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 1.4
Release Date: 12/05/2019

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
## 1 Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/12/2018</td>
<td>1.0</td>
<td>Initial document.</td>
</tr>
<tr>
<td>10/05/2018</td>
<td>1.1</td>
<td>Updated ACL configuration details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added port splitting details.</td>
</tr>
<tr>
<td>02/20/2019</td>
<td>1.2</td>
<td>Added loop protection in System Configuration section and unknown Multicast Filtering in IGMP Snooping section.</td>
</tr>
<tr>
<td>03/06/2019</td>
<td>1.3</td>
<td>Updated for software release 1.1.0.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Section 3 Introduction to add terminal settings configuration and CLI grep option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added “show chassis info” command to Section 3 Introduction.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added TACACS accounting subsection under TACACS configuration section in Security section 15.</td>
</tr>
<tr>
<td>12/05/2019</td>
<td>1.4</td>
<td>Updated default unique password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added L2 ECMP load balancing details.</td>
</tr>
</tbody>
</table>
2 Contents

3 Introduction .................................................................................................................................................. 13

3.1 Command Line Interface ................................................................................................................................. 13
  3.1.1 Terminal Settings ........................................................................................................................................ 13
  3.1.2 Grep option ............................................................................................................................................... 14
  3.1.3 Console Port ............................................................................................................................................. 15

3.2 Blade Chassis .................................................................................................................................................... 16

4 System Configurations ........................................................................................................................................ 17

4.1 Management IP .................................................................................................................................................. 17
  4.1.1 Static Management IP Address .................................................................................................................. 17
  4.1.2 DHCP ....................................................................................................................................................... 17
  4.1.3 Default IP Gateway .................................................................................................................................... 18

4.2 Management Access ......................................................................................................................................... 19
  4.2.1 User login ............................................................................................................................................... 19
  4.2.2 Enable ...................................................................................................................................................... 20
  4.2.3 Enable Password ...................................................................................................................................... 21
  4.2.4 IP Authorized Manager ............................................................................................................................ 21

4.3 Interface Properties ......................................................................................................................................... 23
  4.3.1 Interfaces in SBM-25G-100 ....................................................................................................................... 23
  4.3.2 Interfaces in MBM-XEM-100 ..................................................................................................................... 24
  4.3.3 Description .............................................................................................................................................. 26
  4.3.4 Negotiation .............................................................................................................................................. 28
  4.3.5 Speed ....................................................................................................................................................... 31
  4.3.6 Duplex Operation .................................................................................................................................... 33
  4.3.7 MTU ......................................................................................................................................................... 33
  4.3.8 Flow control ............................................................................................................................................ 36
  4.3.9 Storm control ......................................................................................................................................... 38
  4.3.10 Forward Error Correction (FEC) Mode ................................................................................................... 39
  4.3.11 Port Splitting ......................................................................................................................................... 40

4.4 Time Management ......................................................................................................................................... 42
4.4.1 NTP server .................................................................42
4.4.2 Enable/Disable NTP .........................................................43
4.4.3 NTP authentication ...........................................................44
4.4.4 NTP broadcast .................................................................45
4.4.5 System clock .................................................................46
4.4.6 Timezone .................................................................46

4.5 System Management .............................................................48
4.5.1 Switch Name .................................................................48
4.5.2 Switch contact ...............................................................49
4.5.3 System location .............................................................50
4.5.4 System MTU .................................................................52
4.5.5 Static MAC .................................................................54
4.5.6 MAC aging .................................................................55

4.6 System Logging (Syslog) .........................................................56
4.6.1 Enable/Disable Syslog .......................................................57
4.6.2 Syslog server .................................................................58
4.6.3 Console Log .................................................................59
4.6.4 Log file .................................................................59
4.6.5 Logging Buffer ............................................................61
4.6.6 Facility .................................................................62
4.6.7 Trap .................................................................63
4.6.8 Clear Log buffer ............................................................65
4.6.9 Clear Log File .............................................................66

4.7 Configuration Management .....................................................66
4.7.1 Save Startup-Config ..........................................................66
4.7.2 Save Running Configuration To File .....................................67
4.7.3 Configuring Startup config file name .....................................68
4.7.4 Copy Startup-config .........................................................69
4.7.5 Copy file .................................................................69
4.7.6 Deleting Saved Configuration ..............................................70
4.7.7 Firmware upgrade ..........................................................70
4.7.8 Boot-up options ...........................................................71
4.7.9 Reset to Factory Defaults

4.8 Zero Touch Provisioning

4.8.1 ZTP Config Restore

4.8.2 ZTP Info

4.8.3 ZTP Firmware Upgrade

4.8.4 Disable ZTP

4.8.5 DHCP Vendor Class

4.9 Tracking Uplink Failure

4.10 Loop Protection

4.10.1 Defaults

4.10.2 Enable Loop Protection

4.10.3 Disable Loop Protection

5 VLAN

5.1 VLAN Basics

5.2 VLAN Support

5.3 VLAN Numbers

5.4 VLAN Defaults

5.5 Creating VLANs

5.6 Removing VLANs

5.7 VLAN Name

5.8 Port Based VLANs

5.8.1 Access Ports

5.8.2 Trunk Ports

5.8.3 Hybrid Ports

5.9 MAC Based VLANs

5.10 Protocol Based VLANs

5.11 Acceptable Frame Types

5.12 Ingress Filter

5.13 VLAN Configuration Example

5.14 Private Edge VLAN / Protected Ports

5.14.1 Unprotected Port

5.14.2 Protected Port
Spanning Tree Support

8.4.4 IPL Interface .............................................................................................................. 162
8.4.5 MLAG Port Channels .................................................................................................. 163
8.4.6 Other configurations ..................................................................................................... 163

9 Spanning Tree ......................................................................................................................... 165

9.1 Root Switch Election Procedure ....................................................................................... 166
9.2 Spanning Tree Support ........................................................................................................ 167
9.3 Spanning Tree Defaults ...................................................................................................... 167
9.4 Enabling/ Disabling Spanning Tree .................................................................................... 168

9.4.1 Enable / Disable Spanning Tree Globally ........................................................................ 168
9.4.2 Enable / Disable Spanning Tree on Ports ......................................................................... 168

9.5 Configuring MST .................................................................................................................. 170
9.6 Configuring MST region and instances .............................................................................. 171
9.7 Configuring RSTP ................................................................................................................ 172
9.8 Spanning Tree Compatibility .............................................................................................. 173
9.9 Configuring Root Switch (or) Priority ................................................................................. 174

9.10 Port Priority ....................................................................................................................... 175
9.11 Path Cost .......................................................................................................................... 177
9.12 Hello Time ...................................................................................................................... 179
9.13 Max Age .......................................................................................................................... 181
9.14 Forwarding Time ................................................................................................................ 182
9.15 Max Hops .......................................................................................................................... 183
9.16 Path Cost Long / Short ...................................................................................................... 184
9.17 Transmit Hold Count ......................................................................................................... 185
9.18 Root Guard ....................................................................................................................... 186
9.19 Topology Change Guard ................................................................................................. 187
9.20 Port Fast .......................................................................................................................... 189
9.21 Auto Edge ....................................................................................................................... 190
9.22 Link Type ........................................................................................................................ 191
9.23 Spanning Tree Configuration Examples ........................................................................... 193

10 IGMP Snooping ...................................................................................................................... 198
10.1 IGMP Snooping Support ................................................................. 199
10.2 Enabling IGMP Snooping ............................................................ 200
10.3 IGMP Version .............................................................................. 201
10.4 Multicast Router Ports ................................................................. 202
  10.4.1 Router Port Timeouts ............................................................ 202
  10.4.2 Static Router Ports .............................................................. 203
10.5 Leaving a Multicast Group .......................................................... 204
  10.5.1 Group Query Interval .......................................................... 204
  10.5.2 Group Query Retry Count .................................................... 205
  10.5.3 Immediate Leave ............................................................... 206
10.6 IGMP Snooping Querier ............................................................. 207
10.7 Report Forward ........................................................................... 209
10.8 Port Timeout (Port Purge Interval) .............................................. 210
10.9 Report Suppression Interval ....................................................... 211
10.10 Proxy Reporting ......................................................................... 212
10.11 Sending Queries when Topology Changes ................................. 213
10.12 Disabling IGMP Snooping .......................................................... 214
10.13 Unknown Multicast Filtering ....................................................... 215
10.14 IGMP Snooping Configuration Example .................................... 216
11 ACL .................................................................................................. 224
  11.1 Types of ACLs .......................................................................... 224
    11.1.1 MAC Extended ACL .......................................................... 225
    11.1.2 IP Standard ACL .............................................................. 225
    11.1.3 IP Extended ACL ............................................................. 225
  11.2 MAC Extended ACL ................................................................. 225
    11.2.1 Creating MAC Extended ACLs ........................................... 226
    11.2.2 Modifying MAC Extended ACLs ....................................... 228
    11.2.3 Removing MAC Extended ACLs ....................................... 228
    11.2.4 Applying MAC Extended ACLs to Interfaces .................... 229
    11.2.5 ACL Ingress Port Configuration ........................................ 229
    11.2.6 Displaying MAC Extended ACLs ...................................... 231
    11.2.7 MAC Extended ACL Configuration ................................... 232
11.3 IP Standard ACL ........................................................................................................................................ 233
  11.3.1 Creating IP Standard ACLs .................................................................................................................. 234
  11.3.2 Modifying IP Standard ACLs ................................................................................................................ 235
  11.3.3 Removing IP Standard ACLs .................................................................................................................. 236
  11.3.4 Applying IP ACLs to Interfaces ............................................................................................................. 236
  11.3.5 ACL Ingress Port Configuration ........................................................................................................... 236
  11.3.6 Displaying IP Standard ACLs ................................................................................................................ 238
  11.3.7 IP Standard ACL Configuration Example 1 ......................................................................................... 239
  11.3.8 IP Extended ACLs .................................................................................................................................. 240
  11.3.9 Creating IP Extended ACLs for IP Traffic ............................................................................................... 241
  11.3.10 Creating IP Extended ACLs for TCP Traffic ........................................................................................ 243
  11.3.11 Creating IP Extended ACLs for UDP Traffic ...................................................................................... 245
  11.3.12 Creating IP Extended ACLs for ICMP Traffic .................................................................................... 247
  11.3.13 Modifying IP Extended ACLs .............................................................................................................. 248
  11.3.14 Removing IP Extended ACLs .............................................................................................................. 249
  11.3.15 Applying IP Extended ACLs to Interfaces ......................................................................................... 249
  11.3.16 Displaying IP Extended ACLs .............................................................................................................. 249

11.4 IP Extended ACL Configuration Example 1 .............................................................................................. 252

12 QoS ................................................................................................................................................................. 254
  12.1 Policy-Based QoS ....................................................................................................................................... 256
    12.1.1 Classification and Marking .................................................................................................................. 256
  12.2 CoS-Based QoS .......................................................................................................................................... 257
    12.2.1 Egress Queuing ....................................................................................................................................... 257
    12.2.2 Scheduling ........................................................................................................................................... 258
    12.2.3 Default Priority ..................................................................................................................................... 258
    12.2.4 Bandwidth Management ..................................................................................................................... 259
  12.3 Port-Based Rate Limit .............................................................................................................................. 259
  12.4 HOL Blocking Prevention ........................................................................................................................ 259
  12.5 Enabling QoS .............................................................................................................................................. 259
  12.6 Configuring Policy-Based QoS .................................................................................................................. 260
  12.7 Configuring CoS-Based QoS ..................................................................................................................... 268

13 Port Mirroring .................................................................................................................................................. 275
13.1 Port Mirroring Defaults ........................................................................................................... 275
13.2 Configure Port Mirroring in CLI ............................................................................................. 275
14 SNMP ........................................................................................................................................ 278
14.1 SNMP Support ......................................................................................................................... 280
14.2 Interface Numbers .................................................................................................................... 280
14.3 SNMP Configuration .................................................................................................................. 281
   14.3.1 Configuration Steps ............................................................................................................ 282
14.4 SNMP Defaults .......................................................................................................................... 282
14.5 Enable/Disable the SNMP Agent ............................................................................................. 283
   14.5.1 Switch Name ...................................................................................................................... 284
   14.5.2 Switch Contact .................................................................................................................. 285
   14.5.3 System Location ................................................................................................................ 286
14.6 Access Control ........................................................................................................................ 288
   14.6.1 Engine Identifier ................................................................................................................ 288
   14.6.2 Community ....................................................................................................................... 289
   14.6.3 User .................................................................................................................................. 290
   14.6.4 Group ............................................................................................................................... 292
   14.6.5 View ................................................................................................................................ 294
   14.6.6 Group Access .................................................................................................................... 295
14.7 Trap .......................................................................................................................................... 298
   14.7.1 Target Address ................................................................................................................... 298
   14.7.2 Target Parameters .............................................................................................................. 300
   14.7.3 SNMP Notify ..................................................................................................................... 300
   14.7.4 Trap UDP Port .................................................................................................................... 301
   14.7.5 Authentication Traps .......................................................................................................... 303
   14.7.6 Link-State Trap ................................................................................................................ 304
14.8 SNMP Configuration Example ............................................................................................... 307
15 RMON ......................................................................................................................................... 315
15.1 RMON Groups ......................................................................................................................... 317
   15.1.1 Alarm group ...................................................................................................................... 317
   15.1.2 Event Group ...................................................................................................................... 318
   15.1.3 Statistics ........................................................................................................................... 318
15.2 RMON Configuration........................................................................................................................................318
  15.2.1 Enabling RMON ........................................................................................................................................318
  15.2.2 Configuring Alarms and Events ..................................................................................................................319
  15.2.3 Configuring Statistics .................................................................................................................................321
  15.2.4 RMON Configuration Example ..................................................................................................................322
  15.2.5 Configuring Port Rate Limit .......................................................................................................................328
  15.2.6 Configuring HOL Blocking Prevention ....................................................................................................329
16 Security................................................................................................................................................................332
  16.1 Login Authentication Mode ............................................................................................................................332
  16.2 RADIUS .........................................................................................................................................................333
    16.2.1 RADIUS Server ......................................................................................................................................334
  16.3 TACACS .........................................................................................................................................................335
    16.3.1 TACACS Server.......................................................................................................................................336
    16.3.2 TACACS Re-tries.....................................................................................................................................337
    16.3.3 TACACS use-server .................................................................................................................................338
    16.3.4 TACACS Login Authentication Mode .....................................................................................................339
    16.3.5 TACACS Authorization Status ................................................................................................................342
    16.3.6 TACACS Accounting ..............................................................................................................................343
    16.3.7 TACACS Privilege ..................................................................................................................................344
  16.4 SSH ...............................................................................................................................................................345
  16.5 SSL ...............................................................................................................................................................347
    16.5.1 Secure HTTP (https) ..............................................................................................................................347
    16.5.2 Certificate Signing Request (CSR) ........................................................................................................348
    16.5.3 SSL Certificate ......................................................................................................................................350
17 LLDP................................................................................................................................................................352
  17.1.1 Enabling LLDP ..........................................................................................................................................353
  17.1.2 Configuring LLDP Parameters ..................................................................................................................353
  17.1.3 Configuring LLDP Timers ..........................................................................................................................359
  17.1.4 LLDP Configuration ..................................................................................................................................362
3 Introduction
This document explains the configuration for Supermicro switch models SBM-25G-100 and MBM-XEM-100.

The switch SBM-25G-100 and MBM-XEM-100 supports standard layer 2 features.

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 mainly used the command line interface to explain the switch configurations.

3.1 Command Line Interface

The Supermicro Switch command line interface is accessible through an RS232 console port, or via Telnet and SSH connections.

The Supermicro Switch CLI is designed to follow industry standard CLI commands. Standard features including context sensitive “help” and auto-completion-on-tab-key are supported.

After logging in to the switch CLI, you are automatically 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`.

The command prompt always displays the current mode.

- CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the SMIS CLI. For Example: commands like "show ip interface" can be typed as "sh ip int".
- CLI commands are case insensitive.
- CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. Appropriate error messages will be displayed if the dependencies are not satisfied

3.1.1 Terminal Settings
The command line interface displays the output based on default terminal size settings. The default terminal width is 80 characters and length is 25 lines.

Follow the steps below to adjust the terminal display settings.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>

Page 13 of 371
<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Enters the configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>terminal width &lt;characters&gt;</td>
<td>Configures the width of the terminal in characters. &lt;br&gt;characters – Any number between 20 to 512.</td>
</tr>
<tr>
<td>Step 3</td>
<td>terminal length &lt;lines&gt;</td>
<td>Configures the height of the terminal in lines. &lt;br&gt;lines – Any number between 0 to 1024. &lt;br&gt;If length is given as 0, it disables pagination on the output. In this case all the lines will be displayed without page break options.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show terminal</td>
<td>Displays current terminal settings</td>
</tr>
<tr>
<td>Step 5</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

The terminal settings are session based. Terminal settings changed in one CLI session is not effective for other CLI sessions.

On launching of every SSH/telnet session, user need to configure terminal settings if default settings are not desired.

Terminal settings are not saved or restored after switch reloads.

### 3.1.2 Grep option

The CLI command output can be search for desire strings using “grep” option.

CLI commands accept “grep” as a filter option after pipe (|) symbol.

The “grep” search strings need to be given within quotes (”) if space characters used in the search pattern or OR (|) operator used.
The example use cases:

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMIS# show system information</td>
<td>grep &quot;Restore Status&quot;</td>
</tr>
<tr>
<td>Config Restore Status</td>
<td>Successful</td>
</tr>
<tr>
<td>Config Restore Option</td>
<td>Restore</td>
</tr>
<tr>
<td>Config Restore ZTP Filename</td>
<td></td>
</tr>
<tr>
<td>Config Restore ZTP TFTP IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Config Restore Local Filename</td>
<td>iss.conf</td>
</tr>
<tr>
<td>SMIS#</td>
<td></td>
</tr>
</tbody>
</table>

3.1.3 Console Port

SBM-25G-100 and MBM-XEM-100 have a 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**: 9500
- **Data**: 8 bit
- **Parity**: none
- **Stop**: 1 bit
- **Flow Control**: none

### 3.2 Blade Chassis

SBM-25G-100 and MBM-XEM-100 are blade switch modules. These switches can be configured for initial management access from Chassis Management Module (CMM) interface.

Refer the CMM configuration guide for setting switch management IP from CMM interface.

Switch can display the information about currently active CMM and also some basic information about the blade enclosure details along with switch slot number.

The command “show chassis info” displays the above details as shown below.

```
SMIS# show chassis info

CMM Network Info:
   Network mode : Dynamic
   IP Address   : 172.18.0.87
   IP Netmask   : 255.255.255.0
   IP Gateway   : 172.18.0.254
   MAC Address  : 0C:C4:7A:5B:AA:C6

Midplane:
   Model       : BPN-SB-J610
   Enclosure ID : GB182S000283

Switch:
   Model       : SBM-25G-100
   Slot        : B2

SMIS#
```
4 System Configurations

4.1 Management IP
SBM-25G-100 and MBM-XEM-100 switches come up with DHCP IP settings for default management IP.

4.1.1 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 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>Configure the management interface IP address manually.</td>
</tr>
<tr>
<td></td>
<td>/prefix-length] [&lt;subnet-mask&gt;]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip-address – A valid IPv4 Address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip-address/prefix-length - A valid IPv4 Address with a prefix length of value 1-32.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subnet-mask – A valid IP subnet mask.</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 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 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 management interface IP address manually.

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

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

DHCP is the default management IP address mode.
Follow the steps below to obtain 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>
<tr>
<td>Step 2</td>
<td>ip address dhcp</td>
<td>Configures the management interface IP address through 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 interface</td>
<td>Displays the Management interface IP configuration.</td>
</tr>
</tbody>
</table>

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

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

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

SMIS# configure terminal

SMIS(config)# ip address dhcp

SMIS(config)# end

4.1.3 Default IP Gateway

To configure default gateway in blade switches 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>
<tr>
<td>Step 2</td>
<td>ip gateway &lt;ip-address&gt;</td>
<td>Configure IP gateway.</td>
</tr>
</tbody>
</table>

   `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 IP Gateway.

SMIS# configure terminal

SMIS(config)# ip gateway 10.1.1.1
4.2 Management Access
Supermicro switches enable access control of the switch by various mechanisms:

- User name and 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>Default Password for ADMIN</td>
<td>Default password is unique for each switch and it can be found on the label stuck on the switch. Note: Use the password ADMIN for older hardware shipped before 01/01/2020.</td>
</tr>
<tr>
<td>Default 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>

4.2.1 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 Username.

<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 | `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.

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

<table>
<thead>
<tr>
<th>Line</th>
<th>User</th>
<th>Peer-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 con</td>
<td>user1</td>
<td>Local Peer</td>
</tr>
</tbody>
</table>

### 4.2.2 Enable

Supermicro switches provide support for configuring access to various CLI commands. This is achieved by `Enable` password and `privilege levels`. 15 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>*Enable Level – Specify 1-15, any of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 commands used to enable a particular privilege level.

```
SMIS# enable15
```
4.2.3 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>
</tbody>
</table>
| Step 2 | enable password [level (1-15)] <LINE ‘enable' password> | Configure password for a particular privilege level.  
  
  *Level* – Specify 1-15, any of the privilege levels  
  
  *LINE enable password* – Alphanumeric |
| Step 3 | End | Exits the configuration mode |

The `enable password` configuration is saved automatically as part of start-up config. Enable password configurations are not displayed in ‘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
```

4.2.4 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>
</tbody>
</table>
| Step 2 | authorized-manager ip-source <ip-address>[(<subnet-mask> | / <prefix-length(1-32)>)] [interface [<interface-type <0/a-b, 0/c, ...>] [<interface-type <0/a-b, 0/c, ...>]] [vlan<a,b or a-b or a,b,c,d>] [service [snmp] [telnet] [http] [http | Configure the authorized manager  
  
  *ip-address* – Manager IP address  
  
  *subnet mask* – For a given Authorized Manager entry, the switch applies the subnet mask to the IP address to |
If IP Authorized Managers are configured in Supermicro switch, access to switch via telnet, ssh, etc is possible only by those hosts allowed to access. Other hosts will not be permitted access to switch.

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)# authorize-manager ip-source 200.200.200.10 service telnet
SMIS(config)# authorize-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

4.3 Interface Properties
Supermicro switches support various types of interfaces – physical interfaces, port channel interfaces. Each interface has different characteristics some of them are configurable.

4.3.1 Interfaces in SBM-25G-100

Fx-ethernet Ports
The SBM-25G-100 has 28 Fx ports and they operate at 25G speed by default. Also these Fx ports support 10G and 1G speeds. Fx-ethernet ports are internal ports and manual speed configuration is not supported.

Cx-ethernet Ports
The SBM-25G-100 has four 100G capable Cx ports by default. The Cx ports can also operate at 40G speed. Additionally, each Cx ports 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>Gi</td>
<td>1</td>
<td>1G</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Fx</td>
<td>1 – 28</td>
<td>25G default</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can operate in 10G/1G</td>
<td></td>
</tr>
<tr>
<td>Cx</td>
<td>1 – 4</td>
<td>100G default</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can operate in 40G Or can be split into 4 ports</td>
<td></td>
</tr>
<tr>
<td>Fx</td>
<td>29 – 31</td>
<td>25G / 10G</td>
<td>When Cx 0/1 splitted – it becomes Cx 0/1, Fx 29, Fx 30 and Fx 31</td>
</tr>
<tr>
<td>Fx</td>
<td>32 – 34</td>
<td>25G / 10G</td>
<td>When Cx 0/2 splitted – it becomes Cx 0/2, Fx 32, Fx 33 and Fx 34</td>
</tr>
<tr>
<td>Fx</td>
<td>35 – 37</td>
<td>25G / 10G</td>
<td>When Cx 0/3 splitted – it becomes Cx 0/3, Fx 35, Fx 36 and Fx 37</td>
</tr>
</tbody>
</table>
### 4.3.2 Interfaces in MBM-XEM-100

#### Fx-ethernet Ports

The MBM-XEM-100 has 56 Fx ports and they operate at 10G speed by default. Also these Fx ports support 1G speeds. Fx-ethernet ports are internal ports and manual speed configuration is not supported.

#### Cx-ethernet Ports

The SBM-25G-100 has four 100G capable Cx ports by default. The Cx ports can also operate at 40G speed.

Additionally, each Cx ports can be split in to 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>Gi</td>
<td>1</td>
<td>1G</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Fx</td>
<td>1 – 56</td>
<td>25G default</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can operate in 10G/1G</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Cx</td>
<td>1 – 4</td>
<td>100G default</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can operate in 40G</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or can be split into 4 ports</td>
<td>Default Physical interfaces</td>
</tr>
<tr>
<td>Fx</td>
<td>57 – 59</td>
<td>25G / 10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>When Cx 0/1 splitted – it becomes Cx 0/1, Fx 57, Fx 58 and Fx 59</td>
<td></td>
</tr>
<tr>
<td>Fx</td>
<td>60 – 62</td>
<td>25G / 10G</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>When Cx 0/2 splitted – it becomes Cx 0/2, Fx 60, Fx 61 and Fx 62</td>
<td></td>
</tr>
<tr>
<td>Fx</td>
<td>63 – 65</td>
<td>25G / 10G</td>
<td>When Cx 0/3 splitted – it becomes Cx 0/3, Fx 63, Fx 64 and Fx 65</td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>-----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Fx</td>
<td>66 – 68</td>
<td>25G / 10G</td>
<td>When Cx 0/4 splitted – it becomes Cx 0/4, Fx 66, Fx 67 and Fx 68</td>
</tr>
</tbody>
</table>
### Parameter Default Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>1500 bytes</td>
</tr>
</tbody>
</table>
| Speed              | Fx ports FX 0/1 to 0/56 – 10 Gbps  
                  | Cx ports CX 0/1 to 0/4 – 100 Gbps  
                  | Gi port Gi 0/1 – 1 Gbps          |
| Negotiation        | Enabled       |
| Storm-control      | Disabled      |
| Description        | None          |
| Duplex Operation   | Full          |
| Flow Control       | Off           |
| FEC Mode           | Enabled for Cx-ethernet ports.  
                  | Disabled for Cx-ethernet ports. |

#### 4.3.3 Description

Supermicro switches allow user to configure a description string to the interfaces. This descriptive 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>
</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  

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 | description <string> | Configure the interface description
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>String – alphanumeric characters of length 1-64.</td>
</tr>
</tbody>
</table>

Step 4 | End | Exits the configuration mode.

Step 5 | show interface description | Displays the interface description 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 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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/2</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/3</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/4</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/5</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/6</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/7</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/8</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/9</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/10</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/11</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/12</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Fx0/13</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
</tbody>
</table>
```
Fx0/14 up down
Fx0/15 up down
Fx0/16 up down
Fx0/17 up down
Fx0/18 up down
Fx0/19 up down
Fx0/20 up down
Fx0/21 up down
Fx0/22 up down Server_Cluster_0100
Fx0/23 up down
Fx0/24 up down
Fx0/25 up down
Fx0/26 up down
Fx0/27 up down
Fx0/28 up down
Cx0/1 up down
Cx0/2 up down
Cx0/3 up down
Cx0/4 up down
Cx0/5 up down
Cx0/6 up down
po1 up down
po6 up down

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

Auto negotiation is disabled by default for all the ports. It can be enabled for 100G CX ports.

Follow the steps below to configure Interface Negotiation.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>

Page 28 of 371
<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Enters the configuration mode</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td></td>
<td></td>
<td><code>interface-type</code> – may be any of the following: cx-ethernet</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>interface-id</code> 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.: <code>int range cx 0/1-2</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: <code>int range cx 0/1-2, cx 0/3</code></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>
</tbody>
</table>
Fx0/27 not connected Full 25 Gbps Auto
Fx0/28 not connected Full 25 Gbps Auto
Gi0/1 not connected Full 1 Gbps Auto
Cx0/1 not connected Full 100 Gbps Auto
Cx0/2 not connected Full 100 Gbps No-Negotiation
Cx0/3 not connected Full 100 Gbps Auto
Cx0/4 not connected Full 100 Gbps Auto

4.3.5 Speed

Interface speed can be configured only on external interfaces when auto negotiation is disabled.

Speed cannot be set manually on internal Fx-ethernet ports; but Fx-ethernet ports can auto-negotiate to operate at speed 25G, 10G & 1G in SBM-25G-100 models and 10G &1G in MBM-XEM-100 models.

100G Cx-ethernet ports can be configured to operate in speed 100G and 40G. FEC and negotiation has to be disabled before setting the Cx-ethernet ports to 40G.

Follow the steps below to configure 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>
</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  
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 |
The example below shows the commands used to configure Interface Speed.

```
SMIS# configure terminal
SMIS(config)# interface cx 0/2
SMIS(config)# no fec-mode
SMIS(config)# no negotiation
SMIS(config-if)# speed 40000
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>
</tbody>
</table>

The “no speed” command restores the default interface speed.
Fx0/11  not connected  Full  25 Gbps  Auto
Fx0/12  not connected  Full  25 Gbps  Auto
Fx0/13  not connected  Full  25 Gbps  Auto
Fx0/14  not connected  Full  25 Gbps  Auto
Fx0/15  not connected  Full  25 Gbps  Auto
Fx0/16  not connected  Full  25 Gbps  Auto
Fx0/17  not connected  Full  25 Gbps  Auto
Fx0/18  not connected  Full  25 Gbps  Auto
Fx0/19  not connected  Full  25 Gbps  Auto
Fx0/20  not connected  Full  25 Gbps  Auto
Fx0/21  not connected  Full  25 Gbps  Auto
Fx0/22  not connected  Full  25 Gbps  Auto
Fx0/23  not connected  Full  25 Gbps  Auto
Fx0/24  not connected  Full  25 Gbps  Auto
Fx0/25  not connected  Full  25 Gbps  Auto
Fx0/26  not connected  Full  25 Gbps  Auto
Fx0/27  not connected  Full  25 Gbps  Auto
Fx0/28  not connected  Full  25 Gbps  Auto
Gi0/1   not connected  Full  1 Gbps   Auto
Cx0/1   not connected  Full  100 Gbps  Auto
Cx0/2   not connected  Full  40 Gbps   No-Negotiation
Cx0/3   not connected  Full  100 Gbps  Auto
Cx0/4   not connected  Full  100 Gbps  Auto

4.3.6 Duplex Operation
Supermicro switch doesn’t support Half-Duplex operation on its physical interfaces.

4.3.7 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 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  
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 MTU for all the interfaces, “system mtu” command can be used.

The example below shows the commands used to configure 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 00:25:90:80:81:98

MTU 1500 bytes, Full duplex, 10 Gbps, No-Negotiation

HOL Block Prevention enabled.

Input flow-control is off, output flow-control is off

Link Up/Down Trap is enabled

Reception Counters

<table>
<thead>
<tr>
<th>Counter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>0</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Unicast Packets Rate</td>
<td>0/Sec</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast Packets Rate</td>
<td>0/Sec</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>Multicast Packets Rate</td>
<td>0/Sec</td>
</tr>
<tr>
<td>Overall Packets Rate</td>
<td>0/Sec</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

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
Overall Packets Rate : 0/Sec
Pause Frames : 0
Discarded Packets : 0
Error Packets : 0

SMIS(config-if)

# show interface mtu fx-ethernet 0/22

Fx0/22  MTU size is 9000

4.3.8 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 the other port 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, which prevents 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. interface-type – may be any of the following: fx-ethernet – fx cx-ethernte – cx</td>
</tr>
</tbody>
</table>
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 | 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 |

<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 flow-control [ interface &lt;interface-type&gt;&lt;interface-id&gt;]</td>
<td>Displays the Interface Flow 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 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

<table>
<thead>
<tr>
<th>Port</th>
<th>TxFlowControl</th>
<th>Rx FlowControl</th>
<th>Tx Pause</th>
<th>Rx Pause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/22</td>
<td>on</td>
<td>off</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
### 4.3.9 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 in mistakes in network configurations etc. LAN storm degrades 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 and then resumes 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>
</tbody>
</table>
| Step 2 | interface `<interface-type>`<interface-id>` | 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 | storm-control { broadcast | multicast | dlf } level `<kbps (1-10000000)>` | Configure Storm control for broadcast or multicast or DLF packets.  
Level – Threshold level in kbps, in range 1-10000000. |
| Step 4 | End | Exits the configuration mode. |
| Step 5 | show interfaces storm-control | Displays the interface Storm control configuration. |
Step 6 | write startup-config   | Optional step – saves this configuration to be part of startup configuration.

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

4.3.10 Forward Error Correction (FEC) Mode
Supermicro switches allow user to enable FEC mode on the interfaces. FEC mode would be useful in noisy link where a errors in transmission cause retransmission.

Follow the steps below to enable FEC mode on 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:
- 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 FEC.

```
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
```

### 4.3.11 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.

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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type – may be any of the following:</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 cx 0/1-4

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.

| Step 3 | speed 25000  
Or  
speed 10000 | Splits the port into four 25G ports or four 10G ports.  
Note: Fec-mode and negotiation have to be turned off for splitting into 4 x 10G ports. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interface status</td>
</tr>
<tr>
<td>Step 6</td>
<td>write startup-config</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 29, Fx 30 and Fx 31 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 29, Fx 30 and Fx 31 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

4.4 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 a NTP client over UDP and receives its time from a NTP server in the network. The time

<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>
<tr>
<td>NTP authentication</td>
<td>None</td>
</tr>
<tr>
<td>NTP server</td>
<td>None</td>
</tr>
<tr>
<td>NTP Broadcast mode</td>
<td>No</td>
</tr>
</tbody>
</table>

4.4.1 NTP server
Supermicro switches can synchronize time with a 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>
<tr>
<td>Step 2</td>
<td>ntp server &lt;ip_address&gt; [key (1-65535)] [prefer]</td>
<td>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.</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 “enable agent” command enables the agent. NTP servers can be deleted only when NTP status is disabled.

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

The example below shows the commands used to configure 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

4.4.2 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 1 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>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

4.4.3 NTP authentication
Supermicro switches support NTP authentication by the NTP server. The authentication data is encrypted by MD5 algorithm. The NTP authentication key can be configured in the switch and this must be matched with the NTP authentication key in NTP server. The authentication key is a 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>
</tbody>
</table>

**Key-number** – key number in the range 1-65535, used for MD5.

**Key-text** – NTP key text to be used along with key-number for MD5.

| 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 "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
4.4.4 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 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>
</tbody>
</table>
| Step 2 | ntp broadcast [authentication] | Configure NTP broadcast. 

*authentication* – If specified, NTP authentication is enabled for broadcast mode. |
| 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 “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] ntp running broadcast mode

Server Key Prefer

Key # Key

Time zone offset not set
Time zone offset not set

### 4.4.5 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.  
  
  `hh:mm:ss` – Time in Hours:Minutes:Seconds format.  
  
  `day` – Day in 1-31 format.  
  
  `month` – Month in January-December format.  
  
  `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
Wed Aug 31 09:26:15 2013
SMIS# show clock
Wed Aug 31 09:26:20 2013
```

### 4.4.6 Timezone

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 timezone.

<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| `tz posix <std><offset>[<dst>]` | Configure the timezone.  
  
  `<std>` - Standard time text e.g. PST |
<offset> - Time zone offset in 
[+-]hh[ :mm[ :ss]] format. This is 
the value needed to be added to local 
time to get to UST. This value is positive 
if the local time zone is in west of the 
Prime Meridian, otherwise it is negative.

<dst> - Day light savings time text e.g. 
PDT

<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 system information</td>
<td>Displays the timezone 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 example below shows the commands used to configure the timezone 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
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 48 mins 5 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>
</table>

<table>
<thead>
<tr>
<th>Key #</th>
<th>Key</th>
</tr>
</thead>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.5 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>

4.5.1 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><em>Devname-- Switch name specified as 1-15 alphanumeric characters.</em></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 Switch Name.

```plaintext
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
```

### 4.5.2 Switch contact

Supermicro switches provide option to configure the Switch in charge Contact details, usually an email Id.

Follow the steps below to configure 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 256.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode</td>
</tr>
</tbody>
</table>
Step 4 | show system information | Displays the System information configuration.
---|---|---
Step 5 | write startup-config | Optional step – saves this configuration to be part of startup configuration.

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

The example below shows the commands used to configure 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
```

4.5.3 System Location
Supermicro switches provide 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>Configure System Location. Location name – Location of the switch specified as a string of maximum size 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 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 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
Device Up Time : 0 days 0 hrs 51 mins 39 secs
Boot-up Flash Area : Normal
NTP Broadcast Mode : No

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

Follow the steps below to configure 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>
<tr>
<td>Step 2</td>
<td>system mtu &lt;frame-size(1500-9216)&gt;</td>
<td>Configure System MTU. frame-size – Specify MTU of frame in range 1500-9216.</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show interface mtu</td>
<td>Displays the interface MTU.</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 system mtu” command resets the system MTU to its default value of 1500 bytes.

The example below shows the commands used to configure 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
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#

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

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 address 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 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 [interface-type:&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>mac-address-table static unicast <a href="">aa:aa:aa:aa:aa:aa</a> vlan &lt;vlan-id(1-4069)&gt; interface &lt;interface-type&gt;</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>
</tr>
<tr>
<td></td>
<td></td>
<td>Interface - specify the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels.</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.

**Step 3**
End

Exits the configuration mode.

**Step 4**
show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa>] [interface <interface-type>=<interface-id>]

show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa>] [interface <interface-type>=<interface-id>]

Displays the static MAC configuration.

**Step 5**
write startup-config

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

The "no mac-address-table static multicast <aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type>=<interface-id>]

and no mac-address-table static unicast <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> [recv-port <interface-type>=<interface-id>]"

command deletes the particular static multicast MAC entry.

The example below shows the commands used to configure 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

### 4.5.6 MAC aging

Dynamic MAC address table entries are addresses learnt by the switch and they age when they are not in use. The MAC aging time can be configured by user.
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 the 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
```

4.6 System Logging (Syslog)

Supermicro switches send system messages output to a Logging process and this is called System Message Logging (Syslog). Logging can be done at various locations:

- Console
- File
- Server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog status</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
### Logging buffer size
- **50 entries**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<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>

### 4.6.1 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><code>logging disable</code></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><code>show logging</code></td>
<td>Displays the Syslog configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>write startup-config</code></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
```
4.6.2 Syslog server

In Supermicro switches, Syslog messages can be re-directed to a Syslog server.

Follow the steps below to configure 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ip-address –IP address of Syslog server</em></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 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)
```
**4.6.3 Console Log**

System Logging messages can be displayed in switch console.

Follow the steps below to enable 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)
```

**4.6.4 Log file**

System Logging messages can be stored as a Log file in 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>
</table>

LogFile(0 Entries)
### SBM-25G-100 / MBM-XEM-100 Configuration Guide

#### Step 1
configure terminal

Enters the configuration mode

#### Step 2
logging file <filename> max-entries <short (1-8000)>

Enable storing Logs in a File.

*Filename* – Specify file name of upto 32 characters.

*Short*– Specify entries that can stored in file in range 1-8000.

#### 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 file” command disables logging of system message in File.

---

The example below shows the commands used to enable storing Logs in a File.

```plaintext
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)
```
4.6.5 Logging Buffer

The log messages are stored in a circular internal buffer, in which older messages are overwritten once the buffer is full. Syslog buffer size is configurable in Supermicro switches.

Follow the steps below to configure 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
<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 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)

4.6.6 Facility
Syslog Facility provides approximate details regarding which part of the system the Syslog message originated from.

Follow the steps below to configure 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 “no logging facility” command resets the logging Facility to its default value of Local0.

The example below shows the commands used to configure 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)

4.6.7 Trap
Supermicro switches provide 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>
<tr>
<td>Step 2</td>
<td>logging trap [{ &lt;level (0-7)&gt;</td>
<td>alerts</td>
</tr>
</tbody>
</table>

There are various levels of trap 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.

<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 trap” command resets the 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:DHCP-7:Exitting DHPC Task Ini
<135> Apr 29 10:11:05 2013:DHCP-7:Entered in DhcpCIntSelectTaskMain fn
<135> Apr 29 10:11:05 2013:DHCP-7:Entered in DhcpCSocketOpen fn
The Syslog buffer can be cleared to enable fresh logging of messages.

Follow the steps below to Clear Logging 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>
<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 Logging 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)
```
### 4.6.9 Clear Log File

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

Follow the steps below to Clear Logging 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 Logging 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)
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)
```

### 4.7 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.

#### 4.7.1 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.
### 4.7.2 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 existing switch configuration to a file.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>`write { flash:filename</td>
<td>tftp://ip-address/filename}`</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>show stored-config&lt;filename&gt;</code></td>
<td>Displays the stored configuration file from local flash memory. filename – name of the configuration file.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to write 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 ...
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
set ip igmp enable
set ip pim enable
ip pim component 1
exit

4.7.3 Configuring Startup config file name

Supermicro switches provide 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 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>
<tr>
<td>Step 4</td>
<td>show startup-config</td>
<td>Displays the configured startup configuration file contents.</td>
</tr>
</tbody>
</table>

The example below shows the commands used to configure 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

4.7.4 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 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>tftp://ip-address/filename}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filename – name of the configuration file.</td>
</tr>
</tbody>
</table>

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

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

4.7.5 Copy file
The copy command helps copying the configuration files from flash memory to remote TFTP server and vice versa. This command can be used to copy files in the local flash memory also.

Follow the steps below to Copy a file to another file in remote site/flash.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>copy flash: filenametftp://ipaddress/filename</code></td>
<td>Copies a local flash file to remote TFTP server.</td>
</tr>
<tr>
<td></td>
<td><code>copy tftp://ip-address/filename flash: filename</code></td>
<td>Copies a remote file to local flash.</td>
</tr>
<tr>
<td></td>
<td><code>copy flash: filename flash: filename</code></td>
<td>Makes a copy of the file in the flash memory. filename – name of the configuration file.</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
4.7.6 Deleting Saved Configuration
Supermicro switches allow deletion of switch startup configuration and other stored configuration files.

Follow the steps below to delete the startup-config 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>
<tr>
<td></td>
<td>filename – name of the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

The example below shows the commands used to erase startup-config or a 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#

4.7.7 Firmware upgrade
Supermicro Switches support dual firmware images. The default firmware image is referred as “normal” and the backup firmware image is referred as “fallback” image.

The “firmware upgrade” command helps updating both the normal and fallback image.

Follow the steps below to update firmware image:

<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} [normal</td>
<td>fallback]</td>
</tr>
</tbody>
</table>
The example below shows the commands used to configure Firmware Upgrade.

SMIS# firmware upgrade tftp://100.100.100.1/SWITCH_FIRMWARE_1.0.15.bin normal

---

By default switch boots using normal firmware image. To boot up using fallback firmware image use the command “set boot-up {normal | fallback}”.

---

### 4.7.8 Boot-up options

Supermicro Switches support dual firmware images as normal and fallback. The switch boots up from normal firmware image by default. User can configure the switch to boot from fallback firmware image.

Follow the steps below to configure 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 startup-config file.

---

The example below shows the commands used to configure 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>

Time zone offset not set

4.7.9 Reset to Factory Defaults
Supermicro switches can be reset to factory defaults using a CLI command.

Follow the steps below to reset to 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 the stored configurations, files on the flash memory, user accounts and management IP address.

After resetting to factory defaults, the switch can be managed from serial console with default administrator user ID ADMIN and default password. Default password for the switches shipped after 01/01/2020 will be unique and can be found on a label stuck on the switch. For the switches shipped before 01/01/2020 the default password is ADMIN.

The example below shows the command to reset to factory defaults.
SMIS(config)# reset-to_factory_defaults
This command will reset settings to factory defaults.
After resetting to factory defaults, switch will be reloaded immediately.
Do you really want to execute this command and reload the switch? [y/n]

4.8 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.

SBM-25G-100/MBM-XEM-100 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.

4.8.1 ZTP Config Restore

This section explains details about using ZTP for automatically configuring the Supermicro switches.

4.8.1.1 DHCP Server Configuration

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

1. Configuration File Name
2. TFTP Server IP Address

Configuration File Name

Configuration File Name is sent to switches from DHCP server using vendor specific option 43 in sub option 01.

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

TFTP server IP Address

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

TFTP Server IP Address is sent to switches from DHCP server using standard DHCP option 66, `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 added to dhcpd.conf as shown in the below example.

The lines in **bold** are newly required, other lines are shown for clarity.

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

Page 73 of 371
4.8.1.2  Switch Configuration Restore

ZTP configuration restore feature is enabled in Supermicro switches by default. And 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 below diagram shows how switch restores the configuration in ZTP and non-ZTP cases.
Switch Boots up

Static IP

Is Static or DHCP IP

Got

No

Restore Local Config. If no local config, factory defaults

Failed

Download Config File?

Success

ZTP config restore failed.

Restore ZTP config file.
4.8.2 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 download. If ZTP restore is not applied, this field will be empty.

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

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

4.8.3 ZTP Firmware Upgrade

This section explains details about using ZTP for automatically upgrading firmware on Supermicro switches.

4.8.3.1 DHCP Server Configuration

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

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

**Firmware Image File Name**

Firmware Image Name is sent to switches from DHCP server using vendor specific option 43 in sub option 04.

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

**TFTP server IP Address**

The configuration file needs to be available in a TFTP server for switch to download.
TFTP Server IP Address is sent to switches from 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 \texttt{dhcpd.conf} as shown in the below example.

The lines in \textbf{bold} are newly required, other lines are shown for clarity.

\texttt{# Need to add the below lines to define option 43.1 for Supermicro Blade switches}

\begin{verbatim}
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;

# network for Supermicro blade 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
    option smc-op.config-file-name "smcBladeSwitch.conf";

    option tftp-server-name "172.31.43.59";

    option smc-op.fw-img-file-name "SBM-MBM-100-fw-1.0.2.2.img";

}
\end{verbatim}

\textbf{4.8.3.2 Switch Firmware Upgrade}

ZTP firmware upgrade feature is enabled in Supermicro switches by default. And the default management IP address configuration is DHCP mode. Hence when switches boot up with DHCP, it gets the firmware image file and checks upgrade needed or not.

The below diagram shows how switch upgrades firmware in ZTP.
4.8.4 Disable ZTP
If any customer prefers not to use ZTP and likes to disable ZTP for any reason, it can be done. When ZTP is disabled, switch always loads the local configuration file, if no local configuration file available, switch comes up with default configuration. Similarly when ZTP is disabled, 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 web interface in “system settings” page in “system management” group.

4.8.5 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 MBM-XEM-100 switch advertise the vendor class as “MBM-XEM-100”. The SBM-25G-100 series blade switches advertise the vendor class as “SBM-25G-100”.

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

The below example DHCP server configuration uses vendor class information to send ZTP options for Supermicro switch SBM-25G-100.

```plaintext
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" "SBM-25G-100" {
    option smc-op.config-file-name "iss-11.conf";
    option smc-op.fw-img-file-name "SBM-MBM-100-fw-1.0.2.2.img";
    option tftp-server-name "172.31.33.5";
  }
}
```
## 4.9 Tracking Uplink Failure

The Uplink Failure Tracking Feature (ULFT) is useful for blade switches. This helps blade servers to move to downstream Ethernet ports in case any blade 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.
4.10  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.

4.10.1  Defaults

Loop Protection feature is disabled by default.

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

4.10.3  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><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
**Step 2**  
*interface <ifname> <ifid>*  
Enter the interface configuration mode

**Step 3**  
*no loop-protect*  
Disabling the loop protection feature on this interface

**Step 4**  
*End*  
Exits the configuration mode.

**Step 5**  
*show loop protection*  
Displays the loop protection configuration.

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

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><em>configure terminal</em></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td><em>loop-protect disable</em></td>
<td>Disabling the loop protection feature globally</td>
</tr>
<tr>
<td>Step 4</td>
<td><em>End</em></td>
<td>Exits the configuration mode</td>
</tr>
<tr>
<td>Step 5</td>
<td><em>show loop protection</em></td>
<td>Displays the loop protection configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td><em>write startup-config</em></td>
<td>Optional step – saves this configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
5 VLAN

5.1 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 flood 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”.

5.2 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 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, switch checks the received port is member of this identifier VLAN. If the received is not member of the identified VLAN, the packet is dropped. If the received port is 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?
  - Yes: VLAN ID != 0?
    - Yes: Use VLAN ID from VLAN tag
    - No: Use MAC VLAN ID
  - No: Found Src MAC in MAC VLAN?
    - Yes: Use MAC VLAN ID
    - No: Found Proto VLAN?
      - Yes: Use Protocol VLAN ID
      - No: Is Access Port?
        - Yes: Use Access VLAN ID
        - No: Is Trunk Port?
          - Yes: Use Trunk Native VLAN ID
          - No: Is Hybrid Port?
            - Yes: Use PVID as VLAN ID
            - No: Found VLAN
5.3 VLAN Numbers

This switch model supports 4K static VLANs.

This switch model supports 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.

This switch model 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. Same protocol group can be associated with different VLAN in different port.

5.4 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 as either “Access” or “Trunk” ports and configure the relevant VLANs. The details of “Access” and “Trunk” modes are described in later sections.

VLAN 1 cannot be deleted by the user. Instead, a user can remove all the ports from VLAN 1 to make it nonfunctional. This can be done by using the “no ports” command in VLAN the configuration mode in CLI.

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 section Native VLAN on Trunk.

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.

5.5 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. 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. 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

5.6 Removing VLANs

Follow the steps below to remove VLANs from Supermicro switches.
### VLAN Configuration

#### Step 1
Configure terminal

**Description:** Enter the configuration mode.

#### Step 2
`no vlan <vlan-list>`

**Description:** Remove VLANs using the no vlan command.  

*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`

**Description:** To display the configured VLANs.

#### Step 4
`write startup-config`

**Description:** Optional step – Save these VLAN configuration to be part of startup configuration.

The below examples show sample 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
```

### 5.7 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>
<tr>
<td>Step 2</td>
<td><code>vlan &lt;vlan-list&gt;</code></td>
<td>Enters the VLAN configuration mode.</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 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>name &lt;vlan-name-string&gt;</td>
<td>Associates a name string to this VLAN using the name command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>vlan-name-string</em> is any alphanumeric string up to 32 characters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vlan</td>
<td>Displays the configured VLANs</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 example below shows the necessary steps 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 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>Enters the VLAN configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>vlan-list</em> – 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 name string of all these VLANs will be removed by the next step.</td>
</tr>
<tr>
<td>Step 3</td>
<td>no name</td>
<td>Removes associated name string from this VLAN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vlan</td>
<td>Displays the configured VLANs</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 example below shows steps to remove a name string from a VLAN.

**Remove name from VLAN 50.**

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

### 5.8 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. Mostly ports are associated with VLANs as either “access” port members or “trunk” port members. Supermicro switches support an additional port mode called “hybrid”.

---

**Figure VLAN-4: Port Based VLANs**

---

5.8.1 Access Ports

Access ports carry traffic of only one VLAN. Any switch ports can be configured as access ports. Mostly 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.

Switch will not add VLAN tag header for all the packets sent out on an access port. Switch expects to receive untagged or priority tagged (VLAN identifier 0) packets only in the access ports. If any tagged packets received on access port, 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>
<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. &lt;br&gt;interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cxport-channel – po &lt;br&gt;&lt;br&gt;interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. &lt;br&gt; &lt;br&gt;To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. &lt;br&gt;E.g.: int range fx 0/1-10 &lt;br&gt;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>switchport mode access</td>
<td>Sets the port mode as the access port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport access vlan &lt;vlan-id&gt;</td>
<td>Configures the access VLAN for this interface. The VLAN identifiers may be any VLAN number from 1 to 4069. &lt;br&gt; &lt;br&gt;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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show vlan port config port &lt;iftype&gt; &lt;ifnum&gt;</td>
<td>Displays the configured mode and access the VLAN for this interface.</td>
</tr>
</tbody>
</table>
Step 6 | write startup-config
| Optional step – saves this VLAN configuration to be part of startup configuration.

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

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

“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

5.8.2 Trunk Ports
Trunk ports carry the traffic of one or more VLANs. Any switch ports can be configured as trunk ports. 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 trunk port, by default it will be added to all the VLANs in the switch as a tagged port. To restrict the VLANs carried in trunk ports, refer section Allowed VLANs on a Trunk.
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>
<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. &lt;interface-type&gt; – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po &lt;interface-id&gt; 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</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>Sets the port mode as a trunk port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vlan port config port &lt;iftype&gt; &lt;ifnum&gt; and show running-config</td>
<td>Displays the configured mode for this interface.</td>
</tr>
</tbody>
</table>
Step 5 | **write startup-config**  
---|---  
**Optional step** – saves this VLAN configuration to be part of startup configuration.

“**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**

### 5.8.2.1 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><strong>configure terminal</strong></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  
rx-ethernet – rx  
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>switchport mode trunk</th>
<th>Sets the port mode as trunk port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 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>
</tbody>
</table>

**Step 4a**: `switchport trunk allowed vlan <vlan-list>`  
This command configures the list of allowed VLANs on this trunk. Only the VLANs provided on the `vlan-list` will be carried over the trunk.

**Step 4b**: `switchport trunk allowed vlan add <vlan-list>`  
This command adds the given list of VLANs to the existing set of allowed VLANs on this trunk.

**Step 4c**: `switchport trunk allowed vlan remove <vlan-list>`  
This command removes the given list of VLANs from the existing set of allowed VLANs on this trunk.

**Step 4d**: `switchport trunk allowed vlan except <vlan-list>`  
This command makes all the configured VLANs allowed on this trunk except for the given list of VLANs.

**Step 4e**: `switchport trunk allowed vlan all`  
This command sets the default behavior of allowing all VLANs configured in the switch as allowed VLANs on this trunk.

**Step 4f**: `switchport trunk allowed vlan none`  
This command removes all the allowed VLANs from this trunk.

**Step 5**: `show vlan port config port <iftype> <ifnum>` and `show running-config`  
Displays the configured, allowed VLANs for this trunk interface.

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

---

```
"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

**5.8.2.2 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>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  
**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.

---

```
“switchport trunk native vlan” command will be accepted only if the port is in trunk mode.

“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.**

```
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.**

```
SMIS# configure terminal  
SMIS(config)# interface fx 0/1  
SMIS(config-if)# no switchport trunk native vlan
```
5.8.3 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 simultaneously as a tagged or untagged port 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 ports 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</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Use steps 3a to 3c below one or more times to configure the required port configurations for the VLANs provided in Step 2 above.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3a</strong></td>
<td><strong>ports</strong> <code>&lt;ports-list&gt;</code> <strong>tagged</strong> or <strong>no ports</strong> <code>[&lt;ports-list&gt;]</code> <strong>tagged</strong></td>
</tr>
<tr>
<td></td>
<td>Adds the tagged ports list to this VLAN.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ports-list&gt;</code> – up to three ports or three ranges of ports separated by spaces.</td>
</tr>
<tr>
<td></td>
<td>The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/1.</td>
</tr>
<tr>
<td></td>
<td>Use the <strong>no</strong> form of this command to remove tagged ports from this VLAN.</td>
</tr>
<tr>
<td></td>
<td>If <code>&lt;ports-list&gt;</code> is not provided to the <strong>no</strong> command, all the tagged ports are removed from this VLAN.</td>
</tr>
</tbody>
</table>

| **Step 3b** | **ports** `<ports-list>` **untagged** or **no ports** `[<ports-list>]` **untagged**                                                                                                    |
|            | Adds the untagged 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 0/1.                                                                                   |
|            | Use the **no** form of this command to remove untagged ports from this VLAN.                                                                                                             |
|            | If `<ports-list>` is not provided to the **no** command, all the untagged ports are removed from this VLAN.                                                                            |

| **Step 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 0/1.                                                                                   |
|            | Use the **no** form of this command to remove forbidden ports from this VLAN.                                                                                                           |
| Step 4 | Exit | If *ports-list* is not provided to the **no** command, all the forbidden ports are removed from this VLAN. |
| Step 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`

| Step 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** `<iftype> <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 the “hybrid” mode.

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

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

A port can be configured as untagged port for multiple VLANs. This case is useful for MAC based VLANs. For 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 MAC based VLAN case, 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
```
5.9 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 with port-based VLAN configurations.

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

The switch administrator could 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

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:30:48:0a:dd:e3</td>
<td>10</td>
</tr>
<tr>
<td>00:30:48:04:02:89</td>
<td>20</td>
</tr>
<tr>
<td>00:30:48:01:72:58</td>
<td>20</td>
</tr>
<tr>
<td>00:30:48:d8:ed:54</td>
<td>30</td>
</tr>
</tbody>
</table>

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>vlan &lt;vlan-list&gt;</td>
<td>Creates the required VLANs. <em>vlan-list</em> may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN numbers are treated as a single entry.</td>
</tr>
</tbody>
</table>
numbers can be provided as ranges such as 5-10.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>ports &lt;ports-list&gt; untagged</em></td>
<td>Adds the ports given by <em>ports-list</em> to this VLAN as untagged ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ports-list</em> – 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 ports from fx 0/1 to fx 0/1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exit</td>
<td>Exits the VLAN configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>mac-vlan &lt;ucast_mac&gt; vlan &lt;vlan-id&gt;</em></td>
<td>Configures MAC VLAN mapping entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ucast_mac</em> – Unicast MAC address. This VLAN will be applied to all incoming untagged packets from this unicast MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>vlan-id</em> - VLAN identifiers may be any VLAN number from 1 to 4069. The VLAN must have already been created in this switch.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>show mac-vlan</em></td>
<td>Displays the configured MAC based VLANs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>write startup-config</em></td>
<td>Optional step – saves this VLAN configuration to be part of startup 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><em>configure terminal</em></td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><em>no mac-vlan &lt;ucast_mac&gt;</em></td>
<td>Removes MAC VLAN mapping entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>ucast_mac</em> – Unicast MAC address for which MAC VLAN mapping is to be removed.</td>
</tr>
<tr>
<td>Step 3</td>
<td><em>show mac-vlan</em></td>
<td>Displays the configured MAC based VLANs.</td>
</tr>
</tbody>
</table>
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

### 5.10 Protocol Based VLANs

Protocol Based VLAN features help to classify incoming traffic to different VLANs based on 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.

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

**Figure VLAN-7: Protocol Based VLAN Configuration Steps**

1. Create VLANs and add ports
2. Create protocol groups
3. Associate groups to VLANs in ports

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>
</tbody>
</table>
### Step 2

**Command:** `vlan <vlan-list>`

- **Description:** Adds a VLAN. `<vlan-list>` can 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.

### Step 3

**Command:** `ports <ports-list> untagged`

- **Description:** Adds the required ports for this VLAN as untagged ports.

**Ports List:** 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`.

### Step 4

**Command:** `Exit`

- **Description:** Exits the VLAN configuration mode.

### Step 5

**Command:** `map protocol {arp | ip | rarp | ipx | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa> | enet-v2 | RFC1042 | llcOther | snap8021H | snapOther} protocols-group <Group id integer(0-2147483647)>`

- **Description:** Creates a protocol group.

**Protocol Group Creation:** Takes three parameters.
- **First:** Protocol field as `arp`, `ip`, `rarp`, `ipx`, `novell`, `netbios`, `appletalk`, or `other`.
- **Second:** Frame type as `enet-v2`, `llc`, or `snap`.
- **Third:** Protocol group identifier number.

### Step 6

**Command:** `interface <interface-type> <interface-id>`

- **Description:** 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 could 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.

**Example:** `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>
</table>
| Step 7 | `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. |
| Step 8 | `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. |
| Step 9 | `Exit`                                       | Exits the interface configuration mode.                                                          |
| Step 10| `show vlan protocols-group`                  | Displays the configured protocol based VLANs.                                                   |
|        | `show protocol-vlan`                         | Optional step – saves this VLAN configuration to be part of startup configuration.               |
| Step 11| `write startup-config`                       | Optional step – saves this VLAN configuration to be part of startup configuration.               |

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><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  
cl-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 |
Step 3. **no switchport map protocols-group** <Group id integer(0-2147483647)>  
Provides a range, use a hyphen (-) between the start and end interface numbers.  
Example: `int range fx 0/1-10`  
To provide multiple interfaces or ranges, separate with a comma (,).  
Example: `int range fx 0/1-10, fx 0/20`  

Removes the protocol groups from interface mode.  

*Group id* – Protocol Group Identifier

---

**Step 4. Exit**  
Exits VLAN configuration mode.

**Step 5. no map protocol** {arp | ip | rarp | ipx | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa>} {enet-v2 | RFC1042 | llcOther | snap8021H | snapOther}  
Removes the protocol group.  

Before removing any protocol group, it must have been removed from all interfaces.

**Step 6. no vlan** <vlan-list>  
`or`  
`vlan <vlan-list>`  
`no ports <ports-list> untagged`  
Removes the VLANS created for protocol based VLANS.  

If the VLAN is shared with a MAC or port based VLAN, then remove only the ports added during the protocol based VLAN configuration. To remove the ports use the “no ports” command in 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 may be provided as a range, such as 5-10.

**Step 7. show vlan protocols-group**  
`show protocol-vlan`  
Displays the protocol based VLANS.

**Step 8. write startup-config**  
Optional step – saves this VLAN configuration to be part of startup configuration.

---

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

5.11 Acceptable Frame Types
By default, Supermicro switch ports accept all frame 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>
<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

Step 3
Use any of the below steps 3a to 3d to configure acceptable frame types for the ports provided in Step 2 above.

Step 3a switchport acceptable-frame-type tagged
This command makes only tagged frame types accepted on these ports. Any untagged or priority tagged packets received will be dropped.

Step 3b switchport acceptable-frame-type untaggedAndPrioritytagged
This command makes only untagged and priority tagged frame types accepted on these ports. Any tagged packets received will be dropped.

Step 3c switchport acceptable-frame-type all
This command makes accepting all frame types the default behavior.

Step 3d no switchport acceptable-frame-type
This command makes accepting all frame types the default behavior.

Step 4 show vlan port config port <iftype> <ifnum>
Displays the configured mode and access VLAN for this interface.

Step 5 write startup-config
Optional step – saves this VLAN configuration to be part of startup configuration.

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

5.12 Ingress Filter

By default, Supermicro switch has the ingress filter enabled. Ingress filter helps to drop the packets not matching the configured VLAN membership.

For example if the switch has two VLANs configured 10 and 20, the ports configured with only VLAN 10 can accept the packets with VLAN header having VLAN identifier 20. This is called VLAN hoping. To prevent VLAN hoping, the ingress filter is enabled to drop the packets with different VLAN identifier than 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 <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>
<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 may be a 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 hypen (-) between the start and end interface numbers. 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`

| Step 3 | switchport ingress-filter | This command enables ingress filtering function. This is the default behavior. |
|        | (or)                       | The no form of this command disables ingress filtering. |
|        | no switchport ingress-filter |                                      |

| Step 4 | show vlan port config port `<iftype>` `<ifnum>` | Displays the configured ingress filter mode for this interface. |

| Step 5 | write startup-config | Optional step – saves this VLAN configuration to be part of startup configuration. |

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.**

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

### 5.13 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.
SMIS# configure terminal

# 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...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.0.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

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 : fx 0/11-14 fx 0/17-19 fx 0/41-48 cx 0/1-6
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 :
Status : Permanent

---------
Vlan ID : 30
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 :
Status : Permanent
5.14 Private Edge VLAN / Protected Ports

The Private Edge VLAN or also called Protected Ports feature helps to isolate the 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 on one of the following three modes.

5.14.1 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.

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

5.14.3 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>
</table>
| Unprotected Ports| Unprotected Ports
|                 | Protected Ports
|                 | Community Ports                         |
| Protected Ports | Unprotected Ports                      |
| Community Ports | Unprotected Ports
|                 | Other ports in the same community       |

5.15 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.

noswitchport protected

There is no limit on the number of unprotected ports supported in the switch.
5.16 Protected Ports configuration

Any port can be configured as protected port with the below CLI command in interface configuration mode.

switchport protected

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

There is no limit on the number of protected ports supported in the switch.

5.17 Community Ports configuration

Any port can be configured as community port with the below CLI command in interface configuration mode.

switchport protected group <group number>

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

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.

5.17.1 Configuration Example 1

Configure all the 48 downlink Fx ports as isolated (or protected ports). These 48 ports should not be able to communicate 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 simple as below. The uplink ports can be left with the 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
```

### 5.17.2 Configuration Example 2

The Fx ports 1 to 24 should be able to communicate among themselves and also should be able to communicate with up link 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 up link 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 the 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
6 Link Aggregation

The Link Aggregation feature when helps connecting 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 set to 10Gig speed, user can aggregate eight 10Gig ports to get up to 80 Gbps speed aggregated uplink.

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

The “port channel”, “channel group” and “ether channels” are used synonymously to refer to aggregate links.
6.1 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 not support the Multiple Chassis Link Aggregation (MLAG) feature.

6.2 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.

6.3 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.

6.4 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.
6.5 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 “bundle” state will be used for data traffic.

Ports in LACP mode exchange LACP packets with other end device. 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
Figure LA-2: Dynamic Link Aggregation 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.

### 6.6 Link Aggregation Port Channel

#### 6.6.1 Creating Port Channels

Port channel creation involves two steps: the first step is creating the port channel interfaces and the second step is adding member ports to the port channel interfaces.

#### 6.6.1.1 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></td>
<td>Creates a port channel using “interface port—channel” command.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no interface range port-channel <code>&lt;channel-group-number&gt;</code> ....</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>channel-group-number</em> – may be any number from 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To configure multiple port channel 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.: int range po 1-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>
the port channel interfaces using the description command.

The string may be up to 64 characters in length.
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. <code>framesize</code> may be any number from Port channel MTU will be used on its all member ports.</th>
</tr>
</thead>
</table>

| Step 5  | VLAN Configurations | Optional step – configures the VLAN parameters for port channel interfaces. Refer to the VLAN configuration guide for all VLAN configuration details. |
|---------|---------------------|---------------------------------------------------------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Spanning Tree Configurations</th>
<th>Optional step – configures the spanning tree parameters for port channel interfaces. Refer to the spanning Tree configuration guide for all spanning tree configuration details.</th>
</tr>
</thead>
</table>
### Step 7
End

Ends the configuration mode.

### Step 8
`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 9
`write startup-config`

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

---

### 6.6.1.2 Adding Member Ports to Port Channels

Users can add up to eight member ports to static port channels. For LACP port channels, user 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>
</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... |
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

| 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> | Displays the configured port channel information. |
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
```
6.6.2 Modifying Port Channels

6.6.2.1 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.

```plaintext
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
```

6.6.2.2 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.

6.6.2.3 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.

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

6.6.2.4 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 <code>&lt;interface-type&gt; &lt;interface-id&gt;</code></td>
<td>Enters the interface mode.</td>
</tr>
</tbody>
</table>
Or

interface range <interface-type><interface-id>

...-

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>
<tr>
<td>Step 5</td>
<td>show interface port-channel &lt;channel-group-number&gt; show etherchannel [[channel-group-number]</td>
<td>Displays the configured port channel information.</td>
</tr>
</tbody>
</table>
When a port is removed from a port channel, that port will be added to VLAN 1 automatically. The MTU and spanning tree configurations of that port will not be changed to the default configurations automatically. 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 &lt;interface-type&gt;&lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>Interface-type - may be any of the following:</td>
</tr>
<tr>
<td></td>
<td>interface range &lt;interface-type&gt;&lt;interface-id&gt;...</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</td>
</tr>
</tbody>
</table>
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 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

<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>channel-group &lt;channel-group-number&gt; mode {active</td>
<td>passive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For LACP aggregation, use the active or passive mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For static link aggregation, use the mode on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>channel-group-number – The port channel to which these member ports are added.</td>
</tr>
<tr>
<td>Step 5</td>
<td>End</td>
<td>Exits the interface configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interface port-channel &lt;channel-group-number&gt;</td>
<td>Displays the configured port channel information.</td>
</tr>
<tr>
<td></td>
<td>show etherchannel [[channel-group-number] { detail</td>
<td>load-balance</td>
</tr>
<tr>
<td>Step 7</td>
<td>write startup-config</td>
<td>Optional step – saves this port channel configuration to be part of startup</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

6.6.3 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>
<tr>
<td>Or</td>
<td>no interface range port-channel &lt;channel-group-number&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E.g.: no int range po 1-3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide multiple interfaces or ranges, separate with a comma (,).</td>
</tr>
</tbody>
</table>
### 6.6.4 LACP Parameters

Users can configure the following LACP parameters on Supermicro switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP System</td>
<td></td>
</tr>
<tr>
<td>Priority LACP</td>
<td></td>
</tr>
<tr>
<td>Port Priority</td>
<td></td>
</tr>
<tr>
<td>LACP</td>
<td></td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
</tr>
</tbody>
</table>

#### 6.6.4.1 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

---

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

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

Remove the 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
SMIS(config-if)# exit
```
eight member ports are configured, the switch that has low 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

6.6.4.2 LACP Port Priority
When more than eight member ports are configured, the ports that have the lowest port priority value get selected as active member ports. If multiple ports have the same port priority value, the ports with the numerically lower port numbers will be selected 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 <code>&lt;interface-type&gt;</code>&lt;<code>interface-id</code>&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td>Or</td>
<td>interface range <code>&lt;interface-type&gt;</code>&lt;<code>interface-id</code>&gt;</td>
<td><code>interface-type</code> – may be any of the following: fx-ethernet – fx cx-ethernet – cx</td>
</tr>
<tr>
<td></td>
<td>....</td>
<td><code>interface-id</code> 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
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
### 6.6.4.3 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 different LACP timeout selections. 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></td>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface <code>&lt;interface-type&gt;</code>&lt;interface-id&gt;</td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td></td>
<td>Or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface range <code>&lt;interface-type&gt;</code>&lt;interface-id&gt;</td>
<td><code>interface-type</code> – 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><code>interface-id</code> is in <code>slot/port</code> format for all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>physical interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>lacp timeout (long</td>
<td>short)</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td>Configures the LACP port timeout.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>long – LACP messages are expected to be received once every 30 seconds. short – LACP messages are expected to be received once every second.</td>
<td></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>Displays the configured port priority information.</td>
</tr>
<tr>
<td></td>
<td>show etherchannel</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 timeout configuration to be part of startup</td>
</tr>
</tbody>
</table>
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

### LACP Wait Time

Switch waits for “LACP wait time” period before adding any member port in 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><code>interface &lt;interface-type&gt;&lt;interface-id&gt;</code></td>
<td>Enters the interface mode.</td>
</tr>
<tr>
<td></td>
<td>Or <code>interface range &lt;interface-type&gt;&lt;interface-id&gt;</code> ....</td>
<td></td>
</tr>
</tbody>
</table>

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

### 6.6.5 Load Balancing

Supermicro switches support load balancing on aggregated links.

Switches distribute outgoing traffic on all member ports that are in 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.
- Packets will be distributed across the member ports based on the source and destination MAC addresses of the packet.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Displays the configured port priority information.</td>
</tr>
<tr>
<td>5</td>
<td>show etherchannel</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>write startup-config</td>
<td>Optional step – saves this LACP wait</td>
</tr>
</tbody>
</table>
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>
</tbody>
</table>
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.

---

Follow the below steps to configure the load balancing algorithm

<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 running-config</td>
<td>Displays the configured load balancing information.</td>
</tr>
<tr>
<td>5</td>
<td>write startup-config</td>
<td>Optional step – saves this load balancing configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
### Step 1
**configure terminal**
Enter the configuration mode.

### Step 2
**set port-channel disable**
Disables the link aggregation feature.

### Step 3
**End**
Exits the configuration mode.

### Step 4
**show etherchannel**
Displays link aggregation feature status.

### Step 5
**write startup-config**
Optional step – saves this configuration to be part of startup configuration.

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>Step 1</td>
<td>configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>set port-channel enable</td>
<td>Enables the link aggregation 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 etherchannel</td>
<td>Displays link aggregation feature status.</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>

### 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)# 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...

ID   Hardware Version     Firmware   OS
0    SBM-25G-100 (B8 R1.01)     1.0.2.0  1.0.6

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted

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
---------------------------------------------------------------------
Cx0/3 Down  128  1  1  0x33  0x45
Cx0/4 Down  128  1  1  0x34  0x45
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 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 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#
7 Layer-2 ECMP Load Balancing

The L2 ECMP feature helps to load balance the incoming traffic to all the blade servers in the chassis.

The L2 ECMP load balance the traffic based on the source and destination IP addresses on the packet. The ECMP supports symmetric load balancing. For example, if a traffic flow with source IP address a.a.a.a and destination IP address b.b.b.b is sent to blade server “N”, then the reverse flow of that traffic with source IP address b.b.b.b and destination IP address a.a.a.a will be sent to the same blade server “N”.

The switch supports one ECMP group where one or more blade server connected “Fx” ports can be added as member ports.

7.1 Configurations

Follow the steps below to add configure layer-2 ECMP load balancing.

<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 on which this layer-2 ECMP load balancing needs to be applied.</td>
</tr>
<tr>
<td>Step 3</td>
<td>l2-ecmp-group &lt;l2-ecmp-group-number(1-65535)&gt;</td>
<td>Configures the ports to be member of the ECMP group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Ends the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Saves this L2 ECMP configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

The example below shows configuring layer-2 ECMP load balancing for the ports fx 0/1 to fx 0/5.

SMIS#configure terminal

SMIS(config)# interface range fx-ethernet 0/1-5

SMIS(config-if)# l2-ecmp-group 100

SMIS(config-if)# end

Removing member port(s) from L2 ECMP 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>interface &lt;interface-type&gt;&lt;interface-id&gt; or</td>
<td>The port or port lists on which this layer-2 ECMP load balancing needs to be removed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>no l2-ecmp-group</td>
<td>Removes the port(s) from the ECMP group.</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Ends the configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>Saves the configuration changes to the startup configuration.</td>
</tr>
</tbody>
</table>

Make sure that all the ports are configured with same parameters such as MTU, speed, etc.

Only one ECMP group is supported.
L2 ECMP is supported only on default VLAN 1.
L2 ECMP is not supported in MLAG and IGMP snooping use cases.

The example below shows the commands for removing port(s) from L2 ECMP group.

SMIS# configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# no l2-ecmp-group
SMIS(config-if)# end

Use the show command to display the current state of layer-2 ECMP configurations.

SMIS# show l2-ecmp-group

L2 ECMP Group Id: 100.

<table>
<thead>
<tr>
<th>Member Ports</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fx0/1</td>
<td>Up</td>
</tr>
<tr>
<td>Fx0/2</td>
<td>Up</td>
</tr>
<tr>
<td>Fx0/3</td>
<td>Down</td>
</tr>
<tr>
<td>Fx0/4</td>
<td>Up</td>
</tr>
<tr>
<td>Fx0/5</td>
<td>Up</td>
</tr>
</tbody>
</table>

SMIS#
8 MLAG

8.1 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 available bandwidth by 50%.

Multi-Chassis Link Aggregation (MLAG) feature allow 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 8 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 peer.

8.1.1 Terminologies

8.1.1.1 IPL – Inter Peer Link
The link connecting between two MLAG peer switches is referred as 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.

8.1.1.2 Peer Switch
The two switches that form a single logical port channel interface is referred as peer switches. The peer switches are connected through IPL interface. For example, in the topology diagrams shown in “Topologies” section, the switches “Switch A” and “Switch B” are peer switches.

8.1.1.3 MLAG Port Channel
The link connecting MLAG peers to MLAG partner switches. MLAG port channel interfaces should be created on both the peer switches with the same port channel number.

8.1.1.4 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.

8.1.1.5 Single Homed Device
The device connected to only one of the peer switch. This connection could be a regular single physical link connection or through a port channel interface.
8.2 Topologies

8.2.1 Topology 1 - Server to switch MLAG topology

In Figure MLAG-1, Switch A and Switch B are peer switches in the MLAG. Switch A and B are connected through IPL port channel interface.

The server is connected to both the MLAG peer switches through regular bonding or teaming LACP interface on the server side.

On the switch side, the ports connected to server, are configured with the same MLAG enabled port channel number.
8.2.2 Topology 2 - Switch to switch MLAG topology

In Figure MLAG-2, Switch A and Switch B are peer switches in the MLAG. Switch A and B are connected through IPL port channel interface.

The Switch C is connected to both the MLAG peer switches through regular LACP port channel interface.

On Switch A and Switch B sides, the ports connected to Switch C, are configured with the same MLAG enabled port channel number.
8.2.3 Topology 3 - Single uplink switch topology

In Figure MLAG-3, Switch A and Switch B are peer switches in the MLAG. Switch A and B are connected through IPL port channel interface.

The Server is connected to both the MLAG peer switches through regular LACP port channel interface.

The Uplink Switch 1 is connected to MLAG peer switches Switch A and Switch B through regular LACP port channel interface.

On Switch A and Switch B sides, the ports connected to 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 same packet (broadcast or multicast) to both the MLAG peer switches.
8.2.4 Topology 4 – Redundant uplink switch topology

In Figure MLAG-4, Switch A and Switch B are peer switches in the MLAG. Switch A and B are connected through IPL port channel interface.

The Server is connected to both the MLAG peer switches through regular LACP port channel interface.

The Uplink Switch 1 and Uplink Switch 2 is connected to MLAG peer switches Switch A and Switch B through MLAG port channel interface.

On Switch A and Switch B sides, the ports connected to 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 same packet (broadcast or multicast) to both the MLAG peer switches.
8.3 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>

8.4 MLAG Configurations

The mandatory configurations for an MLAG are:
1) System ID
2) Priority
3) IPL port channel interface
4) Enabling MLAG on a port channel interfaces

The keep alive time configuration is optional.

8.4.1 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.

MLAG system ID must be configured as same in both the peer switches. If this condition does not meet, 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 MLAG system ID and MLAG system priority.

Follow the steps below to configure 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 <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>
</tbody>
</table>
The “**no mlag system-identifier**” command deletes the MLAG system ID.

When 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
```

### 8.4.2 MLAG System Priority
MLAG switches use this MLAG system priority for LACP exchanges with partner devices.

MLAG system priority must be configured as same in both the peer switches. If this condition does not meet, 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 MLAG system ID and MLAG system priority.

Follow the steps below to configure 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 MLAG system priority is deleted, both IPL and 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

8.4.3 Keep Alive Time
MLAG peer switches periodically transmit keep alive packets to maintain the relationship between peer switches. The value of keep alive transmit timer is user configurable.

Keep alive mechanism identifies one of the peer switches as primary and other as 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 keepalive time to it’s default value.

Keepalive time can be different on both the 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

8.4.4 IPL Interface

The link connecting between two MLAG peer switches is referred as 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.

Only the primary switch among the peers participates in Spanning Tree protocol.

Follow the steps below to configure 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 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
8.4.5 MLAG Port Channels

The link connecting MLAG peers to MLAG partner switches. MLAG port channel interfaces should be created on both the 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. \n<em>channel-group-number</em> – 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 shows the basic port channel details for MLAG port channels also.

8.4.6 Other configurations

MLAG peer switches exchange only the dynamic learned specific information. The configurations across peer switches are not exchanged. Hence user 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>-------------------------------------------------</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>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>
9 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 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 flooding is stopped.

Spanning tree protocols help to avoid the flooding on network loops. Spanning tree protocols form loop free tree structured logical network topology over physical network connections.

Spanning tree enabled switches exchange spanning tree protocol messages (BPDU) to form loop free topology. Based on the exchanged BPDU information, 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 a best loop free path to reach the root switch. The redundant paths to root switch are blocked to form loop free topology.

Spanning tree algorithm assigns one of the following roles to every port on the switches.

<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</td>
</tr>
<tr>
<td></td>
<td>• Root ports forwards the traffic</td>
</tr>
<tr>
<td>Designated Port</td>
<td>• Loop free connection to the other switch on the LAN</td>
</tr>
<tr>
<td></td>
<td>• Designated ports forwards the traffic</td>
</tr>
<tr>
<td>Alternate Port</td>
<td>• Redundant path to the root switch</td>
</tr>
<tr>
<td></td>
<td>• Alternate ports do not forward the traffic</td>
</tr>
<tr>
<td>Blocked Port</td>
<td>• Redundant path to other switches on the LAN</td>
</tr>
<tr>
<td></td>
<td>• Blocked ports do not forward the traffic</td>
</tr>
</tbody>
</table>

When network connections status changes, spanning tree recalculates the paths to form 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. BPDU exchange between switches takes a few seconds in large LAN. To avoid any temporary loops while forming spanning tree topology, the switch ports are moved through different states to reach forwarding state. Switch ports stay in one of the following spanning tree states.
Since spanning tree forms logical loop free topology, it helps to have physical loop connections on the network for redundancy purpose. When an active connection fails, spanning tree enables the blocked redundant connection automatically.

Rapid spanning tree protocol (RSTP) provides faster topology convergence. Spanning tree (STP) takes more than 30 seconds to move a port to forwarding state. But RSTP can move a port to the forwarding state within 3 times of 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.

9.1 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 a switch as a 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 – priority and MAC address of the switch. The spanning tree priority occupies the most significant two bytes of bridge ID. The default spanning tree priority is 32768.
When a switch starts spanning tree it sends out BPDUs with this 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. If the received root bridge ID is higher than its own bridge ID, the received switch ignores the received BPDU and continue to act as the root switch.

If priorities of all switches are same, switch MAC addresses decide the lowest bridge ID and hence switch with lowest MAC address will be elected as the root switch.

### 9.2 Spanning Tree Support
Supermicro switches support STP, RSTP and MSTP protocols based on standards IEEE 802.1D 2004 and 802.1s.

### 9.3 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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello time</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Forwarding time</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Maximum aging time</td>
<td>20 seconds</td>
</tr>
<tr>
<td>Transmit hold count</td>
<td>3</td>
</tr>
<tr>
<td>Max hops</td>
<td>20</td>
</tr>
<tr>
<td>Path cost method</td>
<td>Long</td>
</tr>
<tr>
<td>MST region name</td>
<td>Switch MAC address</td>
</tr>
<tr>
<td>MST region revision</td>
<td>0</td>
</tr>
<tr>
<td>Spanning tree compatibility</td>
<td>In MSTP mode, the default compatibility is MSTP and in RSTP mode the default compatibility is RSTP</td>
</tr>
<tr>
<td>Root guard</td>
<td>Disabled</td>
</tr>
<tr>
<td>Topology change guard</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port fast</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto edge</td>
<td>Enabled</td>
</tr>
<tr>
<td>Link type</td>
<td>Full duplex ports – point to point links</td>
</tr>
</tbody>
</table>
### 9.4 Enabling/Disabling Spanning Tree

#### 9.4.1 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 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

#### 9.4.2 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 the 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 “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 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>
“no spanning-tree disable“ command enables the 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

9.5 Configuring MST
Spanning tree is enabled by default in MST mode in Supermicro switches.

In case if the switch was earlier configured 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 currently running spanning tree and restart it in the given new mode.
### 9.6 Configuring MST region and instances

All the spanning tree switches in a 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>
</tbody>
</table>
| Step 3 | instance<instance-id(1-16)>vlan<vlan-range> | Creates a MST instance and maps it to the given VLAN range.  
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. |
| Step 6 | end | Exits the configuration mode. |
| Step 7 | show spanning-tree mst configuration | Displays the spanning tree MST configuration parameters. |
| Step 8 | write startup-config | Optional step – saves this spanning tree configuration to be part of startup configuration. |
“no name” command removes the configured MST region name.

“no revision” command resets the configured MST region revision number to its default value 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

9.7 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 currently running spanning tree and restart it in the given new mode.

## 9.8 Spanning Tree Compatibility

MSTP is backward compatible with RSTP and STP. Similarly RSTP is backward compatible with STP.

When a MSTP operating switch detects a RSTP operating switch in any port, the MSTP switch will downgrade to RSTP operating mode on that port.

Similarly when a MSTP or RSTP operating switch detects a STP operating switch in any port, the switch will downgrade to STP operating mode on that port.

User can force the switch to operate in any particular compatibility mode. In user configured STP compatible mode, switch will transmit and receive only STP BPDUs and it will drop the RSTP and MSTP BPDUS if received any.

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>spanning-tree mode stp</td>
<td>Configures the spanning tree compatibility.</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree compatibility stp</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree compatibility rst</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>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>
“no spanning-tree compatibility” command resets the spanning tree compatibility mode to 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

9.9 Configuring Root Switch (or) Priority

Switch with the lowest priority value gets elected as the root switch. To make any particular switch as the root switch, configure lower numeric priority value. The default spanning tree priority is 32768.

When priorities of all switches are same, switch with 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>To configure the switch priority in RST mode: spanning-tree priority &lt;priority-value&gt; To configure the switch priority for the default MST instance 0: spanning-tree priority &lt;priority-value&gt; To configure the switch priority for particular MST instance: spanning-tree mst &lt;instance-id&gt; priority &lt;priority-value&gt;</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>
</tbody>
</table>
The MST instance identifier may be from 1 to 16.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show spanning-tree bridge priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show spanning-tree</td>
</tr>
<tr>
<td></td>
<td>Displays the spanning tree</td>
</tr>
<tr>
<td></td>
<td>configuration parameters including</td>
</tr>
<tr>
<td></td>
<td>the switch priority values.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>write startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Optional step – saves this</td>
</tr>
<tr>
<td></td>
<td>spanning tree configuration to</td>
</tr>
<tr>
<td></td>
<td>be part of startup configuration.</td>
</tr>
</tbody>
</table>

“nospanning-tree priority” command resets the spanning tree switch priority to default value 32768. In MST mode, it resets the switch priority for the default MST instance 0.

“no spanning-tree mst <instance-id>priority” command resets the spanning tree switch priority to 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

9.10 Port Priority

When spanning tree detects multiple paths to root switch in loop condition, it selects the port with 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 lowest numeric port priority value as the forwarding port.
When priorities of all the ports are same, the port with lowest port identifier gets selected as the forwarding port.

The port priority used in selection of root port is the priority of the upstream switch port. Changing the port priority will affect the root port selection in 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 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; To configure the port priority for the default MST instance 0: spanning-tree port-priority &lt;priority-value&gt; To configure the port priority for particular MST instance: spanning-tree mst &lt;instance-id&gt;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. 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>
</tbody>
</table>
Step 5  
show spanning-tree interface <interface-type><interface-id>  
Displays the spanning tree port parameters including the port priority values.

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

“nospanning-tree port-priority” command resets the spanning tree port priority to default value 128. In MST mode, it resets the port priority for the default MST instance 0.

“no spanning-tree mst <instance-id>port-priority” command resets the spanning tree port priority to 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 the 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 the 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 the 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

9.11 Path Cost

When spanning tree detects multiple paths to root switch in loop condition, it selects the port with 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 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 speed.

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Default Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>20000000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>2000000</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 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;</td>
<td>Enters the port interface mode.</td>
</tr>
<tr>
<td></td>
<td>or 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 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.</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 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 0 to 200000000.</td>
</tr>
<tr>
<td></td>
<td>To configure the port priority for the default MST instance 0: spanning-tree cost&lt;cost-value&gt;</td>
<td>The default path cost is calculated based on the port speed.</td>
</tr>
<tr>
<td></td>
<td>To configure the port priority for particular MST instance: spanning-tree mst &lt;instance-id&gt;cost&lt;cost-value&gt;</td>
<td>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>
</tbody>
</table>
### Step 5
show spanning-tree interface <interface-type><interface-id>
 Displays the spanning tree port parameters including the port path cost values.

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

---

**Information:**

“nospanning-tree cost” command resets the spanning tree port path cost to default value. In MST mode, it resets the port path cost for the default MST instance 0.

“no spanning-tree mst <instance-id>cost” command resets the spanning tree port path cost to 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 the 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 the 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 the port cx 0/1

```
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# spanning-tree mst 10 cost20
SMIS(config-if)# end
```

### 9.12 Hello Time

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 times of hello time interval, spanning tree protocol assumes the root switch is failed.

In MSTP the hello time is configurable on the individual ports. In RSTP the hello time is configured commonly for all the 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>

“nospanning-tree hello-time” command resets the spanning tree port hello time to default value, 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 interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel 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, use separate with a comma (,).

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

<table>
<thead>
<tr>
<th>Step 3</th>
<th>To configure the hello time in MST mode: spanning-tree mst hello-time&lt;time-value&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configures the hello time interval.</td>
</tr>
<tr>
<td></td>
<td>time-value – Hello time value may be 1 or 2 seconds.</td>
</tr>
<tr>
<td></td>
<td>The default hello time is 2 seconds.</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 spanning-tree bridge hello-time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the spanning tree hello time.</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 spanning tree configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>

“nospanning-tree msthello-time” command resets the spanning tree port hello time to default value, 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
SMIS(config-if)# end

9.13 Max Age

Switches maintain the BPDU information for every port for a period of max age. If BPDU configuration messages are not received on any ports for max age time, switch will reconfigure those ports.
Max age time affects the failure detection and reconfiguration. Smaller max age time will help to detect the failures quickly. It is advisable to choose the 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.

Max age value should be lesser than twice of (forward time – 1).

Follow the steps below to change 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>
</tbody>
</table>
| Step 2 | To configure the max age time: spanning-tree max-age<age-value> | 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. |
| Step 3 | end                            | Exits the configuration mode. |
| Step 4 | show spanning-tree bridge max-age | Displays the spanning tree configuration parameters including the switch priority values. |
|         | show spanning-tree             |                          |
| Step 5 | write startup-config           | Optional step – saves this spanning tree configuration to be part of startup configuration. |

“nospanning-tree max-age” command resets the spanning tree max age to default value 20.

The example below show the way to configure the spanning tree max age.

Configure the max age as 12.

SMIS# configure terminal

SMIS(config)# spanning-tree max-age12

SMIS(config)# end

9.14  Forwarding Time

Switch waits for a period of forwarding time interval on listening and learning states before going to forwarding state.
The default forwarding time is 15 seconds. Hence switch waits for 15 seconds in listening state and waits for another 15 seconds in learning state before going to forwarding state.

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>
</tbody>
</table>
| Step 2 | To configure the max age time: `spanning-tree forward-time<time-value>` | 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. |
| Step 3 | end | Exits the configuration mode. |
| Step 4 | show spanning-tree bridge forward-time | Displays the spanning tree forward time. |
| Step 5 | write startup-config | Optional step – saves this spanning tree configuration to be part of startup configuration. |

“nospanning-tree forward-time” command resets the spanning tree forwarding time to default value 15.

The example below shows the way 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
```

## 9.15 Max Hops

MSTP uses hop count to decide the validity of the BPDU messages. Root switch sends BPDU with hops count as the max hops. Every switch decrements the hops count while forwarding the BPDU. When this hops count reaches zero, the switch discards the BPDU message.

The default max hops 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>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td>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>3</td>
<td>end</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>show spanning-tree mst</td>
<td>Displays the spanning tree max hops along with other MST information.</td>
</tr>
<tr>
<td>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>

“nospanning-tree mst max-hops” command resets the MST max hops to default value 20.

The example below shows the way 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

9.16 Path Cost Long / Short

Spanning tree was originally designed with 16 bit path costs. This was good enough for the fast Ethernet and Gigabit Ethernet speed links. But this 16 bit path costs was not enough for 10Gig and higher speed ports. Hence spanning tree protocol introduced support for 32 bit path costs.

The 16 bit path costs method is referred as short path cost method and the 32 bit path cost method is referred as long path costs method.

In MSTP and RSTP mode, 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>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
Step 2 | To configure the path cost method as short spanning-tree pathcost method short 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.

Step 3 | end | Exits the configuration mode.

Step 4 | show spanning-tree pathcost method | Displays the spanning tree path cost method information.

Step 5 | write startup-config | Optional step – saves this spanning tree configuration to be part of startup configuration.

---

The example below shows the way 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

---

9.17 Transmit Hold Count

Transmit hold count helps to control the BPDU burst traffic. Switch limits the number of BPDUs sent in a second by transmit hold count. Higher value of transmit hold count 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>
<tr>
<td>Step 2</td>
<td>spanning-tree transmit hold-count &lt;count_value&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

“nospanning-tree transmit hold-count” command resets the hold count to default value 3.

The example below shows the way 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

9.18  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 lowest priority to compete for root switch. There is no option to block any switch becoming the root switch to maintain the optimized topology.

The root guard feature helps to avoid any unexpected switch becoming the root switch. If root guard feature is enabled on a port, it prevents any switches connected to that port becoming the root switch. If any superior BPDU received on the root guard enabled port, switch moves that port from forwarding state to listening state.

The root guard feature is disabled on all the 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 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

**Step 3** spanning-tree restricted-role
Enables the root guard feature.
The default option is the root guard feature disabled.

**Step 4** end
Exits the configuration mode.

**Step 5** show spanning-tree detail
Displays the spanning tree root guard information.

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

“nospanning-tree restricted-role” command resets the root guard feature to default value disabled.

The example below shows the way 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

SMIS(config-if)# end

### 9.19 Topology Change Guard

The topology change guard feature helps to prevent unexpected topology changes. Network administrators can configure the topology guard on the 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 the 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>

“nospanning-tree restricted-tcn” command resets the topology guard feature to default value disabled.
The example below shows the way 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

9.20 Port Fast

When a port link up, spanning tree does not allow the port to forward the packets immediately. Spanning tree moves the port through listening and learning states before reaching the forwarding state. This state machine function helps to achieve the loop free topology. But it delays the port operations to forward the traffic.

The switch ports connected to computers and servers are not expected to cause any loops. Those ports can be configured with port fast feature to start forwarding the traffic immediately instead of waiting through learning and listening states.

Configure the port fast feature only to the ports that are connected to computers and servers. Configuring port fast on the ports that are connected to other switches might cause network loops.

The port fast feature is disabled on all the 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.</td>
</tr>
</tbody>
</table>
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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>spanning-tree portfast</td>
<td>Enables the port fast feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default setting is the port fast 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 port fast 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>

“nospanning-tree portfast” command resets the port fast feature to default value disabled.

The example below shows the way 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

9.21 Auto Edge

Auto edge feature helps to detect the other end of the device attached to the ports. If no BPDU received for a period of time on auto edge enabled ports, switch marks those parts as edge ports assuming those ports are not connected to other switches. This helps to move the port state to forwarding quickly. Also switch do not send topology change notifications when edge ports status change.

The auto edge feature is enabled on all the 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:</td>
</tr>
<tr>
<td>Step 3</td>
<td>To enable the auto-edge spanning-tree auto-edge</td>
<td>Enables or disabled the auto edge feature.</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>To disable the auto-edge no spanning-tree auto-edge</td>
<td>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 the way 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

### 9.22 Link Type

Spanning tree decides the link type based on the duplex mode of the ports. It detects the full duplex ports as point to point links and half duplex ports as a shared LAN links.

The point to point links are assumed to be connected directly to another spanning tree switch. The 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 forwarding state.

User 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>
<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>

“nospanning-tree link-type” command resets the user configured link type to let switch 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 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

9.23 Spanning Tree Configuration Examples

Configure the following requirements on the switches as shown below in Figure MSTP-Eg.1.

5. Configure two MST instances separately for VLAN 100 and 200.
6. Configure switch B as the root switch for VLAN 100 instance.
7. Configure switch C as the root switch for VLAN 200 instance.
8. Configure the port fx 0/1-28 in all the switches as port fast.

Figure MSTP-Eg.1 Spanning 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 0/1-28 as port fast
SMIS(config)# interface range fx 0/1-28
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#
10 IGMP Snooping

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

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

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

Figure IGS-1: Multicast Forwarding without IGMP Snooping

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

A switch performs the IGMP snooping function by snooping the Layer 3 IGMP packets and recognizes an IGMP host’s connected ports by snooping the IGMP join messages sent from hosts. Similarly, a switch recognizes an IGMP router’s connected ports by snooping the IGMP control messages sent by IGMP routers. The switch maintains a multicast forwarding table based on the hosts joined and router connected ports for every multicast group and updates the multicast forwarding table when hosts leave multicast groups.
A switch forwards the multicast traffic based on the information available on the multicast table. It sends the multicast traffic of any group to only the ports that have hosts joined for that multicast group. This mechanism prevents the unnecessary flooding of multicast traffic to all the ports.

Figure IGS-2: Multicast Forwarding with IGMP Snooping

### 10.1 IGMP Snooping Support

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

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

Supermicro switches support up to 255 multicast groups.

<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>
10.2 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 to enable IGMP snooping.

Enable IGMP snooping for VLAN 1, 10 and 20.

SMIS# configure terminal
SMIS(config)# ip igmp snooping
10.3 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 IGMP protocol standard.

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

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

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

<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 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

10.4 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.

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

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

<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 mrouter-time-out&lt;timeout&gt;</td>
<td>Configures the router port timeout value in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>timeout – may be any value from 60 to 600 seconds. The default value is 125 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 router port timeout 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 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

### 10.4.2 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. 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 configure the router ports for all these VLANs.</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. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx portchannel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.</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

10.5  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.

10.5.1  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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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

10.5.2 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 messages. The number of times a switch retries sending the group specific query messages is configurable. The default retry count is 2.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>

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

Configure the group specific query interval time as 5 seconds.

SMIS# configure terminal

SMIS(config)# ip igmp snooping group-query-interval 5

SMIS(config)# end
**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
```

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

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

<table>
<thead>
<tr>
<th>Step 1</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.</td>
</tr>
</tbody>
</table>
If multiple VLANs are provided, the next step will enable the immediate leave for all these VLANs.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>ip igmp snooping fast-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 snooping vlan&lt;vlan&gt;</td>
<td>Displays the IGMP snooping immediate leave information for the given VLAN.</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>

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
```

**10.6 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>
<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 configure the switch as an IGMP querier for all these VLANs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>ip igmp snooping querier</td>
<td>Configures the switch to act as an IGMP querier.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp snooping query-interval <code>&lt;interval-value&gt;</code></td>
<td>Configures the periodic interval on the switch that will send IGMP queries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interval-value – may be any value from 60 to 600 seconds. The default value is 125 seconds.</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 <code>&lt;vlan&gt;</code></td>
<td>Displays the IGMP snooping querier configuration 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 "no ip igmp snooping querier" command can be used to remove the IGMP querier configuration from a VLAN. The "no ip igmp snooping query-interval" command can be used to set the querier periodic interval to the default value 125 seconds.

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

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

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

10.7 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></td>
<td></td>
<td>Use all-ports to configure a switch to forward IGMP host member reports to all ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use router-ports to configure the switch to forward the IGMP host member reports to the router ports only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default behavior is 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 commands to configure the IGMP member report forwarding.

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

SMIS# configure terminal

SMIS(config)# ip igmp snooping report-forward all-ports

SMIS(config)# end

### 10.8 Port Timeout (Port Purge Interval)

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

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

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

<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. 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 commands to configure the port purge interval value.

Configure the port purge interval value to 900 seconds.

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

### 10.9 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 will be forwarded to multicast routers.

Supermicro switches suppress the 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. 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 snooping globals</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

10.10 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>
</tbody>
</table>
Step 4 | `show ip igmp snooping globals` | Displays the IGMP snooping proxy reporting status information.
---|---|---
Step 5 | `write startup-config` | Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

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

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

Enable IGMP snooping proxy reporting.

SMIS# configure terminal

SMIS(config)# ip igmp snooping proxy-reporting

SMIS(config)# end

10.11 Sending Queries when Topology Changes

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

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

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

<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>ip igmp snooping send-query enable</code></td>
<td>Enables the switch to send general IGMP queries when spanning tree topology changes.</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 ip igmp snooping globals</code></td>
<td>Displays the IGMP snooping information.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>write startup-config</code></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

10.12 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. 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>
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

### 10.13 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>
</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 next step will disable IGMP snooping on all these VLANs. |
| Step 3 | ip igmp snooping multicast filtering enable | Disables IGMP snooping in VLAN. |
| Step 4 | end | Exits the configuration mode. |
| Step 5 | show ip igmp snooping vlan<vlan> | Displays the IGMP snooping information including Multicast Forwarding feature |
| Step 6 | write startup-config | Optional step – saves this IGMP snooping configuration to be part of the startup configuration. |
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.

10.14 IGMP Snooping Configuration Example

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

- Enable IGMP snooping.
- There is no multicast router for group 225.0.0.1 so configure the switch as a querier for this group.
- Use IGMP v2 for group 225.0.0.1 and also enable fast leave since hosts are directly connected to the switch.
- Disable the proxy reporting.
- 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 0/20-28
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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted

interface port-channel 1
exit vlan 1

ports fx 0/11-19 untagged
ports cx 0/2 untagged
exit

vlan 10

ports fx 0/20-28 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 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
noip igmp snooping proxy-reporting
vlan 20
ip igmp snooping fast-leave
ip igmp snooping version v2
ip igmp snooping querier
exit
SMIS#
SMIS# ship 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 thisport channel configuration.
SMIS# write startup-config
Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS#
11 ACL

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 Layer 3 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 ACL, that packet will be handled according to the matched ACL configured action.

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 ACL and Layer 3 IP ACL 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 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 it 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 Layer 2 ACL table and Layer 3 ACL table 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.

11.1 Types of ACLs

Supermicro switches support the following three different types of ACLs.
### 11.1.1 MAC Extended ACL

A MAC Extended ACL allows users to control the traffic based on fields in Ethernet MAC and VLAN headers.

Users can configure the traffic flow based on 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.

### 11.1.2 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 source IP address and destination IP address.

Users can choose to deny, redirect or permit the configured traffic flow using an IP Standard ACL.

### 11.1.3 IP Extended ACL

An IP Extended ACL allows users to control the 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.

### 11.2 MAC Extended ACL

Supermicro switches support up to 128 MAC Extended ACLs.

Users can define a MAC Extended ACL with a deny, permit or redirect action rule. A MAC Extended ACL can be defined 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. The higher priority ACL rules take 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.

### 11.2.1 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, 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

11.2.2 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

11.2.3 Removing MAC Extended ACLs
Follow the steps below to remove MAC Extended ACLs.
### 11.2.4 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.

### 11.2.5 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 &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 on which this MAC Extended ACL needs to be applied.</td>
</tr>
<tr>
<td>Step 3</td>
<td>mac access-group { &lt;short (1-32768)&gt;</td>
<td>&lt;string(32)&gt; }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-number – the ACL number that needs to be added</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-name – the name of the ACL that needs to be added</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
<td>Displays the configured ACL rules to make sure this port is added to the required ACL.</td>
</tr>
</tbody>
</table>
**Step 5** | **Command** | **Description**  
---|---|---  
**Step 5** | write startup-config | Optional step – Saves this ACL configuration to be part of startup configuration.  

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><strong>Step</strong></th>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></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>` ... | The port or port lists from which this MAC Extended ACL needs to be removed. |
| **Step 3** | no mac access-group { <short (1-32768)> | <string(32)> } | 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. |
| **Step 4** | show access-lists | Displays the configured ACL rules to make sure this port is removed from required ACL. |
| **Step 5** | write startup-config | Optional step – Saves this ACL configuration to be part of startup configuration. |

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, 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

### 11.2.6 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 or show access-lists mac { &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 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 case of configuration errors, the ACL status may be inactive.

The below example displays a MAC Extended ACL
SMIS# show access-lists mac 100

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

11.2.7 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

ACL 1 Configuration
SMIS# configure terminal
SMIS(config)# mac access-list extended 1
SMIS(config-ext-macl)# deny host 00:25:90:01:01:0a host 00:25:90:01:01:0b

ACL 2 Configuration
SMIS# configure terminal
SMIS(config)# mac access-list extended 2
11.3 **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 only with 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 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 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 string.

---

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.

User can associate a priority values 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. The higher priority ACL rules take 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.

---

The priority for IP standard ACL rule “deny any any” is fixed as 1. User cannot configure “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 with the consideration of both IP standard and extended ACLs.
11.3.1 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>
<tr>
<td>Step 3</td>
<td>deny { any</td>
<td>host&lt;ucast_addr&gt;</td>
</tr>
<tr>
<td>or</td>
<td>permit { any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td>or</td>
<td>redirect&lt;interface-type&gt;&lt;interface-id&gt; { any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
<td>Displays the configured ACL rule</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>

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
```

### 11.3.2 Modifying IP Standard ACLs

To modify a configured IP Standard ACL, follow the same steps used to create an 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
```

Page 235 of 371
11.3.3 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>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

11.3.4 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.

11.3.5 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>
</tbody>
</table>
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>&lt;access-list-name&gt; } ]</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, 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. Same way many IP Standard / Extended ACLs can be applied on a single port.

The example below shows the commands 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

11.3.6 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</td>
<td>Enters the configuration mode</td>
</tr>
<tr>
<td></td>
<td>or show access-lists ip { &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 that needs to be displayed</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 |
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

11.3.7 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

### 11.3.8 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.

IP Standard ACLs and IP Extended ACLs share the same ACL table on the hardware. Hence priority values need to be configured with the consideration of both IP standard and extended ACLs.

### 11.3.9 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 Extended ACL 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

### 11.3.10 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></td>
<td></td>
<td>access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny tcp { any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
</tbody>
</table>

Configures a deny, permit or redirect ACL rule.

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.

To apply this rule to packets with specific TCP ports, users can configure either the source or destination TCP ports.
The specific TCP port is provided with the keyword eq.

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.
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 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 fx 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 eq 1000

### 11.3.11 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>permitudp { any</td>
<td>host&lt;src-ip-address&gt;</td>
</tr>
</tbody>
</table>

Configures a deny, permit or redirect ACL rule.

The source and destination IP addresses can be provided with the keyword host.
The keyword any can be used to refer to any IP addresses.
To configure a network IP, address and mask should be provided.

To apply this rule to packets with specific UDP ports, users can configure either the source or destination UDP ports.
The specific UDP port is provided with the keyword eq.

To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be
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)> } ] [ { eq<src-mask (0-63)> } ] [ { tos<value (0-255)> | dscp<value (0-63)> } ] [ { priority<short(1-255)> } ]

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 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

11.3.12 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&gt;(1-32768)&gt;</td>
<td>&lt;access-list-name&gt; }</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny icmp { any | host &lt;src-ip-address&gt;</td>
<td>&lt;src-ip-address&gt;&lt;mask&gt; } { any | host &lt;dest-ip-address&gt;</td>
</tr>
</tbody>
</table>
| | redirect<interface-type><interface-id>icmp \{ any \| host <src-ip-address> | <src-ip-address><mask> \} \{ any \| host <dest-ip-address> | <dest-ip-address><mask> \} \[<message-type (0-255)> \] \[<message-code (0-255)> \] \[priority\<(1-255)\> \] | Redirect ACL rules need additional `<interface-type>` `<interface-id>` parameters to define the port to
### 11.3.13 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.

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 Extended ACL rule 100 being created and then modified with different parameters.

SMIS# configure terminal

SMIS(config)# ip access-list extended 50

SMIS(config-ext-nacl)# redirect fx 0/10 icmp 172.20.20.0 255.255.255.0 host 172.20.0.1 3

---

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show access-lists</th>
<th>which the packets matching this ACL rule need to be redirected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>write startup-config</td>
<td>To display the configured ACL rule Optional step – Saves this ACL configuration to be part of startup configuration.</td>
</tr>
</tbody>
</table>
SMIS(config-ext-nacl)# deny icmp any 172.10.0.0 255.255.0.0

# 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

### 11.3.14 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></td>
<td></td>
<td>access-list-number – the ACL number that needs to be deleted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 Extended ACL.

SMIS# configure terminal

SMIS(config)# no ip access-list extended 50

### 11.3.15 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.

### 11.3.16 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>
<tr>
<td></td>
<td></td>
<td>access-list-number – the ACL number that needs to be displayed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access-list-name – the name of the ACL that needs to be displayed</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 active 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
ICMP type Displays ICMP types if the ACL is applied only to particular ICMP messages.
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Priority</td>
<td>1</td>
</tr>
<tr>
<td>Filter Protocol Type</td>
<td>ANY</td>
</tr>
<tr>
<td>Source IP address</td>
<td>172.10.10.10</td>
</tr>
<tr>
<td>Source IP address mask</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Destination IP address mask</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>In Port List</td>
<td>ALL</td>
</tr>
<tr>
<td>Out Port</td>
<td>ALL Filter TOS</td>
</tr>
<tr>
<td>Filter DSCP</td>
<td></td>
</tr>
<tr>
<td>Filter Action</td>
<td>Deny</td>
</tr>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
</tbody>
</table>

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 : Filter DSCP :
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

11.4 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.

Figure ACL-3: IP Extended ACL Example 1

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

12 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 an equal 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 per-hop behavior. All devices along a network path must provide a consistent per-hop behavior in an end-to-end QoS solution.

![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>
12.1 Policy-Based QoS
Supermicro switch features based on QoS Policies are:

- QoS Classification
- Marking
- Policing

12.1.1 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.

12.1.1.1 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 policy map. 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.
12.1.1.2 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.

12.2 CoS-Based QoS

Supermicro switch features based on Class of Service (CoS) are:

- Queuing
- Scheduling
- Bandwidth Management
- Default Priority

12.2.1 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.

![Figure QoS-3: Egress Queuing](image)

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 queue mapping 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.

### 12.2.2 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.

### 12.2.3 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.

<table>
<thead>
<tr>
<th>CoS Priority</th>
<th>CFI</th>
<th>VLAN ID</th>
</tr>
</thead>
</table>

**Figure QoS-4: VLAN Tag and CoS Priority**

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.

12.2.4 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.

12.3 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.

12.4 HOLBlocking 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 over-subscription 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.

12.5 Enabling QoS
QoS is disabled by default in Supermicro switches. Follow the below steps to enable QoS.
### 12.6 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. &lt;br&gt; 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>
<tr>
<td>Step 3</td>
<td>class-map &lt;class-map-number(1-65535)&gt;</td>
<td>Creates a class map and enters the class-map configuration mode. &lt;br&gt; <em>class-map-number</em> - QoS class map number in range from 1-65535.</td>
</tr>
</tbody>
</table>
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 match criteria.

- **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

Step 5  Exit

Exits the classmap configuration mode.

Step 6  policy-map <policy-map-number(1-65535)>

Creates a policy map and enters the policy-map configuration mode.

- **policy-map-number**: QoS policy map number

Step 7  class <class-map-number(1-65535)>

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.

- **class-map-number**: The class map number to associate the policy, in range of 1-65535

Step 8  set {cos<new-cos(0-7)> | ipdscp<new-dscp(0-63)> | ip precedence <new-precedence(0-7)>}

(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.

- **cos**: New COS value assigned to the classified traffic, in range of 0-7
- **ipdscp**: New DSCP value assigned to the classified traffic, in range of 0-63
- **ip precedence**: New IP-precedence value assigned to the classified traffic, in range of 0-7
Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<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>exceed-action {drop</td>
<td>policed-</td>
</tr>
<tr>
<td>dscp-transmit &lt;new-dscp(0-63)&gt;</td>
<td></td>
</tr>
</tbody>
</table>

rate-kbps - Average traffic rate in kilobits per second (Kbps), in range 64-1048572

Step 10

End

Exits the configuration mode.

Step 11

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show class-map [&lt;class-map-</td>
<td>Displays the classmap configuration.</td>
</tr>
<tr>
<td>num(1-65535)&gt;]</td>
<td></td>
</tr>
<tr>
<td>show policy-map [&lt;policy-map-</td>
<td>Displays the policy map configuration.</td>
</tr>
<tr>
<td>num(1-65535)&gt; [class &lt;class-map-</td>
<td></td>
</tr>
<tr>
<td>num(1-65535)&gt;]</td>
<td></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 “class-map” 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 in
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 in
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...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp

username ADMIN password 0509040770 privilege 15 admin encrypted

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 in
mac access-group mac2 in

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

setcos 6

exit

exit

policy-map 10

class 10

setcos 7

exit

exit

**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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted
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

12.7 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>
</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><code>vlan map-priority &lt;priority value(0-7)&gt;, traffic-class &lt;Traffic class value(0-7)&gt;</code></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><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>(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, 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To provide a range use a hyphen (-) between the start and end interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 (,).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>switchport priority default &lt;priority value(0-7)&gt;</code></td>
<td>(Optional) Configures the default priority for the interface in range of 0-7.</td>
</tr>
<tr>
<td>Step 5</td>
<td>`cosq scheduling algorithm { strict</td>
<td>rr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>strict - strict</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rr - round robin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wrr - weighted round robin (WRR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>deficit – deficit WRR</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>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;]</code></td>
<td>(Optional) Configures the egress queue minimum and maximum bandwidth.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>weight - Configures the queue weights in range of 0-15</td>
</tr>
</tbody>
</table>
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

---

Step 7: End

Exits the configuration mode.

Step 8: show vlan port config port [<interface-type><interface-id>]
show vlan traffic-classes

Displays the port default priority configuration.
Display the traffic class and egress queue mapping.

---

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 Fx0/10
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

------------------------
Interface    Algorithm


<table>
<thead>
<tr>
<th>Port</th>
<th>Priority</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>
<tr>
<td>Fx0/12</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/13</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/14</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/16</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/17</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/18</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/19</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/20</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/21</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/22</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/23</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Fx0/24</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Cx0/1</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Cx0/2</td>
<td>StrictPriority</td>
</tr>
<tr>
<td>Cx0/3</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>Fx0/15</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>6</td>
<td>7</td>
<td>6400</td>
<td>6400000</td>
</tr>
<tr>
<td>Fx0/15</td>
<td>7</td>
<td>1</td>
<td>0</td>
<td>0</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>
13 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.

13.1 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>

13.2 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; source</td>
<td>Configure Port Mirroring</td>
</tr>
<tr>
<td></td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt;</td>
<td>session_number – 1, indicates only one session is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination – Monitoring Port.</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>
<tr>
<td></td>
<td></td>
<td>NOTE: Source and Destination port cannot be same.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Monitor session &lt;session number: 1-4&gt; source</td>
<td>Configure Port Mirroring</td>
</tr>
<tr>
<td></td>
<td>interface &lt;interface-type&gt; &lt;interface-id&gt; {rx</td>
<td>session_number – 1, indicates only one session is supported.</td>
</tr>
<tr>
<td></td>
<td>tx</td>
<td>both}</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>show port-monitoring</td>
<td>Displays the port monitoring 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>

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.

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 cannot 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 0/2` ...

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 deletes 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 0/28
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 : Fx0/28

<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>
</tbody>
</table>
```
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.

<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>
</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>

**14.1 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.

**14.2 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>Fx-ethernet physical</td>
<td>Starts from 1 and goes up to the maximum number of Fx-ethernet interfaces available on the switch. 1 to 28 for SBM-25G-100 and 1 to 56 for MBM-XEM-100.</td>
</tr>
<tr>
<td>interfaces</td>
<td></td>
</tr>
<tr>
<td>Cx-ethernet physical</td>
<td>Starts after 25Gig ifIndexes and goes up to the maximum number of 100 Gig interfaces available on the switch. 29 to 32 for SBM-25G-100 and 57 to 60 for MBM-XEM-100.</td>
</tr>
</tbody>
</table>
14.3 **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.
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.

14.3.1 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).

14.4 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,</td>
</tr>
</tbody>
</table>
### 14.5 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  \textbf{write startup-config} \quad \text{Optional step – saves this SNMP configuration to be part of the startup configuration.}

The “\texttt{enable snmpagent}” command enables the SNMP agent.

To enable the SNMP agent, it must be in the disabled state. The SNMP subagent is disabled by default. If needed, use the command “\texttt{disable snmpsubagent}” to disable the SNMP subagent feature.

The examples below show ways to disable/enable the SNMP agent function on Supermicro switches.

\textbf{Disable the SNMP agent.}

\begin{verbatim}
SMIS# configure terminal
SMIS(config)# disable snmpagent
SMIS(config)# end
\end{verbatim}

\textbf{Enable the SNMP agent.}

\begin{verbatim}
SMIS# configure terminal
SMIS(config)# enable snmpagent
SMIS(config)# end
\end{verbatim}

\textbf{14.5.1 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>
<tr>
<td>Step 2</td>
<td>device name &lt;devname(15)&gt;</td>
<td>Configures switch name and prompt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Devname – Switch name specified with 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>
<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 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
```

### 14.5.2 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>
</tbody>
</table>
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  
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  
=================== ========  
Time zone offset not set

14.5.3 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>
</tbody>
</table>
### Configuration Guide

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td><code>system location &lt;location name&gt;</code></td>
<td>Configures the system location. <code>location name</code> – Location of the switch specified as a string with a maximum size of 256.</td>
</tr>
<tr>
<td>3</td>
<td><code>End</code></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td><code>show system information</code></td>
<td>Displays the system information configuration.</td>
</tr>
<tr>
<td>5</td>
<td><code>write startup-config</code></td>
<td>Optional step – saves this configuration to be part of the startup configuration.</td>
</tr>
</tbody>
</table>

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

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
[NTP] ntp is disabled
Server Key Prefer
=============== ===== ========
Key # Key
======== =======================
Time zone offset not set
```
14.6 Access Control
There are various parameters that control access to the SNMP Agent.

- Engine ID
- Community String
- User
- Group
- Group Access

14.6.1 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. <strong>EngineIdentifier</strong>-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.

14.6.2 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 255 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 40 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name –Alphanumeric value with a maximum of 40 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 255 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.

```plaintext
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
```

14.6.3 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 40 characters.
- Use `auth` to enable authentication for the user.
- **Passwd** – Password used for user Authentication. Alphanumeric value with a maximum of 40 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.

```sh
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

-----------------------------------------------

14.6.4  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>
</tbody>
</table>

GroupName – Alphanumeric value with a maximum of 40 characters.

Security-model – Use v1 or v2c or v3.

UserName - Alphanumeric value with a maximum of 40 characters.
<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 group</strong></td>
<td>Displays the SNMP group 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 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
```
### 14.6.5 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>
</tbody>
</table>
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>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>show snmpviewtree</strong></td>
</tr>
<tr>
<td></td>
<td>Displays the SNMP view information.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>write startup-config</strong></td>
</tr>
<tr>
<td></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

14.6.6 **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><code>configure terminal</code></td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| Step 2 | `snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}[read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}]` | Configures the SNMP group access.  
*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. |
| Step 3 | `end` | Exits the configuration mode. |
| Step 4 | `show snmp group access` | Displays the SNMP group access information. |
| Step 5 | `write startup-config` | Optional step – saves this SNMP configuration to be part of startup configuration. |
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
```
14.7 Trap

14.7.1 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><code>configure terminal</code></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 40 characters.

*ParamName* – The parameter to be notified to the specific target. Alphanumeric value with a maximum of 40 characters.

*IPAddress* – IPv4 address of the target.

*IP6Address* – IPv6 address of the target.

*Seconds* – Specifies the timeout within which the target should be reachable.
### SNMP Configuration Guide

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><strong>end</strong></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>

**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.

---

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

---

"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.
### 14.7.2 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><code>configure terminal</code></td>
<td>Enters the configuration mode.</td>
</tr>
</tbody>
</table>
| 2 | `snmpargetparams<ParamName> user <UserName>security-model {v1 | v2c | v3 {auth | noauth | priv}}message-processing {v1 | v2c | v3} [{volatile | nonvolatile}]` | Configures the SNMP target parameters.  
  
  **ParamName** - The parameter to be notified. Alphanumeric value with a maximum of 40 characters.  
  
  **UserName** - Alphanumeric value with a maximum of 40 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. |
| 3 | `end` | Exits the configuration mode. |
| 4 | `show snmpargetparam` | Displays the SNMP target parameters information. |
| 5 | `write startup-config` | Optional step – saves this SNMP configuration to be part of the startup configuration. |
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.

```
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

-------------------------------------
```

14.7.3 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>
</tbody>
</table>
Step 2  
\texttt{snmp notify <NotifyName> tag <TagName> type \{Trap | Inform\}\{volatile | nonvolatile\}}

Configures the SNMP Notify information.

\textit{NotifyName} - Alphanumeric value with a maximum of 40 characters.

\textit{TagName} - Specifies a group of targets identified by this name. Alphanumeric value with a maximum of 255 characters.

Type – Notification can be Trap or Inform.

Use \texttt{volatile} if the value need not be stored in NVRAM.

Use \texttt{nonvolatile} if the value must be stored in NVRAM and available after restart.

Step 3  
\texttt{end}

Exits the configuration mode.

Step 4  
\texttt{show snmp notify}
\texttt{show snmp inform statistics}

Displays the SNMP notification information and Inform statistics.

Step 5  
\texttt{write startup-config}

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

---

The “\texttt{no snmp notify <NotifyName>}” command deletes the specified SNMP notification.

The example below shows the commands used to configure the SNMP notification.

\begin{verbatim}
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
\end{verbatim}
**14.7.4 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. 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.

14.7.5 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>
<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 enable traps snmp authentication</td>
<td>Enables the SNMP authentication traps.</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</td>
<td>Displays the SNMP 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 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-server traps

SNMP Trap Listen Port is 162
Currently enabled traps:
------------------------
linkup, linkdown,
Login Authentication Traps ENABLED.
14.7.6 **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><code>configure terminal</code></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>&lt;br&gt;or&lt;br&gt;<code>interface range &lt;interface-type&gt;&lt;interface-id&gt; ....</code></td>
<td>Enters the interface configuration mode. &lt;br&gt;interface-type – may be any of the following: &lt;br&gt;fx-ethernet – fx &lt;br&gt;cx-ethernet – cx &lt;br&gt;port-channel &lt;br&gt;interface-id is in slot/port format for all physical interfaces. &lt;br&gt;To configure multiple interfaces, use the “interface range ...” command.</td>
</tr>
</tbody>
</table>
Step 3 **no snmp trap link-status** Disables the SNMP link-state trap on the particular interface.

Step 4 **end** Exits the configuration mode.

Step 5 **show snmp** Displays the SNMP information.

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
```
<table>
<thead>
<tr>
<th>Error Packets : 0</th>
<th>Unknown Protocol : 0</th>
</tr>
</thead>
</table>

Transmission Counters

- Octets : 9043
- Unicast Packets : 0
- Non-Unicast Packets : 74
- Pause Frames : 0
- Discarded Packets : 0
- Error Packets : 0

### 14.8 SNMPConfigurationExample

![PC – SNMP Manager](image)

**Figure SNMP-2 – SNMP Configuration Example**

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...

<table>
<thead>
<tr>
<th>ID</th>
<th>Hardware Version</th>
<th>Firmware</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted
vlan 1
  ports fx 0/1-24 untagged
  ports cx 0/1-3 untagged
exit
15 RMON

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.
15.1 **RMON Groups**

Supermicro supports four groups from RMON MIB1 defined by RMON specifications: event group, alarm group, history group and statistics group.

15.1.1 **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.*
15.1.2 **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.

15.1.3 **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.

15.1.3.1 **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.

15.1.3.2 **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, undervalue/oversize packets, broadcasts, multicasts, bytes received, and packets received etc.

15.2 **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 statistics</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>

15.2.1 **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

### 15.2.2 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)}&lt;rising-event-number (1-65535)&gt; falling-threshold &lt;value (0-2147483647)}&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>
</tbody>
</table>
rising-threshold - A number at which the alarm is triggered. This value ranges between 0 and 2147483647.

falling-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 3) rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>] (Optional) Add an event in the RMON event table that is associated with an RMON event number.

Number - Event number

Description - Description of the event

Log - Used to generate a log entry

Owner - Owner of the event, , in range 1- 127 characters

Trap - Used to generate a trap. The SNMP community string is to be passed for the specified trap.

NOTE: When RMON event trap is enabled, SNMP agent must be configured prior to configuring the RMON alarm function as described in SNMP Configuration guide (www.supermicro.com).

(Step 4) end Exit from Configuration mode.
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.

15.2.3 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>
<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.</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>
</tbody>
</table>
### 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 1.3.6.1.6.3.16.1.2.1.4table.
4) Create statistics collection on an interface.
5) Display all RMON configurations.

This configuration can be executed using the following CLI commands:

```
SMIS# configure terminal
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>rmon collection stats &lt;index (1-65535)&gt; [owner &lt;ownername (127)&gt;]</code></td>
<td>(Optional) Enable RMON statistic collection on the interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>index - Statistics table index, in range 1-65535</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>4</td>
<td><code>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;]</code></td>
<td>(Optional) Enable history collection for the specified number of buckets and time period</td>
</tr>
<tr>
<td></td>
<td></td>
<td>index - History table index, in range 1-65535</td>
</tr>
<tr>
<td></td>
<td></td>
<td>buckets - The maximum number of buckets desired for the RMON collection history group of statistics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interval - The number of seconds in each polling cycle, in range 1-3600</td>
</tr>
<tr>
<td></td>
<td></td>
<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>
</tr>
<tr>
<td>5</td>
<td><code>show rmon [statistics [&lt;stats-index (1-65535)&gt;]] [alarms] [events] [history [history-index (1-65535)]] [overview]</code></td>
<td>Display RMON statistics, history and overview.</td>
</tr>
</tbody>
</table>

The “no rmon collection stats <index (1-65535)>” and “no rmon collection history <index (1-65535)>” commands delete the RMON collection configuration.
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 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
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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted
vlan 1
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 1.3.6.1.6.3.16.1.2.1.4.1.4.110.110.110.101 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

15.2.5 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 &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>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.</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td>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 &lt;rate-value-kbps (1-100000000)&gt;&lt;burst-value-kbits (1-10000000)&gt;</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.</td>
</tr>
<tr>
<td></td>
<td>Rate limit and burst size in range of 1-100000000.</td>
<td></td>
</tr>
</tbody>
</table>
Step 4
End
Exits the configuration mode.

Step 5
show interface [[ [interface-type]<interface-id>]]
rate-limit
Displays the rate limit configuration on an interface.

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.

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

15.2.6 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 [[ [interface-type]&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# 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

<table>
<thead>
<tr>
<th>Metric</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>Broadcast Packets</td>
<td>0</td>
</tr>
<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>Metric</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>
16 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.

16.1 Login Authentication Mode

Supermicro switches allow configuration of the user login authentication mechanism.

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</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 RADUIS server to authenticate users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tacacs – Use TACACS server to authenticate users.</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 mechanism.

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

16.2  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>
</tbody>
</table>
16.2.1 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>- ip-address – serverIP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- timeout – Specify RADIUS server timeout in range 1-120</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- retransmit – Specify number of retries to attempt to connect to RADIUS server in range 1-254</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- key – Specify authentication key</td>
</tr>
<tr>
<td>Step 3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show radius server</td>
<td>Displays the RADIUS configuration.</td>
</tr>
<tr>
<td></td>
<td>show radius statistics</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 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
No of pending requests : 0
No of time outs : 0
No of unknown types : 0

16.3 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>
16.3.1 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>
</tbody>
</table>
| Step 2 | tacacs-server host <ip-address> [single-connection] [port <tcp port (1-65535)>] [timeout <timeout out in seconds>] key <secret key> | Configure TACACS server.  
  *ip-address* – TACACS Server IP-address  
  *single-connection* – When this option is specified, only one connection to one of the configured TACACS servers is permitted.  
  *port* – Specify TCP port in range 1-65535  
  *timeout* - Specify TACACS server timeout in range 0 – 255 seconds  
  *key* – Authentication key of maximum length 64 characters. |
| Step 3 | End | Exits the configuration mode. |
| Step 4 | show tacacs | Displays the TACACS configuration. |
| 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
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

16.3.2 TACACS Re-tries
Supermicro switches retry transmission of messages to the TACACS server, if there is no response from the server. This retry count can be configured by user.

Follow the steps below to configure TACACS server re-tries.

<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: `tacacs-server retransmit <1-100>`
Configure TACACS server re-tries in the range 1-100.

Step 3: `End`
Exits the configuration mode.

Step 4: `show tacacs`
Displays the TACACS configuration.

Step 5: `write startup-config`
Optional step – saves this configuration to be part of startup configuration.

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
```

**16.3.3 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>
<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 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  
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  

16.3.4 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 rvcv. : 11
  Authen. Fails rvcv. : 3
  Authen. Get User rvcv. : 0
  Authen. Get Pass rvcv. : 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
16.3.5 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

16.3.6 TACACS Accounting

Supermicro switches provide an option to configure TACACS accounting feature.

By default, TACACS accounting is disabled. User can enable it using CLI command.

TACACS accounting feature can work independent of TACACS authentication and authorization. To use TACACS accounting, make sure to TACACS server settings are configured.

When TACACS accounting is enabled, for every CLI command executed in the switch, an accounting message with user name, privilege, time, remote system IP along with CLI command is sent to TACACS server.

Follow the steps below to enable the TACACS accounting.
### 16.3.7 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. There are many types of service used by different vendors on the market. For Supermicro switches the supported service type is ‘config’. E.g. user configuration in TACACS+ server: user = test15 { name = &quot;Test15 User&quot; pap = cleartext &quot;test15&quot; service = config { priv-lvl = 15 } }</td>
<td>This is an umbrella requirement to cover the functionality.</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. E.g. user configuration in TACACS+ server: user = test1 { name = &quot;Test1 User&quot; pap = cleartext &quot;test1&quot; }</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>This privilege function should be enabled only when user enables it in CLI, Web, and SNMP. For e.g. the new command “aaa authorization</td>
<td></td>
</tr>
</tbody>
</table>
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

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.

### 16.4 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>1</td>
<td>configure terminal</td>
<td>Enters the configuration mode</td>
</tr>
</tbody>
</table>
| 2    | ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>)       | versioncompatibility- Specify whether switch should process both version 1 and version 2 SSL messages.  
  
cipher – Specify the encryption algorithm.  
  
  auth – Specify the authentication algorithm.  
  
  port - Specify SSH port in range 1024-65535 |
<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 ip ssh</td>
<td>Displays the SSH 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 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
```
16.5 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>

16.5.1 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>
<tr>
<td>Step 2</td>
<td>ip http secure { server</td>
<td>ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha] [dh-rsa-3des-sha]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server -- Enables HTTPS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ciphersuite -- Specify one or many of the supported encryption algorithm to be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>crypto key rsa -- Encryption Key, either 512 or 1024.</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 http secure server status</td>
<td>Displays the SSL 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 Secure HTTP.

SMIS# configure terminal
SMIS(config)# no ip http secure server
SMIS(config)# end

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.
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

16.5.2 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).&lt;br&gt;&lt;br&gt;<strong>SubjectName</strong> – Switch ID or IP-address.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show ssl server-certs</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-----
MIIBTjCbuAIBADAPMQ0wCwYDVQQDEwRTTUlTMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQChj0JzVX1/gZ4SMGekRdrsAnftWnKHG3VypWTtySqvkvTwhnZ2o6Q2o
ADCBiQKBgQChj0JzVX1/gZ4SMGekRdrsAnftWnKHG3VypWTtySqvkvTwhnZ2o6Q2o
cBYJKY4ZCykOxG81mfUhqPfVLy08sbK+RYzEeTMX9lw9iq9yOySolvxY6IoYNsg
O++J502khz0SAbpRkhtGwumBiZQtSj+8Ea3dG8ReoiwpYDvVdlRQIADQABoAAw
DQYJKoZlhcNAQEEBAQADBgYEARK8Nz40QeC8wqwzqy+i0zT5iUMK0keIYTE8mDydt
AvRyc7a3EPraGyOL5W1H94z+wW2wksXRzkuLzAEYRH9f84XB2uCAdl+jkuSBjc
5qd3j4yBtofLu/pXosdKKwuq6LWbi4DCXg9YtE+pOya7nWojVkc2sbvK5CTgG
89s=
-----END CERTIFICATE REQUEST-----
SMIS# show ssl server-certificate

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
### 16.5.3 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>
<tr>
<td>Step 4</td>
<td>Linux commands</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute the below commands in linux shell.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CAkey cakey.pem -Cacreatesarial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This would generate certificate file cert.pem.</td>
</tr>
<tr>
<td>Step 5</td>
<td>ssl server-cert</td>
<td>Open the generate certificate file cert.pem. Delete first line (---BEGIN</td>
</tr>
</tbody>
</table>
| 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.

This step would configure the certificate and save it to flash.

| Step 6 | show ssl server-cert | Displays the SSL configuration. |
17 LLDP

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>
</table>
LLDP Status (global) | Disabled
---|---
LLDP Status (interface level) | Transmit and receive
TLV | None
HoldtimeMultiplier | 4
Message Transmit Interval | 30
ReinitializationDelay | 2
Transmit Delay | 2
Trap Notification Interval | 5
Chassis ID | Switch MAC address
Chasis ID Subtype | MAC address
Port ID Subtype | Interface name
System Capabilities | None
Notification | Disabled
Notification Type | Mis-configuration

### 17.1.1 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.

### 17.1.2 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 <code>&lt;interface-type&gt;</code>&lt;<code>interface-id&gt;</code> or interface range <code>&lt;interface-type&gt;</code>&lt;<code>interface-id&gt;</code> ....</td>
<td>(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 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Step 3</td>
<td>lldp {transmit</td>
<td>receive}</td>
</tr>
<tr>
<td>Step 5</td>
<td>lldp port-id-subtype { if-alias</td>
<td>port-comp &lt;string(255)&gt;</td>
</tr>
<tr>
<td>Step</td>
<td>Command/Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>6</td>
<td>Exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>7</td>
<td>`lldp chassis-id-subtype { chassis-comp &lt;string(255)&gt;</td>
<td>if-alias</td>
</tr>
<tr>
<td></td>
<td>(Optional)</td>
<td>Configures LLDP chassis ID subtype and chassis ID value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>chassis-comp - chassis component</td>
</tr>
<tr>
<td></td>
<td></td>
<td>if-alias - management interface alias</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port-comp - port component</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mac-addr - MAC address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nw-addr - network address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>if-name - interface name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>local - locally assigned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value for chassi-id-subtype is mac-addr.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: To use the if-alias option, the management interface must have been configured with valid description.</td>
</tr>
<tr>
<td>8</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td><code>show lldp interface [&lt;interface-type&gt;&lt;interface-id&gt;]</code></td>
<td>Displays LLDP configuration details on a particular interface or all interfaces</td>
</tr>
</tbody>
</table>
show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [interface-type<interface-id>][detail]

show lldp traffic [<iftype><ifnum>]

show lldp errors

show lldp statistics

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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}
nolldp notification
nolldp-tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}
nolldp-tlv-select dot1tlv { [port-vlan-id] [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}]}
nolldp-tlv-select dot3TLV { [macphy-config] [link-aggregation] [max-framesize] }

### 17.1.2.1 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.

**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

<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.</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 (-)
### Step 3

**lldptlv-select basic-tlv**

```
(port-descr) [sys-name]
(sys-descr) [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}
```

(Optinal)

- 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-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

**lldptlv-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

- `port-vlan-id` - Port VLAN identifier TLV. The keyword `port-vlan-id` keyword is not supported.
17.1.3 Configuring LLDP Timers

Supermicro switches allow for user configuration of LLDP timers:

- Transmit Interval
- Holdtime Multiplier
- ReinitializationDelay
- Transmit Delay
- Notification Delay

17.1.3.1 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)</td>
</tr>
</tbody>
</table>
Configure the message transmit interval, range of 5-32768.

Step 3: End

Exits the configuration mode.

Step 4: show lldp

Displays the LLDP global information.

The “no lldp transmit-interval” command resets the message transmit interval to its default value.

17.1.3.2 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 ((Transmission Interval * Holdtime Multiplier), or 65536)

The default holdtime multiplier is 4 seconds. The default TTL is: 4*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.

17.1.3.3 ReinitializationDelay

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>
</tbody>
</table>

Page 360 of 371
17.1.3.4 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; (Optional)</td>
<td>Configures the message transmit delay, range of 1-8192. NOTE: The Txdelay should be less than 0.25 * message Txinterval</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.

17.1.3.5 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>lldpreinitialization-delay &lt;seconds(1-10)&gt; (Optional)</td>
<td>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.
<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>lldp notification-interval</td>
<td>(Optional) Configures the notification interval,</td>
</tr>
<tr>
<td></td>
<td>&lt;seconds(5-3600)&gt;</td>
<td>range of 5-3600.</td>
</tr>
<tr>
<td>3</td>
<td>End</td>
<td>Exits the configuration mode.</td>
</tr>
<tr>
<td>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.

17.1.4 LLDP Configuration
The example below shows the commands used to configure LLDP by connecting two switches: Switch A and Switch B.

![Switch A](attachment:image1.png)  
![Switch B](attachment:image2.png)

**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

**Switch B**
Fx 0/21
Fx 0/22

**Figure LLDP-3: LLDP Configuration Example**
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)# lldp preinitialization-delay 5
SMIS(config)# lldp preinitialization-delay 9
SMIS(config)# lldp preinitialization-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)# lldpport-select basic-tlv port-descrmgmt-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)# lldptlv-select dot1tlv vlan-name 1
SMIS(config-if)# lldptlv-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></td>
<td>Fx0/22</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
Capacity & 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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp

username ADMIN password 0509040770 privilege 15 admin encrypted

vlan 1

ports fx 0/1-24 untagged

ports cx 0/1-3 untagged

name vlan1

exit

setLldp enable

lldp transmit-interval 10

lldpholdtime-multiplier 7

lldpreinitialization-delay 10

lldp notification-interval 100

lldp chassis-id-subtype if-name

interface Fx 0/21

lldp notification remote-table-chg

lldptlv-select basic-tlv port-descrmgmt-addr all

lldptlv-select dot3tlv macphy-config

lldptlv-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

Chassis ID Local Intf Hold-time Capability Port Id
---------- ----------- ------- --------- -------
00:30:48:e3:04:75 Fx0/22 120 Fx0/21

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

Protocol VLAN Id Support Protocol VLAN Status TxStatus
------------------ ------ --------------------- -----
0 Supported Enabled Disabled
- Vlan Name

<table>
<thead>
<tr>
<th>Vlan Id</th>
<th>Vlan Name</th>
<th>TxStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<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>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SBM-25G-100 (B8 R1.01)</td>
<td>1.0.2.0</td>
<td>1.0.6</td>
</tr>
</tbody>
</table>

ip address dhcp
username ADMIN password 0509040770 privilege 15 admin encrypted

vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit
set lldp enable