets received on a trunk interface will be considered to be native VLAN packets.

VLAN 1 is the default native VLAN for all trunk interfaces.

Users can configure a native VLAN for trunk interfaces by following the steps below.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | `interface <interface-type> <interface-id>` or `interface range <interface-type> <interface-id>` | Enters the interface mode.  
*interface-type* – may be any of the following:  
- fx-ethernet – fx  
- cx-ethernet – cx  
- port-channel – po  
*interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces.  
To configure multiple interfaces, use the “*interface range ...*” command. To provide a range, use a hypen (-) between the start and end interface numbers.  
E.g.: `int range fx 0/1-10`  
To provide multiple interfaces or ranges, separate with a comma (,).  
E.g.: `int range fx 0/1-10, fx 0/20` |
| Step 3 | `switchport mode trunk` | Sets the port mode as a trunk port. |
| Step 4 | `switchport trunk native vlan <vlan-id>` | *vlan-id* - The VLAN identifiers may be from 1 to 4069.  
If the given VLAN does not exist, switch will provide a warning message. In this case the native VLAN traffic will be dropped until the VLAN become available.  
Also, the given VLAN should be part of allowed VLANs in the trunk. If the native VLAN is not member of allowed VLAN list, the native VLAN packets will be dropped. |
| Step 5 | `show vlan port config port <iftype> <ifnum>` and `show running-config` | Displays the configured native VLAN for this trunk interface. |
| Step 6 | `write startup-config` | Optional step – saves this VLAN configuration to be part of startup configuration. |
The “switchport trunk native vlan” command will be accepted only if the port is in trunk mode.

The “no switchport trunk native vlan” command will reset the native VLAN as VLAN 1 for trunk interfaces.

The native VLAN needs to be part of allowed VLANs to pass native VLAN traffic.

The examples below show examples of configuring native VLANs for trunk ports.

**Configure VLAN 20 as a native VLAN for trunk interface fx 0/1.**

```plaintext
SMIS# configure terminal
SMIS(config)# vlan 20
SMIS(config-vlan)# exit
SMIS(config)# interface fx 0/1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk native vlan 20
SMIS(config-if)# exit
```

**Remove a native VLAN from trunk interface fx 0/1.**

```plaintext
SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# no switchport trunk native vlan
SMIS(config-if)# exit
```

### 3.8.3 Hybrid Ports

Hybrid ports carry both untagged and 802.1Q tagged packets.

Hybrid ports carry the traffic of one or more VLANs. Any switch port can be configured as a hybrid port. In Supermicro switches, all switch ports by default come up in hybrid mode.

Users need to explicitly add the hybrid ports to all the required VLANs as either tagged or untagged interfaces. A hybrid port could be configured as a tagged or untagged port simultaneously on one or more VLANs.

Users need to configure the PVID for hybrid ports to correctly handle the incoming untagged packets.

It is recommended for users to use hybrid ports only when they thoroughly understand the PVID, tagged and untagged interfaces of their network.

Hybrid ports might cause VLAN packet forwarding drops if the ports are not correctly added to the required VLANs as untagged or tagged interfaces as needed.

Hybrid port functionality can be achieved through trunk ports with allowed VLANs and a native VLAN configuration.
When MAC based VLANs and protocol based VLANs are used, the ports need to be in “Hybrid” mode.

A switch adds the 802.1Q VLAN tag header for VLAN traffic in which the hybrid port is configured as a tagged interface. The switch sends out packets without a VLAN tag header for the VLAN on which the hybrid port is configured as an untagged interface.

When a packet is received on a hybrid port, a switch identifies the VLAN for the received packet from the packet’s VLAN tag header. If the received packet did not have a VLAN identifier and the packet did not match any MAC or protocol VLAN, the port PVID is used as the VLAN for all the received untagged and priority tagged packets. If the user has not configured the PVID, VLAN 1 will be used as the default PVID for hybrid ports.

Follow the steps below to configure any port as a hybrid port.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan &lt;vlan-list&gt;</td>
<td>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. If multiple VLANs are provided, the ports configuration provided in the next steps will be applied to all these VLANs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Use steps 3a to 3c below one or more times to configure the required port configurations for the VLANs provided in Step 2 above.</td>
<td></td>
</tr>
<tr>
<td>Step 3a</td>
<td>ports &lt;ports-list&gt; tagged or no ports [&lt;ports-list&gt;] tagged</td>
<td>Adds the tagged ports list to this VLAN. ports-list – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10. Use the no form of this command to remove tagged ports from this VLAN. If ports-list is not provided to the no command, all the tagged ports are removed from this VLAN.</td>
</tr>
<tr>
<td>Step 3b</td>
<td>ports &lt;ports-list&gt; untagged or no ports [&lt;ports-list&gt;] untagged</td>
<td>Adds the untagged ports list to this VLAN.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 3c   | **ports** `<ports-list>` **forbidden**  
or  
**no ports** `[<ports-list>]` **forbidden** | Denies traffic from ports given by `<ports-list>` to this VLAN.  
*ports-list* – up to three ports or ranges of ports separated by spaces.  
The range of ports is provided in the format `fx 0/1-10`, which specifies the ports from `fx 0/1` to `fx 0/10`.  
Use the `no` form of this command to remove forbidden ports from this VLAN.  
If `ports-list` is not provided to the `no` command, all the forbidden ports are removed from this VLAN. |
| 4    | **Exit** | Exits the VLAN configuration mode. |
| 5    | **interface** `<interface-type>` `<interface-id>`  
or  
**interface range** `<interface-type>` `<interface-id>` … | Enters the interface mode.  
*interface-type* – may be any of the following:  
`fx-ethernet` – `fx`  
`cx-ethernet` – `cx`  
`port-channel` – `po`  
*interface-id* is in `slot/port` format for all physical interfaces. It may be a port channel identifier for port channel interfaces.  
To configure multiple interfaces, use the “**interface range** …” command. To provide a range, use a hyphen (-) between the start and end interface numbers.  
E.g.: `int range fx 0/1-10`  
To provide multiple interfaces or ranges, separate with a comma (,).  
E.g.: `int range fx 0/1-10, fx 0/20` |
| 6    | **switchport mode hybrid** | Sets the port mode as a hybrid port. |
### Step 7

**switchport pvid <vlan-id>**

Configures the PVID for this interface. The VLANs identifiers could be any VLAN number from 1 to 4069.

The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first.

This command accepted only when the port is “Hybrid” mode.

### Step 8

**show vlan port config port <itype> <ifnum>**

**show running-config**

**show vlan**

Displays the configured VLAN and ports information.

### Step 9

**write startup-config**

Optional step – saves this VLAN configuration to be part of startup configuration.

---

The “ports ...” command can be used only for the ports in “hybrid” mode.

The “switchport pvid ...” command will be accepted only when a port is in “hybrid” mode.

A port can be configured as a tagged port for multiple VLANs.

A port can be configured as an untagged port for multiple VLANs. This is useful for MAC based VLANs. For a port based VLAN configuration, having a port as untagged in multiple VLANs is not a recommended configuration as all the received untagged packets can be associated with only one PVID of that port. In a MAC based VLAN, the received untagged packets will be matched to different VLANs based on the MAC address on the packet.

The examples below show various ways to configure hybrid ports.

**Configure a VLAN 10 with ports fx 0/1 to fx 0/10 as untagged ports and add port cx 0/1 as a tagged port to this VLAN.**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/1-10 untagged
SMIS(config-vlan)# ports cx 0/1 tagged
SMIS(config-vlan)# exit
SMIS(config)# interface range fx 0/1-10
SMIS(config-if)# switchport mode hybrid
SMIS(config-if)# switchport pvid 10
SMIS(config-if)# exit
```
Configure a VLAN 100 with ports fx 0/1, fx 0/10, fx 0/20, fx 0/30, fx 0/40 and cx 0/1-2 as untagged ports and add port channel 1 as a tagged port to this VLAN.

SMIS# configure terminal
SMIS(config)# vlan 100
SMIS(config-vlan)# ports fx 0/1 fx 0/10 fx 0/20 untagged
SMIS(config-vlan)# ports fx 0/30 fx 0/40 cx 0/1-2 untagged
SMIS(config-vlan)# ports po 1 tagged
SMIS(config-vlan)# exit
SMIS(config)# interface range fx 0/1,fx 0/10, fx 0/20, fx 0/30, fx 0/40, cx 0/1-2
SMIS(config-if)# switchport mode hybrid
SMIS(config-if)# switchport pvid 100
SMIS(config-if)# exit

3.9 MAC Based VLANs

When end users move often from one place to another but remain inside the same LAN, it is difficult to maintain the same VLAN for an end user in a port based VLAN configuration.

MAC based VLAN features are used to provide the same VLAN to any end user irrespective of the switch port the end user is connecting to.

The switch administrator may configure MAC to VLAN mappings for unicast MAC addresses. When a switch receives any untagged packets, the source MAC address of the packet refers to this MAC VLAN mapping to identify the VLAN. If MAC VLAN mapping is not found for the received source MAC address, a protocol based VLAN or port based VLAN is used.

Supermicro switches support 1024 MAC based VLANs.

Figure VLAN-6: MAC Based VLANs
Follow the steps below to configure MAC based VLANs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>vlan &lt;vlan-list&gt;</code></td>
<td>Creates the required VLANs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>vlan-list</code> – may be any VLAN number or list of VLAN numbers. Multiple VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>numbers can be provided as comma separated values. Consecutive VLAN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>numbers can be provided as ranges such as 5-10.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ports &lt;ports-list&gt; untagged</code></td>
<td>Adds the ports given by <code>ports-list</code> to this VLAN as untagged ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ports-list</code> – up to three ports or ranges of ports separated by spaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The range of ports is provided in the format fx 0/1-10, which specifies the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ports from fx 0/1 to fx 0/10.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Exit</td>
<td>Exits the VLAN configuration mode</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>mac-vlan &lt;ucast_mac&gt; vlan &lt;vlan-id&gt;</code></td>
<td>Configures MAC VLAN mapping entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ucast_mac</code> – Unicast MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This VLAN will be applied to all incoming untagged packets from this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unicast MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>vlan-id</code> - VLAN identifiers may be any VLAN number from 1 to 4069. The</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VLAN must have already been created in this switch.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show mac-vlan</code></td>
<td>Displays the configured MAC based VLANs.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this VLAN configuration to be part of startup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration.</td>
</tr>
</tbody>
</table>

User has to create the VLANs using the “vlan ..” command prior to configuring MAC address VLAN mapping.

The ports required to support MAC VLAN have to be configured as untagged ports in the hybrid mode to those VLANs.

Follow the steps below to remove MAC based VLANs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | **no mac-vlan** `<ucast_mac>` | Removes MAC VLAN mapping entry.  
`ucast_mac` – Unicast MAC address for which MAC VLAN mapping is to be removed. |
| Step 3 | **show mac-vlan** | Displays the configured MAC based VLANs. |
| Step 4 | **write startup-config** | Optional step – saves this VLAN configuration to be part of startup configuration. |

The examples below show various ways to configure MAC based VLANs.

**Create a VLAN 10 and configure MAC address 00:30:40:10:10:10 to VLAN 10 for the ports fx 0/1 to 10**

SMIS# `configure terminal`
SMIS(config)# `vlan 10`
SMIS(config-vlan)# `ports fx 0/1-10 untagged`
SMIS(config-vlan)# `exit`
SMIS(config)# `mac-vlan 00:30:40:10:10:10 vlan 10`

**Remove MAC VLAN for MAC address 00:30:40:20:20:20.**

SMIS# `configure terminal`
SMIS(config)# `no mac-vlan 00:30:40:20:20:20`

**3.10 Protocol Based VLANs**

Protocol based VLAN features help to classify incoming traffic to different VLANs based on the protocol. The protocol or ethertype field in the Layer 2 header is used to classify the packets to different VLANs.

Protocol VLAN features are enabled by default in Supermicro switches.

The protocol based VLAN features configuration is a three-step process, as shown in the diagram below.

![Figure VLAN-7: Protocol Based VLAN Configuration Steps](image)

Follow the steps below to configure protocol based VLANs.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan &lt;vlan-list&gt;</td>
<td><code>vlan-list</code> – 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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ports &lt;ports-list&gt; untagged</td>
<td>Adds the required ports for this VLAN as untagged ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ports-list</code> – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in a format like fx 0/1-10, which refers to ports from fx 0/1 to fx 0/10.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Exit</td>
<td>Exits the VLAN configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>map protocol {arp</td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protocol group creation takes three parameters. First: protocol field as <code>arp</code>, <code>ip</code>, <code>rarp</code>, <code>ipx</code>, <code>novell</code>, <code>netbios</code> or <code>appletalk</code>. Users can enter any other two-byte protocol fields in hex format as aa:aa.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Second: frame type as <code>enet-v2</code>, <code>llc</code> or <code>snap</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third: protocol group identifier number.</td>
</tr>
<tr>
<td>Step 6</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface range &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-type</code> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-id</code> is in <code>slot/port</code> format for all physical interfaces. It could be the port channel identifier for port channel interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “<code>interface range ...</code>” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E.g.: <code>int range fx 0/1-10</code></td>
</tr>
</tbody>
</table>
To provide multiple interfaces or ranges, separate with a comma (,).  
E.g.: `int range fx 0/1-10, fx 0/20`

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| switchport map protocols-group `<Group id integer(0-2147483647)>` vlan `<vlan-id(1-4069)>` | Associates the group to the VLAN on the above interface.  
`Group id` – Protocol Group Identifier  
`vlan-id` – VLAN identifier. |

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| switchport pvid `<vlan-id>` | Configures the PVID for the default port based VLAN behavior. This will be used for packets that did not match any protocol VLAN map.  
The VLAN identifiers may be any VLAN number from 1 to 4069.  
The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first. |

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit</td>
<td>Exits the interface configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan protocols-group show protocol-vlan</td>
<td>Displays the configured protocol based VLANs.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>write startup-config</td>
<td>Optional step – saves this VLAN configuration to be part of startup configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Follow the below steps to remove protocol based VLANs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | interface `<interface-type> `<interface-id>`  
or  
interface range `<interface-type> `<interface-id>`  
.... | Enters the interface mode.  
`interface-type` – may be any of the following:  
fx-ethernet – fx  
fx-ethernet – cx  
port-channel – po  
`interface-id` is in slot/port format for all physical interfaces. It could be a port channel identifier for port channel interfaces.  
To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers. |
The examples below show various ways to configure protocol based VLANs.

**Assign all IP traffic to VLAN 20 and all other traffic to VLAN 30 on ports fx 0/1 to fx 0/10.**

```
SMIS# configure terminal
SMIS(config)# vlan 20,30
SMIS(config-vlan)# po fx 0/1-10 untagged
SMIS(config-vlan)# exit
SMIS(config)# map protocol arp enet-v2 protocols-group 1
SMIS(config)# map protocol ip enet-v2 protocols-group 2
SMIS(config)# int range fx 0/1-10
SMIS(config-if)# switchport map protocols-group 1 vlan 20
SMIS(config-if)# switchport map protocols-group 2 vlan 20
```
SMIS(config-if)# switchport pvid 30
SMIS(config-if)# exit

Remove protocol VLAN 20.

SMIS# configure terminal
SMIS(config)# int range fx 0/1-10
SMIS(config-if)# no switchport map protocols-group 1
SMIS(config-if)# no switchport map protocols-group 2
SMIS(config-if)# exit
SMIS(config)# no map protocol arp enet-v2
SMIS(config)# no map protocol ip enet-v2
SMIS(config)# no vlan 20

3.11 Acceptable Frame Types

By default, Supermicro switch ports accept all frames types – tagged, untagged and priority tagged.

Priority tagged packets have a VLAN tag header with a VLAN identifier of 0.

For access ports, the default acceptable frame type is untagged and priority tagged only.

Users can control this behavior to make switch ports accept either only tagged or untagged and priority tagged packets.

Follow the steps below to configure acceptable frame types for any port or port channel.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2| interface <interface-type> <interface-id> or interface range <interface-type> <interface-id> | Enters the interface mode.  

- **interface-type** – may be any of the following:
  - fx-ethernet – fx
  - cx-ethernet – cx
  - port-channel – po

- **interface-id** is in **slot/port** format for all physical interfaces. It may be a port channel identifier for port channel interfaces.

To configure multiple interfaces, use the “**interface range ...**” command. To provide a range, use a hyphen (-)
between the start and end interface numbers.
E.g.: `int range fx 0/1-10`
To provide multiple interfaces or ranges, separate with a comma (,).
E.g.: `int range fx 0/1-10, fx 0/20`

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Use any of the below steps 3a to 3d to configure acceptable frame types for the ports provided in Step 2 above.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3a</td>
<td><code>switchport acceptable-frame-type tagged</code></td>
</tr>
<tr>
<td></td>
<td>This command makes only tagged frame types accepted on these ports. Any untagged or priority tagged packets received will be dropped.</td>
</tr>
<tr>
<td>Step 3b</td>
<td><code>switchport acceptable-frame-type untaggedAndPrioritytagged</code></td>
</tr>
<tr>
<td></td>
<td>This command makes only untagged and priority tagged frame types accepted on these ports. Any tagged packets received will be dropped.</td>
</tr>
<tr>
<td>Step 3c</td>
<td><code>switchport acceptable-frame-type all</code></td>
</tr>
<tr>
<td></td>
<td>This command makes accepting all frame types the default behavior.</td>
</tr>
<tr>
<td>Step 3d</td>
<td><code>no switchport acceptable-frame-type</code></td>
</tr>
<tr>
<td></td>
<td>This command makes accepting all frame types the default behavior.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show vlan port config port &lt;iltype&gt; &lt;ilnum&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Displays the configured mode and access VLAN for this interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>write startup-config</code></td>
</tr>
<tr>
<td></td>
<td>Optional step – saves this VLAN configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The examples below show various ways to configure acceptable frame types on switch ports.

**Configure fx 0/1 to fx 0/10 to accept only untagged and priority tagged packets.**

SMIS# configure terminal
SMIS(config)# interface range fx 0/1-10
SMIS(config-if)# switchport acceptable-frame-type untaggedAndPrioritytagged
SMIS(config-if)# exit

**Configure port channel interface 1 to accept only tagged packets.**

SMIS# configure terminal
SMIS(config)# interface po 1
SMIS(config-if)# switchport acceptable-frame-type tagged
SMIS(config-if)# exit
3.12 Ingress Filter

By default, Supermicro switch has the ingress filter enabled. The ingress filter drops packets that do not match the configured VLAN membership.

For example, if the switch has two VLANs configured as 10 and 20, the ports configured with only VLAN 10 can accept packets with the VLAN header having VLAN identifier 20. This is called VLAN hoping. To prevent VLAN hoping, the ingress filter is enabled to drop those packets with a different VLAN identifier than the VLAN configured on the port.

The ingress filter can be disabled to allow VLAN hoping if needed.

Follow the steps below to enable/disable ingress filtering for any port or port channel.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td>or</td>
<td>interface range &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td></td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport ingress-filter (or) no switchport ingress-filter</td>
<td>This command enables ingress filtering function. This is the default behavior. The no form of this command disables ingress filtering.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vlan port config port &lt;iftype&gt; &lt;ifnum&gt;</td>
<td>Displays the configured ingress filter mode for this interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this VLAN configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no switchport ingress-filter” command disables the ingress filter.

The examples below show how to enable ingress filter on switch ports.

**Disable ingress filter for ports fx 0/1 to fx 0/10.**

```bash
SMIS# configure terminal
SMIS(config)# interface range fx 0/1-10
SMIS(config-if)# no switchport ingress-filter
SMIS(config-if)# exit
```

### 3.13 VLAN Configuration Example

Configure the following requirements on switch A, as shown below in Figure VLAN-8.

1. Ports Fx 0/1 to Fx 0/10 are trunk ports connected to servers that have VLANs 10, 20 and 30. Here, VLAN 10 is untagged.
2. Port Fx 0/41 is a trunk port connected to storage, which carries VLAN 20 and 30.
3. Ports Fx 0/20 to Fx 0/40 are access ports for VLAN 10.
4. Ports Fx 0/15 and Fx 0/16 are part of a trunk port channel that carries all the VLANs to other switches with native VLAN 10.

![Figure VLAN-8: VLAN Configuration Example](image-url)
# Create all the VLANs first
SMIS(config)# vlan 10,20,30
SMIS(config-vlan)# exit

# Configure VLANs for ports fx 0/1-10
SMIS(config)# interface range fx 0/1-10
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk native vlan 10
SMIS(config-if)# exit

# Configure VLANs for port fx 0/41
SMIS(config)# int fx 0/41
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit

# Configure the access VLAN for ports fx 0/20 to fx 0/40
SMIS(config)# interface range fx 0/20-40
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# exit

# Configure the port channel trunk interface on fx 0/15 and fx 0/16
SMIS(config)# interface port-channel 1
SMIS(config-if)# exit
SMIS(config)# interface range fx 0/15-16
SMIS(config-if)# channel-group 1 mode on
SMIS(config-if)# exit
SMIS(config)# interface port-channel 1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk native vlan 10
SMIS(config-if)# end

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

Building configuration...

```
ID   Hardware Version       Firmware OS   Boot Loader
0     SSE-F3548             1.0.0.0  6     0.0.0.0

ip address 172.31.30.120
interface port-channel 1
exit

# Vlans and hybrid mode member ports configurations
```
vlan 1
  ports fx 0/11-14 untagged
ports fx 0/17-19 untagged
ports fx 0/41-48 untagged
ports cx 0/1-6 untagged
exit
vlan 10,20,30
exit

interface Fx 0/1
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/2
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/3
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/4
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/5
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/6
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/7
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/8
  switchport mode trunk
  switchport trunk native vlan 10

interface Fx 0/9
  switchport mode trunk
  switchport trunk native vlan 10
interface Fx 0/10
switchport mode trunk
switchport trunk native vlan 10

interface Fx 0/15
channel-group 1 mode on

interface Fx 0/16
channel-group 1 mode on

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

interface Fx 0/21
switchport mode access
switchport access vlan 10

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

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

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

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

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

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

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

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

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

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

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

interface Fx 0/33
switchport mode access
switchport access vlan 10

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

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

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

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

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

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

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

interface po 1
switchport mode trunk
switchport trunk native vlan 10

exit
SMIS# show vlan

Vlan database
-------------
Vlan ID: 1
Member Ports: fx 0/1-14 fx 0/17-19 fx 0/41-48 cx 0/1-6 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: None
Trunk Ports: fx 0/1-10 po 1
Name: 
Status: Permanent
----------------------------------------------------
Vlan ID: 10
Member Ports: fx 0/1-10 fx 0/20-40 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: fx 0/20-40
Trunk Ports: fx 0/1-10 po 1
Name: 
Status: Permanent
----------------------------------------------------
Vlan ID: 20
Member Ports: fx 0/1-10 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: None
Trunk Ports: fx 0/1-10 po 1
Name:
3.14 Private Edge VLAN/Protected Ports

The private edge VLAN (also called the Protected Ports feature) helps to isolate traffic among the same VLAN ports. A protected port cannot forward any traffic to another protected port on the switch even if they are in the same VLAN.

Switch ports can be configured to operate in one of the following three modes.

3.14.1 Unprotected Port
By default all the ports in the switch are unprotected ports. Unprotected ports can send and receive traffic with all the other ports including other unprotected, protected and community ports based on the VLAN membership.

3.14.2 Protected Port
Protected ports can send and receive traffic only with unprotected ports in the same VLAN. A protected port cannot send or receive traffic with other protected ports or community ports. Protected ports are also called isolated ports.

3.14.3 Community Port
Community ports can send and receive traffic with unprotected ports and other ports in the same community.

<table>
<thead>
<tr>
<th>Port Mode</th>
<th>Communicates with</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unprotected Ports</td>
<td>Unprotected Ports</td>
</tr>
<tr>
<td></td>
<td>Protected Ports</td>
</tr>
<tr>
<td></td>
<td>Community Ports</td>
</tr>
<tr>
<td>Protected Ports</td>
<td>Unprotected Ports</td>
</tr>
<tr>
<td>Community Ports</td>
<td>Unprotected Ports</td>
</tr>
<tr>
<td></td>
<td>Other ports in the same community</td>
</tr>
</tbody>
</table>
3.15 Unprotected Ports Configuration
By default, all ports are unprotected ports. A protected port or community port can be configured as unprotected port with the below CLI command in interface configuration mode.

```plaintext
noswitchport protected
```

There is no limit on the number of unprotected ports that can be supported by the switch.

3.16 Protected Ports Configuration
Any port can be configured as a protected port with the below CLI command in interface configuration mode.

```plaintext
switchport protected
```

This can be done in the web interface by changing the port mode to “Protected Port” on the Protected Ports web configuration page in port manager.

There is no limit on the number of protected ports that can be supported by the switch.

3.17 Community Ports Configuration
Any port can be configured as a community port with the below CLI command in interface configuration mode.

```plaintext
switchport protected group <group number>
```

This can be done in the web interface by changing the port mode to “Protected Port” and entering the group number on the Protected Ports web configuration page in port manager.

Use the same group number for all the ports in same community. Here, community is identified with the configured group number.

A maximum of 24 different communities can be configured in the switch.

**Note:**

This feature is not supported for port channel interface and port channel member ports.

3.17.1 Configuration Example 1
Configure all the 48 downlink Fx ports as isolated (or protected) ports. These 48 ports should not be able to communicate with each other. All these 48 ports should communicate only with the uplink ports cx 0/1 and cx 0/2.
The required configuration for this example is shown below. The uplink ports can be left with their default configuration as unprotected ports. All the downlink 25Gig ports need to be configured as protected ports.

```
SMIS# configure term
SMIS(config)# interface range fx 0/1-48
SMIS(config-if)# switchport protected
SMIS(config-if)# exit
```

### 3.17.2 Configuration Example 2
The Fx ports 1 to 24 should be able to communicate among themselves and also should be able to communicate with uplink ports Cx 0/1 and Cx 0/2.

The Fx ports 25 to 48 should be able to communicate among themselves and also should be able to communicate with uplink ports Cx 0/1 and Cx 0/2.

The ports 1 to 24 should not be able to communicate with the ports 25 to 48 and vice versa.

The required configuration for this example is given below. The uplink ports can be left with the default configuration as unprotected ports. The downlink ports 1 to 24 can be configured as one community (group) and ports 25 to 48 can be configured as another community (group).

```
SMIS# configure term
SMIS(config)# interface range fx 0/1-24
SMIS(config-if)# switchport protected group 1
SMIS(config-if)# exit
SMIS(config)# interface range fx 0/25-48
SMIS(config-if)# switchport protected group 2
SMIS(config-if)# exit
```
4 Link Aggregation

The Link Aggregation feature connects two or more physical links between two network devices without forming loops. Link aggregation can be used between switches, servers and routers.

Link aggregation provides the following advantages:

Increased bandwidth – User can connect up to eight physical links between devices to increase the link bandwidth. When 25 Gbps links are aggregated, users can get an aggregated link with up to 200 Gbps bandwidth. When ports are set to 10Gig speed, users can aggregate eight 10Gig ports to get an aggregated uplink with up to 80 Gbps.

Incremental bandwidth – Users can start aggregation with a fewer number of ports and then increase the number of ports in aggregation (up to eight) incrementally based on the bandwidth requirements.

Redundancy - When one of the physical links fails, traffic will be distributed over the other remaining links in the aggregation.

Figure LA-1: Link Aggregation

4.1 Link Aggregation Support
Supermicro switches support both static and dynamic link aggregations. Dynamic link aggregation support is based on the Link Aggregation Control Protocol (LACP).
Supermicro switches support only Layer 2 level link aggregation. Hence, only switching ports can be aggregated.

Supermicro switches do support the Multiple Chassis Link Aggregation (MLAG) feature.

4.2 Link Aggregation Numbers

Supermicro switches support up to 52 port channels.

Each port channel can have eight active links.

Users can configure more than eight ports to a LACP mode port channel. However, a maximum of eight ports only can be in an active bundle state in any port channel.

4.3 Link Aggregation Defaults

The Link Aggregation feature is enabled by default in Supermicro switches.

When a port channel interface is created, it will be added to VLAN 1 by default.

Port channels use the MAC address of the first physical link added to it.

The default LACP system priority is 32768.

The default LACP port priority is 128.

The default LACP timeout is long (30 seconds).

The default LACP wait time is 2 seconds.

4.4 Static Link Aggregation

Supermicro switches support static link aggregation.

User can add up to eight ports to a static port channel group. When the physical link status of one or more ports in a channel group is up, that port channel status will be up. The port channel status will be down when the ports physical link status of all members are down.

Switches do not exchange any port channel control information with other end devices in static link aggregation. Hence, users need to configure the port channel groups and member ports correctly on both end devices.

4.5 Dynamic Link Aggregation - LACP

Supermicro switches support dynamic link aggregation through IEEE 802.3ad Link Aggregation Control Protocol (LACP).
Users can add one or more ports to an LACP mode port channel. When more than eight member ports are configured, only the first eight member ports reaching the “bundle” state will be used for data traffic.

Ports in LACP mode exchange LACP packets with other end devices. The LACP system priority, switch MAC address, port LACP priority, port number and aggregation key are all exchanged between devices. Based on the exchanged information, both end devices agree on the status of the member ports. The member ports that successfully negotiated LACP parameters will be moved to the “bundle” state. The member ports that could not reach agreement on LACP parameters will stay in the “independent” state. Switches do not send traffic on member ports in “independent” state.

When one or more member ports reach the “bundle” state, the port channel status will be up. The port channel status will be down when all its member ports are either physically down or in the “independent” state.

Ports can be configured in either active or passive LACP mode. Ports in active LACP mode will initiate LACP negotiation by sending LACP messages to the other end devices. Ports in passive LACP mode will not initiate the LACP negotiation, but they will respond to LACP messages if received from other end.

Users should configure for an active LACP mode on at least one end of the LACP port channel connection. If LACP mode is configured as passive on both end devices, the port channel interface will not come up. Configuring LACP mode as active on both the end devices is allowed.

![Figure LA-2: Dynamic Link Aggregation](image)

The figure above shows an example of a port channel configuration with port status and aggregated ports. In this example, port 5 is not configured on LACP mode on switch B, and is therefore shown as being in the “independent” state and not part of the aggregated ports.
4.6 Link Aggregation Port Channel

4.6.1 Creating Port Channels
Port channel creation involves two steps: the first is to create the port channel interfaces and the second is to add member ports to the port channel interfaces.

4.6.1.1 Creating Port Channel Interfaces
Follow the steps below to create port channel interfaces in Supermicro switches.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface port-channel <code>&lt;channel-group-number&gt;</code>&lt;br&gt;Or&lt;br&gt;no interface range port-channel <code>&lt;channel-group-number&gt;</code></td>
<td>Creates a port channel using “interface port—channel” command. <code>&lt;channel-group-number&gt;</code> — may be any number from 1 to 65535. To configure multiple port channel interfaces, use the “interface range …” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range po 1-3&lt;br&gt;To provide multiple interfaces or ranges, separate with a comma (,). E.g. : int range po 1, 2</td>
</tr>
<tr>
<td>Step 3</td>
<td>description <code>&lt;string&gt;</code></td>
<td>Optional step - adds any name string to the port channel interfaces using the description command. The <code>&lt;string&gt;</code> may be up to 64 characters</td>
</tr>
</tbody>
</table>
The port channel description strings will not affect the member ports description strings configurations.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>mtu <code>&lt;framesize&gt;</code></th>
<th>Optional step. Configures the MTU for the port channel interfaces. <em>framesize</em> may be any number from Port channel MTU will be used on its all member ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>VLAN Configurations</td>
<td>Optional step – configures the VLAN parameters for port channel interfaces. Refer to the VLAN configuration guide for all VLAN configuration details.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Spanning Tree Configurations</td>
<td>Optional step – configures the spanning tree parameters for port channel interfaces. Refer to the spanning Tree configuration guide for all spanning tree configuration details.</td>
</tr>
<tr>
<td>Step 7</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>show interface port-channel &lt;channel-group-number&gt;</code></td>
<td>Displays the configured port channel information.</td>
</tr>
</tbody>
</table>
Show etherchannel 

```
show etherchannel ([channel-group-number] 

detail | load-balance | port | port 

t-channel | summary | protocol])
```

### Step 9

write startup-config

Optional step – saves this port channel configuration to be part of startup configuration.

---

### 4.6.1.2 Adding Member Ports to Port Channels

Users can add up to eight member ports to static port channels. For LACP port channels, users can add more than eight ports, but only the first eight member ports reaching a bundle state will be part of the port channel for data transfer.

Only ports of same speed can be added to port channel interfaces.

Follow the steps below to add member ports to port channel interfaces.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface range <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-type – may be any of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fx-ethernet – fx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cx-ethernet – cx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range,</td>
<td></td>
</tr>
</tbody>
</table>
use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20

| Step 3 | channel-group `<channel-group-number>` mode {active | passive | on} | Configures the interfaces as member ports for the given port channel. 

*channel-group-number* – The port channel to which these member ports are added.

For LACP aggregation, use the active or passive mode.

For static link aggregation, use mode on. |

| Step 4 | End | Exits the interface configuration mode. |

| Step 5 | show interface port-channel `<channel-group-number>`

show etherchannel `[<channel-group-number>] { detail | load-balance | port | por t-channel | summary | protocol}]` | Displays the configured port channel information. |

| Step 6 | write startup-config | Optional step – saves this port channel configuration to be part of startup configuration. |
The MTU, VLAN and spanning tree parameters of a port channel interface will be used on its member ports. After adding a port to any port channel, users should not configure MTU, VLAN and spanning tree parameters on that port. Instead users should configure MTU, VLAN and spanning tree parameters on the port channel interfaces.

The examples below show various ways to create port channels.

Create an LACP port channel with member ports cx 0/1 and cx 0/2.

```
SMIS# configure terminal
SMIS(config)# interface port-channel 10
SMIS(config-if)# exit
SMIS(config)# int range cx 0/1-2
SMIS(config-if)# channel-group 10 mode active
SMIS(config-if)# end
```

Create a static port channel having MTU 9000 with member ports cx 0/1 and cx 0/2. Also configure this port channel as a trunk interface to carry all the VLANs configured in the switch.

```
SMIS# configure terminal
SMIS(config)# interface port-channel 10
SMIS(config-if)# mtu 9000
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit
SMIS(config)# int range cx 0/1-2
SMIS(config-if)# channel-group 10 mode on
SMIS(config-if)# end
```

4.6.2 Modifying Port Channels

4.6.2.1 Modifying Port Channel Parameters

After a port channel is created, users can modify the port channel configuration for description, MTU, VLAN, and spanning tree parameters. Users should not modify these parameters on port channel member ports directly. Instead, these parameters should be configured on port channel interfaces.

To modify port channel parameters, follow the same steps used to create the port channels as explained in the Creating Port Channel Interfaces section.

The example below shows the steps to modify the parameters of a port channel interface.

Modify port channel 10 as a trunk interface to allow VLANs 100 to 200 with a native VLAN 100.

```
SMIS# configure terminal
SMIS(config)# interface port-channel 10
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan 100-200
SMIS(config-if)# switchport trunk native vlan 100
SMIS(config-if)# exit
```
4.6.2.2 Modifying Port Channel Member Ports

Users can add or remove member ports to the existing port channels. Users can also modify the port modes for member ports.

4.6.2.3 Adding New Member Ports

To add new member ports to an existing port channel, follow the same steps explained in the Adding Member Ports to Port Channels section.

The example below shows the steps necessary to add a new member port to an existing port channel interface.

Add port fx 0/3 to static port channel interface 10.

SMIS# configure terminal
SMIS(config)# int fx 0/3
SMIS(config-if)# channel-group 10 mode on
SMIS(config-if)# exit

4.6.2.4 Removing Member Ports

Follow the steps below to remove member ports from the port channel interfaces.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; Or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the following:

- fx-ethernet – fx
- cx-ethernet – cx

interface-id is in slot/port format for all physical interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface.
numbers.  
E.g.: int range fx 0/1-10  
To provide multiple interfaces or  
ranges, separate with a comma (,).  
E.g.: int range fx 0/1-10, fx 0/20

<table>
<thead>
<tr>
<th>Step 3</th>
<th>no channel-group</th>
<th>Removes the member ports from the port channel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 5 | show interface port-channel `<channel-group-number>`  
show etherchannel [[`channel-group-number`] {  
detail | load-balance | port | port-channel | summary  
|protocol }] | Displays the configured port channel information. |
| Step 6 | write startup-config | Optional step – saves this port channel configuration to be part of startup configuration |

When a port is removed from a port channel, that port will automatically be added to VLAN 1. The MTU and spanning tree configurations of that port will not be automatically changed to the default configurations. After removing any port from a port channel, users must verify and change the port VLAN, MTU and spanning tree configurations as needed.

The example below shows the steps necessary to remove a member port from a port channel interface.

Remove port cx 0/3 from port channel interface 10

```
SMIS# configure terminal  
SMIS(config)# int cx 0/3  
SMIS(config-if)# no channel-group  
SMIS(config-if)# exit
```

To modify the port channel mode (active/passive/on) for any member port, users should first remove the
port from the port channel using the “no channel-group” command. After removing the port from the port channel interface, the channel-group command can be configured with the required port mode.

<table>
<thead>
<tr>
<th>Step</th>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface mode. Interface-type - may be any of the following: fx-ethernet – fx cx-ethernet – cx Interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the &quot;interface range...&quot; command. To provide a range, use a hyphen(-) between the start and end interface numbers. E.g.: int range fx0/1-10 To provide multiple interfaces or ranges, separate with a comma(,). E.g.: int range fx 0/1-10, fx 0/1-20</td>
</tr>
<tr>
<td>Step 3</td>
<td>no channel-group</td>
<td>Removes the member ports from the port channel.</td>
</tr>
<tr>
<td>Step 4</td>
<td>channel-group <code>&lt;channel-group-number&gt;</code> mode {active</td>
<td>passive</td>
</tr>
</tbody>
</table>
The example below shows the steps necessary to modify the member ports modes of a port channel interface.

Modify the member ports’ modes to “active” for ports cx 0/2 and cx 0/3.

SMIS# configure terminal
SMIS(config)# int range cx 0/2-3
SMIS(config-if)# no channel-group
SMIS(config-if)# channel-group 10 mode active
SMIS(config-if)# exit

4.6.3 Removing Port Channels

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no interface port-channel &lt;channel-group-number&gt;</td>
<td>Removes the port channel interface.</td>
</tr>
</tbody>
</table>

channel-group-number – may be any

channel-group-number – The port channel to which these member ports are added.

Step 5: End
Exits the interface configuration mode.

Step 6: show interface port-channel <channel-group-number>
Displays the configured port channel information.

show etherchannel [(channel-group-number) { detail | load-balance | port | port-channel | summary | protocol}]

Step 7: write startup-config
Optional step – saves this port channel configuration to be part of startup configuration.
To remove multiple port channel interfaces, use the “no interface range …” command. To provide a range, use a hyphen (-) between the start and end interface numbers.

E.g.: no int range po 1-3

To provide multiple interfaces or ranges, separate with a comma (,).

E.g.: no int range po 1, 2

| Step 3 | show running-config | Displays the port channel information. |
|        | show etherchannel    |

| Step 4 | write startup-config | Optional step – saves this port channel configuration to be part of startup configuration. |

When a port channel is removed, all its member ports will be automatically added to VLAN 1. The MTU and spanning tree configurations of that port will not automatically be changed to their default configurations.

The example below shows the necessary steps to remove a port channel interface.

Remove port channel 10 and add all its member ports to VLAN 10 as access ports.

```
SMIS# configure terminal
SMIS(config)# no int port-channel 10
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
```
4.6.4 LACP Parameters

Users can configure the following LACP parameters on Supermicro switches.

- LACP System
- Priority LACP
- Port Priority
- LACP
- Timeout

4.6.4.1 LACP System Priority

Every LACP device needs to have a globally unique system identifier. This globally unique system identifier is formed by combining a switch’s MAC address and LACP system priority.

LACP system priority is also used to decide the active member ports of a port channel. When more than eight member ports are configured, the switch that has the lowest system priority value decides the active member ports. If both end devices have the same LACP system priority, the device with the numerically lower MAC address will get to decide the active member ports.

The default LACP system priority value is 32768.

Follow the steps below to modify the LACP system priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2| lACP system-priority <system-priority> | Configures the LACP system priority.  
  system-priority – may be any value  
  from 0 to 65535  |
| Step 3| Exit                            | Exits the configuration mode.                  |
| Step 4| show running-config             | Displays the configured LACP system priority value. |
| Step 5| write startup-config            | Optional step – saves this LACP configuration to be part of startup configuration. |
The “no lacp system-priority” command resets the LACP system priority to the default value 32768.

The example below shows the steps necessary to configure the LACP system priority value.

Set the LACP system priority as 1000.
SMIS# configure terminal
SMIS(config)# lacp system-priority 1000
SMIS(config-if)# exit

4.6.4.2 LACP Port Priority
If a LACP is configured with more than eight member ports then, switch selects the first eight ports that have the lowest port priority value as active member ports. If multiple ports have the same port priority value then, switch selects the first eight ports that have the numerically lower port ID as the active member ports.

The default LACP port priority is 128.

Follow the steps below to modify the LACP port priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; Or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the following:
- fx-ethernet – fx
- cx-ethernet – cx

interface-id is in slot/port format for all physical interfaces.
To configure multiple interfaces, use
the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.
E.g.: int range fx 0/1-10
To provide multiple interfaces or ranges, separate with a comma (,).
E.g.: int range fx 0/1-10, fx 0/20

<table>
<thead>
<tr>
<th>Step 3</th>
<th>lacp port-priority &lt;port-priority&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configures the LACP port priority.</td>
</tr>
<tr>
<td></td>
<td>port-priority – may be any value from 0 to 65535</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>show running-config</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show etherchannel</td>
</tr>
<tr>
<td></td>
<td>Displays the configured port priority information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>write startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Optional step – saves this port priority configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no lacp port-priority” command resets the LACP port priority to the default value of 128.

The example below shows the steps necessary to configure the port priority.
Configure the port priority as 10 for cx 0/1 and 20 for cx 0/2.
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# lacp port-priority 10
SMIS(config-if)# exit
SMIS(config)# interface cx 0/2
SMIS(config-if)# lacp port-priority 20
SMIS(config-if)# exit

### 4.6.4.3 LACP Timeout

Every LACP member port sends LACP messages periodically. The time period between LACP messages is configurable using the “lacp timeout” command.

Users can define the LACP timeout value either as “long” or “short”. Every member port can have a different LACP timeout selection. Also, the LACP timeout selection does not need to match on both end devices. An LACP port with a “long” timeout can be connected to a port which has a “short” timeout.

When the “long” timeout value is chosen, LACP messages are expected to be received once every 30 seconds. When the “short” timeout value is chosen, LACP messages are expected to be received once every second.

The default LACP timeout is “long”.

Follow the steps below to modify the LACP timeout value.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;&lt;interface-id&gt;</code> OR interface range <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface mode.</td>
</tr>
</tbody>
</table>

*interface-type* – may be any of the following:

- fx-ethernet – fx
- cx-ethernet – cx

*interface-id* is in slot/port format for all...
| Step 3 | lACP timeout (long | short) |
|--------|-------------------|

Physical interfaces.

To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hyphen (-) between the start and end interface numbers.

E.g.: int range fx 0/1-10

To provide multiple interfaces or ranges, separate with a comma (,).

E.g.: int range fx 0/1-10, fx 0/20

Configures the LACP port timeout.

Step 4 | End |
|--------|-----|

Exits the configuration mode.

Step 5 | show running-config |
|--------|---------------------|

Displays the configured port priority information.

show etherchannel

Step 6 | write startup-config |
|--------|----------------------|

Optional step – saves this port timeout configuration to be part of startup configuration.
The “no lacp timeout” command resets the LACP timeout to the default value of “long”.

The example below shows the steps necessary to configure the LACP timeout.

Configure the LACP timeout as short for ports cx 0/1 and cx 0/2.

SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# lacp timeout short
SMIS(config-if)# exit

4.6.4.4  LACP Wait Time
Switch waits for the “LACP wait time” period before adding any member port to aggregation. The default LACP wait time period is two seconds.

Users can choose any time interval from 0 to 10 seconds as the LACP wait time. The LACP wait time is port specific and users can configure different LACP wait times on different member ports.

Follow the steps below to modify the LACP wait time

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; Or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td></td>
<td>....</td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
The “no lacp wait-time” command resets the LACP wait time to the default value of “2”.

The example below shows the necessary steps to configure the LACP wait time.

Configure the LACP wait time as 0 for ports cx 0/1 and cx 0/2.

SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# lacp wait-time 0
SMIS(config-if)# exit

4.6.5 Load Balancing

Supermicro switches support load balancing on aggregated links.

Switches distribute outgoing traffic on all member ports that are in a bundle state. The distribution decision to transmit a packet on any particular member port is decided by a hash algorithm. Supermicro switches support the following hash algorithms:

- Packets will be distributed across the member ports based on the source MAC address of the packet.
  - Destination MAC Based
    - Packets will be distributed across the member ports based on the source and destination MAC addresses of the packet.
    - source based IP
      - Packets will be distributed across the member ports based on the source IP address of the packet.
### Destination based IP

- Packets will be distributed across the member ports based on the destination IP address of the packet.

### Source and Destination IP Based

- Packets will be distributed across the member ports based on the source and destination IP addresses of the packet.
- The hash algorithm provides the best distribution when the traffic has multiple streams. Users need to choose the right hash algorithm based on their common traffic scenarios.
- The load balance algorithm selection can be configured for individual port channel interfaces or it can be configured globally for all port channel interfaces. The load balancing algorithm on both ends of a port channel need not be the same.

The default load balancing algorithm is “Source and Destination MAC Based”.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>port-channel load-balance {src-mac</td>
<td>dest-mac</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
<td>Displays the configured load balancing information.</td>
</tr>
</tbody>
</table>
Follow the below steps to configure the load balancing algorithm.

The “no port-channel load-balance” command resets the load balancing algorithm to the default value of “src-dest-mac”.

The example below shows the steps necessary to configure the port channel load balancing algorithm. Configure the load balancing algorithm based upon source and destination IP addresses.

SMIS# configure terminal
SMIS(config)# port-channel load-balance src-dest-ip
SMIS(config-if)# exit

The link aggregation feature is enabled by default in Supermicro switches. Users can disable link aggregation if needed.

Follow the steps below to disable the link aggregation feature.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>set port-channel disable</td>
<td>Disables the link aggregation feature.</td>
</tr>
<tr>
<td>3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>show etherchannel</td>
<td>Displays link aggregation feature status.</td>
</tr>
<tr>
<td>5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

To enable the link aggregation feature, follow the steps below.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>set port-channel enable</td>
<td>Enables the link aggregation feature.</td>
</tr>
<tr>
<td>3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>show etherchannel</td>
<td>Displays link aggregation feature status.</td>
</tr>
<tr>
<td>5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

4.6.6 Link Aggregation Configuration Example

Configure switch A as shown below in Figure LA-3.

1. Aggregate ports Cx 0/3 and Cx 0/4 with LACP mode. Also configure this aggregation as a trunk interface with native VLAN 20.
2. Aggregate ports Cx 0/1 and Cx 0/2 with LACP mode. Configure this aggregation as an access port on VLAN 10.
3. Aggregate ports Fx 0/20 and Fx 0/21 statically.

```
SMIS# configure terminal

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

# Create the port channel 2 interface
SMIS(config)# int port-channel 2
SMIS(config-if)# exit

# Add member ports to the port channel 2 interface
SMIS(config)# int range fx 0/20-21
SMIS(config-if)# channel-group 2 mode on
SMIS(config-if)# exit

# Create the port channel 3 interface
SMIS(config)# int port-channel 3
```
SMIS(config-if)# exit

# Add member ports to the port channel 3 interface
SMIS(config)# int range cx 0/1-2
SMIS(config-if)# channel-group 3 mode active
SMIS(config-if)# exit

# Configure the VLAN requirements for the port channel 3 interface
SMIS(config)# int port-channel 3
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# end

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

Building configuration...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>ID</th>
<th>Hardware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SSE-1.0.0.0</td>
<td>0</td>
<td>SSE-F3548</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSE-F3548</td>
<td>F3548</td>
<td>1.0.0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.0.0.0</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

ip address dhcp interface port-channel 1 exit
interface port-channel 2 exit
interface port-channel 3 exit
vlan 1

ports fx 0/1-19 untagged ports fx 0/22-48 untagged ports po 2 untagged
exit vlan 10
ports po 3 untagged exit
vlan 20
ports po 1 untagged exit

interface Fx 0/20 channel-group 2 mode on
interface Fx 0/21 channel-group 2 mode on
interface Cx 0/1 channel-group 3 mode active
interface Cx 0/2 channel-group 3 mode active
interface Cx 0/3 channel-group 1 mode active
interface Cx 0/4 channel-group 1 mode active
interface po 1
switchport trunk native vlan 20
switchport mode trunk
interface po 3
switchport access vlan 10
switchport mode access
exit

SMIS#
# Check the port channels using the “show etherchannel” command
SMIS# show etherchannel detail
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:30:48:a1:11:01
LACP System Priority: 32768
Channel Group Listing
---------------------
Group: 1
Protocol: LACP
Ports in the Group
---------------------
Port: Cx0/3
-----------
Port State = Down, Not in Bundle
Channel Group: 1
Mode: Active
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Active
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted
Port: Cx0/4
-----------
Port State = Down, Not in Bundle
Channel Group: 1
Mode: Active
Pseudo port-channel = Po1
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Active
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted

LACP Port Admin Oper Port Port Port State Priority Key Key Number State
---------------------------------------------------------------------
Port-channel: Po1

Number of Ports = 2 HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse Protocol = LACP
Default Port = None
Channel Group Listing

Group: 2

Protocol: Manual
Ports in the Group

Port: Fx0/20

Port State = Down, Not in Bundle
Channel Group: 2
Mode: On
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Passive
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted

Port: Fx0/21

Port State = Down, Not in Bundle
Channel Group: 2
Mode: On
Pseudo port-channel = Po2
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Passive
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted

LACP Port Admin Oper Port Port State Priority Key Key Number State

Fx0/20 Down 128 2 2 0x14 0x44
Fx0/21 Down 128 2 2 0x15 0x44
Port-channel: Po2

Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = Manual
Default Port = None
Channel Group Listing
Group: 3
--------
Protocol: LACP
Ports in the Group
--------
Port: Fx0/1
--------
Port State = Down, Not in Bundle
Channel Group: 3
Mode: Active
Pseudo port-channel = Po3
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Active
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted
Port: Fx0/2
--------
Port State = Down, Not in Bundle
Channel Group: 3
Mode: Active
Pseudo port-channel = Po3
LACP port-priority = 128
LACP Wait-time = 2 secs
LACP Activity: Active
LACP Timeout: Long
Aggregation State: Aggregation, Defaulted

LACP Port Admin Oper Port State Priority Key Key Number State
---------------------------------------
Fx0/1  Down  128  3  3  0x31  0x45
Fx0/2  Down  128  3  3  0x32  0x45
Port-channel: Po3
-----------
Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
Default Port = None
SMIS#
# Save this port channel configuration. SMIS# write startup-config
Building configuration, please wait. May take a few minutes . . .
[OK]
SMIS#
5 MLAG

5.1 Overview

Typically data centers provide redundancy by means of oversubscription by connecting switches and servers to dual aggregation switches. In such cases, Spanning Tree Protocol (STP) prevents network loops by blocking half of the links to the aggregation switches. However this reduces the available bandwidth by 50%.

The Multi-Chassis Link Aggregation (MLAG) feature allows users to logically aggregate ports across two switches. This provides increased bandwidth and redundancy.

There can be multiple MLAG interfaces between two switches. The maximum number of MLAG interfaces is limited by the maximum number of LAGs supported in the switch models. Similar to the LAG, MLAG also supports up to eight member ports.

The two switches that logically aggregate are called MLAG peer switches and communicate through an interface called an Inter peer link (IPL). The IPL is primarily used to exchange MLAG control information between peer switches, however it also carries data traffic for devices that are attached to only one of the MLAG peers.

5.1.1 Terminologies

5.1.1.1 IPL - Inter Peer Link

The link connecting two MLAG peer switches is referred as an Inter Peer Link (IPL).

This link should be configured as a LACP port channel. It can have many member ports as supported by the switch model.

5.1.1.2 Peer Switch

The two switches that form a single logical port channel interface is referred to as peer switches. The peer switches are connected through the IPL interface. For example, in the topology diagrams shown in the "Topologies" section, the switches “Switch A” and “Switch B” are peer switches.

5.1.1.3 MLAG Port Channel

The link connecting MLAG peers to MLAG partner switches is called an MLAG port channel. MLAG port channel interfaces should be created on peer switches with the same port channel number.

5.1.1.4 Partner Device

The device connected to both the peer switches using a LACP aggregation link is referred as partner device. For example, in the topology diagrams shown in “Topologies” section, the switch “Switch C” and “Servers” are partner devices for MLAG switches.
5.1.1.5  Single Homed Device

A single homed device is a device connected to only one peer switch. This connection could be a regular single physical link connection or a connection through a port channel interface.
5.2 Topologies

5.2.1 Topology 1 - Server to Switch MLAG Topology

In Figure MLAG-1, Switch A and Switch B are peer switches in the MLAG. Switches A and B are connected through an IPL port channel interface.

The server is connected to both MLAG peer switches either through regular bonding or by a teaming LACP interface on the server side.

On the switch side, the ports connected to the server are configured with the same MLAG enabled port channel number.
5.2.2 Topology 2 - Switch to Switch MLAG Topology

In Figure MLAG-2, Switch A and Switch B are peer switches in the MLAG. Switches A and B are connected through an IPL port channel interface.

Switch C is connected to both MLAG peer switches through a regular LACP port channel interface.

On the Switch A and Switch B sides, the ports connected to Switch C are configured with the same MLAG enabled port channel number.
5.2.3 Topology 3 - Single Uplink Switch Topology

In Figure MLAG-3, Switch A and Switch B are peer switches in the MLAG. Switches A and B are connected through an IPL port channel interface.

The server is connected to both MLAG peer switches through a regular LACP port channel interface.

Uplink Switch 1 is connected to MLAG peer switches Switch A and Switch B through a regular LACP port channel interface.

On the Switch A and Switch B sides, the ports connected to the server are configured with the same MLAG enabled port channel number. Similarly, the ports connected to Uplink Switch 1 are configured with the same MLAG port channel number.

The reason for LAG in the uplink switch is to make sure the uplink switch does not send the same packet (broadcast or multicast) to both MLAG peer switches.
5.2.4 Topology 4 – Redundant Uplink Switch Topology

In Figure MLAG-4, Switch A and Switch B are peer switches in the MLAG. Switches A and B are connected through an IPL port channel interface.

The server is connected to both the MLAG peer switches through regular LACP port channel interface.

Uplink Switch 1 and Uplink Switch 2 are connected to MLAG peer switches Switch A and Switch B through the MLAG port channel interface.

On the Switch A and Switch B sides, the ports connected to the server are configured with the same MLAG enabled port channel number. Similarly, the ports connected to Uplink Switch 1 and Uplink Switch 2 are configured with the same MLAG port channel number.

The reason for MLAG in the uplink switches is to make sure the uplink switch does not send the same packet (broadcast or multicast) to both the MLAG peer switches.
5.2.5 Topology 5 - Server to switch Layer 3 MLAG topology

In Figure MLAG-5 Switches A and B are peer switches in the MLAG. Switches A and B are connected through an IPL port channel interface.

The servers are connected to both of the MLAG peer switches through a regular bonding or teaming LACP interface on the server side. The servers are configured with IP addresses in the L3 VLANs network (configured in MLAG peer switches). The VRRP virtual IP addresses configured in the MLAG peer switches are used as gateway IP addresses in the servers.

On the switch side the ports connected to server are configured with the same MLAG enabled port channel number. Layer 3 VLANs with required IP subnets are configured in the MLAG peer switches. VRRP is configured between the MLAG peer switches.
5.3 Default Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ID</td>
<td>None</td>
</tr>
<tr>
<td>System priority</td>
<td>32768</td>
</tr>
<tr>
<td>Keep alive time</td>
<td>3 seconds</td>
</tr>
<tr>
<td>IPL interface</td>
<td>None</td>
</tr>
<tr>
<td>MLAG status</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

5.4 MLAG Configurations

The mandatory configurations for an MLAG are:
1) System ID
2) Priority
3) IPL port channel interface
4) Enabling MLAG on port channel interfaces

The keep alive time configuration is optional.

5.4.1 MLAG System ID

The MLAG system ID is a text string configured as a unique MAC address. MLAG switches use this MLAG system ID to identify their peers.

The MLAG system ID must be configured the same in both peer switches. If this condition is not met, the peer connection will not be established. All the MLAG links (connected to different partner devices) in the switch will use this globally configured MLAG system ID.

The LACP globally unique system identifier is formed by combining the MLAG system ID and the MLAG system priority.

Follow the steps below to configure the MLAG System ID.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mlag system-identifier <a href="">aa:aa:aa:aa:aa:aa</a></td>
<td>Configure the system ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="">aa:aa:aa:aa:aa:aa</a> - Specify any unicast MAC address to be used as the MLAG system ID</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mlag detail</td>
<td>Displays the MLAG configuration details</td>
</tr>
</tbody>
</table>
The “no mlag system-identifier” command deletes the MLAG system ID.

When the MLAG system ID is deleted, both IPL and MLAG port channel connected to partner devices will go DOWN.

swA#configure terminal
swA(config)# mlag system-identifier 00:01:02:03:04:05
swA#end

swA# show mlag detail
System Identifier: 00:01:02:03:04:05
System Priority: 32768
Keep Alive Time: 90
IPL Interface: po1
Peer System Identifier: 00:01:02:03:04:05
IPL Link Status: Up
Peer Connection State: ESTABLISHED
MLAG Role: PRIMARY

5.4.2 MLAG System Priority
MLAG switches use this MLAG system priority for LACP exchanges with partner devices.

MLAG system priority must be configured the same in both peer switches. If this condition is not met, the peer connection will not be established. All the MLAG links (connected to different partner devices) in the switch will use this globally configured MLAG system priority.

The LACP globally unique system identifier is formed by combining the MLAG system ID and the MLAG system priority.

Follow the steps below to configure the MLAG system priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mlag system-priority &lt;0-65535&gt;</td>
<td>Configure the MLAG system priority</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mlag detail</td>
<td>Displays the MLAG configuration details</td>
</tr>
</tbody>
</table>

The “no mlag system-priority” command deletes the MLAG system priority.

When the MLAG system priority is deleted, both the IPL and the MLAG port channel connected to partner devices will go DOWN.
swA#configure terminal
swA(config)# mlag system-priority 1024
swA#end

swA# show mlag detail
System Identifier: 00:01:02:03:04:05
System Priority: 1024
Keep Alive Time: 90
IPL Interface: po1
Peer System Identifier: 00:01:02:03:04:05
IPL Link Status: Up
Peer Connection State: ESTABLISHED
MLAG Role: PRIMARY

5.4.3 Keep Alive Time
MLAG peer switches periodically transmit keep alive packets to maintain the relationship between peer switches. The value of the keep alive transmit timer is user configurable.

The keep alive mechanism identifies one of the peer switches as the primary and another as the secondary switch based on the switch system MAC address. The switch with the lower MAC address will be the primary switch.

Follow the steps below to configure MLAG Keep alive time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mlag keepalive-time &lt;3-90&gt;</td>
<td>Configure the MLAG keepalive time.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mlag detail</td>
<td>Displays the MLAG configuration details</td>
</tr>
</tbody>
</table>

The “no mlag keepalive-time” command resets the keep alive time to its default value.

Keep alive time can be different on both peers.

swA#configure terminal
swA(config)# mlag keepalive-time 30
swA#end

swA# show mlag detail
System Identifier: 00:01:02:03:04:05
System Priority: 32768
Keep Alive Time: 30
IPL Interface: po1
Peer System Identifier: 00:01:02:03:04:05
IPL Link Status: Up
Peer Connection State: ESTABLISHED
MLAG Role: PRIMARY
5.4.4 IPL Interface
The link connecting between two MLAG peer switches is referred as the Inter Peer Link (IPL). This link should be configured as an LACP port channel. It can have as many member ports as supported by the switch model.

Only the primary switch among the peers participates in spanning tree protocol.

Follow the steps below to configure the IPL interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mlag interface port-channel &lt;port-channel-id (1-65535)&gt;</td>
<td>Configure the IPL interface used to establish the connection between the peers. Note: The given port channel should exist as a LACP port channel prior to this IPL interface configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mlag detail</td>
<td>Displays the MLAG configuration details</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mlag stp</td>
<td>Displays the MLAG Spanning Tree details</td>
</tr>
</tbody>
</table>

The “no mlag interface” command deletes the IPL interface.

The IPL interface cannot be deleted when IPL is in the established state.

swA#configure terminal
swA(config)# mlag interface port-channel 2
swA#end

swA# show mlag detail
System Identifier: 00:01:02:03:04:05
System Priority: 32768
Keep Alive Time: 90
IPL Interface: po2
Peer System Identifier: 00:01:02:03:04:05
IPL Link Status: Up
Peer Connection State: ESTABLISHED
MLAG Role: PRIMARY

5.4.5 MLAG Port Channels
As the link connecting MLAG peers to MLAG partner switches, the MLAG port channel interfaces should be created on both peer switches with the same port channel number.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface port-channel &lt;channel-group-number&gt;</td>
<td>Creates a port channel using “interface port-channel” command. ( channel-group-number ) – may be any number from 1 to 65535.</td>
</tr>
<tr>
<td>Step 3</td>
<td>mlag enable</td>
<td>Configure MLAG link from switch to the partner devices.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mlag interface</td>
<td>Displays the details of MLAG interface between peers and partner devices.</td>
</tr>
</tbody>
</table>

The “mlag disable” command disables the MLAG link between the switch and the partner device.

swA#configure terminal
swA(config)# interface port-channel 1
swA(config-if)# mlag enable
swA#end

```
swA# show mlag interface

MLAGId Local Status Peer Status
------ ----------- -----------
Po 1   UP         UP
```

The “show interface port channel” command also shows the basic port channel details for MLAG port channels.

### 5.4.6 Other Configurations

MLAG peer switches exchange only the dynamic learned specific information. The configurations across peer switches are not exchanged. Hence, users need to make sure MLAG peer switches are configured correctly. The following configurations have to be similar across MLAG peer switches for correct functionality.

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN configurations for MLAG interfaces</td>
<td></td>
</tr>
<tr>
<td>Spanning tree configurations for MLAG interfaces</td>
<td></td>
</tr>
<tr>
<td>ACL configurations related to MLAG interfaces</td>
<td></td>
</tr>
<tr>
<td>QoS configurations related to MLAG interfaces</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--</td>
</tr>
<tr>
<td>MAC aging time</td>
<td></td>
</tr>
<tr>
<td>Static MAC entries</td>
<td></td>
</tr>
<tr>
<td>MTU on MLAG and IPL interfaces</td>
<td></td>
</tr>
</tbody>
</table>
6 Spanning Tree

Switches are interconnected to provide network access to a large number of end stations. In complex networks, it is possible to have multiple network paths between any two end devices. The multiple paths form network loops that lead to a flooding of packets by forwarding broadcast and multicast packets repeatedly over the looped connections. Flooding makes the network unusable until the looped connections are disconnected and the flooding stopped.

Spanning tree protocol helps to avoid flooding on network loops. Spanning tree protocols form a loop-free, tree structured logical network topology over physical network connections.

Spanning tree enabled switches exchange spanning tree protocol messages (BPDU) to form a loop-free topology. Based on the exchanged BPDU information, the spanning tree algorithm selects one of the switches on the network as the root switch for the tree topology. All other switches on the networks choose the best loop-free path to reach the root switch. The redundant paths to root switch are blocked to form a loop-free topology.

The spanning tree algorithm assigns one of the following roles to every port on the switch.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Port</td>
<td>• Port to reach the root switch with lowest path cost&lt;br&gt;• Root ports forwards the traffic</td>
</tr>
<tr>
<td>Designated Port</td>
<td>• Loop-free connection to other switches on the LAN&lt;br&gt;• Designated ports forward the traffic</td>
</tr>
<tr>
<td>Alternate Port</td>
<td>• Redundant path to the root switch&lt;br&gt;• Alternate ports do not forward the traffic</td>
</tr>
<tr>
<td>Blocked Port</td>
<td>• Redundant path to other switches on the LAN&lt;br&gt;• Blocked ports do not forward the traffic</td>
</tr>
</tbody>
</table>

When the network connections status changes, spanning tree recalculates the paths to form a loop-free topology. Spanning tree calculations are based on the following three key factors:

Bridge Identifier: Combination of switch MAC address and switch spanning tree priority

Path Cost: Spanning tree path cost to the root switch

Port Identifier: Combination of port number and port priority

When a switch boots up, it assumes its role as the root switch. It sends out spanning tree BPDUs with its bridge ID as the root bridge ID. When a switch receives spanning tree BPDUs, it compares the received BPDU information. If the received BPDU information is superior, the switch uses the received BPDU information to decide the root bridge and recalculates the spanning tree. If the received BPDU information is inferior, the switch ignores the received BPDU.

Spanning tree operates the switch ports in different states while calculating the loop-free topology. The BPDU exchange between switches takes a few seconds in large LANs. To avoid any temporary loops while
forming spanning tree topology, the switch ports are moved through different states to reach the forwarding state. Switch ports stay in one of the following spanning tree states:

- **Blocking**
  - Receives BPDUs
  - Discards packets
  - Does not learn MAC

- **Listening**
  - Receives BPDUs
  - Discards packets
  - Does not learn MAC

- **Learning**
  - Receives BPDUs
  - Discards packets
  - Learns MAC addresses

- **Forwarding**
  - Receives BPDUs
  - Forwards packets
  - Learns MAC addresses

- **Disabled**
  - Does not receive BPDUs
  - Discards packets
  - Does not learn MAC

Since spanning tree forms a logical loop-free topology, it helps to have physical loop connections on the network for redundancy purposes. When an active connection fails, spanning tree automatically enables the blocked redundant connection.

Rapid Spanning Tree Protocol (RSTP) provides faster topology convergence. Spanning tree (STP) takes more than 30 seconds to move a port to a forwarding state, but RSTP can move a port to the forwarding state within 3 times of the hello interval (default hello interval is 2 seconds). RSTP is compatible with STP.

Multiple Spanning Tree Protocol (MSTP) extends RSTP to provide separate spanning trees for different VLANs or VLAN groups. This helps to use alternate paths efficiently by blocking the ports only for the required VLANs. MSTP is compatible with RSTP.

### 6.1 Root Switch Election Procedure

Spanning tree protocol selects one switch as the root switch for every switched LAN. This root switch is used as the reference point to decide the spanning tree topology. Based on the connections to this root switch, the redundant links on the LAN are identified and blocked. Spanning tree runs an election process to elect one switch as the root switch.

Spanning tree selects the switch with the lowest bridge ID as the root switch. Every switch on the LAN has a bridge ID. The bridge ID has two components: the priority and the MAC address of the switch. The spanning tree priority occupies the most significant two bytes of the bridge ID. The default spanning tree priority is 32768.
When a switch starts spanning tree it sends out BPDUs with its bridge ID as the root bridge ID. When a switch receives the BPDUs, it compares the received root bridge ID with its own bridge ID. If the received root bridge ID is lower than its own bridge ID, the received switch accepts the other switch as the root switch. In case the received root bridge ID is higher than its own bridge ID, the received switch ignores the received BPDU and continues to act as the root switch.

If the priorities of all switches are same, the switch MAC addresses decide the lowest bridge ID and hence the switch with the lowest MAC address will be elected as the root switch.

### 6.2 Spanning Tree Support

Supermicro switches support STP, RSTP and MSTP protocols based on standards IEEE 802.1D 2004 and 802.1s.

### 6.3 Spanning Tree Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning tree global status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Spanning tree port status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Spanning tree mode</td>
<td>MST</td>
</tr>
<tr>
<td>Switch priority</td>
<td>32768</td>
</tr>
<tr>
<td>Port priority</td>
<td>128</td>
</tr>
<tr>
<td>Port cost</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Default Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>2000000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>200000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>20000</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2000</td>
</tr>
</tbody>
</table>

- Hello time: 2 seconds
- Forwarding time: 15 seconds
- Maximum aging time: 20 seconds
- Transmit hold count: 3
- Max hops: 20
- Path cost method: Long
- MST region name: Switch MAC address
- MST region revision: 0
- Spanning tree compatibility: In MSTP mode, the default compatibility is MSTP and in RSTP mode the default compatibility is RSTP
- Root guard: Disabled
- Topology change guard: Disabled
- Port fast: Disabled
- Auto edge: Enabled
| Link type | Full duplex ports – point to point links | Half duplex ports – shared LAN links |

### 6.4 Enabling/Disabling Spanning Tree

#### 6.4.1 Enable/Disable Spanning Tree Globally

Spanning tree is enabled by default in Supermicro switches globally.

Follow the steps below to disable the spanning tree globally.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no spanning-tree</td>
<td>Disables the spanning tree globally</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree</td>
<td>Displays the spanning tree information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “spanning-tree” command enables the spanning tree globally.

The examples below show ways to disable/enable the spanning tree function on Supermicro switches.

**Disable the spanning tree.**

SMIS# configure terminal

SMIS(config)# no spanning-tree

SMIS(config)# end

**Enable the spanning tree.**

SMIS# configure terminal

SMIS(config)# spanning-tree

SMIS(config)# end

#### 6.4.2 Enable/Disable Spanning Tree on Ports

Spanning tree is enabled by default on all the ports and port channels in Supermicro switches.
Follow the steps below to disable spanning tree on ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the &quot;interface range ...&quot; command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>To disable the spanning tree in RST mode: spanning-tree disable To disable the default MST instance spanning tree: spanning-tree disable To disable the particular MST instance spanning tree. spanning-tree mst&lt;instance-id&gt;disable</td>
<td>Disables the spanning tree on the port. instance-id – The MST instance identifier may be from 1 to 16.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree interface &lt;interface-type&gt;&lt;interface-id&gt; show running-config interface &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Displays the spanning tree port information.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no spanning-tree disable” command enables spanning tree on ports.

The examples below show various ways to disable/enable the spanning tree on ports.

Disable the spanning tree on ports cx 0/1 and cx 0/2.

```
SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# spanning-tree disable
SMIS(config)# end
```

Enable the spanning tree on port cx 0/1.

```
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# no spanning-tree disable
SMIS(config)# end
```

### 6.5 Configuring MST

Spanning tree is enabled by default in MST mode in Supermicro switches.

In case the switch was configured earlier in RST mode, follow the steps below to change to MST mode.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree mode mst</td>
<td>Configures the switch to operate in MST mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree</td>
<td>Displays the spanning tree mode information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

Changing the spanning tree mode will shut down the spanning tree currently running and restarts it in the new mode given.
### 6.6 Configuring MST Region and Instances

All the spanning tree switches in an MST region must have the same values configured for the following parameters.

- Region name
- Revision number
- Instance to VLAN mapping

Follow the steps below to configure the MST region parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree mst configuration</td>
<td>Enters the MST configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td>instance&lt;instance-id(1-16)&gt;vlan&lt;vlan-range&gt;</td>
<td>Creates a MST instance and maps it to the given VLAN range.</td>
</tr>
</tbody>
</table>

  - instance-id – The MST instance identifier may be from 1 to 16.
  - vlan-range – 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. User can configure VLANs with identifiers 1 to 4069.

| Step 4 | name<name-string> | Configures the MST region name. |

  - name-string – Alphanumeric case sensitive string with maximum length of 32 characters.
  - The default name is system MAC address.

| Step 5 | revision<revision-number> | Configures the MST region revision number. |

  - revision-number – The MST revision number may be from 0 to 65535.
  - The default revision-number is 0.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>end</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>show spanning-tree mst configuration</td>
<td>Displays the spanning tree MSTconfiguration parameters.</td>
</tr>
<tr>
<td>Step 8</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no name” command removes the configured MST region name.

The “no revision” command resets the configured MST region revision number to its default value of 0.

The examples below show various ways to configure MST region parameters.

Configure the MST region with name dc1_region, revision number 1 and map the VLANs 100 to 300 to MST instance 10.

SMIS# configure terminal
SMIS(config)# spanning-tree mst configuration
SMIS(config-mst)# name dc1_region
SMIS(config-mst)# revision 1
SMIS(config-mst)# instance 10 vlan 100-300
SMIS(config-mst)# end

Remove the VLANs 201 to 250 from MST instance 10.

SMIS# configure terminal
SMIS(config)# spanning-tree mst configuration
SMIS(config-mst)# noinstance 10 vlan 201-250
SMIS(config-mst)# end

Delete the MST instance 10.

SMIS# configure terminal
SMIS(config)# spanning-tree mst configuration
SMIS(config-mst)# noinstance 10
SMIS(config-mst)# end

### 6.7 Configuring RSTP

Spanning tree is enabled by default in MST mode in Supermicro switches.

Follow the steps below to change to RSTP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
Changing the spanning tree mode will shut down the spanning tree currently running and restart it in the new mode given.

### 6.8 Spanning Tree Compatibility

MSTP is backward compatible with RSTP and STP. Similarly, RSTP is backward compatible with STP.

When an MSTP operating switch detects an RSTP operating switch in any port, the MSTP switch will downgrade to RSTP operating mode on that port.

Similarly, when an MSTP or RSTP operating switch detects an STP operating switch in any port, the switch will downgrade to STP operating mode on that port.

Users can force the switch to operate in any particular compatibility mode. In user configured STP compatible mode, a switch will transmit and receive only STP BPDUs and will drop any received RSTP and MSTP BPDUs.

In MSTP mode the default compatibility is MSTP and in RSTP mode the default compatibility is RSTP.

Follow the steps below to configure the spanning tree compatibility.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To force the spanning tree compatibility as STP spanning-tree compatibility stp</td>
<td>Configures the spanning tree compatibility.</td>
</tr>
<tr>
<td></td>
<td>To force the spanning tree compatibility as RSTP spanning-tree compatibility rst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To force the spanning tree compatibility as MSTP spanning-tree compatibility mst</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree</td>
<td>Displays the spanning tree mode information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no spanning-tree compatibility” command resets the spanning tree compatibility mode to the default value.

The examples below show various ways to configure the spanning tree compatibility.

Configure the spanning tree compatibility as STP.

SMIS# configure terminal
SMIS(config)# spanning-tree compatibility stp
SMIS(config)# end

Configure the spanning tree compatibility as RSTP.

SMIS# configure terminal
SMIS(config)# spanning-tree compatibility rst
SMIS(config)# end

### 6.9 Configuring the Root Switch (or) Priority

The switch with the lowest priority value gets elected as the root switch. To make any particular switch the root switch, configure it with a lower numeric priority value. The default spanning tree priority is 32768.

When priorities of all switches are the same, the switch with the lowest MAC address gets elected as the root switch.

Follow the steps below to change spanning tree priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>Configures the switch spanning tree priority. priority-value – Spanning tree switch priority value in multiples of 4096 from 0 to 61440. In other words only the following priority values are valid.</td>
</tr>
<tr>
<td></td>
<td>To configure the switch priority in RST mode: spanning-tree priority &lt;priority-value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To configure the switch priority for the default MST instance 0: spanning-tree priority &lt;priority-value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To configure the switch priority for particular MST instance: spanning-tree mst &lt;instance-id&gt; priority &lt;priority-value&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default priority value is 32768.</td>
</tr>
</tbody>
</table>
The MST instance identifier may be from 1 to 16.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>show spanning-tree bridge priority</td>
<td>Displays the spanning tree configuration parameters including the switch priority values.</td>
</tr>
<tr>
<td></td>
<td>show spanning-tree</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree priority” command resets the spanning tree switch priority to the default value (32768). In MST mode, it resets the switch priority for the default MST instance 0.

The “no spanning-tree mst <instance-id>priority” command resets the spanning tree switch priority to the default value (32768) for the given MST instance.

The examples below show various ways to configure the spanning tree switch priority.

Configure the spanning tree switch priority as 4096 in RST mode.

SMIS# configure terminal

SMIS(config)# spanning-tree priority 4096

SMIS(config)# end

Configure the spanning tree switch priority as 4096 for the default MST instance 0.

SMIS# configure terminal

SMIS(config)# spanning-tree priority 4096

SMIS(config)# end

Configure the spanning tree switch priority as 4096 for the MST instance 10.

SMIS# configure terminal

SMIS(config)# spanning-tree mst 10 priority 4096

SMIS(config)# end

6.10 Port Priority

When spanning tree detects multiple paths to the root switch in a loop condition, it selects the port with the lowest path cost as the forwarding port.
In case of multiple ports having the same path cost to the root switch, spanning tree selects the port with the lowest numeric port priority value as the forwarding port.

When priorities of all the ports are the same, the port with the lowest port identifier gets selected as the forwarding port.

The port priority used in selection of the root port is the priority of the upstream switch port. Changing the port priority will affect the root port selection of the downstream switch connected to this port. It will not affect the root port selection of the switch on which the port priority is changed.

Follow the steps below to change the spanning tree port priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>To configure the port priority in RST mode: spanning-tree port-priority &lt;priority-value&gt;</td>
<td>Configures the port spanning tree priority. priority-value – Spanning tree port priority value may be from 0 to 240. Priority value must be multiple of 16. The default priority value is 128.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>--------</td>
<td>-----</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree interface &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Displays the spanning tree port parameters including the port priority values.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree port-priority” command resets the spanning tree port priority to the default value (128). In MST mode, it resets the port priority for the default MST instance 0.

The “no spanning-tree mst <instance-id>port-priority” command resets the spanning tree port priority to the default value (128) for the given MST instance.

The examples below show various ways to configure the spanning tree port priority.

Configure the spanning tree port priority as 208 in RST mode on ports fx 0/1 and fx 0/2.

```
SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# spanning-tree port-priority 208
SMIS(config-if)# end
```

Configure the spanning tree port priority as 112 for the default MST instance 0 on port fx 0/1.

```
SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# spanning-tree port-priority 112
SMIS(config-if)# end
```

Configure the spanning tree port priority as 64 for the MST instance 10 on port cx 0/1.

```
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# spanning-tree mst 10 port-priority 64
SMIS(config-if)# end
```
6.11 Path Cost

When spanning tree detects multiple paths to root switches in a loop condition, it selects the port with lowest path cost as the forwarding port. If multiple ports have the same path cost to the root switch, spanning tree selects the port with lowest numeric port priority value as the forwarding port.

The default path cost for the ports are calculated based on the port speed. The table below shows the default path costs for different speeds.

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Default Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>2000000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>200000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>20000</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2000</td>
</tr>
</tbody>
</table>

Follow the steps below to change the spanning tree path cost for ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>To configure the port priority in RST mode: spanning-tree cost&lt;cost-value&gt;</td>
<td>Configures the port spanning tree path cost. cost-value – Spanning tree port priority value may be from 1 to 200000000.</td>
</tr>
</tbody>
</table>
To configure the port priority for particular MST instance:
spanning-tree mst <instance-id>cost<cost-value>
The default path cost is calculated based on the port speed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>show spanning-tree interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Displays the spanning tree port parameters including the port path cost values.</td>
</tr>
<tr>
<td>6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “nospanning-tree cost” command resets the spanning tree port path cost to the default value. In MST mode, it resets the port path cost for the default MST instance 0.

The “no spanning-tree mst <instance-id>cost” command resets the spanning tree port path cost to the default value for the given MST instance.

The examples below show various ways to configure the spanning tree port path cost.

Configure the spanning tree port path cost as 200 in RST mode on ports cx 0/1 and cx 0/2.

SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# spanning-tree cost 200
SMIS(config-if)# end

Configure the spanning tree port priority as 200 for the default MST instance 0 on port fx 0/1

SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# spanning-tree cost 200
SMIS(config-if)# end

Configure the spanning tree port priority as 20 for the MST instance 10 on port cx 0/1

SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# spanning-tree mst 10 cost 20
SMIS(config-if)# end
6.12 Hello Time
The root switch sends the BPDU messages on every port periodically for every hello time interval.

The default hello time is 2 seconds.

If switches do not receive BPDU messages for a period of 3 hello time intervals, spanning tree protocol assumes the root switch has failed.

In MSTP, the hello time is configurable on individual ports. In RSTP, the hello time is configured commonly for all ports.

Follow the steps below to change the hello time for RSTP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure the hello time in RST mode: spanning-tree hello-time&lt;time-value&gt;</td>
<td>Configures the hello time interval. time-value – Hello time value may be 1 or 2 seconds. The default hello time is 2 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree interface &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Displays the spanning tree port parameters including the hello time values.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree hello-time” command resets the spanning tree port hello time to the default value of 2 seconds.

Follow the steps below to change the hello time for ports in MSTP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</td>
</tr>
</tbody>
</table>
interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.

To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers.

E.g.: int range fx 0/1-10
To provide multiple interfaces or ranges, use separate with a comma (,).
E.g.: int range fx 0/1-10, fx 0/20

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>To configure the hello time in MST mode:</td>
<td>Configures the hello time interval.</td>
</tr>
<tr>
<td></td>
<td>spanning-tree mst hello-time&lt;time-value&gt;</td>
<td>time-value – Hello time value may be 1 or 2 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default hello time is 2 seconds.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree bridge hello-time</td>
<td>Displays the spanning tree hello time.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree mst hello-time” command resets the spanning tree port hello time to the default value of 2 seconds.

The examples below show various ways to configure the spanning tree port hello time.

Configure the spanning tree port hello time as 1 second in RST mode.

SMIS# configure terminal
SMIS(config)# spanning-tree hello-time 1
SMIS(config)# end

Configure the MSTP hello time as 1 second for the port fx 0/1

SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# spanning-tree mst hello-time 1
6.13 Max Age

Switches maintain the BPDU information for every port for a period called the max age. If BPDU configuration messages are not received on any ports for the max age time, the switch will reconfigure those ports.

The max age time affects failure detection and reconfiguration. A smaller max age time will help detect failures quickly. It is advisable to choose a max age time based on the maximum number of switches on the network between any two hosts.

The default max age time is 20 seconds.

The max age value should be less than twice of (forward time – 1).

Follow the steps below to change the max age time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure the max age time: spanning-tree max-age&lt;age-value&gt;</td>
<td>Configures the switch spanning tree max age time. age-value – Spanning tree max age value may be from 6 to 40 seconds. The default max age is 20.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree bridge max-age show spanning-tree</td>
<td>Displays the spanning tree configuration parameters including the switch priority values.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree max-age” command resets the spanning tree max age to the default value of 20.

The example below shows how to configure the spanning tree max age.

Configure the max age as 12.

SMIS# configure terminal
SMIS(config)# spanning-tree max-age12
6.14 Forwarding Time

The switch waits for the forwarding time interval of the listening and learning states before going to the forwarding state.

The default forwarding time is 15 seconds. Hence, the switch waits for 15 seconds in the listening state and waits for another 15 seconds in the learning state before going to the forwarding state.

The forwarding time value should maintain the following relation with max age:

\[ 2 \times (\text{Forward Time} - 1) \geq \text{MaxAge} \]

Follow the steps below to change the forwarding time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure the max age time: spanning-tree forward-time&lt;time-value&gt;</td>
<td>Configures the switch spanning tree max age time. time-value – Spanning tree forward time may be from 4 to 30 seconds. The default forwarding time is 15 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree bridge forward-time</td>
<td>Displays the spanning tree forward time.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree forward-time” command resets the spanning tree forwarding time to the default value of 15.

The example below shows how to configure the spanning tree forward time.

Configure the forwarding time as 12 seconds.

SMIS# configure terminal

SMIS(config)# spanning-tree forward-time 12

SMIS(config)# end
6.15 Max Hops

MSTP uses a hop count to decide the validity of BPDU messages. The root switch sends a BPDU with a max hops count. Every switch decrements the hops count when forwarding the BPDU. When this hops count reaches zero, the switch discards the BPDU message.

The default max hops count is 20.

Follow the steps below to change the max hops.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure the max age time: spanning-tree mst max-hops &lt;maxhops-value&gt;</td>
<td>Configures the switch MSTP max hops value. maxhops-value – MSTP max hops value may be from 6 to 40 seconds. The default max hops is 20.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree mst</td>
<td>Displays the spanning tree max hops along with other MST information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree mst max-hops” command resets the MST max hops to the default value of 20.

The example below shows how to configure the MSTP max hops.

Configure the MST max hops as 30.

SMIS# configure terminal
SMIS(config)# spanning-tree mst max-hops 30
SMIS(config)# end

6.16 Path Cost Long/Short

Spanning tree was originally designed with 16-bit path costs. This was good enough for fast Ethernet and Gigabit Ethernet speed links, but not for 10Gb and higher speed ports. Hence, spanning tree protocol introduced support for 32-bit path costs.

The 16-bit path costs method is referred to as the short path cost method and the 32-bit path cost method is referred to as the long path costs method.
In MSTP and RSTP modes, Supermicro switches support long path costs by default. In STP compatible RSTP mode, Supermicro switches uses short path costs by default.

Follow the steps below to change the path costs method.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>To configure the path cost method as short spanning-tree pathcost method short</td>
<td>Configures the path cost method. In MSTP and RSTP, the default path cost method is long. In STP compatible RSTP mode, the default path cost is short.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree pathcost method</td>
<td>Displays the spanning tree path cost method information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “nospanning-tree pathcost method” command resets the path cost method to default value.

The example below shows how to configure the path cost method.

Configure the path cost method as short.

SMIS# configure terminal
SMIS(config)# spanning-tree pathcost method short
SMIS(config)# end

6.17 Transmit Hold Count

Transmit hold count helps control the BPDU burst traffic. The switch limits the number of BPDUs sent in one second with the transmit hold count. A higher transmit hold count value of allows switches to send more number of BPDUs for faster convergence. But it might lead to high switch CPU utilization.

The default transmit hold count is 3.

Follow the steps below to change the transmit hold count value.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
Step 2  spanning-tree transmit hold-count <count_value>  Configures the transmit hold count value.
Count-value – Transmit hold count value may be from 1 to 10.
The default transmit hold count value is 3.

Step 3  end  Exits the configuration mode.

Step 4  show spanning-tree detail  Displays the spanning tree hold count information.

Step 5  write startup-config  Optional step – saves this spanning tree configuration to be part of startup configuration.

The “no spanning-tree transmit hold-count” command resets the hold count to the default value of 3.

The example below shows how to configure the transmit hold count value.

Configure the transmit hold count as 8.

SMIS# configure terminal
SMIS(config)# spanning-tree transmit hold-count 8
SMIS(config)# end

6.18  Root Guard
In spanning tree networks, the position of the root switch is important to achieve optimized topology.
According to spanning tree protocol, any switch can become a root switch based on the priority and switch MAC address. Networks managed by multiple administrators can lead to multiple switches with a lowest priority to compete for root switch status. There is no option to block any switch becoming the root switch to maintain the optimized topology.

The root guard feature helps prevent any unexpected switch from becoming the root switch. If the root guard feature is enabled on a port, it prevents any switches connected to that port from becoming the root switch. If any superior BPDU is received on the root guard enabled port, the switch moves that port from a forwarding state to a listening state.

The root guard feature is disabled on all ports by default.

Follow the steps below to enable the root guard feature on the ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step</td>
<td>Command/Description</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>2</td>
<td><code>interface &lt;interface-type&gt;&lt;interface-id&gt;</code> or <code>interface range &lt;interface-type&gt;&lt;interface-id&gt; ...</code></td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: <code>int range fx 0/1-10</code> To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: <code>int range fx 0/1-10, fx 0/20</code></td>
</tr>
<tr>
<td>3</td>
<td><code>spanning-tree restricted-role</code></td>
<td>Enables the root guard feature. The default option is the root guard feature disabled.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td><code>show spanning-tree detail</code></td>
<td>Displays the spanning tree root guard information.</td>
</tr>
<tr>
<td>6</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no spanning-tree restricted-role” command resets the root guard feature to the default value of disabled.

The example below shows how to enable the root guard feature.

Enable the root guard feature on ports cx 0/1 and cx 0/2

SMIS# configure terminal
SMIS(config)# interface range cx 0/1-2
SMIS(config-if)# spanning-tree restricted-role
6.19 **Topology Change Guard**

The topology change guard helps prevent unexpected topology changes. Network administrators can configure the topology guard on ports that are not expected to receive topology change BPDUs.

Topology change BPDUs received on the topology change guard enabled ports will be dropped.

The topology guard feature is disabled on all ports by default.

Follow the steps below to enable the topology guard feature on the ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ...</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree restricted-tcn</td>
<td>Enables the topology guard feature. The default option is the topology guard feature disabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree detail</td>
<td>Displays the spanning tree topology guard information.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no spanning-tree restricted-tcn” command resets the topology guard feature to the default value of disabled.

The example below shows how to enable the topology guard feature.

Enable the topology guard feature on ports cx 0/1 and cx 0/2

SMIS# configure terminal

SMIS(config)# interface range cx 0/1-2

SMIS(config-if)# spanning-tree restricted-tcn

SMIS(config-if)# end

### 6.20 Port Fast

When a port link is up, spanning tree does not allow the port to forward the packets immediately. Spanning tree moves the port through the listening and learning states before reaching the forwarding state. This state machine function helps achieve a loop-free topology, but delays the port operation of forwarding traffic.

Switch ports connected to computers and servers are not expected to cause any loops. Those ports can be configured with the port fast feature to start forwarding traffic immediately instead of waiting through the learning and listening states.

Configure the port fast feature only to ports that are connected to computers and servers. Configuring port fast on ports that are connected to other switches might cause network loops.

The port fast feature is disabled on all ports by default.

Follow the steps below to enable the port fast feature on the ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ...</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port</td>
</tr>
</tbody>
</table>
channel identifier for port channel interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers.

E.g.: int range fx 0/1-10

To provide multiple interfaces or ranges, use separate with a comma (,).

E.g.: int range fx 0/1-10, fx 0/20

Step 3 spanning-tree portfast

Enables the port fast feature.

The default setting is the port fast feature disabled.

Step 4 end

Exits the configuration mode.

Step 5 show spanning-tree detail

Displays the spanning tree port fast information.

Step 6 write startup-config

Optional step – saves this spanning tree configuration to be part of startup configuration.

The “no spanning-tree portfast” command resets the port fast feature to the default value of disabled.

The example below shows how to enable the port fast feature.

Enable the port fast feature on ports cx 0/1 and cx 0/2.

SMIS# configure terminal

SMIS(config)# interface range cx 0/1-2

SMIS(config-if)# spanning-tree portfast

SMIS(config-if)# end

6.21 Auto Edge

The auto edge feature is used to detect the other end of a device attached to a port. If no BPDU is received for a period of time on auto edge enabled ports, the switch marks them as edge ports assuming they are not connected to other switches. This helps quickly move the port to a forwarding state. Also, switches do not send topology change notifications when an edge port’s status changes.

The auto edge feature is enabled on all ports by default.

Follow the steps below to configure the auto edge feature on the ports.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>To enable the auto-edge spanning-tree auto-edge To disable the auto-edge no spanning-tree auto-edge</td>
<td>Enables or disabled the auto edge feature. The default setting is the auto edge feature enabled.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree detail</td>
<td>Displays the spanning tree auto edge information.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows how to disable the auto edge feature.

Disable the auto edge feature on ports cx 0/1 and cx 0/2

SMIS# configure terminal

SMIS(config)# interface range cx 0/1-2

SMIS(config-if)# no spanning-tree auto-edge

SMIS(config-if)# end
6.22 Link Type

Spanning tree decides the link type based on the duplex mode of the ports. It detects full duplex ports as point-to-point links and half duplex ports as a shared LAN links.

Point-to-point links are assumed to be connected directly to another spanning tree switch, whereas shared LAN links are assumed to be connected with multiple switches through hubs.

In point-to-point links, spanning tree negotiates with other end switches to move the ports rapidly to the forwarding state.

Users can override the link type of ports as either point-to-point links or as shared links.

Follow the steps below to configure the link type of the ports.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ...</td>
<td>Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</td>
</tr>
<tr>
<td>Step 3</td>
<td>To configure the link type as point to point spanning-tree link-type point-to-point To configure the link type as shared spanning-tree link-type shared</td>
<td>Configures the link type.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree detail</td>
<td>Displays the spanning tree auto edge information.</td>
</tr>
</tbody>
</table>
Step 6  
write startup-config  

Optional step – saves this spanning tree configuration to be part of startup configuration.

The “no spanning-tree link-type” command resets the user configured link type to let switches detect the link type based on the duplex mode.

The example below shows the way to configure the link type.

Configure the port fx 0/1 as a point-to-point link.

SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# spanning-tree link-type point-to-point
SMIS(config-if)# end

### 6.23 Spanning Tree Configuration Examples

Configure the following requirements on the switches as shown below in FigureMSTP-Eg.1.

1. Configure two MST instances separately for VLANs 100 and 200.
2. Configure switch B as the root switch for the VLAN 100 instance.
3. Configure switch C as the root switch for the VLAN 200 instance.
4. Configure port fx 0/1-40 in all switches as port fast.

Figure MSTP-Eg.1Spanning Tree MSTP Configuration Example
Configurations on switch A
SMIS# configure terminal
# Create the VLANs 100 and 200
SMIS(config)# vlan 100,200
SMIS(config-vlan)# exit
# Create MST instance for vlan 100 and 200
SMIS(config)# spanning-tree mst configuration
SMIS(config-mst)# instance 1 vlan 100
SMIS(config-mst)# instance 2 vlan 200
SMIS(config-mst)# exit
# Configure the port fx 0/1-40 as port fast
SMIS(config)# interface range fx 0/1-40
SMIS(config-if)# spanning-tree portfast

Warning: portfast should only be enabled on ports connected to a single host.

Connecting hubs, concentrators, switches, bridges, etc. to this interface when portfast is enabled can cause temporary bridging loops.

Use with CAUTION
SMIS(config-if)#exit

# Save this spanning tree configuration.
SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS#

Configurations on switch B

SMIS# configure terminal

# Create the VLANs 100 and 200
SMIS(config)# vlan 100,200
SMIS(config-vlan)# exit

# Create MST instance for vlan 100 and 200
SMIS(config)# spanning-tree mst configuration
SMIS(config-mst)# instance 1 vlan 100
SMIS(config-mst)# instance 2 vlan 200
SMIS(config-mst)# exit

# Configure the port fx 0/1-40 as port fast
SMIS(config)# interface range fx 0/1-40
SMIS(config-if)# spanning-tree portfast

Warning: portfast should only be enabled on ports connected to a single host.

Connecting hubs, concentrators, switches, bridges, etc. to this interface when portfast is enabled can cause temporary bridging loops.

Use with CAUTION

SMIS(config-if)# exit

# Configure switch B as the root switch for VLAN 100 instance
SMIS(config)# spanning-tree mst 1 priority 4096
SMIS(config)# end

# Check the spanning tree MST configurations
SMIS# show spanning-tree mst 1 detail

## MST01

Vlans mapped: 100

Bridge: Address 00:30:48:a1:11:01 Priority 4096

Root: Address 00:30:48:a1:11:01 Priority 4096

Root: this switch for MST01

Fx0/47 of MST01 is Designated, Forwarding

Port info: port id 128.47 priority 128 cost 200000

Designated root: address 00:30:48:a1:11:01 priority 4096 cost 0

Designated bridge address 00:30:48:a1:11:01 priority 4096 port id 128.47

SMIS#

# Save this spanning tree configuration.

SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS# Configurations on switch C

SMIS# configure terminal

# Create the VLANs 100 and 200

SMIS(config)# vlan 100,200

SMIS(config-vlan)# exit

# Create MST instance for vlan 100 and 200

SMIS(config)# spanning-tree mst configuration

SMIS(config-mst)# instance 1 vlan 100

SMIS(config-mst)# instance 2 vlan 200

SMIS(config-mst)# exit

# Configure the port fx 0/1-40 as port fast

SMIS(config)# interface range fx 0/1-40

SMIS(config-if)# spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

SMIS(config-if)# exit

# Configure switch C as the root switch for VLAN 200 instance
SMIS(config)# spanning-tree mst 2 priority 4096
SMIS(config)# end

# Check the spanning tree MST configurations
SMIS# show spanning-tree mst 2 detail

## MST02
Vlans mapped: 200
Bridge Address 00:30:48:e3:56:12 Priority 4096
Root Address 00:30:48:e3:56:12 Priority 4096
Root this switch for MST02
Fx0/47 of MST02 is Designated, Forwarding
Port info port id 128.47 priority 128 cost 200000
Designated root address 00:30:48:e3:56:12 priority 4096 cost 0
Designated bridge address 00:30:48:e3:56:12 priority 4096 port id 128.47

SMIS#

# Save this spanning tree configuration.
SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS#
7 IGMP Snooping

Switches learn the source MAC addresses for unicast traffic and forward the unicast traffic only to the required ports. However, 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 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.

The IGMP snooping function helps 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 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

7.1 IGMP Snooping Support
Supermicro switches support IGMP snooping for all three IGMP versions (1, 2 and 3). Supermicro switches support the forwarding of multicast traffic based on MAC and IP addresses. Supermicro switches support up to 255 multicast groups.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping global status</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP snooping status in VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>Multicast forwarding mode</td>
<td>MAC based</td>
</tr>
<tr>
<td>Send query on topology change</td>
<td>Disabled</td>
</tr>
<tr>
<td>Proxy report</td>
<td>Enabled</td>
</tr>
<tr>
<td>Router port purge interval</td>
<td>125 seconds</td>
</tr>
<tr>
<td>Port purge interval</td>
<td>260 seconds</td>
</tr>
<tr>
<td>Report forward interval</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Group specific query interval</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Forwarding reports</td>
<td>To only router ports</td>
</tr>
<tr>
<td>Group specific query retry count</td>
<td>2</td>
</tr>
<tr>
<td>IGMP version</td>
<td>3</td>
</tr>
<tr>
<td>Immediate leave (fast leave)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Querier</td>
<td>Non-querier</td>
</tr>
<tr>
<td>Query interval</td>
<td>125 seconds</td>
</tr>
<tr>
<td>Unknown multicast filtering</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
7.2 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping</td>
<td>Enables IGMP snooping globally.</td>
</tr>
<tr>
<td>Step 3</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>_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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple VLANs are provided, the next step will enable IGMP snooping on all these VLANs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp snooping</td>
<td>Enables IGMP snooping on VLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp snooping globals</td>
<td>Displays the IGMP snooping information.</td>
</tr>
<tr>
<td></td>
<td>show ip igmp snooping vlan&lt;vlan&gt;</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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 used 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

7.3 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 the IGMP protocol standard.

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode. 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. If multiple VLANs are provided, the next step will be applied on all these VLANs.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping version {v1</td>
<td>v2</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp snooping vlan&lt;vlan&gt;</td>
<td>Displays the IGMP snooping version information for the given VLAN.</td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used 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

### 7.4 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.

#### 7.4.1 Router Port Timeouts

After finding the router ports, switches expect to periodically receive IGMP control messages from them. If IGMP receives no control messages 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2| ip igmp snooping mrouter-time-out <timeout> | Configures the router port timeout value in seconds.  
<timeout> – may be any value from 60 to 600 seconds.  
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. |

---

**i** 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

7.4.2 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If multiple VLANs are provided, the next step will configure the router ports for all these VLANs.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping mrouter&lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Configures the router port.</td>
</tr>
<tr>
<td></td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx portchannel – po</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp snooping mrouter [vlan&lt;vlan&gt;]</td>
<td>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.</td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
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 fx 0/1 as the router port for VLAN 10.

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

7.5 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.

7.5.1 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping group-query-interval &lt;timeout&gt;</td>
<td>Configures the group query interval timeout. ( \text{timeout} ) may be any value from 2 to 5 seconds. The default is 2 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping globals</td>
<td>Displays the IGMP snooping group query interval information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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

### 7.5.2 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 message. The number of times a switch retries sending the group specific query message is configurable. The default retry count is 2.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
### Step 1
**configure terminal**
Enters the configuration mode.

### Step 2
**ip igmp snooping retry-count**<count>
Configures the group specific query message retry count.
- 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 for 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

### 7.5.3 Immediate Leave

The switch can be configured to immediately remove a port from the group entry on the multicast table if it 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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
```

### 7.6 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode.</td>
</tr>
</tbody>
</table>

vIan-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.
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.

- `interval-value` – may be any value from 60 to 600 seconds.
- 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 of 125 seconds.

The example below shows the commands used 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
```

### 7.7 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping report-forward { all-ports</td>
<td>router-ports }</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping globals</td>
<td>Displays the IGMP snooping information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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 the commands used to configure 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
```

### 7.8 Port Timeout (Port Purge Interval)

A switch recognizes an 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 an IGMP member’s 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.

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

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 the commands used 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

7.9 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 passes will be forwarded to multicast routers.

Supermicro switches suppress IGMP reports for IGMP versions 1 and 2 only. If an 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping report-suppression-interval&lt;interval&gt;</td>
<td>Configures the port purge interval value in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interval – may be any value from 1 to 25 seconds. The default value is 5 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snoopingglobals</td>
<td>Displays the IGMP snooping report suppression interval information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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

### 7.10 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping proxy-reporting</td>
<td>Enables the proxy reporting feature.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snoopingglobals</td>
<td>Displays the IGMP snooping proxy reporting status information.</td>
</tr>
</tbody>
</table>
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

7.11 Sending Queries When Topology Changes

When spanning tree topology changes, multicast traffic is often flooded. To quickly recover from flooding, 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping send-query enable</td>
<td>Enables the switch to send general IGMP queries when spanning tree topology changes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping globals</td>
<td>Displays the IGMP snooping information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
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

7.12 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>no ip igmp snooping</td>
<td>Disables IGMP snooping globally.</td>
</tr>
<tr>
<td>Step 3</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>_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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple VLANs are provided, the next step will disable IGMP snooping on all these VLANs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>no ip igmp snooping</td>
<td>Disables IGMP snooping in VLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp snooping globals</td>
<td>Displays the IGMP snooping information.</td>
</tr>
<tr>
<td></td>
<td>show ip igmp snooping vlan&lt;vlan&gt;</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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

7.13 Unknown Multicast Filtering
Unknown multicast packets are flooded to all the VLAN member ports by default. This functionality can be modified to drop all the unknown multicast packets.

This feature, unknown multicast filtering, can be configured per VLAN.

Follow the steps below to enable unknown multicast filtering for any VLAN.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan&lt;vlan-list&gt;</td>
<td>Enters the VLAN configuration mode. 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. If multiple VLANs are provided, the next step will disable IGMP snooping on all these VLANs.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping multicast filtering enable</td>
<td>Disables IGMP snooping in VLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp snooping vlan&lt;vlan&gt;</td>
<td>Displays the IGMP snooping information including Multicast Forwarding feature</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP snooping configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
To disable unknown multicast filtering feature for any VLAN and flood all the unknown multicast packets to all the member ports of that VLAN, use the command “ip igmp snooping multicast filtering disable” in the VLAN configuration mode.

7.14 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)# exit
# Add member ports to VLAN 10
SMIS(config)# int range fx 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 cx 0/1 fx 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 cx 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...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
<th>Boot Loader</th>
<th>SSE-F3548</th>
<th>1.0.0.0</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

interface port-channel 1
exit

vlan 1

ports fx 0/11-19 untagged
ports fx 0/41-48 untagged
ports cx 0/2 untagged
exit

vlan 10

ports fx 0/20-40 untagged
ports po 1 untagged
exit

vlan 20
exit

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

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

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

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

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

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

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

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

interface Fx 0/9
switchport trunk allowed vlan 20
switchport mode trunk
interface Fx 0/10
switchport trunk allowed vlan 20
switchport mode trunk
interface Fx 0/20
switchport access vlan 10
switchport mode access
interface Fx 0/21
switchport access vlan 10
switchport mode access
interface Fx 0/22
switchport access vlan 10
switchport mode access
interface Fx 0/23
switchport access vlan 10
switchport mode access
interface Fx 0/24
switchport access vlan 10
switchport mode access
interface Fx 0/25
switchport access vlan 10
switchport mode access
interface Fx 0/26
switchport access vlan 10
switchport mode access
interface Fx 0/27
switchport access vlan 10
switchport mode access
interface Fx 0/28
switchport access vlan 10
switchport mode access
interface Fx 0/29
switchport access vlan 10
switchport mode access
interface Fx 0/30
switchport access vlan 10
switchport mode access
interface Fx 0/31
switchport access vlan 10
switchport mode access
interface Fx 0/32
switchport access vlan 10
switchport mode access
interface Fx 0/33
switchport access vlan 10
switchport mode access
interface Fx 0/34
switchport access vlan 10
switchport mode access
interface Fx 0/35
switchport access vlan 10
switchport mode access
interface Fx 0/36
switchport access vlan 10
switchport mode access
interface Fx 0/37
switchport access vlan 10
switchport mode access
interface Fx 0/38
switchport access vlan 10
switchport mode access
interface Fx 0/39
switchport access vlan 10
switchport mode access
interface Fx 0/40
switchport access vlan 10
switchport mode access
interface Cx 0/1
switchport trunk allowed vlan 20
switchport mode trunk
interface Cx 0/3
channel-group 1 mode active
interface Cx 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# show 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#
ACL is used to filter or redirect any particular traffic flow on the switch.

ACLs can be configured to match packets based on Layer 2 MAC or Layer3 or Layer 4 TCP/UDP parameters.

Every packet entering the switch is checked for the configured ACLs. If any packet contents match any of the configured ACLs, that packet will be handled according to the matched ACL configured action.

The ACL configuration provides the following actions that can be applied on matched traffic flow.

- **Deny**: The switch drops all packets matching this ACL
- **Redirect**: The switch redirects all packets matching this ACL to any configured redirect port
- **Permit**: The switch permits all packets matching this ACL

Supermicro switches implement ACL in hardware ASIC (Application Specific Integrated Circuit) to provide line rate ACL processing for all incoming traffic.

User configured ACL rules are programmed in an ACL table in ASIC. Layer 2 MAC extended ACLs and Layer 3 IP ACLs are implemented in two separate hardware tables, which are TCAM tables in ASIC.

ASIC analyzes the first 128 bytes of every received packet and extracts the packet contents for key fields in the Layer 2, Layer 3 and Layer 4 headers. ASIC then looks up the ACL tables to find a matching ACL rule for the extracted content of the packet. ASIC compares the values of the configured fields only and treats all other fields as “do not care”. Once a matching ACL is found, ASIC stops looking in that ACL table.

ASIC applies the configured action of the matching ACL rule to the matched packet. This could result in it dropping that packet, redirecting it to any particular port or simply allowing the packet to be forwarded through the switch.

A lookup on the Layer 2 and Layer 3 ACL tables happens simultaneously. If any packet matches the ACL rules of both Layer 2 and Layer 3 ACL tables, the actions configured on both ACL rules will be applied. In this case, conflicting actions configured on Layer 2 and Layer 3 ACL tables for the same traffic could lead to unpredictable behavior. Hence, it is suggested to avoid such ACL use cases.

**8.1 Types of ACLs**

Supermicro switches support the following three different types of ACLs.
### Three types of ACL

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Extended ACL</td>
</tr>
<tr>
<td>IP Standard ACL</td>
</tr>
<tr>
<td>IP Extended ACL</td>
</tr>
</tbody>
</table>

#### 8.1.1 MAC Extended ACL

A MAC Extended ACL allows users to control the traffic based on the fields in Ethernet MAC and VLAN headers.

Users can configure the traffic flow based on the source MAC address, destination MAC address or Ethernet type field value. Users can also use VLAN identifiers to configure the traffic flow.

Users can choose to deny, redirect or permit the configured traffic flow using a MAC Extended ACL.

#### 8.1.2 IP Standard ACL

An IP Standard ACL allows users to control the traffic based on the fields in an IP header.

Users can configure the traffic flow based on the source IP address and destination IP address.

Users can choose to deny, redirect or permit the configured traffic flow using an IP Standard ACL.

#### 8.1.3 IP Extended ACL

An IP Extended ACL allows users to control traffic based on fields in an IP header, ICMP header, TCP header and UDP header.

Users can configure the traffic flow based on source IP address, destination IP address, protocol field in IP header, TOS field in IP header or by using a DSCP priority in an IP header.

Users can also configure the traffic flow based on ICMP message type, ICMP message code, TCP port number or UDP port number.

Users can choose to deny, redirect or permit the configured traffic flow using an IP Extended ACL.

#### 8.2 MAC Extended ACL

Supermicro switches support up to 128 MAC Extended ACLs.

Users can configure a MAC Extended ACL with a deny, permit or redirect action rule. A MAC Extended ACL can be configured only with one rule. To implement multiple rule ACLs, configure multiple MAC Extended ACLs.

---

There is no implied deny all rule in Supermicro switch ACLs. By default, all packets not matching a configured ACL rule will be forwarded automatically. For any traffic to be denied, it has to be configured with an explicit deny rule.
The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted. In this case, permit rules have to be created before deny rules to make sure switch hardware processes permit rules first.

MAC Extended ACLs allow users to configure the traffic flow with the following fields.

- Source MAC Address
- Destination MAC Address
- Non-IP Protocol
- Ethernet type field in an Ethernet Header
- VLAN Identifier

MAC Extended ACL rules can be created and identified either with an ACL number such as 1, 2, 3 or with a name string. An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters. No special characters are allowed.

User can associate priority values to MAC extended ACL rules. Based on the configured priority, the rules will be orderly arranged in the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. Higher priority ACL rules take precedence over lower priority rules. In case of multiple rules with the same priority value, rules that were created earlier will take precedence over those created later.

If the user does not specify the priority, all rules will have a priority value of 1 by default.

### 8.2.1 Creating MAC Extended ACLs

Follow the steps below to create a MAC Extended ACL.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>mac access-list extended { &lt;access-list-number&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny { any</td>
<td>host&lt;src-mac-address&gt;}{ any</td>
</tr>
</tbody>
</table>
redirect <interface-type> <interface-id> { any | host <src-mac-address> } { any | host <dest-mac-address> } priority <value (1-65535)> } [ Vlan <vlan-id (1-4069)> ] [ priority <value (1-255)> ]

The protocol keyword can be used to configure the Ethernet header Encap Type field to be matched to apply this ACL rule. This protocol is an optional parameter. If not provided, switch will not check this field while matching packets for this ACL.

If this ACL rule is to be applied only to a particular VLAN, user can configure VLAN number using Vlan keyword. This Vlan is an optional parameter. If not provided, the switch will not check VLAN while matching packets for this ACL.

The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1.

Redirect ACL rule needs additional <interface-type> <interface-id> parameters to define the port to which the packets matching this ACL rule need to be redirected.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show access-lists</th>
<th>Displays the configured ACL rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

Every ACL is applied to all ports by default. Any ACL that needs to be applied only to particular ports needs to be configured as described in section Applying MAC Extended ACL to Interfaces.

The below examples show various ways of creating a MAC Extended ACL.

Create a deny MAC Extended ACL with ACL number 100 to deny all traffic from MAC 00:25:90:01:02:03

SMIS# configure terminal
SMIS(config)# mac access-list extended 100
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 any

Create a permit MAC Extended ACL with ACL name acl_cw3 to permit all traffic from MAC 00:25:30:01:02:03

SMIS# configure terminal
SMIS(config)# mac access-list extended acl_cw3

SMIS(config-ext-macl)# permit host 00:25:30:01:02:03 any

Create a redirect MAC Extended ACL to redirect all packets from MAC 00:25:90:01:02:03 going to MAC 00:25:90:01:02:04 to interface fx 0/10.

SMIS# configure terminal
SMIS(config)# mac access-list extended 1

SMIS(config-ext-macl)# redirect fx 0/10 host 00:25:90:01:02:03 host 00:25:90:01:02:04

8.2.2 Modifying MAC Extended ACLs
To modify a configured MAC Extended ACL, follow the same steps used to create a MAC Extended ACL. When users modify an ACL with a deny, permit or redirect rule, the previously configured rule and its parameters for that ACL will be completely overwritten with the newly provided rules and parameters.

When an ACL rule is modified, it is removed from the hardware ACL table and added back based on the priority of the rule.

The below example shows a MAC Extended ACL rule 50 that is created and later modified with different parameters.

SMIS# configure terminal
SMIS(config)# mac access-list extended 50
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 any
SMIS(config-ext-macl)# end

# Modify this ACL’s rule 50 to deny traffic destined to a particular host MAC instead of any

SMIS# configure terminal
SMIS(config)# mac access-list extended 50
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 host 00:25:90:01:02:04

8.2.3 Removing MAC Extended ACLs
Follow the steps below to remove MAC Extended ACLs.
### Step | Command | Description
--- | --- | ---
Step 1 | configure terminal | Enters the configuration mode
Step 2 | no mac access-list extended \{ <access-list-number> | <access-list-name> \} | Deletes a MAC Extended ACL using `no mac-access-list extended` command.
access-list-number – the ACL number that needs to be deleted
access-list-name – the name of the ACL that needs to be deleted
Step 3 | show access-lists | Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4 | write startup-config | Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove a MAC Extended ACL.

SMIS# configure terminal

SMIS(config)# no mac access-list extended 50

### 8.2.4 Applying MAC Extended ACLs to Interfaces
MAC Extended ACLs are applied to all physical interfaces by default. If users prefer to apply any MAC Extended ACL only to certain ports, the steps below need to be followed.

### 8.2.5 ACL Ingress Port Configuration
User can associate an ACL with multiple ingress ports. Follow the steps below to add ingress port(s) to an ACL.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>Interface <code>&lt;interface-type&gt;</code>&lt;interface-id&gt; or interface range <code>&lt;interface-type&gt;</code>&lt;interface-id&gt;</td>
<td>The port or port lists on which this MAC Extended ACL needs to be applied.</td>
</tr>
</tbody>
</table>
| Step 3 | mac access-group \{ `<short (1-32768)>` | Adds the MAC Extended ACL to this port.
access-list-number – the ACL number that needs to be added
access-list-name – the name of the ACL that needs to be added
| Step 4 | show access-lists | Displays the configured ACL rules to make sure this port is added to the required ACL. |
The example below shows applying a MAC Extended ACL rule 100 to ingress ports fx 0/1 and fx 0/10.

SMIS# configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# mac access-group 100
SMIS(config-if)# exit
SMIS(config)# int fx 0/10
SMIS(config-if)# mac access-group 100

Removing MAC Extended ACL from ingress port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>Interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ..</td>
<td>The port or port lists from which this MAC Extended ACL needs to be removed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>no mac access-group { &lt;short (1-32768)&gt;</td>
<td>Removes the MAC Extended ACL from this port. access-list-number – the ACL number that needs to be removed from this interface. access-list-name – the name of the ACL which needs to be removed from this interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
<td>Displays the configured ACL rules to make sure this port is removed from required ACL.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

1. When a MAC Extended ACL is removed from all the ports it was applied to, that ACL will become a switch-wide ACL (applied to all physical ports).
2. MAC Extended ACLs can be added only to physical ports like fx and cx ports. They cannot be added to Layer 3 vlan interfaces or port channel interfaces.
3. A MAC Extended ACL can be applied to many ports by following the above steps. In the same way, many MAC Extended ACLs can be applied to a single port.

The example below shows the commands for removing a MAC Extended ACL from a port.

SMIS#configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# no mac access-group 100

### 8.2.6 Displaying MAC Extended ACLs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show access-lists</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td></td>
<td>or show access-lists mac { &lt;access-list-number (1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-name – the name of the ACL which needs to be displayed</td>
</tr>
</tbody>
</table>

The show command displays the following information for every MAC Extended ACL:

- **Filter Priority**: ACL’s configured or default priority
- **Protocol Type**: Configured protocol. If not configured, it shall be displayed as zero.
- **Vlan Id**: Configured VLAN identifier.
- **Destination MAC Address**: Configured destination host MAC address. Displays 00:00:00:00:00:00 for any destination MAC address
- **Source MAC Address**: Configured source host MAC address. Displays 00:00:00:00:00:00 for any source MAC address
- **In Port List**: The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.
- **OutPort**: The egress port configured for this ACL. If no egress port configured, this will be ALL.
- **Filter Action**: Configured ACL action rule – deny, permit or redirect
- **Status**: Current status of the ACL. The status should normally be **active**. In the case of configuration errors, the ACL status may be inactive.

The below example displays a MAC Extended ACL.
Extended MAC Access List 100

Filter Priority : 1
Protocol Type : 0
EncapType : 0
Vlan Id :
Destination MAC Address : 00:25:90:01:02:03
Source MAC Address : 00:00:00:00:00:00
In Port List : Fx/0/2
Out Port : ALL
Filter Action : Deny
Status : Active

8.2.7 MAC Extended ACL Configuration
This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-1.
ACL 1 – Deny all traffic going from Server A to the gateway.
ACL 2 – Redirect all vlan 20 traffic coming from the gateway to Server B.

Figure ACL-1: MAC Extended ACL Example 1
8.3 IP Standard ACL

Supermicro switches support 128 IP ACLs, which includes both IP Standard and IP Extended ACLs.

Users can define IP Standard ACLs with deny, permit or redirect action rules. An IP Standard ACL can be defined with only one rule. To implement multiple rule ACLs, configure multiple IP Standard ACLs.

There is no implied deny all rule in Supermicro switch ACLs. By default, all packets not matching a configured ACL rule will be forwarded automatically. For any traffic to be denied, it has to be configured with an explicit deny rule.

The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted.

IP Standard ACLs allow users to configure the traffic flow with the following fields.

- Source IP Address
- Destination IP Address

IP Standard ACL rules can be created and identified either a with an ACL number as such as 1, 2 or 3 or with a name string. An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters. No special characters are allowed in ACL name strings.

IP Standard ACLs and IP Extended ACLs share the same ACL numbers and names. Hence ACL numbers and names across all IP Standard and IP Extended ACLs have to be unique. In other words, the same ACL number or name cannot be used for both IP Standard ACLs and IP Extended ACLs.

Users can associate a priority value to IP standard ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. Higher priority ACL rules take precedence over lower priority rules. In case of multiple rules with the same priority value, the rules that were created earlier will take precedence over those created later.

If the user does not specify the priority, all rules will have a priority value of 1 by default.

The priority for the IP standard ACL rule “deny any any” is fixed as 1. Users cannot configure the “deny any any” rule with different priority value. Since this rule will drop all the IP packets, this rule is added at the end of the IP ACL table on the hardware.

IP Standard ACLs and IP Extended ACLs share the same ACL table on the hardware. Hence priority values need to be configured while considering both IP standard and extended ACLs.
8.3.1 Creating IP Standard ACLs

Follow the steps below to create an IP Standard ACL.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-list standard { &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
</tbody>
</table>
| Step 3 | deny { any | host<ucast_addr> | <ucast_addr><ip_mask> } | [ { any | host<ip_addr> | <ip_addr><ip_mask> } ] [priority<value (1-255)>] 
\| or 
\| permit { any | host<src-ip-address> | <src-ip-address><mask> } | [ { any | host<dest-ip-address> | <dest-ip-address><mask> } ] [priority<value (1-255)>] \| or 
| 1. redirect<interface-type><interface-id> { any | host<src-ip-address> | <src-ip-address><mask> } | [ { any | host<dest-ip-address> | <dest-ip-address><mask> } ] [priority<value (1-255)>] | Configure a deny ACL rule or permit ACL rule or redirect ACL rule. The source and destination IP addresses are provided with the keyword host. The keyword any is used to refer to any IP addresses. To configure a network IP, address and mask should be provided. A redirect ACL rule needs additional <interface-type><interface-id> parameters to define the port to which the packets matching this ACL rule need to be redirected. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1. |
| Step 4 | show access-lists | Displays the configured ACL rule |
| Step 5 | write startup-config | Optional step – Saves this ACL configuration to be part of startup configuration. |

Every ACL is applied to all ports by default. If any ACL needs to be applied only to particular ports, it needs to be configured as described in section Applying IP ACL to Interfaces.
The examples below show different ways to create IP Standard ACLs.

Create a deny IP Standard ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 to IP 172.10.10.1

SMIS# configure terminal

SMIS(config)# ip access-list standard 100

SMIS(config-std-nacl)# deny host 172.10.10.10 host 172.10.10.1

Create a permit IP Standard ACL with ACL name acl_cw3 to permit all traffic from IP 172.10.10.1

SMIS# configure terminal

SMIS(config)# ip access-list standard acl_cw3

SMIS(config-std-nacl)# permit host 172.10.10.1 any

Create a redirect IP Standard ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 to interface fx 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list standard 1

SMIS(config-std-nacl)# redirect fx 0/10 172.20.20.0 255.255.255.0 host 172.20.0.1

8.3.2 Modifying IP Standard ACLs
To modify a configured IP Standard ACL, follow the same steps used to create a IP Standard ACL. When users modify an ACL with a deny, permit or redirect rule, the previously configured rule and its parameters for that ACL will be completely overwritten with the newly provided rules and parameters.

When an ACL rule is modified, it is removed from the hardware ACL table and added back based on the priority of the rule.

The example below shows an IP Standard ACL rule 50 being created and then modified with different parameters.

SMIS# configure terminal

SMIS(config)# ip access-list standard 50

SMIS(config-std-nacl)# deny 172.10.0.0 255.255.0.0 any

# Modify this ACL rule 50 to deny traffic destined to a particular host IP instead of to any.

SMIS# configure terminal

SMIS(config)# ip access-list standard 50
SMIS(config-std-nacl)# deny 172.10.0.0 255.255.0.0 host 172.50.0.1

### 8.3.3 Removing IP Standard ACLs

Follow the below steps to remove IP Standard ACLs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no ip access-list standard { &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-number – the ACL number that needs to be deleted access-list-name – the name of the ACL that needs to be deleted</td>
</tr>
<tr>
<td>Step 3</td>
<td>show access-lists</td>
<td>Displays the configured ACL rules to make sure the deleted ACL is removed properly</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration</td>
</tr>
</tbody>
</table>

The example below shows how to remove an IP Standard ACL.

SMIS# configure terminal
SMIS(config)# no ip access-list standard 50

### 8.3.4 Applying IP ACLs to Interfaces

IP Standard and Extended ACLs are applied to all physical interfaces by default. If users prefer to apply any IP Standard or Extended ACL only to certain ports, the steps below need to be followed.

### 8.3.5 ACL Ingress Port Configuration

User can associate an ACL with multiple ingress ports. Follow the steps below to add ingress port(s) to an ACL.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Defines the port or port lists on which this IP Standard / Extended ACL needs to be applied</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip access-group { &lt;access-list-number (1-32768)&gt;</td>
<td>&lt;access-list-name&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-number – the ACL number that needs to be added access-list-name – the name of the ACL which needs to be added</td>
</tr>
</tbody>
</table>
Step 4 | show access-lists | Displays the configured ACL rules to make sure this port has added the required ACL

Step 5 | write startup-config | Optional step – Saves this ACL configuration to be part of startup configuration

The example below shows applying an IP Standard ACL rule 100 to ports fx 0/1 and fx 0/10.

SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# ip access-group 100
SMIS(config-if)# exit
SMIS(config)# int fx 0/10
SMIS(config-if)# ip access-group 100

Removing an IP Standard / Extended ACL from a port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>The port or port lists from which this IP Standard or Extended ACL needs to be removed</td>
</tr>
<tr>
<td>Step 3</td>
<td>no ip access-group[ { &lt;access-list-number (1-65535)&gt; }</td>
<td>Removes the IP Standard / Extended ACL from this ingress port access-list-number – the ACL number that needs to be removed from this interface access-list-name – the name of the ACL that needs to be removed from this interface</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
<td>Displays the configured ACL rules to make sure this port has been removed from the required ACL</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration</td>
</tr>
</tbody>
</table>
1. When an IP Standard/Extended ACL is removed from all the ports it was applied to, that ACL will become a switch wide ACL (applied to all physical ports).
2. IP Standard and Extended ACLs can be added only to physical ports like fx or cx ports. ACLs cannot be added to Layer 3 vlan interfaces or port channel interfaces.
3. An IP Standard/Extended ACL can be applied to many ports by following the above steps. In the same way, many IP Standard/Extended ACLs can be applied on a single port.

The example below shows the commands used for removing an IP Extended ACL from a port.

SMIS# configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# no ip access-group 100

8.3.6 Displaying IP Standard ACLs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show access-lists or show access-lists ip { &lt;access-list-number (1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
</tbody>
</table>

The show command displays the following information for every IP Standard ACL.

- Source IP Address: Configured source host or subnet IP address. Displays 0.0.0.0 for any source IP.
- Source IP Address Mask: Configured source subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
- Destination IP Address: Configured destination host or subnet IP address. Displays 0.0.0.0 for any destination IP.
- Destination IP Address Mask: Configured destination subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
- In Port List: The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.
- Out Port: The egress port configured for this ACL. If no egress port configured, this will be ALL.
- Filter Action: Configured ACL action rule – deny, permit or redirect.
Status

Current status of the ACL. The status should normally be active. In case of configuration errors, the ACL status may be inactive.

The example below displays an IPStandard ACL

SMIS# show access-lists ip 1

Standard IP Access List 1

-------------
Source IP address : 172.20.20.0
Source IP address mask : 255.255.255.0
Destination IP address : 172.20.0.1
Destination IP address mask : 255.255.255.255
In Port List : ALL
Out Port : ALL
Filter Action : Redirect to Fx0/10
Status : Active

8.3.7 IP Standard ACL Configuration Example 1

This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-2.

ACL 1 – Deny all traffic going from 172.20.0.0 network to 172.100.0.0 network, but allow only server 172.20.20.1 to access the 172.100.0.1 gateway.

ACL 2 – Redirect all traffic destined to IP 172.10.0.0 network to server 172.10.10.10.

Figure ACL-2: IP Standard ACL Example 1

ACL 1 Configuration

This ACL has two rules; one to allow traffic from 172.20.20.1 and the other to deny all traffic from the 172.20.0.0 network.
A permit rule needs to be created first.

SMIS# configure terminal

SMIS(config)# ip access-list standard acl_1a

SMIS(config-std-nacl)# permit host 172.20.20.1 host 172.100.0.1

Then create the deny rule for the subnet 172.20.0.0.

SMIS# configure terminal

SMIS(config)# ip access-list standard acl_1b

SMIS(config-std-nacl)# deny 172.20.0.0 255.255.0.0 172.100.0.0 255.255.0.0

ACL 2 Configuration

SMIS# configure terminal

SMIS(config)# ip access-list standard 2

SMIS(config-std-nacl)# redirect fx 0/1 any 172.10.0.0 255.255.0.0

8.3.8 IP Extended ACLs

Supermicro switches support 128 IP ACLs, which includes both IP Standard and IP Extended ACLs.

Users can define IP Extended ACLs with deny, permit or redirect action rules. An IP Extended ACL can be defined only with one rule.

There is no implied deny all rule in Supermicro switch ACLs. By default, all packets not matching a configured ACL rule will be forwarded automatically. For any traffic to be denied, it has to be configured with an explicit deny rule.

The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted. IP Extended ACLs allow users to configure traffic flow with the following fields.

- IP - Protocol, Source IP Address, Destination IP Address, Type Of Service (TOS), DSCP
- TCP – Source Port, Destination Port, TCP message type – acknowledgement / reset
- UDP – Source Port, Destination Port
- ICMP – Message Type, Message Code

IP Extended ACL rules can be created and identified either a with an ACL number such as 1,2 or 3 or with a name string. ACL identifier numbers can be any number from 1 to 65535. ACL identifier names can be any string length not exceeding 32 characters.
IP Standard ACLs and IP Extended ACLs share the ACL numbers and names. Hence ACL numbers and names across all IP Standard and IP Extended ACLs have to be unique. In other words, the same ACL number or name cannot be used for both IP Standard ACLs and IP Extended ACLs.

User can associate priority values to IP Extended ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules takes precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules that created earlier will take precedence over the later ones.

If the user does not specify the priority, by default all rules will have same priority value as 1.

User can associate priority values to IP Extended ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules takes precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules that created earlier will take precedence over the later ones.

If the user does not specify the priority, by default all rules will have same priority value as 1.

### 8.3.9 Creating IP Extended ACLs for IP Traffic

Follow the steps below to create an IP Extended ACL for IP, OSPF or PIM traffic.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-list extended { &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny { ip</td>
<td>ospf</td>
</tr>
</tbody>
</table>
To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional.

To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP values from 0 to 63. The DSCP configuration is optional.

The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It may be any value from 1 to 255. The default value is 1.

Redirect ACL rules need additional <interface-type><interface-id> parameters to provide the port to which the packets matching this ACL rule should be redirected.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show access-lists</th>
<th>Displays the configured ACL rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The examples below show various ways to create an IP Extended ACL for IP traffic.

Create a deny IP Extended ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 with TOS8.

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# deny ip host 172.10.10.10 any tos 8

Create a deny IP ExtendedACL with ACL name acl_cw3 to deny all OSPF packets from network 172.20.1.0.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny ospf 172.20.1.0 255.255.255.0 any

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 with DSCP value 10 to interface fx 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# redirect fx 0/10 ip 172.20.20.0 255.255.255.0 host 172.20.0.1 dscp 10

### 8.3.10 Creating IP Extended ACLs for TCP Traffic

Follow the below steps to create an IP Extended ACL for TCP traffic.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-list extended {&lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt;}</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny tcp {any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>The source and destination IP addresses are provided with the keyword host. The keyword any may be used to refer to any IP addresses. To configure a network IP, address and mask should be provided.</td>
</tr>
<tr>
<td></td>
<td>permit tcp {any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>To apply this ACL rule to only TCP ACK packets, the keyword ack can be used. Similarly, to apply this ACL rule to only TCP RST packets, the keyword rst could be used.</td>
</tr>
</tbody>
</table>
To apply this rule to packets with specific TOS values, use the keyword `tos` and specify the TOS value to be matched. Users can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional.

To apply this rule to packets with specified DSCP values, use the keyword `dscp` and specific DSCP values to be matched. Users can specific any DSCP values from 0 to 63. This DSCP configuration is optional.

The priority keyword lets users assign a priority to this ACL rule. This priority is an optional parameter. It could be any value from 1 to 255. The default value is 1.

Redirect ACL rules need additional `<interface-type><interface-id>` parameters to define the port to which the packets matching this ACL rule need to be redirected.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show access-lists</th>
<th>Displays the configured ACL rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The examples below show various ways to create IP Extended ACLs for TCP traffic.

Create a deny IP Extended ACL with ACL number 100 to deny all traffic to TCP port 23.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny tcp any any eq 23

Create a deny IP Extended ACL with ACL name acl_cw3 to deny all TCP traffic on 172.20.0.0 network.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny tcp any 172.20.0.0 255.255.0.0

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 with TCP ports equal to 1000 to interface fx 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect fx0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 eq 1000

### 8.3.11 Creating IP Extended ACLs for UDP Traffic

Follow the steps below to create an IP Extended ACL for TCP traffic.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-list extended{ &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td></td>
<td>denyudp (any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>permitudp (any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
</tbody>
</table>
redirect<interface-type><interface-id>tcp { any | host<src-ip-address> | <src-ip-address><src-mask> } [{ eq<port-number (0-65535)> } ] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{ eq<port-number (0-65535)> } ] { tos<value (0-255)> | dscp<value (0-63)> } [ priority<short(1-255)> ]

provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional.

To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP value from 0 to 63. This DSCP configuration is optional.

The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1.

A Redirect ACL rule needs additional <interface-type><interface-id> parameters to define the port to which the packets matching this ACL rule need to be redirected.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show access-lists</th>
<th>Displays the configured ACL rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The examples below show various ways to create IP Extended ACLs for TCP traffic.

Create a deny IP Extended ACL with ACL number 100 to deny all traffic to UDP port 1350.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny udp any any eq 1350

Create a deny IP Extended ACL with ACL name acl_cw3 to deny all UDP traffic on 172.20.0.0 network.

SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny udp any 172.20.0.0 255.255.0.0
Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 with destination UDP ports equal to 1000 to interface fx 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 500

SMIS(config-ext-nacl)# redirect fx 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 eq 1000

### 8.3.12 Creating IP Extended ACLs for ICMP Traffic

Follow the steps below to create an IP Extended ACL for TCP traffic.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip access-list extended { &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny icmp { any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
</tbody>
</table>
The examples below show various ways to create IP Extended ACLs for ICMP packets.

Create a deny IP Extended ACL with ACL number 100 to deny all ICMP “traceroute” messages.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny icmp any any 30

Create a deny IP Extended ACL with ACL name acl_cw3 to deny all ICMP traffic on 172.20.0.0 network.

SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny icmp any 172.20.0.0 255.255.0.0

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 with ICMP message type “Destination Unreachable” to interface fx 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect fx 0/10 icmp 172.20.20.0 255.255.255.0 host 172.20.0.1 3

8.3.13 Modifying IP Extended ACLs
To modify a configured IP Extended ACL, follow the same steps used to create an IP Extended ACL. When users modify an ACL with a deny, permit or redirect rule, the previously configured rule and its parameters for that ACL will be completely overwritten with the newly provided rules and parameters.
# Modify this ACL rule 50 to deny ICMP redirect messages instead of all ICMP messages

SMIS# configure terminal

SMIS(config)# ip access-list extended 50

SMIS(config-ext-nacl)# deny icmp any 172.10.0.0 255.255.0.0 5

### 8.3.14 Removing IP Extended ACLs

Follow the steps below to remove IP Extended ACLs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no ip access-list extended { &lt;access-list-number(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td>Step 3</td>
<td>show access-lists</td>
<td>Displays the configured ACL rules to make sure the deleted ACL is removed properly</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows how to remove an IP Extended ACL.

SMIS# configure terminal

SMIS(config)# no ip access-list extended 50

### 8.3.15 Applying IP Extended ACLs to Interfaces

The procedure to apply IP Extended ACLs to an interface is the same as the procedure used for IP Standard ACLs. Hence, refer to the section Apply IP ACL to Interfaces.

### 8.3.16 Displaying IP Extended ACLs

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show access-lists or show access-lists ext-ip { &lt;access-list-number (1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
</tbody>
</table>
This show command displays the following information for every IP Extended ACL.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Priority</td>
<td>Configured or default priority of the ACL</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>IP Protocol Type</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Configured source host or subnet IP address. Displays 0.0.0.0 for any source IP.</td>
</tr>
<tr>
<td>Source IP Address Mask</td>
<td>Configured source subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>Configured destination host or subnet IP address. Displays 0.0.0.0 for any destination IP.</td>
</tr>
<tr>
<td>Destination IP Address Mask</td>
<td>Configured destination subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.</td>
</tr>
<tr>
<td>In Port List</td>
<td>The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.</td>
</tr>
<tr>
<td>Out Port</td>
<td>The egress port configured for this ACL. If no egress port configured, this will be ALL.</td>
</tr>
<tr>
<td>Filter Action</td>
<td>Configured ACL action rule – deny or permit or redirect</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the ACL. The status should normally be <strong>active</strong> always. In case of configuration errors, the ACL status may be inactive.</td>
</tr>
</tbody>
</table>

The following fields are displayed for TCP and UDP rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Ports From</td>
<td>Starting TCP/UDP source port. If the ACL needs to be applied to only one port, the “Ports From” will specify that port. If the ACL needs to be applied to all ports, “Ports From” will be 0.</td>
</tr>
<tr>
<td>Source Ports Till</td>
<td>Starting TCP/UDP source port. If the ACL needs to be applied to only one port, the “Ports Till” will specify that port. If this ACL needs to be applied to all ports, “Ports Till” will be 65535.</td>
</tr>
<tr>
<td>Destination Ports From</td>
<td>Starting TCP/UDP destination port. If the ACL needs to be applied to only one port, the “Ports From” will specify that port. If the ACL needs to be applied to all ports, “Ports From” will be 0.</td>
</tr>
<tr>
<td>Destination Ports Till</td>
<td>Starting TCP/UDP destination port. If the ACL needs to be applied to only one port, the “Ports Till” will specify that port. If the ACL needs to be applied to all ports, “Ports Till” will be 65535.</td>
</tr>
</tbody>
</table>

The following fields are displayed only for TCP rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RST bit</td>
<td>If the ACL is applied only to TCP Reset messages</td>
</tr>
<tr>
<td>ACK bit</td>
<td>If the ACL is applied only to TCP acknowledgement messages</td>
</tr>
</tbody>
</table>

The following fields are displayed only for ICMP rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP type</td>
<td>Displays ICMP types if the ACL is applied only to particular ICMP messages.</td>
</tr>
</tbody>
</table>
Displays “No ICMP types to be filtered” if the ACL is applied to all ICMP message types.

ICMP code
Displays ICMP message codes if the ACL is applied only to particular ICMP message codes.
Displays “No ICMP codes to be filtered” if the ACL is applied to all ICMP message codes.

The examples below display different IP Extended ACLs.

IP Extended ACLs with IP/OSPF/PIM rules display the following fields:

Filter Priority : 1
Filter Protocol Type : ANY
Source IP address : 172.10.10.10
Source IP address mask : 255.255.255.255
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List : ALL
Out Port : ALL
Filter TOS : 0 None
Filter DSCP : Deny
Status : Active

IP Extended ACLs with TCP rules display the following fields:

SMIS# show access-lists ext-ip 1
Extended IP Access List 1

-------------------------
Filter Priority : 1
Filter Protocol Type : TCP
Source IP address : 172.20.0.0
Source IP address mask : 255.255.0.0
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List : ALL
Out Port : ALL
Filter TOS : 0
Filter DSCP : 0
Filter Source Ports From : 0
Filter Source Ports Till : 65535
Filter Destination Ports From : 25
Filter Destination Ports Till : 25
Filter Action : Permit
Status : Active

IP Extended ACLs with ICMP rules display the following fields:

SMIS# show access-lists ext-ip 100
Extended IP Access List 100
---

Filter Priority : 1
Filter Protocol Type : ICMP
ICMP type : No ICMP types to be filtered
ICMP code : No ICMP codes to be filtered
Source IP address : 0.0.0.0
Source IP address mask : 0.0.0.0
Destination IP address : 172.10.0.0
Destination IP address mask : 255.255.0.0
In Port List : ALL
Out Port : ALL
Filter Action : Redirect to Fx0/1
Status : Active

SMIS#

IP Extended ACLs with UDP rules display the following fields:

SMIS# show access-lists ext-ip 200
Extended IP Access List 200

---

Filter Priority : 1
Filter Protocol Type : UDP
Source IP address : 0.0.0.0
Source IP address mask : 0.0.0.0
Destination IP address : 172.100.0.0
Destination IP address mask : 255.255.0.0
In Port List : ALL
Out Port : ALL
Filter TOS : 
Filter DSCP : 
Filter Source Ports From : 0
Filter Source Ports Till : 65535
Filter Destination Ports From : 1001
Filter Destination Ports Till : 65535
Filter Action : Deny
Status : Active

### 8.4 IP Extended ACL Configuration Example 1

This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-3.

ACL 1 – Allow SMTP TCP traffic from the 172.20.0.0 network and deny all other TCP traffic from this network.

ACL 2 – Redirect all ICMP traffic destined to the IP 172.10.0.0 network to server 172.10.10.10.

ACL 3 – Deny all UDP traffic going to 172.100.0.0 with a destination UDP port greater than 1000.
ACL 1 Configuration

This ACL has two rules: one to allow traffic from 172.20.20.1 and the other is to deny all traffic from the 172.20.0.0 network.

Create the permit rule first.

SMIS# configure terminal
SMIS(config)# ip access-list extended acl_1a
SMIS(config-ext-nacl)# permit tcp 172.20.0.0 255.255.0.0 any eq 25

Then create the deny rule for the subnet 172.20.0.0.

SMIS# configure terminal
SMIS(config)# ip access-list extended acl_1b
SMIS(config-ext-nacl)# deny tcp 172.20.0.0 255.255.0.0 any

ACL 2 Configuration

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# redirect fx 0/1 icmp any 172.10.0.0 255.255.0.0

ACL 3 Configuration

SMIS# configure terminal
SMIS(config)# ip access-list extended 200
SMIS(config-ext-nacl)# deny udp any 172.100.0.0 255.255.0.0 eq 1000
9 QoS

Typically, networks operate on a best-effort delivery basis providing all traffic equal priority and an equal chance of being delivered in a timely manner. However, during congestion, all traffic has unequal chance of being dropped. The QoS feature allows one to select specific network traffic and prioritize it according to its relative importance to provide preferential treatment. Implementing QoS makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation in Supermicro switches is based on the Differentiated Services (DiffServ) architecture. DiffServ architecture specifies that each packet is classified upon entry into the network. The classification is carried in the IP packet header using six bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

- Classification bits in Layer 2 frames:
  Layer 2 frame headers contain a class of service (CoS) value as a 3-bit field in the VLAN Header. Layer 2 CoS values range from 0 for low priority to 7 for high priority.

The same forwarding treatment is provided to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by other switches or routers based on a configured policy, detailed examination of the packet, or both.

Switches and routers use the class information to limit the amount of resources allocated per traffic class. The behavior of a switch/router when handling traffic in the DiffServ architecture is called \textit{per-hop behavior}. All devices along a network path must provide a consistent per-hop behavior in an end-to-end QoS solution.

![Figure QoS-1: QoS Model](image)

The QoS Model can be divided into Ingress packet processing and Egress packet processing.

Actions at the ingress interface include classifying traffic, policing, and marking:

Classifying distinguishes one kind of traffic from another.
Policing determines whether a packet is in or out of profile according to the configured policer. The policer also limits the bandwidth consumed by a flow of traffic.

Marking allows for the differentiation of packets by designating different identifying values, e.g., packets can be marked by setting the IP precedence bits or the IP differentiated services code point (DSCP) in the type of service (ToS) byte.

Actions at the egress interface include queuing and scheduling:

Queuing evaluates the CoS value and determines in which of the eight egress queues to place the packet.

Scheduling services the eight egress queues based on a configured scheduling algorithm.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Class Map</td>
<td>None</td>
</tr>
<tr>
<td>Policy Map</td>
<td>None</td>
</tr>
<tr>
<td>Default Priority</td>
<td>0</td>
</tr>
<tr>
<td>Minimum Bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
<tr>
<td>Scheduling Algorithm</td>
<td>Strict Queuing</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>0</td>
</tr>
<tr>
<td>Burst Size</td>
<td>0</td>
</tr>
<tr>
<td>HOL</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

The default priority to traffic class queue mapping:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Traffic Class queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

9.1 Policy-Based QoS

Supermicro switch features based on QoS Policies are:
9.1.1 Classification and Marking
Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Supermicro switches use ACL’s to specify the fields in the frame or packet based on which incoming IP traffic is classified.

Classification is enabled only if QoS is globally enabled on the switch. QoS is globally disabled by default, so no classification occurs. In Supermicro switches, classification can be configured for all interfaces of the switch or for particular interfaces only.

After classification, the packet is sent for policing, marking, queuing and scheduling. Marking is the process of setting or modifying values in the classified traffic. In Supermicro switches, marking can be configured using a policy map.

9.1.1.1 ClassMap and PolicyMap
IP standard, IP extended, and Layer 2 MAC access control lists (ACLs) can be used to define a group of packets with the same characteristics (class). Only the permit action of ACL’s is permitted for use with QoS.

The Deny and Redirect ACL actions are not applicable for QoS.

After an ACL is associated with a class-map, it can be applied for QoS. When such a configured ACL has a match with a permit action, further classification can be done using a policymap. A policy map specifies the actions to perform for the traffic class of a class-map. Actions can include setting a specific DSCP value or the action to take when the traffic is out of profile.

An ACL must be created for each policy and class-map. If more than one type of traffic needs to be classified, another ACL and class map can be created and associated. This relationship between the ACL, class map and policy map is depicted below.
9.1.1.2 Policing
Policing involves creating a policer that specifies the bandwidth limits for the traffic. Each policer specifies the action to take for packets that are in or out of profile. Packets that exceed the limits are out of profile and various actions are carried out by the marker on out of profile packets, which may include dropping the packet or marking down the packet with a new user-defined value.

9.2 CoS-Based QoS
Supermicro switch features based on Class of Service (CoS) are:

- Queuing
- Scheduling
- Bandwidth Management
- Default Priority

9.2.1 Egress Queuing
The CoS priority of a packet is mapped to a traffic class. Supermicro switches provide support to configure the mapping of CoS priority to a traffic class. Each traffic class is mapped to eight egress queues in the switch.

The traffic class is taken from the CoS value of the ingress packet. If an ingress packet does not have a CoS (untagged packets), the port default priority will be used.

The above figure shows the egress queuing procedure. When a tagged packet with CoS value 3 (packet1) arrives in the switch, the CoS to egress queuemapping for the particular destination port is looked up. Based on CoS to egress queue mapping, packets with CoS value 3 are queued in Queue-3 and transmitted. Similarly, when a tagged packet with CoS value 7 (packet2) arrives in switch, the CoS to egress queue mapping for the particular destination port is looked up. Based on CoS to egress queue mapping, packets with CoS value 7 are queued in Queue-7 and transmitted.
9.2.2 Scheduling
Supermicro switches support eight CoS queues for each egress port. For each of the eight queues, various types of scheduling can be configured:

*Strict Priority*

Strict priority scheduling is based on the priority of queues. Packets in a high-priority queue are always sent first and packets in a low-priority queue are not sent until all the high-priority queues are empty.

*Round Robin (RR)*

Using the round-robin (RR) scheduling algorithm, packets in queues are transmitted in a FIFO manner, i.e. one packet after the other. All queues have the same priority and weight in an RR configuration.

*Weighted Round Robin (WRR)*

In WRR scheduling, the user specifies a number to indicate the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler sends some packets from each queue in turn. The number of packets it sends corresponds to the relative importance of the queue. By using WRR, low-priority queues can send packets even when high-priority queues are not empty.

*Deficit WRR*

Bandwidth allocation can be unfair when the average packet sizes are different between the queues and their flows. This behavior can result in service degradation for queues with smaller average packet sizes. Deficit Weighted Round Robin (DWRR) is a modified weighted round-robin scheduling that can handle packets of variable size.

9.2.3 Default Priority

The Class of Service (CoS) priority field is taken from the VLAN header of a received packet. If the received packet does not have a VLAN header, the default port priority is used as the CoS value. Supermicro switches provide an option to configure the default priority.

![Figure QoS-4: VLAN Tag and CoS Priority](image)

In the above figures, CoS priority is a 3-bit field in a tagged frame that indicates the frame priority level, ranging from 0 (best effort) to 7 (highest) with 1 representing the lowest priority. These values can be used to prioritize different classes of traffic (voice, video, data, etc.).

For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used. Supermicro switches allow users to configure the default port priority.
Each ingress port on the switch has a single receive queue buffer for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. Tagged frames use the assigned CoS value when it passes through the ingress port.

9.2.4 Bandwidth Management
Bandwidth limiting is configured at the level of traffic classes. Traffic classes can be assigned minimum bandwidths, maximum bandwidths, and weights. Weights are used to divide the bandwidth proportionally among all traffic classes within a QoS policy, in such a way that a traffic class does not receive more than its maximum bandwidth or less than its minimum bandwidth.

9.3 Port-Based Rate Limit
Rate limits define which packets conform to or exceed the defined rate based on the following two parameters:

*Average rate* determines the average transmission rate. Traffic that falls under this rate will always conform.

*Burst size* specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time without causing scheduling concerns. It determines how large a traffic burst can be before it exceeds the rate limit.

Traffic that exceeds the rate limit is dropped. Supermicro switches support output rate limits.

9.4 HOL Blocking Prevention
Supermicro switches provide eight egress queues per port. Each queue has a dynamic packet limit based on the availability of packet buffer memory. When a switch receives packets at a fast rate destined to a particular egress port, its egress port queues become filled up. When the egress queue is full, all packets at ingress are dropped. This phenomenon of dropping ingress packets due to egress port/CoS queue oversubscription is called Head of Line (HOL) blocking.

Supermicro switches provide support to prevent HOL blocking. When HOL blocking prevention is enabled in the switch, it drops packets newly arriving on the ingress if they are destined to an oversubscribed egress port, based on the egress queue threshold. The switch stops dropping ingress packets once it determines the egress queue is not over-subscribed by using specific counters and thresholds. This mechanism ensures fair access to all port buffers.

HOL blocking prevention provides lossy buffer management, however it improves overall system throughput.

9.5 Enabling QoS
QoS is disabled by default in Supermicro switches. Follow the below steps to enable QoS.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set qos enable</td>
<td>Enables QoS on all interfaces</td>
</tr>
</tbody>
</table>
The “set qos disable” command disables QoS in the switch.

QoS must be enabled before configuring any of the QoS features.

The example below shows the commands used to enable QoS.

SMIS# configure terminal
SMIS(config)# set qos enable
SMIS(config)# end
SMIS(config)# show running-config

Building configuration...
ID   Hardware Version                   Firmware    OS        Boot Loader
0          SSE-F3548                    1.0.0.0     6         0.0.0.0
vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit

setqos enable

**9.6 Configuring Policy-Based QoS**

Follow the steps below to configure Policy-Based QoS features such as classification, marking and policing.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create MAC Extended or IP Standard or IP Extended ACL. If required, apply ACL to specific Interface(s).</td>
<td>Refer to the ACL Configuration Guide at <a href="http://www.supermicro.com/products/nfo/networking.cfm">www.supermicro.com/products/nfo/networking.cfm</a>.</td>
</tr>
</tbody>
</table>
| Step 3 | class-map <class-map-number(1-65535)> | Creates a class map and enters the class-map configuration mode. 

*class-map-number* - QoS class map number in range from 1-65535. |
| Step 4 | match access-group { mac-access-list | ip-access-list } { <acl-index-num (1-65535) > | <acl-name> } | This command specifies the fields in the incoming packets that are to be examined to classify the packets. The IP access group / MAC access group can be used as matchcriteria. 

*mac-access-list* - Accesses list created based on MAC addresses for non-IP traffic |
ip-access-list - Accesses list created based on IP addresses. The IP-access list can either be defined as a standard IP-access list or an extended IP-access list.

acl-index-num - Specifies the ACL index range. The ACL index range for an IP standard ACL is 1 to 1000 and 1001 to 65535 for an IP extended ACL. The ACL index range for a MAC extended ACL is 1 to 65535.

ACL-name – Specifies the configured ACL name as a string not exceeding 32 characters

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Exit</th>
<th>Exit the classmap configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>policy-map &lt;policy-map-number(1-65535)&gt;</td>
<td>Creates a policy map and enters the policy-map configuration mode.</td>
</tr>
<tr>
<td></td>
<td>policy-map-number - QoS policy map number</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>class &lt;class-map-number(1-65535)&gt;</td>
<td>This command defines a traffic classification for the policy to act upon. The class-map-number that is specified in the policy map ties the characteristics for that class to the class map and its match criteria as configured with the class-map global configuration command. Upon execution of the class command, the switch enters the policy-map class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>class-map-number – The class map number to associate the policy, in range of 1-65535</td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td>set {cos&lt;new-cos(0-7)&gt;</td>
<td>(Optional) Configures the in-profile action by setting a class of service (CoS), differentiated services code point (DSCP), or IP-precedence value in the packet.</td>
</tr>
<tr>
<td></td>
<td>ipdscp&lt;new-dscp(0-63)&gt;</td>
<td>cos - New COS value assigned to the classified traffic, in range of 0-7</td>
</tr>
<tr>
<td></td>
<td>ip precedence &lt;new-precedence(0-7)&gt;}</td>
<td>ipdscp - New DSCP value assigned to the classified traffic, in range of 0-63</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip precedence - New IP-precedence value assigned to the classified traffic, in range of 0-7</td>
</tr>
<tr>
<td>Step 9</td>
<td>police &lt;rate-Kbps(64-1048572)&gt;</td>
<td>(Optional) Configures a policer for the classified traffic. This command also specifies the action to be taken if the specified rate is exceeded or if there is no match for the policy configured.</td>
</tr>
<tr>
<td></td>
<td>exceed-action {drop</td>
<td>policed-dscp-transmit &lt;new-dscp(0-63)&gt;}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>exceed-action - Indicates the action of the switch when the specified rate is exceeded.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>11</td>
<td>show class-map [&lt;class-map-num(1-65535)&gt;]</td>
<td>Displays the classmap configuration.</td>
</tr>
<tr>
<td></td>
<td>show policy-map [&lt;policy-map-num(1-65535)&gt;] [class &lt;class-map-num(1-65535)&gt;]</td>
<td>Displays the policy map configuration.</td>
</tr>
</tbody>
</table>

ACL cannot be modified unless it is removed from the class-map.

For modifying an ACL associated with a classmap, follow the steps below:
1) Remove policy map
2) Remove classmap
3) Modify the ACL
4) Re-create the classmap
5) Re-create the policy map

If required, an ACL’s association with an interface must be configured before the “classmap” configuration, i.e. after associating the ACL with a classmap using the “match” command, the ACL cannot be associated with an interface.

These commands either delete the particular configuration or reset it to its default value.

- no class-map <class-map-number(1-65535)>
- no policy-map <policy-map-number(1-65535)>
- no class <class-map-number(1-65535)>

Before deleting a classmap, any policy map associated with it must first be deleted.

The example below shows the commands used to configure QoS classification, marking and policing.

**Example 1: Classification and Marking**

Create a Layer 2 MAC ACL with two permit statements and attach it to an ingress interface. The first permit statement allows traffic from the host with a MAC address of 00:30:48:14:c8:29 to be sent to any host.

SMIS# configure terminal

SMIS(config)# mac access-list extended mac1

SMIS(config-ext-macl)# permit host 00:30:48:14:c8:29 any

SMIS(config-ext-macl)# exit
SMIS(config)# set qos enable
SMIS(config)# interface Fx 0/3
SMIS(config-if)# mac access-group mac1
SMIS(config-if)# exit
SMIS(config)# class-map 5
SMIS(config-cmap)# match access-group mac-access-list mac1
SMIS(config-cmap)# exit
SMIS(config)# policy-map 5
SMIS(config-pmap)# class 5
Existing Policymap configurations have been deleted. Please apply the policymap to make it active.
SMIS(config-pmap-c)# set cos 6
SMIS(config-pmap-c)# end
SMIS(config)# mac access-list extended mac2
SMIS(config-ext-macl)# permit host 00:b0:d0:86:bb:f7 any
SMIS(config-ext-macl)# exit
SMIS(config)# interface Fx 0/3
SMIS(config-if)# mac access-group mac2
SMIS(config-if)# exit
SMIS(config)# class-map 10
SMIS(config-cmap)# match access-group mac-access-list mac2
SMIS(config-cmap)# exit
SMIS(config)# policy-map 10
SMIS(config-pmap)# class 10
Existing policymap configurations have been deleted. Please apply the policymap to make it active.
SMIS(config-pmap-c)# set cos 7
SMIS(config-pmap-c)# end
SMIS# show policy-map
DiffServ Configurations:
Quality of Service has been enabled

Policy Map 5 is active
Class Map: 5

In Profile Entry

In profile action : policed-cos6

Policy Map 10 is active
Class Map: 10

In Profile Entry

In profile action : policed-cos7

SMIS# show class-map

DiffServ Configurations:

Class map 5

Filter ID : mac1
Filter Type : MAC-FILTER

DiffServ Configurations:

Class map 10

Filter ID : mac2
Filter Type : MAC-FILTER

SMIS# show running-config

Building configuration...

ID   Hardware Version                   Firmware    OS        Boot Loader
0    SSE-F3548                        1.0.0.0     6         0.0.0.0

vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit
mac access-list extended mac1
permit host 00:30:48:14:c8:29   any
exit
mac access-list extended mac2
permit host 00:b0:d0:86:bb:f7   any
exit
interface Fx 0/3
mac access-group mac1
mac access-group mac2
exit
setqos enable
class-map 5
match access-group mac-access-list mac1
exit
class-map 10
match access-group mac-access-list mac2
exit
policy-map 5
class 5
Example 2: Policing

Create a policy map for the switch without attaching it to an ingress interface. In the configuration, the IP standard ACL permits traffic from network 20.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. If the matched traffic exceeds an average traffic rate of 4800 bps, its DSCP is marked down to a value of 10 and transmitted.

SMIS# configure terminal
SMIS(config)# ip access-list standard 1
SMIS(config-std-nacl)# permit 20.1.0.0 255.255.0.0 any
SMIS(config-std-nacl)# exit
SMIS(config)# set qos enable
SMIS(config)# class-map 1
SMIS(config-cmap)# match access-group ip-access-list 1
SMIS(config-cmap)# exit
SMIS(config)# policy-map 1
SMIS(config-pmap)# class 1

Existing policymap configurations have been deleted. Please apply the policymap to make it active.
SMIS(config-pmap-c)# police 500000 exceed-action policed-dscp-transmit 10
SMIS(config-pmap-c)# end
SMIS# show policy-map

DiffServ Configurations:
Quality of Service has been enabled

Policy Map 1 is active

Class Map: 1

Out Profile Entry

Metering on
burst bytes/token size : 6
Refresh count : 500000
Out profile action : policed-dscp 10

SMIS# show class-map

DiffServ Configurations:

Class map 1

Filter ID : 1
Filter Type : IP-FILTER

SMIS# show running-config

Building configuration...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
<th>Boot Loader</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SSE-F3548</td>
<td>1.0.0.0</td>
<td>6</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit
ip access-list standard 1
permit 20.1.0.0 255.255.0.0 any
exit
setqos enable
class-map 1
match access-group ip-access-list 1
exit
policy-map 1
class 1
police 500000 exceed-action policed-dscp-transmit 10
exit
exit

## 9.7 Configuring CoS-Based QoS

Follow the steps below to configure CoS-Based features such as default priority, scheduling and bandwidth.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan map-priority &lt;priority value(0-7)&gt; traffic-class &lt;Traffic class value(0-7)&gt;</td>
<td>Maps a priority to a traffic class in the switch. The frame received with the configured priority will be processed in the configured traffic class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Priority- Priority of the packet, in range of 0-7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Class –Traffic class in range of 0-7.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>(Optional) Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type – may be any of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fx-ethernet – fx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cx-ethernet – cx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-id is in slot/port format for all physical interfaces.</td>
</tr>
</tbody>
</table>
To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10

To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20

If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>switchport priority default &lt;priority value (0-7)&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Configures the default priority for the interface in range of 0-7.</td>
</tr>
</tbody>
</table>

| Step 5 | cosq scheduling algorithm { strict | rr | wrr | deficit } |
|--------|--------------------------------------------------|
|        | (Optional) Configures the QoS Egress queue scheduling algorithm. strict - strict rr - round robin wrr - weighted round robin (WRR) deficit – deficit WRR |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>traffic-class &lt;integer (0-7)&gt; weight &lt;integer (0-15)&gt; [ minbandwidth&lt;integer (64-16777152)&gt;] [maxbandwidth&lt;integer (64-16777152)&gt;]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Configures the egress queue minimum and maximum bandwidth. weight - Configures the queue weights in range of 0-15 minbandwidth - Configures the minimum bandwidth for the queue in range of 64-16777152 maxbandwidth - Configures the maximum bandwidth for the queue in range of 64-16777152</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>show vlan port config port [&lt;interface-type&gt;&lt;interface-id&gt;]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the port default priority configuration. show vlan traffic-classes</td>
</tr>
<tr>
<td></td>
<td>Display the traffic class and egress queue mapping.</td>
</tr>
</tbody>
</table>

The “no cosq scheduling algorithm” resets the CoS queue scheduling algorithm configuration to its default value of strict.
The “no traffic-class <integer (0-7)> [weight] [minbandwidth] [maxbandwidth]” command resets the minimum/maximum bandwidth configuration to its default value of 0 and weight to 1.
The “no switchport priority default” command resets the default priority configuration to its default value of 0.
The “no vlan map-priority <priority value (0-7)>” command resets the egress CoS queue mapping to its default value.

The example below shows the commands used to configure QoS default priority, scheduling and bandwidth.

**Example 1: Default Priority**

SMIS# configure terminal

SMIS(config)# interface Fx 0/10

SMIS(config-if)# switchport priority default 5

SMIS(config-if)# end

SMIS# show vlan port config port Fx 0/10

Vlan Port configuration table

-------------------------------
Port                                          Fx 0/10
Port Vlan ID                                  1
Port Access Vlan ID                            1
Port Acceptable Frame Type                    Admit All
Port Ingress Filtering                        Disabled
Port Mode                                     Hybrid
Port Gvrp Status                              Disabled
Port Gmrp Status                              Disabled
Port Gvrp Failed Registrations                0
Gvrp last pdu origin                          00:00:00:00:00:00
Port Restricted Vlan Registration            Disabled
Port Restricted Group Registration           Disabled
Mac Based Support                             Disabled
Port-and-Protocol Based Support               Enabled
Default Priority : 5
Filtering Utility Criteria : Default
Allowed Vlans on Trunk : 1-4069
Trunk Native Vlan Id : 0
-------------------------------------------------------

Example 2: Scheduling
The example below shows the commands used to configure the QoS scheduling algorithm.

SMIS# configure terminal
SMIS(config)# set qos enable
SMIS(config)# interface Fx 0/8
SMIS(config-if)# cosq scheduling algorithm wrr
SMIS(config-if)# end
SMIS# show cosq algorithm
CoSq Algorithm

---------------

<table>
<thead>
<tr>
<th>Interface</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/2</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/6</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/7</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/8</td>
<td>WeightedRoundRobin</td>
</tr>
<tr>
<td>Fx0/9</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/10</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/11</td>
<td>StrictPriority</td>
</tr>
</tbody>
</table>
Example 3: Egress Bandwidth

SMIS# configure terminal
SMIS(config)# set qos enable
SMIS(config)# interface Fx 0/15
SMIS(config-if)# traffic-class 6 weight 7 minbandwidth 6400 maxbandwidth 6400000
SMIS(config-if)# end
SMIS# show cosq weights-bw interface Fx 0/15
CoSq Weights and Bandwidths

---------------------------
<table>
<thead>
<tr>
<th>Interface</th>
<th>CoSqId</th>
<th>CoSqWeight</th>
<th>MinBw</th>
<th>MaxBw</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------</td>
<td>--------</td>
<td>------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>Fx0/12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fx0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cx0/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cx0/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cx0/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cx0/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example 4: Egress Queue

SMIS# configure terminal
SMIS(config)# vlan map-priority 2 traffic-class 7
SMIS(config)# end
SMIS# show vlan traffic-classes

Priority to Traffic Class Queue Mapping

<table>
<thead>
<tr>
<th>Priority</th>
<th>Traffic Class Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
10 Port Mirroring

Supermicro switches support Port Mirroring function. Users can configure the Port mirroring session(s) to provide a method to monitor networking traffic flow on another port.

Port mirroring feature allow user to configure up to 4 independent sessions. Each session will have one destination port and as many source ports as available in the Switch. Networking traffic flowing in any direction for the source ports(s), being transmit only, receive only or both transmit and receive, will be monitored, or mirroring at the destination port.

10.1 Port Mirroring Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port mirroring</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring direction</td>
<td>Both</td>
</tr>
</tbody>
</table>

10.2 Configure Port Mirroring in CLI

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>Monitor session &lt;session number: 1-4&gt; destination interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Configure Port Mirroring. session_number – 1, indicates only one session is supported. Destination – Monitoring Port. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id – is in slot/port format for all physical interfaces. NOTE: Source and Destination port cannot be same.</td>
</tr>
</tbody>
</table>
| Step 3 | Monitor session <session number: 1-4> source interface <interface-type> <interface-id> {rx } tx | Configure Port Mirroring. session_number – 1, indicates only one session is supported.
Source – Monitored Port.

interface-type – may be any of the following:
fx-ethernet – fx
cx-ethernet – cx

interface-id – is in slot/port format for all physical interfaces.

rx – Packets received on source port are monitored (Ingress).

tx – Packets transmitted on source port are monitored (Egress).

both – Packets received and transmitted on source port are monitored.

NOTE: Source and Destination port cannot be same.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>End</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>show port-monitoring</td>
<td>Displays the port monitoring configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The following command in Switch configuration mode is used to configure a session of mirroring for one unique source port to one destination port. The source port has to be unique, because once the source port is used in one session, it can not be used in another session, unless the port is removed first. Destination port does not have this restriction.

The mirroring action is carried out only when both destination port and source port(s) are in place for the same session. Hence, the execution to carry out a mirroring action generally is composed of these commands.

The first command will establish the mirroring session with the destination port. The interface-id is the port that user wanted to be mirrored to, with format of example like fx 0/1, cx 0/1, cx 0/23 ...

The second command will establish the other half of the mirroring action, in which the session, if it is the same as the session of the previous destination port command, will mirror traffic from the source port <interface-id>, with direction of ingress (Rx), egress (Tx) or both. If direction is not given, then both is the default direction.

In CLI, user can only add one source port at a time to any session.

In the same session, user’s new command for direction of same port, will overwrite the previous configuration of the same source port.
Once the source port is used in a session, to use it in another session, user needs to remove the source port first. If not, the recently input source port will overwrite the previous source port.

The "no monitor session [session_number:1-4] destination interface <interface-type> <interface id>" command delete the destination port mirroring.

The "no monitor session [session_number:1-4] source interface <interface-type> <interface-id>" command deletes the source port mirroring.

Note that in the command to remove the source port, there is no provision for the direction field {rx, tx, both}.

The example below shows the commands used to configure Port Mirroring.

SMIS# configure terminal
SMIS(config)# monitor session destination interface fx 0/48
SMIS(config)# monitor session source interface fx 0/22
SMIS(config)# monitor session source interface fx 0/23
SMIS(config)# monitor session source interface fx 0/24
SMIS(config)# monitor session source interface fx 0/25
SMIS(config)# end

SMIS# show port-monitoring

Port Monitoring is enabled
Monitor Port : Fx0/48

<table>
<thead>
<tr>
<th>Port</th>
<th>Ingress-Monitoring</th>
<th>Egress-Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/2</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/6</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/7</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/8</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/9</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/10</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/11</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/12</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/13</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/14</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/16</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/17</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Fx0/18</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/19</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/20</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/21</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/22</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Fx0/23</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Fx0/24</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Fx0/25</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Fx0/26</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/27</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/28</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/29</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/30</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/31</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/32</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/33</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/34</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/35</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/36</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/37</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/38</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/39</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/40</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/41</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/42</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/43</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/44</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/45</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/46</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/47</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Fx0/48</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cx0/1</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cx0/2</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cx0/3</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Cx0/4</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
11 SNMP

SNMP helps to monitor and manage the switches from network management systems (NMS). SNMP solutions contain three major components – SNMP manager, SNMP agent and MIB (Management Information Base) as shown in Figure – SNMP-1.

The SNMP MIB contains all the configuration and status information of the switch. MIB is organized in a tree structure with branches and leaf nodes. Each node contains an object of information and is identified with an object identifier (OID). SNMP MIB is stored and maintained in the switch.

The SNMP agent also resides on the switch. It processes the SNMP requests received from the SNMP manager. It sends responses to SNMP managers by retrieving required information from the MIB. It also updates the MIB based on SNMP messages sent by the SNMP managers. SNMP agents also send voluntary traps to SNMP managers. Traps are sent to alert the SNMP managers on events happening on the switch.

The SNMP manager is an NMS application. It monitors and manages switches by communicating to the SNMP agents running on the switch. The SNMP manager application provides command or graphical interfaces to the network administrators to help them manage the networks.

There are three versions of SNMP protocols available.

USM (User based Security Model) and VACM (View based Access Control Model) are the main features in SNMPv3. USM provides user authentication and message encryption. VACM provides MIB access control by associating views and users.
SNMPv3 uses a combination of security model and security level to define switch access. Security model specifies the authentication mechanism for the user and the group to which the user belongs. The security models in the Supermicro switch are v1, v2c and v3.

Security level specifies the permitted security within the particular security model. The security levels in Supermicro switches are

- NoAuthNoPriv
- AuthNoPriv
- AuthPriv

The security model and level combinations possible in Supermicro switch are listed in the table below.

<table>
<thead>
<tr>
<th>Security Model</th>
<th>Security Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>None</td>
<td>Community string and community user are used to authenticate user login.</td>
</tr>
<tr>
<td>V2c</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>None</td>
<td>Community string and community user are used to authenticate user login.</td>
</tr>
<tr>
<td>V3</td>
<td>noAuthNoPriv</td>
<td>User name</td>
<td>None</td>
<td>User configuration is used to authenticate user login.</td>
</tr>
<tr>
<td>V3</td>
<td>Auth</td>
<td>MD5 or SHA</td>
<td>None</td>
<td>MD5 or SHA algorithm is used to verify user login.</td>
</tr>
<tr>
<td>V3</td>
<td>Priv</td>
<td>None</td>
<td>DES</td>
<td>DES is used to encrypt all SNMP messages.</td>
</tr>
</tbody>
</table>

SNMP uses multiple messages between managers and agents. The below table describes the SNMP messages.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Originator</th>
<th>Receiver</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Manager</td>
<td>Agent</td>
<td>To get the value of a particular MIB object</td>
</tr>
<tr>
<td>get-next-request</td>
<td>Manager</td>
<td>Agent</td>
<td>To get the value of the next object in a table</td>
</tr>
<tr>
<td>get-bulk-request</td>
<td>Manager</td>
<td>Agent</td>
<td>To get the values of multiple MIB objects in one transaction</td>
</tr>
<tr>
<td>get-response</td>
<td>Agent</td>
<td>Master</td>
<td>Response for get-request, get-next-request and get-bulk-request messages.</td>
</tr>
<tr>
<td>set-request</td>
<td>Manager</td>
<td>Agent</td>
<td>To set the value of a particular MIB object</td>
</tr>
<tr>
<td>Trap</td>
<td>Agent</td>
<td>Master</td>
<td>To notify the events occurring on agents</td>
</tr>
<tr>
<td>Inform</td>
<td>Agent</td>
<td>Master</td>
<td>To guarantee delivery of traps to Manager</td>
</tr>
</tbody>
</table>

### 11.1 SNMP Support

Supermicro switches support three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3.

A switch supports 50 users, 50 groups, 50 views and 50 views.
11.2 Interface Numbers
IF-MIB contains information about all the interfaces on the switch. Users can access the interface specific MIB object values using interface index (ifIndex) numbers. The ifIndex numbers are assigned by switch software for every physical and logical interface. The table below shows ifIndex to interface mapping method.

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>ifIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 Gig physical interfaces</td>
<td>Starts from 1 and goes up to the maximum number of 25 Gig interfaces available on the switch. 1 to 48</td>
</tr>
<tr>
<td>100 Gig physical interfaces</td>
<td>Starts after 1Gig ifIndexes and goes up to the maximum number of 100 Gig interfaces available on the switch. 49 to 54</td>
</tr>
<tr>
<td>Port channel interfaces</td>
<td>Starts after 10Gig ifIndexes and goes up to the maximum number of port channel interfaces supported on the switch. 53 to 108</td>
</tr>
<tr>
<td>Management IP interfaces</td>
<td>109</td>
</tr>
</tbody>
</table>

11.3 SNMP Configuration
SNMP Configuration involves configuring user, group, access, view, community etc.

SNMP Users: SNMP users have a specified username, authentication password, privacy password, (if required) and authentication and privacy algorithms to use.

SNMP Groups: When a user is created, it is associated with an SNMP group. SNMPv3 groups are the means by which users are assigned their views and access control policy.

SNMP View: An SNMP MIB view is a defined list of objects within the MIB that can be used to control what parts of the MIB can be accessed by users belonging to the SNMP group that is associated with that particular view. When you want to permit a user to access a MIB view, you include a particular view. When you want to deny a user access to a MIB view, you exclude a particular view.

SNMP Group access: An SNMP group access is essentially an access control policy to which users can be added. Each SNMP group is configured with a security level, and is associated with an SNMP view.

There are three possible types of access that can be configured for the users in that SNMP group to have access to an SNMP view.

- ReadView - Specifies Read access for an SNMP view
- WriteView - Specifies Write access for an SNMP view
- NotifyView - Specifies SNMP view for which the group will receive notifications.
The figure below shows the relationship between the various SNMP tables: User, group, access and view.

![SNMP Relationships Diagram]

**Figure SNMP-2: SNMP - Relationships**

The following mapping can exist between the SNMP tables user, group, access and view:

- Multiple users can belong to one group
- An user can belong to multiple groups.
- Multiple groups can be associated with a view.
- Multiple views can be created.
- More than one group can be associated with a particular view.
- More than one view can be associated with a group. For instance, a group can have read access to the entire MIB, but write access only for certain MIB objects.

### 11.3.1 Configuration Steps

The sequence of steps for SNMP Configuration in Supermicro switches are:

1. Create a **User** Name
2. Create a **community** name and associate user with the community (Optional).
3. Create a **group** and associate the user name with the group name.
4. The **view** is then defined to include or exclude whole/part MIB sub trees.
5. Define type of **access** for each group for a view.
6. Finally, **traps** can be defined based on the User Name (Optional).

### 11.4 SNMP Defaults

<table>
<thead>
<tr>
<th>Function</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Agent Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMP Sub-Agent Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Engine Id</td>
<td>80.00.08.1c.04.46.53</td>
</tr>
<tr>
<td>Communities</td>
<td>PUBLIC, NETMAN</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Users</td>
<td>initial, TemplateMD5, TemplateSHA</td>
</tr>
<tr>
<td>Authentication</td>
<td>initial : none TemplateMD5: MD5 TemplateSHA: SHA</td>
</tr>
<tr>
<td>Privacy</td>
<td>initial : none TemplateMD5: none TemplateSHA: DES</td>
</tr>
<tr>
<td>Groups</td>
<td>iso, initial</td>
</tr>
<tr>
<td>Access</td>
<td>iso, initial</td>
</tr>
<tr>
<td>View (for default groups)</td>
<td>iso: iso, initial: restricted</td>
</tr>
<tr>
<td>Notify View Name</td>
<td>iss, iss1</td>
</tr>
<tr>
<td>Read, Write, Notify</td>
<td>Iso</td>
</tr>
<tr>
<td>Target Parameters</td>
<td>Internet, test1</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Volatile</td>
</tr>
<tr>
<td>Context</td>
<td>None</td>
</tr>
<tr>
<td>SNMP Port</td>
<td>161</td>
</tr>
<tr>
<td>SNMP Trap Port</td>
<td>162</td>
</tr>
<tr>
<td>Trap Status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Authentication Trap</td>
<td>Disabled</td>
</tr>
<tr>
<td>Link-State Trap</td>
<td>Enabled</td>
</tr>
<tr>
<td>Switch Name</td>
<td>SMIS</td>
</tr>
<tr>
<td>System Contact</td>
<td><a href="http://www.supermicro.com">http://www.supermicro.com</a></td>
</tr>
<tr>
<td>System Location</td>
<td>Supermicro</td>
</tr>
</tbody>
</table>

# 11.5 Enable/Disable the SNMP Agent

The SNMP Agent is enabled by default in Supermicro switches.

Follow the steps below to disable the SNMP agent.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>disable snmpagent</td>
<td>Disables the SNMP agent</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
Step 4 | **write startup-config** | Optional step – saves this SNMP configuration to be part of the startup configuration.

---

The “enablesnmpagent” command enables the SNMP agent.

To enable the SNMP agent, it must be in the disabled state.

The examples below show ways to disable/enable the SNMP agent function on Supermicro switches.

**Disable the SNMP agent.**

SMIS# configure terminal  
SMIS(config)# disable snmpagent  
SMIS(config)# end

**Enable the SNMP agent.**

SMIS# configure terminal  
SMIS(config)# enable snmpagent  
SMIS(config)# end

11.5.1 Switch Name
Supermicro switches can be assigned a name for identification purposes. The default switch name is SMIS. The switch name is also used as a prompt.

Follow the steps below to configure the switch name.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | device name <devname(15)> | Configures switch name and prompt.  
Devname – Switch name specified with 1-15 alphanumeric characters. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show system information | Displays the system information configuration. |
| Step 5 | write startup-config | Optional step – saves this configuration to be part of the startup configuration. |

The device name configuration is automatically stored as part of the startup configuration file.
The example below shows the commands used to configure the switch name.

```
SMIS# configure terminal
SMIS(config)# device name switch1
switch1(config)# end
```

```
switch1# show system information
Switch Name: switch1
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 1 mins 11 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
   =============== ===== ======
   Key # Key
   ================
Time zone offset not set
```

### 11.5.2 Switch Contact

Supermicro switches provide an option to configure the switch in charge Contact details, usually an email ID.

Follow the steps below to configure the switch contact.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>system contact &lt;string - to use more than one word, provide the string within double quotes&gt;</td>
<td>Configures the switch contact. String – Contact information entered as a String of maximum length 256.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the system information configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
The Switch contact configuration is automatically stored as part of the startup configuration file.

The example below shows the commands used to configure a switch contact.

```
SMIS# configure terminal
SMIS(config)# system contact "User1 at CA"
SMIS(config)# end

SMIS# show system information
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: User1 at CA
System Location: Supermicro
 Logging Option: Console Logging
 Login Authentication Mode: Local
 Snoop Forward Mode: MAC based
 Config Restore Status: Not Initiated
 Config Restore Option: No restore
 Config Restore Filename: iss.conf
 Config Save IP Address: 0.0.0.0
 Device Up Time: 0 days 0 hrs 50 mins 51 secs
 Boot-up Flash Area: Normal
 NTP Broadcast Mode: No
 [NTP] ntp is disabled
 Server Key Prefer
 ============ =======
 Key # Key
 =========== ===========
 Time zone offset not set
```

### 11.5.3 System Location
Supermicro switches provide an option to configure the switch location details.

Follow the steps below to configure system location.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>system location &lt;location name&gt;</td>
<td>Configures the system location.</td>
</tr>
</tbody>
</table>
The example below shows the commands used to configure system location.

SMIS# configure terminal
SMIS(config)# system location "Santa Clara"
SMIS(config)# end

SMIS# show system information
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com
System Location: Santa Clara
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Supermicro L2/L3 Switches Configuration Guide 43
Device Up Time: 0 days 0 hrs 51 mins 39 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTPI] ntp is disabled
Server Key Prefer

Time zone offset not set

11.6 Access Control

There are various parameters that control access to the SNMP Agent.
11.6.1 Engine Identifier

The SNMP Engine Identifier is a unique identifier for the SNMP agent in a switch. It is used with a hashing function in the agent to generate keys for authentication and encryption. Hence after any change in the Engine Identifier, the following must be re-configured:

- SNMPv3 authentication
- SNMPv3 encryption/privacy
- Community

Follow the steps below to configure the SNMP Engine Identifier.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmpengineid&lt;EngineIdentifier&gt;</td>
<td>Configures the SNMP Engine Identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>EngineIdentifier</em>-Hexadecimal number, with length between 5 and 32 octets. Each octet should be separated by a period.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show snmpengineID</td>
<td>Displays the SNMP engine Identifier information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure the SNMP Engine Identifier.

```
SMIS# configure terminal
SMIS(config)# snmpengineid 80.00.08.1c.44.44
SMIS(config)# end

SMIS# show snmpengineid

EngineId: 80.00.08.1c.44.44
```

The “no snmpengineid” command resets the SNMP engineid to its default value of 80.00.08.1c.04.46.53.
11.6.2 Community

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

The SNMP v1/v2 community is also used as a form of security. The community of SNMP managers that can access the agent MIB in the switch is defined by a community string.

Follow the steps below to configure an SNMP community.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp community index &lt;CommunityIndex&gt; name &lt;CommunityName&gt; security &lt;SecurityName&gt; [context &lt;name&gt;] [{volatile</td>
<td>nonvolatile}] [transporttag&lt;TransportTagIdentifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CommunityIndex—Alphanumeric value with a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CommunityName—Alphanumeric value with a maximum of 64 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SecurityName—This is the user name associated with the community. Alphanumeric value with a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name—Alphanumeric value with a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TransportTagIdentifier—Identifies the transport end points between agent and manager. Alphanumeric value with a maximum of 64 characters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show snmp community</td>
<td>Displays the SNMP community information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step—saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no snmp community index <CommunityIndex>” command deletes the specified community index.

SNMP User Name is also referred to as SNMP Security Name in Supermicro switches.
The example below shows the commands used to configure the SNMP community.

SMIS(config)# snmp community index test1 name test1 security user1 nonvolatile

SMIS(config)# show snmp community

Community Index: NETMAN
Community Name: NETMAN
Security Name: none
Context Name:
Transport Tag:
Storage Type: Volatile
Row Status: Active

Community Index: PUBLIC
Community Name: PUBLIC
Security Name: none
Context Name:
Transport Tag:
Storage Type: Volatile
Row Status: Active

Community Index: test1
Community Name: test1
Security Name: user1
Context Name:
Transport Tag:
Storage Type: Non-volatile
Row Status: Active

11.6.3 User
SNMP user configuration is used only for SNMPv3. An SNMP user requests and receives information about switch status and traps.

Follow the steps below to configure an SNMP user.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | snmp user <UserName> [auth {md5 | sha} <passwd>][priv DES <passwd>]][(volatile | nonvolatile)] | Configures the SNMP user, authentication and encryption.  
*UserName* - Alphanumeric value with a maximum of 32 characters.  
Use auth to enable authentication for the user. |
Passwd—Password used for user Authentication. Alphanumeric value with a maximum of 32 characters.

Use priv to enable encryption of packets.

Passwd—Password used to generate keys for encryption of messages. Alphanumeric value with a maximum of 40 characters.

Use volatile if the value need not be stored in NVRAM.

Use nonvolatile if the value must be stored in NVRAM and available after restart.

Step 3  **end**  Exits the configuration mode.

Step 4  **show snmp user**  Displays the SNMP user information.

Step 5  **write startup-config**  Optional step – saves this SNMP configuration to be part of the startup configuration.

The "no snmp user <UserName>" command deletes the specified user.

---

The example below shows the commands used to configure the SNMP user.

```
SMIS# configure terminal
SMIS(config)# snmp user user5 auth md5 abc123 priv DES xyz123
SMIS# end

SMIS# show snmp user

Engine ID: 80.00.08.1c.04.46.53
User: user5
Authentication Protocol: MD5
Privacy Protocol: DES_CBC
Storage Type: Volatile
Row Status: Active

Engine ID: 80.00.08.1c.04.46.53
```
User: initial
Authentication Protocol: None
Privacy Protocol: None
Storage Type: Volatile
Row Status: Active

-----------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateMD5
Authentication Protocol: MD5
Privacy Protocol: None
Storage Type: Volatile
Row Status: Active

-----------------------------
Engine ID: 80.00.08.1c.04.46.53
User: templateSHA
Authentication Protocol: SHA
Privacy Protocol: DES_CBC
Storage Type: Volatile
Row Status: Active

-----------------------------

11.6.4 Group
A group identifies a set of users in SNMPv3.

Follow the steps below to configure an SNMP group.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp group &lt;GroupName&gt; user &lt;UserName&gt; security-model {v1</td>
<td>v2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>GroupName</strong> – Alphanumeric value with a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Security-model</strong> – Use v1 or v2c or v3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>UserName</strong> - Alphanumeric value with a maximum of 32 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use <strong>volatile</strong> if the value need not be stored in NVRAM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use <strong>nonvolatile</strong> if the value must be stored in NVRAM and available after restart.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show snmp group</td>
<td>Displays the SNMP group information.</td>
</tr>
</tbody>
</table>
Step 5  **write startup-config**  Optional step – saves this SNMP configuration to be part of the startup configuration.

The “no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3}” command deletes the specified group.

The example below shows the commands used to configure the SNMP group.

```
SMIS# configure terminal
SMIS(config)# snmp group group5 user user5  security-model v3
SMIS# end

SMIS# show snmp group

Security Model: v1
Security Name: none
Group Name: iso
Storage Type: Volatile
Row Status: Active

Security Model: v2c
Security Name: none
Group Name: iso
Storage Type: Volatile
Row Status: Active

Security Model: v3
Security Name: user5
Group Name: group5
Storage Type: Volatile
Row Status: Active

Security Model: v3
Security Name: initial
Group Name: initial
Storage Type: Non-volatile
Row Status: Active

Security Model: v3
Security Name: templateMD5
Group Name: initial
Storage Type: Non-volatile
Row Status: Active
```
11.6.5  View
A view specifies limited access to MIBs. A view can be associated with one or many groups.

In an SNMP, parameters are arranged in a tree format. SNMP uses an Object Identifier (OID) to identify the exact parameter in the tree. An OID is a list of numbers separated by periods.

Follow the steps below to configure the SNMP view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmpview &lt;ViewName&gt;&lt;OIDTree&gt; [mask &lt;OIDMask&gt;] {included</td>
<td>excluded} {[volatile</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show snmpviewtree</td>
<td>Displays the SNMP view information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
The “no snmp view <ViewName><OIDTree>” command deletes the specified SNMP view.

The example below shows the commands used to configure the SNMP view.

SMIS(config)# snmp view view1 1.3.6.1 included

SMIS(config)# show snmpviewtree

View Name: iso
Subtree OID: 1
Subtree Mask: 1
View Type: Included
Storage Type: Non-volatile
Row Status: Active

View Name: view1
Subtree OID: 1.3.6.1
Subtree Mask: 1.1.1.1
View Type: Included
Storage Type: Volatile
Row Status: Active

View Name: Restricted
Subtree OID: 1
Subtree Mask: 1
View Type: Excluded
Storage Type: Non-volatile
Row Status: Active

11.6.6 Group Access
Group access defines the access policy for a set of users belonging to a particular group. Group access is used only for SNMPv3.

Follow the steps below to configure SNMP group access.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp access &lt;GroupName&gt; {v1</td>
<td>v2c</td>
</tr>
</tbody>
</table>

GroupName - Alphanumeric value with a maximum of 40 characters.

Security model – Mention one of v1, v2c or v3.
Use `auth` to enable authentication for the user.

Use `priv` to enable encryption of packets.

**ReadView** - View name that specifies read access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters.

**WriteView** - View name that specifies write access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters.

**NotifyView** - View name that specifies a particular MIB sub-tree used in notification. Alphanumeric value with a maximum of 40 characters.

Use `volatile` if the value need not be stored in NVRAM.

Use `nonvolatile` if the value must be stored in NVRAM and available after restart.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>show snmp group access</td>
<td>Displays the SNMP group access information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this SNMP configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

Group, user and view should be created before configuring group access.

The “`no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}`” command deletes the specified SNMP group access.

The sequence of steps to delete a group that is associated with a group access and view:

1. Delete the view
2. Delete the group access.
3. Delete the group.

The example below shows the commands used to configure the SNMP group access.
SMIS# configure terminal
SMIS(config)# snmp access group5 v3 auth read view1 write view2 notify none nonvolatile
SMIS(config)# end

SMIS# show snmp group access

Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Volatile
Row Status: Active

Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Volatile
Row Status: Active

Group Name: group5
Read View: view1
Write View: view2
Notify View: 
Storage Type: Non-volatile
Row Status: Active

Group Name: Initial
Read View: Restricted
Write View: Restricted
Notify View: Restricted
Storage Type: Non-volatile
Row Status: Active

Group Name: Initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Non-volatile
Row Status: Active

Group Name: initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Non-volatile
Row Status: Active
### 11.7 Trap

#### 11.7.1 Target Address

A target is a receiver of SNMP notification(s), which are usually SNMP Managers. The target address defines the transport parameters of the receivers.

Follow the steps below to configure the SNMP Target address.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmpTargetAddr&lt;TargetAddressName&gt;param&lt;ParamName&gt; {&lt;IPAddress&gt;</td>
<td>&lt;IP6Address&gt;} [timeout &lt;Seconds(1-1500)] [retries &lt;RetryCount(1-3)] [taglist&lt;TagIdentifier</td>
</tr>
</tbody>
</table>

**TargetAddressName** - Alphanumeric value with a maximum of 32 characters.

**ParamName** – The parameter to be notified to the specific target. Alphanumeric value with a maximum of 32 characters.

**IPAddress** – IPv4 address of the target.

**IP6Address** – IPv6 address of the target.

**Seconds** – Specifies the timeout within which the target should be reachable.

**RetryCount** – Specifies the number of retries to reach the target.

**TagIdentifier** - A set of targets can be grouped under a tag Identifier.

Use **volatile** if the value need not be stored in NVRAM.
Use **nonvolatile** if the value must be stored in NVRAM and available after restart.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td><strong>show snmptargetaddr</strong></td>
<td>Displays the SNMP target address information.</td>
</tr>
<tr>
<td>5</td>
<td><strong>write startup-config</strong></td>
<td>Optional step – saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no snmptargetaddr<TargetAddressName>” command deletes the specified SNMP target address information.

The example below shows the commands used to configure the SNMP target address.

```
SMIS# configure terminal
SMIS(config)# snmptargetaddr host1 param param1 192.168.1.10 taglist tg1
SMIS# end
```

```
SMIS# show snmptargetaddr
Target Address Name: host1
IP Address: 192.168.1.10
Tag List: tg1
Parameters: param1
Storage Type: Volatile
Row Status: Active
```

### 11.7.2 Target Parameters

Target parameters define the MIB objects that should be notified to an SNMP target, usually an SNMP manager.

Follow the steps below to configure SNMP target parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>configure terminal</strong></td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>**snmptargetparams&lt;ParamName&gt; user &lt;UserName&gt;security-model {v1</td>
<td>v2c</td>
</tr>
</tbody>
</table>
noauth | priv}message-processing {v1 | v2c | v3} [(volatile | nonvolatile)]

**ParamName**
The parameter to be notified. Alphanumeric value with a maximum of 32 characters.

**UserName** - Alphanumeric value with a maximum of 32 characters.

Security model – Use one of v1, v2c, v3.

Use **auth** to enable authentication for the user.

Use **priv** to enable encryption of packets.

Message processing - Specifies the SNMP version for sending/receiving the parameter via a notification message.

Use **volatile** if the value need not be stored in NVRAM.

Use **nonvolatile** if the value must be stored in NVRAM and available after restart.

---

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><strong>show snmptargetparam</strong></td>
<td>Displays the SNMP target parameters information.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>write startup-config</strong></td>
<td>Optional step – saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

---

The “**no snmptargetparams<ParamName>**” command deletes the specified SNMP target parameters information.

The example below shows the commands used to configure the SNMP target parameters.

```plaintext
SMIS# configure terminal
SMIS(config)# snmptargetparams param4 user user4 security-model v2c message-processing v2c
SMIS# end

SMIS# show snmptargetparam

Target Parameter Name: Internet
```
Message Processing Model: v2c
Security Model: v2c
Security Name: None
Security Level: No Authentication, No Privacy
Storage Type: Volatile
Row Status: Active

-------------------------------
Target Parameter Name: param4
Message Processing Model: v2c
Security Model: v2c
Security Name: user4
Security Level: No Authentication, No Privacy
Storage Type: Volatile
Row Status: Active

-------------------------------
Target Parameter Name: test1
Message Processing Model: v2c
Security Model: v1
Security Name: None
Security Level: No Authentication, No Privacy
Storage Type: Volatile
Row Status: Active

-------------------------------

11.7.3 SNMP Notify

Notify is used to specify the type of notifications to be sent to particular targets that are grouped under a particular tag.

Follow the steps below to configure the SNMP Notification.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp notify &lt;NotifyName&gt; tag &lt;TagName&gt; type {Trap</td>
<td>Inform}{{volatile</td>
</tr>
</tbody>
</table>

- **NotifyName**: Alphanumeric value with a maximum of 32 characters.
- **TagName**: Specifies a group of targets identified by this name. Alphanumeric value with a maximum of 32 characters.
- **Type**: Notification can be Trap or Inform.
Use **volatile** if the value need not be stored in NVRAM.

Use **nonvolatile** if the value must be stored in NVRAM and available after restart.

<table>
<thead>
<tr>
<th>Step 3</th>
<th><strong>end</strong></th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><strong>show snmp notify</strong></td>
<td>Displays the SNMP notification information and Inform statistics.</td>
</tr>
<tr>
<td></td>
<td><strong>show snmp inform statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>write startup-config</strong></td>
<td>Optional step – saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no snmp notify <NotifyName>” command deletes the specified SNMP notification.

The example below shows the commands used to configure the SNMP notification.

```
SMIS# configure terminal
SMIS(config)# snmp notify PUBLIC tag tag1 type trap nonvolatile
SMIS(config)# end

SMIS# show snmpnotify

Notify Name: PUBLIC
Notify Tag: tag1
Notify Type: trap
Storage Type: Non-volatile
Row Status: Active

-----------------------------

Notify Name: iss
Notify Tag: iss
Notify Type: trap
Storage Type: Volatile
Row Status: Active

-----------------------------

Notify Name: iss1
Notify Tag: iss1
Notify Type: trap
Storage Type: Volatile
Row Status: Active

-----------------------------
```
11.7.4 Trap UDP Port

The default UDP port for traps is 162. Supermicro switches provide an option for users to change this trap UDP port.

Follow the steps below to configure the SNMP UDP port for traps.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server trap udp-port &lt;port&gt;</td>
<td>Configures the SNMP UDP port for traps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port—UDP port for traps in the range 1 – 65535.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show snmp-server traps</td>
<td>Displays the SNMP traps information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step — saves this SNMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no snmp-server trap udp-port” command resets the SNMP UDP port to its default value of 162.

The example below shows the commands used to configure the SNMP UDP port for traps.

```
SMIS# configure terminal
SMIS(config)# snmp-server trap udp-port 170
SMIS(config)# end

SMIS(config)# show snmp-server traps

SNMP Trap Listen Port is 170
Currently enabled traps:
------------------------
linkup, linkdown,
Login Authentication Traps DISABLED.
```

11.7.5 Authentication Traps

Traps can be generated when a user login authentication fails at the SNMP agent. In Supermicro switches, authentication traps are disabled by default.

Follow the steps below to enable an SNMP authentication trap.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
### Step 1
**configure terminal**
Enters the configuration mode.

### Step 2
**snmp-server enable traps snmp authentication**
Enables the SNMP authentication traps.

### Step 3
**end**
Exits the configuration mode.

### Step 4
**show snmp**
Displays the SNMP information.

### Step 5
**write startup-config**
Optional step – saves this SNMP configuration to be part of the startup configuration.

---

The **"no snmp-server enable traps snmp authentication"** command disables SNMP authentication traps.

---

The example below shows the commands used to enable the SNMP authentication traps.

```
SMIS# configure terminal
SMIS(config)# snmp-server enable traps snmp authentication
SMIS# end
SMIS(config)# show snmp
```

SNMP Trap Listen Port is 162
Currently enabled traps:
------------------------
linkup,linkdown,
Login Authentication Traps ENABLED.

---

### 11.7.6 Link-State Trap

Link-state traps are enabled for all interfaces by default in Supermicro switches. Traps are generated when an interface toggles its state from Up to down or vice-versa.

Follow the steps below to disable SNMP Link-state trap.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>interface &lt;interface-type&gt;&lt;interface-id&gt;</strong>&lt;br&gt;or&lt;br&gt;<strong>interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</strong></td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the
following:

fx-ethernet – fx  
cx-ethernet – cx  
port-channel - po

interface-id is in slot/port format for all physical interfaces.

To configure multiple interfaces, use the “interface range …” command.

To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10

To provide multiple interfaces or ranges, separate with a comma (,).  
E.g.: int range fx 0/1-10, fx 0/20

If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>no snmp trap link-status</th>
<th>Enables the SNMP link-state trap on the particular interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show snmp</td>
<td>Displays the SNMP information.</td>
</tr>
</tbody>
</table>

| Step 6 | write startup-config | Optional step – saves this SNMP configuration to be part of the startup configuration. |
The “snmp trap link-status” command enables SNMP link-state traps.

The example below shows the commands used to disable the SNMP Link-state trap.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/21
SMIS(config-if)# no snmp trap link-status
SMIS(config-if)# end

SMIS# show interface Fx 0/21

Fx0/21 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port

Hardware Address is 00:30:48:e3:04:89
MTU 1500 bytes, Full duplex, 1 Gbps, Auto-Negotiation
HOL Block Prevention enabled.
Input flow-control is off, output flow-control is off

Link Up/Down Trap is disabled

Reception Counters
- Octets: 753
- Unicast Packets: 0
- Broadcast Packets: 0
- Multicast Packets: 9
- Pause Frames: 0
- Undersize Frames: 0
- Oversize Frames: 0
- CRC Error Frames: 0
- Discarded Packets: 0
- Error Packets: 0
- Unknown Protocol: 0

Transmission Counters
- Octets: 9043
- Unicast Packets: 0
- Non-Unicast Packets: 74
- Pause Frames: 0
- Discarded Packets: 0
- Error Packets: 0
```

11.8 SNMPConfigurationExample

PC – SNMP Manager       Switch – SNMP Agent
Configure the following requirements on a switch acting as an SNMP agent as shown above in Figure SNMP-2.

1) Creates SNMP users
   a. Create an SNMP user ‘user1’ Specify the authentication and privacy protocol and the authentication and privacy passwords.
   b. Creates an SNMP user ‘user2’. Specify the authentication protocol and password.
2) Creates SNMP groups
   a. Create group called superusers and associate user1 with this group.
   b. Create group called generalusers and associate user1 with this group.
3) Create views
   a. Creates an SNMP view ‘full’ which will allow access to everything from the specified Object Identifier
   b. Creates an SNMP view ‘restricted’ which will allow access to everything from the specified OID onwards, and also adds a restriction to anything on a particular sub-tree.
4) Create group access
   a. Access for superusers- fullread/write and notify privilege to the ‘full’ view
   b. Access for generalusers- full read, notify privilege to the ‘full’ view and, restricted write
5) Display all configuration

SMIS# configure terminal
SMIS(config)# snmp user user1 auth md5 pwd1
SMIS(config)# snmp user user2 auth sha abcd priv deS 1b12
SMIS(config)# snmp group superuser user user1 security-model v3 volatile
SMIS(config)# snmp group generalusers user user2 security-model v3 volatile
SMIS(config)# snmp view full 1.3.6.1 included volatile
SMIS(config)# snmp view restricted 1.3.6.1 included volatile
SMIS(config)# snmp view restricted 1.3.6.3.10.2.1 excluded volatile
SMIS(config)# snmp access superuser v3 auth read full write full notify full
SMIS(config)# snmp access generalusers v3 noauth read full write restricted notify full
SMIS(config)# end

SMIS# show snmp user

Engine ID : 80.00.08.1c.04.46.53
User : user1
Authentication Protocol : MD5
Privacy Protocol : None
Storage Type : Volatile
Row Status : Active

--------------------
Engine ID : 80.00.08.1c.04.46.53
User : user2
Authentication Protocol : SHA
Privacy Protocol : DES_CBC
Storage Type : Volatile
Row Status : Active

--------------------
Engine ID : 80.00.08.1c.04.46.53
User : initial
Authentication Protocol : None
Privacy Protocol : None
Storage Type : Volatile
Row Status : Active

--------------------
Engine ID : 80.00.08.1c.04.46.53
User : templateMD5
Authentication Protocol : MD5
Privacy Protocol : None
Storage Type     : Volatile
Row Status       : Active

-----------------------------
Engine ID               : 80.00.08.1c.04.46.53
User                    : templateSHA
Authentication Protocol : SHA
Privacy Protocol        : DES_CBC
Storage Type            : Volatile
Row Status              : Active

-----------------------------
SMIS# show snmp group

Security Model : v1
Security Name  : none
Group Name     : iso
Storage Type   : Volatile
Row Status     : Active

-----------------------------
Security Model : v2c
Security Name  : none
Group Name     : iso
Storage Type   : Volatile
Row Status     : Active

-----------------------------
Security Model : v3
Security Name  : user1
Group Name : superuser
Storage Type : Volatile
Row Status : Active

--------------------------
Security Model : v3
Security Name : user2
Group Name : generalusers
Storage Type : Volatile
Row Status : Active

--------------------------
Security Model : v3
Security Name : initial
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

--------------------------
Security Model : v3
Security Name : templateMD5
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

--------------------------
Security Model : v3
Security Name : templateSHA
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

--------------------------
SMIS# `show snmp group access`

Group Name : iso
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Volatile
Row Status : Active

Group Name : iso
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Volatile
Row Status : Active

Group Name : initial
Read View : restricted
Write View : restricted
Notify View : restricted
Storage Type : Non-volatile
Row Status : Active

Group Name : initial
Read View : iso
Write View : iso
Notify View : iso
Storage Type: Non-volatile
Row Status: Active

-----------------------------
Group Name: initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Non-volatile
Row Status: Active

-----------------------------
Group Name: superuser
Read View: full
Write View: full
Notify View: full
Storage Type: Volatile
Row Status: Active

-----------------------------
Group Name: generalusers
Read View: full
Write View:
Notify View: full
Storage Type: Volatile
Row Status: Active

-----------------------------
SMIS# show snmp viewtree

View Name: iso
Subtree OID : 1
Subtree Mask : 1
View Type : Included
Storage Type : Non-volatile
Row Status : Active

----------------------------
View Name : full
Subtree OID : 1.3.6.1
Subtree Mask : 1.1.1.1
View Type : Included
Storage Type : Volatile
Row Status : Active

----------------------------
View Name : restricted
Subtree OID : 1
Subtree Mask : 1
View Type : Excluded
Storage Type : Non-volatile
Row Status : Active

----------------------------
View Name : restricted
Subtree OID : 1.3.6.1
Subtree Mask : 1.1.1.1
View Type : Included
Storage Type : Volatile
Row Status : Active

----------------------------
View Name : restricted
Subtree OID : 1.3.6.3.10.2.1
Subtree Mask : 1.1.1.1.1.1.1
View Type    : Excluded
Storage Type : Volatile
Row Status   : Active

---------------

SMIS# show running-config

Building configuration...

ID   Hardware Version                   Firmware    OS        Boot Loader
0    SSE-F3548                    1.0.0.0     6         0.0.0.0

vlan 1
  ports fx 0/1-24 untagged
  ports cx 0/1-3 untagged
  exit

snmp user user1 auth md5 AUTH_PASSWD volatile
snmp user user2 auth sha AUTH_PASSWD priv DES DES_CBC volatile
snmp group superuser user user1 security-model v3 volatile
snmp group generalusers user user2 security-model v3 volatile
snmp access superuser v3 auth read full write full notify full volatile
snmp access generalusers v3 noauth read full notify full volatile
snmp view full 1.3.6.1 included volatile
snmp view restricted 1.3.6.1 included volatile
snmp view restricted 1.3.6.3.10.2.1 excluded volatile
Remote monitoring (RMON) is a method similar to Simple Network Management Protocol (SNMP) and uses a client-server model to monitor/manager remote devices on the network. RMON and SNMP differ in the approach used:

- RMON is used for "flow-based" monitoring, while SNMP is often used for "device-based" management. The data collected in RMON deals mainly with traffic patterns rather than the status of individual devices as in SNMP.
- RMON is implemented based on SNMP. RMON sends traps to the management device to notify the abnormality of the alarm variables by using the SNMP trap mechanism. Traps in RMON and those in SNMP have different monitored targets, triggering conditions, and report contents.
- RMON provides an efficient means of monitoring subnets. The managed device sends a trap to the management device automatically once an alarm has reached a certain threshold value.
- Unlike SNMP, the management device need not get the values of MIB variables multiple times for comparison. Hence the communication traffic between the management device and the managed device is reduced.

RMON provides statistics and alarm functionality to monitor managed devices.

- The statistics function tracks traffic information on the network segments connecting to its ports. For e.g. number of oversize packets received.
- The alarm function aids in monitoring the value of a specified MIB variable. It also handles events such as trap or log to be sent to the management device when its value reaches a particular threshold. For e.g. rate of packets received reaches a certain value.

RMON protocol allows multiple monitors or management devices. A monitor provides two ways of data gathering:

- Using RMON probes from which Management devices can get data directly and control network resources. In this approach, management devices can obtain all RMON MIB information.
- RMON agents in routers and switches. Management devices exchange data with RMON agents using SNMP operations, which, due to system resources limitation, may not cover all MIB information but four groups of information, alarm, event, history, and statistics, in most cases.

Supermicro supports minimal RMON agent implementation for Ethernet interfaces.
12.1 RMON Groups

Supermicro supports four groups from RMON MIB1 defined by RMON specifications: event group, alarm group, history group and statistics group.

12.1.1 Alarm group

The RMON alarm group monitors specified alarm variables, such as total number of received packets on an interface. Once an alarm entry is defined, the switch checks the value of the monitored alarm variable at the specified interval. When the value of the monitored variable is greater than or equal to the upper threshold, an upper event is triggered; when the value of the monitored variable is smaller than or equal to the lower threshold, a lower event is triggered. The event is then handled as specified in the event group.

If the value of a specified alarm MIB variable fluctuates, then the rising alarm and falling alarm alternate i.e. only the first one triggers an alarm event.
12.1.2 Event Group
The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group. The events can be handled by either of the following ways:
- Logging event related information in the event log table of the RMON MIB of the switch.
- Trap: Sending a trap to notify the occurrence of this event to the management device.

12.1.3 Statistics
RMON statistics function is implemented by either the Ethernet statistics group or the history group. The objects of the statistics are different for both these groups; however both groups record statistics on the interfaces as a cumulative sum for a particular period.

12.1.3.1 History group
The history group specifies periodic collection of traffic information statistics on an interface and saves the statistics in the history record table. The statistics data includes bandwidth utilization, number of error packets, and total number of packets.

12.1.3.2 Ethernet statistics group
The statistics group specifies collection of various traffic statistics information on an Ethernet interface and saves it in the Ethernet statistics table. The statistics data includes network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received etc.

12.2 RMON Configuration
This section describes RMON configuration for Supermicro switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMON status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Collection statistic</td>
<td>None</td>
</tr>
<tr>
<td>Collection history</td>
<td>None</td>
</tr>
<tr>
<td>Alarms</td>
<td>None</td>
</tr>
<tr>
<td>Events</td>
<td>None</td>
</tr>
</tbody>
</table>

12.2.1 Enabling RMON
RMON is disabled by default in Supermicro switches. Follow the below steps to enable RMON.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set rmon enable</td>
<td>Enable RMON in the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exit from Configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Show rmon</td>
<td>Display RMON status.</td>
</tr>
</tbody>
</table>
The “set rmon disable” command disables RMON in the switch.

RMON must be enabled before any other RMON configuration.

The example below shows the commands used to enable RMON.

SMIS# configure terminal
SMIS(config)# set rmon enable
SMIS(config)# end
SMIS# show rmon
RMON is enabled

### 12.2.2 Configuring Alarms and Events

The alarm group periodically takes statistical samples from variables and compares them with the configured thresholds. When a threshold is crossed, an event is generated using the alarm mechanism.

The event group generates events whenever an alarm condition takes place in the device. The alarm group calls the event group, so an event must already be created for the alarm to call.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>rmon alarm &lt;alarm-number&gt;&lt;mib-object-id (255)&gt;&lt;sample-interval-time (1-65535)&gt;{absolute</td>
<td>delta } rising-threshold &lt;value 0-2147483647&gt;&lt;rising-event-number (1-65535)&gt;falling-threshold &lt;value 0-2147483647&gt;&lt;falling-event-number (1-65535)&gt;[owner &lt;ownername (127)&gt;]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>alarm-number - Alarm Number. This value ranges between 1 and 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mib-object-id - The mib object identifier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sample-interval-time - Time in seconds during which the alarm monitors the MIB variable. This value ranges between 1 and 65535 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>absolute - Used to test each mib variable directly.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>delta - Used to test the change between samples of a variable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rising-threshold - A number at which the alarm is triggered. This value ranges between 0 and 2147483647.</td>
</tr>
</tbody>
</table>
**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon event &lt;number (1-65535)&gt; [description &lt;event-description (127)&gt;] [log] [owner &lt;ownername (127)&gt;] [trap &lt;community (127)&gt;]</td>
<td>(Optional) Add an event in the RMON event table that is associated with an RMON event number.</td>
</tr>
</tbody>
</table>

**failing-threshold value** - A number at which the alarm is reset. This value ranges between 0 and 2147483647.

**NOTE**: Falling threshold must be less than rising threshold.

**rising-event-number** - The event number to trigger when the rising threshold exceeds its limit. This value ranges between 1 and 65535.

**falling-event-number** - The event number to trigger when the falling threshold exceeds its limit. This value ranges between 1 and 65535.

**Owner** – Owner of the alarm, string of length 127.

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Exit from Configuration mode.</td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon [statistics [&lt;stats-index (1-65535)&gt;]] [alarms] [events] [history [history-index (1-65535)] [overview]]</td>
<td>Display RMON statistics, alarms, events history and overview.</td>
</tr>
</tbody>
</table>
The “no rmon alarm <number (1-65535)>” and “no rmon event <number (1-65535)>” commands delete the RMON alarm configuration and RMON event configuration respectively.

When the alarm variable is the MIB variable defined in the history group or the Ethernet statistics group, RMON Ethernet statistics function or RMON history statistics function should be configured on the particular Ethernet interface, else the creation of the alarm entry fails, and no alarm event is triggered.

### 12.2.3 Configuring Statistics

The RMON Ethernet statistics group collects statistics for each monitored interface on the switch and stores them in the Ethernet statistics table. Only one statistics entry can be created per interface.

The RMON Ethernet history group collects a periodic statistical sampling of the data collected by the Ethernet statistics group and stores them in the Ethernet history table. Multiple history entries can be configured on one interface, however all should have different values.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | interface <interface-type><interface-id>  or  interface range <interface-type><interface-id> .... | (Optional) Enters the interface configuration mode. 
interface-type – may be any of the following:  
fx-ethernet – fx  
 cx-ethernet – cx  
interface-id is in slot/port format for all physical interfaces.  
To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10  
To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20  
If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces. |
| Step 3 | rmon collection stats <index (1-65535)> [owner <ownername (127)>] | (Optional) Enable RMON statistic collection on the interface  
index - Statistics table index, in range 1-65535 |
<table>
<thead>
<tr>
<th>Step 4</th>
<th>rmon collection history &lt;index (1-65535)&gt; [buckets &lt;bucket-number (1-65535)&gt;] [interval &lt;seconds (1-3600)&gt;] [owner &lt;ownername (127)&gt;]</th>
<th>owner - Optional field that allows you to enter the name of the owner of the RMON group of statistics with a string length of 127</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Enable history collection for the specified number of buckets and time period</td>
<td></td>
<td></td>
</tr>
<tr>
<td>index - History table index, in range 1-65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>buckets - The maximum number of buckets desired for the RMON collection history group of statistics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interval - The number of seconds in each polling cycle, in range 1-3600</td>
<td></td>
<td></td>
</tr>
<tr>
<td>owner - Optional field - allows the user to enter the name of the owner of the RMON group of statistics, string of length 127.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Step 5 | show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)]] [overview] | Display RMON statistics, history and overview. |

---

The “no rmon collection stats <index (1-65535)>” and “no rmon collection history <index (1-65535)>” commands delete the RMON collection configuration.

### 12.2.4 RMON Configuration Example

A sample RMON configuration of alarms, events and collection statistics and History in a Supermicro switch is specified below.

1) Enable RMON
2) Create events for Rising and falling threshold.
3) Create the alarm for the MIB object in 1.1.3.6.1.6.3.16.1.2.1.4table.
4) Create statistics collection on an interface.
5) Display all RMON configurations.

SMIS# configure terminal
SMIS(config)# set rmon enable
SMIS(config)# rmon event 1 description rise log owner smicro1 trap PUBLIC
SMIS(config)# rmon event 2 description fall log owner smicro1 trap NETMAN
SMIS(config)# rmon alarm 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.1012 absolute rising-threshold 2 1 falling-threshold 1 2 owner smicro1

SMIS(config)# interface Fx 0/5

SMIS(config-if)# rmon collection history 1 buckets 2 interval 20

SMIS(config-if)# rmon collection stats 1

SMIS(config-if)# end

SMIS# show rmon statistics

RMON is enabled

Collection 1 on Fx0/5 is active, and owned by monitor,

Monitors ifEntry.1.5 which has

Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.

# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0

SMIS# show rmon events

RMON is enabled

Event 1 is active, owned by smicro1

Description is rise

Event firing causes log and trap to community PUBLIC,

Time last sent is Apr 29 10:12:20 2013

Logging Event With Description : rise

Event 2 is active, owned by smicro1

Description is fall

Event firing causes log and trap to community NETMAN,

Time last sent is Apr 29 10:11:01 2013
SMIS# show rmon history
RMON is enabled

Entry 1 is active, and owned by
Monitors ifEntry.1.5 every 20 second(s)
Requested # of time intervals, ie buckets, is 2,
Granted # of time intervals, ie buckets, is 2,
Sample 2 began measuring at Apr 29 10:13:52 2013
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0
Sample 3 began measuring at Apr 29 10:14:12 2013
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events is 0
Network utilization is estimated at 0

SMIS# show rmon alarms
RMON is enabled
Alarm 1 is active, owned by smicro1
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)

Taking absolute samples, last value was 2
Rising threshold is 2, assigned to event 1
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm

SMIS# show rmon history overview

RMON is enabled
Entry 1 is active, and owned by
Monitors ifEntry.1.5 every 20 second(s)
Requested # of time intervals, ie buckets, is 2,
Granted # of time intervals, ie buckets, is 2,

SMIS# show rmon statistics 1 alarms events history 1

RMON is enabled
Collection 1 on Fx0/5 is active, and owned by monitor,
Monitors ifEntry.1.5 which has
Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of packets received of length (in octets):
64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm 1 is active, owned by smicro1
Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)
Taking absolute samples, last value was 2
Rising threshold is 2, assigned to event 1
Falling threshold is 1, assigned to event 2
On startup enable rising or falling alarm

Event 1 is active, owned by smicro1
Description is rise
Event firing causes log and trap to community PUBLIC,
Time last sent is Apr 29 10:12:20 2013
Logging Event With Description : rise
Event 2 is active, owned by smicro1
Description is fall
Event firing causes log and trap to community NETMAN,
Time last sent is Apr 29 10:11:01 2013
Entry 1 is active, and owned by
Monitors ifEntry.1.5 every 20 second(s)
Requested # of time intervals, ie buckets, is 2,
Granted # of time intervals, ie buckets, is 2,
Sample 4 began measuring at Apr 29 10:14:32 2013
  Received 0 octets, 0 packets,
  0 broadcast and 0 multicast packets,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers,
  0 CRC alignment errors and 0 collisions,
  # of dropped packet events is 0
  Network utilization is estimated at 0
Sample 5 began measuring at Apr 29 10:14:52 2013
  Received 0 octets, 0 packets,
0 broadcast and 0 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
  # of dropped packet events is 0
  Network utilization is estimated at 0
SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]
SMIS# show running-config

Building configuration...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
<th>Boot Loader</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SSE-F3548</td>
<td>1.0.0.0</td>
<td>6</td>
<td>0.0.0.0vlan 1</td>
</tr>
</tbody>
</table>

ports fx 0/1-24 untagged
ports cx 0/1-3 untagged

exit

set rmon enable

rmon event 1 description rise log owner smicro1  trap PUBLIC

rmon event 2 description fall log owner smicro1  trap NETMAN

rmon alarm 1 1.3.6.1.6.3.16.1.2.1.4.1.4.1.10.110.111.110.101 2 absolute rising-thresh

old 2 1 falling-threshold 1 2 owner smicro1

interface Fx 0/5

rmon collection stats 1 owner monitor

rmon collection history 1 buckets 2 interval 20

exit

12.2.5 Configuring Port Rate Limit

Rate limit is disabled by default in Supermicro switches. Follow the below steps to enable the port rate limit.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt;&lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>(Optional) Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>rate-limit output <code>&lt;rate-value-kbps (1-10000000)&gt;&lt;burst-value-kbits (1-10000000)&gt;</code></td>
<td>Enables the egress rate limit for the interface(s), set to the closest rate (kbps) and burst size (kbits) as the hardware capabilities. Rate limiting is applied to packets sent out on a particular interface. Rate limit and burst size in range of 1-10000000.</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface [[ &lt;interface-type&gt;&lt;interface-id&gt;] rate-limit</td>
<td>Displays the rate limit configuration on an interface</td>
</tr>
</tbody>
</table>

The “no rate-limit output” command disables the rate limit on a particular interface.

The example below shows the commands used to configure the rate limit.

---

The example below shows the commands used to configure the rate limit.

---
SMIS# configure terminal
SMIS(config)# interface Fx 0/20
SMIS(config-if)# rate-limit output 500000 4800
SMIS(config-if)# end

SMIS# show interface Fx 0/20 rate-limit

Fx0/20
Rate Limit : 500000 Kbps
Burst Size : 4800 Kbps

### 12.2.6 Configuring HOL Blocking Prevention
HOL is enabled by default in Supermicro switches. Follow the steps below to disable HOL blocking.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>no hol blocking prevention</td>
<td>Disables HOL blocking</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show interfaces [(&lt;interface-type&gt;&lt;interface-id&gt;)]</td>
<td>Displays the interface configuration.</td>
</tr>
</tbody>
</table>

The “hol blocking prevention” command enables HOL blocking.

The example below shows the commands used to disable HOL blocking.

SMIS# configure terminal
SMIS(config)# interface Fx 0/4
SMIS(config-if)# no hol blocking prevention
SMIS(config-if)# end
SMIS(config-if)# show interface Fx 0/4

Fx0/4 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port
Hardware Address is 00:30:48:e3:04:78

MTU 1500 bytes, Full duplex, 25 Gbps, Auto-Negotiation
HOL Block Prevention disabled.
Input flow-control is off, output flow-control is off

Link Up/Down Trap is enabled

Reception Counters

Octets : 0
Unicast Packets : 0
Broadcast Packets : 0
<table>
<thead>
<tr>
<th>Count Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Pause Frames</td>
<td>0</td>
</tr>
<tr>
<td>Undersize Frames</td>
<td>0</td>
</tr>
<tr>
<td>Oversize Frames</td>
<td>0</td>
</tr>
<tr>
<td>CRC Error Frames</td>
<td>0</td>
</tr>
<tr>
<td>Discarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Error Packets</td>
<td>0</td>
</tr>
<tr>
<td>Unknown Protocol</td>
<td>0</td>
</tr>
</tbody>
</table>

**Transmission Counters**

<table>
<thead>
<tr>
<th>Count Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>0</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Non-Unicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Pause Frames</td>
<td>0</td>
</tr>
<tr>
<td>Discarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Error Packets</td>
<td>0</td>
</tr>
</tbody>
</table>
13 Security

Supermicro switches support four methods of user authentication:

- **RADIUS** – Remote Authentication Dial-In User Service (RADIUS) uses AAA service for ID verification, granting access and tracking actions of remote users.
- **TACACS** – Terminal Access Controller Access Control System (TACACS) provides accounting information and administrative control for authentication and authorization. RADIUS encrypts only password, whereas TACACS encrypts username as well, hence it is more secure.
- **SSH** – Secure Shell (SSH) is a protocol for secure remote connection to a device. SSH provides more security than telnet by encryption of messages during authentication.
- **SSL** – Secure Socket Layer (SSL) provides server authentication, encryption and message integrity as well as HTTP client authentication.

13.1 Login Authentication Mode

Supermicro switches allow login authentication against users in local configuration or users in RADIUS or TACACS. Switch can also be configured to fallback to local authentication if authentication with RADIUS or TACACS fails.

Follow the steps below to configure Login Authentication Mechanism.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>login authentication {local</td>
<td>RADIUS [local]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Local – Use the local database in switch to authenticate users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Radius – Use RADIUS server to authenticate users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Radius local – Use RADIUS server to authenticate users and in case of failure fallback to local authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tacacs – Use TACACS server to authenticate users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tacacs local – Use TACACS server to authenticate users and in case of failure fallback to local authentication.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show system information</td>
<td>Displays the Login Authentication mechanism.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
The “no login authentication” command resets the login authentication to its default of ‘local’.

The example below shows the commands used to configure Login Authentication with RADIUS.

SMIS# configure terminal
SMIS(config)# login authentication radius
SMIS(config)# end
SMIS# show system information

Switch Name : SMIS
Switch Base MAC Address : 00:30:48:e3:70:bc
SNMP EngineID : 80.00.08.1c.04.46.53
System Contact : http://www.supermicro.com/support
System Location : Supermicro
Logging Option : Console Logging
Login Authentication Mode : RADIUS
Snoop Forward Mode : MAC based
Config Restore Status : Not Initiated
Config Restore Option : No restore
Config Restore Filename : iss.conf
Config Save IP Address : 0.0.0.0
Device Up Time : 0 days 0 hrs 15 mins 43 secs
Boot-up Flash Area : Normal
NTP Broadcast Mode : No

[ NTP ] ntp is disabled

<table>
<thead>
<tr>
<th>Server</th>
<th>Key</th>
<th>Prefer</th>
</tr>
</thead>
<tbody>
<tr>
<td>======</td>
<td>===</td>
<td>======</td>
</tr>
</tbody>
</table>

Key # Key
======== ===================================================================
Time zone offset not set

The example below shows the commands to configure RADIUS authentication with fallback to local.

SMIS# configure terminal
SMIS(config)# login authentication radius local
SMIS(config)# end
13.2 RADIUS

A sequence of events occurs during RADIUS client-server communication at the time of user login.

- The username and password are encrypted by the client and sent to RADIUS server.
- The client receives a response from the RADIUS server:
  - ACCEPT—User authentication is successful.
  - REJECT—User authentication failed. User is prompted to re-enter username/password, or access is denied.
  - CHALLENGE—Additional data is requested from the user.
  - CHALLENGE PASSWORD—User is prompted to select a new password.

Along with ACCEPT or REJECT packets, service options (Telnet, SSH, rlogin, or privileged EXEC services) and connection parameters like user timeouts are sent by RADIUS server.

Defaults – RADIUS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
</tr>
<tr>
<td>Timeout</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Re-transmit</td>
<td>3</td>
</tr>
<tr>
<td>Key</td>
<td>None</td>
</tr>
</tbody>
</table>

13.2.1 RADIUS Server

Supermicro switches function as a RADIUS client. The RADIUS server to be contacted for authentication can be configured in the switch.

Follow the steps below to configure RADIUS server Parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>`radius-server host &lt;ip-address&gt; [timeout &lt;1-120&gt;] [retransmit &lt;1-254&gt;] key &lt;secret-key-string&gt; [type {authenticating</td>
<td>accounting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* <code>ip-address</code> – server IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* <code>timeout</code> – Specify RADIUS server timeout in range 1-120</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* <code>retransmit</code> – Specify number of retries to attempt to connect to RADIUS server in range 1-254</td>
</tr>
<tr>
<td></td>
<td></td>
<td>* <code>key</code> – Specify authentication key</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>End</code></td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show radius server</code></td>
<td>Displays the RADIUS configuration.</td>
</tr>
<tr>
<td></td>
<td><code>show radius statistics</code></td>
<td></td>
</tr>
</tbody>
</table>
Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration.

The “no radius-server host <ip-address>” command deletes the RADIUS client.

The example below shows the commands used to configure RADIUS server.

SMIS# configure terminal
SMIS(config)#radius-server host 200.200.200.1 timeout 50 retransmit 250 key key1

SMIS(config)# end

SMIS# show radius server

Radius Server Host Information

-----------------------------
Index : 1
Server address : 200.200.200.1
Shared secret : key1
Radius Server Status : Enabled
Response Time : 50
Maximum Retransmission : 250

-----------------------------

SMIS# show radius statistics

Radius Server Statistics

--------------------
Index : 1
Radius Server Address : 200.200.200.1
UDP port number : 1812
Round trip time : 0
No of request packets : 0
No of retransmitted packets : 0
No of access-accept packets : 0
No of access-reject packets : 0
No of access-challenge packets : 0
No of malformed access responses : 0
No of bad authenticators : 0
13.3 TACACS

TACACS provides access control to switch through a client-server model, similar to RADIUS except that it provides enhanced security by encryption of all messages and reliability via TCP.

Defaults – TACACS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS server</td>
<td>None</td>
</tr>
<tr>
<td>TACACS server re-tries</td>
<td>2</td>
</tr>
<tr>
<td>TACACS TCP port</td>
<td>49</td>
</tr>
<tr>
<td>TACACS Authentication Mode</td>
<td>PAP</td>
</tr>
<tr>
<td>TACACS Authorization status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Privilege</td>
<td>1</td>
</tr>
</tbody>
</table>

13.3.1 TACACS Server

Supermicro switches allow configuration of multiple TACACS servers. One of these servers provides the authentication support.

Follow the steps below to configure TACACS server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>tacacs-server host &lt;ip-address&gt; [single-connection] [port &lt;tcp port (1-65535)&gt;] [timeout &lt;time out in seconds&gt;] key &lt;secret key&gt;</td>
<td>Configure TACACS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip-address – TACACS Server IP-address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>single-connection – When this option is specified, only one connection to one of the configured TACACS servers is permitted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port – Specify TCP port in range 1-65535</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timeout - Specify TACACS server timeout in range 0 – 255 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>key – Authentication key of maximum length 64 characters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>show tacacs</td>
<td>Displays the TACACS configuration.</td>
</tr>
</tbody>
</table>
Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration.

The “no tacacs-server host <ip-address>” command deletes the TACACS server.

The example below shows the commands used to configure TACACS server.

```
SMIS# configure terminal
SMIS(config)# tacacs-server host 10.10.10.1 port 500 timeout 200 key key123
SMIS(config)# end
SMIS# show tacacs

Server : 1
    Address           : 10.10.10.1
    Single Connection : no
    TCP port          : 500
    Timeout           : 200
    Secret Key        : key123

Client uses server: 0.0.0.0
    Authen. Starts sent : 0
    Authen. Continues sent : 0
    Authen. Enables sent : 0
    Authen. Aborts sent : 0
    Authen. Pass rcvd. : 0
    Authen. Fails rcvd. : 0
    Authen. Get User rcvd. : 0
    Authen. Get Pass rcvd. : 0
    Authen. Get Data rcvd. : 0
    Authen. Errors rcvd. : 0
    Authen. Follows rcvd. : 0
    Authen. Restart rcvd. : 0
    Authen. Sess. timeouts : 0

Author. Requests sent : 0
    Author. Pass Add rcvd. : 0
    Author. Pass Repl rcvd. : 0
    Author. Fails rcvd. : 0
    Author. Errors rcvd. : 0
    Author. Follows rcvd. : 0
    Author. Sess. timeouts : 0
```
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>tacacs-server retransmit &lt;1-100&gt;</td>
<td>Configure TACACS server re-tries in the range 1-100.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show tacacs</td>
<td>Displays the TACACS configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The “no tacacs-server retransmit” command resets the TACACS server re-tries to its default value.

The example below shows the commands used to configure TACACS server re-tries.

SMIS# configure terminal
SMIS(config)# tacacs-server retransmit 5
SMIS(config)# end

### 13.3.3 TACACS use-server

Supermicro switches provide option to configure multiple TACACS servers. User can specify one of these available servers to be used at a time.

Follow the steps below to configure TACACS server to be used.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>tacacs use-server address&lt;ip-address&gt;</td>
<td>Configure TACACS server to be used.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show tacacs</td>
<td>Displays the TACACS configuration.</td>
</tr>
</tbody>
</table>
The “no tacacs use-server address<ip-address>” command deletes the TACACS client.

The example below shows the commands used to configure TACACS server to be used.

SMIS# configure terminal
SMIS(config)# tacacs use-server address 10.10.10.1
SMIS(config)# end
SMIS# show tacacs

Server : 1
  Address : 10.10.10.1
  Single Connection : no
  TCP port : 49
  Timeout : 200
  Secret Key : key123

Server : 2
  Address : 50.50.50.1
  Single Connection : no
  TCP port : 49
  Timeout : 5
  Secret Key : key789

Client uses server: 10.10.10.1

Authen. Starts sent : 0
Authen. Continues sent : 0
Authen. Enables sent : 0
Authen. Aborts sent : 0
Authen. Pass rcvd. : 0
Authen. Fails rcvd. : 0
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Get Data rcvd. : 0
Authen. Errors rcvd. : 0
Authen. Follows rcvd. : 0
Authen. Restart rcvd. : 0
Authen. Sess. timeouts : 0
Author. Requests sent : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd. : 0
### 13.3.4 TACACS Login Authentication Mode

Supermicro switches provide an option to configure TACACS login authentication mode. Users can specify one of the mode PAP or CHAP.

In TACACS+ mode, authentication request is sent to the configured TACACS+ server. The user name and passwords are authenticated using TACACS+ server.

Follow the steps below to configure the TACACS login authentication mode to be used.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authentication tacacs { chap</td>
<td>pap }</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show Tacacs</td>
<td>Displays the TACACS configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

> The "no aaa authentication tacacs" command deletes the TACACS login mode.

The example below shows the commands used to configure the TACACS login mode to be used.

SMIS# configure terminal

SMIS(config)# aaa authentication tacacs chap
SMIS(config)# end

SMIS# show tacacs
Server : 1
    Address : 192.168.2.11
    Single Connection : no
    TCP port : 49
    Timeout : 5
    Key Type : 0
    Secret Key : testing123
    Mode : Chap
Client uses server: 192.168.2.11

Authen. Starts sent : 14
Authen. Continues sent : 0
Authen. Enables sent : 0
Authen. Aborts sent : 0
Authen. Pass rvcd. : 11
Authen. Fails rcvd. : 3
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Sess. timeouts : 0
Author. Requests sent : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd. : 0
Author. Fails rcvd. : 0
Author. Errors rcvd. : 0
Author Follows rcvd. : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent : 0
Acct. Stop reqs. sent : 0
Acct. Success rcvd. : 0
Acct. Errors rcvd. : 0
Acct. Follows rcvd. : 0
Acct. Sess. timeouts : 0
Malformed Pkts. rcvd. : 0
Socket failures : 0
Connection failures : 0
13.3.5 TACACS Authorization Status

Supermicro switches provide an option to configure TACACS authorization status. Users can specify one of the option Enable or Disable.

If authorization status is enabled, during TACACS+ authentication switch will also send out the authorization request to TACACS+ server. The authorization requests are used to get privilege levels for TACACS+ users. When authorization status is disabled, all TACACS+ authenticated users will be logged in with default privilege level 1. When authorization status is enabled, the TACACS+ authentication users will be logged in with privilege levels configured in TACACS+ server.

Follow the steps below to configure the TACACS authorization to be used.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authorization group Tacacs</td>
<td>Configures TACACS authorization to be used.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show tacacs</td>
<td>Displays the TACACS configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no aaa authorization group tacacs” command disables the TACACS authorization status.

The example below shows the commands used to configure the TACACS authorization status to be used.

SMIS# configure terminal

SMIS(config)# aaa authorization group tacacs

SMIS(config)# end

SMIS(config)# show tacacs
Server : 1
    Address : 192.168.2.11
    Single Connection : no
    TCP port : 49
    Timeout : 5
    Key Type : 0
    Secret Key : test123
    Mode : Pap
Client uses server: 192.168.2.11

Authorization Enable

- Authen. Starts sent : 8
- Authen. Continues sent : 0
- Authen. Enables sent : 0
- Authen. Aborts sent : 0
- Authen. Pass rcvd. : 5
- Authen. Fails rcvd. : 3
- Authen. Get User rcvd. : 0
- Authen. Get Pass rcvd. : 0
- Authen. Sess. timeouts : 0
- Author. Requests sent : 4
- Author. Pass Add rcvd. : 0
- Author. Pass Repl rcvd : 0
- Author. Fails rcvd. : 0
- Author. Errors rcvd. : 0
- Author Follows rcvd. : 0
- Author. Sess. timeouts : 0
- Acct. start reqs. sent : 0
- Acct. WD reqs. sent : 0
- Acct. Stop reqs. sent : 0
- Acct. Success rcvd. : 0
- Acct. Errors rcvd. : 0
- Acct. Follows rcvd. : 0
- Acct. Sess. timeouts : 0
- Malformed Pkts. rcvd. : 0
- Socket failures : 0
- Connection failures : 0

### 13.3.6 TACACS Privilege

<table>
<thead>
<tr>
<th>Req. #</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>The privilege configured in TACACS+ server should be used while logging in to Supermicro switch using TACACS+ authentication.</td>
<td>This is an umbrella requirement to cover the functionality.</td>
</tr>
<tr>
<td></td>
<td>There are many types of service used by different vendors on the market. For Supermicro switches the supported service type is ‘config’.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.g. user configuration in TACACS+ server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user = test15 {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>name = &quot;Test15 User&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pap = cleartext &quot;test15&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>service= <strong>config</strong> {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>priv-lvl = 15</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>TACACS+ users without privilege configured also should be able to login to switch with the default privilege level 1.</td>
<td></td>
</tr>
</tbody>
</table>
E.g. user configuration in TACACS+ server:
user = test1 {
    name = "Test1 User"
    pap = cleartext "test1"
}

1.2 This privilege function should be enabled only when user enables it in CLI, Web, and SNMP.

Proposed new CLI command to enable:
aaa authorization group tacacs

In Web, it should be enabled in “Management Security” page.

In SNMP, the following OID can be used:
1.3.6.1.4.1.2076.77.1.6.0

For e.g. the new command “aaa authorization

1.3 If this function is not enabled (using the command in Req. 2), switch should behave as before. It means the irrespective of the privilege configured on the TACACS+ server, it will login the users with the default privilege 1.

1.4 The TACACS+ privilege function should work in telnet, ssh and Web login.

1.5 The new authorization status configuration (Req. 2) should be saved and restored.

13.4 SSH
Supermicro switches act as a SSH client and support both SSH version 1 and SSH version 2.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH status</td>
<td>Enabled</td>
</tr>
<tr>
<td>SSH version compatibility</td>
<td>Off</td>
</tr>
<tr>
<td>SSH port</td>
<td>22</td>
</tr>
<tr>
<td>SSH Key</td>
<td>RSA</td>
</tr>
<tr>
<td>Cipher Algorithm</td>
<td>3DES-CBC</td>
</tr>
<tr>
<td>SSH Version</td>
<td>2</td>
</tr>
<tr>
<td>Authentication</td>
<td>HMAC-SHA1</td>
</tr>
</tbody>
</table>

Follow the steps below to configure SSH.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip ssh {version compatibility</td>
<td>cipher ([des-cbc] [3des-cbc])</td>
</tr>
</tbody>
</table>
auth – Specify the authentication algorithm.

port - Specify SSH port in range 1024-65535

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>End</td>
<td>show ip ssh</td>
<td>write startup-config</td>
</tr>
</tbody>
</table>

- **Step 3** End
  - Exits the configuration mode.
- **Step 4** show ip ssh
  - Displays the SSH configuration.
- **Step 5** write startup-config
  - Optional step – saves this configuration to be part of startup configuration.

The “no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>)” command disables SSH.

The example below shows the commands used to configure SSH.

SMIS# configure terminal
SMIS(config)# ip ssh version compatibility
SMIS(config)# end
SMIS# show ip ssh

Version : Both
Cipher Algorithm : 3DES-CBC
Authentication : HMAC-SHA1
Trace Level : None

SMIS# configure terminal
SMIS(config)# ip ssh cipher des-cbc
SMIS(config)# end
SMIS# show ip ssh

Version : 2
Cipher Algorithm : DES-CBC
Authentication : HMAC-SHA1
Trace Level : None

SMIS# configure terminal
SMIS(config)# ip ssh auth hmac-md5
SMIS(config)# end
SMIS# show ip ssh

Version : 2
Cipher Algorithm : 3DES-CBC
Authentication : HMAC-MD5
Trace Level : None
### 13.5 SSL
SSL provides server authentication, encryption, and message integrity, as well as HTTP client authentication, to allow secure HTTP communications. To use this feature, the cryptographic (encrypted) software image must be installed on the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Secure server status</td>
<td>Enabled</td>
</tr>
<tr>
<td>HTTP Secure server encryption</td>
<td>rsa-null-md5</td>
</tr>
<tr>
<td>HTTP Secure server keys</td>
<td>None</td>
</tr>
<tr>
<td>SSL Server certificate</td>
<td>None</td>
</tr>
<tr>
<td>SSL Server certificate request</td>
<td>None</td>
</tr>
</tbody>
</table>

#### 13.5.1 Secure HTTP (https)
On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption (HTTPS) provides a secure connection to allow such functions as configuring a switch from a Web browser.

Follow the steps below to configure Secure HTTP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha] [rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] } | Configure Secure HTTP.  
  
  server – Enables HTTPS server  
  ciphersuite – Specify one or many of the supported encryption algorithm to be used.  
  crypto key rsa – Encryption Key, either 512 or 1024. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show ip http secure server status | Displays the SSL configuration. |
| Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration. |

The “no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha] [rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }” command enables the agent.

The example below shows the commands used to configure Secure HTTP.

SMIS# configure terminal  
SMIS(config)# no ip http secure server  
SMIS(config)# end  
SMIS# show ip http secure server status  
HTTP secure server status : Disabled
HTTP secure server ciphersuite: RSA-DES-SHA:RSA-3DES-SHA:RSA-EXP1024-DES-SHA
HTTP crypto key rsa 1024

13.5.2 Certificate Signing Request (CSR)
An SSL certificate provides security for online communications. Before requesting an SSL certificate, a Certificate Signing Request (CSR) must be generated and submitted to the Certification Authority (CA). Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. CA servers are called as trustpoints, e.g. thawte.com.

Supermicro switches create a Certificate Signing Request (CSR) using RSA key pair and Switch Identification.

Follow the steps below to configure Certificate Signing Request (CSR).

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ssl gen cert-req algo rsa sn &lt;SubjectName&gt;</td>
<td>Configure Certificate Signing Request (CSR). SubjectName – Switch ID or IP-address.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show ssl server-cert</td>
<td>Displays the SSL configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>write startup-config</td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure Certificate Signing Request (CSR).

SMIS# ssl gen cert-req algo rsa sn SMIS

-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBADAPMQ0wCwYDVQQDEwRTTUITMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChj0JzVX1/gZ4SMGeKrRdrAnftWnKHG3VypWTtySqqvTwahnZ206Q2o
cBYJNKY4ZCykOXG81mfUhpPfVLyO8sbK+RYzEeTMXl9lw9iq9yOySOLvxY6IoYNsg
O++J502khz0SAbpRkhtGuwmBiZQtSj+8Ea3dG8ReoixpcYDVVdlrDQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAXR8Nz40QeC8wqwzqy+iozT5iUMK0keIXTE8mdDydt
AvRyc7a3EPragJyOL5W1H94z+wW2wkxXTrzKuLzAEYRH9fB4XB2uCADf+jkuSBJc
5qdJ4yBtolu/pxOsdKKwuq6LWbi44DCXg975Ke+pOYa7nWojVkc2SbjvK5CTgG
89s=

-----END CERTIFICATE REQUEST-----

SMIS# show ssl server-cert

Certificate:
Data:
Version: 1 (0x0)
Serial Number: 10 (0xa)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=CA, L=SanJose, O=Supermicro, OU=Switch, CN=Switch/Email
=support@supermicro.com

Validity
  Not After: Sep 10 22:18:10 2011 GMT
Subject: CN=SMIS
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
    Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
  32:6c

13.5.3 SSL Certificate
Each SSL Certificate contains
  • A public/private key pair: a private key with the code and a public key used to decode it. The private key is installed on the server and is not shared with anyone. The public key is incorporated into the SSL certificate and shared with web browsers.
  • Identification information. E.g. When you request an SSL certificate, a third party (such as Thawte) verifies your organization’s information and issues a unique certificate to you with that information.
SSL Certificate can be configured in Supermicro switches. The certificate should be specified in PEM format.

Follow the steps below to configure SSL server certificate.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ip http secure</td>
<td>Configure Cipher Suite and Crypto Key RSA of your choice using “ip http secure” command.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ssl gen cert-req algo rsa sn</td>
<td>Enter the subject name and create certificate request by using the “ssl gen cert-req algo rsa sn” command.</td>
</tr>
<tr>
<td>Step 3</td>
<td>show ssl server-cert</td>
<td>The “show ssl server-cert” command will display certificate request. Copy paste these contents to a text file, say a.csr.</td>
</tr>
</tbody>
</table>
| Step 4 | Linux commands | To generate SSL certificate openssl application can be used. The following steps can be executed in any linux machine to generate SSL certificates. For other openssl implementation refer the openssl documentation to find the equivalent steps. Execute the below commands in linux shell.  
   1. openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem  
   2. openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CAkey cakey.pem -CAcreateserial  
This would generate certificate file cert.pem. |
| Step 5 | ssl server-cert | Open the generate certificate file cert.pem. Delete first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--). Join all the remaining lines as single line to avoid line breaks processed.  
Copy paste these joined texts in “Enter Certificate” prompt– This prompt appears after entering the “ssl server-cert” command in CLI. |
| Step 6 | show ssl server-cert | This step would configure the certificate and save it to flash. | Displays the SSL configuration. |
LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

Devices in a LAN maintain operations-related configuration information in management information bases (MIBs). LLDP helps avoid misconfiguration problems in LANs by enabling LAN devices to be aware of other devices’ configuration information.

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. Details such as configuration information, device capabilities, and device identity can be advertised using LLDP.

Supermicroswitches provides the following LLDP features:

- Support all mandatory TLVs (chassis identifier, port identifier and time-to-live).
- Support optional TLVs - port description, system name, system description, system capabilities and management address.
- Support organizationally specific optional TLVs - port VLAN identifier, port and protocol VLAN identifier, VLAN name, MAC or PHY configuration or status, link aggregation and maximum frame size.
- Provide support for notifications through traps.

An LLDP agent operates in any one of the following three modes:

1. Transmit-only mode: The agent can only transmit the information about the capabilities and the status of the local system.
2. Receive-only mode: The agent can only receive information about the capabilities and the status of the remote systems.
3. Transmit and receive mode: The agent can transmit the local system capabilities and status information and receive the capabilities and status information of remote systems.

The LLDP transmit only mode sends the local device's information at regular intervals in LLDP TLV's. Whenever the transmit mode is disabled, the device transmits an LLDP PDU with a time-to-live (TTL) TLV containing "0" in the information field. Upon reception of a PDU with TLV 0, remote devices are then enabled to remove the information associated with this local device from their databases.

The LLDP receive only mode receives a remote device's information and updates the remote system's LLDP MIB database. When new or updated information is received, the receive module initiates a timer for a valid duration indicated by the TTL TLV in the received LLDP PDU. The remote system's information is removed from the database when an LLDP PDU is received with TTL TLV containing "0" in its information field.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Status (global)</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP Status (interface level)</td>
<td>Transmit and receive</td>
</tr>
<tr>
<td>TLV</td>
<td>None</td>
</tr>
<tr>
<td>HoldtimeMultiplier</td>
<td>4</td>
</tr>
<tr>
<td>--------------------</td>
<td>---</td>
</tr>
<tr>
<td>Message Transmit Interval</td>
<td>30</td>
</tr>
<tr>
<td>ReinitializationDelay</td>
<td>2</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>2</td>
</tr>
<tr>
<td>Trap Notification Interval</td>
<td>5</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Switch MAC address</td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>MAC address</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>Interface name</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>None</td>
</tr>
<tr>
<td>Notification</td>
<td>Disabled</td>
</tr>
<tr>
<td>Notification Type</td>
<td>Mis-configuration</td>
</tr>
</tbody>
</table>

14.1.1 Enabling LLDP

LLDP is disabled by default in Supermicro switches. Follow the steps below to enable LLDP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set lldp enable</td>
<td>Enables LLDP in the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global configuration details</td>
</tr>
</tbody>
</table>

The “set lldp disable” command disables LLDP in the switch.

14.1.2 Configuring LLDP Parameters

Once LLDP is enabled globally, it is enabled on all supported interfaces by default. Supermicro switches provide a user configuration to place an interface in only send or only receive mode.

Other LLDP parameters that can be configured in Supermicro switches are Notification type, Chassis-ID Sub-type and Port-ID Sub-type.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</td>
<td>(Optional) Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
</tbody>
</table>
port-channel – po

interface-id is in slot/port format for all physical interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10

To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20

If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

Step 3  lldp {transmit | receive}  (Optional)
Sets LLDP admin status on an interface to Transmit or Receive

Step 4  lldp notification [remote-table-chg][mis-configuration]  (Optional)
Enables LLDP trap notification on an interface.

remote-table-chg - Trap notification for change in neighbor’s table.
mis-configuration - Trap notification for mis-configuration.

Step 5  lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }  (Optional)
Configures LLDP port ID subtype and port ID value

if-alias - interface alias

port-comp - port component

mac-addr - MAC address

if-name - interface name

local - locally assigned

The default value for port-id-subtype is if-name.
Note: The if-alias option can be used only for the interfaces which have valid description configured.
<table>
<thead>
<tr>
<th>Step 6</th>
<th>Exit</th>
<th>Exits interface configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>lldp chassis-id-subtype { chassis-comp &lt;string(255)&gt;</td>
<td>if-alias</td>
</tr>
</tbody>
</table>

(Optional) Configures LLDP chassis ID subtype and chassis ID value.

The chassis identifier value can only be set for the chassis-component and local system subtypes. For all other subtypes, the value is taken from the system automatically.

chassis-comp - chassis component
if-alias - management interface alias
port-comp - port component
mac-addr - MAC address
nw-addr - network address
if-name - interface name
local - locally assigned

The default value for chassis-id-subtype is mac-addr.

Note: To use the if-alias option, the management interface must have been configured with valid description.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>End</th>
<th>Exits the configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>show lldp interface [&lt;interface-type&gt;&lt;interface-id&gt;]</td>
<td>Displays LLDP configuration details on a particular interface or all interfaces</td>
</tr>
<tr>
<td></td>
<td>show lldp neighbors [chassis-id &lt;string(255)&gt; port-id &lt;string(255)&gt;] [&lt;interface-type&gt;&lt;interface-id&gt;] [detail]</td>
<td>Displays information about neighbors learned on an interface or all interfaces</td>
</tr>
<tr>
<td></td>
<td>show lldp traffic [&lt;iftype&gt;&lt;ifnum&gt;]</td>
<td>Displays LLDP counters, including the number of frames sent, received, discarded, etc.</td>
</tr>
<tr>
<td></td>
<td>show lldp errors</td>
<td>Displays information about errors such as memory allocation failures, queue overflows, table overflows, etc.</td>
</tr>
<tr>
<td></td>
<td>show lldp statistics</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>clear lldp counters</td>
<td>Clears LLDP transmit and receive statistics</td>
</tr>
<tr>
<td>11</td>
<td>clear lldp table</td>
<td>Clears LLDP neighbors information</td>
</tr>
</tbody>
</table>

These commands reset the particular configuration to its default value.

```
lldp {transmit | receive}
no lldp notification
no lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}
no lldp tlv-select dot1tlv {{port-vlan-id} [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}]}
no lldp tlv-select dot3TLV { [macphy-config] [link-aggregation] [max-framesize] }
```

### 14.1.2.1 Configuring LLDP TLV

Supermicro switches provide support for user configuration of LLDP TLV’s. The TLV types supported by Supermicro switches are: Basic TLV, DOT1 TLV and DOT3 TLV. The figure below displays the TLV types and their content.

**Figure LLDP-1: LLDP TLV Types**

The content of the various TLVs supported by Supermicro switches are specified in the figure below.
### Step 1
Configure terminal

Enters the configuration mode

### Step 2
interface `<interface-type><interface-id>`

(Optional) Enters the interface configuration mode.

interface-type – may be any of the following:
- `fx-ethernet` – fx
- `cx-ethernet` – cx
- `port-channel` – po

interface-id is in slot/port format for all physical interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: `int range fx 0/1-10`

To provide multiple interfaces or ranges, separate with a comma (,). E.g.: `int range fx 0/1-10, fx 0/20`

---

### Basic TLV - Mandatory
- Chassis ID - Sender MAC address
- Port ID TLV - Sender Port number
- TTL - Time to Live
- End of LLDP PDU

### Basic TLV - Optional
- Port Description
- System Name
- System Description
- System Capabilities
- Management Address

### DOT1 TLV
- Port VLAN ID
- Port Protocol VLAN ID
- VLAN Name
- Protocol Identity

### DOT3 TLV
- MAC/PHY Configuration (speed, duplex, negotiation, etc.)
- Link Aggregation TLV
- Maximum Frame Size TLV

---

**Figure LLDP-2: LLDP TLV Content**
| Step 3 | lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}} | If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces. |
|--------|--------------------------------------------------|--------------------------------------------------|
|        | (Optional) Enables the basic TLV transmission on a given port | port-descr - Port description TLV |
|        | sys-name - System name TLV | sys-descr - System description TLV |
|        | sys-descr - System description TLV | sys-capab - System capabilities TLV |
|        | mgmt-addr all- Enables the transmission of the management address on the current interface. If no management address is present or configured in the system, the switch’s MAC address will be used for transmission. | mgmt-addr ipv4 ucast-addr - Enables the transmission of a particular IPv4 address on the current interface. |
|        | mgmt-addr ipv6 ipv6-addr - Enables the transmission of a particular IPv6 address on the current interface. | |
| Step 4 | lldp tlv-select dot1tlv {{port-vlan-id} [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}]}} | (Optional) Configure dot1 TLV types to be transmitted on a port |
|        | (Optional) Configure dot3 TLV types to be transmitted on a port | port-vlan-id - Port VLAN identifier TLV. The keyword port-vlan-id keyword is not supported. |
|        | protocol-vlan-id - Protocol VLAN identifier TLV. The keyword protocol-vlan-id is not supported. | vlan-name – VLAN name TLV |
|        | NOTE: VLAN name must be configured prior to this LLDP configuration. | |
| Step 5 | lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] } | (Optional) Configure dot3 TLV types to be transmitted on a port |
14.1.3 Configuring LLDP Timers
Supermicro switches allow for user configuration of LLDP timers:
- Transmit Interval
- Holdtime Multiplier
- ReinitializationDelay
- Transmit Delay
- Notification Delay

14.1.3.1 Message Transmit Interval
The message transmit interval is the period between transmission of the periodic LLDP advertisements. The default message transmit interval is 30 seconds.

Supermicro switches allow for user configuration of the message transmit interval. Follow the below steps to change the message transmit interval.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>lldp transmit-interval &lt;seconds(5-32768)&gt;</td>
<td>(Optional) Configures the message transmit interval, range of 5-32768.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global information</td>
</tr>
</tbody>
</table>

The “no lldp transmit-interval” command resets the message transmit interval to its default value.
14.1.3.2 Message Transmit Holdtime Multiplier

The Message Transmit Holdtime Multiplier is used to calculate the time-to-live (TTL) value sent in LLDP advertisements. The time-to-live informs the receiving LLDP agent of the time to retain remote LLDP information if LLDP advertisements are not received periodically.

The TTL is calculated as: the minimum of \((\text{Transmission Interval} \times \text{Holdtime Multiplier}), \text{or} 65536\)

The default holdtime multiplier is 4 seconds. The default TTL is: \(4 \times 30 = 120\) seconds. Supermicro switches allow for the user configuration of the message transmit holdtime multiplier. Follow the steps below to change the message transmit holdtime multiplier.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>lldpholdtime-multiplier &lt;value(2-10)&gt;</td>
<td>(Optional) Configures the message transmit holdtime multiplier, range of 2-10.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global information</td>
</tr>
</tbody>
</table>

The “no lldpholdtime-multiplier” command resets the message transmit holdtime multiplier to its default value.

14.1.3.3 Reinitialization Delay

When LLDP ports are disabled or the link goes down, LLDP is reinitialized on a port. The delay between the port going down and the reinitialization is called the reinitialization delay. When LLDP is reinitialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Supermicro switches allow user configuration of the reinitialization delay. Follow the steps below to change the reinitialization delay.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>lldpreinitialization-delay &lt;seconds(1-10)&gt;</td>
<td>(Optional) Configures the reinitialization delay, range of 1-10.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global information</td>
</tr>
</tbody>
</table>

The “no lldpreinitialization-delay” command resets the reinitialization delay to its default value.
14.1.3.4 Transmit Delay
Any change in local LLDP MIB variables initiates the transmission of LLDP advertisements. The delay between the successive transmissions of such advertisements is called the Transmit Delay. The transmit delay helps prevent unnecessary LLDP transmissions when rapid changes occur in local LLDP MIB objects.

Supermicro switches allow for user configuration of the message transmit delay. Follow the steps below to change the message transmit delay.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>lldptx-delay &lt;seconds(1-8192)&gt;</td>
<td>(Optional) Configures the message transmit delay, range of 1-8192.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: The Tx delay should be less than 0.25 * message Tx interval</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global information</td>
</tr>
</tbody>
</table>

The “no lldptx-delay” command resets the message transmit delay to its default value.

14.1.3.5 Notification Interval
The Notification Interval is the time interval between successive periodic SNMP notifications about LLDP MIB changes. Any change in LLDP neighbors that occurs between SNMP notifications is not transmitted; only state changes that exist at the expiry of the notification interval are included in the transmission.

Supermicro switches allow for user configuration of the notification interval. Follow the steps below to change the notification interval.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>lldp notification-interval &lt;seconds(5-3600)&gt;</td>
<td>(Optional) Configures the notification interval, range of 5-3600.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show lldp</td>
<td>Displays the LLDP global information</td>
</tr>
</tbody>
</table>

The “no lldp notification-interval” command resets the notification interval to its default value.
14.1.4 LLDP Configuration

The example below shows the commands used to configure LLDP by connecting two switches: Switch A and Switch B.

**Figure LLDP-3: LLDP Configuration Example**

Switch A

SMIS# configure terminal

SMIS(config)# set lldp enable

SMIS(config)# end

SMIS# show lldp

LLDP is enabled

Transmit Interval : 30

Holdtime Multiplier : 4

Reinitialization Delay : 2

Tx Delay : 2

Notification Interval : 5

Chassis Id SubType : Mac Address

Chassis Id : 00:30:48:e3:04:75

SMIS# show lldp neighbors

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

<table>
<thead>
<tr>
<th>Chassis ID</th>
<th>Local Intf</th>
<th>Hold-time</th>
<th>Capability</th>
<th>Port Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:30:48:e3:70:bc</td>
<td>Fx0/21</td>
<td>120</td>
<td></td>
<td>Fx0/22</td>
</tr>
</tbody>
</table>
Total Entries Displayed : 1

SMIS(config)# lldp chassis-id-subtype if-name
SMIS(config)# lldpholdtime-multiplier 7
SMIS(config)# lldp notification-interval 100
SMIS(config)# lldpreinitialization-delay 5
SMIS(config)# lldpreinitialization-delay 9
SMIS(config)# lldpreinitialization-delay 10
SMIS(config)# lldp transmit-interval 100
SMIS(config)# lldp transmit-interval 10
SMIS(config)# end
SMIS(config)# interface Fx 0/21
SMIS(config-if)# lldp notification remote-table-chg
SMIS(config-if)# lldp port-id-subtype if-name
SMIS(config-if)# lldp tlv-select basic-tlv port-dscrmgmt-addr all
SMIS(config-if)# exit
SMIS(config)# vlan 1
SMIS(config-vlan)# name vlan1
SMIS(config-vlan)# exit
SMIS(config)# interface Fx 0/21
SMIS(config-if)# lldp tlv-select dot1tlv vlan-name 1
SMIS(config-if)# lldp tlv-select dot3tlv macphy-config
SMIS(config-if)# end

SMIS# show lldp
LLDP is enabled
Transmit Interval : 10
Holdtime Multiplier : 7
Reinitialization Delay : 10
Tx Delay : 2
Notification Interval : 100
Chassis Id SubType : Interface Name
Chassis Id : eth0
SMIS# show lldp neighbors

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

<table>
<thead>
<tr>
<th>Chassis ID</th>
<th>Local Intf</th>
<th>Hold-time</th>
<th>Capability</th>
<th>Port Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:30:48:e3:70:bc</td>
<td>Fx0/21</td>
<td>120</td>
<td>Fx0/22</td>
<td></td>
</tr>
</tbody>
</table>

Total Entries Displayed : 1
SMIS# show lldp errors

Total Memory Allocation Failures : 0
Total Input Queue Overflows : 0
Total Table Overflows : 0
SMIS# show lldp traffic

Total Frames Out : 71
Total Entries Aged : 0
Total Frames In : 28
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVs Discarded : 0
SMIS# show lldp interface Fx 0/21

Fx0/21:
Tx State : Enabled
Rx State : Enabled
Tx SEM State : IDLE
Rx SEM State : WAIT FOR FRAME
Notification Status : Enabled
Notification Type : Remote Table Change
SMIS# show lld statistics
Remote Table Last Change Time : 217700
Remote Table Inserts : 1
Remote Table Deletes : 0
Remote Table Drops : 0
Remote Table Ageouts : 0
Remote Table Updates : 0

SMIS# show lldp local Fx 0/21
Port Id SubType : Interface Name
Port Id : Slot0/21
Port Description :
Enabled TxTlvs : Port Description, Management Address, Mac Phy

Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status : Supported, Enabled
Advertised Capability Bits : 6c11
10base-T(HD)
10base-T(FD)
100base-TX(HD)
100base-TX(FD)
Asym and SymmPAUSE(FD)
1000base-T(FD)
Operational MAU Type : 30
-Link Aggregation

Capability & Status : Not Capable, Not In Aggregation
Aggregated Port Id : 21
-Maximum Frame Size : 1500

Extended 802.1 TLV Info

-Port VLAN Id : 1

-Port & Protocol VLAN Id

<table>
<thead>
<tr>
<th>Protocol VLAN Id</th>
<th>Support</th>
<th>Protocol VLAN Status</th>
<th>TxStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Supported</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

-Vlan Name

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>Vlan Name</th>
<th>TxStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vlan1</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

SMIS# show running-config

Building configuration...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
<th>Boot Loader</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SSE-F3548</td>
<td>1.0.0.0</td>
<td>6</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
name vlan1
exit

setlldp enable
lldp transmit-interval 10
lldp holdtime-multiplier 7
lldp preinitialization-delay 10
lldp notification-interval 100
lldp chassis-id-subtype if-name
interface Fx 0/21
lldp notification remote-table-chg
lldp tlv-select basic-tlv port-descrmgmt-addr all
lldp tlv-select dot3tlv macphy-config
lldp tlv-select dot1tlv vlan-name 1
exit

Switch B
SMIS# configure terminal
SMIS(config)# set lldp enable
SMIS(config)# end
SMIS# show lldp

LLDP is enabled
Transmit Interval : 30
Holdtime Multiplier : 4
Reinitialization Delay : 2
Tx Delay : 2
Notification Interval : 5
Chassis Id SubType : Mac Address
Chassis Id : 00:30:48:e3:70:bc

SMIS# show lldp neighbors

Capability Codes :
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device, 
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

<table>
<thead>
<tr>
<th>Chassis ID</th>
<th>Local Intf</th>
<th>Hold-time</th>
<th>Capability</th>
<th>Port Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:30:48:e3:04:75</td>
<td>Fx0/22</td>
<td>120</td>
<td></td>
<td>Fx0/21</td>
</tr>
</tbody>
</table>

Total Entries Displayed : 1

**SMIS# show lldp statistics**

Remote Table Last Change Time : 80900
Remote Table Inserts : 4
Remote Table Deletes : 3
Remote Table Drops : 0
Remote Table Ageouts : 3
Remote Table Updates : 7

SMIS(config)# show lldp traffic

Total Frames Out : 52
Total Entries Aged : 3
Total Frames In : 144
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 0
Total TLVs Discarded : 0

SMIS(config)# show lldp errors

Total Memory Allocation Failures : 0
Total Input Queue Overflows : 0
Total Table Overflows : 0

SMIS(config)# show lldp interface Fx 0/22
Fx0/22:
Tx State : Enabled
Rx State : Enabled
Tx SEM State : IDLE
Rx SEM State : WAIT FOR FRAME
Notification Status : Disabled
Notification Type : Mis-configuration

SMIS# show lldp local Fx 0/22
Port Id SubType : Interface Alias
Port Id : Fx0/22
Port Description :
Enabled TxTlvs :

Extended 802.3 TLV Info
-MAC PHY Configuration & Status
Auto-Neg Support & Status : Supported, Enabled
Advertised Capability Bits : 6c11
10base-T(HD)
10base-T(FD)
100base-TX(HD)
100base-TX(FD)
Asym and SymmPAUSE(FD)
1000base-T(FD)
Operational MAU Type : 30
-Link Aggregation
Capability & Status : Not Capable, Not In Aggregation
Aggregated Port Id : 22
-Maximum Frame Size : 1500
Extended 802.1 TLV Info

- Port VLAN Id : 1

- Port & Protocol VLAN Id

<table>
<thead>
<tr>
<th>Protocol VLAN Id</th>
<th>Support</th>
<th>Protocol VLAN Status</th>
<th>TxStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Supported</td>
<td>Enabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

-Vlan Name

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>Vlan Name</th>
<th>TxStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

SMIS# show running-config

Building configuration...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
<th>Boot Loader</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SSE-F3548</td>
<td>1.0.0.0</td>
<td>6</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

vlan 1

ports fx 0/1-24 untagged

ports cx 0/1-3 untagged

exit

setlldp enable
15 Data Centre Bridging Exchange

DCBX is a discovery & capability exchange protocol that is capable of discovering DCB compliant devices and exchange DCBX configuration information with them. Supermicro switches SSE-F3548S/SR support DCBX (Data centre Bridging Exchange) feature.

15.1 Overview

DCBX runs on the Physical Ethernet link between Supermicro switch (e.g SSE-F3548S) and Host Server’s Network Card adapter (e.g. AOC-MH25G-m2S2T,AOC-S100G-m2C) that has DCBX capabilities. DCBX protocol relies on the Link Layer Discovery Protocol (LLDP) to exchange DCBX information with its DCBX peer. DCBX peers (switch and the host adapter) negotiate the capabilities between them to send configuration values to the adapter. Auto PFC configuration from the switch to the host can be achieved with DCBX TLVs.

- DCBX capability on the switch remain disabled if the host network adapter does not support the DCBX.
- Please make sure that the DCBX feature is enabled on the host network adapter if it is not turned on by default.

15.2 DCB Feature Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Bridging Exchange (DCBX) Protocol</td>
<td>It Allows exchange of Ethernet parameters between switches and Host Adapters.</td>
</tr>
<tr>
<td>Congestion notification</td>
<td>Provides end to end congestion management for protocols that are capable of transmission rate limiting to avoid frame loss.</td>
</tr>
<tr>
<td>Enhanced transmission selection</td>
<td>Provides bandwidth management between traffic types.</td>
</tr>
<tr>
<td>Priority Based Flow Control (PFC)</td>
<td>Provides a link level flow control mechanism that can be controlled independently for each frame priority.</td>
</tr>
</tbody>
</table>
Data Center Bridging Exchange (DCBX) Protocol

**Congestion Notification**, IEEE 802.1Qau is a congestion management mechanism that sends a congestion notification message to the source of the congestion. It tries to stop congestion at its source—where the “end host” originates the congestion and causing flow.

**Enhanced Transmission Selection (ETS)** IEEE 802.1Qaz is a bandwidth management mechanism which enables us to allocate port bandwidth in such a way that maximizes bandwidth utilization for all flows on a link. ETS allows a port to share and re-allocate BW dynamically among its flows while guaranteeing a minimum amount of bandwidth to each flow.

**Priority-based flow control (PFC)**, IEEE standard 802.1Qbb, is a link-level flow control mechanism. Which is an enhancement to the Ethernet pause mechanism, operates on single priority rather than pausing all traffic on a link.

PFC creates eight logically divided virtual links from a physical link and provides the capability to use pause on a single virtual link without affecting traffic on the other virtual links. PFC allows us to pause traffic selectively according to its class.

**PFC Priority based Flow Control (Figure A)**
15.3 DCBX configuration steps

Configuring DCBX involves the steps listed below.

1. Enable LLDP.
2. Create cee-map.
   a. Create a name for Priority (optional).
   b. Mark the application-protocol packets with required priority.
   c. Create a name for Priority-group (optional).
   d. Map priority to priority-group.
   e. Allocate bandwidth to the priority-group.
3. Apply cee-map to the interface.
4. Configure TLVs (optional).

Commands to configure the above steps on Super Micro Switch are given below in detail.

15.3.1 Enable LLDP feature on the switch

DCBX protocol relies on Link Layer Discovery Protocol (LLDP) to exchange information with peer. So LLDP must be enabled for DCBX feature to work.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>set lldp enable</td>
<td>Enable and Configure LLDP</td>
</tr>
<tr>
<td>Step 3</td>
<td>Exit</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# set lldp enable
SMIS(config)# exit

15.3.2 Create cee-map

Converged Enhanced Ethernet map creates an association among application-protocol, priority, priority-group, and group-bandwidth. Four cee-maps can be created.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Exit</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-ceed-map)# exit
SMIS(config)# exit

SMIS# show cee-map 1

15.3.2.1 Create a description for Priority (optional)
There are 8 priorities available and they are identified by number 0 - 7. Creating a description for the priority helps to easily identify the traffic assigned to that priority. This step is optional and doesn’t affect the functionality. Description has to be created before assigning the cee-map to the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>Step 3</td>
<td>priority &lt;pri(0-7)&gt; description {&lt;string(63)&gt;}</td>
<td>Creates a description for priority, which can be viewed in the show commands.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Exit</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# priority 1 description "FTP traffic"
SMIS(config-cee-map)# exit
SMIS(config)# exit
SMIS# show cee-map 1

15.3.2.2 Mark the application-protocol packets with required priority
The application-protocol of interest can be assigned to required priority. There are 8 priorities available and they are identified by number 0 - 7. More than one application-protocol can be assigned to the same priority. The default application-protocol configuration after creating a cee-map is shown below.

<table>
<thead>
<tr>
<th>Application-Protocol-ID</th>
<th>Type</th>
<th>Protocol-ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ether-type</td>
<td>0x8906</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ether-type</td>
<td>0x8914</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>tcp-udp</td>
<td>3260</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>ether-type</td>
<td>0x8915</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>tcp-udp</td>
<td>445</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>Step 3</td>
<td>application-protocol &lt;id(1-5)&gt; type {ether-type</td>
<td>tcp-udp</td>
</tr>
</tbody>
</table>
Step 4 | Exit | Exit from configuration mode.

Example:
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# application-protocol 5 type tcp-udp protocol-id 22 priority 2
SMIS(config-cee-map)# exit
SMIS(config)# exit

SMIS# show cee-map 1

15.3.2.3 Create a name for Priority-group (optional)
CEE supports 9 priority-groups and they are identified by PGID number 0 – 7 and 15. Creating a description for the priority-group helps to easily identify the traffic assigned to that priority-group. This step is optional and doesn’t affect the functionality. Description has to be created before assigning the cee-map to the interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>Step 3</td>
<td>group &lt;id(0-7,15)&gt; description {&lt;string(63)&gt;}</td>
<td>Creates a description for priority-group, which can be viewed in the show commands.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Exit</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# group 0 description "Download Traffic"
SMIS(config-cee-map)# exit
SMIS(config)# exit

SMIS# show cee-map 1

15.3.2.4 Map priority to priority-group
Multiple priorities can be bundled together to form a priority-group. In other words, the traffic will be assigned to priority-group based on their priority. The priority-groups are identified by PGID number 0 – 7 and 15. There are 8 priorities available and they are identified by number 0 - 7. More than one priority can be assigned to a priority-group.

A default priority-to-priority-group mapping will be created when a cee-map is created. The default mapping is shown below.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Group</th>
<th>PFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>No</td>
<td>LAN</td>
</tr>
</tbody>
</table>
### Allocate bandwidth to the priority-group

The 100% of bandwidth has to be divided as required and allocated among the 8 priority-groups. The total bandwidth allocated to 7 groups has to be 100.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>3</td>
<td>group-bandwidth &lt;bandwidth(0-100)&gt;</td>
<td>Allocates the bandwidth respectively to the priority-groups 0 - 7.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-ceed-map)# group-bandwidth 10 10 10 20 10 10 10 20
SMIS(config-ceed-map)# end

SMIS# show cee-map 1

---

Priority-group 15 is a special group; traffic shall be assigned to this group with no bandwidth limit, group-level PFC and members of this group are scheduled in strict priority order.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>3</td>
<td>pri2pg &lt;group(0-7, 15)&gt; &lt;&gt; &lt;&gt; &lt;&gt; &lt;&gt; &lt;&gt; &lt;&gt; &lt;&gt;</td>
<td>Maps the priority 0-7 respectively to the priority-groups.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-ceed-map)# pri2pg 1 1 1 2 2 7 1 15
SMIS(config-ceed-map)# end

SMIS# show cee-map 1
15.3.2.6 Enable PFC
Priority Flow Control (PFC) can be enabled for traffics based on priorities or priority-groups. PFC can be enabled/disabled in a cee-map before applying it to an interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>cee-map &lt;CEE-map-id(1-4)&gt;</td>
<td>Creates a cee-map.</td>
</tr>
<tr>
<td>Step 3</td>
<td>PFC priority &lt;pri(0-7)&gt; {enable</td>
<td>disable}</td>
</tr>
<tr>
<td></td>
<td>PFC group &lt;id(0-7)&gt; {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# pfc priority 1 enable
SMIS(config-cee-map)# pfc group 2 enable
SMIS(config-cee-map)# end

SMIS# show cee-map 1

Use disable option to disable the PFC.
SMIS# configure terminal
SMIS(config)# cee-map 1
SMIS(config-cee-map)# pfc priority 1 disable
SMIS(config-cee-map)# pfc group 2 disable
SMIS(config-cee-map)# end

15.3.3 Apply cee-map to the interface
After the cee-map configuration is complete, it has to be applied to the physical interface for it to take effect. Same cee-map can be applied to multiple interfaces.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>CEE &lt;CEE-map-id(1-4)&gt;</td>
<td>Applies the cee-map.</td>
</tr>
<tr>
<td>Step 4</td>
<td>dcbx cee</td>
<td>Enables DCBX.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

Example:
SMIS# configure terminal
SMIS(config)# interface fx-ethernet 0/1
SMIS(config-if)# cee 1
### 15.3.4 Configure TLVs (optional)

Information such as DCBX control state, configuration, etc are exchanged between DCBX peers using Type Length Value (TLV) over LLDP protocol. Local operational configuration of each DCBX parameter is handled by DCBX state machine by comparing and synchronizing with the settings of its DCBX peer. TLV configuration are setup specific or NIC specific. The example show below are only for illustration purpose.

Apply CEE-map and enable DCBX before configuring TLVs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface configuration mode. &lt;br&gt;<code>Interface-type</code> – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td>Step 3</td>
<td>CEE &lt;CEE-map-id(1-4)&gt;</td>
<td>Applies the cee-map.</td>
</tr>
<tr>
<td>Step 4</td>
<td>dcbx cee</td>
<td>Enables DCBX.</td>
</tr>
<tr>
<td>Step 5</td>
<td>LLDP TLV-select DCBX-CEE-PFC [advertise {on</td>
<td>off}] [willing {0</td>
</tr>
<tr>
<td>Step 6</td>
<td>LLDP TLV-select DCBX-CEE-pg [advertise {on</td>
<td>off}] [willing {0</td>
</tr>
<tr>
<td>Step 7</td>
<td>LLDP TLV-select basic-TLV { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all</td>
<td>IPV4 &lt;ucast_addr&gt;</td>
</tr>
<tr>
<td>Step 8</td>
<td>LLDP TLV-select dot1tlv { [port-VLAN-id] [protocol-VLAN-id {all</td>
<td>&lt;VLAN-id&gt;}] [VLAN-name {all</td>
</tr>
<tr>
<td>Step 9</td>
<td>LLDP TLV-select dot3tlv { [MACphy-config] [link-aggregation] [max-framesize] }</td>
<td>Configures dot3tlv.</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
<td>Exit from configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
SMIS# configure terminal
SMIS(config)# interface fx-ethernet 0/1
SMIS(config-if)# cee 1
SMIS(config-if)# dcbx cee
```
SMIS(config-if)# lldp tlv-select dcbx-cee-pfc advertise on willing 1 enable 0
SMIS(config-if)# lldp tlv-select dcbx-cee-pg advertise on willing 1 enable 0
SMIS(config-if)# end

Use the no form of the command to remove the configuration; shown below are some example.
SMIS(config-if)# no lldp tlv-select dcbx-cee-pfc
SMIS(config-if)# no lldp tlv-select dcbx-cee-pg
SMIS(config-if)# no lldp tlv-select basic-tlv port-descr
SMIS(config-if)# no lldp tlv-select basic-tlv sys-name
SMIS(config-if)# no lldp tlv-select basic-tlv sys-capab
SMIS(config-if)# no lldp tlv-select basic-tlv mgmt-addr all
SMIS(config-if)# no lldp tlv-select basic-tlv
# 15.4 Show commands for CEE-MAP and DCBX

Use ‘show interface’ command to check whether DCBX is enabled/disabled for the interface.

```
show cee-map [cee-map-id(1-4)]
```

**Example:**

```
SMIS# show interface cx-ethernet 0/1
Cx0/1 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port

Hardware Address is 0c:c4:7a:2c:19:63
MTU  1500 bytes, Full duplex, 100 Gbps, FEC is on, No-Negotiation
HOL Block Prevention enabled.
Input flow-control is off, output flow-control is off
**DCBX is Enable**
PFC is controlled by DCBX protocol

Link Up/Down Trap is enabled

Reception Counters
Octets                  : 1028282
Unicast Packets         : 7
Unicast Packets Rate    : 0/Sec
Broadcast Packets       : 0
Broadcast Packets Rate  : 0/Sec
Multicast Packets       : 13741
Multicast Packets Rate  : 0/Sec
Pause Frames            : 0
Undersize Frames        : 0
Oversize Frames         : 0
CRC Error Frames        : 0
Discarded Packets       : 0
Error Packets           : 0
Unknown Protocol        : 0

Transmission Counters
Octets                  : 219288
Unicast Packets         : 9
Unicast Packets Rate    : 0/Sec
Broadcast Packets       : 1
Broadcast Packets Rate  : 0/Sec
```
Multicast Packets : 2539  
Multicast Packets Rate : 0/Sec  
Pause Frames : 0  
Discarded Packets : 0  
Error Packets : 0  

Use ‘show cee-map’ to check the CEE-MAP configuration. This command displays the application-protocol to priority mapping, priority to priority-group mapping, and bandwidth allocation for the priority-groups.

**show cee-map [<cee-map-id(1-4)>]**

**Example:**

```
SMIS# show cee-map 1

CEE-Map 1

Ports : fx 0/1

<table>
<thead>
<tr>
<th>Priority</th>
<th>Group</th>
<th>PFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>No</td>
<td>LAN</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Yes</td>
<td>FCoE/FIP</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group</th>
<th>Bandwidth(%)</th>
<th>PFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10</td>
<td>No</td>
<td>LAN</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>Yes</td>
<td>SAN</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>20</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>MAX</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application-Protocol-ID</th>
<th>Type</th>
<th>Protocol-ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ether-type 0x8906</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
Use ‘show lldp dcbx’ command to check the current status/result of DCBX (CEE) use the below show command.

`show lldp dcbx interface [<interface-type> <interface-id>]`

**Example:**

SMIS# show lldp dcbx interface fx-ethernet 0/1
Fx0/1:
DCBX Control Message Exchange Information
--------------------------------------------
Status: Non-synchronized

Peer message seq#: 16777216 (acknowledged: 0)
Local message seq#: 2 (acknowledged: 16777216)

DCBX Feature Information
--------------------------------------------
Feature: PG, Priority Groups
Type/subtype: 2/0
Enabled: Yes
Advertisement: Yes
Willing: No
Error: No
Operation status: Operational
Config (operation/desired/peer):
  PG0...10 / 10 / 10
  PG1...10 / 10 / 10
  PG2...10 / 10 / 10
  PG3...20 / 20 / 20
  PG4...10 / 10 / 10
  PG5...10 / 10 / 10
  PG6...10 / 10 / 10
  PG7...20 / 20 / 20
  PG15...MAX / MAX / MAX
  #TCs...8 / 8 / 8

Feature: PFC, Priority-based Flow Control
Type/subtype: 3/0
Enabled: Yes
Advertisement: Yes
Willing: No
Error: No
Operation status: Operational
Config (operation/desired.pg/peer):
  Pri0...1 / 0.1 / 1
  Pri1...0 / 0.0 / 0
  Pri2...0 / 0.0 / 0
  Pri3...1 / 1.0 / 1
  Pri4...0 / 0.0 / 0
Pri5...0 / 0.0 / 0
Pri6...0 / 0.0 / 0
Pri7...1 / 0.1 / 1
#TCs...8 / 8 / 8

**Feature**: Application Protocol
**Type/subtype**: 4/0
**Enabled**: Yes
**Advertisement**: Yes
**Willing**: No
**Error**: No

**Operation status**: Operational

**Config (operation/desired/peer)**:

<table>
<thead>
<tr>
<th>Operation Config</th>
<th>Type</th>
<th>Protocol-ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ether-type</td>
<td>0x8906</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ether-type</td>
<td>0x8914</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>tcp-udp</td>
<td>3260</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Desired Config</th>
<th>Type</th>
<th>Protocol-ID</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ether-type</td>
<td>0x8906</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ether-type</td>
<td>0x8914</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>tcp-udp</td>
<td>3260</td>
<td></td>
</tr>
</tbody>
</table>

**Other related show commands:**

- SMIS# show lldp neighbors
- SMIS# show lldp neighbors detail
- SMIS# show lldp traffic
- SMIS# show lldp traffic [<iftype> <ifnum>]
15.5 Sample DCBX configuration

The sample configuration shown below is only for illustration purpose. As the DCBX configurations are setup specific, the configuration below doesn’t guarantee any function.

```
SMIS # show running-config

ip address dhcp

vlan 1
  ports fx 0/1-48 untagged
  ports cx 0/1-6 untagged
exit

set lldp enable

cee-map 2
  pri2pg 1 2 4 2 2 4 4 1
  pfc priority 1 enable
  group-bandwidth 10 10 10 20 10 10 10 20
  pfc group 2 enable
exit

ces-map 4
  pri2pg 0 1 2 3 4 5 6 7
  pfc priority 1 enable
  pfc priority 3 disable
  group-bandwidth 25 75 0 0 0 0 0 0
  pfc group 0 enable
exit

interface Fx 0/6
  cee 2
  dcbx cee

interface Cx 0/1
  cee 4
  dcbx cee
exit

SMIS#
```
16 IP Overview

Internet Protocol (IP), the foundation of the IP Protocol suite, is a packet-based protocol used for exchange of data over computer networks. IP is a network layer that contains addressing and control information to allow routing of data packets. IP handles addressing, fragmentation, reassembly, and protocol demultiplexing.

Supermicro switches supports both TCP and UDP at the transport layer, for maximum flexibility in services.
- Transmission Control Protocol (TCP) is a connection-oriented protocol built upon the IP layer. TCP specifies the format of data and acknowledgments used in the transfer of data and also the procedures used to ensure that the data arrives in correct order. With TCP multiple applications on a system can communicate concurrently as it handles all demultiplexing of the incoming traffic among the application programs.

- With UDP, applications can send messages, also called datagrams to other hosts on an IP network without prior setup of transmission channels or data paths. UDP is suitable when error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.

The following features of IP implementation in Supermicro switches are covered in this document.

- Layer 3 Interface
- Inter-VLAN routing
- Static Route
- ARP
- DHCP
- VRRP

16.1 Layer 3 Interface

The network layer or Layer 3 handles the routing of data in packets across logical internetwork paths. The data link layer or Layer 2 contains protocols that control the physical layer/Layer 1 and data framing for transmission on the physical medium. The Layer 2 function of filtering and forwarding data in frames between two segments on a LAN is known as bridging.

Supermicro switches support two types of Layer 3 interfaces.
- The Layer 3 VLAN Interface combines the functionality of routing and bridging.
- The Loopback Interface is a logical interface that is “always up”. It is not tied to any physical interface therefore it does not go down unless it is administratively shut down.

The uses of Layer 3 interface are:
- Allow traffic to be routed between VLANs.
- Provide Layer 3 IP connectivity to the switch.

16.1.1 Layer 3 VLAN Interface

VLANs typically operate at Layer 2. When a layer2 VLAN is configured with an IP address, it behaves as a logical Layer 3 VLAN interface. L3 VLAN interface provides logical routing interfaces to VLANs on Layer 2 switches. It is also called Switch Virtual Interfaces (SVI) and handles processing for all the packets associated with that VLAN.
Follow the steps below to configure Logical Layer3 Interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a Layer 2 VLAN and add all required ports.</td>
<td>For details on configuring Layer 2 VLAN, refer ‘VLAN Config. guide’ from <a href="http://www.supermicro.com">www.supermicro.com</a></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface vlan &lt;vlan-id (1-4069)&gt;</td>
<td>Enters interface configuration mode to specify the interface to be configured as a Layer 3 interface.</td>
</tr>
</tbody>
</table>
| Step 4 | ip address [<ip-address> | Configure IP address.  
| | | ip-address – A valid IPv4 Address.  
| | | ip-address/prefix-length - A valid IPv4 Address with a prefix length of value 1-32.  
| | | subnet-mask – A valid IP subnet mask.  
| | | Secondary - Assigns multiple IP addresses to network interfaces. |
| Step 5 | end | Exits the configuration mode. |
| Step 6 | show ip interface | Displays the Layer 3 interface information. |

The “no ip address [<ip_addr>]” command deletes the layer 3 VLAN interface and resets it as a Layer2 VLAN.

The example below shows the commands used to configure Logical Layer3 Interface.

SMIS# configure terminal  
SMIS(config)# vlan 10  
SMIS(config-vlan)# ports fx 0/22 untagged  
SMIS(config-vlan)# exit  

SMIS(config)# interface vlan 10  
SMIS(config-if)# ip address 10.10.10.1 255.255.255.0  
SMIS(config-if)# end

SMIS# show ip interface  

mgmt is up, line protocol is down  
Internet Address is 192.168.100.102/24  
Broadcast Address 192.168.100.255  
Gateway 0.0.0.0
vlan10 is up, line protocol is up  
Internet Address is 10.10.10.1/24  
Broadcast Address 10.10.10.255

### 16.1.2 Loopback Interface

Supermicro switches support loopback interface which is a virtual interface and is not connected to any other device. Loopback interfaces are very useful since they will never go down, unless the entire router goes down. This is useful for managing routers because there will always be at least one active interface on the routers, the loopback interface.

Follow the steps below to configure Loopback Interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface loopback &lt;interface-id (1-100)&gt;</td>
<td>Enters interface configuration mode to specify the interface to be configured as a Layer 3 interface.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip address [ip-address]</td>
<td>Configure IP address.</td>
</tr>
<tr>
<td></td>
<td>[ip-address]/prefix-length]</td>
<td>ip-address – A valid IPv4 Address.</td>
</tr>
<tr>
<td></td>
<td>[&lt;subnet-mask&gt;]</td>
<td>ip-address/prefix-length – A valid IPv4 Address with a prefix length of value 1-32.</td>
</tr>
<tr>
<td></td>
<td>subnet-mask – A valid IP subnet mask.</td>
<td>NOTE: Subnet mask should be 32 bit for loopback interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>no shutdown</td>
<td>Enable the Loopback interface</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip interface</td>
<td>Displays the Layer 3 interface configuration.</td>
</tr>
<tr>
<td></td>
<td>show interface loopback &lt;1-100&gt;</td>
<td>Display Loopback interface configuration.</td>
</tr>
</tbody>
</table>

---

*IP Routing is not supported on Loopback Interfaces.*

The “no interface loopback <interface-id (1-100)>” command deletes the Loopback interface.

SMIS# configure terminal  
SMIS(config)# interface loopback 1  
SMIS(config-if)# ip address 100.1.1.1/32  
SMIS(config-if)# no shutdown  
SMIS(config-if)# end
SMIS# show interface loopback 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback1</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>

SMIS# show ip interface

mgmt is up, line protocol is down
Internet Address is 192.168.100.102/24
Broadcast Address 192.168.100.255
Gateway 0.0.0.0

loopback1 is up, line protocol is up
Internet Address is 100.1.1.1/32
Broadcast Address 100.1.1.1

16.2 Inter-VLAN Routing

VLANs enable splitting traffic across several manageable broadcast domains. Devices within a VLAN can communicate with one another without requiring routing. Whenever hosts in one VLAN need to communicate with hosts in another VLAN, the traffic must be routed between them. This is known as Inter-VLAN Routing.

Supermicro switches use application-specific integrated circuits (ASICs), which are hardware chips that can route traffic at very high speeds. These ASICs are installed on the switching engine of a Layer 3 switch, which traditionally switches frames at Layer 2. The ASICs allow the switching engine to also switch frames that contain packets sent between different VLANs. Each ASIC is programmed with the information required to route traffic from one VLAN to another, without having to pass the traffic through the CPU of the routing engine.

Advantages of Inter-VLAN routing in L3 switches:
- Layer 3 switches are much more cost effective than routers for delivering high-speed inter-VLAN routing.
- Layer 3 switches are enhanced Layer 2 switches and, hence, have the same high port densities that Layer 2 switches have. Routers on the other hand typically have a much lower port density.
- Layer 3 switches can be configured to operate as a normal Layer 2 switch or Layer 3 switch as required.

Application of Inter-VLAN routing:
The network can be divided based on the group or function the device. For example, the engineering department VLAN would only have devices associated with the engineering department, while the HR VLAN would only have HR related devices. With Inter-VLAN routing, the devices in each VLAN can talk to one another without all the devices being in the same broadcast domain.

To WAN via Router

VLAN 300
Follow the steps below to configure Inter-VLAN Routing.

1. Create 2 Layer 3 interface VLAN’s.
2. Configure an IP address for both these Layer 3 VLAN interfaces.
3. Execute show ip route to check if the VLAN routes specified by VLAN IP address are displayed as connected routes. The routing table has an entry for each VLAN interface subnet, hence devices in VLAN 10 can communicate with devices in VLAN 20 and vice versa.

The example below shows the commands used to configure Inter-VLAN Routing.

SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/21 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.1 255.255.255.0
SMIS(config-if)# exit
SMIS(config)# vlan 20
SMIS(config-vlan)# ports fx 0/22 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 20
SMIS(config-if)# ip address 20.20.20.1 255.255.255.0
SMIS(config-if)# exit
SMIS# show ip interface

mgmt is up, line protocol is down
Internet Address is 192.168.100.102/24
Broadcast Address  192.168.100.255
Gateway 0.0.0.0
vlan10 is up, line protocol is up
Internet Address is 10.10.10.1/24
Broadcast Address  10.10.10.255

vlan20 is up, line protocol is up
Internet Address is 20.20.20.1/8
Broadcast Address  20.255.255.255

SMIS# show ip route

C 10.10.10.0/24 is directly connected, vlan10
C 20.0.0.0/8  is directly connected, vlan20
C 192.168.100.0/24 is directly connected, mgmt

16.3 Static Route

Static route define explicit paths between two routers. Manual reconfiguration of static routes is required when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

Routers forward packets using either route information from manually configured route table entries or the route information calculated using dynamic routing algorithms.

Use of Static route:

- Static routes can be used in environments where network traffic is predictable and where the network design is simple.
- Static routes are also useful for specifying a gateway of last resort (a default router to which all non-routable packets are sent).

Follow the steps below to configure Static Route.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip route &lt;prefix&gt; &lt;mask&gt; {&lt;next-hop&gt;</td>
<td>Vlan &lt;vlan-id (1-4096)&gt;</td>
</tr>
</tbody>
</table>

Prefix – The destination network IP address the route leads to.

Mask – A valid IP subnet mask

Next-hop – specify next-hop IP address.

Null - Specifies a null interface

Distance – specifies the administrative distance in the range 1 to 255. The default is 1.
Private - Specify whether this route can be shared with other routes when RIP is enabled.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exits the configuration mode.</strong></td>
<td></td>
</tr>
</tbody>
</table>

| Step 4 | show ip route [ { <ip-address> [mask] | bgp | connected | ospf | rip | static | summary } ] |
|--------|--------------------------------------------------|
| **Displays the route information** |

When an interface goes down, static routes through that interface are removed from the IP routing table.

When the next hop for the address is unreachable, the static route is removed from the IP routing table.

The “no ip route <prefix> <mask> { <next-hop> | Vlan <vlan-id(1-4069)> | <interface-type> <interface-id> | null0 } [private]” command deletes the static route.

The example below shows the commands used to configure Static Route.

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/21 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.1
SMIS(config-if)# exit
SMIS(config)# ip route 200.200.200.0 255.255.255.0 10.10.10.2
SMIS(config)# end

SMIS# show ip route static
S 200.200.200.0/24 [1] via 10.10.10.2
```

**16.4 ARP**

The Address Resolution Protocol (ARP) feature finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. This mapping of MAC addresses to IP addresses is stored in a table called ARP cache.

ARP is part of all Supermicro switches systems that run IP. Though Supermicro switches are layer 3 switches that forward packets based on IP address, ARP is required for certain cases like default gateway or for ping within same subnet.

**16.4.1.1 Cache Timeout**

The ARP cache can contain dynamic (learned) entries and static (user-configured) entries. Dynamic ARP entry is created in the ARP cache when the Layer 3 Switch learns a device’s MAC address from an ARP request or ARP reply from a device. ARP entries are refreshed periodically otherwise these entries are timed out and deleted from ARP cache.
16.4.1.2 ARP request retry
ARP requests can be re-sent by a device before confirming the host as unreachable. The number of times ARP request can be re-transmitted is user configurable in Supermicro switches.

16.4.1.3 Static ARP
For hosts that do not support dynamic Address Resolution Protocol (ARP), static entries can be added by defining static mapping between an IP address (32-bit address) and a Media Access Control (MAC) address (48-bit address). Static ARP entry in the ARP cache never times out. The entries remain in the ARP table until they are removed by user configuration.

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP request retry</td>
<td>3</td>
</tr>
<tr>
<td>ARP cache timeout</td>
<td>300</td>
</tr>
<tr>
<td>Static ARP entries</td>
<td>None</td>
</tr>
</tbody>
</table>

Follow the steps below to configure ARP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>arp timeout &lt;seconds (30-86400)&gt;</code></td>
<td>(Optional) Sets the length of time, in seconds, an Address Resolution Protocol (ARP) cache entry stays in the cache. The range is 30-86400 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: If there is frequent change in cache entries in network, suggest to ARP timeout to a shorter value.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`arp &lt;ip address&gt; &lt;hardware address&gt; {Vlan &lt;vlan-id(1-4069)&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ip-address</em> —IP address in four-part dotted decimal format corresponding to the local data-link address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>hardware-address</em>—Local data-link address (a 48-bit address).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Linuxvlan</em> - Interface name of Linux VLAN interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Cpu0</em> - Out-of-band management interface</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip arp max-retries &lt;value (2-10)&gt;</code></td>
<td>(Optional) To set the maximum number of ARP request retries in the range 2-10.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show ip arp</code></td>
<td>Displays the ARP table entries</td>
</tr>
</tbody>
</table>
These commands delete values or reset to default values, as applicable:

- `no arp timeout`
- `no arp <ip address>`
- `no ip arp max-retries`

The example below shows the commands used to configure ARP.

```
SMIS# configure terminal
SMIS(config)# arp timeout 800
SMIS(config)# ip arp max-retries 10
SMIS(config)# arp 10.0.0.0 48:2C:6A:1E:59:3D vlan 1
SMIS(config)# end
```

```
SMIS# show ip arp
Address          Hardware Address   Type  Interface  Mapping
-------                      -----------  ---  --------  ------
10.0.0.0         48:2c:6a:1e:59:3d  ARPA  vlan1      Static
```

```
SMIS# show ip arp summary
1 IP ARP entries, with 0 of them incomplete
```

```
SMIS# show ip arp information
ARP Configurations:
-------------------
Maximum number of ARP request retries is 10
ARP cache timeout is 800 seconds

16.5 DHCP

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP), which can automatically allocate reusable network addresses and configuration options to Internet hosts. DHCP is built on a client/server model, where designated DHCP servers allocate network addresses and deliver configuration parameters to DHCP clients.

When a DHCP client requests an IP address from a DHCP server, the client sends a DHCPDISCOVER broadcast message to locate a DHCP server. A relay agent forwards the packets between the DHCP client and server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.
Supermicro switches support Dynamic Host Configuration Protocol (DHCP) server, DHCP client and DHCP relay agent functionality.

### 16.5.1 DHCP Server

Supermicro switches DHCP server implementation assigns and manages IP addresses from specified address pools to DHCP clients. The DHCP server can also be configured to assign additional parameters like default router, IP address of the Domain Name System (DNS) server etc. The DHCP server can accept broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

![Diagram of DHCP server and client](image)

**Figure IP-2: DHCP Server**

#### 16.5.1.1 DHCP Address Pool

Supermicro switches DHCP server accepts address assignment requests and renewals and assigns the addresses from predefined groups of addresses contained within *DHCP address pools*. These address pools can also be configured to supply additional information to the requesting client such as the IP address of the DNS server, the default router, and other configuration parameters.

#### 16.5.1.2 Additional Parameter - Default Router & DNS

The DHCP server can be configured to assign additional parameters such as the IP address of the Domain Name System (DNS) server and the default router to the DHCP clients.

Default route IP address should be on the same subnet as the client. When a DHCP client requests an IP address, the DHCP server accesses the default router list to select another router that the DHCP client is to use as the first hop for forwarding messages.

#### 16.5.1.3 Excluding IP address

By default, the DHCP Server assumes all IP addresses in the configured DHCP address pool are available for assigning to DHCP clients. If a particular address or range of addresses should not be assigned to DHCP clients, users can configure these excluded IP addresses.
16.5.1.4 Utilization Threshold

A DHCP address pool has a threshold associated with it. If a pool’s outstanding addresses exceed the high utilization threshold and the SNMP trap signaling is enabled, SNMP is notified.

16.5.1.5 Lease

DHCP supports three mechanisms for IP address allocation:

• Automatic allocation—DHCP server assigns a permanent IP address to a client.
• Dynamic allocation—DHCP server assigns an IP address to a client from the address pool for a limited period of time called a lease or until the client relinquishes the address.
• Manual allocation—The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

16.5.1.6 Options and Sub-options

Configuration parameters and control information are available in the options field of the DHCP message. This can be used when additional information need not be stored in DHCP client, rather it can be transmitted by the DHCP server to the client.

Some DHCP clients send a client identifier (DHCP option 61) in the DHCP packet to DHCP server. To configure manual bindings for such clients, configure the client-identifier DHCP pool configuration. To configure manual bindings for clients who do not send a client identifier option, configure the hardware-address DHCP pool configuration.

16.5.1.7 Bootfile

The boot file is used to store the boot image for the client. The boot image is generally the operating system the Dynamic Host Configuration Protocol (DHCP) client uses to load.

16.5.1.8 DHCP Ping

The DHCP server pings a pool address twice before assigning a particular address to a requesting client. If the ping is unanswered, the DHCP server assumes that the address is not in use and assigns the address to the requesting client.

16.5.1.9 DHCP Server Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server status</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP Server IP address</td>
<td>None</td>
</tr>
<tr>
<td>DHCP pool index</td>
<td>None</td>
</tr>
<tr>
<td>DHCP network IP</td>
<td>None</td>
</tr>
<tr>
<td>Excluded Address</td>
<td>None</td>
</tr>
<tr>
<td>Domain Name</td>
<td>None</td>
</tr>
<tr>
<td>DNS server</td>
<td>None</td>
</tr>
<tr>
<td>NetBIOS name server</td>
<td>None</td>
</tr>
</tbody>
</table>
### Enabling DHCP server

DHCP server is disabled by default in Supermicro switches. Follow the steps below to enable DHCP Server.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>service dhcp-server</td>
<td>Enable DHCP server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip dhcp server information</td>
<td>Displays the DHCP server configuration details.</td>
</tr>
</tbody>
</table>

DHCP Relay must be disabled before enabling DHCP Server.

The `no service dhcp-server` command disables the DHCP server.

### Configuring DHCP pool

Follow the steps below to configure DHCP Server pool.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip dhcp pool &lt;index (1-2147483647)&gt;</td>
<td>Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>network &lt;network-IP&gt; [ { &lt;mask&gt;</td>
<td>/ &lt;prefix-length (1-31)&gt; } ] [&lt;start-ip&gt; [&lt;end-ip&gt;]]</td>
</tr>
</tbody>
</table>

- **Network-ip** – A valid IPv4 Address.
- **prefix-length** - A valid IPv4 Address with a prefix length of value 1-32.
- **mask** – A valid IP subnet mask.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| 4     | `excluded-address <low-address> < high-address>` | (Optional) Specify the range of IP addresses that the DHCP server must not assign to DHCP clients in the range `low-address` to `high-address`.
<p>| 5     | <code>domain-name &lt;domain (63)&gt;</code>   | (Optional) Specifies the domain name for the client.                                            |
| 6     | <code>dns-server &lt;ip address&gt;</code>     | (Optional) Specifies the IP address of a DNS server that is available to a DHCP client.       |
| 7     | <code>netbios-name-server &lt;ip address&gt;</code> | (Optional) Specifies the NetBIOS WINS server that is available to a Microsoft DHCP client. |
| 8     | <code>netbios-node-type { &lt;0-FF&gt; | b-node | h-node | m-node | p-node }</code> | (Optional) Specifies the NetBIOS node type for a Microsoft DHCP client.                      |
|       |                                | <code>b-node</code> – Broadcast node                                                                    |
|       |                                | <code>h-node</code> – Hybrid node                                                                      |
|       |                                | <code>m-node</code> – Mixed node                                                                       |
|       |                                | <code>p-node</code> – Peer to peer node                                                                 |
| 9     | <code>option &lt;code (1-2147483647)&gt; { ascii &lt;string&gt; | hex &lt;Hex String&gt; | ip &lt;address&gt; }</code> | (Optional) Configures DHCP server options.                                                     |
|       |                                | Configurable DHCP options with corresponding option length values are:                     |
|       |                                | - Options 19, 20, 27, 29, 30, 31, 34, 36, 39, 46 must have length 1                           |
|       |                                | - Options 12, 14, 15, 17, 18, 40, 43, 47, 64, 66, 67 must have length &gt;=1                    |
|       |                                | - Option 16 must have minimum length 4 and the value for this option must be an IP address and Option 25 can have a length of 2 and 2<em>n |
|       |                                | - Option 68 must have length 4 and the value for this option must be an IP address          |
|       |                                | - Options 1-11, 41, 42, 44, 45, 48, 49, 65, 69, 70-76 must have a length of 4. Value for these options must be an IP address |
|       |                                | - Options 21, 33 must have minimum length as 8 and 8</em>n                                        |
|       |                                | - Options 0, 255, 50-60 are non-configurable options                                          |
| 10    | <code>lease { &lt;days (0-365)&gt; [ &lt;hours (0-23)&gt; [ &lt;minutes (0-59)&gt; ] | infinite }</code> | (Optional) Specifies the duration of the lease. The infinite keyword specifies that the duration of the lease is unlimited. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 11</td>
<td>utilization threshold { &lt;integer (0-100)&gt; }</td>
<td>(Optional) Configures the utilization mark of the current address pool size.</td>
</tr>
<tr>
<td>Step 12</td>
<td>default-router &lt;ip address&gt;</td>
<td>(Optional) Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>Step 13</td>
<td>host hardware-type &lt;type (1-2147483647)&gt; client-identifier &lt;mac-address&gt; option &lt;code (1-2147483647)&gt; { ascii &lt;string&gt;</td>
<td>hex &lt;Hex String&gt;</td>
</tr>
</tbody>
</table>

mac-address - Specifies MAC address of a DHCP client in dotted hexadecimal notation.

string - ASCII-format representation of a MAC address

address - Specifies the IP address and network mask for a manual binding to a DHCP client.

| Step 14 | end | Exits the configuration mode. |
| Step 15 | show ip dhcp server pools | Displays the DHCP pool configuration. |

The “no ip dhcp pool <index (1-2147483647)>” command deletes the DHCP pool configuration.

These commands delete values or reset to default values, as applicable:

no network
no excluded-address <low-address> [high-address>]
no domain-name
no dns-server
no netbios-name-server
no netbios-node-type
no default-router
no option <code (1-2147483647)> 
no lease
no utilization threshold
no host hardware-type <host-hardware-type (1-2147483647)> client-identifier <client-mac-address> option <code (1-2147483647)> |

16.5.1.9.3 Configuring other parameters

Follow the steps below to configure DHCP Server parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip dhcp bootfile &lt;bootfile (63)&gt;</td>
<td>(Optional) Specifies the name of the default boot image for a DHCP client.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip dhcp next-server &lt;ip address&gt;</code></td>
<td>(Optional) Configures the next server in the boot process of a DHCP client.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`ip dhcp option &lt;code (1-2147483647)&gt; { ascii &lt;string&gt;</td>
<td>hex &lt;Hex String&gt;</td>
</tr>
<tr>
<td>Step 5</td>
<td>`ip dhcp { ping packets</td>
<td>server offer-reuse &lt;timeout (1-120)&gt; }`</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>Server offer-reuse</code> - Specify the maximum timeframe after which an offered IP address can be returned to the pool of free addresses.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show ip dhcp server information</code></td>
<td>Displays the DHCP server configuration details.</td>
</tr>
<tr>
<td></td>
<td><code>show ip dhcp server statistics</code></td>
<td>Displays DHCP packet statistics.</td>
</tr>
</tbody>
</table>

These commands delete values or reset to default values, as applicable:

- `no ip dhcp bootfile`
- `no ip dhcp next-server`
- `no ip dhcp option <code (1-2147483647)>`
- `no ip dhcp { ping packets | server offer-reuse | binding <ip address> }`

The example below shows the commands used to configure DHCP Server.

```
SMIS# configure terminal
SMIS(config)# service dhcp-server
SMIS(config)# ip dhcp server 100.100.100.1
SMIS(config)# ip dhcp pool 1
SMIS(dhcp-config)# network 200.200.0.0 255.255.0.0
SMIS(dhcp-config)# excluded-address 200.200.20.20 200.200.20.30
SMIS(dhcp-config)# dns-server 10.10.10.1
SMIS(dhcp-config)# domain-name supermicro.com
SMIS(dhcp-config)# netbios-name-server 172.16.1.3
SMIS(dhcp-config)# netbios-node-type h-node
SMIS(dhcp-config)# option 19 hex 1
SMIS(dhcp-config)# lease infinite
SMIS(dhcp-config)# utilization threshold 50
SMIS(dhcp-config)# host hardware-type 1 client-identifier 00:A0:23:C9:12:FF option 10 IP 10.10.10.1
SMIS(dhcp-config)# default-router 192.168.1.10
SMIS(dhcp-config)# exit
SMIS(config)# ip dhcp bootfile abcboot
SMIS(config)# ip dhcp next-server 172.17.10.3
```
SMIS(config)# ip dhcp ping packets
SMIS(config)# end

SMIS# show ip dhcp server information

DHCP server status         : Enable
Send Ping Packets          : Enable
Debug level                : None
Server Address Reuse Timeout : 5 secs
Next Server Address        : 172.17.10.3
Boot file name             : abcboot

SMIS# show ip dhcp server pools

Pool Id : 1
-------------------------------------------
Subnet       : 200.200.0.0
Subnet Mask  : 255.255.0.0
Lease time   : 2147483647 secs
Utilization threshold : 50%
Start Ip     : 200.200.0.1
End Ip       : 200.200.255.255
Exclude Address Start IP  : 200.200.20.20
Exclude Address End IP     : 200.200.20.30

Subnet Options
--------------
Code  : 1, Value : 255.255.0.0
Code  : 3, Value : 192.168.1.10
Code  : 6, Value : 10.10.10.1
Code  : 15, Value : supermicro.com
Code  : 19, Value : 1
Code  : 44, Value : 172.16.1.3
Code  : 46, Value : 8

Host Options
------------
Hardware type : 1
Client Identifier : 00:a0:23:c9:12:ff
Code  : 10, Value : 10.10.10.1

SMIS# show ip dhcp server statistics

Address pools : 1

<table>
<thead>
<tr>
<th>Message</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER</td>
<td>0</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>0</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>0</td>
</tr>
</tbody>
</table>
DHCP RELEASE 0
DHCPINFORM 0

Message Sent
------- ----
DHCP OFFER 0
DHCP ACK 0
DHCP NAK 0

16.5.2 DHCP Client
Supermicro switches can function as Dynamic Host Configuration Protocol (DHCP) client to obtain configuration parameters such as an IP address from the DHCP server.

![Diagram of DHCP Client and Server](image)

**Figure IP-3: DHCP Client**

16.5.2.1 Release Client
The release dhcp command starts the process to immediately release a DHCP lease for the specified interface. After the lease is released, the interface address is deconfigured.

16.5.2.2 Renew Client
The DHCP client lease can be renewed by user configuration. The renew dhcp command advances the DHCP lease timer to the next stage, after which a DHCP REQUEST packet is sent to renew or rebinding the lease.

- If the lease is currently in a BOUND state, the lease is advanced to the RENEW state and a DHCP RENEW request is sent. If there is no response to the RENEW request, the interface remains in the RENEW state and the lease timer will advance to the REBIND state, and then sends a REBIND request. If a NAK response is sent in response to the RENEW request, the interface IP address is deconfigured. The original IP address for the interface must be assigned by the DHCP server.

- If the lease is currently in a RENEW state, the timer is advanced to the REBIND state and a DHCP REBIND request is sent.

Follow the steps below to configure DHCP Client.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>

Page 396
### VLAN should be created before configuring VLAN client on that particular VLAN.

The **no ip address dhcp** command deletes the DHCP client configuration.

The example below shows the commands used to configure DHCP Client.

```
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address dhcp
SMIS(config-if)# end

SMIS# show ip interface

    mgmt is up, line protocol is up
    Internet Address is 172.18.0.84/24
    Broadcast Address 172.18.0.255
    Gateway 172.18.0.254
    IP address allocation method is dynamic
    IP address allocation protocol is dhcp

    vlan200 is up, line protocol is down
    Internet Address is 10.10.10.2/8
    Broadcast Address 10.255.255.255
    IP address allocation method is dynamic
    IP address allocation protocol is dhcp
```

### DHCP Relay Agent

In small networks with only one IP subnet DHCP clients can communicate directly with DHCP servers. In large networks DHCP servers provide IP addresses for multiple subnets. In such cases, a DHCP client that has not yet obtained an IP address from the DHCP server cannot communicate with the DHCP server using IP routing. A DHCP relay agent forwards DHCP packets between clients and servers when they are not on the same physical subnet.
The relay agent receives the broadcast from the DHCP client and unicasts it to one or more DHCP servers. The relay agent stores its own IP address in the GIADDR field of the DHCP packet. The DHCP server uses the GIADDR to determine the subnet on which the relay agent received the broadcast, and allocates an IP address on that subnet. When the DHCP server replies to the client, it unicasts the reply to the GIADDR address. The relay agent then retransmits the response on the local network.

### 16.5.3.1 Relay Agent Information option

The relay agent information option (option 82) includes additional information about DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. The relay agent will automatically add the circuit identifier sub-option and the remote ID suboption to the relay agent information option and forward it to the DHCP server.

### 16.5.3.2 Circuit-ID Sub-option

Agent Circuit ID, suboption 1 is an ASCII string that identifies the interface on which a client DHCP packet is received.

### 16.5.3.3 Remote-ID Sub-option

Agent Remote ID, suboption 2 is an ASCII string assigned by the relay agent that securely identifies the client.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Relay status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Relay Information Option</td>
<td>Disabled</td>
</tr>
<tr>
<td>Circuit ID</td>
<td>None</td>
</tr>
<tr>
<td>Remote ID</td>
<td>None</td>
</tr>
</tbody>
</table>

Follow the steps below to configure DHCP Relay.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>service dhcp-relay</td>
<td>Enable DHCP relay.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dhcp server &lt;ucast_addr&gt;</td>
<td>Configure the DHCP server IP address.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip dhcp relay information option</code></td>
<td>(Optional) Enables DHCP relay agent information option to be sent by DHCP relay agent.</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ip dhcp relay circuit-id &lt;circuit-id&gt;</code></td>
<td>(Optional) Specify Circuit ID sub-option</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ip dhcp relay remote-id &lt;remote-id name&gt;</code></td>
<td>(Optional) Specify Remote ID sub-option</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>show ip dhcp relay information</code></td>
<td>Displays the DHCP relay configuration.</td>
</tr>
</tbody>
</table>

DHCP Server must be disabled before enabling DHCP Relay.

These commands delete values or reset to default values, as applicable:

```
  no service dhcp-relay
  no ip dhcp server <ip address>
  no ip dhcp relay information option
  no ip dhcp relay circuit-id
  no ip dhcp relay remote-id
```

The example below shows the commands used to configure DHCP Relay.

```
SMIS# configure terminal
SMIS(config)# service dhcp-relay
SMIS(config)# ip dhcp server 172.1.3.15
SMIS(config)# ip dhcp relay information option
SMIS(config)# end
SMIS# show ip dhcp relay information

Dhcp Relay : Enabled
Dhcp Relay Servers only : Enabled

DHCP server 1 : 172.1.3.15

Dhcp Relay RAI option : Enabled
Debug Level : 0x0

No of Packets inserted RAI option : 0
No of Packets inserted circuit ID suboption : 0
No of Packets inserted remote ID suboption : 0
No of Packets inserted subnet mask suboption : 0
No of Packets dropped : 0
No of Packets which did not inserted RAI option : 0
```

**16.6 VRRP**

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration.
Examples of dynamic router discovery are Proxy ARP, Routing protocol(s), ICMP Router Discovery Protocol (IRDP) client. The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

Figure IP-4: VRRP

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway.

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

16.6.1.1 Priority
The VRRP priority determines the role of each VRRP router. If a VRRP router owns the virtual IP address and the IP address of the physical interface, this router functions as the master. The priority of the master is 255. Priority also determines the backup router in case of failure of master – The backup router with next highest priority is elected as master.

For example, if Router A, the master in a LAN topology, fails, VRRP must determine if backups B or C should take over. If Router B has priority 101 and Router C has default priority of 100, VRRP selects Router B to become the master because it has the higher priority. If routers B and C have default priority of 100, VRRP selects the backup with the higher IP address to become the master.

16.6.1.2 Preemption
VRRP uses preemption to determine what happens after a VRRP backup router becomes the master. With preemption enabled by default, VRRP switches to a backup if that backup comes online with a priority higher than the new master.

For example, if Router A is the master and fails, VRRP selects Router B (next in order of priority). If Router C comes online with a higher priority than Router B, VRRP selects Router C as the new master, even though Router B has not failed. If preemption is disabled, VRRP switches only if the original master recovers or the new master fails.

16.6.1.3 Periodic Advertisement
The VRRP master sends VRRP advertisements to other VRRP routers in the same group to communicate the priority and state of the master. Supermicro switches encapsulate the VRRP advertisements in IP packets and send them to the IP multicast address assigned to the VRRP group. Supermicro switches send the advertisements once every second by default, but you can configure a different advertisement interval.

16.6.1.4 Authentication
VRRP supports the following authentication functions:
• No authentication
• Plain text authentication

VRRP rejects packets in any of the following cases:
• The authentication schemes differ on the router and in the incoming packet.
• Text authentication strings differ on the router and in the incoming packet.

VRRP is not a replacement for existing dynamic protocols.

Defaults
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>VRID</td>
<td>0</td>
</tr>
<tr>
<td>Priority</td>
<td>100</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>Pre-empt</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>1</td>
</tr>
</tbody>
</table>

Follow the steps below to configure VRRP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router vrrp</td>
<td>Enables VRRP in the switch</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface [{ vlan &lt;vlan-id (1-4069)&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt; }]</td>
</tr>
<tr>
<td>Step 4</td>
<td>vrrp &lt;vrid(1-255)&gt; ipv4 &lt;ucast_addr&gt; [secondary]</td>
<td>Configures the virtual IPv4 address for the specified VRRP group. This address should be in the same subnet as the IPv4 address of the interface. Secondary – Specify VRRP routers accept the packets sent to the virtual router's IP address</td>
</tr>
<tr>
<td>Step 5</td>
<td>vrrp &lt;vrid(1-255)&gt; priority &lt;priority(1-254)&gt;</td>
<td>Sets the priority level used to select the active router in an VRRP group. The default is 100 for backups and 255 for a master that has an interface IP address equal to the virtual IP address.</td>
</tr>
<tr>
<td>Step 6</td>
<td>vrrp &lt;vrid(1-255)&gt; preempt</td>
<td>(Optional) Enable preemption.</td>
</tr>
<tr>
<td>Step 7</td>
<td>vrrp &lt;vrid(1-255)&gt; text-authentication &lt;password&gt;</td>
<td>(Optional) Assigns the simple text authentication option and specifies the keyname password. The keyname range is from 1 to 255 characters. We recommend that you use at least 16 characters. The text password is up to eight alphanumeric characters.</td>
</tr>
<tr>
<td>Step 8</td>
<td>vrrp &lt;vrid(1-255)&gt; timer &lt;interval(1-255)secs&gt;</td>
<td>(Optional) Sets the VRRP advertisement interval time.</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 10</td>
<td>show vrrp</td>
<td>Displays the VRRP configuration.</td>
</tr>
<tr>
<td></td>
<td>show vrrp detail</td>
<td>Displays the VRRP configuration with additional details like advertisement timer, authentication details etc.</td>
</tr>
</tbody>
</table>
These commands delete values or reset to default values, as applicable:

- `no router vrrp`
- `no interface [Vlan <vlan-id (1-4069)> | <interface-type> <interface-id>]`
- `no vrrp <vrid(1-255)> ipv4 [<ucast_addr> [secondary]]`
- `no vrrp <vrid(1-255)> priority`
- `no vrrp <vrid(1-255)> preempt`
- `no vrrp <vrid(1-255)> text-authentication`
- `no vrrp <vrid(1-255)> timer`

The example below shows the commands used to configure VRRP.

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/15 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 172.1.10.1
SMIS(config-if)# end

SMIS# configure terminal
SMIS(config)# router vrrp
SMIS(config-vrrp)# interface vlan 10
SMIS(config-vrrp-if)# vrrp 200 ipv4 10.10.10.1
SMIS(config-vrrp-if)# vrrp 200 preempt
SMIS(config-vrrp-if)# vrrp 200 priority 100
SMIS(config-vrrp-if)# vrrp 200 text-authentication pwd1
SMIS(config-vrrp-if)# vrrp 200 timer 255
SMIS(config-vrrp-if)# vrrp 100 ipv4 100.100.100.1
SMIS(config-vrrp-if)# vrrp 100 priority 254
SMIS(config-vrrp-if)# vrrp 100 text-authentication pwd2
SMIS(config-vrrp-if)# vrrp 100 timer 100
SMIS(config-vrrp-if)# end

SMIS# show vrrp
```

P indicates configured to preempt

```
Interface  vrid Priority  P  State    Master Addr     VRouter Addr
------------ ---- ---------- -  -----     ----------     ---------------
vlan10      100  254       P  Init     0.0.0.0         100.100.100.1
vlan10      200  100       P  Init     0.0.0.0         10.10.1.1

SMIS# show vrrp detail
```

```
vlan10 - vrid 100

State is Init
Virtual IP address is 100.100.100.1
```
Virtual MAC address is 00:00:5e:00:01:64
Master router is 0.0.0.0
Associated IpAddresses :
----------------------
100.100.100.1
Advertise time is 100 secs
Current priority is 254
Configured priority is 254, may preempt
Configured Authentication
Authentication key is pwd2
vlan10 - vrID 200
----------------------

State is Init
Virtual IP address is 10.10.10.1
Virtual MAC address is 00:00:5e:00:01:c8
Master router is 0.0.0.0
Associated IpAddresses :
----------------------
10.10.10.1
Advertise time is 255 secs
Current priority is 100
Configured priority is 100, may preempt
Configured Authentication
Authentication key is pwd1

17 IP Multicast Overview

IP communication is of three types:

- Unicast: Host sends packets to a single host
- Broadcast: Host sends packets to all hosts
- Multicast: Host sends packets to a subset of hosts simultaneously

IP Multicast Routing enables efficient usage of network resources for bandwidth intensive services including video and audio. A multicast group is a set of receivers that want to receive a particular data stream. An IP Multicast Group Address in the range 224.0.0.0 to 239.0.0.0 is selected for receivers of a multicast group. Senders transmit IP data using the Multicast Group address as the destination address to multicast to all group members. Receivers interested in receiving data of a particular group must join the group by signaling a router/switch on their subnet. IGMP is used as the signaling protocol for conveying group membership. Network devices along the path from Source to Receivers forward data only on ports leading to the receivers, rather than flooding on all ports.

Membership in a multicast group is dynamic as hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.
Supermicro switches can send and receive Multicast traffic by supporting the following Multicast features:

- **IGMP** at the access end of the network that processes hosts announcing their participation in a Multicast group(s).

- **Multicast Routing Protocol’s (MRP’s)** at the enterprise and core of the network for maintaining the senders/receivers database and forwarding data from Senders to Receivers.

**Figure IGMP-1: IP Multicast Routing**

17.1 **IGMP Basics**

IGMP is an IPv4 protocol used by hosts to request Multicast data for a particular group. A switch performs the IGMP function by

- Sending IGMP query messages to identify receivers interested in particular Multicast group(s). IGMP query is sent only by a querier.
- Processing IGMP report messages from hosts in response to the query message from the querier.

Switch maintains a multicast forwarding table based on the hosts joined for every multicast group and updates the multicast forwarding table when hosts leave multicast groups.

In figure IGMP-2, the querier switch sends an *IGMP General Query* message on the LAN. Host1 and Host2 respond to the query with the *IGMP report* for G1 Group membership.
IGMP has 3 versions. The basic difference between the versions is:

IGMP v1: Supports basic query-response mechanism to identify active Multicast group(s).

IGMP v2: Extends v1 with features like querier election, IGMP Leave, group-specific query and maximum response time field.

IGMP v3: Provides support for source-specific query and report in addition to IGMP v1 and IGMPv2 features.

Supermicro switch acts as a querier by default as long as it is the Multicast router with lower IP address on the subnet.

### 17.2 IGMP Support

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

Supermicro switches support up to 255 multicast groups.

### 17.3 IGMP Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP global status</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP status in VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP version</td>
<td>2</td>
</tr>
<tr>
<td>Query interval</td>
<td>125</td>
</tr>
</tbody>
</table>
### 17.4 Enabling IGMP

IGMP is disabled by default in Supermicro switches.

IGMP needs to be enabled globally and also needs to be enabled in interfaces individually.

Follow the steps below to enable IGMP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip igmp enable</td>
<td>Enables IGMP globally.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface vlan &lt;id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface range &lt;interface-type&gt; &lt;interface-id&gt; ....</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;interface-type&gt; – may be any of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;interface-id&gt; is the VLAN identifier for VLAN interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide a range use a hyphen (-) between the start and end interface numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E.g.: interface range vlan 10-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.</td>
</tr>
<tr>
<td>Step 4</td>
<td>set ip igmp enable</td>
<td>Enables IGMP on interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp global-config</td>
<td>Displays the IGMP information.</td>
</tr>
<tr>
<td></td>
<td>show ip igmp interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>
The example below shows the commands to enable IGMP.

**Enable IGMP for layer3 VLAN 10**

SMIS(config)#configure terminal
SMIS(config)# set ip igmp enable
SMIS(config)#end

SMIS# show ip igmp global-config
IGMP is globally enabled

SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# set ip igmp enable
SMIS(config-if)#end

SMIS# show ip igmp interface
vlan10, line protocol is up
  Internet Address is 2.2.2.2/8
  IGMP is enabled on interface
  Current IGMP router version is 2
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
  IGMP max query response time is 100 seconds
  Robustness value is 2
  IGMP querying router is 2.2.2.2 (this system)
  Fast leave is disabled on this interface
  No multicast groups joined

### 17.5 IGMP Version

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

The default IGMP version is v2, which works compatible with IGMP versions 1 and 3.

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

Follow the steps below to change IGMP version on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface range &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>
interface-type – may be any of the following:
  vlan

interface-id is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: interface range vlan 10-20

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: interface range vlan 10,20

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

| Step 3 | ip igmp version \{ 1 | 2 | 3\} | Configures IGMP version. |
|--------|--------------------------------|--------------------------|
| Step 5 | end                            | Exits the configuration mode. |
| Step 6 | show ip igmp interface \langle interface-type\rangle \langle interface-id\rangle | Displays the IGMP version information for the given interface. |
| Step 7 | write startup-config           | Optional step – saves this IGMP configuration to be part of the startup configuration. |

The “no ip igmp version” command resets the IGMP version to its default value of 2.

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

**Configure IGMP version 3 for layer3 VLAN 10.**

SMIS# configure terminal
SMIS(config)# interface vlan 10
SMIS(config-if)# ip igmp version 3
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 3
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined

17.6  IGMP query and report

When IGMP is enabled in Supermicro switch, it assumes itself as querier. As long as switch does not receive an IGMP query from another Multicast router in the subnet, with IP address lower than itself, it continues to be the IGMP querier on the subnet. If Supermicro switch acting as querier receives a query from another Multicast router on the subnet with an IP address lower than itself, then the switch transitions to a non-querier role and resets a timer that is based on value of its querier timeout. Upon expiry of the querier timer, Supermicro switch transitions to querier again, if there are no queries from the router with lower IP address, otherwise it continues to remain the non-querier on the subnet.

The querier switch is in charge of sending periodic query messages on the network to determine the presence of any new hosts. In response to query message from the querier, hosts respond with IGMP report messages indicating inclusion or exclusion of a particular Multicast Group address. The querier consolidates the reports from all hosts and maintains it in an IGMP group table.

There are various parameters that control the query messages and report messages:

**Query Interval**: This configures the time interval between transmissions of query messages by querier.

**Max Response Time**: This configures the maximum time interval until which the querier will wait for receiving reports from the hosts

**Robustness Value**: This parameter tunes certain intervals used in IGMP protocol and also determines the retransmissions of IGMPv3 report messages to prevent loss in network.

17.6.1  Query Interval

IGMP querier sends IGMP queries periodically to determine if there are any new hosts. This periodic time interval is called the *query interval*.

The default query interval is 125 seconds.

Supermicro switches provide flexibility for user to configure query interval for individual interfaces. User can configure different query interval on different interfaces.

Follow the steps below to change query interval on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
### Step 2

**Interface** `<interface-type> <interface-id>`  
or  
**interface range** `<interface-type> <interface-id>` ....

Enters the interface configuration mode.

*interface-type* – may be any of the following:

- `vlan`

*interface-id* is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “**interface range** ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: **interface range vlan 10-20**

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: **interface range vlan 10,20**

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

### Step 3

**ip igmp query-interval <value>**

Configures IGMP query interval.

The query interval value can be 1-65535 seconds. Default is 125 seconds.

### Step 5

**end**

Exits the configuration mode.

### Step 6

**show ip igmp interface** `<interface-type> <interface-id>`

Displays the IGMP query interval information for the given interface.

### Step 7

**write startup-config**

Optional step – saves this IGMP configuration to be part of the startup configuration.

---

The “**no ip igmp query-interval**” command resets the IGMP query interval to its default value of 125.

---

The example below shows the commands to configure IGMP query interval.

**Configure IGMP query interval for layer3 VLAN 10**

```
SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
```
SMIS(config-if)# ip igmp query-interval 500
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 500 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined

SMIS# show ip igmp statistics
IGMP Statistics for vlan10
Number of General queries received 0
Number of Group Specific queries received 0
Number of Group and Source Specific queries received 0
Number of v1/v2 reports received 0
Number of v3 reports received 0
Number of v2 leaves received 0
Number of General queries transmitted 32
Number of Group Specific queries transmitted 0
Number of Group and Source Specific queries transmitted 0

17.6.2 Maximum query response time
For every inclusion report received by the querier, the particular interface entry is added in the IGMP
group table for that particular group. A timer of value Group membership timeout is started for each
group/interface entry in the IGMP group table. The query response interval is used to calculate the group
membership timeout.

Group membership timeout = (robustness value * query interval) + max query response interval

Once a query is received by the hosts, the hosts should respond with IGMP reports within Max query
response time. The querier deletes the hosts’ interface entry from the IGMP group table if no reports are
received from the host until expiry of Group membership timeout.

The default query-max-response time is 100 seconds.

Supermicro switches provide flexibility for user to configure query-max-response time for individual
interfaces. User can configure different query-max-response time on different interfaces.

Follow the steps below to change query-max-response on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | interface `<interface-type> <interface-id>` or interface range `<interface-type> <interface-id>` .... | Enters the interface configuration mode.  

`interface-type` – may be any of the following: 

- `vlan`  

`interface-id` is the VLAN identifier for VLAN interfaces.  

To configure multiple interfaces, use the “`interface range ...`” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: `interface range vlan 10-20`  

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: `interface range vlan 10,20`  

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces. |
|-------|-------------------------------------------------|-------------------------------------------------|
| Step 3 | `ip igmp query-max-response-time <value>`   | Configures IGMP query-max-response time.  

The value of query-max-response time is 1-255 seconds. Default is 100 seconds. |
| Step 5 | `end` | Exits the configuration mode. |
| Step 6 | `show ip igmp interface `<interface-type>` `<interface-id>` | Displays the IGMP query-max-response time information for the given interface. |
| Step 7 | `write startup-config` | Optional step – saves this IGMP configuration to be part of the startup configuration. |

The “`no ip igmp query-max-response-time`” command resets the query-max-response-time to its default 100.

Configure query-max-response time only on IGMPv2 interface.

The example below shows the commands to configure IGMP query maximum response time.
Configure IGMP query maximum response time for layer3 VLAN 10

SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# ip igmp query-max-response-time 255
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
**IGMP max query response time is 255 seconds**
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined

17.6.3 Robustness Value
The robustness value can be fine-tuned to allow for expected packet loss on a subnet. The value of this variable affects certain IGMP message intervals for IGMPv2 and IGMPv3 as below:

- **Group membership interval**: Amount of time that must pass before a multicast router determines that there are no more members of a group on a network.
  
  Group membership interval = (Robustness value * query interval) + query response interval

- **Other querier present interval**: The robustness value is used to calculate the amount of time that must pass before a multicast router determines that there is no longer another multicast router that is the querier.
  
  Other querier present interval = (Robustness value * query interval) + (0.5 * query response interval)

- **Last-member query count**: Number of group-specific queries sent before the router assumes there are no local members of a group. The number of queries is equal to the value of the robustness value.

In IGMPv3, devices send a state-change report in case of change of interface state. The number of times state-change report is retransmitted is the robustness value minus one.

The default robustness value is 2. Suggest increasing this value if the subnet is expected to lose packets.

Supermicro switches provide flexibility for user to configure robustness value for individual interfaces. User can configure different robustness value on different interfaces.

Follow the steps below to change robustness value on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> or <code>&lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>
interface range <interface-type> <interface-id> .... 

interface-type – may be any of the following:
  vlan

interface-id is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g interface range vlan 10-20

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: interface range vlan 10,20

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>ip igmp robustness &lt;value&gt;</th>
<th>Configures IGMP robustness value. The robustness value can be any number from 1-255 seconds. Default is 2 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Displays the IGMP robustness information for the given interface.</td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The “no ip igmp robustness” command resets the robustness value to its default 2.

Configure Robustness value only on IGMPv2 and IGMPv3 interfaces.

The example below shows the commands to configure IGMP query maximum response time.

**Configure IGMP robustness value for layer3 VLAN 10**

SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# ip igmp robustness 10
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 10
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined

17.7 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 an interface, it does not delete the interface from the group entry on the multicast table immediately. Instead, the switch sends an IGMP group-specific query message on the interface that received the IGMP leave message. If there is any other IGMP host on that interface that joined the same multicast group, the switch will receive an IGMP member report as a response. If no hosts respond on that interface, the switch will assume no other IGMP hosts are connected on that interface for the same group and will delete the corresponding interface 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.

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 interface that received an IGMP leave message.

These parameters can be configured as explained below.

17.7.1 Last member Query Interval

Switches send a group specific query messages on the interface 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 interface. If they do not receive any response from hosts for a group query interval time, the switches will remove the interface from the group entry in the multicast forwarding table.

Users can configure this last member query interval. The default last member query interval is 10 seconds.

Follow the steps below to configure the last member query interval.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt; &lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

`interface-type` – may be any of the following:
- vlan

`interface-id` is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.:

```
interface range vlan 10-20
```

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.:

```
interface range vlan 10,20
```

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

| Step 3 | `ip igmp last-member-query-interval <value>` | Configures the last member query interval. |

The last member query interval value can be any number from 1-255 seconds. Default is 2 seconds.

| Step 4 | `end` | Exits the configuration mode. |
| Step 5 | `show ip igmp interface <interface-type> <interface-id>` | Displays the IGMP last member query interval information for the given interface(s). |
| Step 6 | `write startup-config` | Optional step – saves this IGMP configuration to be part of the startup configuration. |
The “no ip igmp last-member-query-interval” command resets the last member query interval value to its default value of 10 seconds.

Last member query interval should be configured only on an IGMPv2 or IGMPv3 interface.

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

**Configure the last member query interval time as 250 seconds for layer3 VLAN10.**

```
SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# ip igmp last-member-query-interval 250
SMIS(config-if)#end
```

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 250 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined

**17.7.2 Immediate Leave**

The switch can be configured to immediately remove the interface from the group entry on the multicast table when any interface receives an IGMP leave message without sending out group specific query messages. This function is called immediate leave and it is configurable per interface basis.

Immediate leave is disabled by default in all interfaces.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt; &lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-type</code> – may be any of the following: vlan</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-id</code> is the VLAN identifier for VLAN interfaces.</td>
</tr>
</tbody>
</table>
To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: interface range vlan 10-20

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: interface range vlan 10,20

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>ip igmp immediate leave</th>
<th>Enables the IGMP immediate leave.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Displays the IGMP immediate leave information for the given interface.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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

Immediate leave should be configured only on an IGMPv2 interface.

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

**Enable the immediate leave for Layer3 VLAN 10.**

```
SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# ip igmp immediate-leave
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
```
17.8 Static Multicast Group Membership

IGMP Group membership can be configured statically on an interface. The static IGMP group entries are used to statically forward Multicast data on the particular interface. The entries in the static group membership table exist without any timeout, until they are explicitly deleted.

By default there are no static Multicast memberships.

Follow the steps below to configure static group and source membership.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | `interface <interface-type> <interface-id>` or `interface range <interface-type> <interface-id> ....` | Enters the interface configuration mode.  

  * `interface-type` – may be any of the following:  
 _vlan  
  
  * `interface-id` is the VLAN identifier for VLAN interfaces.  

To configure multiple interfaces, use the “`interface range ...`” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.:  

  * `interface range vlan 10-20`  

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.:  

  * `interface range vlan 10,20`  

If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.

| Step 3 | `ip igmp static-group <Group Address> [source <Source Address>]` | Enables the IGMP static group membership.  

  * **Group:** Mention the IP address of the Multicast group in dotted decimal notation. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>show ip igmp groups</td>
<td>Displays the IGMP group membership information.</td>
</tr>
<tr>
<td></td>
<td>show ip igmp sources</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

Source (optional): Mention the IP address of the Source in dotted decimal notation.

The “no ip igmp static-group <Group Address> [source <Source Address>]” command can be used to remove a statically configured group and source from an interface.

The ‘source’ option should be used only on an IGMPv3 interface.

The example below shows the commands to configure IGMP Static group membership.

**Configure IGMP Static group membership for layer3 VLAN 10**

```
SMIS(config)#configure terminal
SMIS(config)#interface vlan 10
SMIS(config-if)# ip igmp static-group 225.5.5.5
SMIS(config-if)# ip igmp static-group 235.1.1.1
SMIS(config-if)# end

SMIS# show ip igmp groups

<table>
<thead>
<tr>
<th>GroupAddress</th>
<th>Flg</th>
<th>Iface</th>
<th>UpTime</th>
<th>ExpiryTime</th>
<th>LastReporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.5.5.5</td>
<td>S</td>
<td>vlan10</td>
<td>[0d 00:00:06.17]</td>
<td>[0d 00:00:00.00]</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>235.1.1.1</td>
<td>S</td>
<td>vlan10</td>
<td>[0d 01:20:01.36]</td>
<td>[0d 00:00:00.00]</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

SMIS# show ip igmp interface

vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
### 17.9 Disabling IGMP

IGMP is disabled by default in Supermicro switches.

After enabling IGMP, if user needs to disable it, it has to be disabled globally and also in interfaces individually.

Follow the steps below to disable IGMP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip igmp disable</td>
<td>Disables IGMP globally.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface <code>&lt;interface-type&gt;</code> <code>&lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt;</code> <code>&lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-type</code> – may be any of the following: vlan</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-id</code> is the VLAN identifier for VLAN interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “<code>interface range</code> ...” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: <code>interface range vlan 10-20</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: <code>interface range vlan 10,20</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will enable IGMP on all these interfaces.</td>
</tr>
<tr>
<td>Step 4</td>
<td>set ip igmp disable</td>
<td>Disables IGMP in VLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp global-config</td>
<td>Displays the IGMP information.</td>
</tr>
<tr>
<td></td>
<td><code>show ip igmp interface</code> <code>&lt;interface-type&gt;</code> <code>&lt;interface-id&gt;</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this IGMP configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to disable IGMP.

**Disable the IGMP function assuming the switch has layer3 VLAN 10**

```
SMIS(config)# configure terminal
SMIS(config)# set ip igmp disable
SMIS(config)# end

SMIS# show ip igmp global-config
IGMP is globally disabled

SMIS(config)# configure terminal
SMIS(config)# interface vlan 10
SMIS(config-if)# set ip igmp disable
SMIS(config-if)# end

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 2.2.2.2/8
IGMP is disabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 10 0 seconds
Robustness value is 2
IGMP querying router is 2.2.2.2 (this system)
Fast leave is disabled on this interface
No multicast groups joined
```
17.10 IGMP Configuration example

Configure the following requirements as shown below in Figure IGMP-3.

**Switch A:**

5. Enable IGMP.
6. Configure static Multicast group and source on VLAN10.
7. Configure immediate leave and query interval
8. Verify the IGMP group table

**Switch B:**

1. Enable IGMP.
2. Verify the IGMP group table
3. Configure robustness value

**Figure IGMP-3: IGMP Configuration example**

When an MRP like PIM is enabled on interfaces between Switch A and Switch B, traffic flows from Source 200.1.1.1 to receivers for Group 225.1.1.1.
IGMP Configuration on Switch A

#Create Layer3 VLAN interface
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/1 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.10 255.0.0.0
SMIS(config-if)# exit

SMIS(config)# vlan 20
SMIS(config-vlan)# ports fx 0/24 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface vlan 20
SMIS(config-if)# ip address 20.20.20.1 255.0.0.0
SMIS(config-if)# exit

#Enable IGMP on interface
SMIS(config)# interface vlan 1
SMIS(config-if)# set ip igmp enable
SMIS(config-if)# ip igmp version 3
SMIS(config-if)# ip igmp immediate leave
SMIS(config-if)# ip igmp query-interval 60
SMIS(config-if)# ip igmp static-group 225.1.1.1 source 200.1.1.1
SMIS(config-if)# exit

SMIS(config)# interface vlan 20
SMIS(config-if)# set ip igmp enable
SMIS(config-if)# exit

#Enable IGMP globally
SMIS(config)# set ip igmp enable

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

Building configuration...
Switch ID Hardware Version Firmware Version
ip address dhcp
vlan 1
  ports fx 0/2-23 untagged
  ports fx 0/25-48 untagged
  ports fx 0/1-4 untagged
exit
vlan 10
  ports fx 0/1 untagged
exit
vlan 20
  ports fx 0/24 untagged
exit
interface vlan 1
ip address dhcp

interface vlan 10
ip address 10.10.10.10 255.0.0.0
set ip igmp enable
ip igmp immediate-leave
ip igmp version 3
ip igmp query-interval 60
ip igmp static-group 225.1.1.1 source 200.1.1.1

interface vlan 20
ip address 20.20.20.1 255.0.0.0
set ip igmp enable
exit
set ip igmp enable

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

#Display IGMP Global Configuration
SMIS(config)# show ip igmp global-config
IGMP is globally enabled

#Display IGMP interface information
SMIS(config)# show ip igmp interface
vlan10, line protocol is up
  Internet Address is 10.10.10.10/8
  IGMP is enabled on interface
  Current IGMP router version is 3
  IGMP query interval is 60 seconds
  Last member query response interval is 10 seconds
  IGMP max query response time is 100 seconds
  Robustness value is 2
  IGMP querying router is 10.10.10.10 (this system)
  Fast leave is enabled on this interface
  Number of multicast groups joined 1

vlan20, line protocol is up
  Internet Address is 20.20.20.1/8
  IGMP is enabled on interface
  Current IGMP router version is 2
  IGMP query interval is 125 seconds
  Last member query response interval is 10 seconds
  IGMP max query response time is 100 seconds
  Robustness value is 2
IGMP querying router is 20.20.20.1 (this system)
Fast leave is disabled on this interface
No multicast groups joined

#Display IGMP Group information
SMIS(config)# show ip igmp groups

I - Include Mode, E - Exclude Mode
S - Static Mbr, D - Dynamic Mbr

GroupAddress Flg Iface UpTime ExpireTime LastReporter
225.1.1.1 IS vlan10 [0d 00:35:06.25] [0d 00:00:00.00] 10.10.10.10

#Display IGMP Source information
SMIS(config)# show ip igmp sources

I - Include Mode, E - Exclude Mode
S - Static Mbr, D - Dynamic Mbr
F - Forward List, N - Non-Forward List

GroupAddress Iface SrcAddress Flg ExpireTime LastReporter
225.1.1.1 vlan10 200.1.1.1 ISF [0d 00:00:00.00] 10.10.10.10

IGMP Configuration on Switch B

#Create Layer3 VLAN interface
SMIS(config)# vlan 20
SMIS(config-vlan)# ports fx 0/24 untagged
SMIS(config-vlan)# exit

SMIS(config)# interface vlan 20
SMIS(config-if)# ip address 20.20.20.5

#Enable IGMP on Layer3 VLAN interface
SMIS(config-if)# set ip igmp enable
SMIS(config-if)# ip igmp robustness 5
SMIS(config-if)# exit

#Enable IGMP globally
SMIS(config)# set ip igmp enable

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

Building configuration...
Switch ID Hardware Version Firmware Version

ip address dhcp
vlan 1
ports fx 0/1-23 untagged
ports fx 0/1-3 untagged
exit
vlan 20
ports fx 0/24 untagged
exit

interface vlan 20
ip address 20.20.20.5 255.0.0.0
set ip igmp enable
ip igmp robustness 5

exit
set ip igmp enable

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

# Display IGMP Global Configuration
SMIS(config)# show ip igmp global-config
IGMP is globally enabled

# Display IGMP interface information
SMIS(config)# show ip igmp interface
vlan20, line protocol is up
Internet Address is 20.20.20.5/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 (1/10 seconds)
IGMP max query response time is 100 (1/10 seconds)
Robustness value is 5
IGMP querying router is 20.20.20.1
Fast leave is disabled on this interface
No multicast groups joined

18 IP Unicast Routing Overview

Layer 3 switches can route packets in three different ways:

- Default routing: Traffic with an unknown destination is sent to a default destination, usually specified by a default route configuration.
• Static routes: Static unicast routing forwards packets from predetermined ports through a single path into and out of a network. Static routing is secure and uses little bandwidth, but does not automatically respond to changes in the network, such as link failures, and hence may result in unreachable destinations. As networks grow, static routing configuration becomes labor-intensive.

• Dynamically Routing protocol: Dynamic routing protocols are used by routers to dynamically calculate the best route for forwarding traffic. There are two types of dynamic routing protocols:

  • Distance-vector protocols create/maintain routing tables with distance values of network resources, and periodically update these tables to the neighbor routers. Distance-vector protocols use one or a series of metrics for calculating the best routes. These protocols are easy to configure and use. Distance-vector protocols supported by Supermicro switches are Routing Information Protocol (RIP), which uses a single distance metric (cost) to determine the best path and Border Gateway Protocol (BGP), which adds a path vector mechanism.

  • Link-state protocols create/maintain a complex database of network topology, based on the exchange of link-state advertisements (LSAs) between routers. LSAs are triggered by an event in the network, which speeds up the convergence time due to topology changes. Link-state protocols require greater bandwidth and more resources than distance-vector protocols. Supermicro switches support Open Shortest Path First (OSPF) link-state protocol.

Routing in the Internet is divided into two parts – fine-grained topological detail of connected segments of the Internet is managed with interior routing protocols (such as RIP or OSPF), while the interconnection of these segments, or “autonomous systems” is managed by an inter-domain routing protocol (such as Border Gateway Protocol, or BGP).

Administrative distance is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 indicates the routing information should be ignored.

Redistribution is a process of passing the routing information from one routing domain to another. The purpose of redistribution is to provide full IP connectivity between different routing domains and to provide redundant connectivity, i.e. backup paths between routing domains. Routing domain is a set of routers running the same routing protocol. Redistribution process is performed by border routers – i.e. routers belonging to more than one routing domain. Supermicro switches allow redistribution of routes from/to RIP to/from other Unicast Routing Protocols, like OSPF. Differences in routing protocol characteristics, such as metrics, administrative distance, classful and classless capabilities can effect redistribution.

18.1 RIP
Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count (the number of routers) to determine the best way to a remote network. RIP sends the complete routing table out to all active interfaces every 30 seconds.
Supermicro switches support both RIPv1 and RIPv2. RIPv1 is a classful routing protocol that does not include the subnet mask with the network address in routing updates, which causes problems in discontiguous subnets or networks that use Variable-Length Subnet Masking (VLSM). RIPv2 is a classless routing protocol so subnet masks are included in the routing updates, making RIPv2 more compatible with modern routing environments.

RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs. RIP is considered an effective solution for small homogeneous networks. RIP is not suited for larger, more complicated networks since the transmission of the entire routing table every 30 seconds increases network traffic.

18.1.1 Network
Supermicro switches provide user configuration of the network IP address that run RIP. The network number specified must not contain any subnet information. RIP routing updates are sent and received only through interfaces on this network.

18.1.2 Neighbor
By default RIPv2 will send multicast updates out all interfaces specified within the range of the network command. Supermicro switches allow neighbor configuration that enables the switch to send unicast updates to that neighbor out the respected link. Multicast updates are also sent through the same link.

18.1.3 Metric
RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. RIP routing is limited to 15 hops. A metric of 16 hops identifies unreachable network.

18.1.4 Route tag
Route tags are supported in RIP version 2. This functionality allows for routes to be distinguished from internal routes to external redistributed routes from EGP protocols.

18.1.5 Split Horizon
Routers connected to broadcast-type IP networks use the split-horizon mechanism to reduce routing loops, especially when links are broken. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated.

Supermicro switches support the following two mechanisms that help ensure the reachability of routes:

- Split horizon -- This mechanism omits routes learned from one neighbor in updates sent to that neighbor. Split horizon minimizes routing overhead, but may cause slower convergence.
• Split horizon with poison reverse -- This mechanism includes routes learned from one neighbor in updates sent to that neighbor. However, it sets the metric to 16, which avoids loop. Poison reverse speeds up convergence, but it increases routing overhead.

18.1.6 Summarization
In large internetworks, hundreds, or even thousands, of network addresses can exist. It is often problematic for routers to maintain this volume of routes in their routing tables. Route summarization also called route aggregation or supernetting helps reduce the number of routes that a router must maintain as a series of network numbers are represented by a single summary address.

Route summarization is most effective within a subnetted environment when the network addresses are in contiguous blocks in powers of 2. Summarization results in less CPU, memory, and bandwidth usage.

Routing protocols summarize or aggregate routes based on shared network numbers within the network. RIPv2 supports route summarization based on subnet addresses, including VLSM addressing. RIPv1 automatically summarize routes on the classful network boundary only.

If more than one entry in the route summary matches a particular destination, the longest prefix match in the routing table is used.

NOTE: If split horizon is enabled, neither autosummary nor interface IP summary addresses is advertised.

18.1.7 Authentication
RIP Version 1 does not support authentication. RIP Version 2 packets supports RIP authentication on an interface. The key chain and the set of keys that can be used on the interface should be specified for authentication.

18.1.8 Security
RIP supports the following two security mechanisms that prevent unauthorized routers from forming adjacencies:

• Simple text password: This method transmits simple passwords in clear text.
• MD5 authentication (For RIPv2 only): This mechanism provides more protection than a simple password and has a greater probability of detecting hostile messages.
18.1.9 Passive Interface

Passive interfaces are used to suppress routing updates. These interfaces can be used to allow an interface to receive updates but prevent the interface from sending advertisements.

18.1.10 Inter-packet delay

By default, RIP implementation in Supermicro switches does not add delay between packets during a multiple-packet RIP update transmission. If a high-end router is sending packets to a low-speed router, inter-packet delay of RIP updates must be configured, in the range of 8 to 50 milliseconds.

18.1.11 Re-transmission

Supermicro switches support retransmission of Update Request packet or unacknowledged Update response packet. User can specify the timeout interval and the maximum number of retransmissions of the update request and update response packets. During retries, if no response is received then the routes through the next hop router are marked unreachable.

18.1.12 Timers

RIP uses the following timers to maintain routing tables:

Update timer: Routers within an autonomous system exchange routing information through periodic RIP updates. The update timer controls the frequency of these updates.

Expiration timer: RIP expects an update every 30 seconds from its neighbors. If it does not receive an update in that time, RIP waits for a specified expiration time before declaring a route invalid.

Triggered update timer: When routes change, Supermicro switch sends a RIP update almost immediately instead of waiting for its regular update message. This helps to speed up network convergence. The triggered update timer is set to wait for 5 seconds to avoid a storm of triggered updates.

18.1.13 Default route

RIP has a built in feature in which allows it to advertise a default route to its direct neighbors which will propagate throughout the entire RIP routing domain. The default route can be configured by the user. Utilizing this type of configuration reduces the effort required to configure a static default route on each and every router and/or switch in the network.

18.1.14 RIP Configuration

18.1.14.1 Default RIP Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>UDP Port</td>
<td>521</td>
</tr>
<tr>
<td>Update Interval</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Space Interval</td>
<td>2</td>
</tr>
<tr>
<td>Route Age/Expiry</td>
<td>180 seconds</td>
</tr>
<tr>
<td>Maximum paths</td>
<td>16</td>
</tr>
<tr>
<td>Garbage collection Interval</td>
<td>120 seconds</td>
</tr>
</tbody>
</table>
### 18.1.14.2 Enabling RIP

RIP is disabled by default in Supermicro switches. Follow the below steps to enable RIP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router rip</td>
<td>Enables RIP on all interfaces and enters the Router configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exit from Configuration mode.</td>
</tr>
</tbody>
</table>

The “no router rip” command disables RIP in the switch.

### 18.1.14.3 RIP Neighbor

Supermicro switches allow configuration of RIP Neighbor. Follow the below steps to configure a RIP neighbor.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router rip</td>
<td>Enables RIP on all interfaces and enters the Router configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor &lt;ip address&gt;</td>
<td>Add a neighbor router</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exit from Configuration mode.</td>
</tr>
</tbody>
</table>

The “no neighbor <ip address>” command deletes the RIP neighbor.
18.1.14.4 **Interface Parameters**
Supermicro switches provide configuration of Interface parameters for RIP. Follow the below steps to configure a RIP interface parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router rip</code></td>
<td>Enables RIP on all interfaces and enters the Router configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>neighbor &lt;ip address&gt;</code></td>
<td>Add a neighbor router</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>Exit</code></td>
<td>Exit from RIP router configuration mode</td>
</tr>
</tbody>
</table>
| Step 5| `interface <interface-type><interface-id>` or `interface range <interface-type><interface-id> ....` | (Optional) Enters the interface configuration mode.  
  
  **interface-type** – may be any of the following: 
  vlan 
  
  **interface-id** is in *slot/port* format for all physical interfaces. It may be the VLAN identifier for VLAN interfaces. 
  
  To configure multiple interfaces, use the "interface range ..." command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: `int range vlan 1-10` 
  
  To provide multiple interfaces or ranges, separate with a comma (,). E.g.: `int range vlan 1-10,20` 
  
  If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces. |
| Step 6| `ip rip send version { 1 | 2 | 1 2 | none }` | (Optional) Configure IP RIP version number for transmitting advertisements |
| Step 7| `ip rip receive version { 1 | 2 | 1 2 | none }` | (Optional) Configure IP RIP version number for receiving advertisements |
| Step 8| `ip rip authentication mode { text | md5 } key-chain <key-chain-name (16)>` | (Optional) Configures authentication mode and key |
| Step 9| `timers basic <update-value (10-3600)> <routeage-value (30-500)> <garbage-value (120-180)>` | (Optional) Configure update, route age and garbage collection timers |
| Step 10| `ip split-horizon [poison]` | (Optional) Configure the split horizon status |
| Step 11| `ip rip default route originate <metric(1-15)>` | (Optional) Configure the metric to be used for default route propagated over the interface |
### Step 12
**ip rip summary-address <ip-address> <mask>**
(Optional) Configure route aggregation for all subnet routes that falls under the specified ip address and mask.

### Step 13
**ip rip default route install**
(Optional) Install default route received in updates to the rip database.

### Step 14
**end**
Exit from Configuration mode.

### Step 15
**show ip rip { database [ <ip-address> <ip-mask> ] | statistics }**
Display IP RIP protocol database or statistics.

---

These commands either delete the particular configuration or reset it to its default value.

- `no ip rip send version`
- `no ip rip receive version`
- `no ip rip authentication`
- `no timers basic`
- `no ip split-horizon`
- `no ip rip default route originate`
- `no ip rip summary-address <ip-address> <mask>`
- `no ip rip default route install`

---

### 18.1.14.5 Additional Parameters
Supermicro switches provide configuration of certain additional RIP parameters. Follow the below steps to configure additional RIP parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router rip</code></td>
<td>Enables RIP on all interfaces and enters the Router configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>neighbor &lt;ip address&gt;</code></td>
<td>Add a neighbor router</td>
</tr>
<tr>
<td>Step 4</td>
<td>`network &lt;ip-address&gt;[unnum {vlan &lt;integer(1-4069)&gt;</td>
<td>&lt;iftype&gt; &lt;ifnum&gt;}]`</td>
</tr>
<tr>
<td>Step 5</td>
<td>`ip rip retransmission { interval &lt;timeout-value (5-10)&gt;</td>
<td>retries &lt;value (10-40)&gt; }`</td>
</tr>
</tbody>
</table>

**interval** - The timeout interval to be used to retransmit the update request packet or an unacknowledged update response packet.

**retries** - The maximum number of retransmissions of the update request and update response packets.
| Step 6 | redistribute { all | bgp | connected | ospf | static } [route-map <name(1-20)>] | (Optional) Enables redistribution of corresponding protocol routes into RIP.  
  
  *all* - Advertises all routes learned in the RIP process.  
  
  *connected* - Connected routes redistribution.  
  
  *ospf* - Advertises routes learned by OSPF in the RIP process.  
  
  *static* - Statically configured routes to advertise in the RIP process.  
  
  *route-map* - Name of the Route Map to be applied during redistribution of routes from Route Table Manager to RIP. If this is not specified, all routes are redistributed. |
|---|---|---|
| Step 7 | default-metric <value> | (Optional) Configure the metric to be used for redistributed routes.  
  
  The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.  
  
  NOTE: This command can be configured only if RIP redistribution is enabled in Interface mode. |
| Step 8 | route-tag <1-65535> | (Optional) Configure the route tag to be used for redistributed routes. |
| Step 9 | auto-summary {enable | disable} | (Optional) Enable/Disable auto summarization feature in RIP |
| Step 10 | ip rip security { minimum | maximum } | (Optional) Accept/ignore RIP1 packets when authentication is in use  
  
  *minimum* - Denotes that the RIP1 packets will be accepted even when authentication is in use  
  
  *maximum* - Denotes that the RIP1 packets will be ignored when authentication is in use. |
| Step 11 | passive-interface {vlan <vlan-id(1-4069)> | <interface-type> <interface-id>} | (Optional) Suppress routing updates on an interface |
| Step 12 | output-delay | (Optional) Enable inter-packet delay for RIP updates |
### Step 13
end

Exit from Configuration mode.

### Step 14

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip rip { database [ &lt;ip-address&gt; &lt;ip-mask&gt; ]</td>
<td>statistics }</td>
</tr>
</tbody>
</table>

These commands either delete the particular configuration or reset it to its default value.

- no network <ip-address> [unnum {vlan <integer(1-4069)> | <iftype> <ifnum>}]  
- no ip rip security  
- no ip rip retransmission { interval | retries }  
- no passive-interface (vlan <vlan-id(1-4069)> | <interface-type> <interface-id>)  
- no output-delay  
- no redistribute { all | bgp | connected | ospf | static } [route-map <name(1-20)>]  
- no default-metric  
- no route-tag

#### 18.1.14.6 RIP Configuration Example

The example below shows the commands used to configure RIP by using 2 switches: Switch A and switch B.

![Switch A and Switch B](image)

**Figure IP-Unicast-Routing-1: RIP Configuration Example**

**On switch A**

SMIS# configure terminal  
SMIS(config)# vlan 200  
SMIS(config-vlan)# exit  
SMIS(config)# interface fx 0/22  
SMIS(config-if)# switchport mode access  
SMIS(config-if)# switchport access vlan 200  
SMIS(config)# interface vlan 200  
SMIS(config-if)# ip address 10.10.10.2  
SMIS(config-if)# exit  
SMIS(config)# router rip  
SMIS(config-router)# network 10.10.10.2  
SMIS(config-router)# neighbor 10.10.10.1  
SMIS(config-router)# end
SMIS# show ip rip database
10.0.0.0/8  [1] auto-summary
10.0.0.0/8  [1] directly connected, vlan200

SMIS# show ip rip statistics

RIP Global Statistics:
------------------------
Total number of route changes is 0
Total number of queries responded is 0
Total number of dropped packets is 0

RIP Interface Statistics:
-------------------------
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Periodic Updates Sent</th>
<th>BadRoutes Received</th>
<th>Triggered Updates Sent</th>
<th>BadPackets Received</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.2</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

SMIS# show running-config

Building configuration...
Switch ID    Hardware Version    Firmware Version

vlan 1
ports fx 0/1-20 untagged
ports fx 0/22-48 untagged
ports cx 0/1-6 untagged
exit
vlan 200
exit

interface Fx 0/22
  switchport mode access
  switchport access vlan 200
exit

interface vlan 200
  ip address 10.10.10.2 255.0.0.0
exit
router rip
  neighbor 10.10.10.1
  network 10.10.10.2
exit

On switch B
SMIS# configure terminal
SMIS(config)# vlan 200
SMIS(config-vlan)# exit
SMIS(config)# interface fx 0/22
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 200
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address 10.10.10.1
SMIS(config-if)# exit
SMIS(config)# router rip
SMIS(config-router)# network 10.10.10.1
SMIS(config-router)# neighbor 10.10.10.2
SMIS(config-router)# end

SMIS# show ip rip database
10.0.0.0/8 [1] auto-summary
10.0.0.0/8 [1] directly connected, vlan200

SMIS# show ip rip statistics
RIP Global Statistics:
-----------------------
Total number of route changes is 0
Total number of queries responded is 1
Total number of dropped packets is 0

RIP Interface Statistics:
-------------------------
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Periodic Updates Sent</th>
<th>BadRoutes Received</th>
<th>Triggered Updates Sent</th>
<th>BadPackets Received</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

SMIS# show running-config

Building configuration...
Switch ID Hardware Version Firmware Version

vlan 1
  ports fx 0/1-20 untagged
  ports fx 0/22-48 untagged
  ports cx 0/1-6 untagged
exit
vlan 200
exit

interface Fx 0/22
  switchport mode access
  switchport access vlan 200
exit
interface vlan 200
ip address 10.10.10.1 255.0.0.0

exit
router rip
neighbor 10.10.10.2
network 10.10.10.1
exit
interface vlan 200
exit

18.2 OSPF

OSPF is an Interior Gateway routing protocol that can scale well in large environments. OSPF supports the following features:

- Variable Length Subnet masks (VLSM)
- The use of areas to minimize Central Processing Unit (CPU) and memory requirements.
- A simple cost metric that can be manipulated to support up to six equal cost paths.
- The use of authentication to ensure OSPF updates are secure and the use of multicast updates to conserve bandwidth.
- Faster convergence times ensuring updates and changes are propagated across the network.
- No limitation of network diameter or hop count. Limiting factors include only CPU and memory resources.
- The ability to tag OSPF information injected from any autonomous systems.

OSPF enabled switch multicasts Link State Advertisements (LSAs) to inform all other routers in the area of its neighbors and costs. Based on OSPF LSAs, each router constructs a topology table which contains every connection link within the network. Then, the Dijkstra algorithm runs over the topology table to find the shortest path to every other router, and hence creates the routing table. This algorithm, which is also known as the SPF algorithm, runs on every OSPF enabled router on the network, and routers within a particular area all have the same topology tree of the specific area.

18.2.1 Neighbor & DR

OSPF routers exchange hellos with neighboring routers and in the process learn their neighbor’s Router ID (RID) and cost, these values are stored to the adjacency table.

Supermicro switch establishes OSPF adjacencies between all neighbors on a multi-access network (such as Ethernet). This ensures all routers do not need to maintain full adjacencies with each other.

The Designated Router (DR) is selected based on the router priority. In a tie, the router with the highest router ID is selected. Backup DR is a router designed to perform the same functions in case the DR fails.
18.2.2 LSA
Once a router has exchanged hellos with its neighbors and captured Router IDs and cost information, it begins sending LSAs, or Link State Advertisements. Link state is the information shared between directly connected routers. This information propagates throughout the network unchanged and is also used to create a shortest path first (SPF) tree.

The OSPF standard defines a number of LSAs types. Unlike distance vector protocols (for example, RIP), OSPF does not actually send its routing table to other routers. Instead, OSPF sends the LSA database and derives the IP routing table from LSAs.

In order to avoid LSA storm, each LSA has a sequence number which is incremented only if LSA has changed. Each LSA also has an age value that is set to zero by the originating switch and increased by every switch during flooding.

The common types of LSA are

Type 1 – Router LSA, containing router ID and link information

Type 2 – Network LSA contains DR and broadcast segment details

Type 3 – Network Summary LSA originated by ABR only and contains metric and subnet information

Type 4 – ASBR Summary LSA originated by ABR only and advertised to ASBR contains router ID, mask and metric

Type 5 – AS external LSA originated by ASBR contains external route and default route information

18.2.3 Area
An OSPF area is defined as a logical grouping of routers by a network administrator. OSPF routers in any area contain same topological view, also known as the OSPF database of the network. OSPF is configured in multiple areas in order to reduce routing table sizes, which in turn reduces the topological database and switch CPU/memory requirements.

OSPF is not just configured in one large area, so all routers share the same topological database. The use of multiple areas ensures that the flooding and database management required in large OSPF networks is reduced within each area so that the process of flooding the full database and maintaining full network connectivity does not consume a large portion of the CPU processing power and network bandwidth. Every time a network change occurs, the CPU on a router is interrupted and a new OSPF tree is calculated. Running
the shortest path first (SPF) algorithm itself is not CPU intensive, but sending and flooding the network with new topological information is extremely CPU intensive.

Areas are identified through a 32-bit Area ID expressed in dotted decimal notation. All OSPF areas must be connected to the backbone in case of network failure. When an area cannot reside physically or logically on the backbone, a virtual link is required. There are four types of Areas used in OSPF:

- **Backbone Area**: Alternate Name for Area 0. This includes all ABRs and internal routers of the backbone area. The backbone is a hub for inter-area transit traffic and the distribution of routing information between areas. Inter-area traffic is routed to the backbone, then routed to the destination area, and finally routed to the destination host within the destination area. Routers on the backbone also advertise the summarized routes within their areas to the other routers on the backbone. Backbone area helps avoid routing loops as it is the trunk of the network.

- **Regular Area**: Non-backbone area, with both internal and external routes

- **Stub area**: An area that contains a single exit point from the area. Areas that reside on the edge of the network with no exit point except one path can be termed a stub area.

- **Not-So-Stubby-Area (NSSA)**: This area is used to connect to an ISP. All advertised routes can be flooded through the NSSA but are blocked by the ABR.
18.2.4 OSPF Router Types

There are different types of OSPF Routers classified based on functionality.

- **Internal Router**: This router is within a specific area only. Internal router functions include maintaining the OSPF database and forwarding data to other networks. All interfaces on internal routers are in the same area.

- **Backbone Router**: Backbone routers are connected to area 0, which is also represented as area 0.0.0.0. A backbone router can perform ASBR functions as well as ABR functions.

- **Area Border Router (ABR)**: ABRs are responsible for connecting two or more areas. An ABR contains the full topological database for each area it is connected to and sends this information to other areas. ABRs contain a separate Link State Database, separating LSA flooding between areas, optionally summarizing routes, and optionally sourcing default routes.

- **Autonomous System Boundary Router (ASBR)**: Router that has at least one interface in an OSPF area and at least one interface outside of an OSPF area. Routers that connect to, for example, the Internet and redistribute external IP routing tables from such protocols as Border Gateway Protocol (BGP) are termed autonomous system boundary routers (ASBRs).

18.2.5 Types of routes

OSPF supports two types of routes: Internal routers and External OSPF. External routes are routing entries in OSPF route tables injected by an external routing protocol, such as BGP. When calculating the cost to a remote network, internal routes add the total cost to destination; whereas External routes include only the cost to the external network.

18.2.6 Default route

When redistribution of routes into an OSPF routing domain is configured, the route becomes an autonomous system boundary router (ASBR). The ASBR can generate a default route into the OSPF routing domain by user configuration.
18.2.7 Metric
The OSPF process assigns cost values to interfaces based on the inverse of the bandwidth parameter assigned to the interface with the bandwidth command. For calculating the SPF to a given destination, the router takes into consideration the costs of the links along various paths. The path with the lower cost is selected as the shortest path. The SPF algorithm only runs within a single area, so routers only compute paths within their own area. Inter-area routes are passed using border routers.

18.2.8 Router Id
The source of Link-state Advertisements in a given area is identified by the Router ID. This ID has the form of an IP address and can be automatically or manually defined.

18.2.9 Priority
In multi-access networks the router with the highest priority value is chosen as the DR which acts as the central point of LSAs exchange. Supermicro switches provide OSPF DR priority configuration.

18.2.10 Route Summarization
Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. Summarization occurs using the LSA type 4 packet or by the ASBR. OSPF can be configured in two ways to summarize networks:

- Inter-area summarization creating type 3 or 4 LSAs
- External summarization with type 5 LSAs

18.2.11 Authentication
OSPF does not authenticate its protocol's messages or route updates. OSPF does, however, support two message authentication options:

- Simple Authentication- using plaintext keys
- MD5 Authentication - Matching authentication methods and keys must be configured on each interface on a segment. Theoretically, different passwords could be applied to different router interfaces – the routers on the other ends of those links would just be required to have matching information.

18.2.12 Timers
Supermicro switches provide configuration of the delay time between when OSPF receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.
18.2.13 Virtual Link
In OSPF, all areas must be connected to a backbone area. A virtual link can be configured in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the non-backbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.

18.2.14 Passive Interface
The passive-interface interface command disables OSPF hellos from being sent out, thus disabling the interface from forming adjacencies out that interface.

18.2.15 Demand Circuit
A demand circuit is a point-to-point connection between two neighboring interfaces configured for OSPF. Demand circuits increase the efficiency of OSPF on the configured interfaces by stopping the periodic transmission of OSPF packets, like Hello and LSA. OSPF can establish a demand link to form an adjacency and perform initial database synchronization; the adjacency remains active even after Layer 2 of the demand circuit goes down.

18.2.16 Network Type
Internet network types are dependent on the layer 2 technology used such as Ethernet, point-to-point T1 circuit, and frame relay. The various OSPF network types and their compatibility with one another are specified below.

**Non-Broadcast:** This is the default for OSPF enabled frame relay physical interfaces. Non-Broadcast networks require static neighbor configuration and OSPF hellos are sent via unicast. The Non-Broadcast network type has a 30 second hello and 120 second dead timer. An OSPF Non-Broadcast network type requires the use of a DR/BDR.

**Broadcast:** This is the default for an OSPF enabled ethernet interface. The Broadcast network type requires link support Layer 2 Broadcast capabilities. The Broadcast network type has a 10 second hello and 40 second dead timer. An OSPF Broadcast network type requires the use of a DR/BDR.

**Point-to-Point:** A Point-to-Point OSPF network type does not maintain a DR/BDR relationship. The Point-to-Point network type has a 10 second hello and 40 second dead timer. Point-to-Point network types are intended to be used between 2 directly connected routers.

**Point-to-Multipoint:** This is viewed as a collection of point-to-point links. Point-to-Multipoint networks do not maintain a DR/BDR and advertise a hot route for all the frame-relay endpoints. The Point-to-Multipoint network type has a 30 second hello and 120 second dead timer.
18.2.17 OSPF Configuration

18.2.17.1 OSPF Default Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Router Id</td>
<td>None</td>
</tr>
<tr>
<td>Area</td>
<td>None</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Router Dead Interval</td>
<td>40 seconds</td>
</tr>
<tr>
<td>Trans Delay</td>
<td>1</td>
</tr>
<tr>
<td>Router priority</td>
<td>1</td>
</tr>
<tr>
<td>Retransmission Interval</td>
<td>5</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>120</td>
</tr>
<tr>
<td>Passive Interface Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secondary IP</td>
<td>Disabled</td>
</tr>
<tr>
<td>ASBR Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>NSSA ASBR Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>RPF 1583 Compatibility</td>
<td>Enabled</td>
</tr>
<tr>
<td>LSA Interval</td>
<td>5</td>
</tr>
<tr>
<td>SPF Hold time</td>
<td>10 milliseconds</td>
</tr>
<tr>
<td>SPF Interval</td>
<td>1 milliseconds</td>
</tr>
<tr>
<td>ABR</td>
<td>Standard ABR</td>
</tr>
</tbody>
</table>

18.2.17.2 Enabling OSPF

OSPF is disabled by default in Supermicro switches. Follow the steps below to enable OSPF and configure an OSPF router ID.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf</td>
<td>Enable OSPF routing process</td>
</tr>
<tr>
<td>Step 3</td>
<td>router-id &lt;router ip address&gt;</td>
<td>Configure the Router ID</td>
</tr>
<tr>
<td>Step 4</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip ospf info</td>
<td>Display general information about OSPF routing process.</td>
</tr>
</tbody>
</table>

The “no router ospf” command disables OSPF in the switch.
### 18.2.17.3 OSPF Neighbor

Supermicro switches provide option to configure OSPF neighbors. Follow the steps below to configure OSPF neighbor.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router ospf</code></td>
<td>Enable OSPF routing process</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>router-id &lt;router ip address&gt;</code></td>
<td>Configure the Router ID</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>neighbor &lt;neighbor-id&gt; [priority &lt;priority value (0-255)&gt;]</code></td>
<td>Specify a neighbor router and its priority</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>End</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>`show ip ospf neighbor [ { vlan &lt;vlan (1-4069)&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt; } [Neighbor ID] [detail]`</td>
</tr>
</tbody>
</table>

The “no neighbor <neighbor-id> [priority]” command deletes the OSPF neighbor.

### 18.2.17.4 Area Parameters

Supermicro switches provide configuration options for OSPF area. Follow the steps below to configure OSPF area and its parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router ospf</code></td>
<td>Enable OSPF routing process</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>router-id &lt;router ip address&gt;</code></td>
<td>Configure the Router ID</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>neighbor &lt;neighbor-id&gt; [priority &lt;priority value (0-255)&gt;]</code></td>
<td>Specify a neighbor router and its priority</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>network &lt;Network number&gt; area &lt;area-id&gt; [unnum Vlan &lt;PortNumber&gt;]</code></td>
<td>(Optional) Define the interfaces on which OSPF runs and to define the area ID for those interfaces</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>area &lt;area-id&gt; stability-interval &lt;Interval-Value (0-0x7fffffff)&gt;</code></td>
<td>(Optional) Configure the Stability interval for NSSA area</td>
</tr>
<tr>
<td>Step 7</td>
<td>`area &lt;area-id&gt; translation-role { always</td>
<td>candidate }`</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>no area &lt;area-id&gt; translation-role</code></td>
<td>(Optional) Configure the default translation role for the NSSA area</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>compatible rfc1583</code></td>
<td>(Optional) Configure OSPF compatibility list compatible with RFC 1583</td>
</tr>
<tr>
<td>Step 10</td>
<td>`abr-type { standard</td>
<td>cisco</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>area &lt;area-id&gt; nssa [[ { no-summary [ default-information-originate ] } [metric &lt;value&gt;] [metric-type &lt;Type(1-3)&gt;] [tos &lt;tos value (0-30)&gt;] ]]</code></td>
<td>(Optional) Configure an area as a NSSA area and other parameters related to that area</td>
</tr>
<tr>
<td>Step 12</td>
<td>area &lt;area-id&gt; stub [no-summary]</td>
<td>(Optional) Specify an area as a stub area</td>
</tr>
<tr>
<td>Step 13</td>
<td>default-information originate always [metric &lt;metric-value (0-0xffffffff)&gt;] [metric-type &lt;type (1-2)&gt;]</td>
<td>(Optional) Enable generation of a default external route into an OSPF routing domain</td>
</tr>
<tr>
<td>Step 14</td>
<td>area &lt;area-id&gt; virtual-link &lt;router-id&gt; [authentication { simple</td>
<td>message-digest</td>
</tr>
<tr>
<td>Step 15</td>
<td>ASBR Router</td>
<td>(Optional) Specify this router as ASBR</td>
</tr>
<tr>
<td>Step 16</td>
<td>area &lt;AreaId&gt; range &lt;Network&gt; &lt;Mask&gt; [summary</td>
<td>Type7] [[advertise</td>
</tr>
<tr>
<td>Step 17</td>
<td>summary-address &lt;Network&gt; &lt;Mask&gt; &lt;AreaId&gt; [[allowAll</td>
<td>denyAll</td>
</tr>
<tr>
<td>Step 18</td>
<td>redistribute {static</td>
<td>connected</td>
</tr>
<tr>
<td>Step 19</td>
<td>redist-config &lt;Network&gt; &lt;Mask&gt; [metric-value &lt;metric (1 - 16777215)&gt;] [metric-type {asExttype1</td>
<td>asExttype2}] [tag &lt;tag-value&gt;]</td>
</tr>
<tr>
<td>Step 20</td>
<td>set nssa asbr-default-route translator { enable</td>
<td>disable }</td>
</tr>
<tr>
<td>Step 21</td>
<td>passive-interface {vlan &lt;vlan-id(1-4069)&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt;}</td>
</tr>
<tr>
<td>Step 22</td>
<td>passive-interface default</td>
<td>(Optional) Suppress routing updates on all interfaces</td>
</tr>
<tr>
<td>Step 23</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 24</td>
<td>show ip ospf request-list [&lt;neighbor-id&gt;] [[ vlan &lt;vlan-id (1-4069)&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt; ]]</td>
</tr>
<tr>
<td></td>
<td>show ip ospf border-routers</td>
<td>Display OSPF Border and Boundary Router Information</td>
</tr>
<tr>
<td></td>
<td>show ip ospf {area-range</td>
<td>summary-address}</td>
</tr>
<tr>
<td></td>
<td>show ip ospf info</td>
<td>Display general information about OSPF routing process</td>
</tr>
<tr>
<td></td>
<td>show ip ospf [area-id] database [{database-summary</td>
<td>self originate</td>
</tr>
<tr>
<td></td>
<td>show ip ospf [area-id] database { asbr-summary</td>
<td>external</td>
</tr>
<tr>
<td></td>
<td>show ip ospf area &lt;area-id&gt; stub [no-summary]</td>
<td>Display OSPF Database summary for the LSA type</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>show ip ospf request-list [ip_addr] [vlan integer(1-4096)</td>
<td>iftype &lt;ifnum&gt;]</td>
<td>Display OSPF Link state request list information</td>
</tr>
<tr>
<td>show ip ospf virtual-links</td>
<td>Display OSPF Virtual link information</td>
<td></td>
</tr>
<tr>
<td>show ip ospf border-routers</td>
<td>Display OSPF Border and Boundary Router Information</td>
<td></td>
</tr>
<tr>
<td>show ip ospf {area-range</td>
<td>summary-address}</td>
<td>Display OSPF Summary-address redistribution Information</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Display general information about OSPF routing process</td>
<td></td>
</tr>
<tr>
<td>show ip ospf route</td>
<td>Display routes learned by OSPF process</td>
<td></td>
</tr>
<tr>
<td>show ip ospf [area-id] database [{database-summary</td>
<td>self- originate</td>
<td>adv-router &lt;ip-address&gt;}]</td>
</tr>
<tr>
<td>show ip ospf [area-id] database {asbr-summary</td>
<td>external</td>
<td>network</td>
</tr>
</tbody>
</table>

These commands delete the particular configuration or reset it to its default value.

no area <area-id> stability-interval
no compatible rfc1583
no area <area-id> default-cost [tos <tos value (0-30)>]
no area <area-id> [{stub | nssa}]
no default-information originate always [metric <metric-value (0-0xffffffff)>] [metric-type <type (1-2)>]
no area <area-id> virtual-link <router-id> [authentication] [hello-interval] [retransmit-interval] [transmit-delay] [dead-interval] [{authentication-key | message-digest-key <KeyId (0-255)>}]
no ASBR Router
no area <Areaid> range <Network> <Mask>
no summary-address <Network> <Mask> <Areaid>
no redistribute {static | connected | rip | bgp | all}
no redist-config <Network> <Mask>
no network <Network number> area <area-id> [unnum Vlan <PortNumber>]
no passive-interface {vlan <vlan-id(1-4069)> | <interface-type> <interface-id>}
no passive-interface default
### Interface Parameters

All OSPF Interface level configurations are all optional and must be consistent/compatible across all routers in an attached network. Follow the steps below to configure OSPF parameters in Supermicro switch.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf</td>
<td>Enable OSPF routing process</td>
</tr>
<tr>
<td>Step 3</td>
<td>router-id &lt;router ip address&gt;</td>
<td>Configure the Router ID</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor &lt;neighbor-id&gt; [priority &lt;priority value (0-255)&gt;]</td>
<td>Specify a neighbor router and its priority</td>
</tr>
<tr>
<td>Step 5</td>
<td>Exit</td>
<td>Exit the Router Configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>interface &lt;interface-type&gt;&lt;interface-id&gt; or interface range &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>(Optional) Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the following:
- vlan

interface-id is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: `int range vlan 1-10`

To provide multiple interfaces or ranges, separate with a comma (,). E.g.: `int range vlan 1-10, 20`

If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

| Step 7 | ip ospf demand-circuit | Configure OSPF to treat the interface as an OSPF demand circuit |
| Step 8 | ip ospf retransmit-interval <seconds (0-3600)> | Specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface |
| Step 9 | ip ospf transmit-delay <seconds (0-3600)> | (Optional) Configure the estimated time it takes to transmit a link state update packet on the interface |
| Step 10 | ip ospf priority <value (0 - 255)> | (Optional) Configure the router priority |
| Step 11 | ip ospf hello-interval <seconds (1 - 65535)> | (Optional) Specify the interval between hello packets sent on the interface |
| Step 12 | ip ospf dead-interval <seconds (0-0x7fffffff)> | (Optional) Configure the interval at which hello packets must not be seen before neighbors declare the router down |
| Step 13 | ip ospf cost <cost (1-65535)> [tos <tos value (0-30)>] | (Optional) Explicitly specify the cost of sending a packet on an interface. Type of Service (TOS) is defined as a mapping to the IP Type of Service Flags as defined in the IP Forwarding Table MIB. The condition to select next-hop for a destination from a multipath route (set of next hops for a given destination) is referred to as 'policy', which is specified by the TOS Field. However, TOS field is no longer in use. |
| Step 14 | ip ospf network {broadcast | non-broadcast | point-to-multipoint | point-to-point} | (Optional) Configure the OSPF network type to a type other than the default for a given media. |
| Step 15 | ip ospf authentication-key <password (8)> | (Optional) Specify a password to be used by neighboring routers that are using the OSPF simple password authentication. |
| Step 16 | ip ospf authentication [{message-digest | null}] | (Optional) Specify the authentication type for an interface. |
| Step 17 | ip ospf message-digest-key <Key-ID (0-255)> md5 <md5-Key (16)> | (Optional) Enable OSPF MD5 authentication. |
| Step 18 | End | Exits the configuration mode. |
| Step 19 | show ip ospf interface [ { vlan <vlan-id (1-4096)> | <interface-type> <interface-id> } ] | Display OSPF interface information. |
| | show ip ospf retransmission-list [{neighbor-id}] [ { vlan <vlan-id (1-4096)> | <interface-type> <interface-id> } ] | Display OSPF Link state retransmission list information. |
| | show ip ospf info | Display general information about OSPF routing process. |
These commands delete the particular configuration or reset it to its default value.

- `no ip ospf demand-circuit`
- `no ip ospf retransmit-interval`
- `no ip ospf transmit-delay`
- `no ip ospf priority`
- `no ip ospf hello-interval`
- `no ip ospf dead-interval`
- `no ip ospf cost [tos <tos value (0-30)>]`
- `no ip ospf network`
- `no ip ospf authentication-key`
- `no ip ospf authentication`
- `no ip ospf message-digest-key <Key-ID (0-255)>`

---

### 18.2.17.6 OSPF Configuration Example

The example below shows the commands used to configure OSPF by connecting 2 switches: Switch A and Switch B.

**Figure IP-Unicast-Routing-3: OSPF Configuration Example**

**On Switch A**

```
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/21 untagged
SMIS(config-vlan)# exit
```
SMIS(config)# interface fx 0/21
SMIS(config-if)# switchport pvid 10
SMIS(config-if)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.1
SMIS(config-if)# exit
SMIS(config)# router ospf
SMIS(config-router)# router-id 10.10.10.1
SMIS(config-router)# network 10.10.10.1 area 0.0.0.0
SMIS(config-router)# end

SMIS# show ip ospf neighbor

<table>
<thead>
<tr>
<th>Vrf</th>
<th>Neighbor-ID</th>
<th>Pri</th>
<th>State</th>
<th>DeadTime</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>10.10.10.2</td>
<td>100</td>
<td>FULL/DR_OTHER</td>
<td>30</td>
<td>10.10.10.2</td>
<td>vlan10</td>
</tr>
</tbody>
</table>

SMIS# show ip ospf info

OSPF Router with ID (10.10.10.1) (Vrf  default)
Supports only single TOS(TOS0) route
ABR Type supported is Standard ABR
Number of Areas in this router is 1
Area is 0.0.0.0
Number of interfaces in this area is 1
SPF algorithm executed 15 times

SMIS# show ip ospf route

Vrf  default

OSPF Routing Table

<table>
<thead>
<tr>
<th>Dest/Mask</th>
<th>TOS NextHop/Interface</th>
<th>Cost</th>
<th>Rt.Type</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/255.0.0.0</td>
<td>0 0.0.0.0/vlan10</td>
<td>100</td>
<td>IntraArea 0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

SMIS# show ip ospf interface

vlan10 is line protocol is up
Internet Address 10.10.10.1, Mask 255.0.0.0, Area 0.0.0.0
AS 1, Router ID 10.10.10.1, Network Type BROADCAST, Cost 100
Transmit Delay is 500 sec, State 4, Priority 200
Designated RouterId 10.10.10.1, Interface address 10.10.10.1
Backup Designated RouterId 10.10.10.2, Interface address 10.10.10.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 500
Hello due in 4 sec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with the neighbor 10.10.10.2
Connected to VRF  default

SMIS# show running-config

Building configuration...
Switch ID    Hardware Version    Firmware Version

vlan 1
  ports fx 0/1-48 untagged
  ports cx 0/1-6 untagged
exit
vlan 10
  ports fx 0/21 untagged
exit

interface Fx 0/21
  switchport pvid 10

exit
interface vlan 10
  ip address 10.10.10.1 255.0.0.0

exit
router ospf
router-id 10.10.10.1
network 10.10.10.1 area 0.0.0.0
exit

On Switch B

SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/22 untagged
SMIS(config-vlan)# exit
SMIS(config)# interface fx 0/22
SMIS(config-if)# switchport pvid 10
SMIS(config-if)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.2 255.0.0.0
SMIS(config-if)# exit
SMIS(config)# router ospf
SMIS(config-router)# router-id 10.10.10.2
SMIS(config-router)# network 10.10.10.2 area 0.0.0.0
SMIS(config-router)# end

SMIS# show ip ospf neighbor

<table>
<thead>
<tr>
<th>Vrf</th>
<th>Neighbor-ID</th>
<th>Pri</th>
<th>State</th>
<th>DeadTime</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>10.10.10.2</td>
<td>1</td>
<td>UP</td>
<td>60</td>
<td>10.10.10.1</td>
<td></td>
</tr>
</tbody>
</table>
SMIS# show ip ospf info

OSPF Router with ID (10.10.10.2) (Vrf default)
  Supports only single TOS(TOS0) route
  ABR Type supported is Standard ABR
  Number of Areas in this router is 1
  Area is 0.0.0.0
  Number of interfaces in this area is 1
  SPF algorithm executed 17 times

SMIS# show ip ospf interface

vlan10 is line protocol is up
  Internet Address 10.10.10.2, Mask 255.0.0.0, Area 0.0.0.0
  AS 1, Router ID 10.10.10.2, Network Type BROADCAST, Cost 100
  Transmit Delay is 500 sec, State 5, Priority 100
  Designated RouterId 10.10.10.1, Interface address 10.10.10.1
  Backup Designated RouterId 10.10.10.2, Interface address 10.10.10.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 500
  Hello due in 2 sec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with the neighbor 10.10.10.1
  Connected to VRF default

SMIS# show ip ospf route

Vrf default

OSPF Routing Table

Dest/Mask    TOS NextHop/Interface Cost Rt.Type   Area
----------    --- --------/-------- ---- ---- --------
10.0.0.0/255.0.0.0    0 0.0.0.0/vlan10  100 IntraArea 0.0.0.0

SMIS# show running-config

Building configuration...
Switch ID   Hardware Version   Firmware Version
vlan 1
  ports fx 0/1-48 untagged
  ports cx 0/1-6 untagged
  exit
vlan 10
  ports fx 0/22 untagged
  exit

interface Fx 0/22
switchport pvid 10
exit
interface vlan 10
ip address 10.10.10.2 255.0.0.0
exit
router ospf
router-id 10.10.10.2
network 10.10.10.2 area 0.0.0.0
exit

18.3 BGP

Border Gateway Protocol (BGP) is an inter-domain routing protocol designed to provide loop-free routing links between organizations. BGP is designed to run over a reliable transport protocol using Port 179. BGP is used to connect a local network to an external network in order to access the Internet or to connect to other organizations. When connecting to an external organization, external BGP (eBGP) peering sessions are created. BGP peers within the same organization exchange routing information through internal BGP (iBGP) peering sessions. Supermicro switches support BGP version 4.

![BGP Diagram]

**Figure IP-Unicast-Routing-1: BGP**

BGP uses a path-vector routing algorithm to exchange network reachability information with other BGP speaking networking devices. Network reachability information is exchanged between BGP peers in routing updates. Network reachability information contains the network number, path specific attributes, and the list of autonomous system numbers that a route must transit through to reach a destination network. BGP
then selects a single path, by default, as the best path to a destination host or network. The best path selection algorithm utilizes path attributes to determine the route to be installed in the BGP routing table.

18.3.1 Router ID

BGP uses router ID to identify BGP-speaking peers. The BGP router ID is represented by an IPv4 address. The BGP router ID must be unique to the BGP peers in a network.

18.3.2 Speaker and Peer

A peer device is a BGP-speaking router that has an active TCP connection to another BGP-speaking device. BGP devices need not be necessarily directly connected. A BGP speaker is the local router and a peer is any other BGP speaking network device.

When a TCP connection is established between peers, each BGP peer initially exchanges all its routes—the complete BGP routing table with the other peer. After this only incremental updates are sent after a change in network topology or routing policy. Peers exchange special messages called keep alive messages.

18.3.3 Autonomous System (AS)

An autonomous system is a network controlled by a single technical administration entity. In BGP autonomous systems are used in individual routing domains with local routing policies.

Each routing domain can support multiple routing protocols. However, each routing protocol is administrated separately. Other routing protocols can dynamically exchange routing information with BGP through redistribution.

18.3.4 Aggregate Addresses

Classless inter-domain routing (CIDR) enables creation of aggregate routes (or supernets) to minimize the size of routing tables. Aggregate routes can be configured in BGP either by redistributing an aggregate route into BGP or by creating an aggregate entry in the BGP routing table.

18.3.5 Route Reflection

Typical BGP requires all IBGP speakers to be fully meshed i.e. when a router receives a route from an external neighbor, it must advertise it to all internal neighbors. To prevent a routing information loop, all IBPG speakers must be connected and the internal neighbors do not share routes among themselves.

With route reflectors, all IBGP speakers need not be fully meshed because another method is used to pass learned routes to neighbors. When an internal BGP peer is configured to be a route reflector, it is responsible for passing IBGP learned routes to a set of IBGP neighbors. The internal peers of the route reflector are divided into two groups: client peers and non-client peers (all the other routers in the autonomous system). A route reflector reflects routes between these two groups. The route reflector and its client peers form a cluster. The non-client peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with IBGP speakers outside their cluster.

When the route reflector receives an advertised route, it takes one of these actions, depending on the neighbor:

• A route from an external BGP speaker is advertised to all clients and non-client peers.
• A route from a non-client peer is advertised to all clients.
• A route from a client is advertised to all clients and non-client peers. Hence, the clients need not be fully meshed.

To increase redundancy and to avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the same *cluster ID* so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and should have identical sets of client and non-client peers.

### 18.3.6 Confederation

Another way to reduce the IBGP mesh is to divide an autonomous system into multiple sub-autonomous systems and group them into a single confederation to make it appear as a single autonomous system. Each autonomous system is fully meshed within itself and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they were IBGP peers.

Specifically, the next hop, MED and local preference information is preserved. A *confederation identifier* must be configured to act as the autonomous system number for the group of autonomous systems.

### 18.3.7 Attributes

BGP has a number of complex attributes used to determine a path to a remote network. These attributes allow greater flexibility and enable a complex routing decision to ensure that the path to a remote network is the best possible path. BGP always propagates the best path to any peers. BGP attributes are carried in update packets.

#### 18.3.7.1 Multi-Exit Discriminator (MED) Attribute

The multi-exit discriminator (MED) or metric attribute is used as a suggestion to an external AS regarding the preferred route into the AS that is advertising the metric. A lower MED is always preferred.

#### 18.3.7.2 Local Preference Attribute

If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route. A higher local preference is always preferred.

#### 18.3.7.3 Next-Hop Attribute

The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers. For IBGP, the EBGP next-hop address is carried into the local AS.

#### 18.3.7.4 Community Attribute

Communities allow routes to be tagged for use with a group of routers sharing the same characteristics. The community attribute provides a way of grouping destinations, called communities, to which routing decisions (such as acceptance, preference, and redistribution) can be applied. Some of the predefined community attributes are:

- *no-export* - Do not advertise this route to EBGP peers.
- *no-advertise* - Do not advertise this route to any peer.
- *internet* - Advertise this route to the Internet community; all routers in the network belong to it.
The BGP community attribute is an optional transitive attribute of variable length. The attribute consists of a set of four octet values that specify a community. The community attribute values are encoded with an Autonomous System (AS) number in the first two octets, with the remaining two octets defined by the AS. A router can add or modify a community attribute before it passes the attribute to other peers.

The BGP Extended Community Attribute provides a community attribute structuring by means of a type field.

**18.3.7.5 Cluster ID**

This attribute is used in route-reflector environments and is not used for router selection.

A router reflector cluster normally has a single route reflector. To avoid a single point of failure, a cluster can be configured with more than one route reflector. In case of more than one Route Reflector in the group, a cluster of Route reflectors is established. All Router Reflectors in the cluster are in the same cluster-ID.

Route-Reflector algorithm will not accept the update that has the same Cluster-ID as itself in order to prevent looping.

**18.3.8 Filters**

A number of different filter methods control the send and receive of BGP updates. BGP updates can be filtered with route information as a basis, or with communities as a basis. Packets that do not match the configured filters are dropped.

**18.3.9 Overlapping Routes**

Overlapping routes are non-identical routes that point to the same destination, e.g. 10.10.128.0/17 and 10.10.192.0/18, in which the second route is actually included in the first route.

A BGP speaker can be configured to make the following choices:

a) Install both the less and the more specific routes

b) Install the more specific route only

e) Install the less specific route only

**18.3.10 Synchronization**

When a BGP router receives information about a network from an IBGP neighbor, it does not use that information until a matching route is learned via an IGP or static route. This is called Synchronization. It also does not advertise that route to an EBGP neighbor unless a matching route is in the routing table. It is recommended to turn off synchronization when all routers in the autonomous system run BGP.
18.3.11  BGP Path selection
When a BGP speaker receives updates from multiple autonomous systems that describe different paths to the same destination, it must choose the single best path for reaching that destination. When chosen, the selected path is entered into the BGP routing table and propagated to its neighbors. The decision is based on the value of attributes that the update contains and other BGP-configurable factors.

1. If the next hop address is reachable, consider it.
2. Prefer the largest local preference attribute.
3. If the local preference is the same, prefer the route this local router originated.
4. Prefer the route with the shortest AS path.
5. If this is equal, prefer the route with the origin set to originated (through BGP); IGP is preferred to EGP followed by incomplete.
6. If the origin codes are the same, prefer the route with the lowest MED.
7. If the MED is the same, prefer EBGP over IBGP.
8. Prefer the closest path.
9. Finally, if all paths are equal, prefer the path with lowest BGP router ID.

18.3.12  Timers
BGP implementation in Supermicro switches maintains different timers for Peers and Route updates.

- The *keep alive interval* is the time within which keep alive messages are sent to peers.
- The *hold time* is the interval after which a peer is declared inactive after not receiving a keep alive message from it.
- *Route advertisement interval* is the interval between sending BGP routing updates.
- *Connection Retry timer* is the amount of time to wait before re-opening a TCP connection.
- *AS Originate Interval* is the interval between two subsequent update messages for internal peers.

18.3.13  Route dampening
Route flap dampening minimizes the propagation of flapping routes across an internetwork. A route is considered to flap when it is repeatedly available and unavailable. When route dampening is enabled, a numeric penalty value is assigned to a route when it flaps. When a route’s accumulated penalties reach a configurable limit, BGP suppresses advertisements of the route, even if the route is running.

The reuse limit is a configurable value that is compared with the penalty. If the penalty is less than the reuse limit, a suppressed route that is up is advertised again.

Dampening is not applied to routes learned by IBGP as it prevents IBGP peers from having a higher penalty for routes external to the AS.
18.3.14 BGP Configuration

18.3.14.1 BGP Default Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port</td>
<td>179</td>
</tr>
<tr>
<td>Preference</td>
<td>100</td>
</tr>
<tr>
<td>Metric</td>
<td>0</td>
</tr>
<tr>
<td>MED Comparison</td>
<td>Disabled</td>
</tr>
<tr>
<td>Peer</td>
<td>None</td>
</tr>
<tr>
<td>Overlap policy</td>
<td>Both</td>
</tr>
<tr>
<td>Connection retry time</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Hold time</td>
<td>120 seconds</td>
</tr>
<tr>
<td>Keep alive</td>
<td>30 seconds</td>
</tr>
<tr>
<td>AS Originate Interval</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Route Advertisement Interval</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
</tr>
<tr>
<td>EIBGP Multihop</td>
<td>Disable</td>
</tr>
<tr>
<td>Next-hop self</td>
<td>Disable</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Metric</td>
<td>0</td>
</tr>
<tr>
<td>Route dampening</td>
<td>Enabled</td>
</tr>
<tr>
<td>Redistribution</td>
<td>Enabled</td>
</tr>
<tr>
<td>AS Number</td>
<td>None</td>
</tr>
<tr>
<td>Router ID</td>
<td>None</td>
</tr>
<tr>
<td>Community Peer</td>
<td>None</td>
</tr>
<tr>
<td>Community Filter</td>
<td>None</td>
</tr>
<tr>
<td>Extended Community Peer</td>
<td>None</td>
</tr>
<tr>
<td>Extended Community Filter</td>
<td>None</td>
</tr>
</tbody>
</table>

Pre-requisite: Autonomous System (AS) Number “as-num <value (1-65535)>” and Router-ID “router-id <addr>” must be configured in Supermicro switch prior to BGP Configuration.

18.3.14.2 Enabling BGP

BGP is disabled by default in Supermicro switches. Follow the steps below to enable BGP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show bgp-version</code></td>
<td>Displays the BGP Version information.</td>
</tr>
<tr>
<td></td>
<td><code>show ip bgp info</code></td>
<td>Displays the general info about bgp protocol.</td>
</tr>
</tbody>
</table>

The “no router bgp” command disables BGP in the switch.

18.3.14.3  **BGP Peer**

Supermicro switches provide option to configure BGP Peer. Follow the steps below to configure BGP Peer.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router bgp &lt;AS no(1-65535)&gt;</code></td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>bgp router-id &lt;bgp router id (ip-address)&gt;</code></td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>neighbor &lt;ip-address&gt; remote-as &lt;AS no(1-65535)&gt;</code></td>
<td>Creates a Peer and initiates the connection to the peer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>`neighbor &lt;ip-address&gt; {advertisement-interval &lt;seconds&gt;</td>
<td>as-origination-interval &lt;seconds&gt;</td>
</tr>
<tr>
<td>Step 6</td>
<td>`neighbor &lt;ip-address&gt; timers {keepalive &lt;seconds&gt;</td>
<td>holdtime &lt;seconds&gt;}`</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>neighbor &lt;ip-address&gt; shutdown</code></td>
<td>(Optional) Disables the Peer session.</td>
</tr>
<tr>
<td>Step 8</td>
<td>`neighbor &lt;ip-address&gt; send-community {both</td>
<td>standard</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>neighbor &lt;ip-address&gt; password password-string</code></td>
<td>(Optional) Configure the password for TCP-MD5 authentication with peer.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>Exit</code></td>
<td>Exits BGP Router Mode</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>shutdown ip bgp</code></td>
<td>(Optional) Configure the BGP Speaker Global Admin status DOWN.</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>End</code></td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>`show ip bgp {[neighbor [&lt;peer-addr&gt;]]</td>
<td>[rib]}`</td>
</tr>
<tr>
<td></td>
<td><code>show ip bgp timers</code></td>
<td>Displays the value of bgp timers.</td>
</tr>
<tr>
<td></td>
<td><code>show ip bgp info</code></td>
<td>Displays the general info about bgp protocol.</td>
</tr>
</tbody>
</table>
no shutdown ip bgp
no neighbor <ip-address>
no neighbor <ip-address> {advertisement-interval | as-origination-interval | connect-retry-interval}
no neighbor <ip-address> timers {keepalive | holdtime}
no neighbor <ip-address> shutdown
no neighbor <ip-address> password

18.3.14.4 Confederation
Supermicro switches allow configuration of BGP Confederation. Follow the steps below to configure BGP Confederation.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp router-id &lt;bgp router id (ip-address)&gt;</td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor &lt;ip-address&gt; remote-as &lt;AS no(1-65535)&gt;</td>
<td>Creates a Peer and initiates the connection to the peer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>bgp confederation identifier &lt;AS no(1-65535)&gt;</td>
<td>(Optional) Specify BGP confederation identifier.</td>
</tr>
<tr>
<td>Step 6</td>
<td>bgp confederation peers &lt;AS no(1-65535)&gt;</td>
<td>(Optional) Configure the AS that belongs to the confederation</td>
</tr>
<tr>
<td>Step 7</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ip bgp info</td>
<td>Displays the BGP related information.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp confed info</td>
<td>Displays info about confederation feature.</td>
</tr>
</tbody>
</table>

The commands “no bgp confederation identifier” and “no bgp confederation peers <AS no(1-65535)>” delete the Confederation ID and peers.

18.3.14.5 Attributes
Supermicro switches provide user configuration of BGP attributes. Follow the steps below to configure BGP Attributes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp router-id &lt;bgp router id (ip-address)&gt;</td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor &lt;ip-address&gt; remote-as &lt;AS_no(1-65535)&gt;</td>
<td>Creates a Peer and initiates the (Optional) connection to the peer.</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Step 5</td>
<td>bgp default local-preference &lt;Local Pref Value&gt;</td>
<td>(Optional) Configures the Default Local Preference value.</td>
</tr>
<tr>
<td>Step 6</td>
<td>neighbor &lt;ip-address&gt; ebgp-multihop</td>
<td>(Optional) Enables BGP to establish connection with external peers that are not directly connected</td>
</tr>
<tr>
<td>Step 7</td>
<td>neighbor &lt;ip-address&gt; next-hop-self</td>
<td>(Optional) Enables BGP to send itself as the next hop for advertised routes.</td>
</tr>
<tr>
<td>Step 8</td>
<td>neighbor &lt;ip-address&gt; send-community {both</td>
<td>standard</td>
</tr>
<tr>
<td>Step 9</td>
<td>bgp always-compare-med</td>
<td>(Optional) Enables the comparison of med for routes received from different autonomous system.</td>
</tr>
<tr>
<td>Step 11</td>
<td>bgp med &lt;1-100&gt; remote-as &lt;0-65535&gt; &lt;ip-address&gt; &lt;ip_mask&gt; [intermediate-as &lt;AS-no list-AS1,AS2,...&gt;] value &lt;value&gt; direction &lt;in</td>
<td>out&gt; [override]</td>
</tr>
<tr>
<td>Step 12</td>
<td>bgp local-preference &lt;1-100&gt; remote-as &lt;0-65535&gt; &lt;ip-address&gt; &lt;ip_mask&gt; [intermediate-as &lt;AS-no list-AS1,AS2,...&gt;] value &lt;value&gt; direction &lt;in</td>
<td>out&gt; [override]</td>
</tr>
<tr>
<td>Step 13</td>
<td>bgp update-filter &lt;1-100&gt; &lt;permit</td>
<td>deny&gt; remote-as &lt;0-65535&gt; &lt;ip-address&gt; &lt;ip_mask&gt; [intermediate-as &lt;AS-no list-AS1,AS2,...&gt;] direction &lt;in</td>
</tr>
<tr>
<td>Step 14</td>
<td>bgp cluster-id &lt;cluster id value(ip_address)&gt;</td>
<td>(Optional) Configures the Cluster ID for Route Reflector.</td>
</tr>
<tr>
<td>Step 15</td>
<td>bgp comm-route {additive</td>
<td>delete} &lt;ip-address&gt; &lt;ip_mask&gt; comm-value &lt;4294967041-4294967043,65536-4294901759&gt;</td>
</tr>
<tr>
<td>Step 16</td>
<td>bgp comm-peer &lt;ip-address&gt; &lt;permit</td>
<td>deny&gt;</td>
</tr>
<tr>
<td>Step 17</td>
<td>bgp comm-filter &lt;comm-value(4294967041-4294967043,65536-4294901759)&gt; &lt;permit</td>
<td>deny&gt; &lt;in</td>
</tr>
<tr>
<td>Step 18</td>
<td>bgp comm-policy &lt;ip-address&gt; &lt;ip_mask&gt; &lt;set-add</td>
<td>set-none</td>
</tr>
<tr>
<td>Step 20</td>
<td>bgp ecomm-peer &lt;ip-address&gt; &lt;permit</td>
<td>deny&gt;</td>
</tr>
<tr>
<td>Step 21</td>
<td>bgp ecomm-filter &lt;ecomm-value(xx:xx:xx:xx:xx:xx:xx:xx)&gt; &lt;permit</td>
<td>deny&gt; &lt;in</td>
</tr>
</tbody>
</table>
### Step 22
```
bgp ecomm-policy <ip-address> <ip_mask> <set-add|set-none|modify>
```
(Optional) Configures the ext community attribute advertisement policy for specific destination

### Step 23
```
bgp bestpath med confed
```
(Optional) Enables MED comparison among paths learned from confed peers

### Step 24
```
Exit
```
Exits BGP Router Mode

### Step 25
```
clear ip bgp {* | <ip-address>} [soft {in|out}]
```
(Optional) Resets the bgp connection dynamically for inbound and outbound route policy

### Step 26
```
End
```
Exits Configuration mode.

### Step 27
```
show ip bgp community community-number(4294967041-4294967043,65536-4294901759) [exact]
```
Displays routes that belong to specified BGP communities.

```
```
Displays routes that belong to specified BGP extended-communities.

```
show ip bgp filters
```
Displays the contents of filter table.

```
show ip bgp med
```
Displays the contents of MED table.

```
show ip bgp local-pref
```
Displays the contents of local preference table.

```
show ip bgp info
```
Displays the general info about bgp protocol.

```
show ip bgp community {route|peer|policy|filter}
```
Displays the contents of community tables.

```
show ip bgp extcommunity {route|peer|policy|filter}
```
Displays the contents of ext-community tables.

---

- no bgp default local-preference
- no neighbor <ip-address> ebgp-multihop
- no neighbor <ip-address> next-hop-self
- no neighbor <ip-address> send-community {both | standard | extended}
- no bgp always-compare-med
- no bgp med <1-100>
- no bgp local-preference <1-100>
- no bgp update-filter <1-100>
- no bgp cluster-id
- no bgp comm-route {additive|delete} <ip-address> <ip_mask> comm-value <4294967041-4294967043,65536-4294901759>
- no bgp comm-peer <ip-address>
- no bgp comm-filter <comm-value(4294967041-4294967043,65536-4294901759)> <permit|deny> <in|out>
- no bgp comm-policy <ip-address> <ip_mask>
Supermicro switches allow users to configure Route Reflection. Follow the steps below to configure BGP Route Reflection.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp router-id &lt;bgp router id (ip-address)&gt;</td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor &lt;ip-address&gt; remote-as &lt;AS no(1-65535)&gt;</td>
<td>Creates a Peer and initiates the connection to the peer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>bgp client-to-client reflection</td>
<td>(Optional) Configures the Route Reflector to support route reflection to Client Peers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>neighbor &lt;ip-address&gt; route-reflector-client</td>
<td>(Optional) Configures the Peer as Client of the Route Reflector.</td>
</tr>
<tr>
<td>Step 7</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ip bgp {[neighbor [&lt;peer-addr&gt;]]</td>
<td>[rib]}</td>
</tr>
<tr>
<td></td>
<td>show ip bgp info</td>
<td>Displays the BGP related information.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp rfl info</td>
<td>Displays info about Route Reflection feature.</td>
</tr>
</tbody>
</table>

Cluster ID must be configured before configuring Route Reflection.

The “no bgp client-to-client reflection” command disables Route Reflection. The “no neighbor <ip-address> route-reflector-client” commands delete the Route reflection client.

Supermicro switches provide option to configure Route Dampening. Follow the steps below to configure BGP Route Dampening.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>neighbor &lt;ip-address&gt; remote-as &lt;AS no(1-65535)&gt;</td>
<td>Creates a Peer and initiates the connection to the peer.</td>
</tr>
<tr>
<td>Step 4</td>
<td>bgp client-to-client reflection</td>
<td>(Optional) Configures the Route Reflector to support route reflection to Client Peers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>neighbor &lt;ip-address&gt; route-reflector-client</td>
<td>(Optional) Configures the Peer as Client of the Route Reflector.</td>
</tr>
<tr>
<td>Step 6</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip bgp {[neighbor [&lt;peer-addr&gt;]]</td>
<td>[rib]}</td>
</tr>
<tr>
<td></td>
<td>show ip bgp info</td>
<td>Displays the BGP related information.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp rfl info</td>
<td>Displays info about Route Reflection feature.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp router-id &lt;bgp router id (ip-address)&gt;</td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor &lt;ip-address&gt; remote-as &lt;AS no(1-65535)&gt;</td>
<td>Creates a Peer and initiates the connection to the peer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Exit</td>
<td>Exits BGP Router Mode</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip bgp dampening [HalfLife-Time [Reuse Value] [Suppress Value] [Max-Suppress Time] [s] [Array Size]] [s] [Decay Granularity [Reuse Granularity [Reuse Array Size]]]</td>
<td>(Optional) Configures the Dampening Parameters</td>
</tr>
<tr>
<td>Step 7</td>
<td>clear ip bgp &lt;ip-address&gt; flap-statistics</td>
<td>(Optional) Clear flap-statistics counters for all paths from the neighbor at the IP address.</td>
</tr>
<tr>
<td>Step 8</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ip bgp dampening</td>
<td>Displays the contents of dampening table.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp info</td>
<td>Displays the BGP related information.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp dampened-paths</td>
<td>Displays the dammed routes.</td>
</tr>
<tr>
<td></td>
<td>show ip bgp flap-statistics [ip-address]&lt;Mask&gt;</td>
<td>Displays the statistics of flapped routes.</td>
</tr>
</tbody>
</table>

The “`no ip bgp dampening [HalfLife-Time [Reuse-Value [Suppress-Value [Max-Suppress-Time]]]] [s] [Array Granularity [Reuse Granularity [Reuse Array Size]]]`” command deletes the BGP Dampening Parameters.

### 18.3.14.8 Other Parameters

Supermicro switches provide configuration of several BGP parameters, like Synchronization, redistribution etc. Follow the steps below to configure BGP parameters.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp &lt;AS no(1-65535)&gt;</td>
<td>Enable BGP and configure the AS number of the BGP Speaker</td>
</tr>
<tr>
<td>Step 3</td>
<td>bgp router-id &lt;bgp router id (ip-address)&gt;</td>
<td>Configures the BGP Identifier of the BGP Speaker.</td>
</tr>
<tr>
<td>Step 4</td>
<td>bgp nonbgproute-advt &lt;external</td>
<td>both&gt;</td>
</tr>
<tr>
<td>Step 5</td>
<td>default-metric &lt;Default Metric Value&gt;</td>
<td>(Optional) Configures the Default IGP Metric value.</td>
</tr>
<tr>
<td>Step 6</td>
<td>redistribute &lt;static</td>
<td>connected</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Step 7</td>
<td>aggregate-address index &lt;1-100&gt; &lt;ip-address&gt; &lt;ip_mask&gt; [summary-only]</td>
<td>(Optional) Configures an entry in Aggregate Table.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Exit</td>
<td>Exits BGP Router Mode</td>
</tr>
<tr>
<td>Step 9</td>
<td>ip bgp overlap-policy &lt;more-specific</td>
<td>less-specific</td>
</tr>
<tr>
<td>Step 10</td>
<td>ip bgp synchronization</td>
<td>(Optional) Enables synchronization between BGP and IGP.</td>
</tr>
<tr>
<td>Step 11</td>
<td>clear ip bgp {*}</td>
<td>&lt;ip-address&gt; [soft {in</td>
</tr>
<tr>
<td>Step 12</td>
<td>End</td>
<td>Exits Configuration mode.</td>
</tr>
<tr>
<td>Step 13</td>
<td>show ip bgp info</td>
<td>Displays the BGP related information.</td>
</tr>
<tr>
<td>show ip bgp aggregate</td>
<td>Displays the contents of aggregate table.</td>
<td></td>
</tr>
</tbody>
</table>

These commands reset the particular configuration to its default value.

- no ip bgp overlap-policy
- no ip bgp synchronization
- no ip bgp nonbgproute-advt
- no redistribute <static|connected|rip|ospf|all>
- no default-metric

### 18.3.14.9 BGP Configuration Example

The example below shows the commands used to configure BGP by connecting 2 switches: Switch A and Switch B.

**Figure IP-Unicast-Routing-4: BGP Configuration Example**

**On Switch A**
SMIS# configure terminal
SMIS(config)# interface Fx 0/21

SMIS(config)# interface Fx 0/22

Switch B

Switch A
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 200
SMIS(config-if)# exit
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address 10.10.10.2
SMIS(config-if)# exit
SMIS(config)# as-num 1
SMIS(config)# router-id 10.10.10.2
SMIS(config)# router bgp 1
SMIS(config-router)# neighbor 10.10.10.1 remote-as 1
SMIS(config-router)# bgp default local-preference 50
SMIS(config-router)# default-metric 50
SMIS(config-router)# neighbor 10.10.10.1 ebgp-multihop
SMIS(config-router)# neighbor 10.10.10.1 timers keepalive 10
SMIS(config-router)# neighbor 10.10.10.1 advertisement-interval 5
SMIS(config-router)# end

SMIS# show ip bgp neighbor

BGP neighbor is 10.10.10.1, remote AS 1, internal link
BGP version 4, remote router ID 10.10.10.1
BGP state = Established, up for 11 minutes 31 seconds
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30 secs
Neighbors Capability:
   Route-Refresh: Advertised and received
   Address family IPv4 Unicast: Advertised and received
Received 24 messages, 0 Updates
Sent 24 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 10.10.10.2, Local port: 179
Foreign host: 10.10.10.1, Foreign port: 32768
Last Error: Code 0, SubCode 0.

SMIS# show ip bgp info

Routing Protocol is "bgp 1"
IGP synchronization is disabled
Both more-specific and less-specific overlap route policy is set
Local Preference is 50
Non-bgp routes are advertised to both external and internal peers
MED Comparision is disabled
Metric is 50

Peer Table
   Peer Address RemoteAS NextHop   MultiHop
---- -------- ------- --------- ------
   10.10.10.1   1   automatic   enable

TCPMD5 Auth Table
SMIS# show ip bgp summary

BGP router identifier is 10.10.10.2, local AS number 1

BGP table version is 0

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Version</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>4</td>
<td>1</td>
<td>24</td>
<td>24</td>
<td>00:00:11:41</td>
<td>Established</td>
</tr>
</tbody>
</table>

SMIS# show ip bgp dampening

Half Life Time is 900
Reuse value is 500
Suppress value is 3500
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

vlan 1
  ports fx 0/1-20 untagged
  ports fx 0/22-48 untagged
  ports cx 0/1-6 untagged
exit
vlan 200
exit

interface Fx 0/21
  switchport mode access
  switchport access vlan 200
exit

interface vlan 200
  ip address 10.10.10.2 255.0.0.0
exit

as-num 1
router-id 192.168.100.102

router bgp 1
bgp router-id 192.168.100.102
On switch B
SMIS# configure terminal
SMIS(config)# interface Fx 0/21
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 200
SMIS(config-if)# exit
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address 10.10.10.1
SMIS(config-if)# exit
SMIS(config)# as-num 1
SMIS(config)# router-id 10.10.10.1
SMIS(config)# router bgp 1
SMIS(config-router)# neighbor 10.10.10.2 remote-as 1
SMIS(config-router)# bgp always-compare-med
SMIS(config-router)# bgp bestpath med confed
SMIS(config-router)# bgp client-to-client reflection
SMIS(config-router)# bgp comm-peer 10.10.10.2 permit
SMIS(config-router)# bgp default local-preference 80
SMIS(config-router)# default-metric 100
SMIS(config-router)# neighbor 10.10.10.2 timers keepalive 10
SMIS(config-router)# neighbor 10.10.10.2 advertisement-interval 5
SMIS(config-router)# end

SMIS# show ip bgp summary
BGP router identifier is 10.10.10.1, local AS number 1
BGP table version is 0

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Version</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.2</td>
<td>4</td>
<td>1</td>
<td>20</td>
<td>20</td>
<td>00:00:9:43</td>
<td>Established</td>
</tr>
</tbody>
</table>

SMIS# show ip bgp info
Routing Protocol is "bgp 1"
IGP synchronization is disabled
Both more-specific and less-specific overlap route policy is set
Local Preference is 80
Non-bgp routes are advertised to both external and internal peers
MED Comparison is enabled
Metric is 100
Peer Table
Peer Address  RemoteAS  NextHop  MultiHop
---  -------  ------  -------
10.10.10.2  1  automatic  disable

TCPMD5 Auth Table
Peer Address  Password
---  -------

SMIS# show ip bgp neighbor

BGP neighbor is 10.10.10.2, remote AS 1, internal link
BGP version 4, remote router ID 192.168.100.102
BGP state = Established, up for 10 minutes 4 seconds
Rcvd update before 0 secs, hold time is 120, keepalive interval is 30 secs
Neighbors Capability:
   Route-Refresh: Advertised and received
   Address family IPv4 Unicast: Advertised and received
Received 21 messages, 0 Updates
Sent 21 messages, 0 Updates
Route refresh: Received 0, sent 0.
Minimum time between advertisement runs is 5 seconds
Connections established 1 time(s)
Local host: 10.10.10.1, Local port: 32768
Foreign host: 10.10.10.2, Foreign port: 179
Last Error: Code 0, SubCode 0.

SMIS# show ip bgp community peer
Community Peer Table
IpAddress  SendStatus
---------  -------
10.10.10.2  send

SMIS# show ip bgp dampened-paths
Status codes: d dampened, h history,* valid

Network  From  LastUpdt  Path
------  ----  -------  ----

SMIS# show ip bgp dampening
Half Life Time is 900
Reuse value is 500
Suppress value is 3500
Max Suppress time is 3600
Decay timer granularity is 1
Reuse timer granularity is 15
Reuse index array size is 1024
SMIS# show ip bgp timers
Peer Timers
Peer Address Holdtime KeepAliveTime ConnectRetry ASOrig RouteAdvt
---- ------- -------- ------- -------- -------
10.10.10.2 120 10 30 15 5

SMIS# show ip bgp local-pref
Index Admin Remote-AS Prefix PrefixLen Inter-AS Direction Value Preference Status
---- ------ --------- --------- --------- ------- ------- -------

SMIS# show running-config

Building configuration...
Switch ID Hardware Version Firmware Version
vlan 1
ports fx 0/1-20 untagged
ports fx 0/22-48 untagged
ports cx 0/1-6 untagged
exit
vlan 200
exit

interface Fx 0/21
switchport mode access
switchport access vlan 200
exit

interface vlan 200
ip address 10.10.1.1 255.0.0.0
exit

as-num 1
router-id 10.10.1.1

router bgp 1
bgp router-id 10.10.1.1
bgp default local-preference 80
bgp always-compare-med
default-metric 100
bgp bestpath med confed
neighbor 10.10.10.2 remote-as 1
neighbor 10.10.10.2 send-community standard
bgp comm-peer 10.10.10.2 permit
neighbor 10.10.10.2 timers keepalive 10
neighbor 10.10.10.2 advertisement-interval 5
exit
19 PIM Configuration

IP Multicast Overview

IP communication is of three types:

- Unicast: Host sends packets to a single host
- Broadcast: Host sends packets to all hosts
- Multicast: Host sends packets to a subset of hosts simultaneously

IP Multicast Routing enables efficient usage of network resources for bandwidth intensive services including video and audio. A multicast group is a set of receivers that want to receive a particular data stream. An IP Multicast Group Address in the range 224.0.0.0 to 239.0.0.0 is selected for receivers of a multicast group. Senders transmit IP data using the Multicast Group address as the destination address to multicast to all group members. Receivers interested in receiving data of a particular group must join the group by signaling a router/switch on their subnet. IGMP is used as the signaling protocol for conveying group membership. Network devices along the path from Source to Receivers forward data only on ports leading to the receivers, rather than flooding on all ports.

Membership in a multicast group is dynamic as hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

Supermicro switches can send and receive Multicast traffic by supporting the following Multicast features:

- **IGMP** at the access end of the network that processes hosts announcing their participation in a Multicast group(s).

- **Multicast Routing Protocol’s (MRP’s)** at the enterprise and core of the network for maintaining the senders/receivers database and forwarding data from Senders to Receivers.

![Figure PIM-1: IP Multicast Routing](image)
19.1 PIM

Protocol Independent Multicast (PIM) is a Multicast Routing Protocol (MRP) to maintain the Multicast distribution tree and forward Multicast data across the tree. PIM is protocol independent since it works with any unicast routing protocols like RIP, OSPF etc to get route information towards RP and Source.

PIM neighbors are established by exchanging periodic Hello messages. A Designated Router (DR) is chosen in the subnet connected to the receivers and this is the Last-hop DR. A DR is chosen in the subnet connected to the Source, this is the First-hop DR.

The path from receivers to Source or RP is called upstream. The path from Source or RP towards receivers is called downstream.

There are two modes of PIM: Sparse (PIM-SM) and Dense (PIM-DM).

19.1.1 PIM-SM Basics

PIM Sparse mode operates on basis that very few or sparse receivers intend to receive Multicast data from each source. In PIM-SM Multicast data is forwarded only on branches with at least one interested receiver.

Figure PIM-2: Multicast Forwarding with PIM-SM

PIM-SM uses unicast routing protocol like OSPF, RIP etc to perform reverse-path forwarding (RPF) check to determine upstream neighbor to source and/or RP. RPF check helps to eliminate loops in Multicast tree.
formation wherein the forwarding decision for a received packet is done based on the source address in the packet rather than destination address—If router has a route entry to the source address in the packet i.e. upstream router, the packet is forwarded, as RPF check passes; otherwise packet is dropped as RPF check failure.

PIM Sparse mode builds a *shared tree or RPT* with a root called as *Rendezvous Point (RP)*. A *Candidate RP (CRP)* is configured for every group, then by using *Bootstrap router (BSR)* mechanism CRP is populated as a *RP-set* across the domain. After receiving RP set, every router performs a uniform hashing to elect one RP for every group, from the RP-set.

Receivers interested in particular Multicast group data from any source send a (*, G) join to upstream neighbor towards the router elected as RP for the particular group. The last-hop DR can choose to receive Multicast data directly from each source for that group, instead of from the RP. In this case, the last-hop DR sends (S, G) join to upstream towards source and this is called *Source-specific tree or Shortest Path Tree (SPT)*. PIM-SM is typically used in WAN environment.

### 19.1.2 PIM-DM Basics

PIM Dense mode operates on basis that almost all possible subnets have at least one interested receiver. Hence in PIM-DM Multicast data is flooded on all possible branches, and then pruned when branches do not want Multicast data from a particular Group and/or source. PIM-DM is typically used in LAN environment.

**Figure PIM-3: Multicast Forwarding with PIM-DM**

19.2 PIM Support

Supermicro switches support both PIM-SM and PIM-DM.

IP Multicast routing table can hold 2550 entries, which includes 255 Groups and 10 sources per group.
PIM requires a unicast routing protocol such as RIP or OSPF to learn the routes to Source, CRP, and CBSR. PIM uses this information for RPF check.

19.3 PIM Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM-SM global status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Component Identifier</td>
<td>1</td>
</tr>
<tr>
<td>Static RP status</td>
<td>Disabled</td>
</tr>
<tr>
<td>PMBR status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Shortest Path Tree (SPT) threshold</td>
<td>0 packets</td>
</tr>
<tr>
<td>RP threshold</td>
<td>0 packets</td>
</tr>
<tr>
<td>Shortest Path Tree (SPT) switchover period</td>
<td>0 seconds</td>
</tr>
<tr>
<td>RP switchover period</td>
<td>0 seconds</td>
</tr>
<tr>
<td>Register stop Rate limit period</td>
<td>5 seconds</td>
</tr>
</tbody>
</table>

PIM Component defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Component Mode</td>
<td>Sparse</td>
</tr>
<tr>
<td>CRP hold time</td>
<td>70 seconds</td>
</tr>
<tr>
<td>CRP priority</td>
<td>192</td>
</tr>
<tr>
<td>Static RP</td>
<td>None</td>
</tr>
</tbody>
</table>

PIM interface defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello interval</td>
<td>30 seconds</td>
</tr>
<tr>
<td>DR priority</td>
<td>1</td>
</tr>
<tr>
<td>Override interval</td>
<td>0</td>
</tr>
<tr>
<td>LAN Prune Delay status</td>
<td>Enabled</td>
</tr>
<tr>
<td>LAN Prune Delay</td>
<td>0</td>
</tr>
<tr>
<td>Hello hold time</td>
<td>3.5 x Hello interval</td>
</tr>
<tr>
<td>CBSR preference</td>
<td>-1</td>
</tr>
</tbody>
</table>

19.4 Enabling PIM

PIM is disabled by default in Supermicro switches.

PIM needs to be enabled globally for IP Multicast operation. Follow the steps below to enable PIM.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
Step 1  **configure terminal**  Enters the configuration mode.
Step 2  **set ip pim enable**  Enables PIM globally. PIM creates the default PIM Component Identifier 1, once PIM is enabled.
Step 3  **end**  Exits the configuration mode.
Step 4  **show ip pim component**  Displays the PIM information.
Step 5  **write startup-config**  Optional step – saves this PIM configuration to be part of the startup configuration.

---

If PIM is enabled globally, all PIM components are also automatically PIM enabled. All PIM configuration and display commands operate only when PIM is enabled.

The example below shows the commands to enable PIM.

SMIS# **configure terminal**  
SMIS(config)# **set ip pim enable**  
SMIS(config)# **end**  
SMIS# **show ip pim component**  

PIM Component Information

Component-Id: 1  
PIM Mode: sparse, PIM Version: 2  
Elected BSR: 0.0.0.0  
Candidate RP Holdtime: 0

---

19.5  **PIM Component and Interface**

Supermicro switch provides multiple instances of PIM in a router. The PIM instances are referred as PIM component. Every component can be associated with one or more layer3 VLAN interface(s) and is identified by a component Identifier.

Follow the steps below to create PIM component(s).

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | **ip pim component <ComponentId (1-255)>** | Creates the PIM component and enters the Component mode.  
The Component Identifier value can be any number from 1-255. Default is 1. |
| Step 3 | interface <interface-type> <interface-id>
or interface range <interface-type> <interface-id> .... | Enters the interface configuration mode.

interface-type – may be any of the following:
vl

interface-id is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: Int vlan range 1-10

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range vlan 1-10, 20

If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.

| Step 4 | ip pim componentId <value(1-255)> | Configures Interface Component Identifier value.

The Component Identifier value can be any number from 1-255. Default is 1.

| Step 5 | end | Exits the configuration mode.

| Step 6 | show ip pim interface [{ Vlan <vlan-id> | <interface-type> <interface-id> | detail }]
show ip pim component [ComponentId <1-255>] | Displays the component information for the given interface.

| Step 7 | write startup-config | Optional step – saves this PIM configuration to be part of the startup configuration.

Component can be created only if PIM is enabled. An interface can be associated with Component Identifier, only if Component Identifier has been created already.

The ‘no ip pim component <ComponentId>’ command deletes the component and its associated details.

The example below shows the commands to configure PIM component.
SMIS# configure terminal
SMIS(config)# ip pim component 50
SMIS(config-comp)# end

SMIS# configure terminal
SMIS(config)# vlan 100
SMIS(config-vlan)# ports fx 0/22 untagged
SMIS(config-vlan)# end

SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# ip address 100.100.100.1 255.0.0.0
SMIS(config-if)# ip pim componentId 50
SMIS(config-if)# end

SMIS# show ip pim component

PIM Component Information
---------------------------
Component-Id: 1
  PIM Mode: sparse, PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0

Component-Id: 50
  PIM Mode: sparse, PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0

SMIS# show ip pim interface detail

vlan100 504 is up
  Internet Address is 100.100.100.1
  Multicast Switching: Enabled
  PIM: Enabled
  PIMv6: Disabled
  PIM version: 2, mode: Sparse
  PIM DR: 100.100.100.1
  PIM DR Priority: 1
  PIM Neighbour Count: 0
  PIM Hello/Query Interval: 30
  PIM Message Interval: 60
  PIM Override Interval: 0
  PIM Lan Delay: 0
  PIM Lan-Prune-Delay: Disabled
  PIM Component Id: 50
  PIM domain border: disabled
19.6 PIM Mode

PIM operates in sparse mode by default in Supermicro switches. PIM mode can be changed at anytime per component. All routers in a PIM domain must have same PIM mode.

Follow the steps below to set PIM mode in components.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip pim component &lt;ComponentId (1-255)&gt;</td>
<td>Enters the PIM component configuration mode. Component Identifier may be any value from 1 to 255. Default is 1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>set mode {sparse</td>
<td>dense}</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip pim component [ComponentId &lt;1-255&gt;]</td>
<td>Displays the PIM mode for the given component.</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM mode.

SMIS# configure terminal
SMIS(config)# ip pim component 50
SMIS(pim-comp)# set mode dense
SMIS(pim-comp)# end

SMIS# show ip pim component

PIM Component Information
---------------------------
Component-Id: 1
PIM Mode: sparse, PIM Version: 2
Elected BSR: 0.0.0.0
Candidate RP Holdtime: 0

Component-Id: 50
PIM Mode: dense, PIM Version: 2
Graft Retry Count: 1

19.7 PIM neighbor

PIM routers exchange periodic Hello message with directly connected routers. These directly connected routers are the PIM neighbors. PIM Hello message contains different configurable options.
## 19.7.1 DR Priority

DR priority is used to determine the Designated Router in the subnet. The Designated Router in the subnet is the router with highest DR priority. As a last-hop router, the DR is responsible for forwarding joins to upstream. As a first-hop router, the DR is responsible for forwarding data to downstream.

The default DR priority is 1.

Supermicro switches provide flexibility for user to configure DR priority for individual interfaces. User can configure different DR priority on different interfaces.

Follow the steps below to change Hello interval on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt; &lt;interface-id&gt;</code>&lt;br&gt;or interface range <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> ....</td>
<td>Enters the interface configuration mode.&lt;br&gt;<code>interface-type</code> – may be any of the following: vlan&lt;br&gt;<code>interface-id</code> is the VLAN identifier for VLAN interfaces.&lt;br&gt;To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: <code>interface range vlan 10-20</code>&lt;br&gt;OR <code>interface range vlan 1,5,10</code>&lt;br&gt;To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: <code>int range vlan 1-10, 20</code>&lt;br&gt;If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip pim dr-priority &lt;priority(1-65535)&gt;</code></td>
<td>Configures PIM DR priority value.&lt;br&gt;The DR priority value can be any number from 1-65535. Default is 1.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>`show ip pim interface [{ Vlan &lt;vlan-id&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt;</td>
</tr>
</tbody>
</table>
Step 6 | **write startup-config**
---|---
Optional step – saves this PIM configuration to be part of the startup configuration.

The ‘no ip pim dr-priority’ command resets the DR priority to its default value of 1.

The example below shows the commands to configure PIM DR priority.

**Configure PIM DR priority for layer3 VLAN 100**

```
SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# ip pim dr-priority 500
SMIS(config-if)# end

SMIS# show ip pim interface detail
vlan100 504 is up
Internet Address is 100.100.100.1
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
PIM version : 2, mode: Sparse
PIM DR : 100.100.100.1
**PIM DR Priority : 500**
PIM Neighbour Count : 0
PIM Hello/Query Interval : 30
PIM Message Interval : 60
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 50
PIM domain border : disabled
```

**19.7.2 Hello interval**

PIM router sends Hello messages periodically to all its neighbors to maintain information about directly connected upstream router(s) towards Source(s) or RP(s) and downstream routers towards receivers. This periodic time interval is called the **Hello interval**.

The default Hello interval is 30 seconds.

Supermicro switches provide flexibility for user to configure Hello interval for individual interfaces. User can configure different Hello interval on different interfaces.

Follow the steps below to change Hello interval on any interface.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> or interface range <code>&lt;interface-type&gt; &lt;interface-id&gt;</code> { ....</td>
<td>Enters the interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-type</code> – may be any of the following: vlan</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-id</code> is the VLAN identifier for VLAN interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: interface range vlan 10-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range vlan 1-10, 20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim query-interval &lt;Interval (0-65535)secs&gt;</td>
<td>Configures PIM Hello interval value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Hello interval value can be any number from 0-65535. Default is 30seconds.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip pim interface [{ Vlan &lt;vlan-id&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt;</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The ‘no ip pim query-interval’ command resets the query interval to its default value of 30.

The example below shows the commands to configure PIM query-interval.

**Configure PIM query-interval for layer3 VLAN 100**
SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# ip pim query-interval 75
SMIS(config-if)# end

SMIS# show ip pim interface detail

vlan100 504 is up
  Internet Address is 100.100.100.1
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
    PIM version : 2, mode: Sparse
    PIM DR : 100.100.100.1
    PIM DR Priority : 1
    PIM Neighbour Count : 0
    PIM Hello/Query Interval : 75
  PIM Message Interval : 60
  PIM Override Interval : 0
  PIM Lan Delay : 0
  PIM Lan-Prune-Delay : Disabled
  PIM Component Id : 50
  PIM domain border : disabled

19.7.3 Hold time

Hold time is the neighbor timeout set for every neighbor on a PIM interface. If a PIM hello message is not received from a neighbor router for the period of the Hold time, then the neighbor will be deleted from the list of neighbors. Hold time value is sent as an option in the PIM hello message to neighbors.

The default Hold time is 3.5 x Hello Interval (i.e. 3.5 * 30 = 105 seconds).

The show command in example shows PIM Hello hold time.

SMIS# show ip pim interface detail

vlan100 146 is up
  Internet Address is 10.1.2.2
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
    PIM version : 2, mode: Sparse
    PIM DR : 10.1.2.2
    PIM DR Priority : 1
    PIM Neighbour Count : 1
    PIM Hello/Query Interval : 30
    Hello-Holdtime : 105
  PIM Message Interval : 60
  PIM Override Interval : 0
**19.8 Multicast Routing Table**

The Multicast routing table contains information about active Multicast trees. This table lists both forwarding and non-forwarding entries i.e. Multicast entries which have data flowing and entries which do not have data flow.

Every entry in the Multicast routing table has one Incoming Interface (IIF) and one or more Outgoing Interfaces (OIF’s). The entry can be (*,G) or (S,G). (*,G) entries have W and R bit set, while (S,G) entries have Shortest Path Tree (SPT) bit set. The RP and RPF neighbor are also listed.

---

The route to BSR, RP and Source must be reachable via any unicast protocol. Otherwise Multicast routing table is not formed due to RPF check failure.

Below example shows the PIM Multicast routing table display output.

```bash
SMIS# show ip pim mroute

IP Multicast Routing Table
--------------------------
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table For Component 50
(*, 225.1.1.1),00:00:02/--- ,RP : 100.100.100.1
   Incoming Interface : vlan100 ,RPF nbr : NULL ,Route Flags : WR
   Outgoing InterfaceList :
     vlan100, Forwarding/Sparse ,00:00:02/---
```

**19.9 PMBR**

PIM multicast border routers (PMBR) is the border between two or more PIM domains running different MRP’s like PIM-SM, PIM-DM or DVMRP. PMBRs connect each PIM domain to the rest of the Internet. The PMBR forwards multicast packets across different domains, hence receivers in one domain receive packets from sources in another domain. In a PMBR, different interfaces can be configured as DVMRP, PIM-SM or PIM-DM interfaces.

PMBR is disabled by default in Supermicro switches.

Follow the steps below to enable PMBR.
### Step 1
**Command**: configure terminal
**Description**: Enters the configuration mode.

### Step 2
**Command**: set ip pim pmbr enable
**Description**: Enables or disables PMBR.

### Step 3
**Command**: end
**Description**: Exits the configuration mode.

### Step 4
**Command**: write startup-config
**Description**: Optional step – saves this PIM configuration to be part of the startup configuration.

---

**The ‘set ip pim pmbr disable’ command disables PMBR functionality.**

---

The example below shows the commands to configure PIM PMBR.

```
SMIS# configure terminal
SMIS(config)# set ip pim pmbr enable
SMIS(config)# end

SMIS# show ip pim interface detail

vlan100 504 is up
  Internet Address is 100.100.100.1
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
    PIM version : 2, mode: Sparse
    PIM DR : 100.100.100.1
    PIM DR Priority : 1
    PIM Neighbour Count : 0
    PIM Hello/Query Interval : 30
    PIM Message Interval : 60
    PIM Override Interval : 0
    PIM Lan Delay : 0
    PIM Lan-Prune-Delay : Disabled
    PIM Component Id : 50
    PIM domain border : enabled
```

---

### 19.10 Disabling PIM

PIM is disabled by default in Supermicro switches.

After enabling PIM, if user needs to disable it, it has to be disabled globally.

Follow the steps below to disable PIM.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
Step 2  `set ip pim disable`  Disables PIM globally.

Step 3  `end`  Exits the configuration mode.

Step 4  `write startup-config`  Optional step – saves this PIM configuration to be part of the startup configuration.

The example below shows the commands used to disable PIM.

SMIS# configure terminal
SMIS(config)# set ip pim disable
SMIS(config)# end

19.11  PIM-SM Specific Configuration
This section covers Supermicro switch commands that are applicable only in PIM-SM mode.

19.11.1  PIM Join/Prune

19.11.1.1  Join-Prune Interval
PIM router sends Join messages periodically to upstream router towards RP or Source to keep the Multicast tree active. Periodic Prune messages are sent when existing receivers do not want Multicast data. This periodic time interval for sending Join/Prune is called the `Join-Prune interval`.

The default Join-Prune interval is 60 seconds.

Supermicro switches provide flexibility for user to configure Join-Prune interval for individual interfaces. User can configure different Join-Prune interval on different interfaces.

Follow the steps below to change Join-Prune interval on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface &lt;interface-type&gt; &lt;interface-id&gt;</code> or <code>interface range &lt;interface-type&gt; &lt;interface-id&gt;</code></td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

`interface-type` – may be any of the following:

`vlan`

`interface-id` is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the "`interface range` ..." command. To provide a range use a hyphen (-) between the start and end interface...
numbers. E.g.: `interface range vlan 10-20`

To provide multiple interfaces or ranges, use separate with a comma (,).
E.g.: `int range vlan 1-10, 20`

If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>ip pim message-interval &lt;Interval(1-65535)&gt;</code></td>
<td>Configures PIM Join prune interval value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Join prune interval value can be any number from 1-65535. Default is 60.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>`show ip pim interface [{ Vlan &lt;vlan-id&gt;</td>
<td>&lt;interface-type&gt; &lt;interface-id&gt;</td>
</tr>
<tr>
<td>6</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The ‘no ip pim message-interval’ command resets the Join-prune interval to its default value of 60.

The example below shows the commands to configure PIM Join-Prune interval.

**Configure PIM Join-Prune interval for layer3 VLAN 100**

```
SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# ip pim message-interval 300
SMIS(config-if)# end

SMIS# show ip pim interface detail
```

```
vlan100 504 is up
  Internet Address is 100.100.100.1
  Multicast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
    PIM version : 2, mode: Sparse
    PIM DR : 100.100.100.1
    PIM DR Priority : 1
```
PIM Neighbour Count : 0
PIM Hello/Query Interval : 30
PIM Message Interval : 300
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 50
PIM domain border : disabled

19.11.1.2  LAN Prune delay

LAN Prune Delay option is used in Multi-Access network to delay processing of prune messages received at upstream routers. This ensures in a multi-access LAN there is no flapping of Multicast data due to Join by some routers and prune by some other routers.

When an upstream router in a multi-access LAN receives prune message from a downstream router, it does not prune the tree immediately, instead maintains the tree for the LAN prune delay interval. The tree is maintained only if a ‘Join override’ message is received from another downstream router in the multi-access LAN. Otherwise the tree is pruned after ‘LAN Prune Delay interval’.

The default ‘LAN delay’ flag is ‘Disabled’ state. Default value of LAN prune delay is 0 seconds.

Supermicro switches provide flexibility for user to configure LAN Prune Delay for individual interfaces. User can configure different LAN Prune Delay on different interfaces.

Follow the steps below to change LAN Prune Delay on any interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface range &lt;interface-type&gt; &lt;interface-id&gt; ....</td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the following:

vlan

interface-id is the VLAN identifier for VLAN interfaces.

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: interface range vlan 10-20

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range vlan 1-10,20
If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.

| Step 3 | set ip pim lan-prune-delay { enable | disable } | Configures LAN prune delay value. LAN prune-delay is disabled by default. |
|--------|-----------------------------------------------|---------------------------------------------------------------------|
|        | ip pim lan-delay <value(0-65535)>             | The LAN prune delay value can be any number from 0-65535. Default is 0. |
| Step 4 | end                                           | Exits the configuration mode.                                       |
| Step 5 | show ip pim interface [{ Vlan <vlan-id> | <interface-type> <interface-id> | detail }] | Displays the LAN prune delay information for the given interface. |
| Step 6 | write startup-config                          | Optional step – saves this PIM configuration to be part of the startup configuration. |

The ‘no ip pim lan-delay’ command resets the LAN delay to its default value of 0.

The example below shows the commands to configure PIM LAN delay.

**Configure PIM LAN delay for layer3 VLAN 100**

SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# set ip pim lan-prune-delay enable
SMIS(config-if)# ip pim lan-delay 200
SMIS(config-if)#end

SMIS# show ip pim interface detail

vlan100 504 is up
  Internet Address is 100.100.100.1
  Muticast Switching : Enabled
  PIM : Enabled
  PIMv6 : Disabled
  PIM version : 2, mode: Sparse
  PIM DR : 100.100.100.1
  PIM DR Priority : 1
  PIM Neighbour Count : 0
  PIM Hello/Query Interval : 30
  PIM Message Interval : 60
  PIM Override Interval : 0
  PIM Lan Delay : 200
  PIM Lan-Prune-Delay : Enabled
  PIM Component Id : 50
19.11.1.3 Override Interval

The Join/prune override interval is used in a Multi-Access network by downstream routers. The downstream router in a multi-access LAN waits for a period of override interval after sending a prune message, to send a second Prune message if it still continues to receive data due to other routers in multi-access LAN that still want to receive Multicast data.

Override interval ensures in a multi-access LAN, Multicast data is forwarded only if there is at least one router with receivers interested in a particular group and so data is not flooded unnecessarily in the multi-access LAN.

The default Override interval is 0 seconds.

Supermicro switches provide flexibility for user to configure Join/prune override interval for individual interfaces. User can configure different Join/prune override interval on different interfaces.

Follow the steps below to configure Override interval.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; or interface range &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>Enters the interface configuration mode.</td>
</tr>
</tbody>
</table>

interface-type – may be any of the following:

<table>
<thead>
<tr>
<th>interface-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>is the VLAN identifier for VLAN interfaces.</td>
</tr>
</tbody>
</table>

To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: interface range vlan 10-20

To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range vlan 1-10,20

If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces.
### Step 3
`ip pim override-interval <interval(0-65535)>`
- **Configures PIM override interval value.**
- The override interval value can be any number from 0-65535. Default is 0.

### Step 4
`end`
- Exits the configuration mode.

### Step 5
`show ip pim interface [{ Vlan <vlan-id> | <interface-type> <interface-id> | detail }]`
- Displays the override interval information for the given interface.

### Step 6
`write startup-config`
- Optional step – saves this PIM configuration to be part of the startup configuration.

---

The ‘no ip pim override-interval’ command resets the override interval to its default value of 0.

The example below shows the commands to configure PIM override interval.

**Configure PIM override interval for layer3 VLAN 100**

```
SMIS# configure terminal
SMIS(config)# interface vlan 100
SMIS(config-if)# ip pim override-interval 500
SMIS(config-if)# end

SMIS# show ip pim interface detail
```

vlan100 504 is up
Internet Address is 100.100.100.1
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
  PIM version : 2, mode: Sparse
  PIM DR : 100.100.100.1
  PIM DR Priority : 1
  PIM Neighbour Count : 0
  PIM Hello/Query Interval : 30
  PIM Message Interval : 60
  **PIM Override Interval : 500**
  PIM Lan Delay : 0
  PIM Lan-Prune-Delay : Disabled
  PIM Component Id : 50
  PIM domain border : disabled

### 19.11.2 Shared Tree (RPT)

An RP is used as the central information exchange point in PIM domain as it reduces the amount of state in non-RP routers. No network flooding is required to provide non-RP routers information about active sources. All routers in a PIM domain must have same RP information for a particular group.

RP’s in a PIM domain can be learnt by Bootstrap Router (BSR) mechanism or Static RP.
### Bootstrap Router (BSR)

BSR distributes PIM RP information for all groups within the domain. Each PIM domain can have only 1 elected BSR. Several routers are configured as candidate BSRs, the BSR is elected as the router with highest preference. The elected RP’s send their information to the BSR and BSR maintains RP-to-group mapping as the RP-set.

Supermicro switches provide flexibility for user to configure BSR for individual interface.

Follow the steps below to configure Bootstrap router (BSR)

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | interface <interface-type> <interface-id> 
or interface range <interface-type> <interface-id> | Enters the interface configuration mode. |
|      | *interface-type* – may be any of the following: vlan |
|      | *interface-id* is the VLAN identifier for VLAN interfaces. |
|      | To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: **interface range vlan 10-20** |
|      | To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: **int range vlan 1-10,20** |
|      | If multiple interfaces are provided, the next step will perform the particular PIM configuration on all these interfaces. |
| Step 3 | ip pim bsr-candidate <value (0-255)> | Configures PIM BSR candidate. |
|      | The BSR candidate preference value can be any number from -1 to 255. Default is -1. |
| Step 4 | end | Exits the configuration mode. |
| Step 5 | show ip pim bsr [Component-id (1-255)] | Displays the BSR candidate information for the given interface. |
| Step 6 | write startup-config | Optional step – saves this PIM configuration to be part of the startup configuration. |
The ‘no ip pim bsr-candidate’ command deletes the BSR information of the particular interface.

The example below shows the commands to configure PIM Candidate BSR.

**Configure PIM Candidate BSR for layer3 VLAN 100**

SMIS# configure terminal  
SMIS(config)# interface vlan 100  
SMIS(config-if)# ip pim bsr-candidate 155  
SMIS(config-if)# end

SMIS# show ip pim bsr

PIMv2 Bootstrap Configuration For Component 1
-----------------------------------------------
Elected BSR for Component 1
BSR Address : 0.0.0.0  
BSR Priority : 0, Hash Mask Length : 30

This system is the PIMv4 Bootstrap Router (BSR)
BSR Address : 100.100.100.1  
BSR Priority : 155, Hash Mask Length : 30

**19.11.2.2 Candidate RP (CRP)**

The RP is the central convergence point of sources and receivers. In a PIM sparse domain, there are multiple Candidate-RP’s but only one elected RP per group. The elected RP is the candidate RP with highest IP address. The elected RP’s send their information to the BSR and BSR maintains RP-to-group mapping as the RP-set.

Supermicro switches provide flexibility for user to configure CRP for individual components. User can configure different CRP on different component.

Follow the steps below to configure Candidate RP (CRP).

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip pim component &lt;ComponentId (1-255)&gt;</td>
<td>Enters the PIM component configuration mode. Component Identifier may be any value from 1 to 255. Default is 1.</td>
</tr>
<tr>
<td>Step 3</td>
<td>rp-candidate rp-address &lt;Group Address&gt; &lt;Group Mask&gt; &lt;IP address&gt;</td>
<td>Configures Candidate RP value.</td>
</tr>
</tbody>
</table>
**Group Address/Group Mask**: This combination can specify any IP Multicast address from 224.0.0.0 to 239.255.255.255.

**IP Address** should be any interface IP address of the component.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>rp-candidate holdtime &lt;Holdtime value (0-255)&gt;</code></td>
<td>Optional. Configures Candidate RP Hold time value. The hold time value can be any number from 0-255. Default is 70 seconds.</td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>show ip pim rp-candidate [ComponentId &lt;1-255&gt;]</code></td>
<td>Displays the Candidate RP information for the given interface.</td>
</tr>
<tr>
<td>7</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM Candidate RP.

**Configure PIM Candidate RP for PIM component 50**

```
SMIS# configure terminal
SMIS(config)# ip pim component 50
SMIS(pim-comp)# rp-candidate holdtime 180
SMIS(pim-comp)# rp-candidate rp-address 228.0.0.0 255.0.0.0 100.100.100.1
SMIS(pim-comp)# end
```

```
SMIS# show ip pim rp-candidate

<table>
<thead>
<tr>
<th>CompId</th>
<th>GroupAddress</th>
<th>Group Mask</th>
<th>RPAddress/Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>228.0.0.0</td>
<td>255.0.0.0</td>
<td>100.100.100.1/192</td>
</tr>
</tbody>
</table>
```

**19.11.2.3 Static RP**

An RP for a group range can be configured statically on a router, instead of using BSR mechanism. However, using this mechanism requires configuring static RP on all routers in the PIM domain. This configuration can be useful to specify a backup RP for a particular group.
Supermicro switches provide flexibility for user to configure Static RP for individual components. User can configure different Static RP on different component.

Follow the steps below to configure Static RP.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip pim component &lt;ComponentId (1-255)&gt;</code></td>
<td>Enters the PIM component configuration mode. Component Identifier may be any value from 1 to 255. Default is 1.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>set ip pim static-rp enable</code></td>
<td>Static RP is disabled by default. Use the ‘enable’ form of this command to enable Static RP.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>rp-static rp-address &lt;Group Address&gt; &lt;Group Mask&gt; &lt;IP address&gt;</code></td>
<td>Configures static RP value. <em>Group Address/Group Mask:</em> This combination can specify any IP Multicast address from 224.0.0.0 to 239.255.255.255. <em>IP Address</em> should be any interface IP address of the component.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show ip pim rp-static [ComponentId &lt;1-255&gt;]</code></td>
<td>Displays the static RP information for the given interface.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

---

The `no ip pim rp-static` command deletes the static RP information of the particular component.

---

The example below shows the commands to configure PIM Static RP.

**Configure PIM Static RP for PIM component 50**

SMIS(config)# `set ip pim static-rp enable`

SMIS# `configure terminal`
SMIS(config)# `ip pim component 50`
SMIS(pim-comp)# `rp-static rp-address 230.0.0.0 255.0.0.0 100.100.100.1`
SMIS(pim-comp)# `end`

SMIS# `show ip pim rp-static`
### 19.11.2.4 Register-Stop Rate-limit

When first-hop DR receives multicast packet, it encapsulates it in a Register message and unicasts it to the RP for that group. The RP de-encapsulates each Register message and forwards the extracted data packet to downstream members on the RPT. If there are no receivers on RP, it then sends Register stop to First-hop DR as long as there are no receivers. Register-Stop rate limit is used at RP to limit the number of register-stop messages sent per second to the First-hop DR.

The default Register-stop rate limit is 0.

Follow the steps below to configure Register-Stop Rate limit.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip pim regstop-ratelimit-period &lt;0-2147483647(in secs)&gt;</td>
<td>Sets the Register-Stop rate limit for Group and Source. The Register-Stop rate limit interval can be any number from 0 – 2147483647 seconds. Default is 0 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM Register rate limit.

```
SMIS# configure terminal
SMIS(config)# set ip pim regstop-ratelimit-period 100
SMIS(config)# end

SMIS# show ip pim thresholds
PIM SPT Threshold Information
-----------------------------
Group Threshold : 0
Source Threshold : 0
Switching Period : 0

PIM SPT-RP Threshold Information
-----------------------------
Register Threshold : 0
RP Switching Period : 0
Register Stop rate limit : 100
```
19.11.3 Shortest Path Tree (SPT)

19.11.3.1 SPT at RP

When first-hop DR receives multicast packet, it encapsulates it in a Register message and unicasts it to the RP for that group. The RP de-encapsulates each Register message and forwards the extracted data packet to downstream members on the RPT.

The RP then sends an (S, G) Join to the first-hop DR to build the Source-tree or Shortest Path Tree (SPT) back to the source. This mechanism of RP building a SPT is called SPT switchover at RP.

Typically, the SPT switchover occurs when a data-rate threshold is reached which is configurable in Supermicro switches using:

- RP switch period
- RP threshold

19.11.3.1.1 RP switch period

RP switch period is used together with RP threshold to specify the time when the RP can switch over to Shortest Path Tree (SPT). Multicast data packet count is checked every RP-switch-period’ interval and if the count exceeds RP threshold, the RP switches from RP tree to Shortest Path Tree (SPT).

RP switch period is disabled by default in Supermicro switches i.e. RP’s switch to SPT immediately upon receipt of Multicast data packet.

Follow the steps below to configure RP switch period.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip pim rp-switchperiod &lt;0-2147483647(in secs)&gt;</td>
<td>Sets the RP switch period at RP. The RP switch period can be any number from 0 – 2147483647 seconds. Default is 0 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM RP switch period.

SMIS# configure terminal
SMIS(config)# set ip pim rp-switchperiod 300
SMIS(config)# end

SMIS# show ip pim thresholds

PIM SPT Threshold Information
Group Threshold : 0
Source Threshold : 0
Switching Period : 0

PIM SPT-RP Threshold Information
----------------------------------------------
Register Threshold       : 0
RP Switching Period      : 300
Register Stop rate limit : 5

19.11.3.1.2   RP threshold
RP threshold is used together with RP switch period to specify the time when the RP can switch over to Shortest Path Tree (SPT). Multicast data packet count is checked every RP-switch-period’ interval and if the count exceeds RP threshold, the RP switches from RP tree to Shortest Path Tree (SPT).

RP threshold is disabled by default in Supermicro switches i.e. RP’s switch to SPT immediately upon receipt of Multicast data packet.

Follow the steps below to configure RP threshold.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip pim rp-threshold &lt; number of packets(0-2147483647)&gt;</td>
<td>Sets the SPT threshold for Group and Source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Number of packets can be any number from 0 – 2147483647. Default is 0 packets.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM RP threshold.

SMIS# configure terminal
SMIS(config)# set ip pim rp-threshold 50
SMIS(config)# end

SMIS# show ip pim thresholds

PIM SPT Threshold Information
----------------------------------------------
Group Threshold : 0
Source Threshold : 0
Switching Period : 0

PIM SPT-RP Threshold Information
Register Threshold : 50
RP Switching Period : 0
Register Stop rate limit : 5

19.11.3.2 SPT at Last-hop DR
When last-hop DR receives multicast packet from Shared tree or RP tree, it sends an (S, G) Join to the first-hop DR to build the Source-tree or Shortest Path Tree (SPT) back to the source. This mechanism of last-hop DR building a SPT is called SPT switchover at Last-hop DR. Once SPT is established at last-hop DR, the RPT is pruned and data is then received by SPT only.

Typically, the SPT switchover occurs when a data-rate threshold is reached which is configurable in Supermicro switches using:

- SPT switch period
- SPT threshold

19.11.3.2.1 SPT switch period
Shortest Path Tree (SPT) switch period is used together with SPT threshold to specify the time when the last-hop router can switch over to Shortest Path Tree (SPT). Multicast data packet count is checked every 'SPT-switch-period' interval and if the count exceeds SPT threshold, the last-hop router switches from RP tree to Shortest Path Tree (SPT).

Shortest Path Tree (SPT) switch period is disabled by default in Supermicro switches i.e. last-hop routers switch to SPT immediately upon receipt of Multicast data packet.

Follow the steps below to configure Shortest Path Tree (SPT) switch period.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip pim spt-switchperiod &lt;0-2147483647(in secs)&gt;</td>
<td>Sets the Shortest Path Tree (SPT) threshold for Group and Source. The Number of packets can be any number from 0 – 2147483647. Default is 0 packets.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure SPT switch period.

SMIS# configure terminal
SMIS(config)# set ip pim spt-switchperiod 30
SMIS(config)# end
SMIS# show ip pim thresholds

PIM SPT Threshold Information
-------------------------------
Group Threshold : 0
Source Threshold : 0
Switching Period : 30

PIM SPT-RP Threshold Information
---------------------------------
Register Threshold : 0
RP Switching Period : 0
Register Stop rate limit : 5

19.11.3.2.2 SPT threshold

Shortest Path Tree (SPT) threshold is used together with SPT switch period to specify the time when the last-hop router can switch over to SPT. Multicast data packet count is checked every SPT-switch-period’ interval and if the count exceeds SPT threshold, the last-hop router switches from RP tree to SPT.

Shortest Path Tree (SPT) threshold is disabled by default in Supermicro switches i.e. last-hop routers switch to SPT immediately upon receipt of Multicast data packet.

Follow the steps below to configure Shortest Path Tree (SPT) threshold.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set ip pim threshold { spt-grp</td>
<td>spt-src } &lt; number of packets(0-2147483647)&gt;</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>write startup-config</td>
<td>Optional step – saves this PIM configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows the commands to configure PIM SPT threshold.

SMIS# configure terminal
SMIS(config)# set ip pim threshold spt-grp 100
SMIS(config)# set ip pim threshold spt-src 200
SMIS(config)# end

SMIS# show ip pim thresholds

PIM SPT Threshold Information
-------------------------------
Group Threshold : 100
Source Threshold : 200
Switching Period : 0

PIM SPT-RP Threshold Information
---------------------------------
Register Threshold : 0
RP Switching Period : 0
Register Stop rate limit : 5

19.12 PIM Configuration example

Figure PIM-4: PIM Configuration example

On switch A
1) Enable PIM and IGMP globally
2) Configure PIM component 110
3) Create layer 3 VLAN interfaces 10 and 200
4) Configure PIM Component Identifier as 110 for both layer3 VLANs 10 and 200
5) Configure static RP on Component Identifier 110
6) Configure static IGMP groups on Layer 3 VLAN interface 10

On switch B
1) Enable PIM and IGMP globally
2) Configure PIM component 100
3) Create layer 3 VLAN interface 200
4) Configure PIM Component Identifier as 100 for layer3 VLAN 200
5) Configure static RP on Component Identifier 100
**Configuration on switch A**

#configure Layer3 VLAN
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports fx 0/1 untagged
SMIS(config-vlan)# exit
SMIS(config)# vlan 200
SMIS(config-vlan)# ports fx 0/24 untagged
SMIS(config-vlan)# end

SMIS# configure terminal
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address 200.200.200.5 255.255.255.0
SMIS(config-if)# exit
SMIS(config)# interface vlan 10
SMIS(config-if)# ip address 10.10.10.10 255.255.255.0
SMIS(config-if)# end

#Enable PIM and IGMP
SMIS# configure terminal
SMIS(config)# interface vlan 10
SMIS(config-if)# set ip igmp enable
SMIS(config-if)# exit

SMIS(config)# set ip igmp enable
SMIS(config)# set ip pim enable
SMIS(config)# end

#configure Component
SMIS# configure terminal
SMIS(config)# ip pim component 110
SMIS(pim-comp)# end

SMIS# configure terminal
SMIS(config)# interface vlan 200
SMIS(config-if)# ip pim componentId 110
SMIS(config-if)# end

SMIS# configure terminal
SMIS(config)# interface vlan 10
SMIS(config-if)# ip pim componentId 110
SMIS(config-if)# end

#configure Static RP
SMIS# configure terminal
SMIS(config)# set ip pim static-rp enable
SMIS(config)# ip pim component 110
SMIS(pim-comp)# rp-static rp-address 227.0.0.0 255.0.0.0 200.200.200.1
SMIS(pim-comp)# end
#configure Static Group membership
SMIS# configure terminal
interface vlan 10
ip igmp static-group 227.1.1.1

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

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

Building configuration...
Switch ID    Hardware Version    Firmware Version
ip address dhcp
vlan 1
  ports fx 0/2-23 untagged
  ports fx 0/25-48 untagged
  ports ex 0/1-4 untagged
exit
vlan 10
  ports fx 0/1 untagged
exit
vlan 200
  ports fx 0/24 untagged
exit

snmp view restricted 1 excluded nonvolatile

interface vlan 1
  ip address dhcp

interface vlan 200
  ip address 200.200.200.5 255.255.255.0

interface vlan 10
  ip address 10.10.10.10 255.255.255.0
  set ip igmp enable
  ip igmp static-group 227.1.1.1

exit
set ip igmp enable

set ip pim enable
set ip pim static-rp enable
ip pim component 1
exit
ip pim component 110
rp-static rp-address 227.0.0.0 255.0.0.0 200.200.200.1
exit
interface vlan 200
ip pim componentId 110
exit
interface vlan 10
ip pim componentId 110
exit

#Display PIM neighbor information
SMIS# show ip pim neighbor

<table>
<thead>
<tr>
<th>Neighbour Address</th>
<th>IfName/Idx</th>
<th>Uptime/Expiry Interval</th>
<th>Ver</th>
<th>DRPri/Mode</th>
<th>CompId</th>
<th>Override Lan Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.200.200.1</td>
<td>vlan200/910</td>
<td>00:24:17/90</td>
<td>v2</td>
<td>1/S</td>
<td>110</td>
<td>0</td>
</tr>
</tbody>
</table>

#Display PIM interface information
SMIS# show ip pim interface detail

vlan200 910 is up
Internet Address is 200.200.200.5
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
  PIM version : 2, mode: Sparse
  PIM DR : 200.200.200.5
  PIM DR Priority : 1
  PIM Neighbour Count : 1
  PIM Hello/Query Interval : 30
  PIM Message Interval : 60
  PIM Override Interval : 0
  PIM Lan Delay : 0
  PIM Lan-Prune-Delay : Disabled
  PIM Component Id : 110
  PIM domain border : disabled

vlan10 912 is up
Internet Address is 10.10.10.10
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
  PIM version : 2, mode: Sparse
  PIM DR : 10.10.10.10
  PIM DR Priority : 1
  PIM Neighbour Count : 0
  PIM Hello/Query Interval : 30
  PIM Message Interval : 60
  PIM Override Interval : 0
PIM LAN Delay: 0
PIM LAN-Prune-Delay: Disabled
PIM Component Id: 110
PIM domain border: disabled

# Display PIM component
SMIS# show ip pim component

PIM Component Information
---------------------------
Component-Id: 1
  PIM Mode: sparse, PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0

Component-Id: 110
  PIM Mode: sparse, PIM Version: 2
  Elected BSR: 0.0.0.0
  Candidate RP Holdtime: 0

# Display IGMP static group membership
SMIS# show ip igmp groups

I - Include Mode, E - Exclude Mode
S - Static Mbr, D - Dynamic Mbr

<table>
<thead>
<tr>
<th>GroupAddress</th>
<th>Flg</th>
<th>Iface</th>
<th>UpTime</th>
<th>ExpiryTime</th>
<th>LastReporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.1.1.1</td>
<td>S</td>
<td>vlan10</td>
<td>[0d 00:23:17.94] [0d 00:00:00.00] 10.10.10.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>227.5.5.5</td>
<td>S</td>
<td>vlan10</td>
<td>[0d 00:12:30.67] [0d 00:00:00.00] 0.0.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SMIS# show ip igmp interface
vlan10, line protocol is up
Internet Address is 10.10.10.10/8
IGMP is enabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
Last member query response interval is 10 seconds
IGMP max query response time is 100 seconds
Robustness value is 2
IGMP querying router is 10.10.10.10 (this system)
Fast leave is disabled on this interface
Number of multicast groups joined 2

# Display PIM static RP
SMIS# show ip pim rp-static

Static-RP Enabled

<table>
<thead>
<tr>
<th>CompId</th>
<th>GroupAddress</th>
<th>Group Mask</th>
<th>RPAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>110</td>
<td>227.0.0.0</td>
<td>255.0.0.0</td>
<td>200.200.200.1</td>
</tr>
</tbody>
</table>
#Display Multicast routing table
SMIS# show ip pim mroute

IP Multicast Routing Table
------------------------
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table For Component 110
(*, 227.1.1.1) ,00:14:20/--- ,RP : 200.200.200.1
   Incoming Interface : vlan200 ,RPF nbr : 200.200.200.1 ,Route Flags : WR
   Outgoing InterfaceList :
      vlan10, Forwarding/Sparse ,00:14:20/---

(*, 227.5.5.5) ,00:12:48/--- ,RP : 200.200.200.1
   Incoming Interface : vlan200 ,RPF nbr : 200.200.200.1 ,Route Flags : WR
   Outgoing InterfaceList :
      vlan10, Forwarding/Sparse ,00:12:48/---

### Configuration on switch B

#configure Layer3 VLAN
SMIS# configure terminal
SMIS(config)# vlan 200
SMIS(config-vlan)# ports fx 0/24 untagged
SMIS(config-vlan)# end

SMIS# configure terminal
SMIS(config)# interface vlan 200
SMIS(config-if)# ip address 200.200.200.1 255.255.255.0
SMIS(config-if)# end

#Enable PIM and IGMP
SMIS# configure terminal
SMIS(config)# set ip pim enable
SMIS(config)# end

#configure Component
SMIS# configure terminal
SMIS(config)# ip pim component 100
SMIS(pim-comp)# end

SMIS# configure terminal
SMIS(config)# interface vlan 200
SMIS(config-if)# ip pim componentId 100
SMIS(config-if)# end

#configure Static RP
SMIS# configure terminal
SMIS(config)# set ip pim static-rp enable
SMIS(config)# ip pim component 100
SMIS(pim-comp)# rp-static rp-address 227.0.0.0 255.0.0.0 200.200.200.1
SMIS(pim-comp)# end

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

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

Building configuration...

  ip address dhcp
  vlan 1
    ports fx 0/1-23 untagged
    ports ex 0/1-3 untagged
  exit
  vlan 100
  exit
  vlan 200
  ports fx 0/24 untagged
  exit

  interface vlan 200
    ip address 200.200.200.1 255.255.255.0

  interface vlan 100
  exit
  set ip pim enable
  set ip pim static-rp enable
  ip pim component 1
  exit
  ip pim component 100
  rp-static rp-address 227.0.0.0 255.0.0.0 200.200.200.1
  exit
  interface vlan 200
    ip pim componentId 100
  exit

  #Display PIM component
  SMIS# show ip pim component

  PIM Component Information
  ---------------------------
  Component-Id: 1
PIM Mode: sparse, PIM Version: 2
Elected BSR: 0.0.0.0
Candidate RP Holdtime: 0

Component-Id: 100
PIM Mode: sparse, PIM Version: 2
Elected BSR: 0.0.0.0
Candidate RP Holdtime: 0

#Display Static RP
SMIS# show ip pim rp-static

Static-RP Enabled

<table>
<thead>
<tr>
<th>Compld</th>
<th>GroupAddress</th>
<th>Group Mask</th>
<th>RPAddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>227.0.0.0</td>
<td>255.0.0.0</td>
<td>200.200.200.1</td>
</tr>
</tbody>
</table>

#Display PIM neighbor information
SMIS# show ip pim neighbor

<table>
<thead>
<tr>
<th>Neighbour</th>
<th>IfName/Idx</th>
<th>Uptime/Expiry Ver</th>
<th>DRPri/Mode</th>
<th>Compld Override</th>
<th>Lan Address</th>
<th>Interval</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.200.200.5</td>
<td>vlan200/504</td>
<td>00:21:19/84</td>
<td>v2</td>
<td>1/S</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#Display PIM Interface information
SMIS# show ip pim interface detail

vlan200 504 is up
Internet Address is 200.200.200.1
Multicast Switching : Enabled
PIM : Enabled
PIMv6 : Disabled
PIM version : 2, mode: Sparse
PIM DR : 200.200.200.5
PIM DR Priority : 1
PIM Neighbour Count : 1
PIM Hello/Query Interval : 30
PIM Message Interval : 60
PIM Override Interval : 0
PIM Lan Delay : 0
PIM Lan-Prune-Delay : Disabled
PIM Component Id : 100
PIM domain border : disabled

#Display Multicast routing table
SMIS# show ip pim mroute

IP Multicast Routing Table
Route Flags S: SPT Bit W: Wild Card Bit R: RPT Bit
Timers: Uptime/Expires
Interface State: Interface, State/Mode

PIM Multicast Routing Table For Component 100

(*, 227.1.1.1), 00:11:02/----, RP : 200.200.200.1
Incoming Interface : vlan200, RPF nbr : NULL, Route Flags : WR
Outgoing InterfaceList :
  vlan200, Forwarding/Sparse ,00:11:02/00:00:00

(*, 227.5.5.5), 00:09:29/----, RP : 200.200.200.1
Incoming Interface : vlan200, RPF nbr : NULL, Route Flags : WR
Outgoing InterfaceList :
  vlan200, Forwarding/Sparse ,00:09:29/00:00:00