



SBM-25G-100 MBM-XEM-100

Switch Configuration User's Guide

Revision 1.7

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 1.7
Release Date: 01/10/2024

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 © 2024 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

1 Document Revision History

Date	Revision	Description
02/12/2018	1.0	Initial document.
10/05/2018	1.1	Updated ACL configuration details. Added port splitting details.
02/20/2019	1.2	Added loop protection in System Configuration section and unknown Multicast Filtering in IGMP Snooping section.
03/06/2019	1.3	Updated for software release 1.1.0.0. Updated Section 3 Introduction to add terminal settings configuration and CLI grep option. Added “show chassis info” command to Section 3 Introduction. Added TACACS accounting subsection under TACACS configuration section in Security section 15.
12/05/2019	1.4	Updated default unique password. Added L2 ECMP load balancing details.
09/23/2020	1.5	Updated SSH, SSL configurations and reset-to-factory-defaults command. Added HTTP/HTTPS enable/disable, show RESTCONF status, copy debug files, show blade interfaces, debug and mgmt-vlan commands. Removed HTTPS cipher commands.
03/19/2021	1.6	Added telnet enable/disable, show mgmt. status and show ip http statistics commands.
01/10/2024	1.7	Added Password policy, logging configuration and clear user sessions sections were added.

2 Contents

3	Introduction	14
3.1	Command Line Interface	14
3.1.1	Terminal Settings	14
3.1.2	Grep option	15
3.1.3	Console Port	16
3.2	Blade Chassis	17
4	System Configurations	19
4.1	Management IP	19
4.1.1	Static Management IP Address	19
4.1.2	DHCP	19
4.1.3	Default IP Gateway	20
4.1.4	VLAN Tagging On Management Interface	21
4.2	Management Access	22
4.2.1	User login	22
4.2.2	Enable	23
4.2.3	Enable Password	23
4.2.4	WEBUI	24
4.2.5	RESTCONF	26
4.2.6	Telnet	26
4.2.7	Display the status of management access	27
4.2.8	IP Authorized Manager	28
4.2.9	Password Policy	29
4.2.10	Clear User Sessions	31
4.3	Interface Properties	31
4.3.1	Interfaces in SBM-25G-100	31
4.3.2	Interfaces in MBM-XEM-100	32
4.3.3	Description	34
4.3.4	Negotiation	36
4.3.5	Speed	39

SBM-25G-100 / MBM-XEM-100 Configuration Guide

4.3.6	Duplex Operation	41
4.3.7	MTU.....	41
4.3.8	Flow control	44
4.3.9	Storm control	46
4.3.10	Forward Error Correction (FEC) Mode	47
4.3.11	Port Splitting.....	48
4.4	Time Management.....	50
4.4.1	NTP server	50
4.4.2	Enable/Disable NTP.....	51
4.4.3	NTP authentication	52
4.4.4	NTP broadcast	53
4.4.5	System clock.....	54
4.4.6	Timezone	54
4.5	System Management	56
4.5.1	Switch Name	56
4.5.2	Switch contact.....	57
4.5.3	System location	58
4.5.4	System MTU	60
4.5.5	Static MAC.....	62
4.5.6	MAC aging	63
4.6	System Logging (Syslog)	64
4.6.1	Enable/Disable Syslog	65
4.6.2	Syslog server.....	66
4.6.3	Console Log	67
4.6.4	Logging Configuration	67
4.6.5	Log file	68
4.6.6	Logging Buffer	70
4.6.7	Facility	71
4.6.8	Trap	72
4.6.9	Clear Log buffer	74
4.6.10	Clear Log File	74
4.7	Configuration Management.....	75

SBM-25G-100 / MBM-XEM-100 Configuration Guide

4.7.1	Save Startup-Config.....	75
4.7.2	Save Running Configuration To File	76
4.7.3	Configuring Startup config file name	77
4.7.4	Copy Startup-config.....	78
4.7.5	Copy file.....	78
4.7.6	Copy debug files	79
4.7.7	Deleting Saved Configuration.....	79
4.7.8	Firmware upgrade	80
4.7.9	Boot-up options	80
4.7.10	Reset to Factory Defaults	81
4.8	Zero Touch Provisioning.....	84
4.8.1	ZTP Config Restore	84
4.8.2	ZTP Info.....	87
4.8.3	ZTP Firmware Upgrade.....	87
4.8.4	Disable ZTP	90
4.8.5	DHCP Vendor Class.....	90
4.9	Tracking Uplink Failure.....	91
4.10	Loop Protection.....	92
4.10.1	Defaults	92
4.10.2	Enable Loop Protection	92
4.10.3	Disable Loop Protection	92
5	VLAN.....	94
5.1	VLAN Basics	94
5.2	VLAN Support	94
5.3	VLAN Numbers	97
5.4	VLAN Defaults	97
5.5	Creating VLANs.....	98
5.6	Removing VLANs	98
5.7	VLAN Name	99
5.8	Port Based VLANs.....	101
5.8.1	Access Ports.....	101
5.8.2	Trunk Ports	103

SBM-25G-100 / MBM-XEM-100 Configuration Guide

5.8.3	Hybrid Ports.....	110
5.9	MAC Based VLANs	114
5.10	Protocol Based VLANs	116
5.11	Acceptable Frame Types	120
5.12	Ingress Filter	122
5.13	VLAN Configuration Example	123
5.14	Private Edge VLAN / Protected Ports	130
5.14.1	Unprotected Port	130
5.14.2	Protected Port	130
5.14.3	Community Port	130
5.15	Unprotected Ports configuration	130
5.16	Protected Ports configuration.....	131
5.17	Community Ports configuration.....	131
5.17.1	Configuration Example 1	131
5.17.2	Configuration Example 2	132
6	Link Aggregation.....	134
6.1	Link Aggregation Support.....	135
6.2	Link Aggregation Numbers	135
6.3	Link Aggregation Defaults	135
6.4	Static Link Aggregation.....	135
6.5	Dynamic Link Aggregation - LACP	136
6.6	Link Aggregation Port Channel.....	137
6.6.1	Creating Port Channels.....	137
6.6.2	Modifying Port Channels.....	142
6.6.3	Removing Port Channels	146
6.6.4	LACP Parameters	148
6.6.5	Load Balancing	155
6.6.6	Link Aggregation Configuration Example	158
7	Layer-2 ECMP Load Balancing	164
7.1	Configurations	164
8	MLAG.....	166
8.1	Overview	166

SBM-25G-100 / MBM-XEM-100 Configuration Guide

8.1.1	Terminologies.....	166
8.2	Topologies.....	167
8.2.1	Topology 1 - Server to switch MLAG topology.....	167
8.2.2	Topology 2 - Switch to switch MLAG topology	168
8.2.3	Topology 3 - Single uplink switch topology.....	169
8.2.4	Topology 4 – Redundant uplink switch topology.....	170
8.3	Default Configuration.....	171
8.4	MLAG Configurations	171
8.4.1	MLAG System ID.....	171
8.4.2	MLAG System Priority	172
8.4.3	Keep Alive Time.....	173
8.4.4	IPL Interface	174
8.4.5	MLAG Port Channels	175
8.4.6	Other configurations.....	175
9	Spanning Tree.....	177
9.1	Root Switch Election Procedure.....	178
9.2	Spanning Tree Support.....	179
9.3	Spanning TreeDefaults	179
9.4	Enabling/ Disabling Spanning Tree.....	180
9.4.1	Enable / Disable Spanning Tree Globally.....	180
9.4.2	Enable / Disable Spanning Tree on Ports	180
9.5	Configuring MST.....	182
9.6	Configuring MST region and instances.....	183
9.7	Configuring RSTP	184
9.8	Spanning Tree Compatibility	185
9.9	Configuring Root Switch (or) Priority	186
9.10	Port Priority.....	187
9.11	Path Cost	189
9.12	Hello Time	191
9.13	Max Age.....	193
9.14	Forwarding Time	194
9.15	Max Hops	195

SBM-25G-100 / MBM-XEM-100 Configuration Guide

9.16	Path Cost Long / Short	196
9.17	Transmit Hold Count	197
9.18	Root Guard	198
9.19	Topology Change Guard	199
9.20	Port Fast	201
9.21	Auto Edge	202
9.22	Link Type	203
9.23	Spanning Tree Configuration Examples	205
10	IGMP Snooping.....	210
10.1	IGMP Snooping Support.....	211
10.2	Enabling IGMP Snooping	212
10.3	IGMP Version	213
10.4	Multicast Router Ports	214
10.4.1	Router Port Timeouts	214
10.4.2	Static Router Ports	215
10.5	Leaving a Multicast Group	216
10.5.1	Group Query Interval	216
10.5.2	Group Query Retry Count	217
10.5.3	Immediate Leave	218
10.6	IGMP Snooping Querier	219
10.7	Report Forward	221
10.8	Port Timeout (Port Purge Interval)	222
10.9	Report Suppression Interval.....	223
10.10	Proxy Reporting.....	224
10.11	Sending Queries whenTopology Changes.....	225
10.12	Disabling IGMP Snooping	225
10.13	Unknown Multicast Filtering.....	226
10.14	IGMP Snooping Configuration Example	227
11	ACL.....	235
11.1	Types of ACLs	235
11.1.1	MAC Extended ACL.....	236
11.1.2	IP Standard ACL	236

SBM-25G-100 / MBM-XEM-100 Configuration Guide

11.1.3	IP Extended ACL	236
11.2	MAC Extended ACL.....	236
11.2.1	CreatingMAC Extended ACLs.....	237
11.2.2	Modifying MAC Extended ACLs.....	239
11.2.3	Removing MAC Extended ACLs	239
11.2.4	Applying MAC Extended ACLs to Interfaces.....	240
11.2.5	ACL Ingress Port Configuration	240
11.2.6	Displaying MAC Extended ACLs.....	242
11.2.7	MAC Extended ACL Configuration.....	243
11.3	IP Standard ACL	244
11.3.1	Creating IP Standard ACLs	245
11.3.2	Modifying IP Standard ACLs	246
11.3.3	Removing IPStandard ACLs	247
11.3.4	Applying IP ACLs to Interfaces.....	247
11.3.5	ACL Ingress Port Configuration	247
11.3.6	Displaying IP Standard ACLs	249
11.3.7	IP Standard ACL Configuration Example 1	250
11.3.8	IP Extended ACLs.....	251
11.3.9	Creating IP Extended ACLs for IP Traffic.....	252
11.3.10	Creating IP Extended ACLs for TCP Traffic.....	254
11.3.11	Creating IP Extended ACLs for UDP Traffic.....	256
11.3.12	Creating IP Extended ACLs for ICMP Traffic	258
11.3.13	Modifying IP Extended ACLs.....	259
11.3.14	Removing IP Extended ACLs.....	260
11.3.15	Applying IP Extended ACLs to Interfaces.....	260
11.3.16	Displaying IP Extended ACLs	260
11.4	IP Extended ACL Configuration Example 1.....	263
12	QoS	265
12.1	Policy-Based QoS.....	267
12.1.1	Classification and Marking	267
12.2	CoS-Based QoS	268
12.2.1	Egress Queuing.....	268

SBM-25G-100 / MBM-XEM-100 Configuration Guide

12.2.2	Scheduling	269
12.2.3	Default Priority	269
12.2.4	Bandwidth Management	270
12.3	Port-Based Rate Limit.....	270
12.4	HOLBlocking Prevention.....	270
12.5	Enabling QoS	270
12.6	ConfiguringPolicy-Based QoS	271
12.7	Configuring CoS-Based QoS.....	279
13	Port Mirroring	286
13.1	Port Mirroring Defaults	286
13.2	Configure Port Mirroring in CLI	286
14	SNMP	289
14.1	SNMP Support	291
14.2	Interface Numbers	291
14.3	SNMP Configuration.....	292
14.3.1	Configuration Steps.....	293
14.4	SNMP Defaults	293
14.5	Enable/Disablethe SNMP Agent.....	294
14.5.1	Switch Name	295
14.5.2	Switch Contact	296
14.5.3	System Location	297
14.6	Access Control	299
14.6.1	Engine Identifier	299
14.6.2	Community	300
14.6.3	User	301
14.6.4	Group.....	303
14.6.5	View.....	305
14.6.6	Group Access.....	306
14.7	Trap	309
14.7.1	Target Address	309
14.7.2	Target Parameters.....	311
14.7.3	SNMP Notify	312

SBM-25G-100 / MBM-XEM-100 Configuration Guide

14.7.4	Trap UDP Port.....	314
14.7.5	Authentication Traps.....	315
14.7.6	Link-State Trap	316
14.8	SNMPConfigurationExample.....	318
15	RMON.....	326
15.1	RMON Groups	328
15.1.1	Alarm group.....	328
15.1.2	Event Group	329
15.1.3	Statistics	329
15.2	RMON Configuration.....	329
15.2.1	EnablingRMON	329
15.2.2	Configuring Alarms and Events	330
15.2.3	Configuring Statistics.....	332
15.2.4	RMON Configuration Example	333
15.2.5	Configuring Port Rate Limit	339
15.2.6	Configuring HOL Blocking Prevention	340
16	Security.....	343
16.1	Login Authentication Mode	343
16.2	RADIUS	344
16.2.1	RADIUS Server	345
16.3	TACACS	346
16.3.1	TACACS Server	347
16.3.2	TACACS Re-tries.....	348
16.3.3	TACACS use-server	349
16.3.4	TACACS Login Authentication Mode.....	350
16.3.5	TACACS Authorization Status	353
16.3.6	TACACS Accounting	354
16.3.7	TACACS Privilege	355
16.4	SSH.....	356
16.5	SSL / Secure HTTP (HTTPS)	358
17	LLDP	360
17.1.1	EnablingLLDP	361

SBM-25G-100 / MBM-XEM-100 Configuration Guide

17.1.2	Configuring LLDP Parameters.....	361
17.1.3	Configuring LLDP Timers	367
17.1.4	LLDPConfiguration.....	370
18	Show Commands.....	379
18.1.1	show chassis info.....	379
18.1.2	show blade interfaces	380
18.1.3	show lldp traffic.....	381
18.1.4	show ip http statistics	381
19	Debug Commands	382
19.1.1	Debug DHCP Client	382
19.1.2	Debug IGMP Snooping	383
19.1.3	Debug SNMP	384
19.1.4	Debug Link Aggregation	384
19.1.5	Debug LLDP	384
19.1.6	Debug VLAN	385
19.1.7	Debug Packets Handled by CPU	385
19.1.8	Debug Hardware Watchdog Service	387
19.1.9	Debug WEBUI access.....	387
19.1.10	Debug RADIUS	388
19.1.11	Debug REST	389
19.1.12	Debug STP	389
19.1.13	Debug SSH	390
19.1.14	Debug TACACS.....	391
19.1.15	Display Active Debug Settings	392
19.1.16	Disable Debugging.....	394

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 viaTelnet 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.

Step	Command	Description
------	---------	-------------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 1	configure terminal	Enters the configuration mode
Step 2	terminal width <characters>	Configures the width of the terminal in characters. characters – Any number between 20 to 512.
Step 3	terminal length <lines>	Configures the height of the terminal in lines. lines – Any number between 0 to 1024. 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.
Step 4	show terminal	Displays current terminal settings
Step 5	End	Exits the configuration mode.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

The example use cases:

```
SMIS# show system information | grep Restore
ZTP Config Restore Option      : ZTP Disabled
Config Restore Status          : Successful
Config Restore Option          : Restore
Config Restore ZTP Filename    :
Config Restore ZTP TFTP IP Address : 0.0.0.0
Config Restore Local Filename  : iss.conf
SMIS#
```

```
SMIS# show system information | grep "Restore Status"
Config Restore Status          : Successful
SMIS#
```

```
SMIS# show interface fx 0/1 | grep "Unicast|Multicast"
Unicast Packets                : 0
Unicast Packets Rate           : 0/Sec
Multicast Packets              : 0
Multicast Packets Rate         : 0/Sec
Unicast Packets                : 0
Unicast Packets Rate           : 0/Sec
Multicast Packets              : 0
Multicast Packets Rate         : 0/Sec
SMIS#
```

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 chassis 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#
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

The corresponding switch port for each blade server interface can be found by the command 'show blade interfaces'.

```
SMIS# show blade interfaces
```

```
* - Blade server detected at this slot
```

Blade	Node	Nic	Port	Status
=====	=====	=====	=====	=====
Blade A1	1	1	Fx0/1	not connected
Blade A2	1	1	Fx0/3	not connected
Blade A3	1	1	Fx0/5	not connected
Blade A4	1	1	Fx0/7	not connected
Blade A5*	1	1	Fx0/9	connected
Blade A6	1	1	Fx0/11	not connected
Blade A7	1	1	Fx0/13	not connected
Blade A8	1	1	Fx0/15	not connected
Blade A9	1	1	Fx0/17	not connected
Blade A10	1	1	Fx0/19	not connected
Blade A11	1	1	Fx0/21	not connected
Blade A12	1	1	Fx0/23	not connected
Blade A13	1	1	Fx0/25	not connected
Blade A14	1	1	Fx0/27	not connected

```
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip address [<ip-address> <ip-address>/prefix-length] [<subnet-mask>]	Configure the management interface IP address manually. <i>ip-address</i> – A valid IPv4 Address. <i>ip-address/prefix-length</i> - A valid IPv4 Address with a prefix length of value 1-32. <i>subnet-mask</i> – A valid IP subnet mask.
Step 3	end	Exits the configuration mode.
Step 4	show ip interface	Displays the management interface IP configuration.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip address dhcp	Configures the management interface IP address through DHCP server.
Step 3	End	Exits the configuration mode.
Step 4	show ip interface	Displays the Management interface IP configuration.



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

The “no ip address dhcp” command disables configuring 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip gateway <ip-address>	Configure IP gateway. <i>ip-address</i> – 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
```

SMIS(config)# end

4.1.4 VLAN Tagging On Management Interface

Supermicro blade switches support VLAN tagging on management interface. By default mgmt-vlan is disabled. To configure VLAN tagging for the management interface in blade switches follow the steps below.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mgmt-vlan <vlan-id>	Enables VLAN tagging on management interface. <i>vlan-id</i> – VLAN id to tag the packets that are sent out via management interface. Allowed values are 1 to 4094.
Step 3	End	Exits the configuration mode.
Step 4	show ip interface	Displays the management interface's VLAN tagging.



After enabling the mgmt-vlan, all the packets that are sent out via management interface will be tagged. So make sure the backend infrastructure is configured properly to handle tagged packets.

The “no mgmt-vlan” command disables VLAN tagging on management interface.

The example below shows the commands used to enable VLAN tagging on management interface.

SMIS# configure terminal

SMIS(config)# mgmt-vlan 600

SMIS(config)# end

SMIS# show ip interface

mgmt is up, line protocol is up

Internet Address is 172.18.2.52/24

Broadcast Address 172.18.2.255

Gateway 172.18.2.254

IP address allocation method is dynamic

IP address allocation protocol is dhcp

Management vlan 600

4.2 Management Access

Supermicro switches enable access control of the switch by various mechanisms:

- User name and password
- Authorized Managers

Defaults – Management Access

Parameter	Default Value
Default User Name	ADMIN
Default Password for ADMIN	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.
Default privilege for default user, ADMIN	15
Default privilege for configured users	1
IP Authorized Managers	None

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	username <user-name> [password <passwd>] [privilege <1-15>]	Configure username and password. <i>user-name</i> —Alphanumeric characters of length 1-20 <i>password</i> – Alphanumeric characters of length 1-64 <i>privilege</i> - Specify 1-15, any of the privilege levels
Step 3	End	Exits the configuration mode.
Step 4	list users show users	Displays the users available in the switch. 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
```

Users	Privilege
ADMIN	15
user1	15

```
SMIS# show users
```

Line	User	Peer-Address
0 con	user1	Local Peer

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	enable [<1-15> Enable Level]	Enable a privilege level. <i>Enable Level</i> – Specify 1-15, any of the privilege levels
Step 3	End	Exits the configuration mode.

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	enable password [level (1-15)] <LINE 'enable' password>	Configure password for a particular privilege level. <i>Level</i> – Specify 1-15, any of the privilege levels <i>LINE enable password</i> – 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 WEBUI

Supermicro switches allow users to configure and monitor the switch from web browsers via WEBUI. The WEBUI is offered via HTTP and HTTPS protocols. By default both HTTP and HTTPS servers are enabled.

4.2.4.1 HTTPS

Parameter	Default Value
HTTPS server status	Enabled
HTTPS port	443

Follow the steps below to configure HTTPS.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set ip https {enable disable}	Configure HTTPS. <i>enable</i> – Enables HTTPS server <i>disable</i> – Disables HTTPS server.
Step 3	ip https port <port-number(1-65535)>	Configures HTTPS port.
Step 4	End	Exits the configuration mode.
Step 5	show https server status	Displays HTTPS server status.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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



The “no ip https port” command resets the HTTPS port to default value 443.

The example below shows the commands used to configure HTTPS.

```
SMIS# configure terminal
SMIS(config)# ip https port 4430
SMIS(config)# end
SMIS# show https server status
```

```
HTTPS server status      : Enabled
HTTPS port is           : 4430
```

4.2.4.2 HTTP

Parameter	Default Value
HTTP server status	Enabled
HTTP port	80

Follow the steps below to configure HTTP.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set IP HTTP {enable disable}	Configure HTTP. <i>enable</i> – Enables HTTP server <i>disable</i> – Disables HTTP server.
Step 3	ip http port <port-number(1-65535)>	Configures HTTP port.
Step 4	End	Exits the configuration mode.
Step 5	show http server status	Displays HTTP server status.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The “no ip http port” command resets the HTTP port to default value 80.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

The example below shows the commands used to configure HTTP.

```
SMIS# configure terminal
SMIS(config)# ip http port 8080
SMIS(config)# end
SMIS# show http server status
```

```
HTTP server status      : Enabled
HTTP port is           : 8080
```

4.2.5 RESTCONF

Supermicro switches offer RESTCONF interface to configure and manage the switches. Refer to RESTCONF user guide for details about the API offered and step-by-step instructions.

RESTCONF can be enabled or disabled from CLI. By default RESTCONF is enabled.

Parameter	Default Value
Restconf status	Enabled
Restconf port	8538

Follow the steps below to enable or disable RESTCONF.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	restconf {enable disable}	Configure RESTCONF. <i>enable</i> – Enables RESTCONF <i>disable</i> – Disables RESTCONF.
Step 4	End	Exits the configuration mode.
Step 5	show restconf status	Displays RESTCONF status.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to disable RESTCONF.

```
SMIS# configure terminal
SMIS(config)# restconf disable
SMIS(config)# end
SMIS# show restconf status
```

```
Restconf status      : Disabled
```

4.2.6 Telnet

Supermicro switches offer telnet interface to configure and manage the switches.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Telnet can be enabled or disabled from CLI. By default telnet is enabled.

Parameter	Default Value
Telnet status	Enabled
Telnet port	23

Follow the steps below to enable or disable telnet.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	telnet {enable disable}	Configure telnet. <i>enable</i> – Enables telnet access. <i>disable</i> – Disables telnet access.
Step 4	End	Exits the configuration mode.
Step 5	show mgmt status	Displays telnet status.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to disable telnet.

```
SMIS# configure terminal
SMIS(config)# telnet disable
SMIS(config)# end
```

To check the telnet access status use the below show command.

```
SMIS# show mgmt status
```

```
Protocol  Status  Port
-----  -
HTTP      Enabled  80
HTTPS     Enabled  443
Restconf   Enabled  8538
Telnet     Disabled 23
```

4.2.7 Display the status of management access

The command 'show mgmt status' displays the status of the management access and their ports.

```
SMIS# show mgmt status
```

```
Protocol  Status  Port
-----  -
HTTP      Enabled  80
HTTPS     Enabled  443
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Restconf Enabled 8538
Telnet Enabled 23

4.2.8 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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] [https] [ssh]]	<p>Configure the authorized manager</p> <p><i>ip-address</i> – ManagerIP address</p> <p><i>subnet mask</i> – For a given Authorized Manager entry, the switch applies the subnet mask to the IP address to determine a range of authorized IP addresses for management access</p> <p><i>prefix-length</i>- Prefix length of the IP address, in range 1-32.</p> <p><i>interface-type</i> – Specify the interface type through which the IP authorized manager can access the switch. May be any of the following: fx-ethernet – fx cx-ethernet – cx</p> <p><i>interface-id</i> is in slot/port format for all physical interfaces.</p> <p><i>vlan</i> -Specify the vlan id through which the IP authorized manager can access the switch.</p> <p><i>service</i> – Specify the services that can be accessed by the authorized manager</p>
Step 3	End	Exits the configuration mode.
Step 4	show authorized-managers	Displays the Authorized Managers configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



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)#authorized-manager ip-source 200.200.200.10 service telnet
```

```
SMIS(config)# authorized-manager ip-source 100.100.100.10 service http
```

```
SMIS(config)# end
```

```
SMIS# show authorized-managers
```

Ip Authorized Manager Table

```
-----  
Ip Address    : 100.100.100.10
```

```
Ip Mask       : 255.255.255.255
```

```
Services allowed : HTTP
```

```
Ip Address    : 200.200.200.10
```

```
Ip Mask       : 255.255.255.255
```

```
Services allowed : TELNET
```

4.2.9 Password Policy

The complexity of the password could be as important as the need for a password in some environment. Modern organizations would like to enforce their users to have a complex passwords to prevent easy hacking. The password policy feature offers configurations to enforce strong passwords.

Follow the steps below to configure the password policies.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	password-policy account-expire number-of-days <number(1-365)>	Set the user account to expire after configured number of days. User cannot login after the account expires.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 3	password-policy account-lockout failure-attempt <count-in-number(1-10)> duration <number-of-minutes(1-1000)>	Set the user account to get locked out after configured number of failed login attempts. The user account will be automatically unlocked after configured duration.
Step 4	password-policy mandatory numeric-char <number-of-numeric-chars(1-64)> special-char <number-of-special-chars(1-64)>	Configure the password to have the minimum number of numeric and special characters.
Step 5	password-policy maximum-password-length-allowed <number-of-characters(8-64)>	Configure the maximum number of characters that a password can have.
Step 6	password-policy minimum-password-length-allowed <number-of-characters(8-64)>	Configure the minimum number of characters that a password can have.
Step 7	password-policy password-expire number-of-days <number(1-365)>	Set the password to expire after configured number of days. User will be forced to change the password after the password expires.
Step 8	End	Exits the configuration mode.
Step 9	show password policies	Displays the password policy configuration.
Step 10	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to configure the password policies.

SMIS# configure terminal

SMIS(config)# password-policy account-expire number-of-days 365

SMIS(config)# password-policy account-lockout failure-attempt 5 duration 15

SMIS(config)# password-policy mandatory numeric-char 2 special-char 2

SMIS(config)# password-policy maximum-password-length-allowed 15

SMIS(config)# password-policy minimum-password-length-allowed 10

SMIS(config)# password-policy password-expire number-of-days 100

SMIS(config)# end

SMIS# write startup-config

SMIS# show password policies

Maximum password allowed : 15

Minimum password allowed : 10

Number of special characters : 2

Number of numeric characters : 2

Password expiry day(s) : 100

Account expiry day(s) : 365

Account lockout fail attempts : 5

Account lockout duration : 15

4.2.10 Clear User Sessions

The number of concurrent sessions allowed by the switch is limited. Sometimes, the administrators login from different computers and leave the sessions open, which would block others from accessing the switch. In this situation, the clear commands come handy. Note that serial console session is always allowed even after SSH/telnet sessions max out. When the sessions are cleared, the users are logged out immediately without any notifications.

Follow the steps below to clear CLI sessions.

Step	Command	Description
Step 1	clear cli sessions { session_id all }	Clears the CLI sessions. session_id – The session_id can be obtained from the output of 'show users' command.

Follow the steps below to clear web sessions.

Step	Command	Description
Step 1	clear web sessions	Clears the web sessions.

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 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.

Interface Name	Interface Numbers	Speed	Comments
Gi	1	1G	Default Physical interfaces
Fx	1 – 28	25G default Can operate in 10G/1G	Default Physical interfaces
Cx	1 – 4	100G default	Default Physical interfaces

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		Can operate in 40G Or can be split into 4 ports	
Fx	29 – 31	25G / 10G	When Cx 0/1 splitted – it becomes Cx 0/1, Fx 29, Fx 30 and Fx 31
Fx	32 – 34	25G / 10G	When Cx 0/2 splitted – it becomes Cx 0/2, Fx 32, Fx 33 and Fx 34
Fx	35 – 37	25G / 10G	When Cx 0/3 splitted – it becomes Cx 0/3, Fx 35, Fx 36 and Fx 37
Fx	38 – 40	25G / 10G	When Cx 0/4 splitted – it becomes Cx 0/4, Fx 38, Fx 39 and Fx 40

Parameter	Default Value
MTU	1500 bytes
Speed	Fx ports FX 0/1 to 0/28 – 25 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 and Fx-ethernet ports.

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.

Interface Name	Interface Numbers	Speed	Comments
Gi	1	1G	Default Physical interfaces
Fx	1 – 56	25G default Can operate in 10G/1G	Default Physical interfaces

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Cx	1 – 4	100G default Can operate in 40G Or can be split into 4 ports	Default Physical interfaces
Fx	57 – 59	25G / 10G	When Cx 0/1 splitted – it becomes Cx 0/1, Fx 57, Fx 58 and Fx 59
Fx	60 – 62	25G / 10G	When Cx 0/2 splitted – it becomes Cx 0/2, Fx 60, Fx 61 and Fx 62
Fx	63 – 65	25G / 10G	When Cx 0/3 splitted – it becomes Cx 0/3, Fx 63, Fx 64 and Fx 65
Fx	66 – 68	25G / 10G	When Cx 0/4 splitted – it becomes Cx 0/4, Fx 66, Fx 67 and Fx 68

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Parameter	Default Value
MTU	1500 bytes
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 3	description <string>	Configure the interface description <i>String</i> – alphanumeric characters of length 1-64.
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
```

```
Interface  Status  Protocol  Description
-----  -
```

```
Fx0/1      up      down
Fx0/2      up      down
Fx0/3      up      down
Fx0/4      up      down
Fx0/5      up      down
Fx0/6      up      down
Fx0/7      up      down
Fx0/8      up      down
Fx0/9      up      down
Fx0/10     up      down
Fx0/11     up      down
Fx0/12     up      down
Fx0/13     up      down
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
------	---------	-------------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 1	configure terminal	Enters the configuration mode
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: cx-ethernet interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range cx 0/1-2 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range cx 0/1-2, cx 0/3 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step3	Negotiation	Enable Interface Negotiation
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 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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Port	Status	Duplex	Speed	Negotiation
----	-----	-----	-----	-----
Fx0/1	not connected	Full	25 Gbps	Auto
Fx0/2	not connected	Full	25 Gbps	Auto
Fx0/3	not connected	Full	25 Gbps	Auto
Fx0/4	not connected	Full	25 Gbps	Auto
Fx0/5	not connected	Full	25 Gbps	Auto
Fx0/6	not connected	Full	25 Gbps	Auto
Fx0/7	not connected	Full	25 Gbps	Auto
Fx0/8	not connected	Full	25 Gbps	Auto
Fx0/9	not connected	Full	25 Gbps	Auto
Fx0/10	not connected	Full	25 Gbps	Auto
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	<p>Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</p> <p>interface-id is in slot/port format for all physical interfaces.</p> <p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	speed { 1000 10000 25000 40000 100000 }	Configure Interface Speed as 10 or 100 or 1000 or 10000 Mbps.
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 speed” command restores the default interface speed.

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
```

Port	Status	Duplex	Speed	Negotiation
----	-----	-----	-----	-----
Fx0/1	not connected	Full	25 Gbps	Auto
Fx0/2	not connected	Full	25 Gbps	Auto
Fx0/3	not connected	Full	25 Gbps	Auto
Fx0/4	not connected	Full	25 Gbps	Auto
Fx0/5	not connected	Full	25 Gbps	Auto
Fx0/6	not connected	Full	25 Gbps	Auto
Fx0/7	not connected	Full	25 Gbps	Auto
Fx0/8	not connected	Full	25 Gbps	Auto
Fx0/9	not connected	Full	25 Gbps	Auto
Fx0/10	not connected	Full	25 Gbps	Auto

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	<p>Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel</p> <p>interface-id is in slot/port format for all physical interfaces.</p> <p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

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

Undersize Frames : 0

Oversize Frames : 0

CRC Error Frames : 0

Discarded Packets : 0

Error Packets : 0

Unknown Protocol : 0

Transmission Counters

Octets : 0

Unicast Packets : 0

Unicast Packets Rate : 0/Sec

Broadcast Packets : 0

Broadcast Packets Rate : 0/Sec

Multicast Packets : 0

Multicast Packets Rate : 0/Sec

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>interface-id is in slot/port format for all physical interfaces.</p> <p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 3	flowcontrol { send receive } { on off }	<p>Configure flow control</p> <p><i>Send</i> – The port can send pause frames but cannot receive pause frames from a connected device.</p> <p><i>Receive</i> – The port cannot send pause frames but can receive pause frames from a connected device.</p> <p>On – Enable flow control</p> <p>Off - Disable flow control</p>
Step 4	End	Exits the configuration mode.
Step 5	show flow-control [interface <interface-type><interface-id>]	Displays the Interface Flow control configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

Port	TxFlowControl	Rx FlowControl	Tx Pause	Rx Pause
----	-----	-----	-----	-----
Fx0/22	on	off	0	0

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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	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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 3	Fec-mode	Enable FEC mode on interface.
Step 4	End	Exits the configuration mode.
Step 5	show interface	Displays the fec mode for the interface.
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 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	<p>Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: cx-ethernet – cx</p> <p>interface-id is in slot/port format for all physical interfaces.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range cx 0/1-2, cx 0/4</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 3	speed 25000 Or speed 10000	<p>Splits the port into four 25G ports or four 10G ports.</p> <p>Note: Fec-mode and negotiation have to be turned off for splitting into 4 x 10G ports.</p>
Step 4	end	<p>Exits the configuration mode.</p>
Step 5	show interface status	<p>Split ports can be viewed in the output.</p>
Step 6	write startup-config	<p>Optional step – saves this configuration to be part of startup configuration.</p>

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

Parameter	Default Value
Timezone offset	None
NTP status	Disabled
NTP operation	Unicast
NTP authentication	None
NTP server	None
NTP Broadcast mode	No

4.4.1 NTP server

Supermicro switches can synchronize time with a NTP server. Follow the below steps to configure NTP server parameters.

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ntp enable	Enable NTP in switch.
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 “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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

[NTP] ntp running unicast mode

```
Server   Key  Prefer
=====  =====
200.200.200.10  100  YES
100.100.100.1   500
```

```
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ntp key <key_number (1- 65535)><key_text>	Configure NTP authentication key. <i>Key-number</i> –key number in the range 1-65535, used for MD5. <i>Key-text</i> –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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Server Key Prefer

=====

Key # Key

=====

200 For-server1

Time zone offset not set

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ntp broadcast [authentication]	Configure NTP broadcast. <i>authentication</i> – 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

=====

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.

Step	Command	Description
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. <i>hh:mm:ss</i> – Time in Hours:Minutes:Seconds format. <i>day</i> – Day in 1-31 format. <i>month</i> – Month in January-December format. <i>year</i> – 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tz posix <std><offset>[<dst>]	Configure the timezone. <std> - Standard time text e.g. PST

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p><offset> - Time zone offset in <code>[+ -]hh[:mm[:ss]]</code> 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.</p> <p><dst> - Day light savings time text e.g. PDT</p>
Step 3	end	Exits the configuration mode.
Step 4	show system information	Displays the timezone configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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
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 48 mins 5 secs
```

```
Boot-up Flash Area    : Normal
```

```
NTP Broadcast Mode     : No
```

[NTP] ntp is disabled

```
Server  Key  Prefer
```

```
=====
```

```
Key #  Key
```

=====

Time zone offset value: PST8

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

Parameter	Default Value
Switch name	SMIS
System contact	http://www.supermicro.com
System location	Supermicro
MAC aging	300 secs
MAC table static entries	None
System MTU	1500 bytes
Port mirroring	Disabled
Port mirroring direction	Both

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	device name <devname(15)>	Configure Switch Name and prompt. <i>Devname</i> – Switch name specified as 1-15 alphanumeric characters.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the system information configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	system contact <string - to use more than one word, provide the string within double quotes>	Configure Switch Contact. <i>String</i> – Contact information entered as a String of maximum length 256.
Step 3	End	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to configure System Location.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	system location <location name>	Configure System Location. location name –Location of the switch specified as a string of maximum size 256.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the System Location configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The *System Location* configuration is automatically stored as part of startup-config 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
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

4.5.4 System MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces of the switch is 1500 bytes. 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	system mtu <frame-size(1500-9216)>	Configure System MTU. frame-size – Specify MTU of frame in range 1500-9216.
Step 3	End	Exits the configuration mode.
Step 4	show interface mtu	Displays the interface MTU.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The “no system mtu” command resets the system MTU to its default value of 1500 bytes.

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface ([<interface-type><0/a-b,0/c,...>] [<interface-type><0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface <interface-type><iface>	Configure Multicast or unicast static MAC. <i>Vlan</i> – Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. Interface - specify the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<i>Interface-type</i> - 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	<pre>show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type><interface-id> }] show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:a:aa:aa>] [{interface <interface-type><interface-id> }]</pre>	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:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type><interface-id>]andno mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type><interface-id>]” command deletes the particular static MAC entry.

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

Vlan	Mac Address	Status	Ports
1	90:4e:e5:0c:03:75	Permanent	Fx0/14

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to configure MAC Aging.

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



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
-

Parameter	Default Value
Syslog status	Enabled

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Logging buffer size	50 entries
Console logging	Enabled
File Logging	Disabled
Trap Logging	Critical
MAC Address table update Logging	Disabled
Facility	Local0

4.6.1 Enable/Disable Syslog

Syslog is enabled by default in Supermicro switches.

Follow the steps below to disable Syslog.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging disable	Disable Syslog.
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 “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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

LogBuffer(0 Entries)

LogFile(0 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging <ip-address>	Configure Syslog Server. <i>ip-address</i> –IP address of Syslog server
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 <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)
```

LogFile(0 Entries)

4.6.3 Console Log

System Logging messages can be displayed in switch console.

Follow the steps below to enable Syslog Console.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging console	Enable Syslog Console.
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 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 Logging Configuration

The configurations made in the switch can be tracked by enabling the logging configuration. When the logging configuration is enabled, all the commands executed under the configuration mode will be logged. The configuration logs are classified at trap level 5 or more, so to see the configuration changes in the log set the trap level to 5 or more.

Follow the steps below to enable the logging configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging configurations	Enable logging configuration.
Step 3	logging trap 5	Set the trap level to notification.
Step 4	End	Exits the configuration mode.
Step 5	show logging	Displays the Syslog configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The “no logging configuration” command disables logging configuration.

The example below shows the commands used to enable logging configuration.

```
SMIS# configure terminal
SMIS(config)# logging configurations
SMIS(config)# logging trap 5
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)
Mac addr logging : disabled
Log File Name   :
Max File Size   : 4096
Min File Size   : 2048
TimeStamp option : enabled
Trap logging    : Notification
Log server IP    : None
Facility        : Default (local0)
Buffered size    : 5000 Entries
LogBuffer: (0 Entries)
```

LogFile: (0 Entries)

4.6.5 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging file <filename> max-entries <short (1-8000)>	Enable storing Logs in a File.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<i>Filename</i> – Specify file name of upto 32 characters. <i>Short</i> –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.

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

LogFile(2 Entries)

```
<129> Apr 29 10:11:30 2013:INTF-1:Interface Fx0/22 status changed to UP
```

```
<129> Apr 29 10:11:31 2013:INTF-1:Interface Fx0/22 status changed to UP
```

SMIS#

```
SMIS# show logging
```

System Log Information

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

LogBuffer(11 Entries)

```
<135> Apr 29 10:11:05 2013:DHC-7:Exiting DHCP 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 10:11:06 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf2878 type : 1
<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf2890 type : 1
<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf4448 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 13cf4908 type : 1
<129> Apr 29 10:11:31 2013:INTF-1:Interface Fx0/22 status changed to UP
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
```

4.6.6 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging buffered <size (1-200)>	Configure Syslog Buffer with maximum size of 200 entries.
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 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)
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 DHCP 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)
```

4.6.7 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging facility {local0 local1 local2 local3 local4 local5 local6 local7 }	Configure Syslog Facility.
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 “nologging 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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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)
```

4.6.8 Trap

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

Follow the steps below to configure Logging Traps.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging trap [{ <level (0-7)> alerts critical debugging emergencies errors informational notification warnings }]	<p>Configure Logging Traps.</p> <p>There are various levels of trap that can be logged.</p> <p><i>Level 0 – Emergencies</i> Used for logging messages that areequivalent to a panic condition.</p> <p><i>Level 1 –Alerts</i> Used for logging messages that require immediate attention</p> <p><i>Level 2 – Critical</i> Used for logging critical errors</p> <p><i>Level 3 –Errors</i> Used for error messages</p> <p><i>Level 4 –Warning</i> Used for logging warning messages</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<i>Level 5 –Notification</i> Used for logging messages that require attention but are not errors <i>Level 6 – Informational</i> Used for logging informational messages. <i>Level 7 – Debugging</i> Used for logging debug messages.
Step 3	End	Exits the configuration mode.
Step 4	show logging	Displays the Syslog configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The “no logging trap” command resets 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:DHC-7:Exiting DHCP Task Ini
<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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
<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)

4.6.9 Clear Log buffer

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

Follow the steps below to Clear Logging Buffer.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	clear log buffer	Clear Logging Buffer.
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 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)

4.6.10 Clear Log File

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to Clear Logging File.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	clear log file	Clear Logging File.
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 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.

Step	Command	Description
Step 1	write startup-config	Configure Writing of Switch Configuration to a file or startup-config.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	show startup-config	Displays the startup configuration.
--------	---------------------	-------------------------------------

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

```
SMIS# write startup-config
```

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



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

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.

Step	Command	Description
Step 1	write { flash:filename tftp://ip-address/filename }	Configure Writing of Switch Configuration to a file in the local flash memory or in a remote TFTP server. filename – name of the configuration file.
Step 2	show stored-config<filename>	Displays the stored configuration file from local flash memory. filename – name of the configuration file.

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

```
SMIS# write flash:r1sw1.conf
```

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

```
SMIS# writetftp://192.168.1.100/r1sw1.conf
```

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

```
SMIS# show stored-config r1sw1.conf
```

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set startup-config<filename>	Configure Startup-config file name. filename – name of the configuration file.
Step 3	End	Exits the configuration mode.
Step 4	show startup-config	Displays the configured startup configuration file contents.

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.

Step	Command	Description
Step 1	copy startup-config{flash:filename tftp://ip-address/filename}	Copy from startup-config to a file in remote location or flash. filename – name of the configuration file.

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.

Step	Command	Description
Step 1	copy flash: filename tftp://ipaddress/filename	Copies a local flash file to remote TFTP server.
	copy tftp://ip-address/filename flash: filename	Copies a remote file to local flash.
	copy flash: filename flash: filename	Makes a copy of the file in the flash memory. filename – name of the configuration file.

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

```
SMIS# copy flash:config1.txt flash:switch1.conf
Copied flash:/mnt/config1.txt ==> flash:/mnt/switch1.conf
SMIS#
```

4.7.6 Copy debug files

Supermicro switches support copying the switch's current state to remote location for debugging. The information collected using this command will be very useful in troubleshooting an issue. Use this command to collect the configurations and the running state of the switch and upload the file to Supermicro technical support website while opening a support ticket.

Follow the steps below to copy debug-files to a remote TFTP location.

Step	Command	Description
Step 1	copy debug-files {tftp://ip-address/filename}	Copy debug-files to a remote TFTP location. filename – name of the configuration file.

The example below shows the commands used to copy debug-files to a TFTP location.

```
SMIS# copy debug-files tftp://172.18.0.253/Switch-01-techsupport-14-May-2010.tgz
```

Please wait. It may take a few minutes ...

```
Copied tech-support ==> tftp://172.18.0.253/Switch-01-techsupport-14-May-2010.tgz
SMIS#
```

To open the debug file from windows, use any software such as winrar, 7zip, etc that supports opening file in tgz format. To open the debug file from Linux, use tar command as shown below.

```
[root@Linux]# tar -xvzf Switch-01-techsupport-14-May-2010.tgz
techsupport.txt
logging.txt
issnvram.txt
dmesg.txt
system_log
[root@Linux]#
```

4.7.7 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.

Step	Command	Description
Step 1	erase startup-config	Removes the startup-config.
	erase flash:filename	Deletes the configuration file from local flash. filename – name of the configuration file.

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#
```

4.7.8 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.



This command helps upgrading only the firmware image. Some releases might need to upgrade the kernel and boot loader images. Refer the readme file on the release package for release specific firmware upgrade procedure.

Follow the steps below to update firmware image:

Step	Command	Description
Step 1	firmware upgrade { tftp://ip-address/filename} [normal fallback]	Updates the firmware image from remote TFTP server.

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}”.

4.7.9 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set boot-up {normal fallback}	Configure Switch Boot-Up options.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the system information configuration.



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

```
Server  Key  Prefer
=====
Key #   Key
=====
Time zone offset not set
```

4.7.10 Reset to Factory Defaults

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

Follow the steps below to reset to the factory defaults.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	reset-to-factory-defaults [preserve_user {all ADMIN-ADMIN}]	Resets all configurations to Factory Defaults. preserve_user all - resets all configurations to factory defaults but retain the users/passwords. preserve_user ADMIN-ADMIN - reset all configurations to factory defaults and set the ADMIN user password to 'ADMIN'. This option shall be used to avoid the switch using the unique password after resetting to factory default.



Resetting to factory defaults will remove all stored configurations, files on the flash memory, user accounts and the management IP address.

Using the option preserve_user will create a startup configuration file. Hence, ZTP will stay disabled.

After resetting to factory defaults, the switch can be managed from serial console with the default administrator user ID ADMIN and password can be found on the label stuck on the switch.

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

```
SMIS(config)# reset-to-factory-defaults
```

This command will reset settings to factory defaults.

ZTP feature is enabled in factory default. Please remove ZTP option in DHCP server configuration.

After resetting to factory defaults, switch will be reloaded immediately.

Do you really want to execute this command and reload the switch? [y/n]



Default ADMIN password for the switches that were shipped after 01/01/2020 will be unique for each switch and can be found on a label stuck on the switch. For the switches that were shipped before 01/01/2020 the default password is ADMIN.

The example below shows the command to reset all the configurations to the factory defaults and retain the username and password.

```
SMIS(config)# reset-to-factory-defaults preserve_user all
```

This command will reset settings to factory defaults.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

ZTP feature is enabled in factory default. Please remove ZTP option in DHCP server configuration.
After resetting to factory defaults, switch will be reloaded immediately.
Do you really want to execute this command and reload the switch? [y/n]

The example below shows the command to reset all the configurations to the factory defaults and set the ADMIN user password to 'ADMIN'.

```
SMIS(config)# reset-to-factory-defaults preserve_user ADMIN-ADMIN
```

This command will reset settings to factory defaults.

ZTP feature is enabled in factory default. Please remove ZTP option in DHCP server configuration.
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 be added to `dhcpd.conf` as shown in the below example.

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

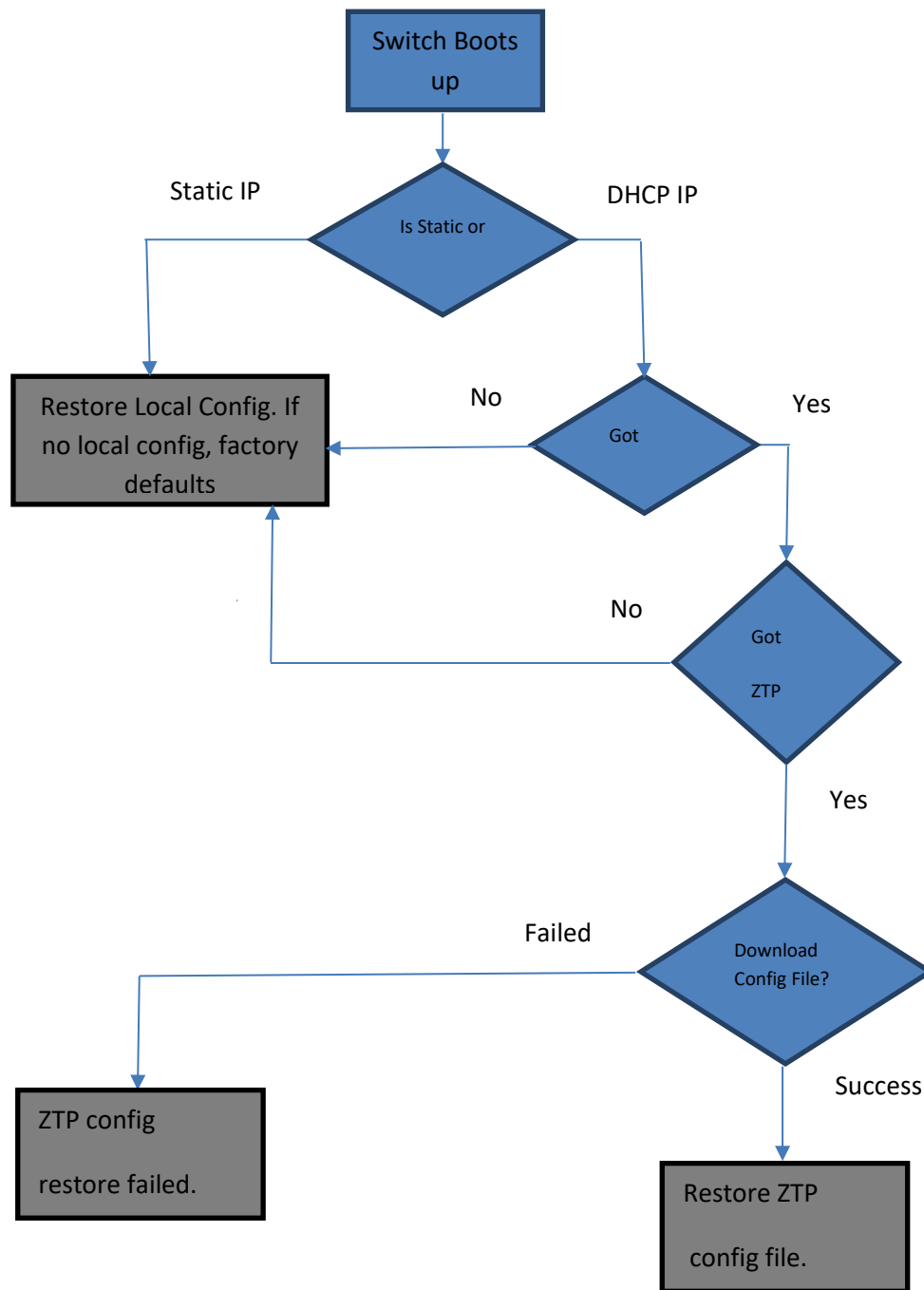
Need to add the below lines to define option 43.1 for Supermicro Blade switches

```
option space smc-op;  
  
option smc-op.config-file-name code 1 = 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";  
  
}
```

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.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 be 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

```
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";

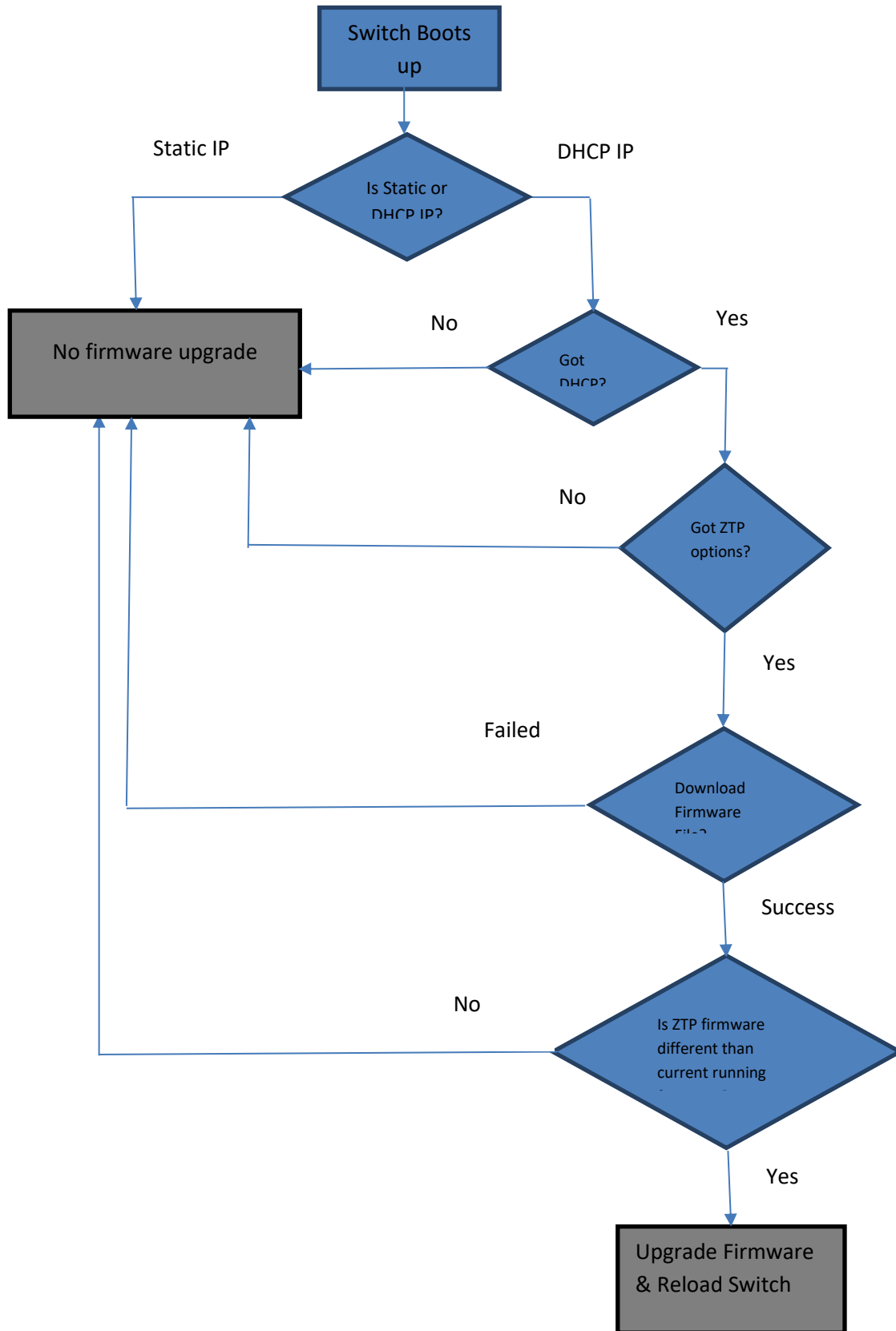
    option smc-op.fw-img-file-name "SBM-MBM-100-fw-1.0.2.2.img";

}
```

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 prefer 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.

```
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 down stream 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.

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

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.

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	<i>interface <ifname> <ifid></i>	Enter the interface configuration mode
Step 3	<i>no loop-protect</i>	Disabling the loop protection feature on this interface
Step 4	End	Exits the configuration mode.
Step 5	<i>show loop protection</i>	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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 3	loop-protect disable	Disabling the loop protection feature globally
Step 4	End	Exits the configuration mode.
Step 5	<i>show loop protection</i>	Displays the loop protection configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

5 VLAN

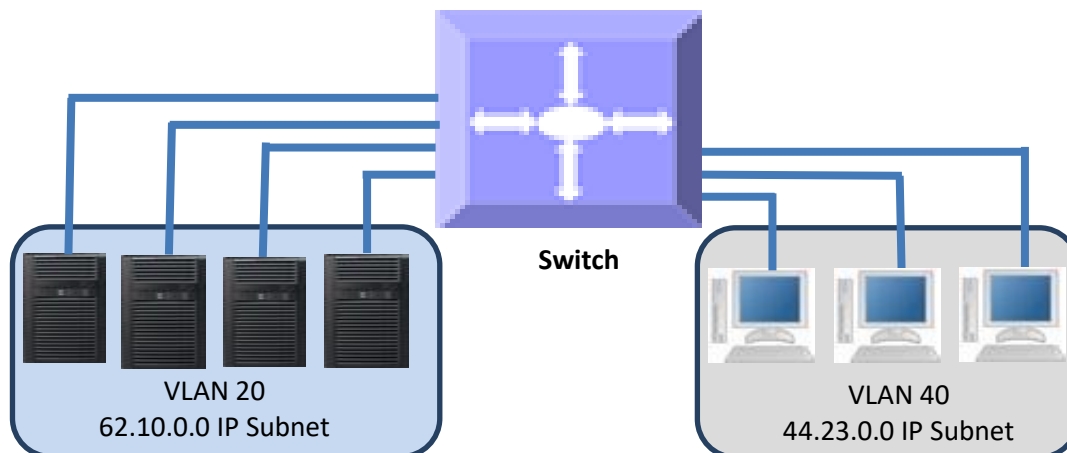
5.1 VLAN Basics

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

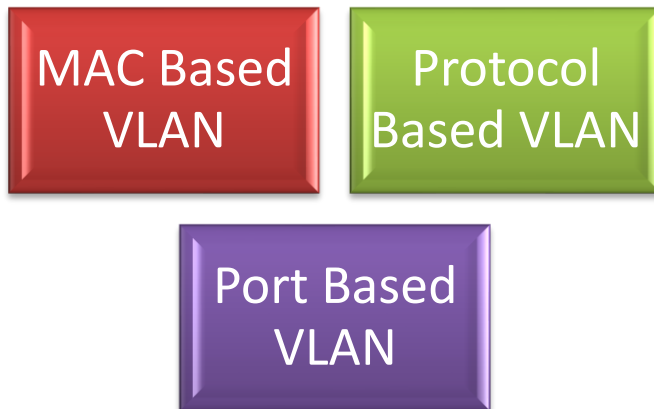


VLANs work in same way as physical LANs. The packets from the end stations of a VLAN are switched only to other end stations or network devices inside that VLAN. To reach devices in another VLAN, the packets have to be routed from one VLAN to another. Supermicro L2/L3 switches support such Inter VLAN 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.

Figure VLAN-2: Types of VLANs Supported



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 VALN 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.

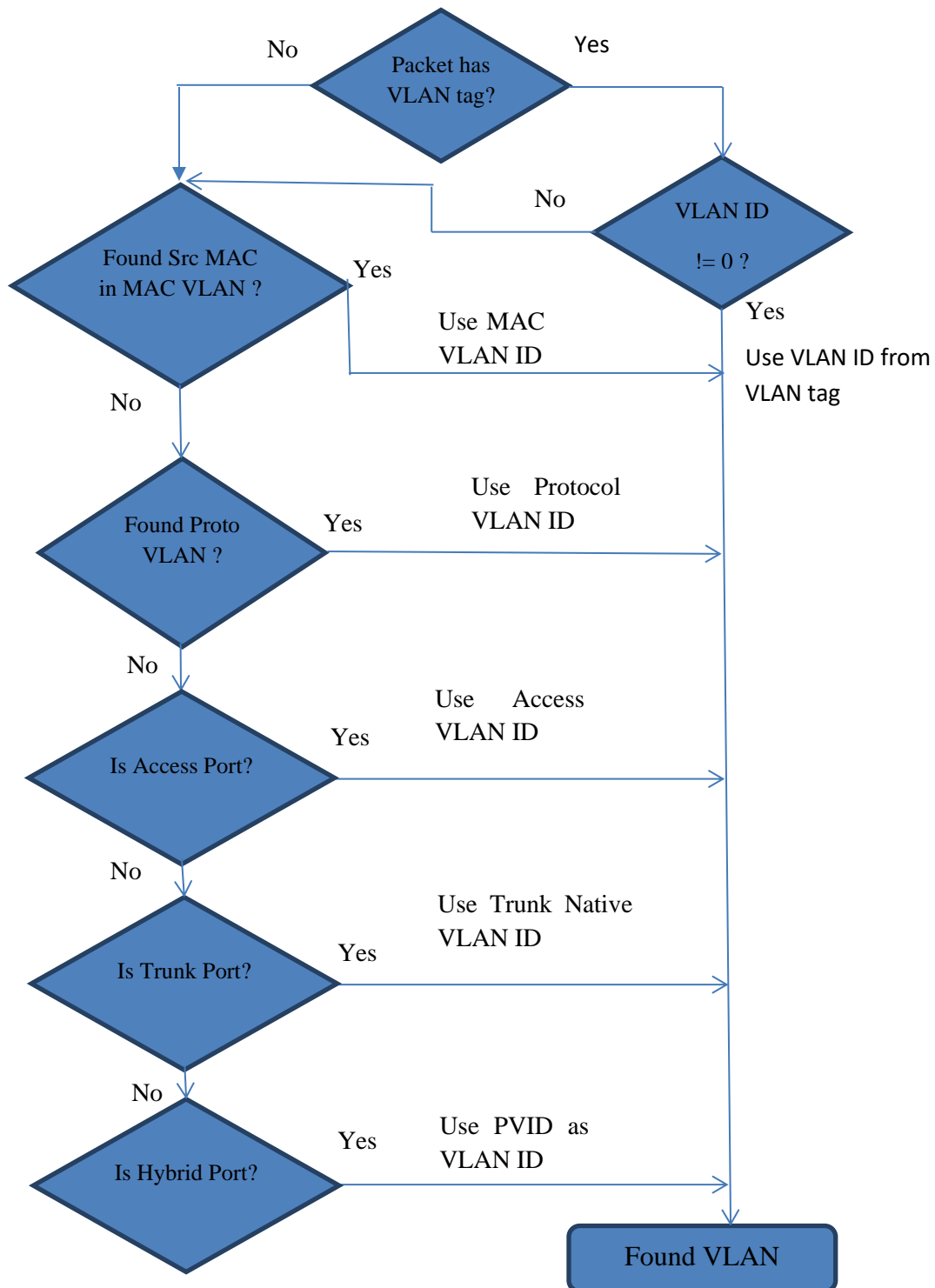
Step 2: Use the protocol field from the incoming packet layer 2 header and check the protocol VLAN table. If a protocol VLAN is found, that VLAN ID is used as the VLAN for this packet. If a protocol VLAN is not found, proceed to the next step.

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



5.3 VLAN Numbers

This switch models supports 4K static VLANs.

This switch models support VLAN identifiers from 1 to 4069 for user created VLANs. VLAN identifiers 4070 to 4094 are reserved for internal use.



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

This switch models 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	vlan <vlan-list>	Creates a VLAN using vlan command. <i>vlan-list</i> – 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 3	show vlan	Displays the configured VLANs
Step 4	write startup-config	Optional step – Save these VLAN configuration to be part of startup configuration.

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enter the configuration mode
Step 2	no vlan <vlan-list>	Remove VLANs using the no vlan command. <i>vlan-list</i> – may be any vlan number or list of vlan numbers. Multiple vlan numbers can be provided as comma separated list. Consecutive vlan numbers can be provided as ranges like 5-10.
Step 3	show vlan	To display the configured VLANs
Step 4	write startup-config	Optional step – Save these VLAN configuration to be part of startup configuration.

The below examples show 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	vlan <vlan-list>	Enters the VLAN configuration mode. <i>vlan-list</i> – 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		If multiple VLANs are provided, the same name string provided in next step will be associated with all these VLANs.
Step 3	name <vlan-name-string>	Associates a name string to this VLAN using the name command. <i>vlan-name-string</i> is any alphanumeric string up to 32 characters.
Step 4	show vlan	Displays the configured VLANs
Step 5	write startup-config	Optional step – saves this VLAN configuration to be part of startup configuration.

The example below shows the 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	vlan <vlan-list>	Enters the VLAN configuration mode. <i>vlan-list</i> – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the name string of all these VLANs will be removed by the next step.
Step 3	no name	Removes associated name string from this VLAN.
Step 4	show vlan	Displays the configured VLANs
Step 5	write startup-config	Optional step – saves this VLAN configuration to be part of startup configuration.

The example below shows steps to remove name string from a VLAN.

Remove name from VLAN 50.

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

5.8 Port Based VLANs

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

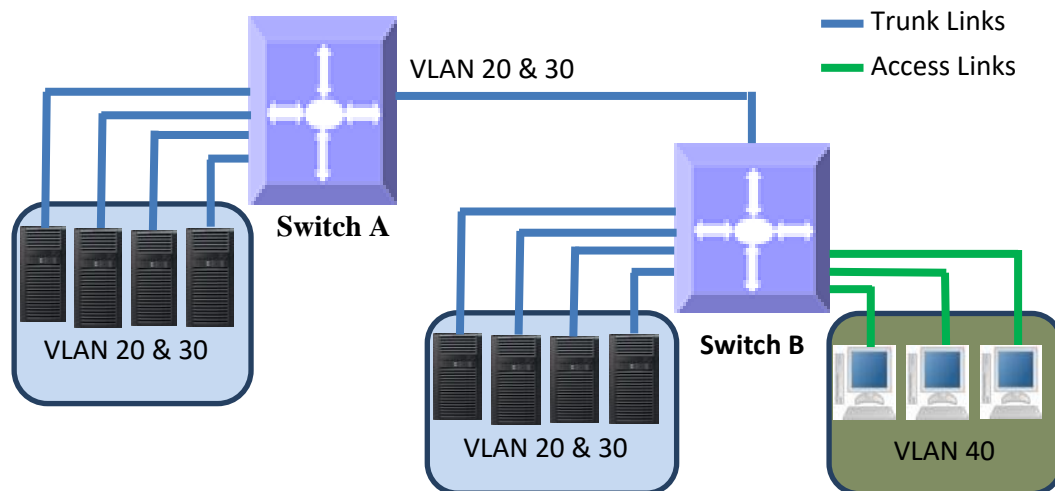
In port based VLAN deployment, switch ports are associated with one or more VLANs as member ports.

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”.



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

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cxport-channel – po <i>interface-id</i> is in <i>slot/port</i> 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	switchport mode access	Sets the port mode as the access port.
Step 4	switchport access vlan <vlan-id>	Configures the access VLAN for this interface. The VLAN identifiers may be any VLAN number from 1 to 4069. If the given VLAN does not exist, switch will provide a warning message. Only when the VLAN available, the port will operate as an access port for that VLAN.
Step 5	show vlan port config port <iftype> <ifnum>	Displays the configured mode and accesses the VLAN for this interface.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po <i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “ interface range ... ” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20
Step 3	switchport mode trunk	Sets the port mode as a trunk port.
Step 4	show vlan port config port <iftype> <ifnum> and show running-config	Displays the configured mode for this interface.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po <i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces. It may be a port channel identifier for port channel interfaces.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	switchport mode trunk	Sets the port mode as trunk port.
Step 4	Use any one of the below steps 4a to 4f based on the need.	The <i>vlan-list</i> 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.
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 <i>vlan-list</i> 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 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
```

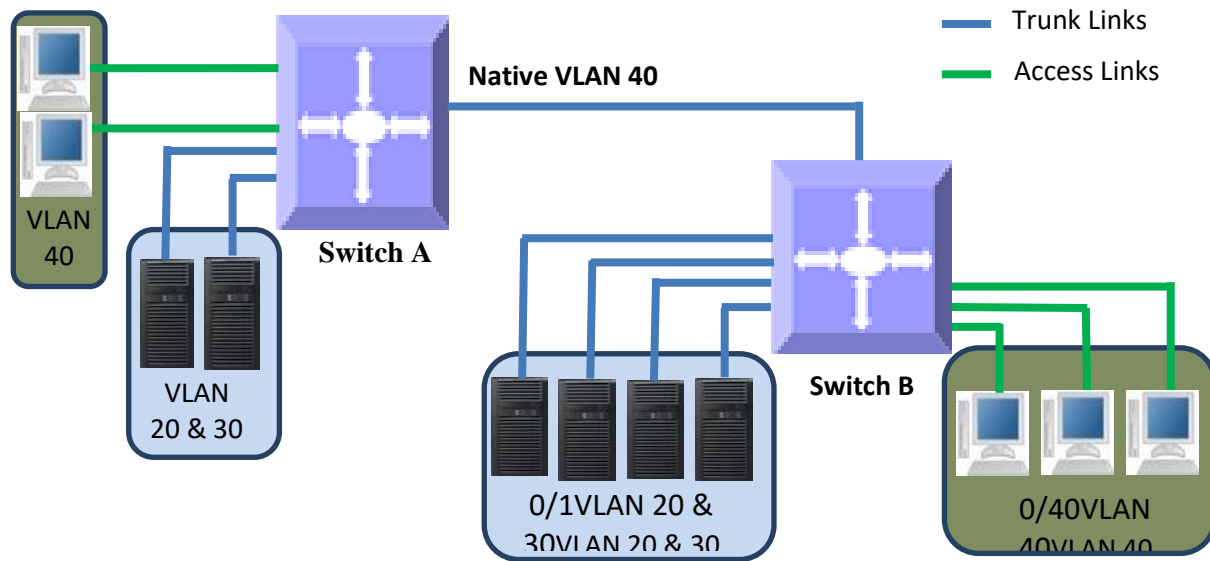
5.8.2.2 Native VLAN on Trunk

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.

Figure VLAN-5: Native VLANs



Users can configure a native VLAN for trunk interfaces by following the steps below.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po <i>interface-id</i> is in <i>slot/port</i> 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>	<p><i>vlan-id</i> - The VLAN identifiers may be from 1 to 4069.</p> <p>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.</p> <p>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.</p>
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
```

SMIS(config-if)# **exit**

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.

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>numbers can be provided as a range, such as 5-10.</p> <p>If multiple VLANs are provided, the ports configuration provided in the next steps will be applied to all these VLANs.</p>
Step 3	Use steps 3a to 3c below one or more times to configure the required port configurations for the VLANs provided in Step 2 above.	
Step 3a	ports <ports-list> tagged or no ports [<ports-list>] tagged	<p>Adds the tagged ports list to this VLAN.</p> <p><i>ports-list</i> – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10.</p> <p>Use the no form of this command to remove tagged ports from this VLAN. If <i>ports-list</i> is not provided to the no command, all the tagged ports are removed from this VLAN.</p>
Step 3b	ports <ports-list> untagged or no ports [<ports-list>] untagged	<p>Adds the untagged ports list to this VLAN.</p> <p><i>ports-list</i> – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10.</p> <p>Use the no form of this command to remove untagged ports from this VLAN. If <i>ports-list</i> is not provided to the no command, all the untagged ports are removed from this VLAN.</p>
Step 3c	ports <ports-list> forbidden or no ports [<ports-list>] forbidden	<p>Denies traffic from ports given by <i>ports-list</i> to this VLAN.</p> <p><i>ports-list</i> – up to three ports or ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10.</p> <p>Use the no form of this command to remove forbidden ports from this VLAN.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		If <i>ports-list</i> is not provided to the no command, all the forbidden ports are removed from this VLAN.
Step 4	Exit	Exits the VLAN configuration mode.
Step 5	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id> ...	<p>Enters the interface mode.</p> <p><i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</p> <p><i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces. It may be a port channel identifier for port channel interfaces.</p> <p>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</p>
Step 6	switchport mode hybrid	Sets the port mode as a hybrid port.
Step 7	switchport pvid <vlan-id>	<p>Configures the PVID for this interface. The VLANs identifiers could be any VLAN number from 1 to 4069.</p> <p>The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first.</p> <p>This command accepted only when the port is “Hybrid” mode.</p>
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.

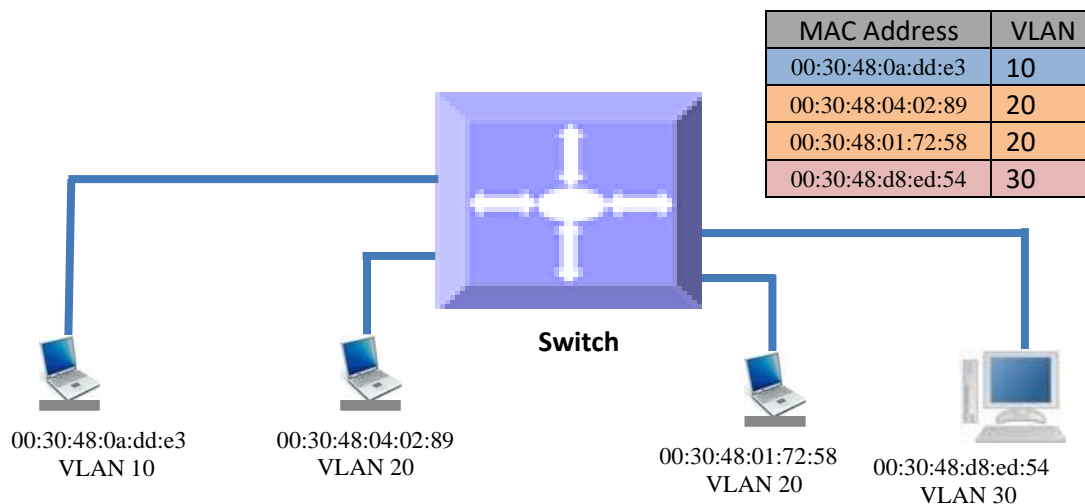
MAC based VLAN features are used to provide the same VLAN to any end user irrespective of the switch port the end user connecting to.

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



Follow the steps below to configure MAC based VLANs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	vlan <vlan-list>	Creates the required VLANs.
		<i>vlan-list</i> – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		numbers can be provided as ranges such as 5-10.
Step 3	ports <ports-list> untagged	Adds the ports given by <i>ports-list</i> to this VLAN as untagged ports. <i>ports-list</i> – up to three ports or ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10.
Step 4	Exit	Exits the VLAN configuration mode.
Step 5	mac-vlan <ucast_mac> vlan <vlan-id>	Configures MAC VLAN mapping entry. <i>ucast_mac</i> – Unicast MAC address. This VLAN will be applied to all incoming untagged packets from this unicast MAC address. <i>vlan-id</i> - VLAN identifiers may be any VLAN number from 1 to 4069. The VLAN must have already been created in this switch.
Step 6	show mac-vlan	Displays the configured MAC based VLANs.
Step 7	write startup-config	Optional step – saves this VLAN configuration to be part of startup configuration.



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no mac-vlan <ucast_mac>	Removes MAC VLAN mapping entry. <i>ucast_mac</i> – Unicast MAC address for which MAC VLAN mapping is to be removed.
Step 3	show mac-vlan	Displays the configured MAC based VLANs.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

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

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

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

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

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	vlan <vlan-list>	<i>vlan-list</i> – 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.
Step 3	ports <ports-list> untagged	<p>Adds the required ports for this VLAN as untagged ports.</p> <p><i>ports-list</i> – 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.</p>
Step 4	Exit	Exits the VLAN configuration mode.
Step 5	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) >	<p>Creates a protocol group.</p> <p>Protocol group creation takes three parameters.</p> <p>First: protocol field as arp, ip, rarp, ipx, novell, netbios or appletalk. Users can enter any other two-byte protocol fields in hex format as aa:aa.</p> <p>Second: frame type as enet-v2, llc or snap.</p> <p>Third: protocol group identifier number.</p>
Step 6	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	<p>Enters the interface mode.</p> <p><i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</p> <p><i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces. It could be the port channel identifier for port channel interfaces.</p> <p>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</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20
Step 7	switchport map protocols-group <i><Group id integer(0-2147483647)></i> vlan <i><vlan-id(1-4069)></i>	Associates the group to the VLAN on the above interface. <i>Group id</i> – Protocol Group Identifier <i>vlan-id</i> – VLAN identifier.
Step 8	switchport pvid <i><vlan-id></i>	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 show protocol-vlan	Displays the configured protocol based VLANs.
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <i><interface-type></i> <i><interface-id></i> or interface range <i><interface-type></i> <i><interface-id></i>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po <i>interface-id</i> is in <i>slot/port</i> 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	no switchport map protocols-group <i><Group id integer(0-2147483647)></i> >	<p>Removes the protocol groups from interface mode.</p> <p><i>Group id</i> – Protocol Group Identifier</p>
Step 4	Exit	Exits VLAN configuration mode.
Step 5	no map protocol {arp ip rarp ipx novell netbios appletalk other <i><aa:aa or aa:aa:aa:aa:aa></i> } {enet-v2 RFC1042 llcOther snap8021H snapOther}	<p>Removes the protocol group.</p> <p>Before removing any protocol group, it must have been removed from all interfaces.</p>
Step 6	<p>no vlan <i><vlan-list></i></p> <p>or</p> <p>vlan <i><vlan-list></i></p> <p>no ports <i><ports-list></i> untagged</p>	<p>Removes the VLANs created for protocol based VLANs.</p> <p>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.</p> <p><i>vlan-list</i> – 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.</p>
Step 7	<p>show vlan protocols-group</p> <p>show protocol-vlan</p>	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 frames types – tagged, untagged and priority tagged.



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

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

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p><i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces. It may be a port channel identifier for port channel interfaces.</p> <p>To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g. : int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g. : int range fx 0/1-10, fx 0/20</p>
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 hopping. To prevent VLAN hopping, 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 hopping if needed.

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type> <interface-id> or interface range <interface-type> <interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po <i>interface-id</i> is in <i>slot/port</i> 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

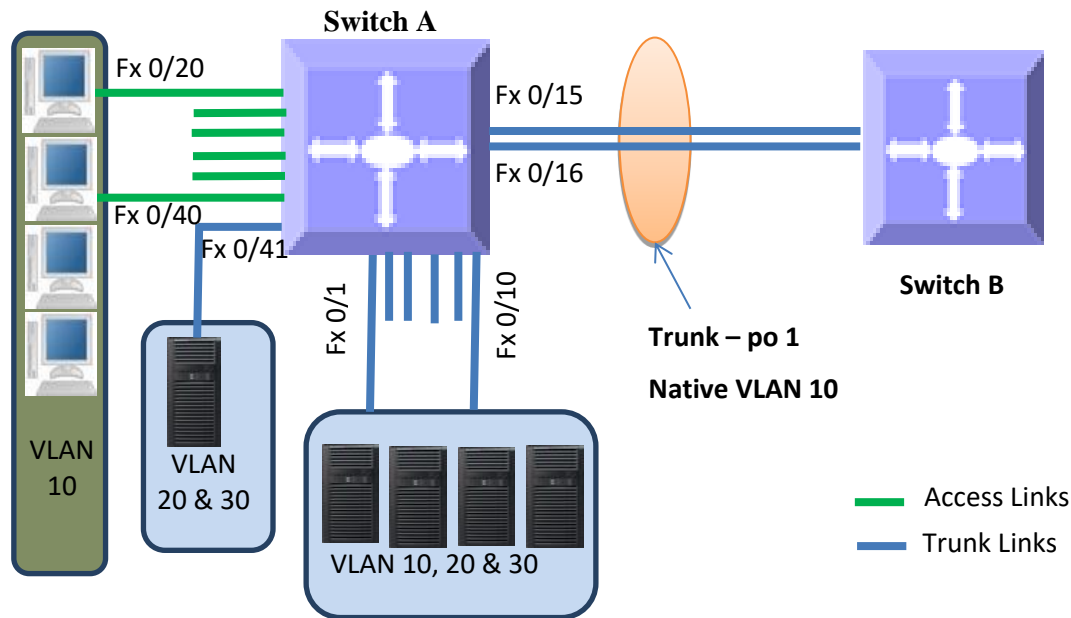
```
SMIS# configure terminal
SMIS(config)# interface range fx 0/1-10
SMIS(config-if)# no switchport ingress-filter
SMIS(config-if)# exit
```

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.

Figure VLAN-8: VLAN Configuration Example



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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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 runnning-config
```

Building configuration...

ID	Hardware Version	Firmware	OS
0	SBM-25G-100 (B8 R1.01)	1.0.0.0	1.0.6

```
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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SMIS#

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.

Port Mode	Communicates with
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.

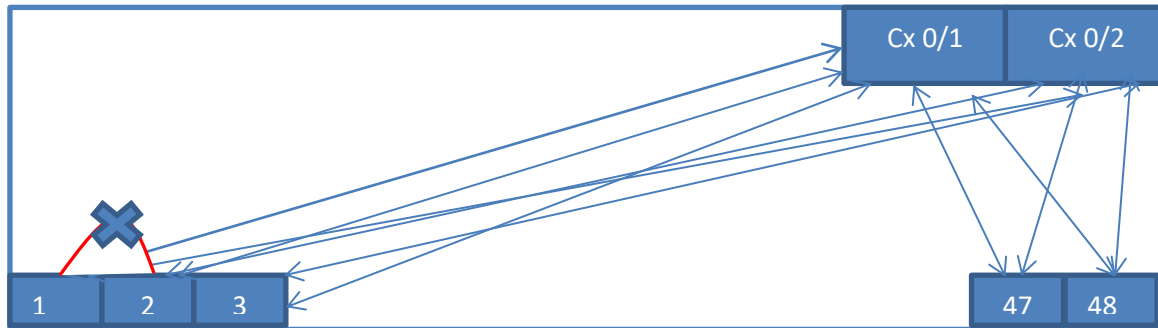
Maximum of 24 different communities can be configured in the switch.

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.

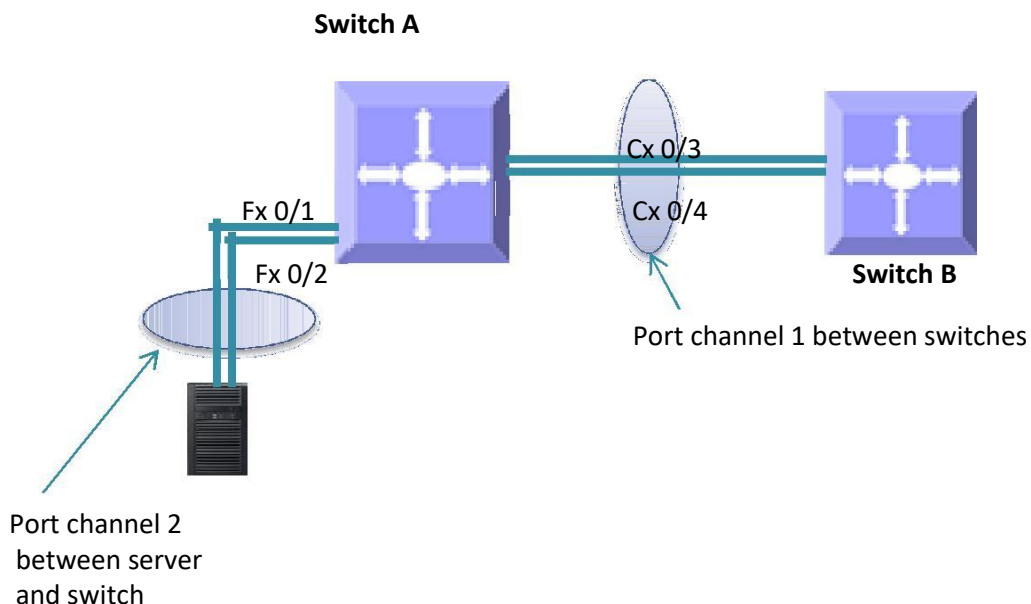
Link Aggregation provides the following advantages:

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 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

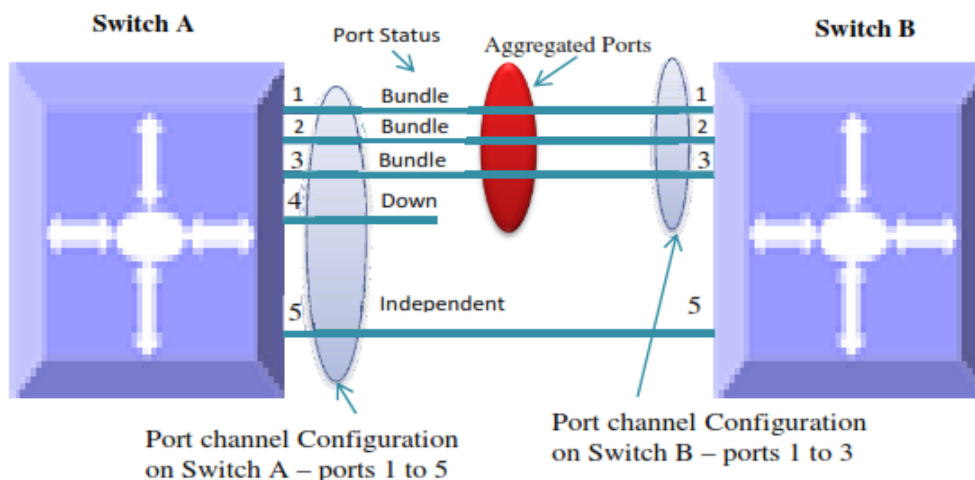


Figure LA-2: Dynamic Link Aggregation shows an example of a port channel configuration with port status and aggregated ports. In this example, port 5 is not configured on LACP mode on switch B, and is therefore shown as being in the “independent” state and not part of the aggregated ports.

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface port-channel <channel-group-number> Or no interface range port-channel <channel-group-number>	Creates a port channel using “interface port—channel” command. <i>channel-group-number</i> – may be any number from 1 to 65535. To configure multiple port channel interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range po 1-3 To provide multiple interfaces or ranges, separate with a comma (,). E.g. : int range po 1, 2
Step 3	description <string>	Optional step - adds any name string to

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>the port channel interfaces using the description command.</p> <p>The <i>string</i> may be up to 64 characters in length.</p> <p>The port channel description strings will not affect the member ports description strings configurations.</p>
Step 4	mtu < <i>framesize</i> >	<p>Optional step.</p> <p>Configures the MTU for the port channel interfaces.</p> <p><i>framesize</i> may be any number from</p> <p>Port channel MTU will be used on its all member ports.</p>
Step 5	VLAN Configurations	<p>Optional step – configures the VLAN parameters for port channel interfaces.</p> <p>Refer to the VLAN configuration guide for all VLAN configuration details.</p>
Step 6	Spanning Tree Configurations	<p>Optional step – configures the spanning tree parameters for port channel interfaces.</p> <p>Refer to the spanning Tree configuration guide for all spanning tree configuration details.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 7	End	Exits the configuration mode.
Step 8	<pre>show interface port-channel <channel-group-number> show etherchannel [[channel-group-number] { detail load-balance port port-channel summary protocol}]</pre>	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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	<pre>interface <interface-type><interface-id> Or interface range <interface-type><interface-id></pre>	Enters the interface mode. <i>interface-type</i> – may be any of the

		<p>following:</p> <p>fx-ethernet – fx</p> <p>cx-ethernet – cx</p> <p><i>interface-id</i> is in <i>slot/port</i> 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</p> <p>ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	channel-group <channel-group-number> mode {active passive on}	<p>Configures the interfaces as member ports for the given port channel.</p> <p><i>channel-group-number</i> – The port channel to which these member ports are added.</p> <p>For LACP aggregation, use the active or passive mode.</p> <p>For static link aggregation, use mode on.</p>
Step 4	End	Exits the interface configuration mode.
Step 5	show interface port-channel <channel-group-number>	Displays the configured port channel information.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>show etherchannel [[channel-group-number] { detail load-balance port por t-channel summary protocol}]</pre>	
Step 6	<pre>write startup-config</pre>	Optional step – saves this port channel configuration to be part of startup configuration.



The MTU, VLAN and spanning tree parameters of a port channel interface will be used on its member ports. After adding a port to any port channel, users should not configure MTU, VLAN and spanning tree parameters on that port. Instead users should configure MTU, VLAN and spanning tree parameters on the port channel interfaces.

The examples below show various ways to create port channels.

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

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

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

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

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.

```
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.

```
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id>	Enters the interface mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<p>Or</p> <p>interface range <i><interface-type><interface-id></i></p> <p>....</p>	<p><i>interface-type</i> – may be any of the following:</p> <p>fx-ethernet – fx</p> <p>cx-ethernet – cx</p> <p><i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces.</p> <p>To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	no channel-group	Removes the member ports from the port channel.
Step 4	End	Exits the configuration mode.
Step 5	<p>show interface port-channel <i><channel-group-number></i></p> <p>show etherchannel <i>[[channel-group-number] {</i></p> <p><i>detail load-balance port port-channel </i></p>	Displays the configured port channel information.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	summary protocol }}	
Step 6	write startup-config	Optional step – saves this port channel configuration to be part of startup configuration



When a port is removed from a port channel, that port will 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

Step	Commands	Description
Step 1	configure terminal	Enters the configuration mode
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 Interface-id is in slot/port format for

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>all physical interfaces.</p> <p>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(,).</p> <p>E.g.: int range fx 0/1-10,fx 0/1-20</p>
Step 3	no channel-group	Removes the member ports from the port channel.
Step 4	channel-group <channel-group-number> mode {active passive on}	<p>Configures the interfaces as member ports with the given port mode.</p> <p>For LACP aggregation, use the active or passive mode.</p> <p>For static link aggregation, use the mode on.</p> <p><i>channel-group-number</i> – The port channel to which these member ports are added.</p>
Step 5	LACP fallback {enable disable}	<p>If LACP fallback is enabled and the member interface doesn't receive LACP packets from peer, then the interface goes to independent mode. LACP fallback is enabled by default.</p> <p>If LACP fallback is disabled and the member interface doesn't receive LACP packets from peer, then the interface will be disabled but still listen for LACP packets.</p>
Step 6	End	Exits the interface configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 7	<pre>show interface port-channel <channel-group-number> show etherchannel [[channel-group-number] { detail load-balance port port-channel summary protocol}]</pre>	Displays the configured port channel information.
Step 8	<pre>write startup-config</pre>	Optional step – saves this port channel configuration to be part of startup configuration.

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

Step	Command	Description
Step 1	<pre>configure terminal</pre>	Enters the configuration mode
Step 2	<pre>no interface port-channel <channel-group-number> Or no interface range port-channel <channel-group-number></pre>	<p>Removes the port channel interface.</p> <p><i>channel-group-number</i> – may be any number from 1 to 65535.</p> <p>To remove multiple port channel</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>interfaces, use the “no interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: no int range po 1-3</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g. : no int range po 1, 2</p>
Step 3	<pre>show running-config show etherchannel</pre>	Displays the port channel information.
Step 4	<pre>write startup-config</pre>	Optional step – saves this port channel configuration to be part of startup configuration.



When a port channel is removed, all its member ports will be 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
```

6.6.4 LACP Parameters

Users can configure the following LACP parameters on Supermicro switches.

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

6.6.4.1 LACP System Priority

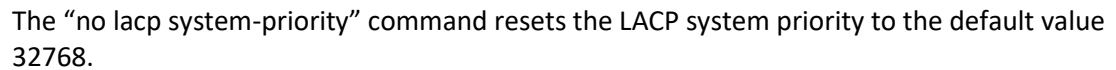
Every LACP device needs to have a globally unique system identifier. This globally unique system identifier is formed by combining a switch's MAC address and LACP system priority.

LACP system priority is also used to decide the active member ports of a port channel. When more than 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	lacp system-priority <system-priority>	Configures the LACP system priority. <i>system-priority</i> – 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



```
SMIS(config-if)# exit
```

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.

Follow the steps below to modify the LACP port priority.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>physical interfaces.</p> <p>To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	lacp port-priority <port-priority>	<p>Configures the LACP port priority.</p> <p><i>port-priority</i> – may be any value from 0 to 65535</p>
Step 4	End	<p>Exits the configuration mode.</p>
Step 5	<p>show running-config</p> <p>show etherchannel</p>	<p>Displays the configured port priority information.</p>
Step 6	write startup-config	<p>Optional step – saves this port priority configuration to be part of startup configuration.</p>



SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

The example below shows the steps necessary to configure the port priority.

Configure the port priority as 10 for cx 0/1 and 20 for cx 0/2.

```
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# lacp port-priority 10
SMIS(config-if)# exit
SMIS(config)# interface cx 0/2
SMIS(config-if)# lacp port-priority 20
SMIS(config-if)# exit
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	interface <interface-type><interface-id> Or interface range <interface-type><interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the

	<p>....</p>	<p>following:</p> <p>fx-ethernet – fx</p> <p>cx-ethernet – cx</p> <p><i>interface-id</i> is in <i>slot/port</i> format for all physical interfaces.</p> <p>To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers.</p> <p>E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,).</p> <p>E.g.: int range fx 0/1-10, fx 0/20</p>
Step 3	lacp timeout {long short}	<p>Configures the LACP port timeout.</p> <p>long – LACP messages are expected to be received once every 30 seconds.</p> <p>short – LACP messages are expected to be received once every second.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	End	Exits the configuration mode.
Step 5	show running-config show etherchannel	Displays the configured port priority information. .
Step 6	write startup-config .	Optional step – saves this port timeout configuration to be part of startup configuration.



The “no lacp timeout” command resets the LACP timeout to the default value of “long”.

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

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

```
SMIS# configure terminal
```

```
SMIS(config)# interface range cx 0/1-2
```

```
SMIS(config-if)# lacp timeout short
```

```
SMIS(config-if)# exit
```

6.6.4.4 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

Step	Command	Description

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 1	configure terminal	Enters the configuration mode.
Step 2	interface <interface-type><interface-id> Or interface range <interface-type><interface-id>	Enters the interface mode. <i>interface-type</i> – may be any of the following: fx-ethernet – fx cx-ethernet – cx
Step 4		Exits the configuration mode.
Step 5	show running-config show etherchannel	Displays the configured port priority information.
Step 6	write startup-config	Optional step – saves this LACP wait



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.

Destination MAC Based

- Packets will be distributed across the member ports based on the source and destination MAC addresses of the packet.

source based IP

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

Destination based IP

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

Source and Destination IP Based

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	port-channel load-balance {src-mac dest-mac src-dest-mac src-ip dest-ip src-dest-ip} [<channel-group>]	<i>channel-group</i> is the port channel identifier to which this load balancing algorithm is configured. <i>channel-group</i> number is an optional parameter for this configuration. When <i>channel-group</i> is not provided, the given port channel algorithm will be applied to all port channel interfaces.
Step 3	End	Exits the configuration mode.
Step 4	show running-config	Displays the configured load balancing information.
Step 5	write startup-config	Optional step – saves this load balancing configuration to be part of startup configuration.

Follow the below steps to configure the load balancing algorithm



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

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

SMIS# configure terminal

SMIS(config)# port-channel load-balance src-dest-ip

SMIS(config-if)# exit

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

Follow the steps below to disable the link aggregation feature.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	set port-channel enable	Enables 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.

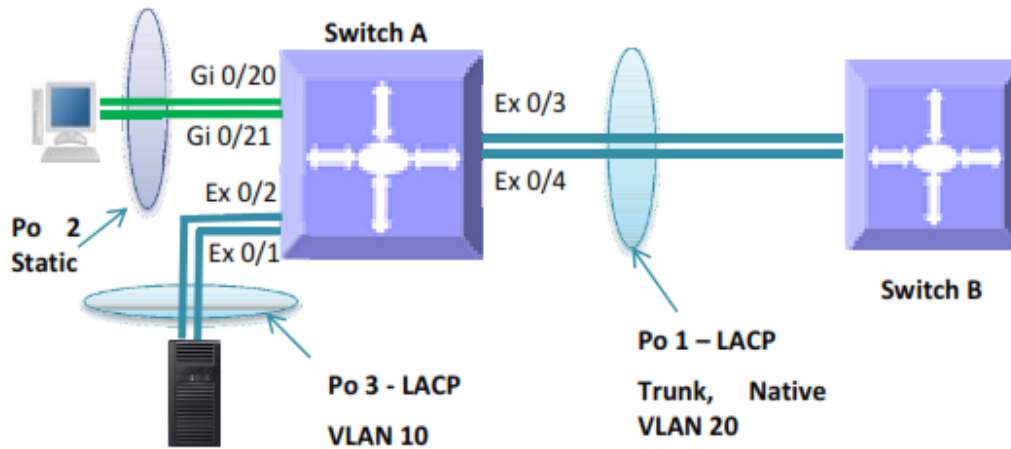
6.6.6 Link Aggregation Configuration Example

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

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

- Aggregate ports Fx 0/20 and Fx 0/21 statically.

Figure LA-3: Link Aggregation Configuration Example



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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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
```


SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	The port or port lists on which this layer-2 ECMP load balancing needs to be applied.
Step 3	l2-ecmp-group <l2-ecmp-group-number(1-65535)>	Configures the ports to be member of the ECMP group.
Step 4	end	Ends the configuration mode.
Step 5	write startup-config	Saves this L2 ECMP configuration to be part of startup configuration.

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id> or	The port or port lists on which this layer-2 ECMP load balancing needs to be removed.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	interface range <interface-type><interface-id>	
Step 3	no l2-ecmp-group	Removes the port(s) from the ECMP group.
Step 4	end	Ends the configuration mode.
Step 5	write startup-config	Saves the configuration changes to the startup configuration.



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.
```

Member Ports	Status
--------------	--------

Fx0/1	Up
-------	----

Fx0/2	Up
-------	----

Fx0/3	Down
-------	------

Fx0/4	Up
-------	----

Fx0/5	Up
-------	----

```
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

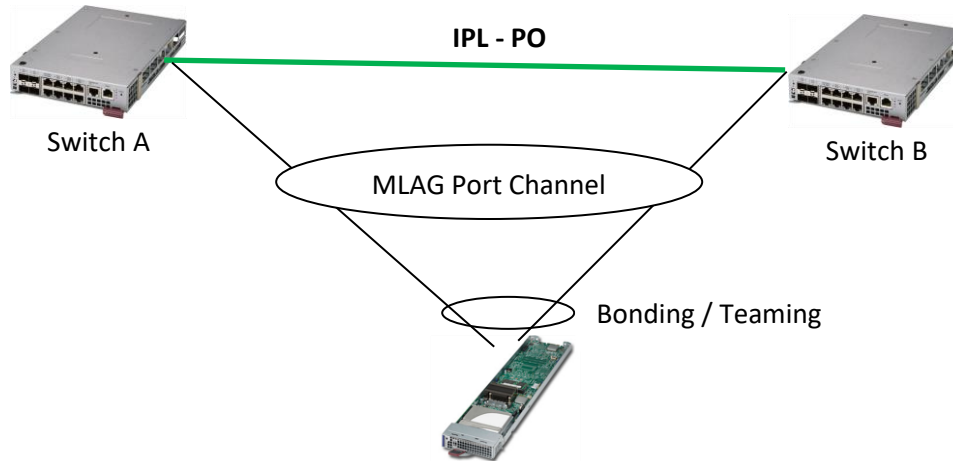


Figure MLAG1

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

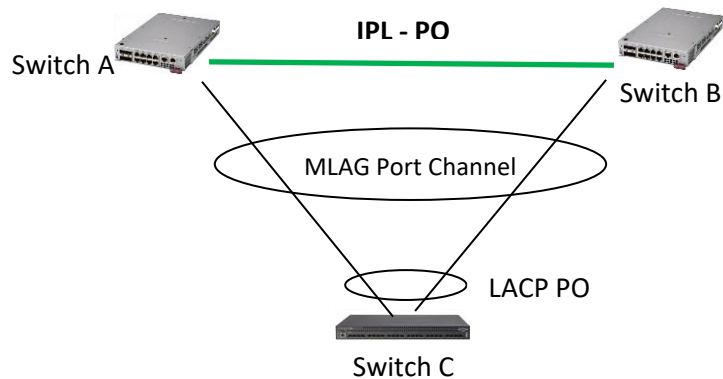


Figure MLAG-2

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

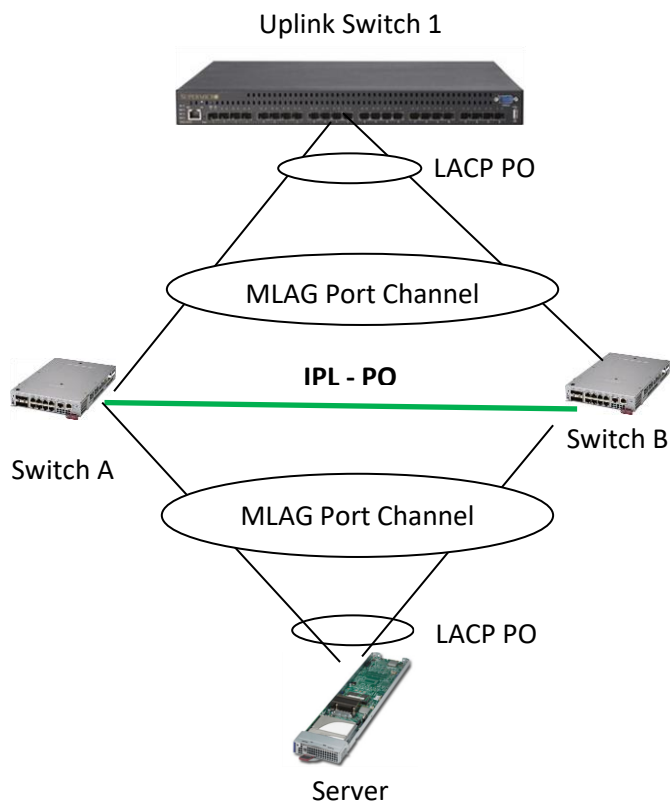


Figure MLAG-3

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

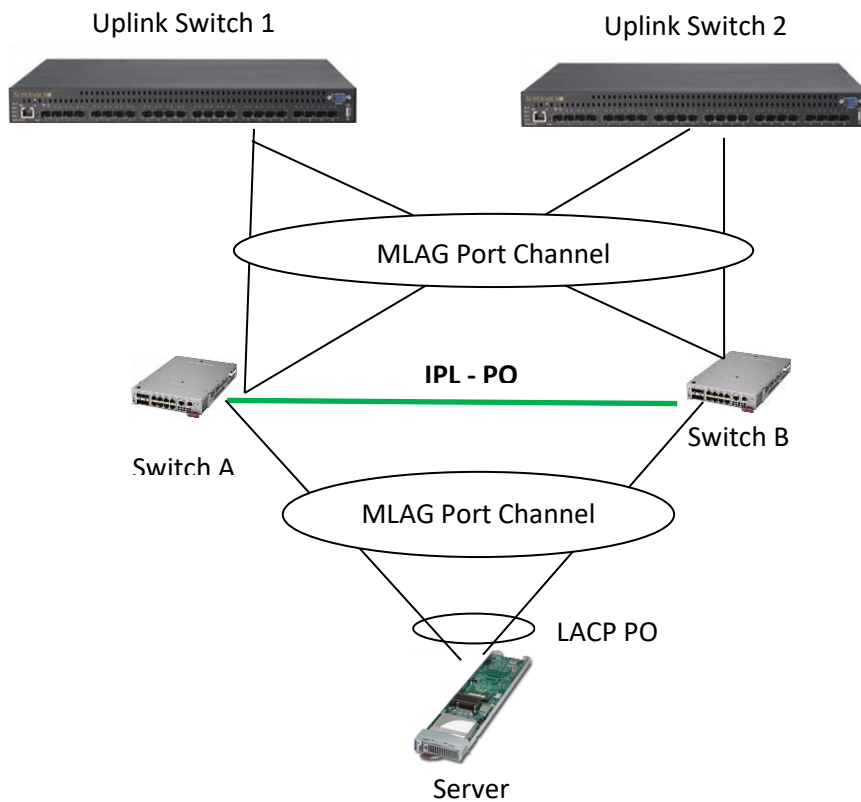


Figure MLAG-4

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

Parameter	Default Value
System ID	None
System priority	32768
Keep alive time	3 seconds
IPL interface	None
MLAG status	Disabled

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mlag system-identifier <aa:aa:aa:aa:aa:aa>	Configure the system ID <aa:aa:aa:aa:aa:aa> - Specify any unicast MAC address to be used as the MLAG system ID
Step 3	end	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	show mlag detail	Displays the MLAG configuration details
--------	------------------	---



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mlag system-priority <0-65535>	Configure the MLAG system priority
Step 3	End	Exits the configuration mode.
Step 4	show mlag detail	Displays the MLAG configuration details



The “**no mlag system-priority**” command deletes the MLAG system priority.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mlag keepalive-time <3-90>	Configure the MLAG keepalive time.
Step 3	End	Exits the configuration mode.
Step 4	show mlag detail	Displays the MLAG configuration details



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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mlag interface port-channel <port-channel-id (1-65535)>	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.
Step 3	End	Exits the configuration mode.
Step 4	show mlag detail	Displays the MLAG configuration details
Step 5	show mlag stp	Displays the MLAG Spanning Tree details



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface port-channel <channel-group-number>	Creates a port channel using “interface port-channel” command. <i>channel-group-number</i> – may be any number from 1 to 65535.
Step 3	mlag enable	Configure MLAG link from switch to the partner devices.
Step 4	end	Exits the configuration mode.
Step 5	show mlag interface	Displays the details of MLAG interface between peers and partner devices.



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.

Requirements	Comments
VLAN configurations for MLAG interfaces	

Spanning tree configurations for MLAG interfaces	
ACL configurations related to MLAG interfaces	
QoS configurations related to MLAG interfaces	
MAC aging time	
Static MAC entries	
MTU on MLAG and IPL interfaces	

9 Spanning Tree

Switches are interconnected to provide network access to 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 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.

Root Port	<ul style="list-style-type: none">•Port to reach the root switch with lowest path cost•Root ports forwards the traffic
Designated Port	<ul style="list-style-type: none">•Loop free connection to the other switch on the LAN• Designated ports forwards the traffic
Alternate Port	<ul style="list-style-type: none">• Redundant path to the root switch•Alternate ports do not forward the traffic
Blocked Port	<ul style="list-style-type: none">•Redundnat path to other switches on the LAN•Blocked ports do not forward the traffic

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:

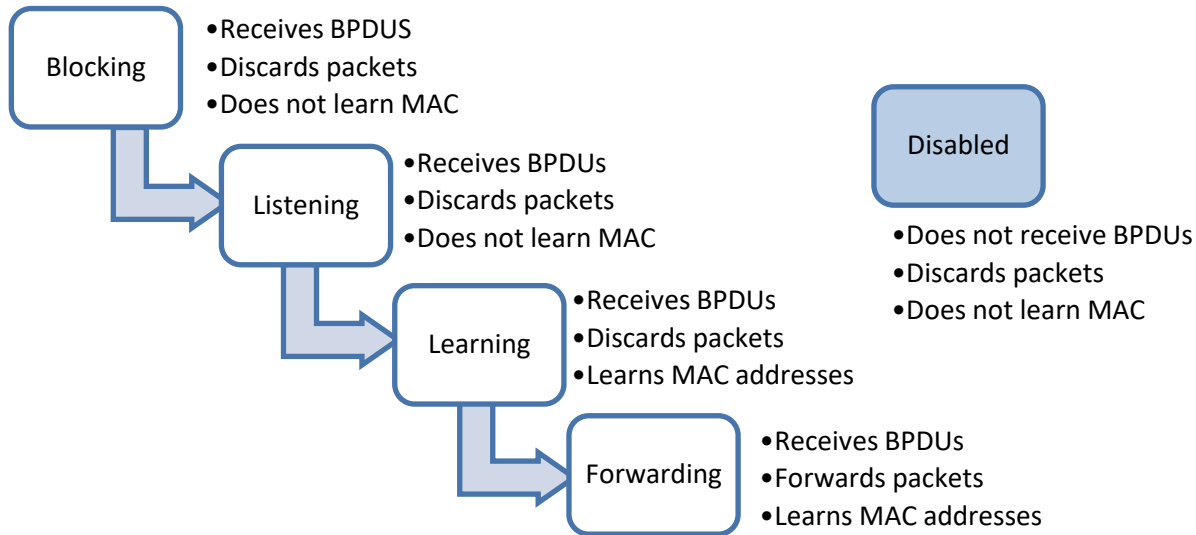
Bridge Identifier: Combination of switch MAC address and switch spanning tree priority

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, switch uses the received BPDU information to decide the root bridge and recalculates the spanning tree. If the received BPDU information is inferior, 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.

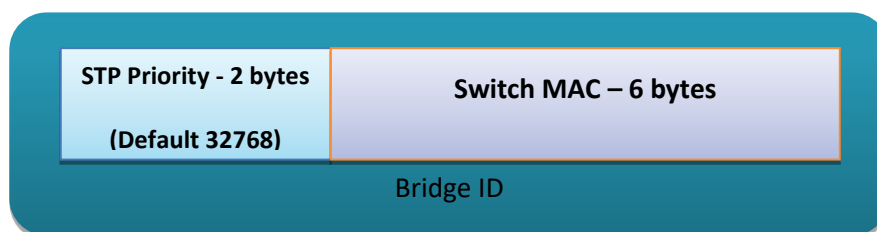
Rapid spanning tree protocol (RSTP) provides faster topology convergence. Spanning tree (STP) takes more than 30 seconds to move a port to forwarding state. But RSTP can move a port to the forwarding state within 3 times of hello interval (default hello interval is 2 seconds). RSTP is compatible with 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. In case 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

Parameter	Default Value										
Spanning tree global status	Enabled										
Spanning tree port status	Enabled										
Spanning tree mode	MST										
Switch priority	32768										
Port priority	128										
Port cost	<table> <tr> <th>Port Speed</th><th>Default Path Cost</th></tr> <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> </table>	Port Speed	Default Path Cost	10 Mbps	2000000	100 Mbps	200000	1 Gbps	20000	10 Gbps	2000
Port Speed	Default Path Cost										
10 Mbps	2000000										
100 Mbps	200000										
1 Gbps	20000										
10 Gbps	2000										
Hello time	2 seconds										
Forwarding time	15 seconds										
Maximum aging time	20 seconds										
Transmit hold count	3										
Max hops	20										
Path cost method	Long										
MST region name	Switch MAC address										
MST region revision	0										
Spanning tree compatibility	In MSTP mode, the default compatibility is MSTP and in RSTP mode the default compatibility is RSTP										
Root guard	Disabled										
Topology change guard	Disabled										
Port fast	Disabled										
Auto edge	Enabled										
Link type	Full duplex ports – point to point links										

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no spanning-tree	Disable the spanning tree globally
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree	Displays the spanning tree information.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“spanning-tree” command enables the spanning tree globally.

The examples below show ways to disable / enable the spanning tree function on Supermicro switches.

Disable the spanning tree.

```
SMIS# configure terminal
```

```
SMIS(config)# no spanning-tree
```

```
SMIS(config)# end
```

Enable the spanning tree.

```
SMIS# configure terminal
```

```
SMIS(config)# spanning-tree
```

```
SMIS(config)# end
```

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to disable the spanning tree on ports.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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
Step 3	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<instance-id>disable	Disables the spanning tree on the port. instance-id – The MST instance identifier may be from 1 to 16.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree interface <interface-type><interface-id> show running-config interface <interface-type><interface-id>	Displays the spanning tree port information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	spanning-tree mode mst	Configures the switch to operate in MST mode.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree	Displays the spanning tree mode information.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	spanning-tree mst configuration	Enters the MST configuration mode
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	spanning-tree mode rst	Configures the switch to operate in RSTP mode.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree	Displays the spanning tree mode information.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	To force the spanning tree compatibility as STP spanning-tree compatibility stp To force the spanning tree compatibility as RSTP spanning-tree compatibility rst To force the spanning tree compatibility as MSTP spanning-tree compatibility mst	Configures the spanning tree compatibility.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree	Displays the spanning tree mode information.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description																
Step 1	configure terminal	Enters the configuration mode																
Step 2	<p>To configure the switch priority in RST mode: spanning-tree priority <priority-value></p> <p>To configure the switch priority for the default MST instance 0: spanning-tree priority <priority-value></p> <p>To configure the switch priority for particular MST instance: spanning-tree mst <instance-id> priority <priority-value></p>	<p>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.</p> <table><tr><td>0</td><td>4096</td><td>8192</td><td>12288</td></tr><tr><td>16384</td><td>20480</td><td>24576</td><td>28672</td></tr><tr><td>32768</td><td>36864</td><td>40960</td><td>45056</td></tr><tr><td>49152</td><td>53248</td><td>57344</td><td>61440</td></tr></table> <p>The default priority value is 32768.</p>	0	4096	8192	12288	16384	20480	24576	28672	32768	36864	40960	45056	49152	53248	57344	61440
0	4096	8192	12288															
16384	20480	24576	28672															
32768	36864	40960	45056															
49152	53248	57344	61440															

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		instance-id – The MST instance identifier may be from 1 to 16.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree bridge priority	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 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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
Step 3	To configure the port priority in RST mode: spanning-tree port-priority <priority-value> To configure the port priority for the default MST instance 0: spanning-tree port-priority <priority-value> To configure the port priority for particular MST instance: spanning-tree mst <instance-id>port-priority <priority-value>	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.
Step 4	end	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Port Speed	Default Path Cost
10 Mbps	2000000
100 Mbps	200000
1 Gbps	20000
10 Gbps	2000

Follow the steps below to change spanning tree path cost for ports.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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
Step 3	To configure the port priority in RST mode: spanning-tree cost<cost-value> To configure the port priority for the default MST instance 0: spanning-tree cost<cost-value> To configure the port priority for particular MST instance: spanning-tree mst <instance-id>cost<cost-value>	Configures the port spanning tree path cost. cost-value – Spanning tree port priority value may be from 0 to 200000000. The default path cost is calculated based on the port speed. instance-id – The MST instance identifier may be from 1 to 16.
Step 4	end	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.



“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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	To configure the hello time in RST mode: spanning-tree hello-time<time-value>	Configures the hello time interval. time-value – Hello time value may be 1 or 2 seconds. The default hello time is 2 seconds.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree interface <interface-type><interface-id>	Displays the spanning tree port parameters including the hello time values.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		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	To configure the hello time in MST mode: spanning-tree mst hello-time<time-value>	Configures the hello time interval. time-value – Hello time value may be 1 or 2 seconds. The default hello time is 2 seconds.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree bridge hello-time	Displays the spanning tree hello time.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“nosp spanning-tree msth hello-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 porthello 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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 show spanning-tree	Displays the spanning tree configuration parameters including the switch priority values.
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 shows the way to configure the spanning tree max age.

Configure the max age as 12.

```
SMIS# configure terminal
```

```
SMIS(config)# spanning-tree max-age 12
```

```
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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.
 $2 * (\text{Forward Time} - 1) \geq \text{MaxAge}$

Follow the steps below to change the forwarding time.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to change the max hops.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	To configure the max age time: spanning-tree mst max-hops <maxhops-value>	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.
Step 3	end	Exits the configuration mode.
Step 4	show spanning-tree mst	Displays the spanning tree max hops along with other MST information.
Step 5	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	To configure the path cost method as short spanning-tree pathcost method short To configure the path cost method as long spanning-tree pathcost method long	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.



“nospanning-tree pathcost method” command resets the path cost method to default value.

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	spanning-tree transmit hold-count <count_value>	Configures the transmit hold count value. Count-value – Transmit hold count value may be from 1 to 10. The default transmit hold count value is 3.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	Enters the port interface mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.</p> <p>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</p>
Step 3	spanning-tree restricted-role	<p>Enables the root guard feature.</p> <p>The default option is the root guard feature disabled.</p>
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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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
Step 3	spanning-tree restricted-tcn	Enables the topology guard feature. The default option is the topology guard feature disabled.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree detail	Displays the spanning tree topology guard information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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 (-)

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20
Step 3	spanning-tree portfast	Enables the port fast feature. The default setting is the port fast feature disabled.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree detail	Displays the spanning tree port fast information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	Enters the port interface mode. interface-type – may be any of the following:

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>fx-ethernet – fx cx-ethernet – cx port-channel – po</p> <p>interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces.</p> <p>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</p>
Step 3	To enable the auto-edge spanning-tree auto-edge	Enables or disabled the auto edge feature.
	To disable the auto-edge no spanning-tree auto-edge	The default setting is the auto edge feature enabled.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree detail	Displays the spanning tree auto edge information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

In point to point links spanning tree negotiates with other end switchesto 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	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
Step 3	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	Configures the link type.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree detail	Displays the spanning tree auto edge information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.



“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
```

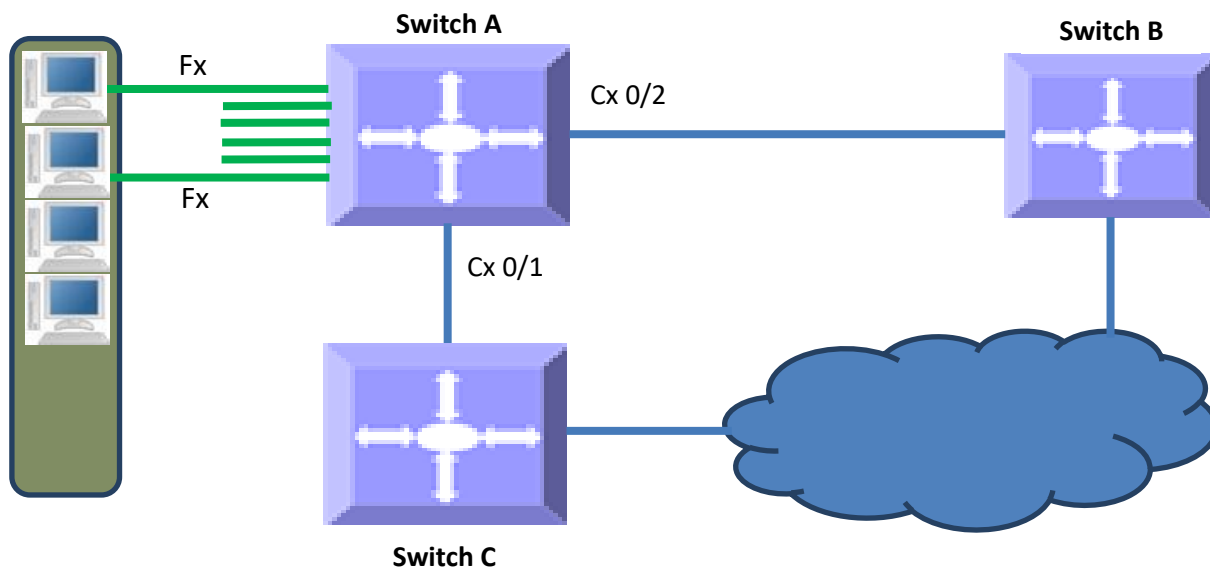
```
SMIS(config-if)# end
```

9.23 Spanning Tree Configuration Examples

Configure the following requirements on the switches as shown below in FigureMSTP-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.1Spanning Tree MSTP Configuration Example



Configurations on switch A

```
SMIS# configure terminal
```

```
# Create the VLANs 100 and 200
```

```
SMIS(config)# vlan 100,200
```

```
SMIS(config-vlan)# exit
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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:e3:56:12priority 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#

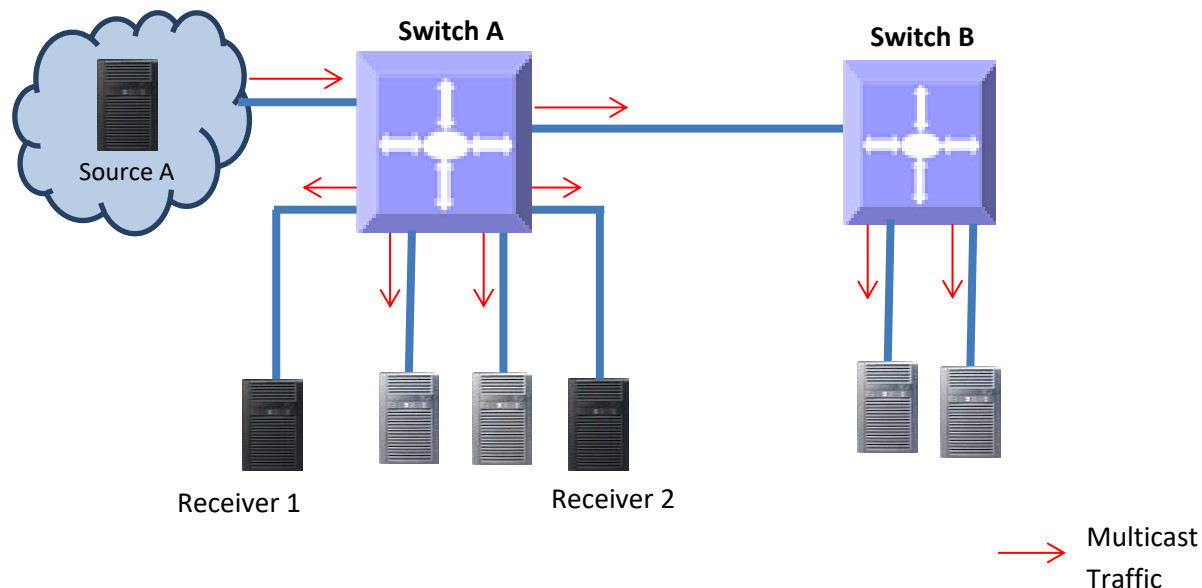
10 IGMP Snooping

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**

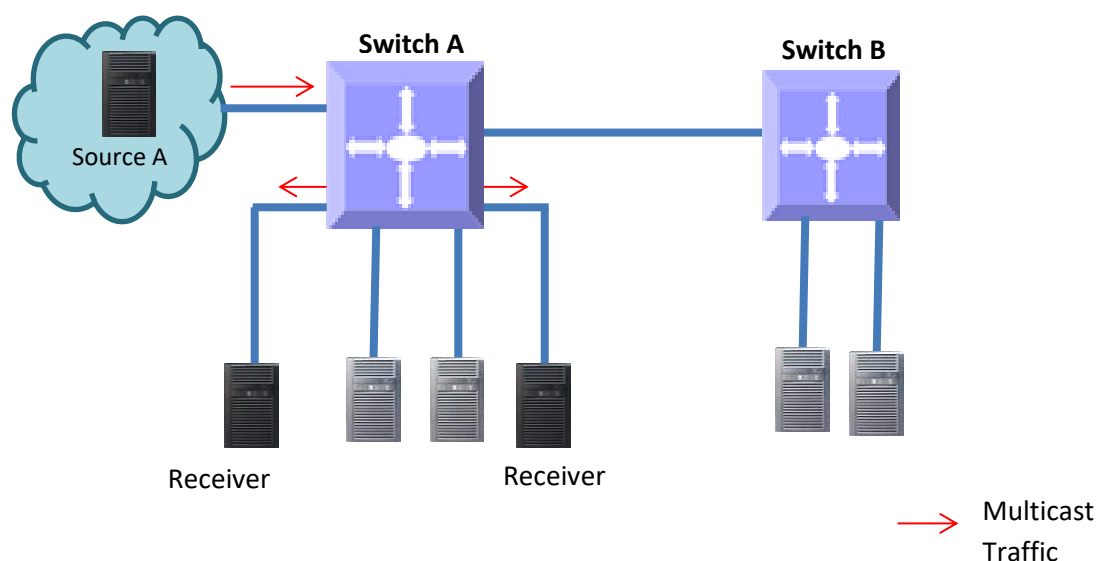


The IGMP snooping function helps the switches to forward IPv4 multicast traffic to only the ports that require IPv4 multicast traffic. This function saves network bandwidth by preventing the unnecessary flooding of IPv4 multicast traffic.

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.

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	ip igmp snooping	Enables IGMP snooping globally.
Step 3	vlan<vlan-list>	Enters the VLAN configuration mode. 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 enable IGMP snooping on all these VLANs.
Step 4	ip igmp snooping	Enables IGMP snooping on VLAN.
Step 5	end	Exits the configuration mode.
Step 6	show ip igmp snooping globals show ip igmp snooping vlan<vlan>	Displays the IGMP snooping information.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

The example below shows the commands to enable IGMP snooping.

Enable IGMP snooping for VLAN 1, 10 and 20.

```
SMIS# configure terminal
```

```
SMIS(config)# ip igmp snooping
```

```
SMIS(config)# vlan 1,10,20
```

```
SMIS(config-vlan)# ip igmp snooping
```

```
SMIS(config-vlan)# end
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
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 be applied on all these VLANs.
Step 3	ip igmp snooping version {v1 v2 v3}	Configures IGMP snooping version.
Step 5	end	Exits the configuration mode.
Step 6	show ip igmp snooping vlan<vlan>	Displays the IGMP snooping version information for the given VLAN.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

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

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

```
SMIS# configure terminal
```

```
SMIS(config)# vlan 10
```

```
SMIS(config-vlan)# ip igmp snooping version v3
```

```
SMIS(config-vlan)# exit
```

```
SMIS(config)# vlan 20
```

```
SMIS(config-vlan)# ip igmp snooping version v2
```

```
SMIS(config-vlan)# end
```

10.4 Multicast Router Ports

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

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



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
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 configure the router ports for all these VLANs.
Step 3	ip igmp snooping mrouter<interface-type><interface-id>	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.
Step 5	end	Exits the configuration mode.
Step 6	show ip igmp snooping mrouter [vlan<vlan>]	Displays the IGMP snooping router port information. If a VLAN identifier is provided it displays the router port for the given VLAN. If a VLAN identifier is not provided it displays the router ports for all the VLANs on the switch.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.



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

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

Configure port 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Follow the steps below to configure the group query interval.

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



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

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

Configure the group query interval time as 5 seconds.

```
SMIS# configure terminal
```

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

```
SMIS(config)# end
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	ip igmp snooping retry-count<count>	Configures the group specific query message retry count. count – may be any value from 1 to 5 seconds. The default is 2.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
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 enable the immediate leave for all these VLANs.
Step 3	ip igmp snooping fast-leave	Enables the IGMP immediate leave.
Step 4	end	Exits the configuration mode.

Step 5	show ip igmp snooping vlan<vlan>	Displays the IGMP snooping immediate leave information for the given VLAN.
Step 6	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.



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

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

Enable the immediate leave for the VLANs 10 and 20.

```
SMIS# configure terminal
```

```
SMIS(config)# vlan 10,20
```

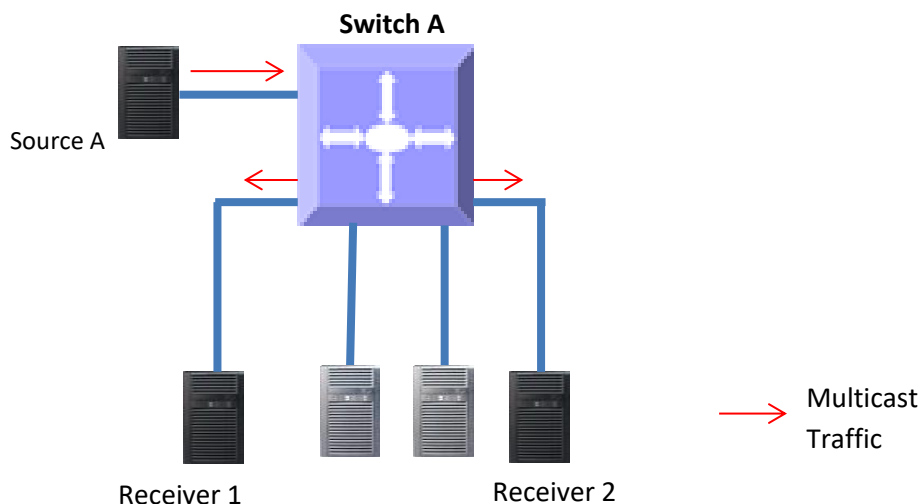
```
SMIS(config-vlan)# ip igmp snooping fast-leave
```

```
SMIS(config-vlan)# end
```

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**



SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

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

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

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	vlan<vlan-list>	Enters the VLAN configuration mode. 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 switch as an IGMP querier for all these VLANs.
Step 3	ip igmp snooping querier	Configures the switch to act as an IGMP querier.
Step 4	ip igmp snooping query-interval <interval-value>	Configures the periodic interval on the switch that will send IGMP queries. interval-value – may be any value from 60 to 600 seconds. The default value is 125 seconds.
Step 5	end	Exits the configuration mode.
Step 6	show ip igmp snooping vlan<vlan>	Displays the IGMP snooping querier configuration for the given VLAN.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	ip igmp snooping report-forward { all-ports router-ports }	<p>Configures the IGMP host member's report forwarding behavior.</p> <p>Use all-ports to configure a switch to forward IGMP host member reports to all ports.</p> <p>Use router-ports to configure the switch to forward the IGMP host member reports to the router ports only.</p> <p>The default behavior is router-ports.</p>
Step 3	end	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	show ip igmp snooping globals	Displays the IGMP snooping information.
Step 5	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.



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

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

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

SMIS# configure terminal

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

SMIS(config)# end

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.

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



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

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

Configure the port purge interval value to 900 seconds.

SMIS# configure terminal

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

SMIS(config)# end

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 aIGMP report contains IGMP version 3 reports, switches will forward these reports to multicast routers without suppressing.

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

Follow the steps below to configure the report suppression interval.

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



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

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

Configure the port report suppression interval value as 90 seconds.

```
SMIS# configure terminal
```

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

```
SMIS(config)# end
```

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.

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



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

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

Enable IGMP snooping proxy reporting.

```
SMIS# configure terminal
```

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

```
SMIS(config)# end
```


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.

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	ip igmp snooping send-query enable	Enables the switch to send general IGMP queries when spanning tree topology changes.
Step 3	end	Exits the configuration mode.
Step 4	show ip igmp snooping globals	Displays the IGMP snooping information.
Step 5	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.



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

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

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

```
SMIS# configure terminal
```

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

```
SMIS(config)# end
```

10.12 Disabling IGMP Snooping

IGMP snooping is disabled by default in Supernetwork switches.

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

Follow the steps below to disable IGMP snooping.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	no ip igmp snooping	Disables IGMP snooping globally.
Step 3	vlan<vlan-list>	<p>Enters the VLAN configuration mode.</p> <p>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.</p> <p>If multiple VLANs are provided, the next step will disable IGMP snooping on all these VLANs.</p>
Step 4	no ip igmp snooping	Disables IGMP snooping in VLAN.
Step 5	end	Exits the configuration mode.
Step 6	show ip igmp snooping globals show ip igmp snooping vlan<vlan>	Displays the IGMP snooping information.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

The 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
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.

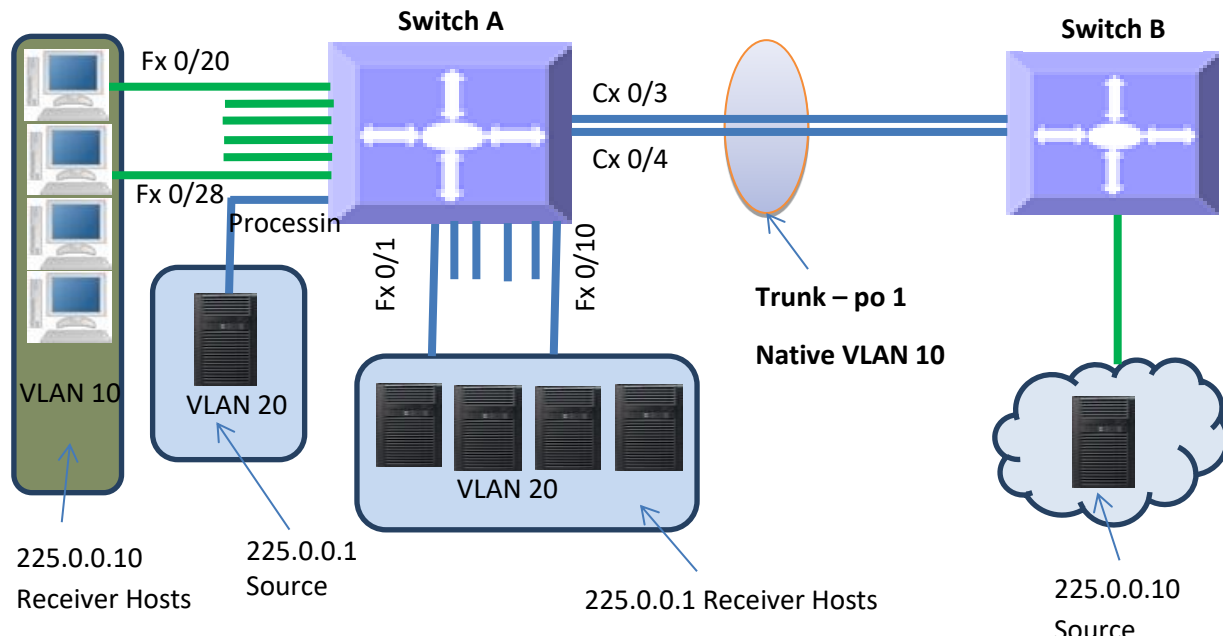
10.14 IGMP Snooping Configuration Example

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-4IGMP Snooping Configuration Example

SBM-25G-100 / MBM-XEM-100 Configuration Guide



SMIS# configure terminal

Create all the required VLANs first

```
SMIS(config)# vlan 10,20
```

```
SMIS(config-vlan)# exit
```

Add member ports to VLAN 10

```
SMIS(config)# int range 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)#switchporttrunk 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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

exitvlan 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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
```


interfacepo 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 Layer3 or Layer 4 TCP/UDP parameters.

Every packet entering the switch is checked for the configured ACLs. If any packet contents match any of the configured 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.

Three types of ACL	MAC Extended ACL
	IP Standard ACL
	IP Extended ACL

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enter the configuration mode
Step 2	mac access-list extended { <access-list-number> <access-list-name> }	Creates a MAC Extended ACL using the mac-access-list extended command. access-list-number—can be any number from 1 to 65535 access-list-name— any name string up to 32 characters.
Step 3	deny { any host<src-mac-address> } { any host<dest-mac-address> } <value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>] or permit { any host<src-mac-address> } { any host<dest-mac-address> } priority<value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>] or	Configures a deny ACL rule, a permit ACL rule or a redirect ACL rule. The source and destination MAC addresses are provided with the keyword host. The keyword any is used to refer any MAC addresses. If a source or destination MAC address is configured as any, the switch will not check that source or destination MAC address to match the packets for this ACL.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>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)>]</pre>	<p>The protocol keyword can be used to configure the Ethernet header Encap Type field to be matched to apply this ACL rule.</p> <p>This protocol is an optional parameter. If not provided, switch will not check this field while matching packets for this ACL.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Step 4	show access-lists	Displays the configured ACL rules
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.



Every ACL is applied to all ports by default. 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no mac access-list extended { <access-list-number> <access-list-name> }	Deletes a MAC Extended ACL using no mac-access-list extended command. access-list-number – the ACL number that needs to be deleted access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove a MAC Extended ACL .

```
SMIS# configure terminal
```

```
SMIS(config)# no mac access-list extended 50
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id> or interface range <interface-type><interface-id>	The port or port lists on which this MAC Extended ACL needs to be applied.
Step 3	mac access-group { <short (1-32768)> <string(32)> }	Adds the MAC Extended ACL to this port. access-list-number – the ACL number that needs to be added access-list-name – the name of the ACL that needs to be added
Step 4	show access-lists	Displays the configured ACL rules to make sure this port is added to the required ACL.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Step	Command	Description
Step 1	show access-lists or show access-lists mac { <access-list-number (1-32768)> <access-list-name> }	Enters the configuration mode access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL which needs to be displayed

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        : Fx0/2
Out Port            : ALLFilter Action      : Deny
Status              : Active
```

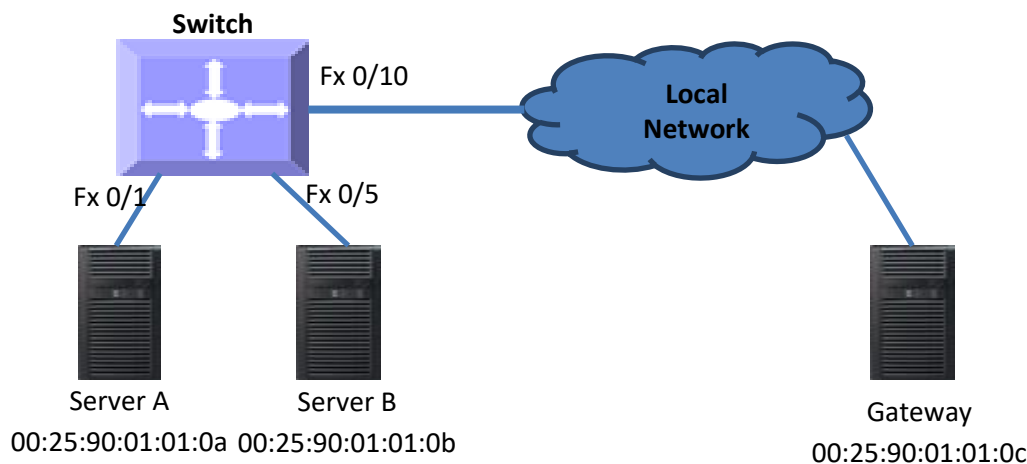
11.2.7 MAC Extended ACL Configuration

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 00:25:90:01:01:0c
```

ACL 2 Configuration

```
SMIS# configure terminal
```

```
SMIS(config)# mac access-list extended 2
```

SMIS(config-ext-macl)# redirect fx 0/5 host 00:25:90:01:01:0c any vlan 20

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 value to IP standard ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list standard { <access-list-number(1-32768)> <access-list-name> }	Creates an IP Standard ACL using ip-access-list standard command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	deny { any host<u>cast_addr</u> <u>cast_addr</u><ip_mask> } [{ any host<ip_addr> <ip_addr><ip_mask> }] [priority<value (1-255)>] or permit { any host<src-ip-address> <src-ip-address><mask> } [{ any host<dest-ip-address> <dest-ip-address><mask> }] [priority<value (1-255)>] or 1. redirect<interface-type><interface-id> { any host<src-ip-address> <src-ip-address><mask> } [{ any host<dest-ip-address> <dest-ip-address><mask> }] [priority<value (1-255)>]	Configure a deny ACL rule or permit ACL rule or redirect ACL rule. The source and destination IP addresses are provided with the keyword host. The keyword any is used to refer to any IP addresses. To configure a network IP, address and mask should be provided. A redirect ACL rule needs additional <interface-type><interface-id> parameters to define the port to which the packets matching this ACL rule need to be redirected. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.



Every ACL is applied to all ports by default. If any ACL needs to be applied only to particular ports, it needs to be configured as described in section Applying IP ACL to Interfaces.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 aIP 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 anIP Standard ACL rule 50being 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
SMIS(config-std-nacl)# deny 172.10.0.0 255.255.0.0 host 172.50.0.1
```

11.3.3 Removing IPStandard ACLs

Follow the below steps to remove IP Standard ACLs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no ip access-list standard { <access-list-number(1-32768)>r> <access-list-name> }	Deletes an IP Standard ACL using no ip-access-list standard command. access-list-number – the ACL number that needs to be deleted access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	Defines the port or port lists on which this IP Standard / Extended ACL needs to be applied
Step 3	ip access-group { <access-list-number (1-32768)> <access-list-name>	Adds the IP Standard / Extended ACL to this ingress port access-list-number – the ACL number that needs to be added access-list-name – the name of the ACL which needs to be added

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	show access-lists	Displays the configured ACL rules to make sure this port has added the required ACL
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration

The example below shows applying an IP Standard ACL rule 100 to ports fx 0/1 and fx 0/10.

SMIS# configure terminal

SMIS(config)# interface fx 0/1

SMIS(config-if)# ip access-group 100

SMIS(config-if)# exit

SMIS(config)# int fx 0/10

SMIS(config-if)# ip access-group 100

Removing an IP Standard / Extended ACL from a port

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	The port or port lists from which this IP Standard or Extended ACL needs to be removed
Step 3	no ip access-group [{ <access-list-number (1-65535)> <access-list-name> }]	Removes the IP Standard / Extended ACL from this ingress port access-list-number – the ACL number that needs to be removed from this interface access-list-name – the name of the ACL that needs to be removed from this interface
Step 4	show access-lists	Displays the configured ACL rules to make sure this port has been removed from the required ACL
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.



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

Step	Command	Description
Step 1	show access-lists or show access-lists ip { <access-list-number (1-32768)> <access-list-name> }	Enters the configuration mode access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL that needs to be displayed

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Status	Current status of the ACL. The status should normally be <i>active</i> . 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
```

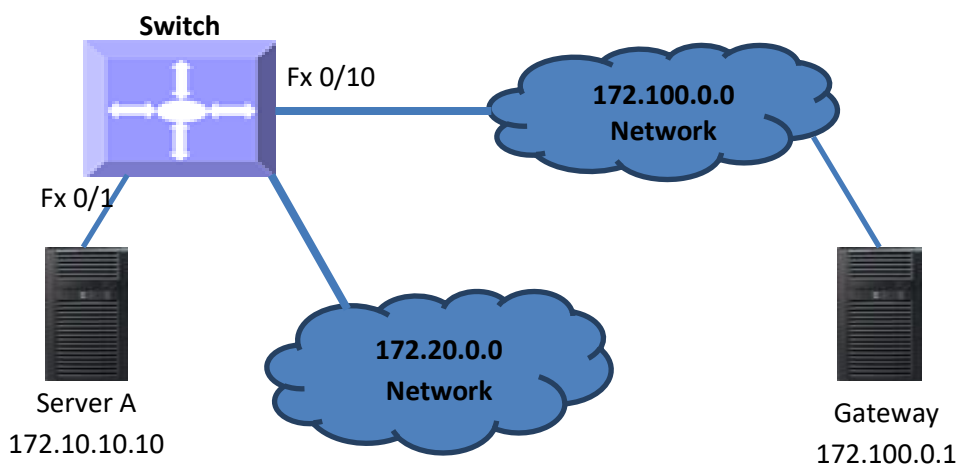
11.3.7 IP Standard ACL Configuration Example 1

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 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> <access-list-name> }	Creates an IP Extended ACL using ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	deny { ip ospf pim <protocol-type (1-255)> } { any host<src-ip-address> <src-ip-address><mask> } { any host<dest-ip-address> <dest-ip-address><mask> } [{ tos<value (0-255)> dscp<value (0-63)> }] [priority<value (1-255)>] or permit { ip ospf pim <protocol-type (1-255)> } { any host<src-ip-address> <src-ip-address><mask> } { any host<dest-ip-address> <dest-ip-address><mask> } [{ tos<value (0-255)> dscp<value (0-63)> }] [priority<value (1-255)>] or	Configures a deny, permit or redirect ACL rule. Use the keyword ip to apply this rule to all IP packets. To apply this rule to only OSPF or PIM packets, use the keywords ospf or pim as needed. The source and destination IP addresses can be 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>redirect<interface-type><interface-id> { ip ospf pim <protocol-type (1-255)> } { any host<src-ip-address> <src-ip-address><mask> } { any host<dest-ip-address> <dest-ip- address><mask> } [{ tos<value (0-255)> dscp<value (0-63)> }] [priority<value (1- 255)>]</pre>	<p>To apply this rule to packets with specific TOS values, use the keyword <code>tos</code> 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.</p> <p>To apply this rule to packets with specified DSCP values, use the keyword <code>dscp</code> and the specific DSCP values to be matched. Users can specify any DSCP values from 0 to 63. The DSCP configuration is optional.</p> <p>The <code>priority</code> 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.</p> <p>Redirect ACL rules need additional <code><interface-type><interface-id></code> parameters to provide the port to which the packets matching this ACL rule should be redirected.</p>
Step 4	<code>show access-lists</code>	Displays the configured ACL rule
Step 5	<code>write startup-config</code>	Optional step – Saves this ACL configuration to be part of startup configuration.

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 TOS 8.

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> <access-list-name> }	Creates an IP Extended ACL using the ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	denytcp {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)> }] [{ack rst }] [{tos<value (0-255)> dscp<value (0-63)>}] [priority<short(1-255)>] or permittcp {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)> }] [{ack rst }] [{tos<value (0-255)> dscp<value (0-63)>}] [priority<short(1-255)>] or	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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>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)> }] [{ ack rst }] [{tos<value (0- 255)> dscp<value (0-63)>}] [priority<short(1-255)>]</pre>	<p>To apply this rule to packets with specific TOS values, use the keyword <code>tos</code> 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.</p> <p>To apply this rule to packets with specified DSCP values, use the keyword <code>dscp</code> and specific DSCP values to be matched. Users can specify any DSCP values from 0 to 63. This DSCP configuration is optional.</p> <p>The <code>priority</code> 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.</p> <p>Redirect ACL rules need additional <code><interface-type><interface-id></code> parameters to define the port to which the packets matching this ACL rule need to be redirected.</p>
Step 4	<code>show access-lists</code>	Displays the configured ACL rule
Step 5	<code>write startup-config</code>	Optional step – Saves this ACL configuration to be part of startup configuration.

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> <access-list-name> }	Creates an IP Extended ACL using the ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	denyudp {any host<src-ip-address> <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any host<dest-ip-address> <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{tos<value (0-255)> dscp<value (0-63)> }] [priority<short(1-255)>] or permitudp {any host<src-ip-address> <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any host<dest-ip-address> <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{tos<value (0-255)> dscp<value (0-63)> }] [priority<short(1-255)>] or	Configures a deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>redirect<interface-type><interface-id>tcp {any host<src-ip-address> <src-ip-address><src- mask> } [{eq<port-number (0-65535)> }] { any host<dest-ip-address> <dest-ip- address><dest-mask> } [{eq<port-number (0- 65535)> }] [{tos<value (0-255)> dscp<value (0-63)>}] [priority<short(1-255)>]</pre>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

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 anyeq 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> <access-list-name> }	Creates an IP Extended ACL using the ip access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	deny 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)>] or permit 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)>] or 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)>]	Configure a deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with keyword host. The keyword any can be used to refer to any IP addresses. To configure a network IP, the address and mask should be provided. To apply this rule to ICMP packets with specific message types or message codes, users should provide matching values for ICMP message types and ICMP message codes. 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. Redirect ACL rules need additional <interface-type> <interface-id> parameters to define the port to

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		which the packets matching this ACL rule need to be redirected.
Step 4	show access-lists	To display the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The examples below show various ways to create IP Extended ACLs for ICMP packets.

Create a deny IP Extended ACL with ACL number 100 to deny all ICMP “traceroute” messages.

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# deny icmp any any 30

Create a deny IP Extended ACL with ACL name acl_cw3 to deny all ICMP traffic on 172.20.0.0 network.

SMIS# configure terminal

SMIS(config)# ip access-list extended acl_cw3

SMIS(config-ext-nacl)# deny icmp any 172.20.0.0 255.255.0.0

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 with ICMP message type “Destination Unreachable” to interface fx 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 500

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

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no ip access-list extended { <access-list-number(1-32768)> <access-list-name> }	Deletes an IP Extended ACL using the ip access-list extended command. access-list-number – the ACL number that needs to be deleted access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove 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

Step	Command	Description
Step 1	show access-lists or show access-lists ext-ip { <access-list-number (1-32768)> <access-list-name> }	Enters the configuration mode access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL that needs to be displayed

SBM-25G-100 / MBM-XEM-100 Configuration Guide

This show command displays the following information for every IP Extended ACL.

Filter Priority	Configured or default priority of the ACL
Protocol Type	IP Protocol Type
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 or permit or redirect
Status	Current status of the ACL. The status should normally be active always. In case of configuration errors, the ACL status may be inactive.

The following fields are displayed for TCP and UDP rules

Source Ports From	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.
Source Ports Till	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.
Destination Ports From	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.
Destination Ports Till	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.

The following fields are displayed only for TCP rules

RST bit	If the ACL is applied only to TCP Reset messages
ACK bit	If the ACL is applied only to TCP acknowledgement messages

The following fields are displayed only for ICMP rules

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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:

```
Filter Priority      : 1
Filter Protocol Type : ANY
Source IP address   : 172.10.10.10
Source IP address mask : 255.255.255.255
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List       : ALL
Out Port           : ALL Filter TOS      : 0 None
Filter DSCP        :
Filter Action       : Deny
Status             : Active
```

IP Extended ACLs with TCP rules display the following fields:

```
SMIS# show access-lists ext-ip 1
```

```
Extended IP Access List 1
```

```
-----
Filter Priority      : 1
Filter Protocol Type : TCP
Source IP address   : 172.20.0.0
Source IP address mask : 255.255.0.0
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List       : ALL
Out Port           : ALL
Filter TOS         :
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.

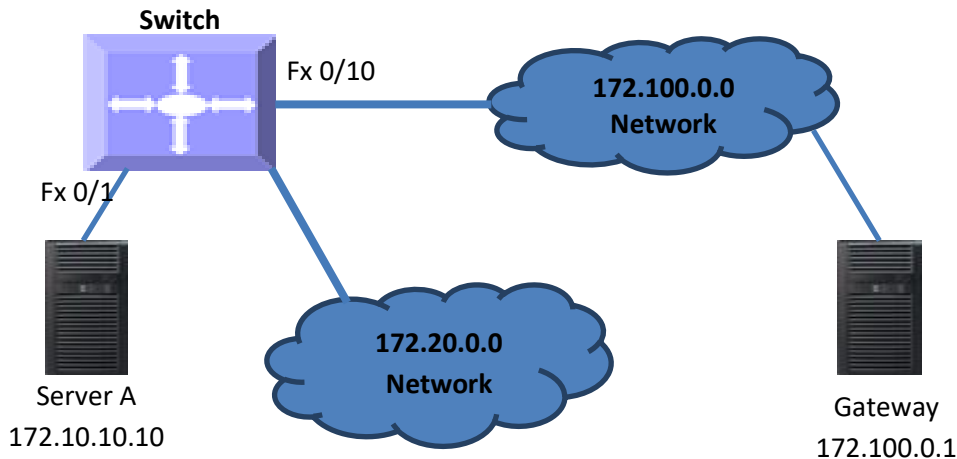
ACL 1 – Allow SMTP TCP traffic from the 172.20.0.0 network and deny all other TCP traffic from this network.

ACL 2 – Redirect all ICMP traffic destined to the IP 172.10.0.0 network to server 172.10.10.10.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

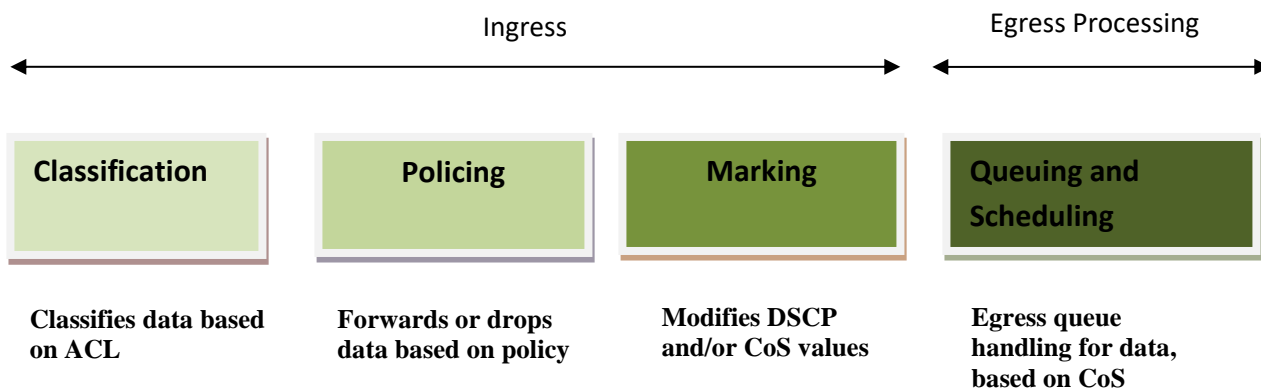


Figure QoS-1: QoS Model

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Parameter	Default Value
QoS Status	Disabled
Class Map	None
Policy Map	None
Default Priority	0
Minimum Bandwidth	0
Maximum Bandwidth	0
Weight	1
Scheduling Algorithm	Strict Queuing
Rate Limit	0
Burst Size	0
HOL	Enabled

The default priority to traffic class queue mapping:

Priority	Traffic Class queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

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.

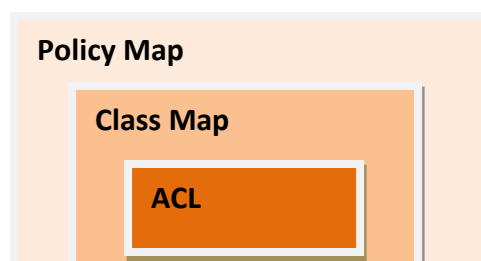


Figure QoS-2: Relationship: ACL, Policy Map & Class Map

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.

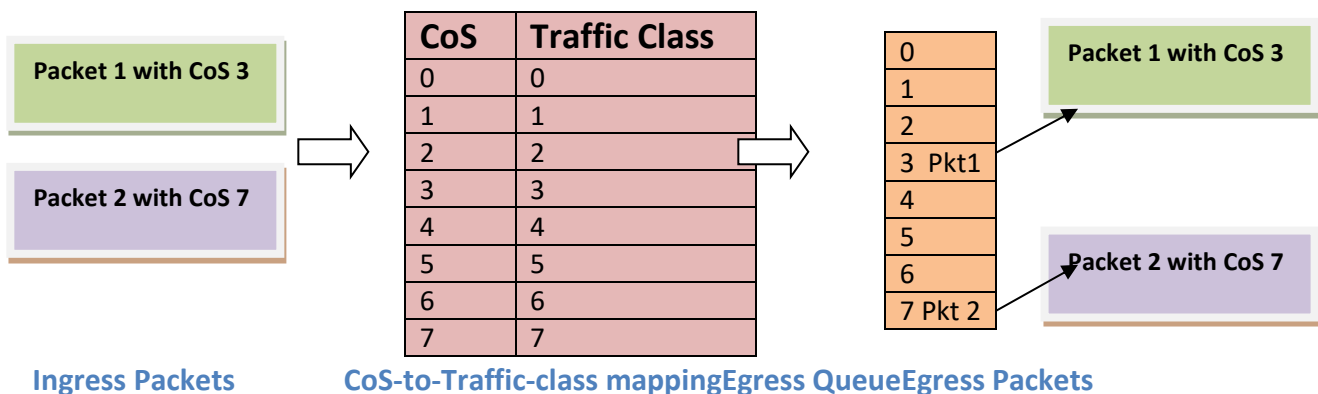


Figure QoS-3: Egress Queuing

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 lookedup. Based on CoS to egress queue mapping, packets with CoS value 7 are queued in Queue-7 and transmitted.

12.2.2 Scheduling

Supernova 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. Supernova switches provide an option to configure the default priority.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set qos enable	Enables QoS on all interfaces
Step 3	End	Exits the configuration mode



The “set qos disable” command disables QoS in the switch.

QoS must be enabled before configuring any of the QoS features.

The example below shows the commands used to enable QoS.

```
SMIS# configure terminal
SMIS(config)# set qos enable
SMIS(config)# end
SMIS(config)# show running-config
```

Building configuration...

ID	Hardware Version	Firmware	OS
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
```

```
vlan 1
ports fx 0/1-24 untagged
ports cx 0/1-3 untagged
exit
```

```
setqos enable
```

12.6 Configuring Policy-Based QoS

Follow the steps below to configure Policy-Based QoS features such as classification, marking and policing.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Create MAC Extended or IP Standard or IP Extended ACL. If required, apply ACL to specific Interface(s).	Refer to the ACL Configuration Guide at www.supermicro.com/products/nfo/networking.cfm .
Step 3	class-map <class-map-number(1-65535)>	Creates a class map and enters the class-map configuration mode. <i>class-map-number</i> - QoS class map number in range from 1-65535.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	<pre>match access-group { mac-access- list ip-access-list } { <acl-index- num (1-65535) > <acl-name> }</pre>	<p>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.</p> <p><i>mac-access-list</i> - Accesses list created based on MAC addresses for non-IP traffic</p> <p><i>ip-access-list</i> - 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.</p> <p><i>acl-index-num</i> - 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.</p> <p><i>ACL-name</i> – Specifies the configured ACL name as a string not exceeding 32 characters</p>
Step 5	Exit	Exits the classmap configuration mode.
Step 6	<pre>policy-map <policy-map- number(1-65535)></pre>	<p>Creates a policy map and enters the policy-map configuration mode.</p> <p><i>policy-map-number</i> - QoS policy map number</p>
Step 7	<pre>class <class-map-number(1- 65535)></pre>	<p>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.</p> <p><i>class-map-number</i> – The class map number to associate the policy, in range of 1-65535</p>
Step 8	<pre>set {cos<new-cos(0-7)> ip dscp<new-dscp(0-63)> ip precedence <new-precedence(0- 7)>}</pre>	<p>(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.</p> <p><i>cos</i> - New COS value assigned to the classified traffic, in range of 0-7</p> <p><i>ip dscp</i> - New DSCP value assigned to the classified traffic, in range of 0-63</p> <p><i>ip precedence</i> - New IP-precedence value assigned to the classified traffic, in range of 0-7</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 9	<code>police <rate-Kbps(64-1048572)> exceed-action {drop policed- dscp-transmit <new-dscp(0-63)>}</code>	(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. rate-kbps- Average traffic rate in kilobitsper second (Kbps), in range 64-1048572 exceed-action - Indicates the action of the switch when the specified rate is exceeded. drop - drops the packet policed-dscp-transmit - changes the differentiated services code point (DSCP) of the packet to that specified in the policed-DSCP map and then sends the packet. The DSCP range is 0-63.
Step 10	End	Exits the configuration mode.
Step 11	<code>show class-map [<class-map- num(1-65535)>] show policy-map [<policy-map- num(1-65535)> [class <class-map- num(1-65535)>]</code>	Displays the classmap configuration. Displays the policy map configuration.



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 policymap

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

DiffServ Configurations:

Class map 10

Filter ID : mac2

Filter Type : MAC-FILTER

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

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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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
```

```
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.

Step	Command	Description
------	---------	-------------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 1	configure terminal	Enters the configuration mode
Step 2	vlan map-priority <priority value(0-7)> traffic-class <Traffic class value(0-7)>	<p>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.</p> <p>Priority- Priority of the packet, in range of 0-7.</p> <p>Class –Traffic class in range of 0-7.</p>
Step 3	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	<p>(Optional) Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx</p> <p>interface-id is in slot/port format for all physical interfaces.</p> <p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 4	switchport priority default <priority value(0-7)>	(Optional) Configures the default priority for the interface in range of 0-7.
Step 5	cosq scheduling algorithm { strict rr wrr deficit }	<p>(Optional) Configures the QoS Egress queue scheduling algorithm.</p> <p>strict - strict rr - round robin wrr - weighted round robin (WRR) deficit – deficit WRR</p>
Step 6	traffic-class <integer(0-7)> weight <integer(0-15)> [minbandwidth<integer(64-16777152)>] [maxbandwidth<integer(64-16777152)>]	<p>(Optional) Configures the egress queue minimum and maximum bandwidth.</p> <p>weight - Configures the queue weights in range of 0-15</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>minbandwidth - Configures the minimum bandwidth for the queue in range of 64-16777152</p> <p>maxbandwidth - Configures the maximum bandwidth for the queue in range of 64-16777152</p>
Step 7	End	Exits the configuration mode.
Step 8	show vlan port config port [<interface-type><interface-id>]	Displays the port default priority configuration.
	show vlan traffic-classes	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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

-----	-----
Fx0/1	StrictPriority
Fx0/2	StrictPriority
Fx0/3	StrictPriority
Fx0/4	StrictPriority
Fx0/5	StrictPriority
Fx0/6	StrictPriority
Fx0/7	StrictPriority
Fx0/8	WeightedRoundRobin
Fx0/9	StrictPriority
Fx0/10	StrictPriority
Fx0/11	StrictPriority
Fx0/12	StrictPriority
Fx0/13	StrictPriority
Fx0/14	StrictPriority
Fx0/15	StrictPriority
Fx0/16	StrictPriority
Fx0/17	StrictPriority
Fx0/18	StrictPriority
Fx0/19	StrictPriority
Fx0/20	StrictPriority
Fx0/21	StrictPriority
Fx0/22	StrictPriority
Fx0/23	StrictPriority
Fx0/24	StrictPriority
Cx0/1	StrictPriority
Cx0/2	StrictPriority
Cx0/3	StrictPriority

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Cx0/3 StrictPriority

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

Interface CoSqlIdCoSqWeightMinBwMaxBw

Fx0/15 0 1 0 0
Fx0/15 1 1 0 0
Fx0/15 2 1 0 0
Fx0/15 3 1 0 0
Fx0/15 4 1 0 0
Fx0/15 5 1 0 0
Fx0/15 6 7 6400 6400000
Fx0/15 7 1 0 0

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Priority	Traffic Class Queue
----------	---------------------

0	0
---	---

1	1
---	---

2	7
---	---

3	3
---	---

4	4
---	---

5	5
---	---

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

Parameter	Default Value
Port mirroring	Disabled
Port mirroring direction	Both

13.2 Configure Port Mirroring in CLI

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Monitor session <session number: 1-4> destination interface <interface-type> <interface-id>	<p>Configure Port Mirroring.</p> <p><i>session_number</i> – 1, indicates only one session is supported.</p> <p><i>Destination</i> – Monitoring Port.</p> <p><i>interface-type</i> –may be any of the following: fx-ethernet – fx cx-ethernet – cx</p> <p><i>interface-id</i> –is in <i>slot/port</i> format for all physical interfaces.</p> <p>NOTE: Source and Destination port cannot be same.</p>
Step 3	Monitor session <session number: 1-4>source interface <interface-type> <interface-id> {rx } tx both}	<p>Configure Port Mirroring.</p> <p><i>session_number</i> – 1, indicates only one session is supported.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p><i>Source</i> – Monitored Port.</p> <p><i>interface-type</i> –may be any of the following: fx-ethernet – fx cx-ethernet – cx</p> <p><i>interface-id</i> –is in <i>slot/port</i> format for all physical interfaces.</p> <p><i>rx</i> – Packets received on source port are monitored (Ingress).</p> <p><i>tx</i> – Packets transmitted on source port are monitored (Egress).</p> <p><i>both</i> – Packets received and transmitted on source port are monitored.</p> <p>NOTE: Source and Destination port cannot be same.</p>
Step 3	End	Exits the configuration mode.
Step 4	show port-monitoring	Displays the port monitoring configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The following command in Switch configuration mode is used to configure a session of mirroring for one unique source port to one destination port. The source port has to be unique, because once the source port is used in one session, it can not be used in another session, unless the port is removed first. Destination port does not have this restriction.

The mirroring action is carried out only when both destination port and source port(s) are in place for the same session. Hence, the execution to carry out a mirroring action generally is composed of these commands.

The first command will establish the mirroring session with the destination port. The interface-id is the port that user wanted to be mirrored to, with format of example like fx 0/1, cx 0/1, cx 0/2 ...

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Once the source port is used in a session, to use it in another session, user needs to remove the source port first. If not, the recently input source port will overwrite the previous source port.



The "**no monitor session [session_number:1-4] destination interface <interface-type> <interface id>**" command delete the destination port mirroring.

The "**no monitor session [session_number:1-4] source interface <interface-type> <interface-id>**" command deletes the source port mirroring.



Note that in the command to remove the source port, there is no provision for the direction field {**rx ,tx, both**}.

The example below shows the commands used to configure Port Mirroring.

```
SMIS# configure terminal
SMIS(config)# monitor session destination interface fx 0/28
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

Port	Ingress-Monitoring	Egress-Monitoring
----	-----	-----
Fx0/1	Disabled	Disabled
Fx0/2	Disabled	Disabled
Fx0/3	Disabled	Disabled
Fx0/4	Disabled	Disabled
Fx0/5	Disabled	Disabled
Fx0/6	Disabled	Disabled
Fx0/7	Disabled	Disabled
Fx0/8	Disabled	Disabled
Fx0/9	Disabled	Disabled
Fx0/10	Disabled	Disabled
Fx0/11	Disabled	Disabled
Fx0/12	Disabled	Disabled
Fx0/13	Disabled	Disabled
Fx0/14	Disabled	Disabled
Fx0/15	Disabled	Disabled
Fx0/16	Disabled	Disabled

Fx0/17	Disabled	Disabled
Fx0/18	Disabled	Disabled
Fx0/19	Disabled	Disabled
Fx0/20	Disabled	Disabled
Fx0/21	Disabled	Disabled
Fx0/22	Enabled	Enabled
Fx0/23	Enabled	Enabled
Fx0/24	Enabled	Enabled
Fx0/25	Enabled	Enabled
Fx0/26	Disabled	Disabled
Fx0/27	Disabled	Disabled
Fx0/28	Disabled	Disabled
Cx0/1	Disabled	Disabled
Cx0/2	Disabled	Disabled
Cx0/3	Disabled	Disabled
Cx0/4	Disabled	Disabled

14 SNMP

SNMP helps to monitor and manage the switches from network management systems (NMS). SNMP solutions contain three major components – SNMP manager, SNMP agent and MIB (Management Information Base) as shown in Figure – SNMP-1.

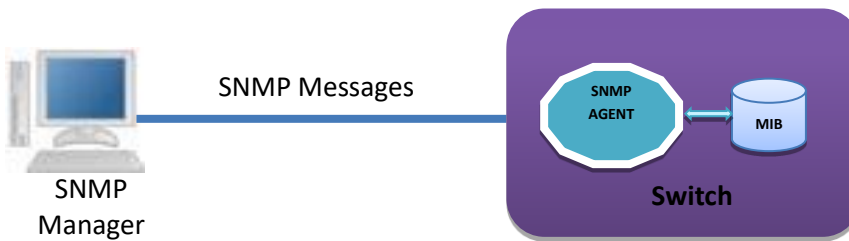
The SNMP MIB contains all the configuration and status information of the switch. MIB is organized in a tree structure with branches and leaf nodes. Each node contains an object of information and is identified with an object identifier (OID). SNMP MIB is stored and maintained in the switch.

The SNMP agent also resides on the switch. It processes the SNMP requests received from the SNMP manager. It sends responses to SNMP managers by retrieving required information from the MIB. It also updates the MIB based on SNMP messages sent by the SNMP managers. SNMP agents also send voluntary traps to SNMP managers. Traps are sent to alert the SNMP managers on events happening on the switch.

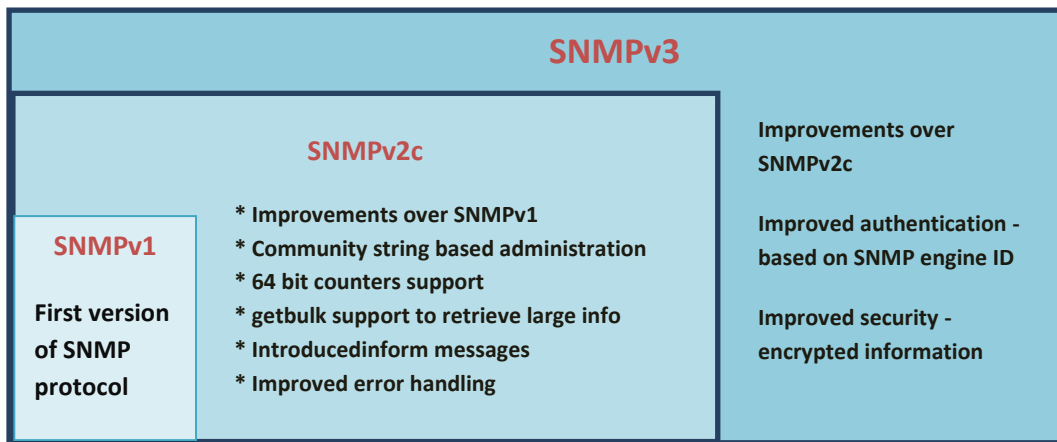
The SNMP manager is an NMS application. It monitors and manages switches by communicating to the SNMP agents running on the switch. The SNMP manager application provides command or graphical interfaces to the network administrators to help them manage the networks.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Figure SNMP-1: SNMP Systems



There are three versions of SNMP protocols available.



USM (User based Security Model) and VACM (View based Access Control Model) are the main features in SNMPv3. USM provides user authentication and message encryption. VACM provides MIB access control by associating views and users.

SNMPv3 uses a combination of *security model* and *security level* to define switch access. *Security model* specifies the authentication mechanism for the user and the group to which the user belongs. The security models in the Supermicro switch are v1, v2c and v3.

Security level specifies the permitted security within the particular security model. The security levels in Supermicro switches are

- NoAuthNoPriv
- AuthNoPriv
- AuthPriv

The security model and level combinations possible in Supermicro switch are listed in the table below.

Security Model	Security Level	Authentication	Encryption	Purpose
V1	noAuthNoPriv	Community string	None	Community string and community user are used to authenticate user login.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

V2c	noAuthNoPriv	Community string	None	Community string and community user are used to authenticate user login.
V3	noAuthNoPriv	User name	None	User configuration is used to authenticate user login.
V3	Auth	MD5 or SHA	None	MD5 or SHA algorithm is used to verify user login.
V3	Priv	None	DES	DES is used to encrypt all SNMP messages.

SNMP uses multiple messages between managers and agents. The below table describes the SNMP messages.

Message Type	Originator	Receiver	Purpose
get-request	Manager	Agent	To get the value of a particular MIB object
get-next-request	Manager	Agent	To get the value of the next object in a table
get-bulk-request	Manager	Agent	To get the values of multiple MIB objects in one transaction
get-response	Agent	Master	Response for get-request, get-next-request and get-bulk-request messages.
set-request	Manager	Agent	To set the value of a particular MIB object
Trap	Agent	Master	To notify the events occurring on agents
Inform	Agent	Master	To guarantee delivery of traps to Manager

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.

Interface Type	ifIndex
Fx-ethernet physical interfaces	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.
Cx-ethernet physical interfaces	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.

Port channel interfaces	Starts after 100Gig ifIndexes and goes up to the maximum number of port channel interfaces supported on the switch. 33 to 97 for SBM-25G-100 and 61 to 125 for MBM-XEM-100.
Management IP interfaces	98 for SBM-25G-100 and 126 for MBM-XEM-100.

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.

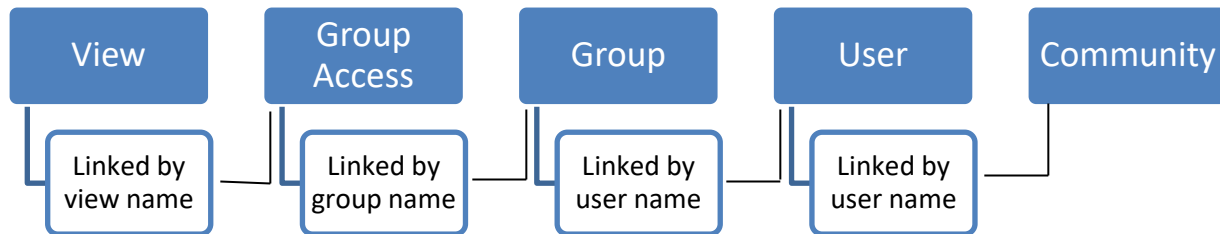


Figure SNMP-2: SNMP - Relationships

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

Function	Default Value
SNMP Agent Status	Enabled
SNMP Sub-Agent Status	Disabled
Version	3
Engine Id	80.00.08.1c.04.46.53
Communities	PUBLIC,

	NETMAN
Users	initial, TemplateMD5, TemplateSHA
Authentication (for default users)	initial : none TemplateMD5: MD5 TemplateSHA: SHA
Privacy (for default users)	initial : none TemplateMD5: none TemplateSHA: DES
Groups	iso, initial
Access	iso, initial
View (for default groups)	iso: iso, initial: restricted
Notify View Name	iss, iss1
Read, Write, Notify	Iso
Target Parameters	Internet, test1
Storage Type	Volatile
Context	None
SNMP Port	161
SNMP Trap Port	162
Trap Status	Enabled
Authentication Trap	Disabled
Link-State Trap	Enabled
Switch Name	SMIS
System Contact	http://www.supermicro.com
System Location	Supermicro

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	disable snmpagent	Disables the SNMP agent
Step 3	end	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.
--------	-----------------------------	--



The “**enablesnmpagent**” command enables the SNMP agent.

To enable the SNMP agent, it must be in the disabled state. The SNMP subagent is disabled by default. If needed, use the command “**disablesnmpsubagent**” to disable the SNMP subagent feature.

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

Disable the SNMP agent.

```
SMIS# configure terminal
SMIS(config)# disable snmpagent
SMIS(config)# end
```

Enable the SNMP agent.

```
SMIS# configure terminal
SMIS(config)# enable snmpagent
SMIS(config)# end
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	device name <devname(15)>	Configures switch name and prompt. Devname – Switch name specified with 1-15 alphanumeric characters.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the system information configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	system contact <string - to use more than one word, provide the string within double quotes>	Configures the switch contact. String – Contact information entered as a String of maximum length 256.
Step 3	End	Exits the configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 4	show system information	Displays the system information configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.



The Switch contact configuration is automatically stored as part of the startup configuration file.

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

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

```
SMIS# show system information
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: User1 at CA
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 50 mins 51 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
=====
Key # Key
=====
Time zone offset not set
```

14.5.3 System Location

Supermicro switches provide an option to configure the switch location details.

Follow the steps below to configure system location.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	system location <location name>	Configures the system location. location name – Location of the switch specified as a string with a maximum size of 256.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the system information configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.



The 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmpengineid<EngineIdentifier>	Configures the SNMP Engine Identifier. <i>EngineIdentifier</i> -Hexadecimal number, with length between 5 and 32 octets. Each octet should be separated by a period.
Step 3	end	Exits the configuration mode.
Step 4	show snmpengineid	Displays the SNMP engine Identifier information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <name>] [{volatile nonvolatile}] [transporttag<TransportTagIdentifier none>]	<p>Configures the SNMP community.</p> <p><i>CommunityIndex</i>—Alphanumeric value with a maximum of 32 characters.</p> <p><i>CommunityName</i>—Alphanumeric value with a maximum of 255 characters.</p> <p><i>SecurityName</i> – This is the user name associated with the community. Alphanumeric value with a maximum of 40 characters.</p> <p><i>Name</i> –Alphanumeric value with a maximum of 40 characters.</p> <p><i>TransportTagIdentifier</i> –Identifies the transport end points between agent and manager. Alphanumeric value with a maximum of 255 characters.</p>
Step 3	end	Exits the configuration mode.
Step 4	show snmp community	Displays the SNMP community information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



The “**no snmp community index <CommunityIndex>**” command deletes the specified community index.

SNMP *User Name* is also referred to as *SNMP Security Name* in Supermicro switches.

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

```
SMIS(config)# snmp community index test1 name test1 security user1 nonvolatile
```

```
SMIS(config)# show snmp community
```

```
Community Index: NETMAN
Community Name: NETMAN
Security Name: none
Context Name:
Transport Tag:
Storage Type: Volatile
Row Status: Active
```

```
-----
Community Index: PUBLIC
Community Name : PUBLIC
Security Name: none
Context Name :
Transport Tag:
Storage Type: Volatile
Row Status: Active
```

```
-----
Community Index: test1
Community Name: test1
Security Name: user1
Context Name:
Transport Tag:
Storage Type: Non-volatile
Row Status: Active
-----
```

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	snmp user <UserName> [auth {md5 sha} <passwd>[priv DES <passwd>]] [{volatile nonvolatile}]	<p>Configures the SNMP user, authentication and encryption.</p> <p><i>UserName</i> - Alphanumeric value with a maximum of 40 characters.</p> <p>Use auth to enable authentication for the user.</p> <p><i>Passwd</i>—Password used for user Authentication. Alphanumeric value with a maximum of 40 characters.</p> <p>Use priv to enable encryption of packets.</p> <p><i>Passwd</i>—Password used to generate keys for encryption of messages. Alphanumeric value with a maximum of 40 characters.</p> <p>Use volatile if the value need not be stored in NVRAM.</p> <p>Use nonvolatile if the value must be stored in NVRAM and available after restart.</p>
Step 3	end	Exits the configuration mode.
Step 4	show snmp user	Displays the SNMP user information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



The “no snmp user <UserName> ”command deletes the specified user.

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

```
SMIS# configure terminal
SMIS(config)# snmp user user5 auth md5 abc123 priv DES xyz123
SMIS# end
```

```
SMIS# show snmp user
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp group <GroupName> user <UserName> security-model {v1 v2c v3 } [{volatile nonvolatile}]	Configures the SNMP group. <i>GroupName</i> – Alphanumeric value with a maximum of 40 characters. <i>Security-model</i> – Use v1 or v2c or v3. <i>UserName</i> - Alphanumeric value with a maximum of 40 characters.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		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	Displays the SNMP group information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



The “**no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3}**” command deletes the specified group.

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

```
SMIS# configure terminal
SMIS(config)# snmp group group5 user user5 security-model v3
SMIS# end
```

```
SMIS# show snmp group
```

```
Security Model: v1
Security Name: none
Group Name: iso
Storage Type: Volatile
Row Status: Active
-----
```

```
Security Model: v2c
Security Name: none
Group Name: iso
Storage Type: Volatile
Row Status: Active
-----
```

```
Security Model: v3
Security Name: user5
Group Name: group5
Storage Type: Volatile
Row Status: Active
-----
```

```
Security Model: v3
Security Name: initial
```


SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmpview <ViewName><OIDTree> [mask <OIDMask>] {included excluded} [{volatile nonvolatile}]	<p>Configures the SNMP view.</p> <p><i>ViewName</i>- Alphanumeric value with a maximum of 40 characters.</p> <p><i>OIDTree</i>-OID number, with a maximum of 32 numbers.</p> <p><i>OIDMask</i>- OID number, with a maximum of 32 numbers.</p> <p>Use included to specify that the MIB sub-tree is included in the view.</p> <p>Use excluded to specify that the MIB sub-tree is excluded from the view.</p> <p>Use volatile if the value need not be stored in NVRAM.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		Use nonvolatile if the value must be stored in NVRAM and available after restart.
Step 3	end	Exits the configuration mode.
Step 4	show snmpviewtree	Displays the SNMP view information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to configure SNMP group access.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp access <GroupName> {v1 v2c v3 {auth noauth priv}}[read <ReadView none>] [write <WriteView none>] [notify <NotifyView none>] [{volatile nonvolatile}]	<p>Configures the SNMP group access.</p> <p><i>GroupName</i> - Alphanumeric value with a maximum of 40 characters.</p> <p>Security model – Mention one of v1, v2c or v3.</p> <p>Use auth to enable authentication for the user.</p> <p>Use priv to enable encryption of packets.</p> <p><i>ReadView</i> - View name that specifies read access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters.</p> <p><i>WriteView</i> - View name that specifies write access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters.</p> <p><i>NotifyView</i> - View name that specifies a particular MIB sub-tree used in notification. Alphanumeric value with a maximum of 40 characters.</p> <p>Use volatile if the value need not be stored in NVRAM.</p> <p>Use nonvolatile if the value must be stored in NVRAM and available after restart.</p>
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: Rrestricted

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmptargetaddr<TargetAddressName>param<ParamName> {<IPAddress> <IP6Address>} [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)] [taglist<TagIdentifier none>] [{volatile nonvolatile}]	Configures the SNMP target address information. <i>TargetAddressName</i> - Alphanumeric value with a maximum of 40 characters. <i>ParamName</i> – The parameter to be notified to the specific target. Alphanumeric value with a maximum of 40 characters. <i>IPAddress</i> – IPv4 address of the target. <i>IP6Address</i> – IPv6 address of the target. <i>Seconds</i> – Specifies the timeout within which the target should be reachable.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p><i>RetryCount</i> – Specifies the number of retries to reach the target.</p> <p><i>TagIdentifier</i>- A set of targets can be grouped under a tag Identifier.</p> <p>Use volatile if the value need not be stored in NVRAM.</p> <p>Use nonvolatile if the value must be stored in NVRAM and available after restart.</p>
Step 3	end	Exits the configuration mode.
Step 4	show snmptargetaddr	Displays the SNMP target address information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp target params <ParamName> user <UserName> security-model {v1 v2c v3 {auth noauth priv}} message-processing {v1 v2c v3} [{volatile nonvolatile}]	<p>Configures the SNMP target parameters.</p> <p><i>ParamName</i> The parameter to be notified. Alphanumeric value with a maximum of 40 characters.</p> <p><i>UserName</i> - Alphanumeric value with a maximum of 40 characters.</p> <p>Security model – Use one of v1, v2c, v3.</p> <p>Use auth to enable authentication for the user.</p> <p>Use priv to enable encryption of packets.</p> <p>Message processing- Specifies the SNMP version for sending/receiving the parameter via a notification message.</p> <p>Use volatile if the value need not be stored in NVRAM.</p> <p>Use nonvolatile if the value must be stored in NVRAM and available after restart.</p>
Step 3	end	Exits the configuration mode.
Step 4	show snmp target param	Displays the SNMP target parameters information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



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)# snmptargetparamsparam4 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 Authentitcation, 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 Authentitcation, 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 Authentitcation, 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	snmp notify <NotifyName> tag <TagName> type {Trap Inform} [{volatile nonvolatile}]	Configures the SNMP Notify information. <i>NotifyName</i> - Alphanumeric value with a maximum of 40 characters. <i>TagName</i> –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 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 notify show snmp inform statistics	Displays the SNMP notification information and Inform statistics.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



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

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

```
SMIS# configure terminal
SMIS(config)# snmp notify PUBLIC tag tag1 type trap nonvolatile
SMIS(config)# end
```

```
SMIS# show snmpnotif
```

```
Notify Name: PUBLIC
Notify Tag: tag1
Notify Type: trap
Storage Type: Non-volatile
```

Row Status: Active

Notify Name: iss
Notify Tag: iss
Notify Type: trap
Storage Type: Volatile
Row Status: Active

Notify Name: iss1
Notify Tag: iss1
Notify Type: trap
Storage Type: Volatile
Row Status: Active

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp-server trap udp-port <port>	Configures the SNMP UDP port for traps. <i>Port</i> —UDP port for traps in the range 1 – 65535.
Step 3	end	Exits the configuration mode.
Step 4	show snmp-server traps	Displays the SNMP traps information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	snmp-server enable traps snmp authentication	Enables the SNMP authentication traps.
Step 3	end	Exits the configuration mode.
Step 4	show snmp	Displays the SNMP information.
Step 5	write startup-config	Optional step – saves this SNMP configuration to be part of the startup configuration.



The “**no snmp-server enable traps snmp authentication**” command disables SNMP authentication traps.

The example below shows the commands used to enable the SNMP authentication traps.

SMIS# configure terminal

SMIS(config)# **snmp-server enable traps snmp authentication**

SMIS# end

SMIS(config)# **show snmp-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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Error Packets : 0
Unknown Protocol : 0

Transmission Counters

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

14.8 SNMPConfigurationExample

PC – SNMP Manager

Switch - SNMP Agent



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*- full read/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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

View Name : restricted

Subtree OID : 1.3.6.1

Subtree Mask : 1.1.1.1

View Type : Included

Storage Type : Volatile

Row Status : Active

View Name : restricted

Subtree OID : 1.3.6.3.10.2.1

Subtree Mask : 1.1.1.1.1.1.1

View Type : Excluded

Storage Type : Volatile

Row Status : Active

SMIS# **show running-config**

Building configuration...

ID	Hardware Version	Firmware	OS
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

vlan 1

ports fx 0/1-24 untagged

ports cx 0/1-3 untagged

exit

```
snmp user user1 auth md5 AUTH_PASSWD volatile
snmp user user2 auth sha AUTH_PASSWD priv DES DES_CBC volatile
snmp group superuser user user1 security-model v3 volatile
snmp group generalusers user user2 security-model v3 volatile
snmp access superuser v3 auth read full write full notify full volatile
snmp access generalusers v3 noauth read full notify full volatile
snmp view full 1.3.6.1 included volatile
snmp view restricted 1.3.6.1 included volatile
snmp view restricted 1.3.6.3.10.2.1 excluded volatile
```

15 RMON

Remote monitoring (RMON) is a method similar to Simple Network Management Protocol (SNMP) and uses a client-server model to monitor/manageremote 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 basedon 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. Italso handleevents 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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

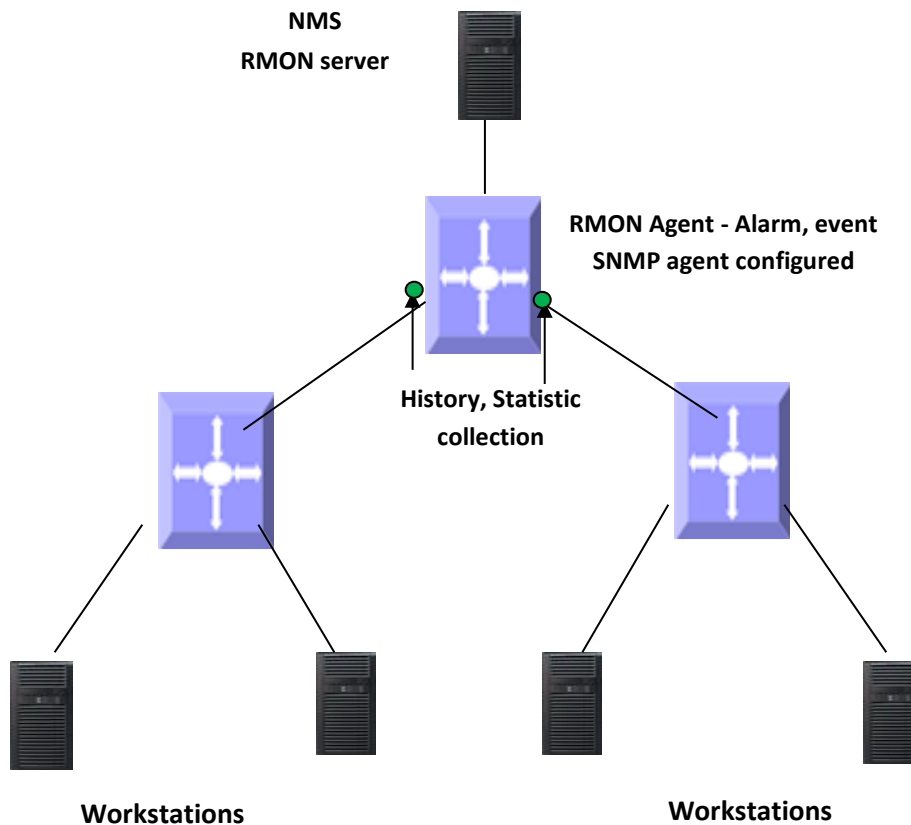


Figure RMON-1: RMON Operation

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, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received etc.

15.2 RMON Configuration

This section describes RMON configuration for Supermicro switches.

Parameter	Default Value
RMON status	Disabled
Collection statistics	None
Collection history	None
Alarms	None
Events	None

15.2.1 Enabling RMON

RMON is disabled by default in Supermicro switches. Follow the below steps to enable RMON.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set rmon enable	Enable RMON in the switch.
Step 3	End	Exit from Configuration mode.
Step 4	Show rmon	Display RMON status.



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	rmon alarm <alarm-number><mib-object-id (255)><sample-interval-time (1-65535)>{absolute delta } rising-threshold <value (0-2147483647)><rising-event-number (1-65535)> falling-threshold <value (0-2147483647)><falling-event-number (1-65535)> [owner <ownername (127)>]	<p>(Optional) Set an alarm on a MIB object.</p> <p>alarm-number - Alarm Number. This value ranges between 1 and 65535.</p> <p>mib-object-id - The mib object identifier.</p> <p>sample-interval-time - Time in seconds during which the alarm monitors the MIB variable. This value ranges between 1 and 65535 seconds.</p> <p>absolute - Used to test each mib variable directly.</p> <p>delta - Used to test the change between samples of a variable.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>rising-threshold - A number at which the alarm is triggered. This value ranges between 0 and 2147483647.</p> <p>falling-thresholdvalue - A number at which the alarm is reset. This value ranges between 0 and 2147483647.</p> <p>NOTE: Falling threshold must be less than rising threshold.</p> <p>rising-event-number - The event number to trigger when the rising threshold exceeds its limit. This value ranges between 1 and 65535.</p> <p>falling-event-number - The event number to trigger when the falling threshold exceeds its limit. This value ranges between 1 and 65535.</p> <p>Owner – Owner of the alarm, string of length 127.</p>
Step 3	<p>rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]</p>	<p>(Optional) Add an event in the RMON event table that is associated with an RMON event number.</p> <p>Number - Event number</p> <p>Description - Description of the event</p> <p>Log - Used to generate a log entry</p> <p>Owner - Owner of the event, , in range 1- 127 characters</p> <p>Trap - Used to generate a trap. The SNMP community string is to be passed for the specifiedtrap.</p> <p>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).</p>
Step 4	end	Exit from Configuration mode.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 5	show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)]] [overview]]	Display RMON statistics, alarms, events history and overview.
--------	---	---



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	(Optional) Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 3	rmon collection stats <index (1-65535)> [owner <ownername (127)>]	(Optional) Enable RMON statistic collection on the interface index - Statistics table index, in range 1-65535 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
Step 4	rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]	(Optional) Enable history collection for the specified number of buckets and time period index - History table index, in range 1-65535 buckets - The maximum number of buckets desired for the RMON collection history group of statistics. interval - The number of seconds in each polling cycle, in range 1-3600 owner - Optional field - allows the user to enter the name of the owner of the RMON group of statistics, string of length 127.
Step 5	show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)]] [overview]]	Display RMON statistics, history and overview.



The “no rmon collection stats <index (1-65535)>” and “no rmon collection history <index (1-65535)>” commands delete the RMON collection configuration.

15.2.4 RMON Configuration Example

A sample RMON configuration of alarms, events and collection statistics and History in a Supermicro switch is specified below.

- 1) Enable RMON
- 2) Create events for Rising and falling threshold.
- 3) Create the alarm for the MIB object in 1 1.3.6.1.6.3.16.1.2.1.4table.
- 4) Create statistics collection on an interface.
- 5) Display all RMON configurations.

SMIS# configure terminal

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
SMIS(config)# set rmon enable
```

```
SMIS(config)# rmon event 1 description rise log owner smicro1 trap PUBLIC
```

```
SMIS(config)# rmon event 2description 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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Description is fall

Event firing causes log and trap to community NETMAN,

Time last sent is Apr 29 10:11:01 2013

SMIS# show rmon history

RMON is enabled

Entry 1 is active, and owned by

Monitors ifEntry.1.5 every 20 second(s)

Requested # of time intervals, ie buckets, is 2,

Granted # of time intervals, ie buckets, is 2,

Sample 2 began measuring at Apr 29 10:13:52 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

of dropped packet events is 0

Network utilization is estimated at 0

Sample 3 began measuring at Apr 29 10:14:12 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

of dropped packet events is 0

Network utilization is estimated at 0

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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,

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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...

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

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 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 2 absolute rising-thresh

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	(Optional) Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range ...” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	rate-limit output <rate-value-kbps (1-10000000)><burst-value-kbits (1-10000000)>	Enables the egress rate limit for the interface(s), set to the closest rate (kbps) and burst size (kbits) as the hardware capabilities. Rate limiting is applied to packets sent out on a particular interface. Rate limit and burst size in range of 1-10000000.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no hol blocking prevention	Disables HOL blocking
Step 3	End	Exits the configuration mode.
Step 4	show interfaces [{ [<interface-type><interface-id>]	Displays the interface configuration.



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)
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Bridge Port Type: Customer Bridge Port
Hardware Address is 00:30:48:e3:04:78

MTU 1500 bytes, Full duplex, 25 Gbps, Auto-Negotiation
HOL Block Prevention disabled.
Input flow-control is off, output flow-control is off

Link Up/Down Trap is enabled

Reception Counters

Octets	: 0
Unicast Packets	: 0
Broadcast Packets	: 0
Multicast Packets	: 0
Pause Frames	: 0
Undersize Frames	: 0
Oversize Frames	: 0
CRC Error Frames	: 0
Discarded Packets	: 0
Error Packets	: 0
Unknown Protocol	: 0

Transmission Counters

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

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	login authentication { local radius tacacs }	Configure the login authentication mechanism to be used for switch access. Local – Use the local database in switch to authenticate users. Radius – Use RADIUS server to authenticate users. Tacacs – Use TACACS server to authenticate users.
Step 3	End	Exits the configuration mode.
Step 4	show system information	Displays the Login Authentication mechanism.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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
```

```
Server  Key  Prefer
=====
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

Parameter	Default Value
Server	None
Timeout	3 seconds
Re-transmit	3

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Key	None
-----	------

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 RADIUSserver Parameters.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	radius-server host <ip-address> [timeout <1-120>] [retransmit <1-254>] key <secret-key-string> [type {authenticating accounting both}]	Configure RADIUS server for purpose of authenticating or accounting or both. <i>ip-address</i> – serverIP address. <i>timeout</i> – Specify RADIUS server timeout in range 1-120 <i>retransmit</i> – Specify number of retries to attempt to connect to RADIUS server in range 1-254 <i>key</i> –Specify authentication key
Step 3	End	Exits the configuration mode.
Step 4	show radius server show radius statistics	Displays the RADIUS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



The “no radius-server host <ip-address>” command deletes the RADIUS client.

The example below shows the commands used to configure RADIUS server.

```
SMIS# configure terminal
```

```
SMIS(config)#radius-server host 200.200.200.1 timeout 50 retransmit 250 key key1
```

```
SMIS(config)# end
```

```
SMIS# show radius server
```

```
Radius Server Host Information
```

```
-----
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Parameter	Default Value
TACACS server	None
TACACS server re-tries	2
TACACS TCP port	49
TACACS Authentication Mode	PAP
TACACS Authorization status	Diabled
Privilege	1

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tacacs-server host <ip-address> [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds>] key <secret key>	Configure TACACS server. <i>ip-address</i> – TACACS Server IP-address <i>single-connection</i> – When this option is specified, only one connection to one of the configured TACACS servers is permitted. <i>port</i> – Specify TCP port in range 1-65535 <i>timeout</i> - Specify TACACS server timeout in range 0 – 255 seconds <i>key</i> – 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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tacacs use-server address<ip-address>	Configure TACACS server to be used.
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 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
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Follow the steps below to configure the TACACS login authentication mode to be used.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	aaa authentication tacacs { chap pap }	Configures TACACS authentication mode to be used.
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 the startup configuration.



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 rcvd.       : 11
Authen. Fails rcvd.      : 3
Authen. Get User rcvd.   : 0
Authen. Get Pass rcvd.   : 0
Authen. Sess. timeouts   : 0
```

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	aaa authorization group Tacacs	Configures TACACS authorization to be used.
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 the startup configuration.



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.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	aaa accounting group Tacacs	Enables the TACACS accounting feature
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 the startup configuration.



The “no aaa accounting group tacacs” command disables the TACACS accounting feature.

16.3.7 TACACS Privilege

Req. #	Description	Comments
1.0	<p>The privilege configured in TACACS+ server should be used while logging in to Supermicro switch using TACACS+ authentication.</p> <p>There are many types of service used by different vendors on the market. For Supermicro switches the supported service type is ‘config’.</p> <p>E.g. user configuration in TACACS+ server:</p> <pre>user = test15 { name = "Test15 User" pap = cleartext "test15" service=config { priv-lvl = 15 } }</pre>	<p>This is an umbrella requirement to cover the functionality.</p>
1.1	<p>TACACS+ users without privilege configured also should be able to login to switch with the default privilege level 1.</p> <p>E.g. user configuration in TACACS+ server:</p> <pre>user = test1 { name = "Test1 User" pap = cleartext "test1" }</pre>	
1.2	<p>This privilege function should be enabled only when user enables it in CLI, Web, and SNMP.</p>	<p>For e.g. the new command “aaa authorization</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	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.

Parameter	Default Value
SSH status	Enabled
SSH version compatibility	Off
SSH port	22
SSH Key	RSA
Cipher Algorithm	3DES-CBC, AES128-CBC, AES256-CBC, ARCFOUR128, ARCFOUR256, CAST128-CBC, AES192-CBC, ARCFOUR, RIJNDAEL-CBC, AES128-CTR, AES192-CTR, AES256-CTR
SSH Version	2
Authentication	HMAC-SHA1

Follow the steps below to configure SSH.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip ssh cipher {3des-cbc cast128-cbc arcfour arcfour128 arcfour256 aes128-cbc aes192-cbc aes256-cbc rijndael-cbc aes128-ctr aes192-ctr aes256-ctr} ip ssh {version compatibility auth ([hmac-md5] [hmac-sha1]) port <(1024-65535)>}	<i>versioncompatibility</i> - Specify whether switch should process both version 1 and version 2 SSL messages. <i>cipher</i> – Specify the encryption algorithm.

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<i>auth</i> –Specify the authentication algorithm. <i>port</i> - Specify SSH port in range 1024-65535
Step 3	End	Exits the configuration mode.
Step 4	show ip ssh	Displays the SSH configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.



Use the “no ip ssh cipher {3des-cbc|cast128-cbc|arcfour|arcfour128|arcfour256|aes128-cbc| aes192-cbc|aes256-cbc|rijndael-cbc|aes128-ctr|aes192-ctr|aes256-ctr}” command to disable a cipher.

Use the “no ip ssh {version compatibility | auth ([hmac-md5] [hmac-sha1]) | port}” command to remove the version compatibility, auth and port configuration.

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 : 2

Cipher Algorithm : 3DES-CBC, AES128-CBC, AES256-CBC, ARCFOUR128

ARCFOUR256, CAST128-CBC, AES192-CBC, ARCFOUR

RIJNDAEL-CBC, AES128-CTR, AES192-CTR, AES256-CTR

Authentication : HMAC-SHA1

Trace Level : None

Port : 22

```
SMIS(config)# no ip ssh cipher 3des-cbc
```

```
SMIS(config)# end
```

```
SMIS# show ip ssh
```

Version : 2

Cipher Algorithm : AES128-CBC, AES256-CBC, ARCFOUR128, ARCFOUR256

CAST128-CBC, AES192-CBC, ARCFOUR, RIJNDAEL-CBC

AES128-CTR, AES192-CTR, AES256-CTR,

Authentication : HMAC-SHA1

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Trace Level : None

Port : 22

SMIS# configure terminal

SMIS(config)# ip ssh auth hmac-md5

SMIS(config)# end

SMIS# show ip ssh

Version : 2

Cipher Algorithm : AES128-CBC, AES256-CBC, ARCFOUR128, ARCFOUR256

CAST128-CBC, AES192-CBC, ARCFOUR, RIJNDAEL-CBC

AES128-CTR, AES192-CTR, AES256-CTR,

Authentication : HMAC-MD5

Trace Level : None

Port : 22

16.5 SSL / Secure HTTP (HTTPS)

SSL provides server authentication, encryption, and message integrity, as well as HTTP client authentication, to allow secure HTTP communications.

Parameter	Default Value
HTTP Secure server status	Enabled
HTTPS port	443

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 functions such as configuring a switch from a Web browser.

Follow the steps below to configure Secure HTTP.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set ip https {enable disable}	Configure Secure HTTP. <i>enable</i> – Enables HTTPS server <i>disable</i> – Disables HTTPS server
Step 3	ip https port <port-number(1-65535)>	Configures HTTPS port.
Step 4	End	Exits the configuration mode.
Step 5	show https server status	Displays HTTPS server status.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

SBM-25G-100 / MBM-XEM-100 Configuration Guide



The “no ip https port” command resets the HTTPS port to default value 443.

The example below shows the commands used to configure Secure HTTP.

```
SMIS# configure terminal
SMIS(config)# ip https port 4430
SMIS(config)# end
SMIS# show https server status
```

```
HTTPS server status      : Enabled
HTTPS port is            : 4430
```

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.

Parameter	Default Value
-----------	---------------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 EnablingLLDP

LLDP is disabled by default in Supermicro switches. Follow the steps below to enable LLDP.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	set lldpenable	Enables LLDP in the switch.
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global configuration details



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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 2	<p>interface <interface-type><interface-id> or interface range <interface-type><interface-id></p>	<p>(Optional) Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</p> <p>interface-id is in slot/port format for all physical interfaces.</p> <p>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</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 3	lldp {transmit receive}	<p>(Optional) Sets LLDP admin status on an interface to Transmit or Receive</p>
Step 4	lldp notification [remote-table-chg][mis-configuration]	<p>(Optional) Enables LLDP trap notification on an interface.</p> <p>remote-table-chg - Trap notification for change in neighbor’s table.</p> <p>mis-configuration - Trap notification for mis-configuration.</p>
Step 5	lldp port-id-subtype { if-alias port-comp <string(255)> mac-addr if-name local <string(255)> }	<p>(Optional) Configures LLDPport IDsubtype and port IDvalue</p> <p>if-alias - interface alias</p> <p>port-comp - port component</p> <p>mac-addr - MAC address</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>if-name - interface name</p> <p>local - locally assigned</p> <p>The default value for port-id-subtype is if-name.</p> <p>Note: The if-alias option can be used only for the interfaces which have valid description configured.</p>
Step 6	Exit	Exits interface configuration mode.
Step 7	<pre>lldp chassis-id-subtype { chassis-comp <string(255)> if-alias port-comp <string(255)> mac-addr nw-addr if-name local <string(255)> }</pre>	<p>(Optional)</p> <p>Configures LLDP chassis ID subtype and chassis ID value.</p> <p>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.</p> <p>chassis-comp - chassis component</p> <p>if-alias - management interface alias</p> <p>port-comp - port component</p> <p>mac-addr - MAC address</p> <p>nw-addr - network address</p> <p>if-name - interface name</p> <p>local - locally assigned</p> <p>The default value for chassis-id-subtype is mac-addr.</p> <p>Note: To use the if-alias option, the management interface must have been configured with valid description.</p>
Step 8	End	Exits the configuration mode.
Step 9	show lldp interface [<interface-type><interface-id>]	Displays LLDP configuration details on a particular interface or all interfaces

SBM-25G-100 / MBM-XEM-100 Configuration Guide

	<pre>show lldp neighbors [chassis-id <string(255)> port-id <string(255)> [<interface-type><interface-id>][detail]</pre> <pre>show lldp traffic [<iftype><ifnum>]</pre> <pre>show lldp errors</pre> <pre>show lldp statistics</pre>	<p>Displays information about neighbors learned on an interface or all interfaces</p> <p>Displays LLDP counters, including the number of frames sent, received, discarded, etc.</p> <p>Displays information about errors such as memory allocation failures, queue overflows, table overflows, etc.</p> <p>Displays the LLDP remote table statistics information</p>
Step 10	<pre>clear lldp counters</pre>	Clears LLDP transmit and receive statistics
Step 11	<pre>clear lldp table</pre>	Clears LLDP neighbors information



These commands reset the particular configuration to its default value.

```
lldp {transmit | receive}
```

```
no lldp notificationno lldptlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}] }
```

```
no lldptlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all | <vlan-id>}] [vlan-name {all | <vlan-id>}] }
```

```
no lldptlv-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

Basic TLV	DOT1 TLV	DOT3 TLV
<ul style="list-style-type: none">• Mandatory• Optional	<ul style="list-style-type: none">• IEEE 802.1 organizationally specific TLVs	<ul style="list-style-type: none">• IEEE 802.3 organizationally specific TLVs

their content.

Figure LLDP-1: LLDP TLV Types

The content of the various TLVs supported by Supermicro switches are specified in the figure below.

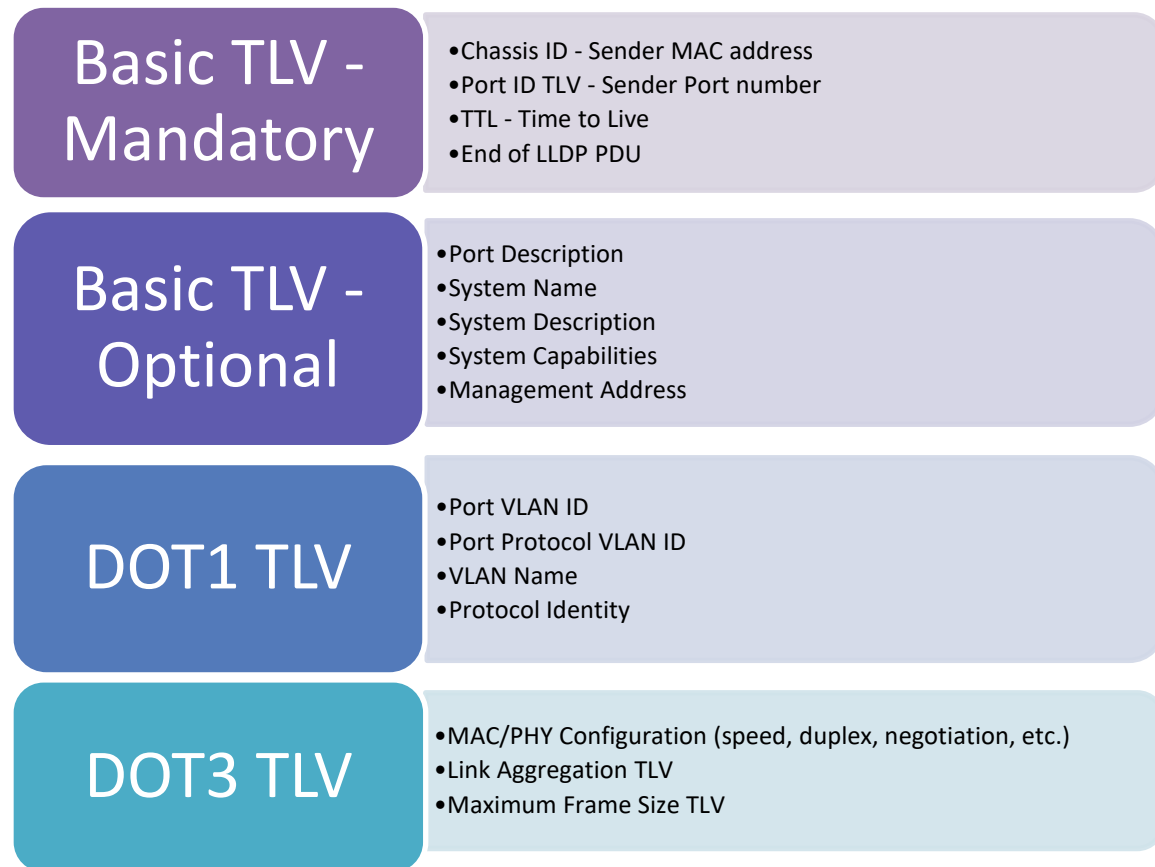


Figure LLDP-2: LLDP TLV Content

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id>	<p>(Optional) Enters the interface configuration mode.</p> <p>interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po</p> <p>interface-id is in slot/port format for all physical interfaces.</p> <p>To configure multiple interfaces, use the “interface range ...” command. To provide a range use a hyphen (-)</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		<p>between the start and end interface numbers. E.g.: int range fx 0/1-10</p> <p>To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20</p> <p>If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.</p>
Step 3	<pre>lldptlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all ipv4 <ucast_addr> ipv6 <ip6_addr>}]}</pre>	<p>(Optional)</p> <p>Enables the basic TLV transmission on a given port</p> <p>port-descr - Port description TLV</p> <p>sys-name - System name TLV</p> <p>sys-descr- System description TLV</p> <p>sys-capab - System capabilities TLV</p> <p>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.</p> <p>mgmt-addr ipv4 <i>ucast-addr</i> - Enables the transmission of a particular ipv4 address on the current interface.</p> <p>mgmt-addr ipv6 <i>ip6-addr</i> - Enables the transmission of a particular ipv6 address on the current interface.</p>
Step 4	<pre>lldptlv-select dot1tlv {[port-vlan-id] [protocol-vlan- id {all <vlan-id>}] [vlan-name {all <vlan-id>}]}</pre>	<p>(Optional)</p> <p>Configure dot1 TLV types to be transmitted on a port</p> <p>port-vlan-id - Port VLAN identifier TLV. The keyword port-vlan-id keyword is not supported.</p>

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		protocol-vlan-id - Protocol VLAN identifier TLV. The keyword protocol-vlan-id is not supported. vlan-name – VLAN name TLV NOTE: VLANname must be configured prior to this LLDP configuration.
Step 5	lldptlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] }	(Optional) Configure dot3 TLV types to be transmitted on a port macphy-config - MAC or PHY TLV. link-aggregation - Link aggregation TLV. max-framesize - Maximum frame size TLV.
Step 6	End	Exits the configuration mode.
Step 7	show lldp interface [<interface-type><interface-id>] show lldp local {[<interface-type><interface-id>] [mgmt-addr]}	Displays LLDP configuration details on a particular interface or all interfaces Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	lldp transmit-interval <seconds(5-32768)>	(Optional)

SBM-25G-100 / MBM-XEM-100 Configuration Guide

		Configures 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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	lldp holdtime-multiplier <value(2-10)>	(Optional) Configures the message transmit holdtime multiplier, range of 2-10.
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information



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

17.1.3.3 Reinitialization Delay

When LLDP ports are disabled or the link goes down, LLDP is reinitialized on a port. The delay between the port going down and the reinitialization is called the reinitialization delay. When LLDP is reinitialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Supermicro switches allow user configuration of the reinitialization delay. Follow the steps below to change the reinitialization delay.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step2	lldpreinitialization-delay <seconds(1-10)>	(Optional) Configures the reinitialization delay, range of 1-10.
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information



The “no lldpreinitialization-delay” command resets the reinitialization delay to its default value.

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.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	lldptx-delay <seconds(1-8192)>	(Optional) Configures the message transmit delay, range of 1-8192. NOTE: The Tx delay should be less than $0.25 * \text{message Tx interval}$
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information



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 the notification interval.

Step	Command	Description
------	---------	-------------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Step 1	configure terminal	Enters the configuration mode
Step 2	lldp notification-interval <seconds(5-3600)>	(Optional) Configures the notification interval, range of 5-3600.
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information



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.

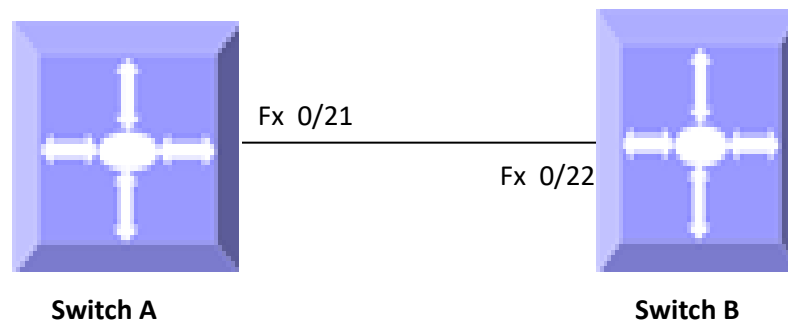


Figure LLDP-3: LLDP Configuration Example

Switch A

```
SMIS# configure terminal
```

```
SMIS(config)# set lldp enable
```

```
SMIS(config)# end
```

```
SMIS# show lldp
```

LLDP is enabled

Transmit Interval : 30

Holdtime Multiplier : 4

Reinitialization Delay : 2

Tx Delay : 2

Notification Interval : 5

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

Chassis ID	Local Intf	Hold-time	Capability	Port Id
-----	-----	-----	-----	-----
00:30:48:e3:70:bc	Fx0/21	120		Fx0/22

Total Entries Displayed : 1

SMIS(config)# lldp chassis-id-subtype if-name

SMIS(config)# lldpholdtime-multiplier 7

SMIS(config)# lldp notification-interval 100

SMIS(config)# lldpreinitialization-delay 5

SMIS(config)# lldpreinitialization-delay 9

SMIS(config)# lldpreinitialization-delay 10

SMIS(config)# lldp transmit-interval 100

SMIS(config)# lldp transmit-interval 10

SMIS(config)# end

SMIS(config)# interface Fx 0/21

SMIS(config-if)# lldp notification remote-table-chg

SMIS(config-if)# lldp port-id-subtype if-name

SMIS(config-if)# lldptlv-select basic-tlv port-descrmgmt-addr all

SMIS(config-if)# exit

SMIS(config)# vlan 1

SMIS(config-vlan)# name vlan1

SBM-25G-100 / MBM-XEM-100 Configuration Guide

```
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

Chassis ID	Local Intf	Hold-time	Capability	Port Id
------------	------------	-----------	------------	---------

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

00:30:48:e3:70:bc	Fx0/21	120		Fx0/22
-------------------	--------	-----	--	--------

Total Entries Displayed : 1

```
SMIS# show lldp errors
```

Total Memory Allocation Failures : 0

Total Input Queue Overflows : 0

Total Table Overflows : 0

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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 :

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Enabled TxTlvs : Port Description, Management Address, Mac Phy

Extended 802.3 TLV Info

-MAC PHY Configuration & Status

Auto-Neg Support & Status : Supported, Enabled

Advertised Capability Bits : 6c11

10base-T(HD)

10base-T(FD)

100base-TX(HD)

100base-TX(FD)

Asym and SymmPAUSE(FD)

1000base-T(FD)

Operational MAU Type : 30

-Link Aggregation

Capability & Status : Not Capable, Not In Aggregation

Aggregated Port Id : 21

-Maximum Frame Size : 1500

Extended 802.1 TLV Info

-Port VLAN Id : 1

-Port & Protocol VLAN Id

Protocol VLAN Id	Support	Protocol VLAN Status	TxStatus
------------------	---------	----------------------	----------

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

0	Supported	Disabled	Disabled
---	-----------	----------	----------

-Vlan Name

Vlan Id	Vlan Name	TxStatus
---------	-----------	----------

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

1	vlan1	Enabled
---	-------	---------

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

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-desccrmtgmt-addr all

lldptlv-select dot3tlv macphy-config

lldptlv-select dot1tlv vlan-name 1

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

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

SBM-25G-100 / MBM-XEM-100 Configuration Guide

-Vlan Name

Vlan Id	Vlan Name	TxStatus
-----	-----	-----
1		Disabled

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

vlan 1

ports fx 0/1-24 untagged

ports cx 0/1-3 untagged

exit

set lldp enable

18 Show Commands

Supermicro switch offer show commands to check the running state of the switch. Show commands also help to troubleshoot some issues.

Some of the show commands and their details are given below. To see all the available show commands, type '?' in the switch CLI prompt.

18.1.1 show chassis info

The command "show chassis info" displays the chassis details as shown below.

Command:

show chassis info

SBM-25G-100 / MBM-XEM-100 Configuration Guide

Example:

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#

18.1.2 show blade interfaces

The corresponding switch port for each blade server interface can be found by the command 'show blade interfaces'.

Command:

show blade interfaces

Example:

SMIS# show blade interfaces

* - Blade server detected at this slot

Blade	Node	Nic	Port	Status
=====	=====	=====	=====	=====
Blade A1	1	1	Fx0/1	not connected
Blade A2	1	1	Fx0/3	not connected
Blade A3	1	1	Fx0/5	not connected
Blade A4	1	1	Fx0/7	not connected
Blade A5*	1	1	Fx0/9	connected
Blade A6	1	1	Fx0/11	not connected
Blade A7	1	1	Fx0/13	not connected
Blade A8	1	1	Fx0/15	not connected

Blade A9	1	1	Fx0/17	not connected
Blade A10	1	1	Fx0/19	not connected
Blade A11	1	1	Fx0/21	not connected
Blade A12	1	1	Fx0/23	not connected
Blade A13	1	1	Fx0/25	not connected
Blade A14	1	1	Fx0/27	not connected

SMIS#

18.1.3 show lldp traffic

The command “show lldp traffic” displays the statistics for the LLDP packets sent and received.

Command:

```
show lldp traffic
```

Example:

```
SMIS# show lldp traffic
Total Frames Out      : 3239
Total Entries Aged    : 4
Total Frames In       : 3309
Total DCBX Frames Out : 0
Total DCBX Frames In  : 0
Total Frames Received In Error : 0
Total Frames Discarded : 0
Total TLVS Unrecognized : 3
Total TLVs Discarded  : 0
```

18.1.4 show ip http statistics

The command “show ip http statistics” displays the statistics for the HTTP GET and POST requests.

Command:

```
show ip http statistics
```

Example:

```
SMIS# show ip http statistics
HTTP Statistics:
HTTPS Connections      : 0
HTTP Connections      : 385
GET Request           : 379
POST Request          : 1
Unknown Request       : 0
```

19 Debug Commands

Supermicro switch offer debug commands to help troubleshooting some of the issues. When enabled the debug, user can see debug prints on the switch console. Debug should be enabled with caution on switches deployed in production, as it affect the switch performance.

Below are some of the debug commands and it's examples.

19.1.1 Debug DHCP Client

To debug the DHCP client issues use the command 'debug ip DHCP client'.

Command:

```
debug IP DHCP client {all | event | packets | errors | bind}
```

Example:

```
debug IP DHCP client all
```

Sample Debug Output:

```
Sep 23 13:46:31 2020 DHCP CLIENT: Rcvd Event 4
Sep 23 13:46:31 2020 DHCP CLIENT: Rcvd Msg 180b1de0 type : 3
Sep 23 13:46:31 2020 DHCP CLIENT: DHCP Client is not enabled on Interface
Sep 23 13:46:31 2020 DHCP CLIENT: Rcvd Event 4
Sep 23 13:46:31 2020 DHCP CLIENT: Rcvd Msg 180b1de0 type : 1
Sep 23 13:46:31 2020 DHCP CLIENT: Entered DhcpCopyDefaultOpt fn
Sep 23 13:46:33 2020 DHCP CLIENT: Rcvd Event 2
Sep 23 13:46:33 2020 DHCP CLIENT: Entering DhcpCProcessTmrExpiry fn
Sep 23 13:46:33 2020 DHCP CLIENT: pre-init timeout timer expired for 3 intf
Sep 23 13:46:33 2020 DHCP CLIENT: Pre-Init Timeout Expired
Sep 23 13:46:33 2020 DHCP CLIENT: Entered DhcpCInitState fn
Sep 23 13:46:33 2020 DHCP CLIENT: Entered DhcpCSendDiscover fn
Sep 23 13:46:36 2020 DHCP CLIENT: Rcvd Event 2
```

```
Sep 23 13:46:36 2020 DHCP CLIENT: Entering DhcpCProcessTmrExpiry fn
Sep 23 13:46:36 2020 DHCP CLIENT: Multiple offer timer expired for 3 intf
Sep 23 13:46:36 2020 DHCP CLIENT: Entered MultipleOfferTimerExpiry fn
Sep 23 13:46:36 2020 DHCP CLIENT: Entering DhcpCSendRequest fn
Sep 23 13:46:36 2020 DHCP CLIENT:
In the process of sending the DHCP_REQUESTmessage in S_SELECTING State
Sep 23 13:46:38 2020 DHCP CLIENT: Rcvd Event 2
Sep 23 13:46:38 2020 DHCP CLIENT: Entering DhcpCProcessTmrExpiry fn
Sep 23 13:46:38 2020 DHCP CLIENT: ARP timer expired for 3 intf in 3 state
Sep 23 13:46:38 2020 DHCP CLIENT: Entering DhcpCArpTimerExpiry fn
Sep 23 13:46:38 2020 DHCP CLIENT: ARP_RESOLVE not successful
Sep 23 13:46:38 2020 DHCP CLIENT: Entered DhcpCGetOption fn
Current DHCP Client Bindings for 3 Intf are:
```

client-id	IpAddress	expiretime
~~~~~	~~~~~	~~~~~
1> 0c:c4:7a:2c:25:ac	172.18.0.73	1295995
_____	_____	_____

### 19.1.2 Debug IGMP Snooping

To debug the IGMP snooping issues use the command 'debug IP IGMP snooping'.

Command:

```
debug IP IGMP snooping {[init][resources][tmr][src][grp][qry] [VLAN][pkt][fwd] [mgmt]
[redundancy] | all}
```

Example:

```
debug IP IGMP snooping all
```

Sample Debug Output:

```
Sep 23 18:07:01 2020 SNOOP:-GRP: Processing topology change event for port 70 failed
Sep 23 18:13:50 2020 SNOOP:-GRP: Processing topology change event for port 69 failed
Sep 23 18:18:00 2020 SNOOP:-RESRC: Vlan entry not found ,in Snoop Vlan Entry table for,VLAN 1
```

---

## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

Sep 23 18:18:00 2020 SNOOP:-VLAN: Create new VLAN entry for VLAN id 1. Hence skip this frame!

Sep 23 18:18:02 2020 SNOOP:-VLAN: Snooping Disabled for VLAN id 1. Hence fwd all!

### 19.1.3 Debug SNMP

To debug the SNMP issues use the command 'debug IP SNMP'.

Command:

```
debug IP SNMP
```

Example:

```
debug IP SNMP
```

### 19.1.4 Debug Link Aggregation

To debug the Link aggregation issues use the command 'debug LA'.

Command:

```
debug LA [{all | [init-shut] [mgmt] [data] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [sel] [pdu  
<interface-type> <interface-id>}]}
```

Example:

```
debug LA all
```

Sample Debug Output:

```
Sep 23 15:09:00 2020 LA: Called LaEnqueueControlFrame for Port 9
```

```
Sep 23 15:09:00 2020 LA: Called LaProcessLacpFrame for Port 9
```

```
Sep 23 15:09:31 2020 LA: Called LalsThisLAControlPacket
```

```
Sep 23 15:09:31 2020 LA: LalsThisLAControlPacket:Received an LA Control Frame
```

```
Sep 23 15:09:31 2020 LA: Called LaEnqueueControlFrame for Port 9
```

```
Sep 23 15:09:31 2020 LA: Called LaProcessLacpFrame for Port 9
```

```
Sep 23 15:10:02 2020 LA: Called LalsThisLAControlPacket
```

```
Sep 23 15:10:02 2020 LA: LalsThisLAControlPacket:Received an LA Control Frame
```

### 19.1.5 Debug LLDP

To debug the LLDP issues use the command 'debug LLDP'.

Command:

```
debug LLDP [{all | [init-shut] [mgmt] [data-path] [ctrl] [pkt-dump] [resource] [all-fail] [buf] [neigh-  
add] [neigh-del] [neigh-updt] [neigh-drop] [neigh-ageout] [critical]}[tlv {all | [chassis-id][port-id] [ttl] [port-
```



## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr] [port-VLAN] [PPVLAN] [VLAN-name] [proto-id]  
[MAC-phy] [pwr-mdi] [lagg] [max-frame] [dcbx]]]]]

Example:

```
debug LLDP all
```

Sample Debug Output:

```
Sep 23 15:16:07 2020 [LLDP] : MAIN: Recvd Tmr Exp Event
```

```
Sep 23 15:16:07 2020 [LLDP] : LldpTimerExpHandler: Timer expiry to be handled
```

```
Sep 23 15:16:07 2020 [LLDP] : Timer to be processed d400ba30
```

```
Sep 23 15:16:07 2020 [LLDP] : TimerId: 2      Offset: 80
```

```
Sep 23 15:16:07 2020 [LLDP] : LLDP TxDelay timer expired
```

```
Sep 23 15:16:07 2020 [LLDP] : LldpTxUtilAddChassisIdTlv: Adding Chassis ID TLV to preformed  
buffer...
```

### 19.1.6 Debug VLAN

To debug the VLAN related issues use the command 'debug VLAN'.

Command:

```
debug VLAN {global | [{fwd | priority | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os]  
[failall] [buffer] [all]] }
```

Example:

```
debug VLAN global
```

### 19.1.7 Debug Packets Handled by CPU

To debug the packets handled by CPU use the command 'debug cpu packet'. The Hex form of the packet is printed on the console, if no file name is provided. If a filename is provided, then the packets will be written to the file and stored in flash. The file can be opened and viewed with wireshark or similar applications.

Command:

```
debug cpu packet {all | rx | tx} [<interface-type> <interface-id>] <msg_limit(1-100)> [file  
<string(32)>]
```

Example:

```
debug cpu packet all fx-ethernet 0/9 3
```

```
debug cpu packet all fx-ethernet 0/9 10 file test.pcap
```

Sample Debug Output:

## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

SMIS# Sep 23 15:30:26 2020 CPU PACKET:

Tx Interface : Fx0/9

Total Bytes : 119

Data :

0180 C200 0000 OCC4 7A2C 25B6 0069 4242  
0300 0003 027E 8000 OCC4 7A2C 25AE 0000  
0000 8000 OCC4 7A2C 25AE 8009 0000 1400  
0200 0F00 0000 4000 3063 3A63 343A 3761  
3A32 633A 3235 3A61 6500 0000 0000 0000  
0000 0000 0000 0000 0000 AC36 177F 5028  
3CD4 B838 21D8 AB26 DE62 0000 0000 8000  
OCC4 7A2C 25AE 14

SMIS# Sep 23 15:30:28 2020 CPU PACKET:

Tx Interface : Fx0/9

Total Bytes : 119

Data :

0180 C200 0000 OCC4 7A2C 25B6 0069 4242  
0300 0003 027E 8000 OCC4 7A2C 25AE 0000  
0000 8000 OCC4 7A2C 25AE 8009 0000 1400  
0200 0F00 0000 4000 3063 3A63 343A 3761  
3A32 633A 3235 3A61 6500 0000 0000 0000  
0000 0000 0000 0000 0000 AC36 177F 5028  
3CD4 B838 21D8 AB26 DE62 0000 0000 8000  
OCC4 7A2C 25AE 14

Sep 23 15:30:30 2020 CPU PACKET:

Tx Interface : Fx0/9

Total Bytes : 119

Data :

```
0180 C200 0000 OCC4 7A2C 25B6 0069 4242
0300 0003 027E 8000 OCC4 7A2C 25AE 0000
0000 8000 OCC4 7A2C 25AE 8009 0000 1400
0200 0F00 0000 4000 3063 3A63 343A 3761
3A32 633A 3235 3A61 6500 0000 0000 0000
0000 0000 0000 0000 0000 AC36 177F 5028
3CD4 B838 21D8 AB26 DE62 0000 0000 8000
OCC4 7A2C 25AE 14
```

### 19.1.8 Debug Hardware Watchdog Service

To debug the hardware watchdog service use the command 'debug hwsrv'.

Command:

```
debug hwsrv {all | timer | watchdog | error}
```

Example:

```
debug hwsrv all
```

Sample Debug Output:

```
[2020/9/23 15:41:34] Reset CPLD Watchdog Timer.
```

```
[2020/9/23 15:41:44] Reset CPLD Watchdog Timer.
```

```
[2020/9/23 15:41:54] Reset CPLD Watchdog Timer.
```

```
[2020/9/23 15:42:04] Reset CPLD Watchdog Timer.
```

### 19.1.9 Debug WEBUI access

To debug the WEBUI access issues use the command 'debug nm'.

Command:

```
debug nm [{all | info | errors | mgmt | data}]
```

Example:

```
debug nm all
```

Sample Debug Output:

```
Sep 23 15:49:02 2020 log repeats 4 times after it
Sep 23 15:49:02 2020 WEBNM: Sockid:32 IP:10.1.10.15 accept() successfully!
Sep 23 15:49:02 2020 WEBNM: Sockid:32 IP:10.1.10.15:60830 enter ProcessHttpRequest
Sep 23 15:49:02 2020 WEBNM: Retrieve GET or Post
Sep 23 15:49:02 2020 WEBNM: Retrieve URL
Sep 23 15:49:02 2020 WEBNM: Retrieve version
Sep 23 15:49:03 2020 WEBNM: Retrieve URL
Sep 23 15:49:03 2020 WEBNM: Retrieve version
Sep 23 15:49:03 2020 WEBNM: HttpGetProtocol
Sep 23 15:49:03 2020 WEBNM: Read POST content
Sep 23 15:49:03 2020 WEBNM: Leave POST content
Sep 23 15:49:03 2020 WEBNM: Sockid:32 MGMT_LOCK on processing http request (lock:0x11b39
unlock:0x11b39)
Sep 23 15:49:13 2020 WEBNM: select() successfully! MaxSocketId=22
Sep 23 15:49:40 2020 Sep 23 15:49:40 2020 log repeats 6 times after it
Sep 23 15:49:40 2020 WEBNM: Retrieve GET or Post
Sep 23 15:49:40 2020 WEBNM: Retrieve URL
Sep 23 15:49:40 2020 WEBNM: Retrieve version
Sep 23 15:49:51 2020 WEBNM: select() successfully! MaxSocketId=22
```

### 19.1.10 Debug RADIUS

To debug the RADIUS issues use the command 'debug radius'.

Command:

```
debug radius {all | errors | events | packets | responses | timers}
```

Example:

```
debug radius all
```

Sample Debug Output:

Sep 23 15:55:55 2020 RAD: Sending Authentication Request to the Server.

Sep 23 15:55:55 2020 RAD: Sending to Server Address: ac1200de, Port No = 1812

Sep 23 15:55:55 2020 RAD: Packet Transmitted (AUTH):

Sep 23 15:55:55 2020 RAD: Access Request transmitted successfully...

Sep 23 15:55:55 2020 RAD: Waiting For The Response From The Server.

Sep 23 15:56:05 2020 RAD: Retransmit TIMER Expired...

Sep 23 15:56:05 2020 RAD: Retransmitting Access Request.

COUNT:[1] Id: 1

Sep 23 15:56:05 2020 RAD: Sending to Server Address: ac1200de, Port No = 1812

Sep 23 15:56:05 2020 RAD: Packet Transmitted (AUTH):

### 19.1.11 Debug REST

To debug the REST issues use the command 'debug rest'.

Command:

```
debug rest [{all | api | errors | event}]
```

Example:

```
debug rest all
```

Sample Debug Output:

```
|<0xfffeb0008ac0>| Received record packet of unknown type 71
```

```
|<0xfffeb0008ac0>| Received record packet of unknown type 71
```

```
|<0xfffeb0008ac0>| Received record packet of unknown type 71
```

### 19.1.12 Debug STP

To debug the spanning-tree issues use the 'debug spanning-tree' command.

Command:

```
debug spanning-tree { global | { all | errors | init-shut | management | memory | bpdu | events |  
timer | state-machine { port-info | port-recieve | port-role-selection | role-transition | state-transition |  
protocol-migration | topology-change | port-transmit | bridge-detection } | redundancy | sem-variables} }
```

Example:

## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

debug spanning-tree all

Sample Debug Output:

```
Sep 23 16:09:07 2020 AST: :SNMP: Management SET of Debug Option as 131071 Success
Sep 23 16:09:07 2020 AST: :SNMP: Resetting the Trace Option...
Sep 23 16:09:08 2020 AST: :TMR: HOLD Timer EXPIRED for Instance: 0, Port: 9, TxCount: 0
Sep 23 16:09:08 2020 AST: :TMR: Expired Timer processed
Sep 23 16:09:08 2020 AST: :TMR: Timer Expiry event successfully processed ...
Sep 23 16:09:09 2020 AST: :TMR: HELLOWHEN Timer EXPIRED for Instance: 0, Port: 9
Sep 23 16:09:09 2020 AST: :TXSM: Port 9: Tx Machine Called with Event: HELLOWHEN_EXP,State:
IDLE of Instance 0
Sep 23 16:09:09 2020 AST: :TXSM: Port 9: Moved to state TRANSMIT_PERIODIC
Sep 23 16:09:09 2020 AST: :TXSM: Port 9: Moved to state IDLE
Sep 23 16:09:09 2020 AST: :TMR: Starting Timer HELLOWHEN for port 9 and Instance 0 for duration
2
Sep 23 16:09:09 2020 AST: :TMR: Port 9: Inst 0: Started Timer HELLOWHEN for duration 2
Sep 23 16:09:10 2020 AST: :TMR: HOLD Timer EXPIRED for Instance: 0, Port: 9, TxCount: 0
```

### 19.1.13 Debug SSH

To debug the SSH issues use the command 'debug SSH'.

Command:

```
debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [counter] [mem])
```

Example:

```
debug ssh all
```

Sample Debug Output:

```
Sep 23 16:16:25 2020 SSH: servconf.c Updating session timeout 1800 for ConnIndex 1
Sep 23 16:16:25 2020 SSH: debug3: Normalising mapped IPv4 in IPv6 address
Sep 23 16:16:25 2020 Sep 23 16:16:25 2020 log repeats 1 times after it
Sep 23 16:16:25 2020 SSH: debug1: Client protocol version 2.0; client software version
PuTTY_Release_0.68
Sep 23 16:16:25 2020 SSH: debug1: no match: PuTTY_Release_0.68
```

## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

Sep 23 16:16:25 2020 SSH: debug1: Enabling compatibility mode for protocol 2.0

Sep 23 16:16:26 2020 SSH: debug3: receive packet: type 21

Sep 23 16:16:26 2020 SSH: debug2: set_newkeys: mode 0

Sep 23 16:16:26 2020 SSH: debug1: rekey after 4294967296 blocks

Sep 23 16:16:26 2020 SSH: debug1: SSH2_MSG_NEWKEYS received

Sep 23 16:16:26 2020 SSH: debug1: KEX done

Sep 23 16:16:26 2020 SSH: debug3: receive packet: type 5

Sep 23 16:16:28 2020 SSH: debug3: receive packet: type 50

Sep 23 16:16:28 2020 SSH: debug1: userauth-request for user ADMIN service ssh-connection method none

Sep 23 16:16:28 2020 SSH: debug1: attempt 0 failures 0

Sep 23 16:16:28 2020 SSH: debug2: Unrecognized authentication method name: none

Sep 23 16:16:28 2020 SSH: Failed none for ADMIN from none port 41112 ssh2

Sep 23 16:16:28 2020 SSH: debug3: userauth_finish: failure partial=0 next methods="password,keyboard-interactive,hostbased"

Sep 23 16:16:30 2020 SSH: debug3: receive packet: type 50

Sep 23 16:16:30 2020 SSH: debug1: userauth-request for user ADMIN service ssh-connection method password

Sep 23 16:16:30 2020 SSH: debug1: attempt 2 failures 1

Sep 23 16:16:30 2020 SSH: debug2: input_userauth_request: try method password

Sep 23 16:16:30 2020 SSH: Accepted password for ADMIN from ssh-connection port 41112 ssh2

Sep 23 16:16:30 2020 SSH: debug3: send packet: type 52

Sep 23 16:16:33 2020 SSH: Connection closed by

Sep 23 16:16:33 2020 SSH: Disconnecting: Connection Closed

### 19.1.14 Debug TACACS

To debug the TACACS issues use the command 'debug tacacs'.

Command:

```
debug tacacs {all | info | errors | dumptx | dumprx}
```

## SBM-25G-100 / MBM-XEM-100 Configuration Guide

---

Example:

```
debug tacacs all
```

Sample Debug Output:

```
Sep 23 19:14:19 2020 TACACS+: Tx Pkt:
```

```
Sep 23 19:14:19 2020 0xc1 0x01 0x01 0x00 0x1a 0x6e 0x9a 0x6f 0x00 0x00
```

```
Sep 23 19:14:19 2020 0x00 0x1e 0x01 0x0f 0x02 0x01 0x06 0x0a 0x00 0x06
```

```
Sep 23 19:14:19 2020 0x74 0x61 0x63 0x61 0x63 0x73 0x6c 0x6f 0x67 0x69
```

```
Sep 23 19:14:19 2020 0x6e 0x5f 0x61 0x75 0x74 0x68 0x74 0x61 0x63 0x61
```

```
Sep 23 19:14:19 2020 0x63 0x73
```

```
Sep 23 19:14:19 2020 TACACS+: Rx Pkt:
```

```
Sep 23 19:14:19 2020 0xc1 0x01 0x02 0x00 0x1a 0x6e 0x9a 0x6f 0x00 0x00
```

```
Sep 23 19:14:19 2020 0x00 0x06 0x01 0x00 0x00 0x00 0x00 0x00
```

```
Sep 23 19:14:36 2020 TACACS+: Tx Pkt:
```

```
Sep 23 19:14:36 2020 0xc1 0x01 0x01 0x00 0x61 0x14 0xc9 0xcb 0x00 0x00
```

```
Sep 23 19:14:36 2020 0x00 0x1e 0x01 0x0f 0x02 0x01 0x05 0x0a 0x00 0x07
```

```
Sep 23 19:14:36 2020 0x41 0x44 0x4d 0x49 0x4e 0x6c 0x6f 0x67 0x69 0x6e
```

```
Sep 23 19:14:36 2020 0x5f 0x61 0x75 0x74 0x68 0x61 0x6b 0x61 0x6b 0x61
```

```
Sep 23 19:14:36 2020 0x6b 0x61
```

```
Sep 23 19:14:36 2020 TACACS+: Rx Pkt:
```

```
Sep 23 19:14:36 2020 0xc1 0x01 0x02 0x00 0x61 0x14 0xc9 0xcb 0x00 0x00
```

```
Sep 23 19:14:36 2020 0x00 0x06 0x02 0x00 0x00 0x00 0x00 0x00
```

### 19.1.15 Display Active Debug Settings

To find the currently enabled debug settings use the command 'show debugging'.

Example:

```
SMIS# show debugging
```

```
IGS :
```



Init debugging is on

Resource debugging is on

Timer debugging is on

Source debugging is on

Group debugging is on

Query debugging is on

SNOOP Vlan debugging is on

Packet debugging is on

Forward debugging is on

Management debugging is on

IGS Redundancy debugging is on

RADIUS :

RADIUS error debugging is on

RADIUS event debugging is on

RADIUS packet debugging is on

RADIUS response debugging is on

RADIUS timer debugging is on

DHCP Client :

DHCP Client event handling related debugging is on

DHCP Client packets debugging is on

DHCP Client errors debugging is on

DHCP Client binding debugging is on

TACACS :

TACACS info debugging is on

TACACS error debugging is on

TACACS packet transmission debugging is on

TACACS packet reception debugging is on

SMIS#

### **19.1.16    Disable Debugging**

To disable any active debugging, use the 'no' form of the debug command. See the examples below.

Example:

```
SMIS# no debug ip igmp snooping all
```

```
SMIS# no debug radius
```

```
SMIS# no debug tacacs
```

```
SMIS# no debug ip dhcp client all
```

To disable all the active debug settings at once, use the command 'no debug all'.

Example:

```
SMIS# no debug all
```

