MBM-GEM-004

Switch Configuration Guide

The information in this USER'S MANUAL has been carefully reviewed and is believed to be accurate. Thevendor 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 ororganization of the updates. Please Note: For the most up-to-date version of this manual, please seeour web site at www.supermicro.com.

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

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

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa ClaraCounty in the State of California, USA. The State of California, County of Santa Clara shall be theexclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will notexceed the price paid for the hardware product.

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

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

Manual Revison 1.1

Release Date: April 28, 2016

Contents

1 Introduction

This document explains the switch configuration for Supermicro blade switch model MBB-GEM-004.

The switch MBB-GEM-004 supports only layer 2 features.

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*.

Console Port

MBM-GEM-004 has 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: 9600
Data: 8 bit
Parity: none
Stop: 1 bit
Flow Control: none

2 System Configurations

Supermicro switches come with a default static management IP address 192.168.100.102

In blade switches the management IP address is assigned to internal management Ethernet ports connected to CMM. Hence the management IP address is reachable through CMM Ethernet connection. This management IP address is not reachable through front panel 1G or 10Gig ports.

Parameter	Default Value
IP address	192.168.100.102
Broadcast Address	255.255.255.255
Gateway	0.0.0.0

2.1Static 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. *ip-address* – A valid IPv4 Address. *ip-address/prefix-length* - A valid IPv4 Address with a prefix length of value 1-32. *subnet-mask* – A valid IP subnet mask.
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

2.2DHCP

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.

2.2.1 Management IP address

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 interfaceIP 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

2.2.2 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. *ip-address* – IP address of a directly connected router.
Step 3	End	Exits the configuration mode.

Step 4	show ip interface	Displays the interface IP configuration.

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

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

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

SMIS# configure terminal

SMIS(config)# ip gateway 10.1.1.1

SMIS(config)# end

2.3 Management Access

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

- User name and password
- Enable password
- Authorized Managers

Defaults – Management Access

Parameter	Default Value
User Name/Password/Privilege	ADMIN/ADMIN/15 1
Privilege (For configured users)	1
Enable Password	ADMIN
IP Authorized Managers	None

2.3.1 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. *user-name*–Alphanumeric characters of

		length 1-20 *password* – Alphanumeric characters of length 1-20 *privilege* - Specify 1-15, any of the privilege levels
Step 3	End	Exits the configuration mode.
Step 4	list users 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. Configured users are not displayed in 'show running config' command.

The "no username <user-name>" command deletes the configured user.

The example below shows the commands used to configure users.

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

SMIS(config)# end

SMIS# list users

Users Privilege
----- ---------
ADMIN 15
user1 15
SMIS# show users

Line User Peer-Address
0 con user1 Local Peer

2.3.2 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.

		Enable Level – 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

2.3.3 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.

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. *Level* – Specify 1-15, any of the privilege levels *LINE enable password* – Alphanumeric
Step 3	End	Exits the configuration mode.

The *enable password*configuration is saved automatically as part of start-up config.Enable password configuration is 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

2.3.4 IP Authorized Manager

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

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

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

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]]	Configure the authorized manager *ip-address* – ManagerIP address *subnet mask* – 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 *prefix-length*- Prefix length of the IP address, in range 1-32. *interface-type* – Specify the interface typethrough which the IP authorized manager can access the switch.*M*ay be any of the following: gigabitethernet – gi extreme-ethernet – ex interface-id is in slot/port format for all physical interfaces. *vlan* -Specify the vlan idthrough which the IP authorized manager can access the switch. *service* – Specify the services that can be accessed by the authorized manager
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

Ports allowed : Gi0/1, Gi0/2, Gi0/3, Gi0/4

Gi0/5, Gi0/6, Gi0/7, Gi0/8

Gi0/9, Gi0/10, Gi0/11, Gi0/12

Gi0/13, Gi0/14, Gi0/15, Gi0/16

Gi0/17, Gi0/18, Gi0/19, Gi0/20

Gi0/21, Gi0/22, Gi0/23, Gi0/24

Ex0/1, Ex0/2, Ex0/3

Vlans allowed : All Available Vlans

Ip Address : 200.200.200.10

Ip Mask : 255.255.255.255

Services allowed : TELNET

Ports allowed : Gi0/1, Gi0/2, Gi0/3, Gi0/4

Gi0/5, Gi0/6, Gi0/7, Gi0/8

Gi0/9, Gi0/10, Gi0/11, Gi0/12

Gi0/13, Gi0/14, Gi0/15, Gi0/16

Gi0/17, Gi0/18, Gi0/19, Gi0/20

Gi0/21, Gi0/22, Gi0/23, Gi0/24

Ex0/1, Ex0/2, Ex0/3

Vlans allowed : All Available Vlans

2.4Interface Properties

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

Parameter	Default Value
MTU	1500 bytes
Speed	For 1G – 1Gbps For 10G – 10Gbps
Negotiation	For 1G interfaces – Auto For 10G – Fixed speed 10000
Storm-control	Disabled
Description	None
Duplex Operation	Full
Flow Control	Off

2.4.1 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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20

		If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	description <string>	Configure the interface description *String* – 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 Gi 0/22
SMIS(config-if)# description server1-server2
SMIS(config-if)# end
SMIS# show interface description

Interface    Status   Protocol  Description
---------    ------   --------  -----------
Gi0/1        up       down
Gi0/2        up       down
Gi0/3        up       down
Gi0/4        up       down
Gi0/5        up       down
Gi0/6        up       down
Gi0/7        up       down
Gi0/8        up       down
Gi0/9        up       down
Gi0/10       up       down
Gi0/11       up       down
Gi0/12       up       down
Gi0/13       up       down
Gi0/14       up       down
Gi0/15       up       down
Gi0/16       up       down
Gi0/17       up       down
Gi0/18       up       down
Gi0/19       up       down
Gi0/20       up       down
Gi0/21       up       down
Gi0/22       up       up

Gi0/23       up       down
```

Gi0/24 up down
Ex0/1 up down
Ex0/2 up down
Ex0/3 up down

2.4.2 Negotiation

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

Auto negotiation is enabled by default in all external 1Gig interfaces. In 10Gig interfaces auto negotiation is not supported.

Follow the steps below to configure Interface Negotiation.

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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 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 Gi 0/22
SMIS(config-if)# no negotiation

SMIS(config-if)# end
SMIS# show interface status

Port	Status	Duplex	Speed	Negotiation
Gi0/1	not connected	Full	1 Gbps	Auto
Gi0/2	not connected	Full	1 Gbps	Auto
Gi0/3	not connected	Full	1 Gbps	Auto
Gi0/4	not connected	Full	1 Gbps	Auto
Gi0/5	not connected	Full	1 Gbps	Auto
Gi0/6	not connected	Full	1 Gbps	Auto
Gi0/7	not connected	Full	1 Gbps	Auto
Gi0/8	not connected	Full	1 Gbps	Auto
Gi0/9	not connected	Full	1 Gbps	Auto
Gi0/10	not connected	Full	1 Gbps	Auto
Gi0/11	not connected	Full	1 Gbps	Auto
Gi0/12	not connected	Full	1 Gbps	Auto
Gi0/13	not connected	Full	1 Gbps	Auto
Gi0/14	not connected	Full	1 Gbps	Auto
Gi0/15	not connected	Full	1 Gbps	Auto
Gi0/16	not connected	Full	1 Gbps	Auto
Gi0/17	not connected	Full	1 Gbps	Auto
Gi0/18	not connected	Full	1 Gbps	Auto
Gi0/19	not connected	Full	1 Gbps	Auto
Gi0/20	not connected	Full	1 Gbps	Auto
Gi0/21	not connected	Half	1 Gbps	Auto
Gi0/22	not connected	Full	1 Gbps	No-Negotiation
Gi0/23	not connected	Half	1 Gbps	Auto
Gi0/24	not connected	Half	1 Gbps	Auto
Ex0/1	not connected	Full	10 Gbps	No-Negotiation
Ex0/2	not connected	Full	10 Gbps	No-Negotiation
Ex0/3	not connected	Full	10 Gbps	No-Negotiation

2.4.3 Speed

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

1Gig RJ45 interfaces can be configured to operate in 10Mbps or 100Mbps or 1000Mbps speed.

10Gig interfaces can be configurable to operate in 1Gig or 10Gig speed.

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*> ….	Enters the interface configuration mode. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	speed { 10 | 100 | 1000 | 10000 }	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 Gi 0/44
SMIS(config-if)# speed 100

```
SMIS(config-if)# end
SMIS# show interface status

Port      Status        Duplex  Speed     Negotiation
----      ------        ------  -----     -----------
Gi0/1     not connected  Full   1 Gbps    Auto
Gi0/2     not connected  Full   1 Gbps    Auto
Gi0/3     not connected  Full   1 Gbps    Auto
Gi0/4     not connected  Full   1 Gbps    Auto
Gi0/5     not connected  Full   1 Gbps    Auto
Gi0/6     not connected  Full   1 Gbps    Auto
Gi0/7     not connected  Full   1 Gbps    Auto
Gi0/8     not connected  Full   1 Gbps    Auto
Gi0/9     not connected  Full   1 Gbps    Auto
Gi0/10    not connected  Full   1 Gbps    Auto
Gi0/11    not connected  Full   1 Gbps    Auto
Gi0/12    not connected  Full   1 Gbps    Auto
Gi0/13    not connected  Full   1 Gbps    Auto
Gi0/14    not connected  Full   1 Gbps    Auto
Gi0/15    not connected  Full   1 Gbps    Auto
Gi0/16    not connected  Full   1 Gbps    Auto
Gi0/17    not connected  Full   1 Gbps    Auto
Gi0/18    not connected  Full   1 Gbps    Auto
Gi0/19    not connected  Full   1 Gbps    Auto
Gi0/20    not connected  Full   1 Gbps    Auto
Gi0/21    not connected  Half   1 Gbps    Auto
Gi0/22    not connected  Full   10 Mbps   No-Negotiation

Gi0/23    not connected  Half   1 Gbps    Auto
Gi0/24    not connected  Half   1 Gbps    Auto
Ex0/1     not connected  Full   10 Gbps   No-Negotiation
Ex0/2     not connected  Full   10 Gbps   No-Negotiation
Ex0/3     not connected  Full   10 Gbps   No-Negotiation
```

2.4.4 Duplex Operation

Supermicro switches support configuration of Full-Duplex operation or Half-Duplex operation to physical interfaces.

Follow the steps below to configure Duplex operation.

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: gigabitethernet – gi extreme-ethernet – ex

		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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	duplex { full | half }	Configure Duplex operation.
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 duplex” command restores the default interface full duplex operation.

The example below shows the commands used to configure Duplex operation.

```
SMIS# configure terminal
SMIS(config)# interface Gi 0/22
SMIS(config-if)# duplex half
SMIS(config-if)# end
SMIS# show interface status

Port      Status        Duplex  Speed     Negotiation
----      ------        ------  -----     -----------
Gi0/1     not connected Full    1 Gbps    Auto
Gi0/2     not connected Full    1 Gbps    Auto
Gi0/3     not connected Full    1 Gbps    Auto
Gi0/4     not connected Full    1 Gbps    Auto
Gi0/5     not connected Full    1 Gbps    Auto
Gi0/6     not connected Full    1 Gbps    Auto
Gi0/7     not connected Full    1 Gbps    Auto
Gi0/8     not connected Full    1 Gbps    Auto
Gi0/9     not connected Full    1 Gbps    Auto
```

Gi0/10	not connected	Full	1 Gbps	Auto
Gi0/11	not connected	Full	1 Gbps	Auto
Gi0/12	not connected	Full	1 Gbps	Auto
Gi0/13	not connected	Full	1 Gbps	Auto
Gi0/14	not connected	Full	1 Gbps	Auto
Gi0/15	not connected	Full	1 Gbps	Auto
Gi0/16	not connected	Full	1 Gbps	Auto
Gi0/17	not connected	Full	1 Gbps	Auto
Gi0/18	not connected	Full	1 Gbps	Auto
Gi0/19	not connected	Full	1 Gbps	Auto
Gi0/20	not connected	Full	1 Gbps	Auto
Gi0/21	not connected	Half	1 Gbps	Auto
Gi0/22	not connected	Half	1 Gbps	No-Negotiation
Gi0/23	not connected	Half	1 Gbps	Auto
Gi0/24	not connected	Half	1 Gbps	Auto
Ex0/1	not connected	Full	10 Gbps	No-Negotiation
Ex0/2	not connected	Full	10 Gbps	No-Negotiation
Ex0/3	not connected	Full	10 Gbps	No-Negotiation

2.4.5 MTU

The default maximum transmission unit (MTU) size for frames received and transmitted is 1500 bytes. The MTU size can be increased for an interface.

Follow the steps below to configure Interface MTU.

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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,).

		E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	mtu<frame-size(1500-9216)>	Configure interface MTU in the range 1500-9216.
Step 4	End	Exits the configuration mode.
Step 5	show interface status	Displays the interface configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

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

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

Gi0/22 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port
Hardware Address is 00:30:48:e3:70:d1

MTU 9000 bytes, Half duplex, 1 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 : 3549
Unicast Packets : 0
Broadcast Packets : 13
Multicast Packets : 26
Pause Frames : 0
Undersize Frames : 0
Oversize Frames : 0
CRC Error Frames : 0
Discarded Packets : 39
Error Packets : 0
Unknown Protocol : 0

Transmission Counters

Octets : 7198
Unicast Packets : 0
Non-Unicast Packets : 59
Pause Frames : 0
Discarded Packets : 0
Error Packets : 0
SMIS(config-if)# show interface mtu Gi 0/22

Gi0/22 MTU size is 9000

2.4.6 Flow control

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

If a port experiences congestion and cannotreceive any more traffic, it notifies the other port by sending a pause frame to stop sending until thecondition 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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	flowcontrol { send | receive} { on | off }	Configure flow control *Send* – The port can send pause frames

		but cannot receive pause frames from a connected device. *Receive* – The port cannot send pause frames but can receive pause frames from a connected device. On – Enable flow control Off - Disable flow control
Step 4	End	Exits the configuration mode.
Step 5	show flow-control [interface <interface-type><interface-id>]	Displays the Interface Flow control configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

Port	TxFlowControl	Rx FlowControl	Tx Pause	Rx Pause
Gi0/22	on	off	0	0

2.4.7 Storm control

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

Storm control monitors packets passing from an interface to the switching busand determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packetsof a specified type received within the 1-second time interval and compares the measurement with apredefined 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 normalforwarding.

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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 <pps-rate-value (1-10000000)>	Configure Storm control for broadcast or multicast or DLF packets. Level – Threshold level in Packets per second, in range 1-10000000.
Step 4	End	Exits the configuration mode.
Step 5	show interfaces storm-control	Displays the interface Storm control configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

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

SMIS# show interfaces Gi 0/22 storm-control

Gi0/22

DLF Storm Control : Disabled

Broadcast Storm Control : Enabled

Broadcast Storm Control : 50000

Multicast Storm Control : Disabled

2.5Time 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

2.5.1 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. *ip_addr* – IP address of server. *key* – Authentication Key for server connectivity in the range 1-65535. *prefer* –This option can be used to specify a preferred NTP server when multiple NTP servers are configured in the switch. Only 1 server can be configured 'prefer' at a time.
Step 3	End	Exits the configuration mode.
Step 4	show ntp	Displays the NTP configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

If 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
```

2.5.2 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.

```
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
```

2.5.3 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. *Key-number* –key number in the range 1-65535, used for MD5. *Key-text*–NTP key text to be used along with key-number for MD5.
Step 3	End	Exits the configuration mode.
Step 4	show ntp	Displays the NTP configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

The example below shows the commands used to configure NTP.

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

SMIS(config)# show ntp

[NTP] ntp is enabled
```

```
   Server     Key   Prefer

=============== ===== ======

 Key #    Key

======= ==================================

  200    For-server1

 Time zone offset not set
```

2.5.4 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. *authentication* – If specified, NTP authentication isenabled for broadcast mode.
Step 3	End	Exits the configuration mode.
Step 4	show ntp	Displays the NTP configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no ntp broadcast” command disables NTP broadcast.

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

```
SMIS(config)# ntp broadcast authentication

SMIS(config)# show ntp

[NTP] ntp running broadcast mode

   Server     Key   Prefer

=============== ===== ======

 Key #    Key
```

```
======= ==================================
```

Time zone offset not set

2.5.5 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. *hh:mm:ss* – Time in Hours:Minutes:Seconds format. *day* – Day in 1-31 format. *month* – Month in January-December format. *year* – Year in yyyy format.
Step 2	show clock	Displays the system clock.

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

SMIS# clock set 09:26:15 31 august 2013

Wed Aug 31 09:26:15 2013

SMIS# show clock

Wed Aug 31 09:26:20 2013

2.5.6 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 offset HH<-12 to 13>:MM<0, 30 or 45>	Configure the timezone. *HH* – Hour in range -12 to 13.

		MM – Minutes specified as 0 or 30 or 45.
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 offset 12:30
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: 12:30
```

2.6System 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

2.6.1 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. *Devname*– 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.

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
```

2.6.2 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. *String* – Contact information entered as a String of maximum length 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 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
```

2.6.3 System location

Supermicro switches provide 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
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

2.6.4 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

Gi0/1   MTU size is 9200
Gi0/2   MTU size is 9200
Gi0/3   MTU size is 9200
Gi0/4   MTU size is 9200
Gi0/5   MTU size is 9200
Gi0/6   MTU size is 9200
Gi0/7   MTU size is 9200
Gi0/8   MTU size is 9200
Gi0/9   MTU size is 9200
Gi0/10  MTU size is 9200
Gi0/11  MTU size is 9200
Gi0/12  MTU size is 9200
Gi0/13  MTU size is 9200
Gi0/14  MTU size is 9200
Gi0/15  MTU size is 9200
Gi0/16  MTU size is 9200
Gi0/17  MTU size is 9200
Gi0/18  MTU size is 9200
Gi0/19  MTU size is 9200
Gi0/20  MTU size is 9200
Gi0/21  MTU size is 9200
Gi0/22  MTU size is 9200
Gi0/23  MTU size is 9200
Gi0/24  MTU size is 9200
```

Ex0/1 MTU size is 9200
Ex0/2 MTU size is 9200
Ex0/3 MTU size is 9200

2.6.5 Static MAC

The MAC address table stores MAC addressesused by the switch to forward traffic betweenports. 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 addressesi.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 floodedto all ports and not learned.
- A static address is created by specifying the destination MAC unicast address and theVLAN from which it is received. Packets received with this destination address are forwarded to theinterface 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>]]) [forbidden-ports ([<interface-type><0/a-b,0/c,...>] [<interface-type><0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) [status { permanent | deleteOnReset | deleteOnTimeout }] mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface <interface-type><iface> [status { permanent | deleteOnReset | deleteOnTimeout }]	Configure Multicast or unicast static MAC. *Vlan* – Specify the VLAN for which the packet with thespecified 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. *Interface-type* - may be any of the following: gigabitethernet – gi extreme-ethernet – ex interface-id is in slot/port format for all physical interfaces. Forbidden-ports - Set of ports

		forbidden for the VLAN. *Permanent*–Static MAC is not deleted even after switch reboot. *deleteOnReset* – Static MAC is deleted on switch reset/reboot. *deleteOnTimeout* - Static MAC is deleted along with dynamic MAC entries, after the aging time timesout.
Step 3	End	Exits the configuration mode.
Step 4	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 a:aa:aa>] [{interface <interface-type><interface-id> }]	Displays the static MAC configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “ no mac-address-table static multicast <aa:aa:aa:aa: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 Gi 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    Gi0/14
```

Total Mac Addresses displayed: 1

2.6.6 MAC aging

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

Follow the steps below to configure MAC Aging.

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   Gi0/21
1       94:d7:23:94:88:d8   Learnt   Gi0/21
Total Mac Addresses displayed: 2
```

2.7 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
Logging buffer size	50 entries
Console logging	Enabled
File Logging	Disabled
Trap Logging	Critical
MAC Address table update Logging	Disabled
Facility	Local0

2.7.1 Enable/Disable Syslog

Syslog is enabled by default in Supermicro switches.

Follow the steps below to disableSyslog.

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
LogBuffer(0 Entries)

LogFile(0 Entries)

2.7.2 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. *ip-address* –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)

2.7.3 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)

2.7.4 Log file

System Logging messages can be stored as a Log file in switch NVRAM.

Follow the steps below to enable storing Logs in a File.

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. *Filename* – Specify file name of upto 32 characters. *Short*–Specify entries that can stored in file in range 1-8000.
Step 3	End	Exits the configuration mode.
Step 4	show logging	Displays the Syslog configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

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 Gi0/22 status changed to UP

<129> Apr 29 10:11:31 2013:INTF-1:Interface Gi0/22 status changed to UP

SMIS#
SMIS# show logging

System Log Information

Syslog logging : enabled(Number of messages 0)
Console logging : disabled(Number of messages 0)
File logging : enabled(Number of messages 2)
Log File Name : log1
File Max Entries : 500

TimeStamp option : enabled
Trap logging : Critical
Log server IP : None
Facility : Default (local0)
Buffered size : 50 Entries

LogBuffer(11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7:Exitting DHCPC Task Init
<135> Apr 29 10:11:05 2013:DHC-7:Entered in 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 Gi0/22 status changed to UP
LogFile(2 Entries)
<129> Apr 29 10:11:30 2013:INTF-1:Interface Gi0/22 status changed to UP

<129> Apr 29 10:11:31 2013:INTF-1:Interface Gi0/22 status changed to UP

2.7.5 Logging Buffer

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

Follow the steps below to configure Syslog Buffer.

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)
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:Exitting DHCPC Task Init
<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCIntSelectTaskMain fn
<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCSocketOpen fn
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cb8128 type : 1
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4

<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cb8128 type : 1
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cf4258 type : 1
<135> Apr 29 10:11:08 2013:DHC-7:Rcvd Event 4
<135> Apr 29 10:11:08 2013:DHC-7:Rcvd Msg 13cf4858 type : 1
LogFile(0 Entries)
```

2.7.6 Facility

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

Follow the steps below to configure Syslog Facility.

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
SMIS(config)# end
SMIS# show logging

System Log Information

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

Buffered size : 50 Entries
LogBuffer(0 Entries)

LogFile(0 Entries)

2.7.7 MAC table logging

Supermicro switches support logging of MAC address table updates.

Follow the steps below to enable logging of MAC address table updates.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	logging mac-address-table	Enable logging of MAC address table updates.
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 mac-address-table” command disables Logging of MAC Address table updates.

The example below shows the commands used to enable logging of MAC address table updates.

SMIS# configure terminal
SMIS(config)# logging mac-address-table

SMIS(config)# end

2.7.8 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 }]	Configure Logging Traps. There are various levels of trap that can be logged. *Level 0 – Emergencies* Used for logging messages that areequivalent to a panic condition. *Level 1 –Alerts* Used for logging messages that require immediate attention *Level 2 – Critical* Used for logging critical errors *Level 3 –Errors* Used for error messages *Level 4 –Warning* Used for logging warning messages *Level 5 –Notification* Used for logging messages that require attention but are not errors *Level 6 – Informational* Used for logging informational messages. *Level 7 – Debugging* Used for logging debug messages.
Step 3	End	Exits the configuration mode.

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

The “no logging trap” command resets 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:Exitting DHCPC 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
<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)

2.7.9 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)

2.7.10 Clear Log File

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

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)
```

2.8Configuration Management

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

2.8.1 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.
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.

2.8.2 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 writeexisting 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 writeexisting 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 gi 0/1-48 untagged
ports ex 0/1-4 untagged
exit
snmp view restricted 1 excluded nonvolatile
setip igmp enable
setip pim enable
ip pim component 1
exit

2.8.3 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 gi 0/1-48 untagged

ports ex 0/1-4 untagged

exit

snmp view restricted 1 excluded nonvolatile

setip igmp enable

setip pim enable

ip pim component 1

exit

2.8.4 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-	Copy from startup-config to a file in

	address/filename}	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#

2.8.5 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: filenametftp://ipaddress/filename copy tftp://ip-address/filename flash: filename copy flash: filename flash: filename	Copies a local flash file to remote TFTP server. Copies a remote file to local flash. 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#

2.8.6 Deleting Saved Configuration

Supermicro switches allow deletion of switch startup configuration and other stored configuration files.

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

Step	Command	Description
Step 1	erase startup-config erase flash:filename	Removes the startup-config. 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#

2.8.7 Firmware upgrade

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

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

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}”.

2.8.8 Boot-up options

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

Follow the steps below to configure Switch Boot-Up firmware option.

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
```

2.8.9 Reset to Factory Defaults

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

Follow the steps below to reset to Factory Defaults.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	reset-to-factory-defaults	Configure Factory Defaults.

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

After reset to factory defaults, switch can be managed using the default management IP address 192.168.100.102 with default administrator user name ADMINand password ADMIN.

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

2.9 Tracking Uplink Failure

The Uplink Failure Tracking Feature (ULFT) is useful for blade switches. This helps blade servers to move to redundant 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	***link-status-tracking enable***	Enabling uplink failure tracking feature
Step 3	***link-status-tracking group <id>***	Creating group
Step 4	***link-status-tracking group <id> upstream***	Adding uplink to group
Step 5	***link-status-tracking group <id> downstream***	Adding downstream ports to group
Step 6	***link-status-tracking disable***	Disabling uplink failure tracking feature
Step 7	**End**	Exits the configuration mode.
Step 8	***show link-status-tracking***	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 gi 0/1 to gi 0/14 when uplink interfaces gi 0/15 and gi 0/16 go down:

SMIS# configure terminal
SMIS(config)# link-status-tracking enable
SMIS(config)# link-status-tracking group 1
SMIS(config)# interface range gi0/15-16
SMIS(config-if)# link-status-tracking group 1 upstream
SMIS(config-if)# exit
SMIS(config)# interface range gi0/1-14
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

Note:

If more than one uplink port is configured, all downstream ports will be brought down only when all upstream ports are down.

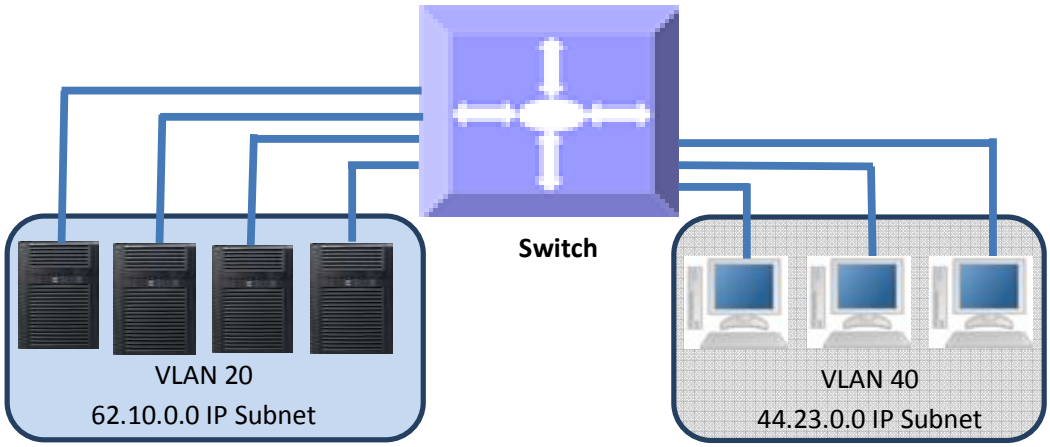
3 VLAN

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 VLANsprovides the following advantages:

- ⇒ Limitsmulticast 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**

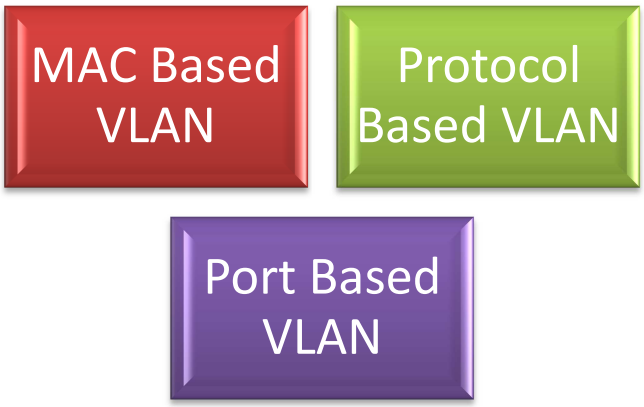


VLANswork in same way as physical LANs. The packets from the end stations of a VLAN are switched only to other end stations or network devices inside that VLAN. To reach devices in another VLAN, the packets have to be routed from one VLAN to another. Supermicro L2 switch support such InterVLAN Routing to route packets across different VLANs.

3.1VLAN 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 procedurebelow.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.

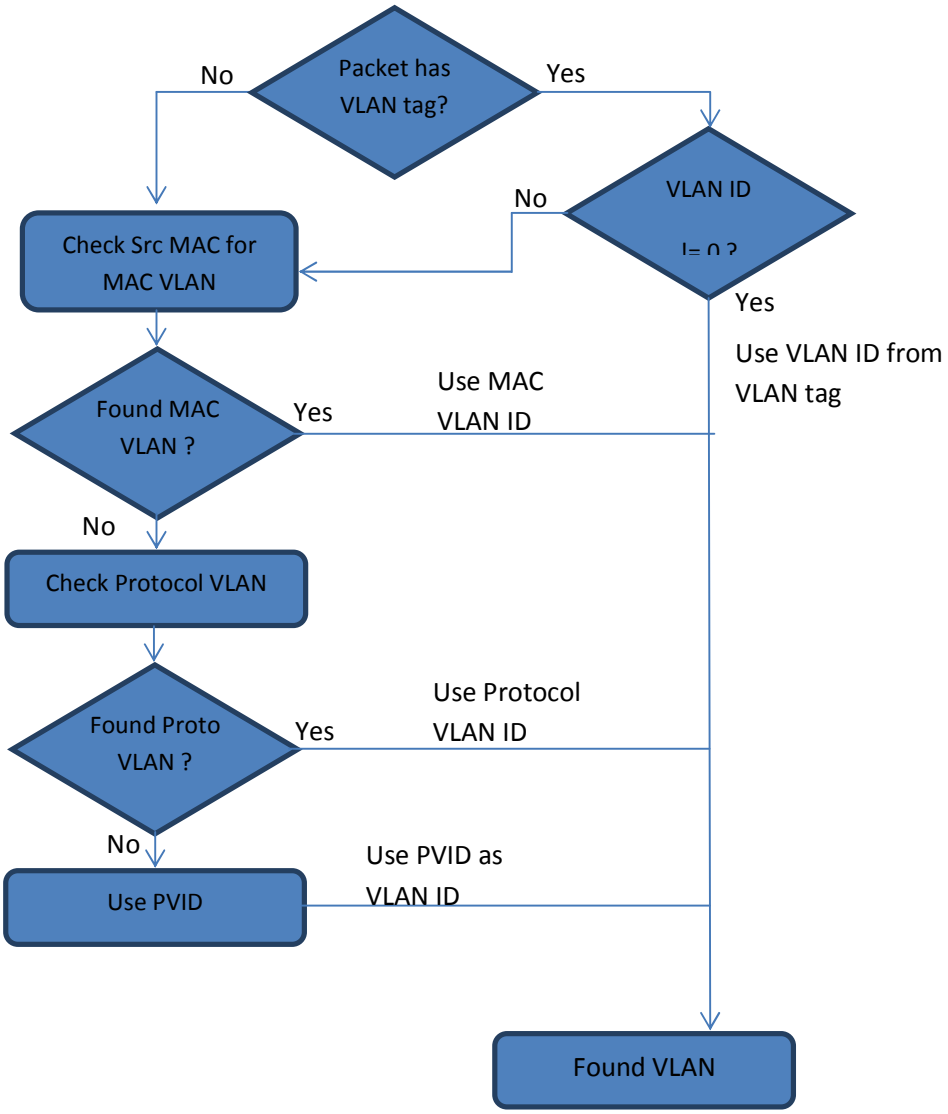
Step 2: Use the protocol field from the incoming packet layer 2 header and check the protocol VLAN table. If a protocol VLAN is found, that VLAN ID is used as the VLAN for this packet. If a protocol VLAN is not found, proceed to the next step.

Step 3: Use the PVID from the port on which the packet is received as the VLAN ID 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, it will be forwarded to any other member port 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



3.2VLAN Numbers

Supermicro switches support VLAN identifiers from 1 to 4069 for user created VLANs. VLAN identifiers 4070 to 4094 are reserved for internal use.

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

Supermicro switches support 16 protocol groups for protocol based VLANs. These 16 protocol groups can be mapped todifferent VLANs in every port. Same protocol group can be associated with different VLAN in different port.

3.3VLAN 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 access 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.

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 config.

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.Users can modify the PVID for switch ports to any VLAN identifier.

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

3.4Creating 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. vlan-list – may be any vlan number or list of vlan numbers. Multiple vlan numbers can be provided as comma-separated values. Consecutive vlan numbers can be provided as a range,such as 5-10. User can configure VLANs with identifiers 1 to 4069.
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 creatingVLANs.

Create a VLAN with identifier 10

SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# exit
Create VLANs with identifiers20 to 30, 50 and 100

SMIS# configure terminal

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

3.5Removing VLANs

Follow the steps below to remove VLANsfrom Supermicro switches.

Step	Command	Description
Step 1	configure terminal	Enter the configuration mode
Step 2	no vlan <vlan-list>	RemoveVLANs using the**no vlan** command. vlan-list – may be any vlan number or list of vlan numbers. Multiple vlan numbers can be provided as comma separated list. Consecutive vlan numbers can be provided as ranges like 5-10.
Step 3	show vlan	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)# novlan 10

Delete VLANs with identifier 20 to 30, 50 and 100

SMIS# configure terminal

SMIS(config)# novlan 20-30,50,100

SMIS(config-vlan)# exit

3.6VLAN Name

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

Follow the steps below to add or modifya name string to any VLAN in Supermicro switches.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	vlan <vlan-list>	Entersthe VLAN configuration mode. vlan-list – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the same name string provided in next step will be associated with all these VLANs.
Step 3	name <vlan-name-string>	Associates aname string to this VLAN using thename command. vlan-name-string is any alphanumeric string up to 32 characters.
Step 4	show vlan	Displays the configured VLANs
Step 5	write startup-config	Optional step – savesthis VLAN configuration to be part of startup configuration.

The examplebelow 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)# vlan50

SMIS(config-vlan)# namemain_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>	Entersthe VLAN configuration mode. vlan-list – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-

		separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the name string of all these VLANs will be removed by the next step.
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 – savesthis 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)# vlan50
SMIS(config-vlan)# no name
SMIS(config-vlan)# exit

3.7Port Based VLANs

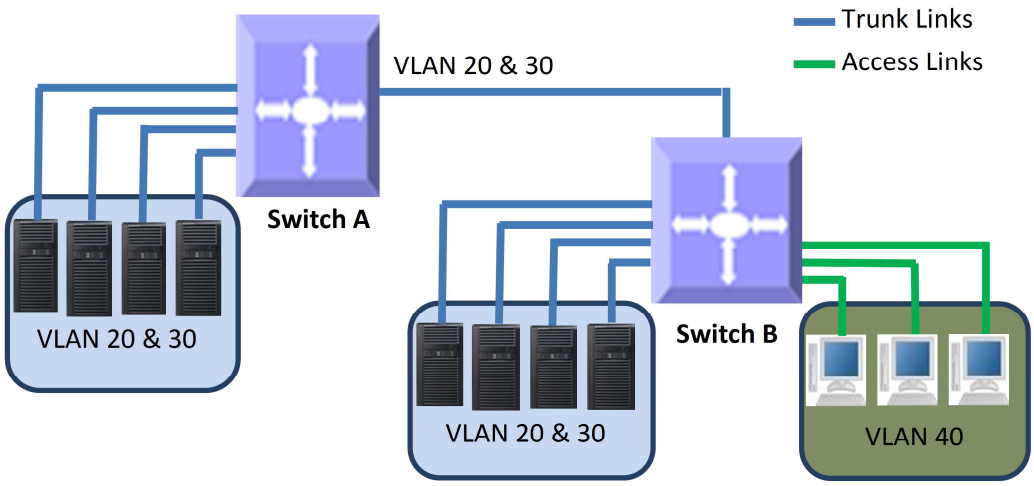
Port based VLANsare the simplest and most useful type of VLAN.

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

The VLAN traffic sent on the ports is decided by the VLAN membership modes 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



3.7.1 Access Ports

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

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

Switch will not add VLAN tag header for all the packets sent out on an access port.Switch expects to receive untagged or priority tagged (VLAN identifer 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. interface-type– may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-idis in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-)

		between the start and end interface numbers. E.g.:int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 VLANs identifiers may be any VLAN number from 1 to 4069. If the given VLAN does not exist, switch will provide a warning message. Only when the VLAN available, the port will operate as an access port for that VLAN.
Step 5	show vlan port config port <iftype><ifnum>	Displays the configured mode and accesses the VLAN for this interface.
Step 6	write startup-config	Optional step – savesthis VLAN configuration to be part of startup configuration.

"switchport access vlan" command will be effective 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 sectionHybrid 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 50and configure ports gi 0/2 to gi 0/10 as access ports to this VLAN.
SMIS# configure terminal
SMIS(config)# vlan 50
SMIS(config-vlan)# exit
SMIS(config)# interface range gi 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 10and configure port channel 1 as access port to this VLAN.
SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# exit
SMIS(config)# interface po 1
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# exit

3.7.2 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 sectionAllowed VLANs on a Trunk.

Trunk ports will not carry traffic for VLANs that are not configured in a switch.
For example, if the user wants to carry traffic for all the VLANs from 1 to 1024 in a trunk port, VLANs 1 to 1024 need to be created in the switch using the “vlan” command.

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

When a packet is received on a trunk port, the switch identifies the VLAN for the received packet from the packet’s VLAN tag header. If the received packet did not have a VLAN identifier and the packet did not match any MAC or protocol VLAN, the native VLAN is used to determine the VLAN for all untagged and priority tagged packetsthat 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. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,).

		E.g.: int range gi 0/1-10, gi 0/20
Step 3	switchport mode trunk	Sets the port mode as a trunk port.
Step 4	show vlan port config port <iftype><ifnum> and show running-config	Displays the configured mode for this interface.
Step 5	write startup-config	Optional step – savesthis 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 ex 0/1 and ex 0/2as trunk ports.
SMIS# configure terminal
SMIS(config)# interface range ex 0/1-2
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit
Configure port channel 1 as a trunk port.
SMIS# configure terminal
SMIS(config)# interface po 1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit

3.7.2.1 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 stepsbelow.

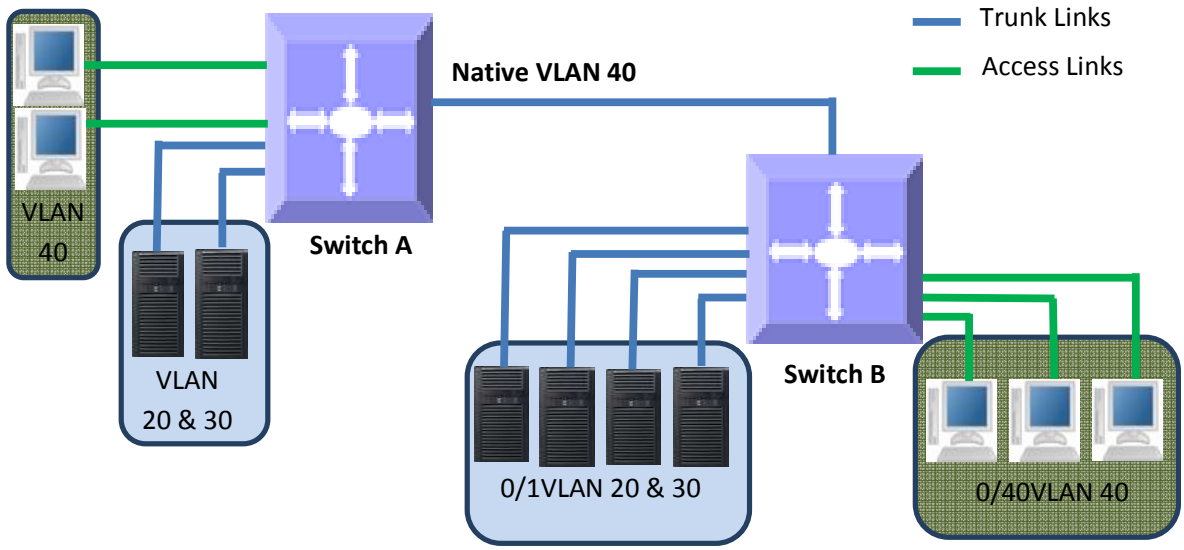
Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	Enters the interface mode. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel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

		To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
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 vlan-list 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 vlan-list will be carried over the trunk.
Step 4b	switchport trunk allowed vlan add<vlan-list>	This command adds the given list of VLANS to the existing set of allowed VLANs on this trunk.
Step 4c	switchport trunk allowed vlan remove<vlan-list>	This command removes the given list of VLANS from the existing set of allowed VLANs on this trunk.
Step 4d	switchport trunk allowed vlan except<vlan-list>	This command makes all the configured VLANs allowed on this trunk except for the given list of VLANs.
Step 4e	switchport trunk allowed vlan all	This command sets the default behavior of allowing all VLANs configured in the switch as allowed VLANs on this trunk.
Step 4f	switchport trunk allowed vlan none	This command removes all the allowed VLANs from this trunk.
Step 5	show vlan port config port <iftype><ifnum> and show running-config	Displays the configured, allowed VLANs for this trunk interface.
Step 6	write startup-config	Optional step – savesthis VLAN configuration to be part of startup configuration.

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 ex 0/1.
SMIS# configure terminal
SMIS(config)# vlan 2-20
SMIS(config-vlan)# exit
SMIS(config)# interface ex 0/1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan 2-20
SMIS(config-if)# exit
Configure to not to allow VLANs 30 to 50 on trunk interface ex 0/1.
SMIS# configure terminal
SMIS(config)# interface ex 0/1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan except 30-50
SMIS(config-if)# exit
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 configurea native VLAN for trunk interfaces by following the stepsbelow.

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. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	switchport mode trunk	Sets the port mode as a trunk port.
Step 4	switchport trunk native vlan<vlan-id>	vlan-id - The VLAN identifiers may be from 1 to 4069. If the given VLAN does not exist, switch will provide a warning message. In this case the native VLAN traffic will be dropped until the VLAN become available.
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 – savesthis VLAN configuration to be part of startup configuration.

“switchport trunk native vlan” command will be effective 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 examples below show examplesof configuringnative VLANs for trunk ports.

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

SMIS# configure terminal
SMIS(config)# vlan 20
SMIS(config-vlan)# exit
SMIS(config)# interface ex 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 ex 0/1.
SMIS# configure terminal
SMIS(config)# interface ex 0/1
SMIS(config-if)# no switchport trunk native vlan
SMIS(config-if)# exit

3.7.3 Hybrid Ports

Hybrid ports carry both untagged and 802.1Q tagged packets. Hybrid ports are equivalent to trunk ports, with a limited amount of allowed VLANs and native VLANs.

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.

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>	vlan-list – may be any VLAN number or

		list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the ports configuration provided in the next steps will be applied to all these VLANs.
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	Adds the tagged ports list to this VLAN. ports-list–up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format gi 0/1-10, whichspecifies the ports from gi 0/1 to gi 0/10. Use the no form of this command to remove tagged ports from this VLAN. If ports-listis not provided to theno command, all the tagged ports are removed from this VLAN.
Step 3b	ports <ports-list> untagged or no ports [<ports-list>] untagged	Adds the untagged ports list to this VLAN. ports-list – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format gi 0/1-10, whichspecifiesthe ports from gi 0/1 to gi 0/10. Use the no form of this command to remove untagged ports from this VLAN. If ports-listis not provided to theno command, all the untagged ports are removed from this VLAN.
Step 3c	ports <ports-list> forbidden or no ports [<ports-list>] forbidden	Denies traffic from ports given by ports-list to this VLAN. ports-list – up to three ports or ranges of ports separated by spaces. The range of ports is provided in the format gi 0/1-10,which specifies the ports from gi 0/1 to gi 0/10.

		Use the no form of this command to remove forbidden ports from this VLAN. If ports-listis not provided to theno command, all the forbidden ports are removed from this VLAN.
Step 4	Exit	Exitsthe VLAN configuration mode.
Step 5	interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	Enters the interface mode. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 6	switchport mode hybrid	Sets the port mode as a hybrid port.
Step 7	switchport pvid <vlan-id>	Configures the PVID for this interface. The VLANs identifiers could be any VLAN number from 1 to 4069. The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first.
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 – savesthis 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 effective only when the ports is in “hybrid” mode.

The examples below show various ways to configure hybrid ports.

Configure a VLAN 10 with ports gi 0/1 to gi 0/10 as untagged ports and add port ex 0/1as a tagged port to this VLAN.

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

3.8MAC Based VLANs

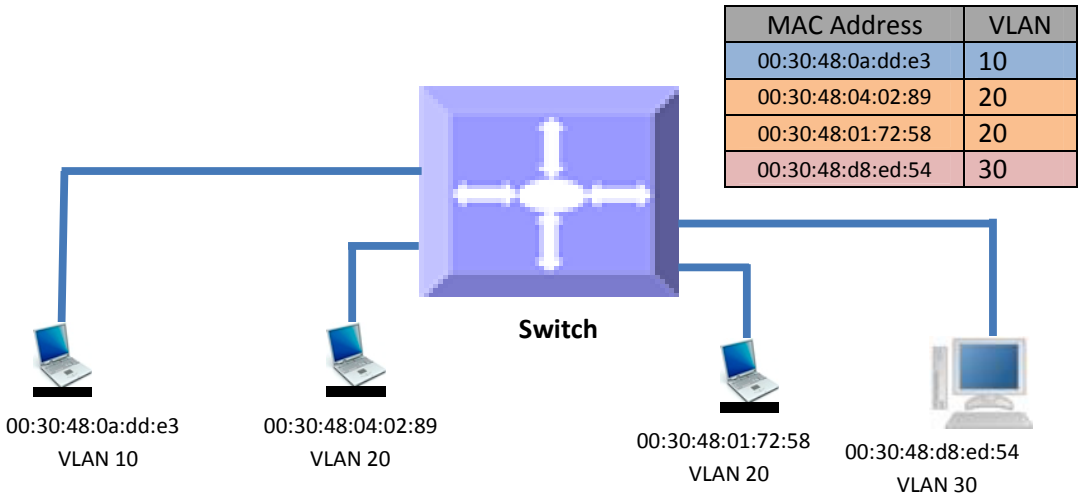
When end users move often from one place to another but remain inside the same LAN, it is difficult to maintain the same VLAN for an end user with port based VLAN configurations.

MAC based VLAN featuresare 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. 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 ranges such as 5-10.
Step 3	ports <ports-list> untagged	Adds the ports given by ports-list to this VLAN as untagged ports. ports-list – up to three ports or ranges of ports separated by spaces. The range of ports is provided in the format gi 0/1-10, which specifies the ports from gi 0/1 to gi 0/10.
Step 4	Exit	Exits the VLAN configuration mode.
Step 5	mac-vlan**<ucast_mac>**vlan<vlan-id>	Configures MAC VLAN mapping entry. ucast_mac – Unicast MAC address. This VLAN will be applied to all incoming untagged packets from this unicast MAC address. vlan-id - 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. ucast_mac – Unicast MAC address for which MAC VLAN mapping is to be removed.
Step 3	show mac-vlan	Displays the configured MAC based VLANs.
Step 4	write startup-config	Optional step – savesthis VLAN configuration to be part of startup configuration.

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

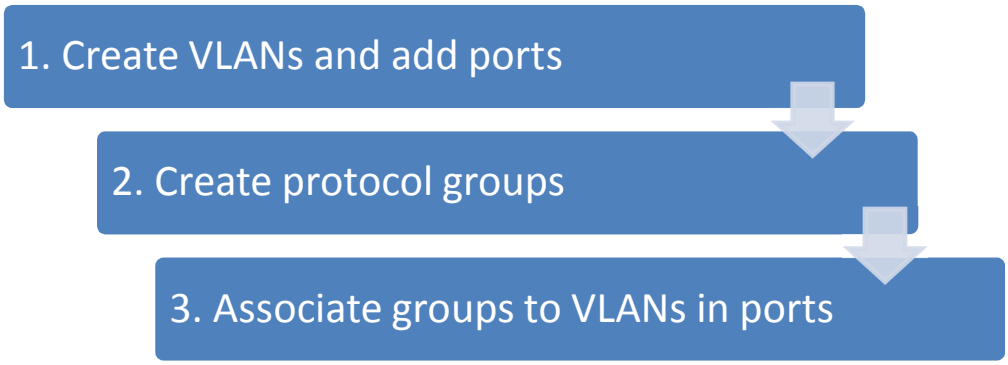
Create a VLAN 10 and configure MAC address 00:30:40:10:10:10 to VLAN 10 for the ports gi 0/1 to 10

SMIS# configure terminal
SMIS(config)# vlan 10
SMIS(config-vlan)# ports gi 0/1-10 untagged
SMIS(config-vlan)# exit
SMIS(config)# mac-vlan 00:30:40:10:10:10 vlan 10
Remove MAC VLAN for MAC address 00:30:40:20:20:20.
SMIS# configure terminal
SMIS(config)#no mac-vlan 00:30:40:20:20:20

3.9Protocol 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 featuresare enabled by default in Supermicro switches.
Protocol based VLAN features configuration is a three-step process, as shown in the diagrambelow.
Figure VLAN-7:Protocol Based VLAN Configuration Steps



Follow the steps below to configure protocol based VLANs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	vlan <vlan-list>	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.
Step 3	ports <ports-list> untagged	Adds the required ports for this VLAN as untagged ports. ports-list – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in a format like gi 0/1-10, which refers to ports from gi 0/1 to gi 0/10.
Step 4	Exit	Exits the VLAN configuration mode.
Step 5	map protocol {arp | ip | rarp | ipx | novell | netbios | appletalk | other <aa:aa oraa:aa:aa:aa:aa>} {enet-v2 | RFC1042 | llcOther | snap8021H | snapOther}protocols-group<Group id integer(0-2147483647)>	Createsa protocol group. Protocol group creation takes three parameters. 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. Second: frame type as enet-v2,llc or snap. Third: protocol group identifier

		number.
Step 6	interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	Enters the interface mode. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It could be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the "interface range …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 7	switchport map protocols-group<Group id integer(0-2147483647)>vlan<vlan-id(1-4069) >	Associatesthe group to the VLAN on the above interface. Group id – Protocol Group Identifier vlan-id – VLAN identifier.
Step 8	switchport pvid <vlan-id>	Configures the PVID for the default port based VLAN behavior. This will be used for packets that did not match any protocol VLAN map. The VLAN identifiers may be any VLAN number from 1 to 4069. The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first.
Step 9	Exit	Exits the interface configuration mode.
Step 10	show vlan protocols-group show protocol-vlan	Displays the configured protocol based VLANs.
Step 11	write startup-config	Optional step – savesthis 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 <interface-type><interface-id> or interface range <interface-type><interface-id> ….	Enters the interface mode. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It could be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	no switchport map protocols-group<Group id integer(0-2147483647)>	Removes the protocol groups from interface mode. Group id – Protocol Group Identifier
Step 4	Exit	Exits VLAN configuration mode.
Step 5	no map protocol {arp | ip | rarp | ipx | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa:aa>} {enet-v2 | RFC1042 | llcOther | snap8021H | snapOther}	Removes the protocol group. Before removing any protocol group, it must have been removed from all interfaces.
Step 6	no vlan <vlan-list> or vlan <vlan-list> no ports <ports-list> untagged	Removes the VLANs created for protocol based VLANs. If the VLAN is shared with a MAC or port based VLAN, then remove only the ports added during the protocol based VLAN configuration. To remove the ports use the “no ports” command in the VLAN configuration mode. vlan-list – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN

		numbers may be provided as a range, such as 5-10.
Step 7	show vlan protocols-group show protocol-vlan	Displays the protocol based VLANs.
Step 8	write startup-config	Optional step – savesthis 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 gi 0/1 to gi 0/10.
SMIS# configure terminal
SMIS(config)# vlan 20,30
SMIS(config-vlan)# po gi 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 gi 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 gi 0/1-10
SMIS(config-if)# no switchport map protocols-group 1
SMIS(config-if)# no switchport map protocols-group 2
SMIS(config-if)# exit
SMIS(config)# no map protocol arp enet-v2
SMIS(config)#no map protocol ip enet-v2
SMIS(config)# no vlan 20

3.10 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, thedefault 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. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g. : int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g. : int range gi 0/1-10, gi 0/20
Step 3	Use any of the below steps 3a to 3d to configure acceptable frame types for the ports provided in Step 2 above.	
Step 3a	switchport acceptable-frame-type tagged	This command makes only tagged frame types accepted on these ports. Any untagged or priority tagged packets received will be dropped.
Step 3b	switchport acceptable-frame-type untaggedAndPrioritytagged	This command makes only untagged and priority tagged frame types accepted on these ports. Any tagged packets received will be dropped.
Step 3c	switchport acceptable-frame-type all	This command makes accepting all frame types the default behavior.
Step 3d	no switchport acceptable-frame-type	This command makes accepting all frame types the default behavior.
Step 4	show vlan port config port <iftype><ifnum>	Displays the configured mode and access VLAN for this interface.
Step 5	write startup-config	Optional step – saves this VLAN configuration to be part of startup configuration.

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

Configure gi 0/1 to gi 0/10 to accept only untagged and priority tagged packets.
SMIS# configure terminal
SMIS(config)# interface range gi 0/1-10
SMIS(config-if)# switchport acceptable-frame-type untaggedAndPrioritytagged
SMIS(config-if)# exit
Configure port channel interface 1 to accept only tagged packets.
SMIS# configure terminal
SMIS(config)# interface po 1
SMIS(config-if)# switchport acceptable-frame-type tagged
SMIS(config-if)# exit

3.11 Ingress Filter

By default, Supermicro switch has the ingress filter disabled. Ingress filter can be enabled 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 still accept the packets with VLAN header having VLAN identifier20. This is called VLAN hoping. To prevent VLAN hoping, the ingress filter can be enabled to drop the packets with different VLAN identifier than VLAN configured on the port.

Follow the steps below to enable 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. interface-type – may be any of the following: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g. : int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g. : int range gi 0/1-10, gi 0/20

Step 3	switchport ingress-filter	This command enables ingress filtering function.
Step 4	show vlan port config port <iftype><ifnum>	Displays the configured ingress filtermode for this interface.
Step 5	write startup-config	Optional step – saves this VLAN configuration to be part of startup configuration.

The “no swithcport ingress-filter” command disables the ingress filter.

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

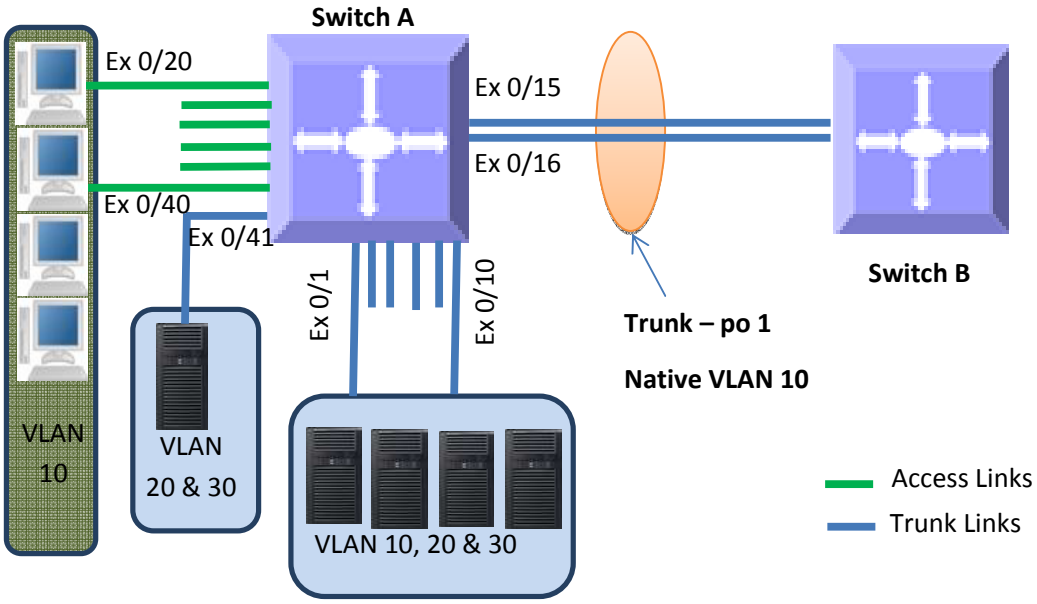
Enable ingress filter for ports gi 0/1 to gi 0/10.
SMIS# configure terminal
SMIS(config)# interface range gi 0/1-10
SMIS(config-if)# switchport ingress-filter
SMIS(config-if)# exit

3.12 VLAN Configuration Example

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

1. Ports Ex 0/1 to Ex0/10 are trunk ports connected to servers that have VLANs 10, 20 and 30. Here, VLAN 10 is untagged.
2. Port Ex 0/41 is a trunk port connected to storage, which carries VLAN 20 and 30.
3. Ports Ex 0/20 to Ex 0/40 are access ports for VLAN 10.
4. Ports Ex 0/15 and Ex 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 ex 0/1-10
SMIS(config)# interface range ex 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 ex 0/41
SMIS(config)# int ex 0/41
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# exit
Configure the access VLAN for ports ex 0/20 to ex 0/40
SMIS(config)# interface range ex 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 ex 0/15 and ex 0/16
SMIS(config)# interface port-channel 1
SMIS(config-if)# exit
SMIS(config)# interface range ex 0/15-16
SMIS(config-if)# channel-group 1 mode on
SMIS(config-if)# exit
SMIS(config)# interface port-channel 1
SMIS(config-if)# switchport mode trunk

```
SMIS(config-if)# switchport trunk native vlan 10
SMIS(config-if)# end
# Check the running-configuration for accuracy
SMIS# show running-config

Building configuration...
Switch ID      Hardware Version          Firmware Version     OS Version
0              MBM-GEM-004               1.0.0                1.0.0

ip address 172.31.30.120
interface port-channel 1
exit
vlan 1
  ports gi 0/1-2 untagged
 ports ex 0/11-14 untagged
 ports ex 0/17-19 untagged
 ports ex 0/42-48 untagged
exit

vlan 10,20,30
exit

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

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

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

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

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

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

interface Ex 0/7
 switchport trunk native vlan 10
```

```
 switchport mode trunk

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

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

interface Ex 0/10
 switchport trunk native vlan 10
 switchport mode trunk

interface Ex 0/15
 channel-group 1 mode on

interface Ex 0/16
 channel-group 1 mode on

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

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

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

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

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

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

interface Ex 0/26
 switchport access vlan 10
 switchport mode access
```

```
interface Ex 0/27
 switchport access vlan 10
 switchport mode access

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

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

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

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

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

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

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

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

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

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

interface Ex 0/38
 switchport access vlan 10
 switchport mode access
```

```
interface Ex 0/39
 switchport access vlan 10
 switchport mode access

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

interface Ex 0/41
 switchport mode trunk

interface po 1
 switchport trunk native vlan 10
 switchport mode trunk

# Check the VLANs using the “show vlan” command
SMIS# show vlan
Vlan database
-------------
Vlan ID          : 1
Member Ports      : gi 0/1-2 ex 0/1-14 ex 0/17-19 ex 0/41-48 po 1
Tagged Ports      : None
Untagged Ports    : gi 0/1-2 ex 0/11-14 ex 0/17-19 ex 0/42-48
Forbidden Ports   : None
Access Ports      : None
Trunk Ports       : ex 0/1-10 ex 0/41 po 1
Name              :
Status            : Permanent
-----------------------------------------------------
Vlan ID          : 10
Member Ports      : ex 0/1-10 ex 0/20-41 po 1
Tagged Ports      : None
Untagged Ports    : None
Forbidden Ports   : None
Access Ports      : ex 0/20-40
Trunk Ports       : ex 0/1-10 ex 0/41 po 1
Name              :
Status            : Permanent
-----------------------------------------------------
Vlan ID          : 20
Member Ports      : ex 0/1-10 ex 0/41 po 1
Tagged Ports      : None
Untagged Ports    : None
Forbidden Ports   : None
Access Ports      : None
Trunk Ports       : ex 0/1-10 ex 0/41 po 1
Name              :
Status            : Permanent
```

```
------------------------------------------------------
Vlan ID          : 30
Member Ports     : ex 0/1-10 ex 0/41 po 1
Tagged Ports     : None
Untagged Ports   : None
Forbidden Ports  : None
Access Ports     : None
Trunk Ports      : ex 0/1-10 ex 0/41 po 1
Name             :
Status           : Permanent
------------------------------------------------------
# Save these VLAN configurations
SMIS# write startup-config
Building configuration, Please wait. May take a few minutes ...
[OK]
SMIS#
```

3.13 Private Edge VLAN / Protected Ports

The Private Edge VLAN or also called Protected Portsfeature 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.

3.13.1 Unprotected Port

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

3.13.2 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.

3.13.3 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

3.14 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.

3.15 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.

3.16 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.

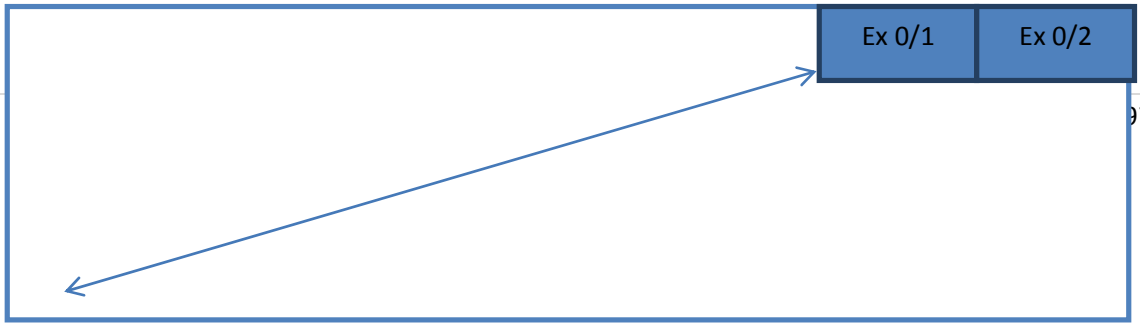
Maximum of 24 different communities can be configured in the switch.

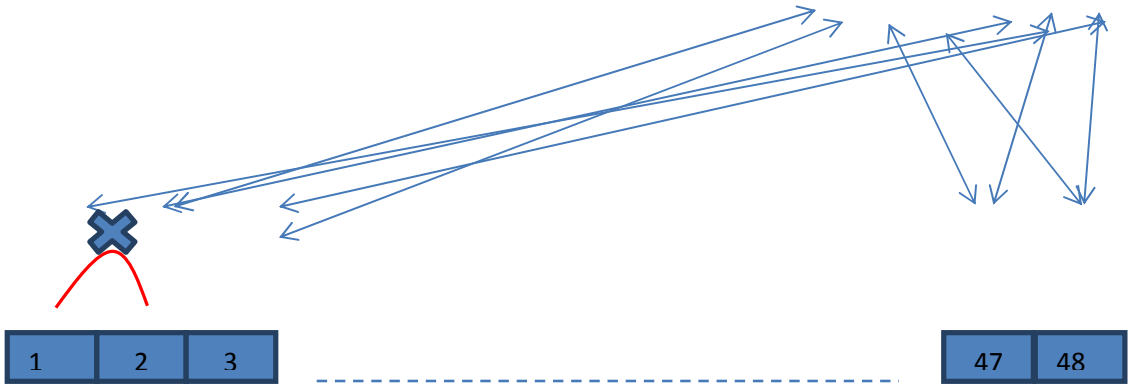
Note:

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

3.16.1 Configuration Example 1

Configure all the 48 downlink 1Gig 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 ex 0/1 and ex 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 1Gig ports need to be configured as protected ports.

```
SMIS# configure term

SMIS(config)# interface range gi 0/1-48

SMIS(config-if)# switchport protected

SMIS(config-if)# exit
```

3.16.2 Configuration Example 2

The 1Gig ports 1 to 24 should be able to communicate among themselves and also should be able to communicate with up link ports ex 0/1 and ex 0/2.

The 1Gig ports 25 to 48 should be able to communicate among themselves and also should be able to communicate with up link ports ex 0/1 and ex 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 gi 0/1-24
SMIS(config-if)# switchport protected group 1
SMIS(config-if)# exit
SMIS(config)# interface range gi 0/25-48
SMIS(config-if)# switchport protected group 2
SMIS(config-if)# exit
```

4 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.

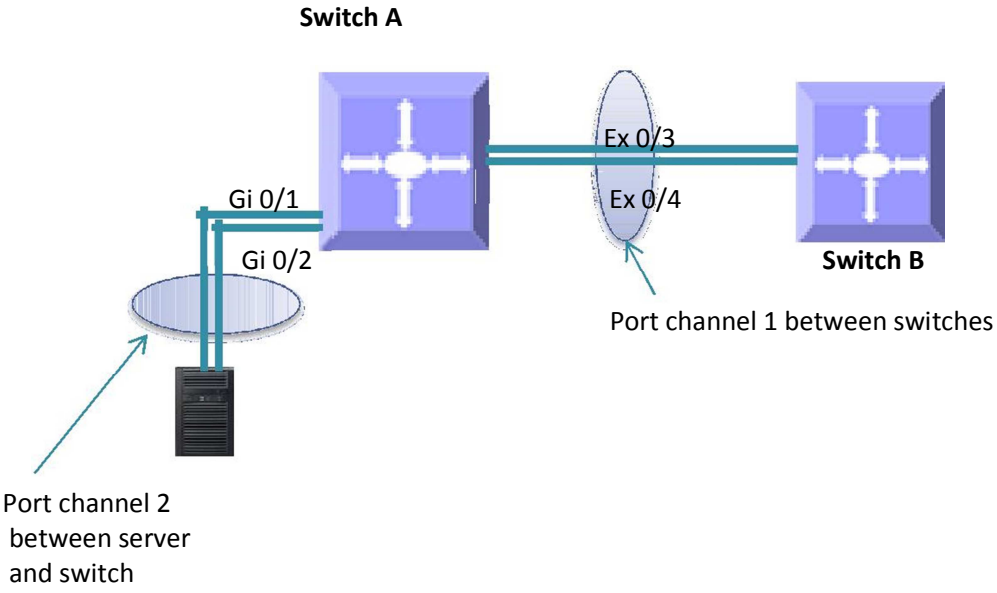
Link Aggregation provides the following advantages:

Increased bandwidth – User can connect up to eight physical links between devices to increase the link bandwidth. When 1 Gbps links are aggregated, users can get an aggregated link with up to 8 Gbps bandwidth . In 10Gig switches, 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 agrregatelinks

4.1 Link Aggregation Support

Supermicro switches support both static and dynamic link aggregations. Dynamic link aggregation support is based on the Link Aggregation Control Protocol (LACP).
Supermicro switches support only Layer 2 level link aggregation. Hence, only switching ports can be aggregated.
Supermicro switches do not support the Multiple Chassis Link Aggregation (MLAG) feature

4.2 Link Aggregation Numbers

Supermicro switches support up to 52 port channels.
Each port channel can have eight active links.

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

4.3 Link Aggregation Defaults

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

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

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

The default LACP system priority is 32768.

The default LACP port priority is 128.

The default LACP timeout is long (30 seconds).

The default LACP wait time is 2 seconds.

4.4 Static Link Aggregation

Supermicro switches support static link aggregation.

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

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

4.5Dynamic 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 “ndependent” 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

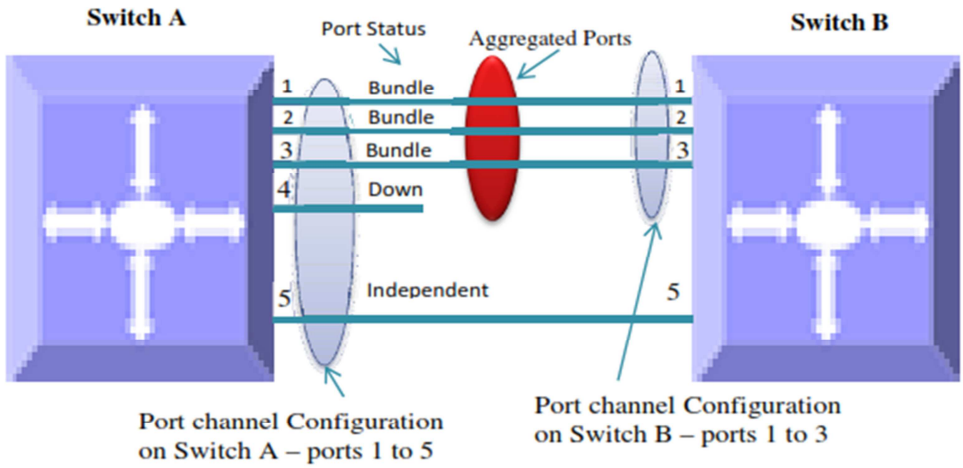


Figure LA-2: Dynamic Link Aggregation shows an example of a port channel configuration with port status and aggregated ports. In this example, port 5 is not configured on LACP mode on switch B, and is therefore shown as being in the “independent” state and not part of the aggregated ports.

4.6Link Aggregation Port Channel

4.6.1 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.

4.6.1.1 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. *channel-group-number* – 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

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

Step 7	End	Exits the configuration mode.
Step 8	show interface port-channel *<channel-group-number>* show etherchannel [[*channel-group-number*] { detail | load-balance | port | por t-channel | summary | protocol}]	Displays the configured port channel information.
Step 9	write startup-config	Optional step – saves this port channel configuration to be part of startup configuration.

4.6.1.2 Adding Member Ports to Port Channels

Users can add up to eight member ports to static port channels. For LACP port channels, 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	interface **<***interface-type***><***interface-id***>** Or interface range *<interface-type><interface-id>*	Enters the interface mode. *interface-type* – may be any of the

		following: gigabite ethernet-gi extreme-ethernet-ex *interface-id* is in *slot/port* format for allphysical interfaces.To configure multiple interfaces, usethe "interface range …" command. Toprovide a range, use a hyphen (-).between the start and end interfacenumbers. E.g.: int range gi 0/1-10To provide multiple interfaces or ranges, separate with a comma (,).E.g.: int range gi 0/1-10, gi 0/20
Step 3	channel-group <channel-group-number> mode {active | passive | on}	Configures the interfaces as member ports for the given port channel. *channel-group-number* – The port channel to which these member ports are added. For LACP aggregation, use the active or passive mode. For static link aggregation, use mode on.
Step 4	End	Exits the interface configuration mode.
Step 5	show interface port-channel *<channel-group-number>*	Displays the configured port channel information.

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

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

The examples below show various ways to create port channels.

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

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

4.6.2 Modifying Port Channels

4.6.2.1 Modifying Port Channel Parameters

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

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

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

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

```
SMIS# configure terminal
SMIS(config)# interface port-channel 10
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk allowed vlan 100-200
SMIS(config-if)# switchport trunk native vlan 100
SMIS(config-if)# exit
```

4.6.2.2 Modifying Port Channel Member Ports

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

4.6.2.3 Adding New Member Ports

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

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

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

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

4.6.2.4 Removing Member Ports

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

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

	Or interface range <*interface-type*><*interface-id*> ….	*interface-type* – may be any of the following: gigabitethernet – gi extreme-ethernet – ex *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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	no channel-group	Removes the member ports from the port channel.
Step 4	End	Exits the configuration mode.
Step 5	show interface port-channel <*channel-group-number*> show etherchannel [[*channel-group-number*] { detail | load-balance | port | port-channel |	Displays the configured port channel information.

	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 ex 0/3 from port channel interface 10

SMIS# configure terminal
SMIS(config)# int ex 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 configuredwith 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: Gigabitethernet - gi Extreme-ethernet -ex Interface-id is in slot/port format for

		allphysical interfaces. To configure multiple interfaces,use the "interface range..." commnad. To provide a range, use a hyphen(-) between the start and end interface numbers. E.g.: int range gi0/1-10 To provide multiple interfaces or ranges,separate with a comma(,). E.g.: int range gi 0/1-10,gi 0/1-20
Step 3	no channel-group	Removes the member ports from the port channel.
Step 4	channel-group <channel-group-number> mode {active | passive | on}	Configures the interfaces as member ports with the given port mode. For LACP aggregation, use the active or passive mode. For static link aggregation, use the mode on. *channel-group-number* – The port channel to which these member ports are added.
Step 5	End	Exits the interface configuration mode.
Step 6	show interface port-channel <*channel-group-number*> show etherchannel [[*channel-group-number*] { detail | load-balance | port | por t-channel | summary | protocol}]	Displays the configured port channel information.
Step 7	write startup-config	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 ex 0/2 and ex 0/3.

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

4.6.3 Removing Port Channels

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no interface port-channel <*channel-group-number*> Or no interface range port-channel <*channel-group-number*> ….	Removes the port channel interface. *channel-group-number* – may be any number from 1 to 65535. To remove multiple port channel interfaces, use the “no interface range …” command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: no int range po 1-3 To provide multiple interfaces or ranges, separate with a comma (,).

		E.g. : no int range po 1, 2
Step 3	show running-config show etherchannel	Displays the port channel information.
Step 4	write startup-config	Optional step – saves this port channel configuration to be part of startup configuration.

When a port channel is removed, all its member ports will be 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 ex 0/1-2
SMIS(config-if)# switchport mode access
SMIS(config-if)# switchport access vlan 10
SMIS(config-if)# exit
```

4.6.4 LACP Parameters

Users can configure the following LACP parameters on Supermicro switches.

LACP System
Priority LACP
Port Priority
LACP
Timeout

4.6.4.1 LACP System Priority

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

LACP system priority is also used to decide the active member ports of a port channel. When more than eight member ports are configured, the switch that has 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. *system-priority* – may be any value from 0 to 65535
Step 3	Exit	Exits the configuration mode.
Step 4	show running-config	Displays the configured LACP system priority value.
Step 5	write startup-config	Optional step – saves this LACP configuration to be part of startup configuration.

The “no lacp system-priority” command resets the LACP system priority to the default value 32768.

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

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

4.6.4.2 LACP Port Priority

When more than eight member ports are configured, the ports that have the lowest port priority value get selected as active member ports. If multiple ports have the same port priority value, the ports with the numerically lower port numbers will be selected as the active member ports.

The default LACP port priority is 128.

Follow the steps below to modify the LACP port priority.

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. *interface-type* – may be any of the following: gigabitethernet – gi extreme-ethernet – ex *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 gi 0/1-10 To provide multiple interfaces or

		ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	lacp port-priority <*port-priority*>	Configures the LACP port priority. *port-priority* – may be any value from 0 to 65535
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 priority configuration to be part of startup configuration.

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 ex 0/1 and 20 for ex 0/2.

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

SMIS(config-if)# exit

4.6.4.3 LACP Timeout

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

Users can define the LACP timeout value either as “long” or “short”. Every member port can have 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. *interface-type* – may be any of the following: gigabitethernet – gi extreme-ethernet – ex *interface-id* is in *slot/port* format for all physical interfaces.

Step 3	lacp timeout {long | short}	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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 Configures the LACP port timeout. long – LACP messages are expected to be received once every 30 seconds. short – LACP messages are expected to be received once every second.
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 ex 0/1 and ex 0/2.

SMIS# configure terminal

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

SMIS(config-if)# lacp timeout short

SMIS(config-if)# exit

4.6.4.4 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
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: gigabitethernet – gi extreme-ethernet – ex

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 ex 0/1 and ex 0/2.

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

4.6.5 Load Balancing

Supermicro switches support load balancing on aggregated links.

Switches distribute outgoing traffic on all member ports that are in 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 IPaddresses 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.
Step 2	port-channel load-balance {src-mac | dest-mac | src-dest-mac| src-ip | dest-ip | src-dest-ip} [<*channel-group*>]	*channel-group* is the port channel identifier to which this load balancing algorithm is configured. *channel-group* number is an optional parameter for this configuration. When *channel-group* 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 ofstartup 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.

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.

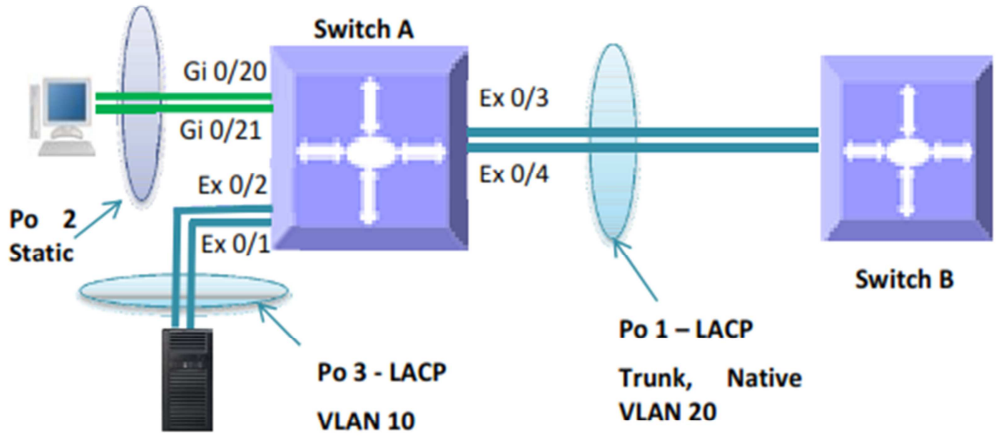
4.6.6 Link Aggregation Configuration Example

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

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

3. Aggregate ports Gi 0/20 and Gi 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 ex 0/3-4
SMIS(config-if)# channel-group 1 mode active
SMIS(config-if)# exit

Configure the VLAN requirements for the port channel 1 interface
SMIS(config)# int port-channel 1
SMIS(config-if)# switchport mode trunk
SMIS(config-if)# switchport trunk native vlan 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 gi 0/20-21
SMIS(config-if)# channel-group 2 mode on
SMIS(config-if)# exit

Create the port channel 3 interface
SMIS(config)# int port-channel 3

SMIS(config-if)# exit

Add member ports to the port channel 3 interface
SMIS(config)# int range ex 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...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

ip address dhcp interface port-channel 1 exit
interface port-channel 2 exit
interface port-channel 3 exit
vlan 1

ports gi 0/1-19 untagged ports gi 0/22-48 untagged ports po 2 untagged
exit vlan 10
ports po 3 untagged exit
vlan 20
ports po 1 untagged
exit

interface Gi 0/20 channel-group 2 mode on
interface Gi 0/21 channel-group 2 mode on
interface Ex 0/1 channel-group 3 mode active
interface Ex 0/2 channel-group 3 mode active
interface Ex 0/3 channel-group 1 mode active
interface Ex 0/4 channel-group 1 mode active
interface po 1
switchport trunk native vlan 20 switchport mode trunk
interface po 3 switchport access vlan 10 switchport mode access
exit

SMIS#
Check the port channels using the “show etherchannel” command SMIS# show etherchannel detail
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is 00:30:48:a1:11:01
LACP System Priority: 32768

```
Channel Group Listing
---------------------

Group: 1
Protocol: LACP
Ports in the Group
------------------
Port: Ex0/3
-------------
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: Ex0/4
-------------
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
---------------------------------------------------------------------------

Ex0/3  Down   128     1      1     0x33    0x45
Ex0/4  Down   128     1      1     0x34    0x45
Port-channel: Po1
-------------------
Number of Ports = 2 HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse Protocol = LACP
Default Port = None
Channel Group Listing
---------------------
Group: 2
----------
Protocol: Manual
Ports in the Group
------------------
Port: Gi0/20
```

```
-------------
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: Gi0/21
-------------
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
------------------------------------------------------------------------------
Gi0/20 Down   128     2      2     0x14    0x44
Gi0/21 Down   128     2      2     0x15    0x44
Port-channel: Po2
------------------
Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = Manual
Default Port = None
Channel Group Listing
---------------------
Group: 3
----------
Protocol: LACP
Ports in the Group
------------------
Port: Ex0/1
-------------
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: Ex0/2

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
---
Ex0/1 Down 128 3 3 0x31 0x45
Ex0/2 Down 128 3 3 0x32 0x45
Port-channel: Po3

Number of Ports = 2
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
Default Port = None
SMIS#
Save this port channel configuration. SMIS# write startup-config
Building configuration, please wait. May take a few minutes . . .
[OK]
SMIS#

5 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	•Port to reach the root switch with lowest path cost •Root ports forwards the traffic
Designated Port	•Loop free connection to the other switch on the LAN • Designated ports forwards the traffic
Alternate Port	• Redundant path to the root switch •Alternate ports do not forward the traffic
Blocked Port	•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:

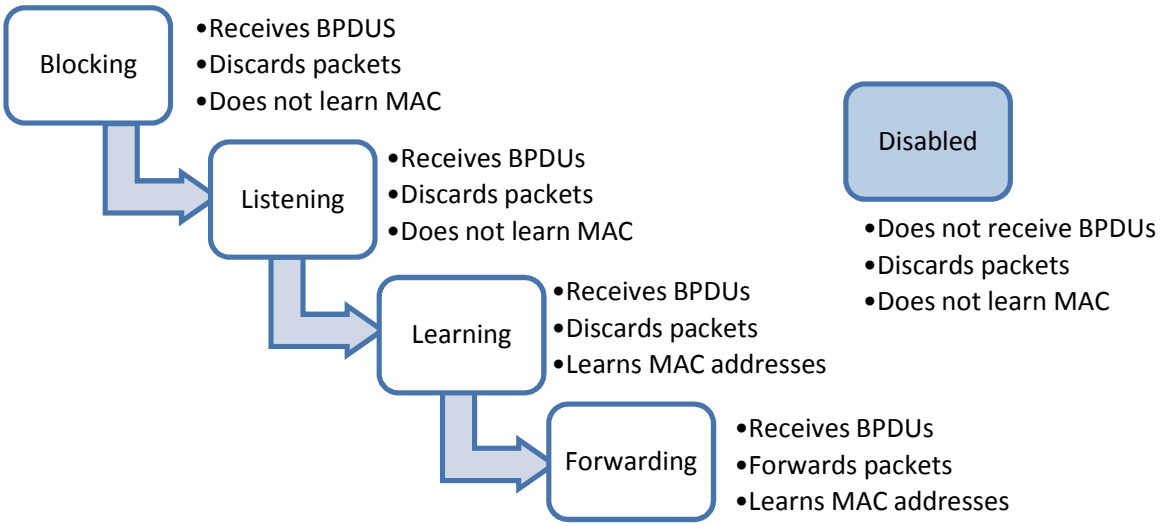
Bridge Identifier: Combination of switch MAC address and switch spanning tree priority

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.

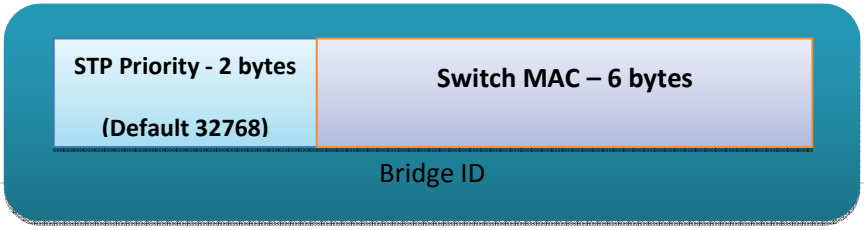
Raping spanning tree protocol (RSTP) provides faster topology convergence. Spanning tree (STP) takes more than 30 seconds to move a port to forwarding state. But RSTP can move a port to the forwarding state within 3 times of hello interval (default hello interval is 2 seconds). RSTP is compatible with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

5.1Root 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 BDPUs 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.

5.2Spanning Tree Support

Supermicro switches support STP, RSTP and MSTP protocols based on standards IEEE 802.1D 2004 and 802.1s.

5.3Spanning TreeDefaults

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

	Half duplex ports – shared LAN links

5.4Enabling/ Disabling Spanning Tree

5.4.1 Enable / Disable Spanning Tree Globally

Spanning tree is enabled by default in Supermicro switches globally.

Follow the steps below to disablethe spanning tree globally.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no spanning-tree	Disablesthe 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

5.4.2 Enable / Disable Spanning Tree on Ports

Spanning tree is enabled by default on all the ports and port channels in Supermicro switches.

Follow the steps below to disablethe 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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 variousways to disable / enable the spanning tree on ports.

Disable the spanning tree on ports ex 0/1 and ex 0/2.

SMIS# configure terminal

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

SMIS(config-if)# spanning-tree disable

SMIS(config)# end

Enable the spanning tree on port ex 0/1.

SMIS# configure terminal

SMIS(config)# interface ex 0/1

SMIS(config-if)# **no**spanning-tree disable

SMIS(config)# end

5.5Configuring 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.

5.6Configuring 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 MSTconfiguration 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

5.7 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
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.

5.8Spanning 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

5.9Configuring Root Switch (or) Priority

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

When priorities of all switches are same, switch with lowest MAC address gets elected as the root switch.

Follow the steps below to change spanning tree priority.

<table>
<tr><th>Step</th><th>Command</th><th>Description</th></tr>
<tr><td>Step 1</td><td>configure terminal</td><td>Enters the configuration mode</td></tr>
<tr><td>Step 2</td><td>To configure the switch priority in RST mode:
spanning-tree priority <priority-value>

To configure the switch priority for the default MST instance 0:
spanning-tree priority <priority-value>

To configure the switch priority for particular MST instance:
spanning-tree mst <instance-id> priority <priority-value></td><td>Configures the switch spanning tree priority.
priority-value – Spanning tree switch priority value in multiples of 4096 from 0 to 61440. In other words only the following priority values are valid.

<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>
The default priority value is 32768.</td></tr>
</table>

		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 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 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

5.10 Port Priority

When spanning tree detects multiple paths to root switch in loop condition, it selects the port with lowest path cost as the forwarding port. In case of multiple ports having the same path cost to the root switch, spanning tree selects the port with lowest numeric port priority value as the forwarding port.

When priorities of all the portsare same, the port with lowest port identifier gets selected as the forwarding port.

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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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.
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 ex 0/1 and ex 0/2.

SMIS# configure terminal

SMIS(config)# interface range ex 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 gi 0/1

SMIS# configure terminal

SMIS(config)# interface gi 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 ex 0/1

SMIS# configure terminal

SMIS(config)# interface ex 0/1

SMIS(config-if)# spanning-tree mst 10 port-priority 64

SMIS(config-if)# end

5.11 Path Cost

When spanning tree detects multiple paths to root switch in loop condition, it selects the port with lowest path cost as the forwarding port. In case of multiple ports having the same path cost to the root switch, spanning tree selects the port with lowest numeric port priority value as the forwarding port.

The default path cost for the ports are calculated based on the port speed. The table below shows the default path costs for different speed.

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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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.
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 ex 0/1 and ex 0/2.

SMIS# configure terminal

SMIS(config)# interface range ex 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 gi 0/1

SMIS# configure terminal

SMIS(config)# interface gi 0/1

SMIS(config-if)# spanning-tree cost200

SMIS(config-if)# end

Configure the spanning tree port priority as 20 for the MST instance 10 on the port ex 0/1

SMIS# configure terminal

SMIS(config)# interface ex 0/1

SMIS(config-if)# spanning-tree mst 10 cost20

SMIS(config-if)# end

5.12 Hello Time

Root switch sends the BPDU messages on every port periodically for every hello time interval.

The default hello time is 2 seconds.

If switches do not receive BPDU messages for a period of 3 times of hello time interval, spanning tree protocol assumes the root switch is failed.

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

Follow the steps below to change the hello time for RSTP.

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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the "interface range …" command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10

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

"nospanning-tree msthello-time" command resets the spanning tree port hello time to default value, 2 seconds.

The examples below show various ways to configure the spanning tree 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 gi 0/1

SMIS# configure terminal

SMIS(config)# interface gi 0/1

SMIS(config-if)# spanning-tree mst hello-time 1

SMIS(config-if)# end

5.13 Max Age

Switches maintain the BPDU information for every port for a period of max age. If BPDU configuration messages are not received on any ports for max age time, switch will reconfigure those ports.

Max age time affects the failure detection and reconfiguration. Smaller max age time will help to detect the failures quickly. It is advisable to choose the max age time based on the maximum number of switches on the network between any two hosts.

The default max age time is 20 seconds.

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

Follow the steps below to change max age time.

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 showsthe way to configure the spanning tree max age.

Configure the max age as 12.

SMIS# configure terminal

SMIS(config)# spanning-tree max-age12

SMIS(config)# end

5.14 Forwarding Time

Switch waits for a period of forwarding time interval on listening and learning states before going to forwarding state.

The default forwarding time is 15 seconds. Hence switch waits for 15 seconds in listening state and waits for another 15 seconds in learning state before going to forwarding state.

Forwarding time value should maintain the following relation with max age.
2*(Forward Time -1)>=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

5.15 Max Hops

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

The default max hops is 20.

Follow the steps below to change the max hops.

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

5.16 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
Step 2	To configure the path cost method as short	Configures the path cost method.

	spanning-tree pathcost methodshort To configure the path cost method as long spanning-tree pathcost method long	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

5.17 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.

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

5.18 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: gigabitethernet – gi extreme-ethernet – ex port-channel – po

		interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	spanning-tree restricted-role	Enables the root guard feature. The default option is the root guard feature disabled.
Step 4	end	Exits the configuration mode.
Step 5	show spanning-tree detail	Displays the spanning tree root guard information.
Step 6	write startup-config	Optional step – saves this spanning tree configuration to be part of startup configuration.

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

The example below shows the way to enable the root guard feature.

Enable the root guard feature on ports ex 0/1 and ex 0/2

SMIS# configure terminal

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

SMIS(config-if)# spanning-tree restricted-role

SMIS(config-if)# end

5.19 Topology Change Guard

The topology change guard feature helps to prevent unexpected topology changes. Network administrators can configure the topology guard on the ports that are not expected to receive topology change BPDUs.

Topology change BPDUs received on the topology change guard enabled ports will be dropped.

The topology guard feature is disabled on all the ports by default.

Follow the steps below to enable the topology guard feature on the ports.

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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 ex 0/1 and ex 0/2

SMIS# configure terminal

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

SMIS(config-if)# spanning-tree restricted-tcn

SMIS(config-if)# end

5.20 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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-)

		between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 ex 0/1 and ex 0/2.

SMIS# configure terminal

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

SMIS(config-if)# spanning-tree portfast

SMIS(config-if)# end

5.21 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:

		gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20
Step 3	To enable the auto-edge spanning-tree auto-edge To disable the auto-edge no spanning-tree auto-edge	Enables or disabled the auto edge feature. 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 ex 0/1 and ex 0/2

SMIS# configure terminal

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

SMIS(config-if)# no spanning-tree auto-edge

SMIS(config-if)# end

5.22 Link Type

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

The point to point links are assumed to be connected directly to another spanning tree switch. The shared LAN links are assumed to be connected with multiple switches through hubs.

In point to point links spanning tree negotiates with other end 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: gigabitethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 gi 0/1 as point to point link.

SMIS# configure terminal

SMIS(config)# interface gi 0/1

SMIS(config-if)# spanning-tree link-type point-to-point

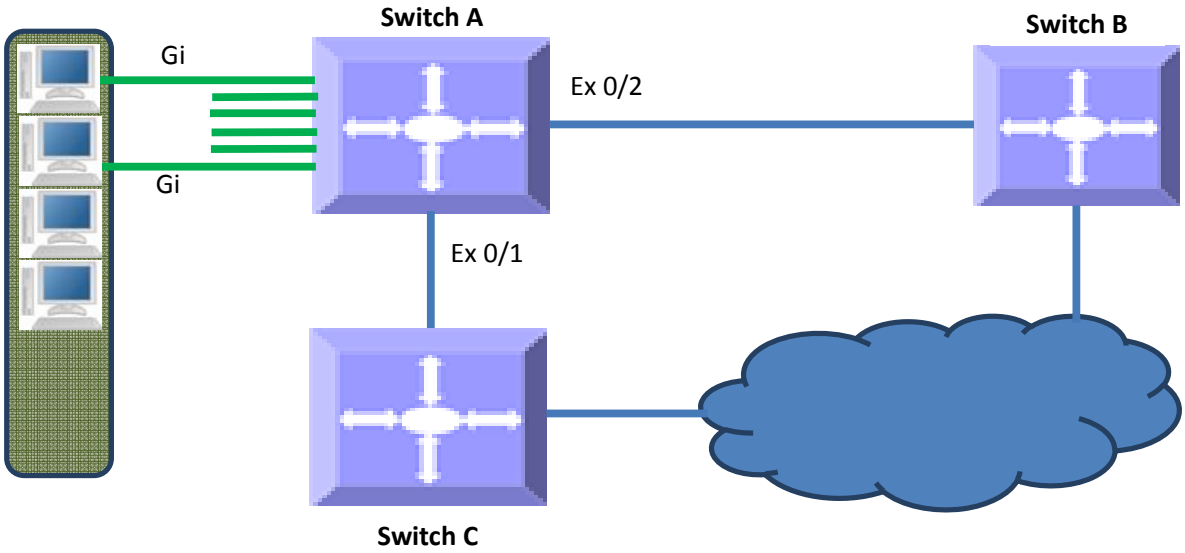
SMIS(config-if)# end

5.23 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 gi 0/1-40 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

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 gi 0/1-40 as port fast

SMIS(config)# interface range gi 0/1-40

SMIS(config-if)# spanning-tree portfast

Warning: portfast should only be enabled on ports connected to a single host.

Connecting hubs, concentrators, switches, bridges, etc... to this interface

when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

SMIS(config-if)#exit

Save thisspanning tree configuration.

SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS#

Configurations on switch B

SMIS# configure terminal

Create the VLANs 100 and 200

SMIS(config)# vlan 100,200

SMIS(config-vlan)# exit

Create MST instance for vlan 100 and 200

SMIS(config)# spanning-tree mst configuration

SMIS(config-mst)# instance 1 vlan 100

SMIS(config-mst)# instance 2 vlan 200

SMIS(config-mst)# exit

Configure the port gi 0/1-40 as port fast

SMIS(config)# interface range gi 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

Gi0/47 of MST01 is Designated, Forwarding

Port info port id 128.47 priority 128 cost 200000

Designated root address 00:30:48:a1:11:01 priority 4096 cost 0

Designated bridge address 00:30:48:a1:11:01 priority 4096 port id 128.47

SMIS#

Save this spanning tree configuration.

SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS#Configurations on switch C

SMIS# configure terminal

Create the VLANs 100 and 200

SMIS(config)# vlan 100,200

SMIS(config-vlan)# exit

Create MST instance for vlan 100 and 200

SMIS(config)# spanning-tree mst configuration

SMIS(config-mst)# instance 1 vlan 100

SMIS(config-mst)# instance 2 vlan 200

SMIS(config-mst)# exit

Configure the port gi 0/1-40 as port fast

SMIS(config)# interface range gi 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

Gi0/47 of MST02 is Designated, Forwarding

Port info port id 128.47 priority 128 cost 200000

Designated root address 00:30:48:e3:56:12 priority 4096 cost 0

Designated bridge address 00:30:48:e3:56:12priority 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#

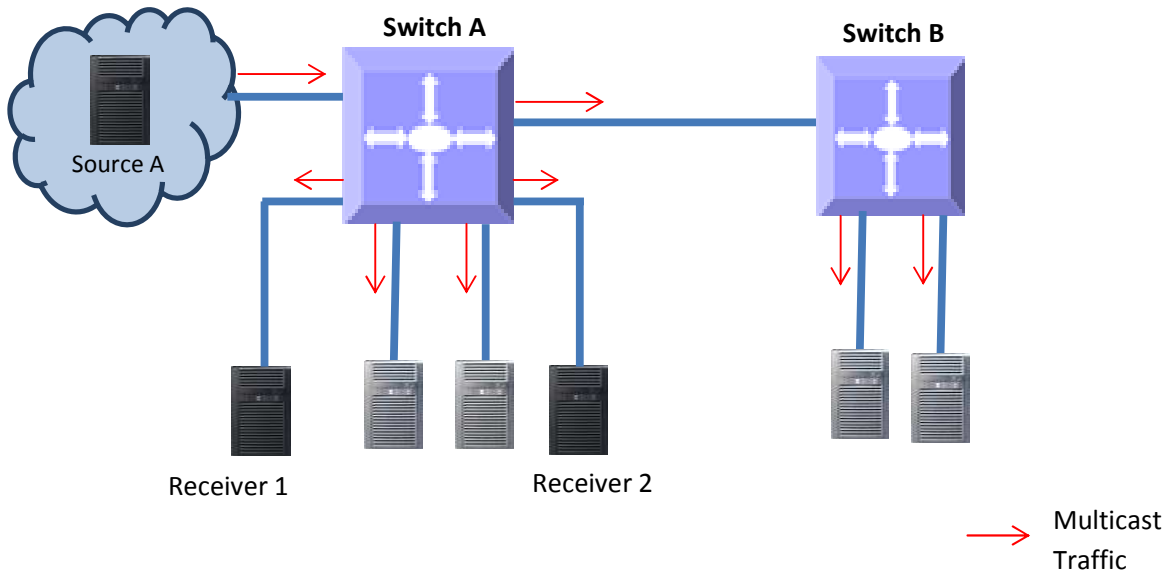
6 IGMP Snooping

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**

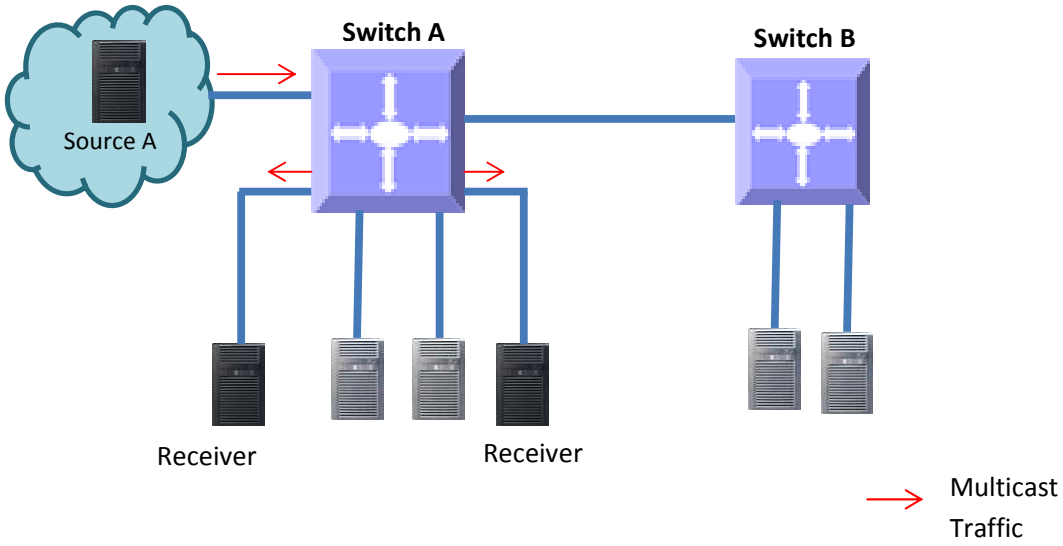


The IGMP snooping function helps the switches to forward IPv4 multicast traffic to only the ports that require IPv4 multicast traffic. This function saves network bandwidth by preventing the unnecessary flooding of IPv4 multicast traffic.

A switch performsthe IGMP snooping function by snooping the Layer 3 IGMP packets andrecognizes 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 snoopingthe IGMP control messages sent by IGMP routers. The switch maintains a multicast forwarding table based on the hosts joined and router connected portsforevery 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**



6.1IGMP 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

6.2Enabling 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 GMRP feature needs to be in the disabled state while enabling IGMP snooping. GMRP is disabled by default in Supermicro switches.
Use the “set gmrp disable” command to disable the GMRP feature if needed.

The example below shows the commands to enable IGMP snooping.

Enable IGMP snooping for VLAN 1, 10 and 20.

SMIS# configure terminal

SMIS(config)# ip igmp snooping

SMIS(config)# vlan 1,10,20

SMIS(config-vlan)# ip igmp snooping

SMIS(config-vlan)# end

6.3IGMP 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 differentversions 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

6.4Multicast Router Ports

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

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

6.4.1 Router Port Timeouts

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

By default, Supermicro switches havea 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 timeoutinformation.
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

6.4.2 Static Router Ports

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

Follow the steps below to configure the static router portfor 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 configurethe 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: gigabitethernet – gi extremeethernet – ex 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 portsfor 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 staticallyconfigured router port from a VLAN.

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

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

SMIS# configure terminal

SMIS(config)# vlan 10

SMIS(config-vlan)# ip igmp snooping mrouter gi 0/1

SMIS(config-vlan)# end

6.5Leaving 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 itsgroup 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.

6.5.1 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 metwithoutaresponse from any of the hosts, the switches will remove the port from the group entry in the multicast forwarding table.

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

Follow the steps below to configure the group query interval.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	ip igmp snooping group-query-interval <timeout>	Configures the group query interval timeout. 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

6.5.2 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.
Step 3	end	Exits the configuration mode.
Step 4	show ip igmp snooping globals	Displays the IGMP snooping group specific query message retry count information.
Step 5	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

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

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

Configure the group specific query message retry count as 3.

SMIS# configure terminal

SMIS(config)# ip igmp snooping retry-count 3

SMIS(config)# end

6.5.3 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

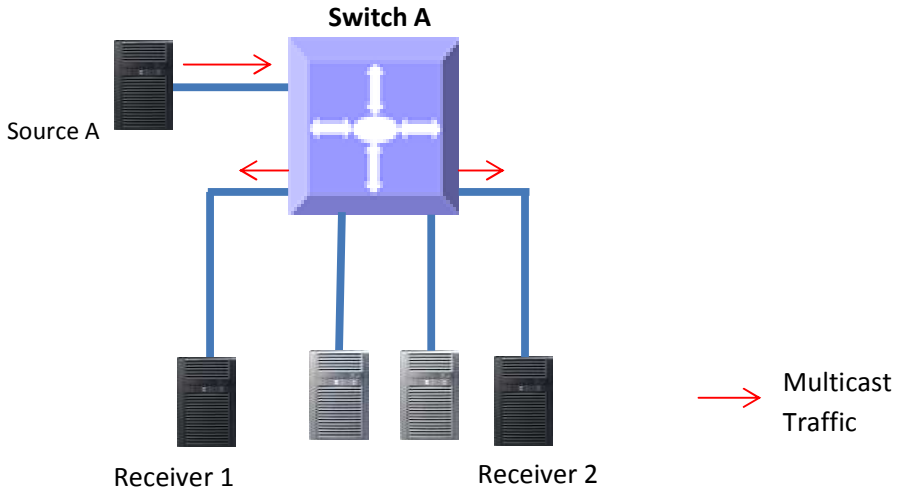
SMIS(config-vlan)# ip igmp snooping fast-leave

SMIS(config-vlan)# end

6.6IGMP Snooping Querier

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

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



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

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

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

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	vlan<**vlan-list**>	Enters the VLAN configuration mode. 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 querierconfiguration for the given VLAN.
Step 7	write startup-config	Optional step – saves this IGMP snooping configuration to be part of the startup configuration.

The “no ip igmp snooping querier” command can be used toremove 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

6.7Report Forward

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

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

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

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

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

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

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

SMIS# configure terminal

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

SMIS(config)# end

6.8Port Timeout (Port Purge Interval)

A switch recognizes a IGMP host's connected ports by snooping the IGMP join messages sent bythe 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 theport 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 stepsbelow.

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

6.9Report 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

6.10 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

6.11 Sending QuerieswhenTopology Changes

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

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

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

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

The “ip igmp snooping send-query disable” command configuresthe 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

6.12 Disabling IGMP Snooping

IGMP snooping is disabled by default in Supermicro switches.

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

Follow the steps below to disable IGMP snooping.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	no ip igmp snooping	Disables IGMP snooping globally.
Step 3	vlan<vlan-list>	Enters the VLAN configuration mode. 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 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

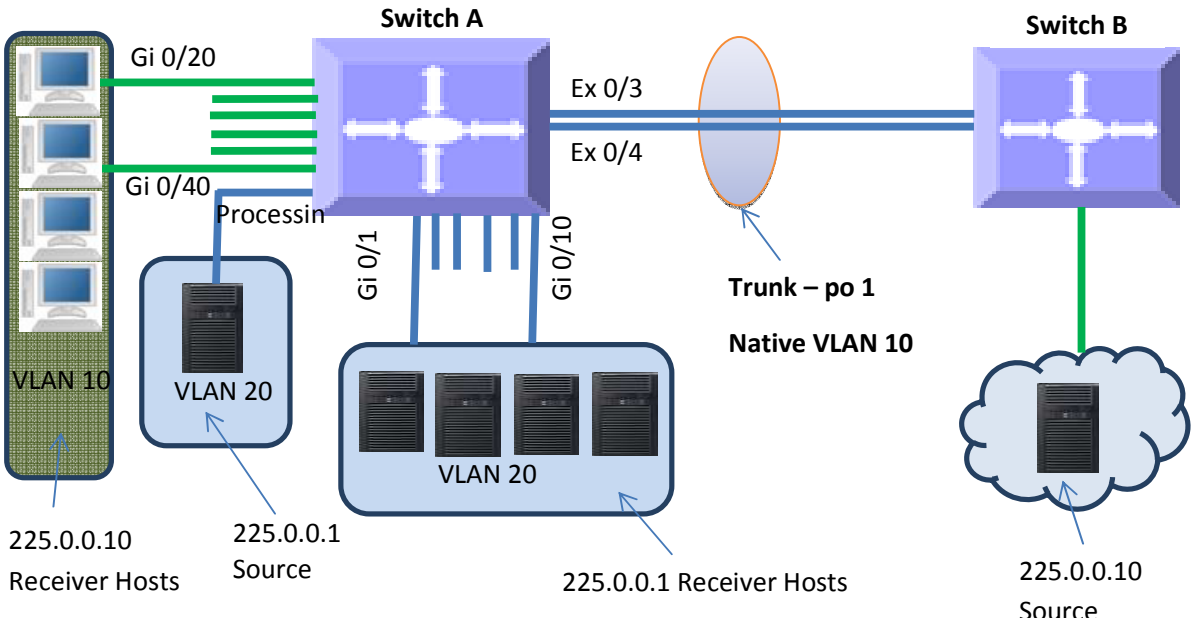
SMIS(config-vlan)# end

6.13 IGMP Snooping Configuration Example

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

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

Figure IGS-4IGMP Snooping Configuration Example



SMIS# configure terminal

Create all the required VLANs first

SMIS(config)# vlan 10,20

SMIS(config-vlan)# exit

Add member ports to VLAN 10

SMIS(config)# int range gi 0/20-40

SMIS(config-if)#switchport mode access

SMIS(config-if)#switchport access vlan 10

SMIS(config-if)# exit

Add member ports to VLAN 20

SMIS(config)# int range ex 0/1 gi 0/1-10

SMIS(config-if)#switchport mode trunk

SMIS(config-if)#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 ex 0/3-4

SMIS(config-if)#channel-group 1 mode active

SMIS(config-if)# exit

Configure the VLAN requirements for the port channel 1 interface

SMIS(config)# int port-channel 1

SMIS(config-if)# switchport mode trunk

SMIS(config-if)# switchport trunk native vlan 10

SMIS(config-if)# exit

Req.1 Enable IGMP Snooping

SMIS(config)# ip igmp snooping

SMIS(config)# vlan 10,20

SMIS(config-vlan)# ip igmp snooping

SMIS(config-vlan)# exit

Req.2 Configure the switch as a querier for group 225.0.0.1

SMIS(config)# vlan 20

SMIS(config-vlan)# ip igmp snooping querier

SMIS(config-vlan)# exit

Req.3 Configure IGMP v2 and fast leave for group 225.0.0.1

SMIS(config)# vlan 20

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

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

SMIS(config-vlan)# exit

Req.4 Disable proxy reporting

SMIS(config)# no ip igmp snooping proxy reporting

Req.5 Enable the switch to send general IGMP queries when spanning tree topology changes

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

Check the running-configuration for accuracy

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

interface port-channel 1

exit

vlan 1

ports gi 0/11-19 untagged

ports gi 0/41-48 untagged

ports ex 0/2 untagged

exit

vlan 10

ports gi 0/20-40 untagged

portspo 1 untagged

exit

vlan 20

exit

interface Gi 0/1

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/2

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/3

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/4

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/5

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/6

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/7

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/8

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/9

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/10

switchport trunk allowed vlan 20

switchport mode trunk

interface Gi 0/20

switchport access vlan 10

switchport mode access

interface Gi 0/21

switchport access vlan 10

switchport mode access

interface Gi 0/22

switchport access vlan 10

switchport mode access

interface Gi 0/23

switchport access vlan 10

switchport mode access

interface Gi 0/24

switchport access vlan 10

switchport mode access

interface Gi 0/25

switchport access vlan 10

switchport mode access

interface Gi 0/26

switchport access vlan 10

switchport mode access

interface Gi 0/27

switchport access vlan 10

switchport mode access

interface Gi 0/28

switchport access vlan 10

switchport mode access

interface Gi 0/29

switchport access vlan 10

switchport mode access

interface Gi 0/30

switchport access vlan 10

switchport mode access

interface Gi 0/31

switchport access vlan 10

switchport mode access

interface Gi 0/32

switchport access vlan 10

switchport mode access

interface Gi 0/33

switchport access vlan 10

switchport mode access

interface Gi 0/34

switchport access vlan 10

switchport mode access

interface Gi 0/35

switchport access vlan 10

switchport mode access

interface Gi 0/36

switchport access vlan 10

switchport mode access

interface Gi 0/37

switchport access vlan 10

switchport mode access

interface Gi 0/38

switchport access vlan 10

switchport mode access

interface Gi 0/39

switchport access vlan 10

switchport mode access

interface Gi 0/40

switchport access vlan 10

switchport mode access

interface Ex 0/1

switchport trunk allowed vlan 20

switchport mode trunk

interface Ex 0/3

channel-group 1 mode active

interface Ex 0/4

channel-group 1 mode active

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

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#

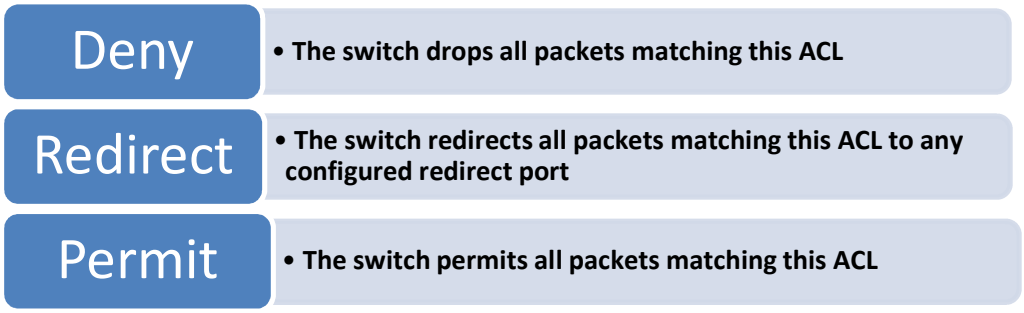
7 ACL

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.



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 droppingthat packet, redirecting itto 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.

7.1Types 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

7.1.1 MAC Extended ACL

A MAC Extended ACLallows 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 orEthernet 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.

7.1.2 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.

7.1.3 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.

7.2MAC Extended ACL

Supermicro switches support up to 128 MAC Extended ACLs.

Users can define a MAC Extended ACL with a deny, permit or redirect action rule. A MAC Extended ACL can be defined only with one rule. To implement multiple rule ACLs, configure multiple MAC Extended ACLs.

There is no implied deny all rule in Supermicro switch ACLs. By default, all packets not matching a configured ACL rule will be forwarded automatically. For any traffic to be denied, it has to be configured with an explicit deny rule.

The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted. In this case, permit rules have to be created before deny rules to make sure switch hardware processes permit rules first.

MAC Extended ACLs allow users to configure the traffic flow with the following fields.

- Source MAC Address
- Destination MAC Address
- Non-IP Protocol
- Ethernet type field in an Ethernet Header
- VLAN Identifier

MAC Extended ACL rules can be created and identified either with an ACL number such as 1,2,3 or with a name string.An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters No special characters are allowed.

User can associate priority values to MAC extended ACL rules. Based on the configured priority, the rules will be orderly arranged in the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules take precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules that created earlier will take precedence over the later ones

If the user does not specify the priority, by default all rules will have same priority value as 1.

7.2.1 CreatingMAC 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	Configuresa 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 anyis 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.

	redirect<interface-type><interface-id> { any | host<src-mac-address>}{ any | host<dest-mac-address> } priority<value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>]	The protocolkeyword can be used to configure the Ethernet header Encap Type field to be matched to apply this ACL rule. This protocolis an optional parameter. If not provided, switch will not check this field while matching packets for this ACL. If this ACL rule is to be applied only to a particular VLAN, user can configure VLAN number using Vlan keyword. This Vlan is an optional parameter. If not provided, switch will not check VLAN while matching packets for this ACL. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. Itcanbe any value from 1 to 255. The default value is 1. Redirect ACL rule needs additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
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 creatinga 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 00:25:90:01:02:03going to MAC 00:25:90:01:02:04 to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# mac access-list extended 1

SMIS(config-ext-macl)# redirect gi 0/10 host 00:25:90:01:02:03 host 00:25:90:01:02:04

7.2.2 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 50that 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

7.2.3 Removing MAC Extended ACLs

Follow the steps below to remove MAC Extended ACLs.

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

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

SMIS# configure terminal

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

7.2.4 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.

7.2.5 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)>**} in	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.
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 gi 0/1 and gi 0/10.

SMIS#configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# mac access-group 100 in

SMIS(config-if)# exit

SMIS(config)# int gi 0/10

SMIS(config-if)# mac access-group 100 in

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)>} in	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 gi, ex ports. They cannot be added to Layer 3 vlan interfaces or port channel interfaces.
3. A MAC Extended ACL can be applied to many ports by following the above steps. In

the same way, many MAC Extended ACLs can be applied to a single port.

The example below shows the commands for removinga MAC Extended ACLfrom a port.

SMIS#configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# no mac access-group 100 in

7.2.6 ACL Egress Port Configuration

User can associate an ACL with only one egress port. Follow the steps below to configure the egress port to an ACL.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id>	The egress port on which this MAC Extended ACL needs to be applied.
Step 3	mac access-group { <short (1-32768)> | <string(32)>} out	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.
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 egress port gi 0/1.

SMIS# configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# mac access-group 100 out

SMIS(config-if)# exit

Removing MAC Extended ACL from egress port

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id>	The egress port from which this MAC Extended ACL needs to be removed.
Step 3	no mac access-group { <short (1-32768)> | <string(32)>} in	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 the egress port it was applied to, that ACL will become a switch-wide ACL (applied to all physical ports).
2. MAC Extended ACLs can be configured with only physical egress ports like gi, ex ports. They cannot be configured with port channel interfaces.

The example below shows the commands for removing a MAC Extended ACL from a port.

SMIS# configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# no mac access-group 100 in

7.2.7 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

Theshow 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

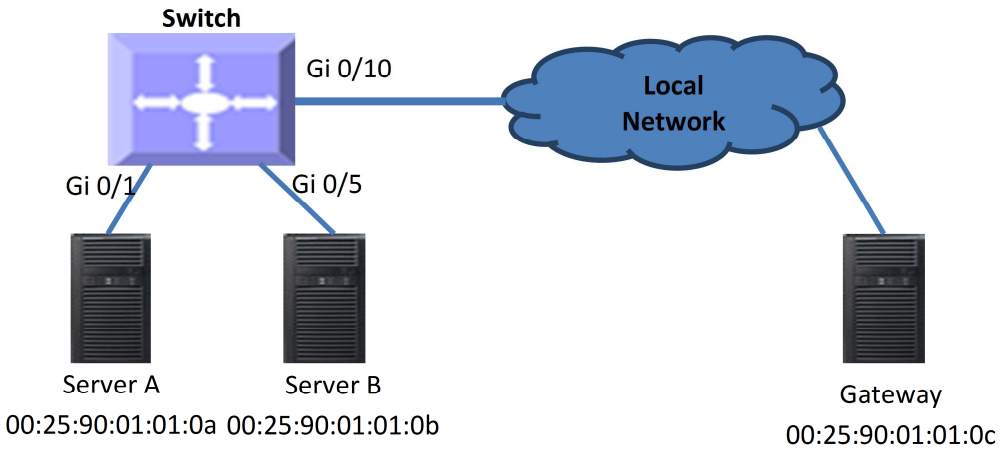
Extended MAC Access List 100

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 : Gi0/2
Out Port : ALLFilter Action : Deny
Status : Active

7.2.8 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 gi 0/5 host 00:25:90:01:01:0c any vlan 20

7.3IP 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 a with an ACL number as such as 1,2 or 3 or with a name string. An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters. No special characters are allowed in ACL name string.

IP Standard ACLs and IP Extended ACLs share the same ACL numbers and names. Hence ACL numbers and names across all IP Standard and IP Extended ACLs have to be unique. In other words, the same ACL number or name cannot be used for both IP Standard ACLs and IP Extended ACLs.

User can associate a priority values to IP standard ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules take precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules that created earlier will take precedence over the later ones.

If the user does not specify the priority, by default all rules will have same priority value as 1.

The priority for IP standard ACL rule “deny any any” is fixed as 1. User cannot configure “deny any any” rule with different priority value. Since this rule will drop all the IP packets, this rule is added at the end of the IP ACL table on the hardware.

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

7.3.1 Creating IP Standard ACLs

Follow the steps below to create anIP 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<ucast_addr> | <ucast_addr><ip_mask> } [{any | host<ip_addr> | <ip_addr><ip_mask> }] [priority<value (1-255)>] or	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.

	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)>]	The keyword anyis 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 definethe port to which the packets matching this ACL rule need to be redirected. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

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

The examples below show different ways to create IP Standard ACLs.

Create a deny IP Standard ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 to IP 172.10.10.1

SMIS# configure terminal

SMIS(config)# ip access-list standard 100

SMIS(config-std-nacl)# deny host 172.10.10.10 host 172.10.10.1

Create a permit IP Standard ACL with ACL name acl_cw3 to permit all traffic from IP 172.10.10.1

SMIS# configure terminal

SMIS(config)# ip access-list standard acl_cw3

SMIS(config-std-nacl)# permit host 172.10.10.1 any

Create a redirect IP Standard ACL to redirect all packets from subnet 172.20.20.Xgoing to IP 172.20.0.1 to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list standard 1

SMIS(config-std-nacl)# redirect gi 0/10 172.20.20.0 255.255.255.0 host 172.20.0.1

7.3.2 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

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

7.3.3 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 StandardACL .

SMIS# configure terminal

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

7.3.4 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.

7.3.5 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> in	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
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 anIP Standard ACL rule 100 to ports gi 0/1 and gi 0/10.

SMIS# configure terminal

SMIS(config)# interface gi 0/1

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

SMIS(config-if)# exit

SMIS(config)# int gi 0/10

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

Removing anIPStandard / 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> }] in	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 gi, ex 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 anIP Extended ACL from a port.

SMIS# configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# no ip access-group 100 in

7.3.6 ACL Egress Port Configuration

User can associate an ACL with only one egress port. Follow the steps below to configure the egress port to an ACL.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id>	Defines the egress port on which this IP

		Standard / Extended ACL needs to be applied
Step 3	ip access-group { <access-list-number (1-32768)> | <access-list-name>out	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
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 anIP Standard ACL rule 100 to egress port gi 0/1.

SMIS# configure terminal

SMIS(config)# interface gi 0/1

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

SMIS(config-if)# exit

Removing anIPStandard / Extended ACL from an egressport

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id>	The egress port from which this IP Standard or Extended ACL needs to be removed
Step 3	no ip access-group[{ <access-list-number (1-32768)> | <access-list-name> }]out	Removes the IP Standard / Extended ACL from this egress 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 the egress port 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 gi, ex ports. ACLs cannot be added to Layer 3 vlan interfaces or port channel interfaces.

The example below shows the commands for removing an IP Standard ACL from a port.

SMIS# configure terminal

SMIS(config)# int gi 0/1

SMIS(config-if)# no ip access-group 100out

7.3.7 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

Theshow command displays the following information for every IP Standard ACL.

Source IP Address	Configured source host or subnet IP address. Displays 0.0.0.0 for any source IP.
Source IP Address Mask	Configured source subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
Destination IP Address	Configured destination host or subnet IP address. Displays 0.0.0.0 for any destination IP.
Destination IP Address Mask	Configured destination subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
In Port List	The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.
Out Port	The egress port configured for this ACL. If no egress port configured, this will be ALL.
Filter Action	Configured ACL action rule – deny,permit or redirect
Status	Current status of the ACL. The status should normally be *active*. In case

of configuration errors, the ACL status may be inactive.

The example below displays an IPStandard ACL

SMIS# show access-lists ip 1

Standard IP Access List 1

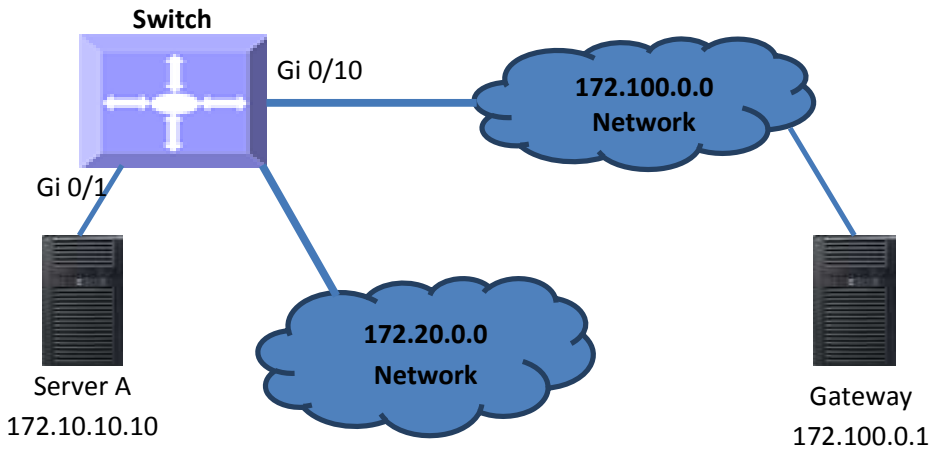
Source IP address : 172.20.20.0
Source IP address mask : 255.255.255.0
Destination IP address : 172.20.0.1
Destination IP address mask : 255.255.255.255
In Port List : ALL
Out Port : ALL
Filter Action : Redirect to Gi0/10
Status : Active

7.3.8 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 gi 0/1 any 172.10.0.0 255.255.0.0

7.3.9 IP Extended ACLs

Supermicro switches support 128 IP ACLs, which includes both IP Standard and IP Extended ACLs.

Users can define IP Extended ACLs with deny, permit or redirect action rules. An IP Extended ACL can be defined only with one rule.

There is no implied deny all rule in Supermicro switch ACLs. By default, all packets not matching a configured ACL rule will be forwarded automatically. For any traffic to be denied, it has to be configured with an explicit deny rule.

The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted. IP Extended ACLs allow users to configure traffic flow with the following fields.

- IP - Protocol, Source IP Address, Destination IP Address, Type Of Service (TOS), DSCP
- TCP – Source Port, Destination Port, TCP message type – acknowledgement / reset
- UDP – Source Port, Destination Port
- ICMP – Message Type, Message Code

IP Extended ACL rules can be created and identified either a with an ACL number such as 1,2 or 3 or with a name string. ACL identifier numberscan be any number from 1 to 65535. ACL identifier namescan 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 associatepriority 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.

7.3.10 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	Configuresa deny, permitor 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 pimas needed. The source and destination IP addresses can be provided with the keyword host. The keyword anymay 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

	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)>]	specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets.Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP values from 0 to 63. The DSCP configuration is optional. The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It may be any value from 1 to 255. The default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to provide the port to which the packets matching this ACL rule should be redirected.
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 an IP Extended ACL for IP traffic.

Create a deny IP Extended ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 with TOS8**.**

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# deny ip host 172.10.10.10 any tos 8

Create a deny IP ExtendedACL with ACL name acl_cw3 to deny all OSPF packets from network 172.20.1.0.

SMIS# configure terminal

SMIS(config)# ip access-list extended acl_cw3

SMIS(config-ext-nacl)# deny ospf 172.20.1.0 255.255.255.0 any

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with DSCP value 10 to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# redirect gi 0/10 ip 172.20.20.0 255.255.255.0 host 172.20.0.1 dscp 10

7.3.11 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> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)>|eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><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> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> |eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-	Configuresa deny, permit or redirect ACL rule. The source and destination IP addresses are provided with the keyword host. The keyword anymay 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, userscan configure either the source or destination TCP ports. The specific TCP port is provided with the keyword eq. A range of ports is provided with the keyword range. Keywords lt or gt can be used to provide port numbers in less than or greater than conditions. To apply this ACL rule to only TCP ACK packets, the keyword ackcan be used.

	65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] [{ ack | rst }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or redirect<interface-type><interface-id>tcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> |eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] [{ ack | rst }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>]	Similarly, to apply this ACL rule to only TCP RST packets, the keyword rst could be used. To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and specific DSCP values to be matched. Users can specific any DSCP values from 0 to 63. This DSCP configuration is optional. The priority keyword lets users assign a priority to this ACL rule. This priority is an optional parameter. It could be any value from 1 to 255. The default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
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 toTCP port 23.

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# deny tcp any anyeq 23

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

SMIS# configure terminal

SMIS(config)# ip access-list extended acl_cw3

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

Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with TCP ports greater than 1000to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 500

SMIS(config-ext-nacl)# redirect gi 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 gt 1000

7.3.12 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> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><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> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)>	Configuresa deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with keyword host. The keyword anycan 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, userscan configure either the source or destination UDP ports. The specific UDP port is provided with the keyword eq. A range of ports can be provided with the keyword range. Keywords lt or gt can be used to

	|eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or redirect<interface-type><interface-id>tcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> |eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{gt<port-number (0-65535)> | lt<port-number (1-65535)> | eq<port-number (0-65535)> | range<port-number (0-65535)><port-number (0-65535)>}] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>]	provide port numbers in less than or greater than conditions. To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP value from 0 to 63. This DSCP configuration is optional. The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1. A Redirect ACL rule needs additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
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 toUDP 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

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 172.20.0.1with destination UDP ports greater than 1000 to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 500

SMIS(config-ext-nacl)# redirect gi 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 gt 1000

7.3.13 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 theip-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	denyicmp {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 permiticmp {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)>]	Configure a deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with keyword host. The keyword anycan 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, usersshould 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

	[<message-code (0-255)>] [priority<(1-255)>]	default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to definethe port to 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 ICMPpackets.

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 172.20.0.1with ICMP message type “Destination Unreachable”to interface gi 0/10.

SMIS# configure terminal

SMIS(config)# ip access-list extended 500

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

7.3.14 Modifying IP Extended ACLs

To modify a configured IP Extended ACL, follow the same steps used to create an IP Extended ACL. When users modify an ACL with a deny, permit or redirect rule, the previously configured rule and its parameters for that ACL will be completely overwritten with the newly provided rules and parameters.

When an ACL rule is modified, it is removed from the hardware ACL table and added back based on the priority of the rule.

The example below shows an IP Extended ACL rule 100 being created and then modified with different parameters.

SMIS# configure terminal

SMIS(config)# ip access-list extended 50

SMIS(config-ext-nacl)# 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

7.3.15 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)r> | <access-list-name> }	Deletes an IP Extended ACL using theip-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

7.3.16 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.

7.3.17 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

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	
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 examplesbelow 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 Gi0/1
 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
```

7.4IP Extended ACL Configuration Example 1

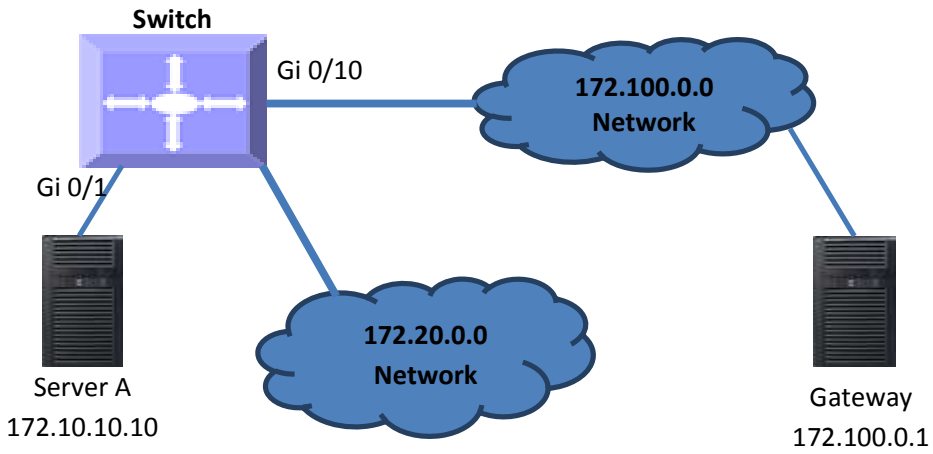
This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-3.

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

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

ACL 3 –Deny all UDP traffic going to 172.100.0.0 with a destination UDP port greater than 1000.

Figure ACL-3: IP Extended ACL Example 1



ACL 1 Configuration

This ACL has two rules: one to allow traffic from 172.20.20.1 and the other is to deny all traffic from the 172.20.0.0 network.

Create the permit rule first.

SMIS# configure terminal

SMIS(config)# ip access-list extended acl_1a

SMIS(config-ext-nacl)# permit tcp 172.20.0.0 255.255.0.0 any eq 25

Then create the deny rule for the subnet 172.20.0.0.

SMIS# configure terminal

SMIS(config)# ip access-list extended acl_1b

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

ACL 2 Configuration

SMIS# configure terminal

SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# redirect gi 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 gt 1000

8 QoS

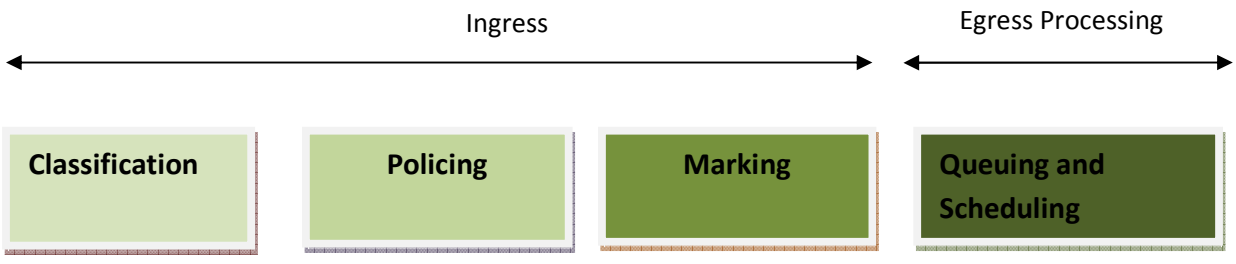
Typically, networks operate on a best-effort delivery basis providing all traffic equal priorityand an equal chance of being delivered in a timely manner. However, during congestion, all traffic has anequal chance of being dropped.The QoS featureallows one to select specific network traffic and prioritize it according toits relative importancetoprovide preferential treatment. Implementing QoS makes network performance morepredictable and bandwidth utilization more effective.

The QoS implementation in Supermicro switches is based on the Differentiated Services (DiffServ)architecture. DiffServarchitecture specifies that each packetis 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 theLayer 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 sameforwarding treatment is provided to packets with the same class information and different treatment to packets withdifferent class information. The class information in the packet can be assigned by end hosts or byother switches or routers based on a configured policy, detailed examination of the packet, orboth.

Switches and routers use the class information to limit the amount of resourcesallocated per traffic class. The behavior of a switch/router when handling traffic in the DiffServarchitecture is called *per-hop behavior*. All devices along anetwork path must provide a consistent per-hop behavior in an end-to-end QoS solution.



Classifies data based on ACL	Forwards or drops data based on policy	Modifies DSCP and/or CoS values	Egress queue handling for data, based on CoS

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.

Policing determines whether a packet is in or out of profile according to the configured policer. The policeralso 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 placethe 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 classqueue mapping:

Priority	Traffic Class queue
0	0
1	1

2	2
3	3
4	4
5	5
6	6
7	7

8.1Policy-Based QoS

Supermicro switch features based on QoS Policies are:

- QoS Classification
- Marking
- Policing

8.1.1 Classification and Marking

Classification is the process of distinguishing one kind of traffic from another by examining the fieldsin 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 isglobally disabledby 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 sentfor 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.

8.1.1.1 ClassMap and PolicyMap

IP standard, IP extended, and Layer 2 MAC access control lists (ACLs) can be used to define a group ofpackets 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.

Afteran 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 doneusinga policymap.A policy map specifies the actions to perform for the traffic class of a class-map. Actions can include setting a specific DSCP value or the action to take when the traffic is out of profile.

An ACL must be created for each policy and class-map,If more thanone 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.

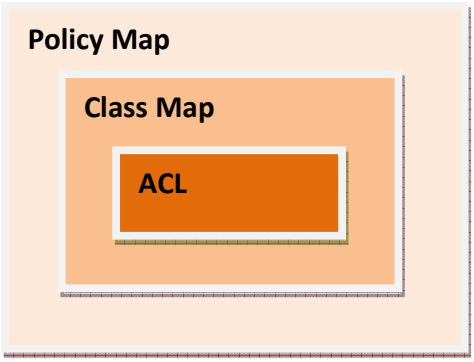


Figure QoS-2: Relationship: ACL, Policy Map & Class Map

8.1.1.2 Policing

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Each policer specifies the action to take for packets thatare in or out of profile. Packets that exceedthe limits are out of profile and various actions are carried out by the marker on out of profile packets, which may includedropping the packet or markingdown the packet with a new user-defined value.

8.2 CoS-Based QoS

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

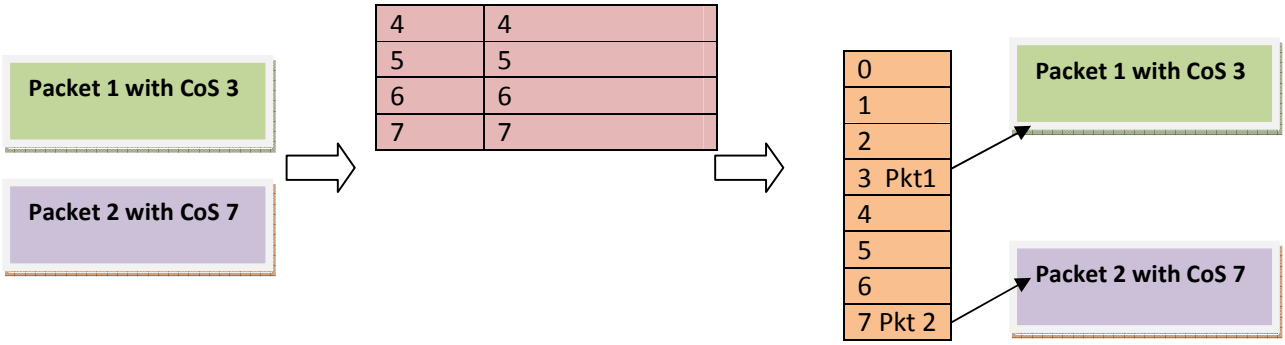
- Queuing
- Scheduling
- Bandwidth Management
- Default Priority

8.2.1 Egress Queuing

The CoS priority of a packet is mapped to a traffic class.Supermicro switchesprovide 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.

CoS	Traffic Class
0	0
1	1
2	2
3	3



Ingress Packets **CoS-to-Traffic-class mappingEgress QueueEgress Packets**

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 queuemapping for the particular destination port is lookedup. 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.

8.2.2 Scheduling

Supermicro switches support eight CoS queues for each egress port. For each of the eightqueues, various typesof scheduling can be configured:

Strict Priority

Strict priority scheduling is based on the priority of queues. Packets in ahigh-priority queue arealways sent first and packets in alow-priority queue are not sent until all the high-priority queuesareempty.

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 havethe same priority and weight in an RR configuration.

Weighted RoundRobin (WRR)

In WRR scheduling, theuser specifies a number to indicate the importance (weight) of thequeue relative to the other CoS queues. WRR scheduling prevents low-priority queues frombeing completely neglected during periods of high-priority traffic. The WRR scheduler sends somepackets from each queue in turn. The number of packets it sends corresponds to the relativeimportance of the queue. By using WRR,low-priority queues can send packets even when high-priority queues are not empty.

DeficitWRR

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.

8.2.3 Default Priority

The Class of Service (CoS) priority field is taken from the VLAN header of a received packet. If the received packet does not have a VLAN header, the default port priority is used as the CoS value. Supermicro switches provide an option to configure the default priority.

Figure QoS-4: VLAN Tag and CoS Priority

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.

8.2.4 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.

8.3 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.

8.4HOLBlocking 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 queuesbecome 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-subscriptionis called Head of Line (HOL) blocking.

Supermicro switches provide support to prevent HOL blocking. When HOL blocking prevention is enabled in the switch, itdropspackets newly arriving on the ingress if they aredestined 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.

8.5Enabling QoS

QoS is disabled by default in Supermicro switches. Follow the below steps to enable QoS.

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...
Switch ID     Hardware Version          Firmware Version
0             MBM-GEM-004                    1.0.0

vlan 1
portsgi 0/1-24 untagged
ports ex 0/1-3 untagged
exit

setqos enable
```

8.6ConfiguringPolicy-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
Step2	Create MAC Extended or IP Standard or IP Extended ACL. If required, apply ACL to specific Interface(s).	Refer to the ACL Configuration Guide atwww.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. *class-map-number* - QoS class map number in range from 1-65535.
Step 4	match access-group { mac-access-list | ip-access-list } { <acl-index-num (1-65535) > | <acl-name> }	This command specifies the fields in the incoming packets that are to be examined toclassify the packets. The IP access group / MAC access group can be used as matchcriteria. mac-access-list - Accesses list created based on MAC addresses for non-IP traffic ip-access-list - Accesses list created based on IP addresses. The IP-access list can either bedefined as a standard IP-access list or an extended IP-access list. acl-index-num - Specifies the ACL index range. The ACL index range for an IP standard ACLis 1 to 1000 and 1001 to 65535for an IP extended ACL. The ACL index range for a MAC extendedACL is 1 to 65535. ACL-name – Specifies the configured ACL name as a string not exceeding 32 characters
Step 5	Exit	Exits theclassmap configuration mode.
Step 6	policy-map <policy-map-number(1-65535)>	Creates a policy map and enters the policy-map configuration mode. policy-map-number - QoS policy map number
Step 7	class <class-map-number(1-65535)>	This command defines a traffic classification for the policy to act upon. The class-map-number that isspecified in the policy map ties the characteristics for that class to the class map and its matchcriteria as configured with the class-map global configuration command. Uponexecution of theclass command, the switch enters the policy-map class configuration mode.

		class-map-number – The class map number to associate the policy, in range of 1-65535
Step 8	set {cos<new-cos(0-7)> | ipdscp<new-dscp(0-63)> | ip precedence <new-precedence(0-7)>}	(Optional) Configures the in-profile action by setting a class of service (CoS), differentiatedservices code point (DSCP), or IP-precedence value in the packet. *cos* - New COS value assigned to the classified traffic, in range of 0-7 *ipdscp* - New DSCP value assigned to the classified traffic, in range of 0-63 *ip precedence* - New IP-precedence value assigned to the classified traffic, in range of 0-7
Step 9	police <rate-Kbps(64-1048572)> exceed-action {drop | policed-dscp-transmit <new-dscp(0-63)>}	(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 whenthe specified rate is exceeded. drop - drops the packet policed-dscp-transmit - changes the differentiated services code point (DSCP) ofthe packet to that specified in the policed-DSCP map and then sends the packet. The DSCP range is 0-63.
Step 10	End	Exits theconfiguration mode.
Step 11	show class-map [<class-map-num(1-65535)>] show policy-map [<policy-map-num(1-65535)> [class <class-map-num(1-65535)>]	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

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:c8:29to 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 Gi 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 Gi 0/3

SMIS(config-if)# mac access-group mac2 in

SMIS(config-if)# exit

SMIS(config)# class-map 10

SMIS(config-cmap)# match access-group mac-access-list mac2

SMIS(config-cmap)# exit

SMIS(config)# policy-map 10

SMIS(config-pmap)# class 10

Existing policymap configurations have been deleted. Please apply the policymap to make it active.

SMIS(config-pmap-c)# set cos 7

SMIS(config-pmap-c)# end

SMIS# show policy-map

DiffServ Configurations:

Quality of Service has been enabled

Policy Map 5 is active

Class Map: 5

In Profile Entry

In profile action : policed-cos6

Policy Map 10 is active

Class Map: 10

In Profile Entry

In profile action : policed-cos7

SMIS# show class-map

DiffServ Configurations:

Class map 5

Filter ID : mac1

Filter Type : MAC-FILTER

DiffServ Configurations:

Class map 10

Filter ID : mac2

Filter Type : MAC-FILTER

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

vlan 1

portsgi 0/1-24 untagged

ports ex 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

interfaceGi 0/3

mac access-group mac1 in

mac access-group mac2 in

exit

setqos enable

class-map 5

match access-group mac-access-list mac1

exit

class-map 10

match access-group mac-access-list mac2

exit

policy-map 5

class 5

setcos 6

exit

exit

policy-map 10

class 10

setcos 7

exit

exit

Example 2: Policing

Create a policy map for the switch without attaching it to an ingress interface. In the configuration, the IP standard ACL permits traffic from network 20.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. If the matched traffic exceeds an average traffic rate of 4800 bps, its DSCP is marked down to a value of 10 and transmitted.

SMIS# configure terminal

SMIS(config)# ip access-list standard 1

SMIS(config-std-nacl)# permit 20.1.0.0 255.255.0.0 any

SMIS(config-std-nacl)# exit

SMIS(config)# set qos enable

SMIS(config)# class-map 1

SMIS(config-cmap)# match access-group ip-access-list 1

SMIS(config-cmap)# exit

SMIS(config)# policy-map 1

SMIS(config-pmap)# class 1

Existing policymap configurations have been deleted. Please apply the policymap to make it active.

SMIS(config-pmap-c)# police 500000 exceed-action policed-dscp-transmit 10

SMIS(config-pmap-c)# end

SMIS# show policy-map

DiffServ Configurations:

Quality of Service has been enabled

Policy Map 1 is active

Class Map: 1

Out Profile Entry

Metering on

burst bytes/token size : 6

Refresh count : 500000

Out profile action : policed-dscp 10

SMIS# show class-map

DiffServ Configurations:

Class map 1

Filter ID : 1

Filter Type : IP-FILTER

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

vlan 1

portsgi 0/1-24 untagged

ports ex 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

8.7Configuring CoS-Based QoS

Follow the steps below to configure CoS-Based features such as default priority, scheduling and bandwidth.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	vlan map-priority <priority value(0-7)> traffic-class <Traffic class value(0-7)>	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. Priority- Priority of the packet, in range of 0-7. Class –Traffic class in range of 0-7.
Step 3	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: gigabit-ethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
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 }	(Optional) Configures the QoS Egress queue scheduling algorithm. strict - strict rr - round robin wrr - weighted round robin (WRR)

		deficit – deficit WRR
Step 6	traffic-class <integer(0-7)> weight <integer(0-15)> [minbandwidth<integer(64-16777152)>] [maxbandwidth<integer(64-16777152)>]	(Optional) Configures the egress queue minimum and maximum bandwidth. weight - Configures the queue weights in range of 0-15 minbandwidth - Configures the minimum bandwidth for the queue in range of 64-16777152 maxbandwidth - Configures the maximum bandwidth for the queue in range of 64-16777152
Step 7	End	Exits the configuration mode.
Step 8	show vlan port config port [<interface-type><interface-id>] show vlan traffic-classes	Displays the port default priority configuration. Display the traffic class and egress queue mapping.

The “no cosq scheduling algorithm” resets the CoS queue scheduling algorithm configuration to its default value of*strict*.
The “no traffic-class [<integer(0-7)>] [weight] [minbandwidth] [maxbandwidth]” command resets the minimum/maximum bandwidth configuration to its default valueof 0 and weight to 1.
The “no switchport priority default” command resets the default priority configuration to its default valueof 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 Gi 0/10

SMIS(config-if)# switchport priority default 5

SMIS(config-if)# end

SMIS# show vlan port config port Gi 0/10

Vlan Port configuration table

Port Gi0/10

Port Vlan ID : 1

Port Access Vlan ID : 1

Port Acceptable Frame Type : Admit All

Port Ingress Filtering : Disabled

Port Mode : Hybrid

Port Gvrp Status : Disabled

Port Gmrp Status : Disabled

Port Gvrp Failed Registrations : 0

Gvrp last pdu origin : 00:00:00:00:00:00

Port Restricted Vlan Registration : Disabled

Port Restricted Group Registration : Disabled

Mac Based Support : Disabled

Port-and-Protocol Based Support : Enabled

Default Priority : 5

Filtering Utility Criteria : Default

Allowed Vlans on Trunk : 1-4069

Trunk Native Vlan Id : 0

Example 2: Scheduling

The example below shows the commands used to configure the QoS scheduling algorithm.

SMIS# configure terminal

SMIS(config)# set qos enable

SMIS(config)# interface Gi 0/8

SMIS(config-if)# cosq scheduling algorithm wrr

SMIS(config-if)# end

SMIS# show cosq algorithm

CoSq Algorithm

Interface Algorithm

--- ---

Gi0/1 StrictPriority

Gi0/2 StrictPriority

Gi0/3 StrictPriority

Gi0/4 StrictPriority

Gi0/5 StrictPriority

Gi0/6 StrictPriority

Gi0/7 StrictPriority

Gi0/8 WeightedRoundRobin

Gi0/9 StrictPriority

Gi0/10 StrictPriority

Gi0/11 StrictPriority

Gi0/12 StrictPriority

Gi0/13 StrictPriority

Gi0/14 StrictPriority

Gi0/15 StrictPriority

Gi0/16 StrictPriority

Gi0/17 StrictPriority

Gi0/18 StrictPriority

Gi0/19 StrictPriority

Gi0/20 StrictPriority

Gi0/21 StrictPriority

Gi0/22 StrictPriority

Gi0/23 StrictPriority

Gi0/24 StrictPriority

Ex0/1 StrictPriority

Ex0/2 StrictPriority

Ex0/3 StrictPriority

Ex0/3 StrictPriority

Example 3: Egress Bandwidth

SMIS# configure terminal

SMIS(config)# set qos enable

SMIS(config)# interface Gi 0/15

SMIS(config-if)# traffic-class 6 weight 7 minbandwidth 6400 maxbandwidth 6400000

SMIS(config-if)# end

SMIS# show cosq weights-bw interface Gi 0/15

CoSq Weights and Bandwidths

Interface CoSqIdCoSqWeightMinBwMaxBw

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

Gi0/15 0 1 0 0

Gi0/15 1 1 0 0

Gi0/15 2 1 0 0

Gi0/15 3 1 0 0

Gi0/15 4 1 0 0

Gi0/15 5 1 0 0

Gi0/15 6 7 6400 6400000

Gi0/15 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

Priority	Traffic Class Queue
0	0
1	1
2	7
3	3
4	4
5	5

9 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.

9.1 Port Mirroring Defaults

Parameter	Default Value
Port mirroring	Disabled
Port mirroring direction	Both

9.2 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>**	Configure Port Mirroring. *session_number* – 1, indicates only one session is supported. *Destination* – Monitoring Port. *interface-type* –may be any of the following: gigabitethernet – gi extreme-ethernet – ex *interface-id* –is in *slot/port* format for all physical interfaces. NOTE: Source and Destination port cannot be same.
Step 3	**Monitor session <session number: 1-4>source interface <interface-type> <interface-id> {rx } tx | both}**	Configure Port Mirroring. *session_number* – 1, indicates only one session is supported.

		Source – Monitored Port. *interface-type* –may be any of the following: gigabitethernet – gi extreme-ethernet – ex *interface-id –i*s in *slot/port* format for all physical interfaces. *rx* – Packets received on source port are monitored (Ingress). *tx* – Packets transmitted on source port are monitored (Egress). *both* – Packets received and transmitted on source port are monitored. NOTE: Source and Destination port cannot be same.
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 gi 0/1, ex 0/1, ex 0/23 …

The second command will establish the other half of the mirroring action, in which the session, if it is the same as the session of the previous destination port command, will mirror traffic from the source port <interface-id>, with direction of ingress (Rx), egress (Tx) or both. If direction is not given, then both is the default direction.

In CLI, user can only add one source port at a time to any session.

In the same session, user's new command for direction of same port, will overwrite the previous configuration of the same source port.

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

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

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

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

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

SMIS# configure terminal
SMIS(config)# **monitor session destination interface gigabitethernet 0/48**
SMIS(config)# **monitor session source interface gigabitethernet 0/22**
SMIS(config)# **monitor session source interface gigabitethernet 0/23**
SMIS(config)# **monitor session source interface gigabitethernet 0/24**
SMIS(config)# **monitor session source interface gigabitethernet 0/25**
SMIS(config)# end

SMIS# **show port-monitoring**

Port Monitoring is enabled
Monitor Port : Gi0/48

Port	Ingress-Monitoring	Egress-Monitoring
Gi0/1	Disabled	Disabled
Gi0/2	Disabled	Disabled
Gi0/3	Disabled	Disabled
Gi0/4	Disabled	Disabled
Gi0/5	Disabled	Disabled
Gi0/6	Disabled	Disabled
Gi0/7	Disabled	Disabled
Gi0/8	Disabled	Disabled
Gi0/9	Disabled	Disabled
Gi0/10	Disabled	Disabled
Gi0/11	Disabled	Disabled
Gi0/12	Disabled	Disabled
Gi0/13	Disabled	Disabled

Gi0/14	Disabled	Disabled
Gi0/15	Disabled	Disabled
Gi0/16	Disabled	Disabled
Gi0/17	Disabled	Disabled
Gi0/18	Disabled	Disabled
Gi0/19	Disabled	Disabled
Gi0/20	Disabled	Disabled
Gi0/21	Disabled	Disabled
Gi0/22	Enabled	Enabled
Gi0/23	Enabled	Enabled
Gi0/24	Enabled	Enabled
Gi0/25	Enabled	Enabled
Gi0/26	Disabled	Disabled
Gi0/27	Disabled	Disabled
Gi0/28	Disabled	Disabled
Gi0/29	Disabled	Disabled
Gi0/30	Disabled	Disabled
Gi0/31	Disabled	Disabled
Gi0/32	Disabled	Disabled
Gi0/33	Disabled	Disabled
Gi0/34	Disabled	Disabled
Gi0/35	Disabled	Disabled
Gi0/36	Disabled	Disabled
Gi0/37	Disabled	Disabled
Gi0/38	Disabled	Disabled
Gi0/39	Disabled	Disabled
Gi0/40	Disabled	Disabled
Gi0/41	Disabled	Disabled
Gi0/42	Disabled	Disabled
Gi0/43	Disabled	Disabled
Gi0/44	Disabled	Disabled
Gi0/45	Disabled	Disabled
Gi0/46	Disabled	Disabled
Gi0/47	Disabled	Disabled
Gi0/48	Disabled	Disabled
Ex0/1	Disabled	Disabled
Ex0/2	Disabled	Disabled
Ex0/3	Disabled	Disabled
Ex0/4	Disabled	Disabled

10 SNMP

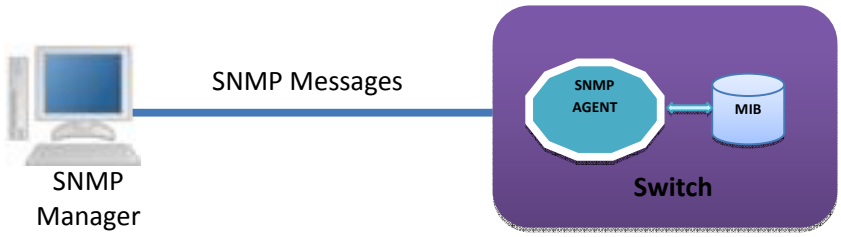
SNMP helps to monitor and manage the switches from network management systems (NMS). SNMP solutions contain three major components – SNMP manager, SNMP agent and MIB (Management Information Base) as shown in Figure – SNMP-1.

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.

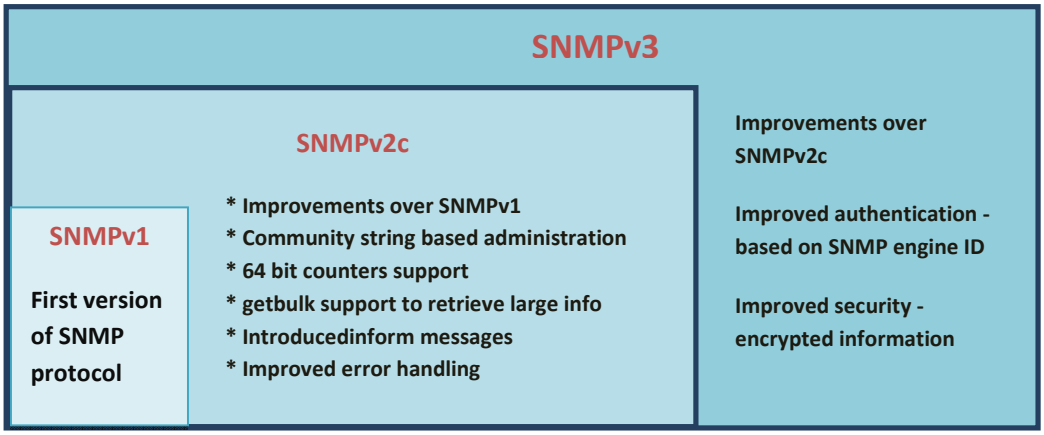
The SNMP agent also resides on the switch. It processes the SNMP requests received from the SNMP manager. It sends responses to SNMP managers by retrieving required information from the MIB. It also updates the MIB based on SNMP messages sent by the SNMP managers. SNMP agents also send voluntary traps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

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.
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

10.1 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.

10.2 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
1Gig physical interfaces	Starts from 1 and goes up to the maximum number of 1Gig interfaces available on the switch. 1 to 48
10Gig physical interfaces	Starts after 1Gig ifIndexes and goes up to the maximum number of 10Gig interfaces available on the switch. 49 to 52
Port channel interfaces	Starts after 10Gig ifIndexes and goes up to the maximum number of port channel interfaces supported on the switch. 53 to 104
Management IP interfaces	105

10.3 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.

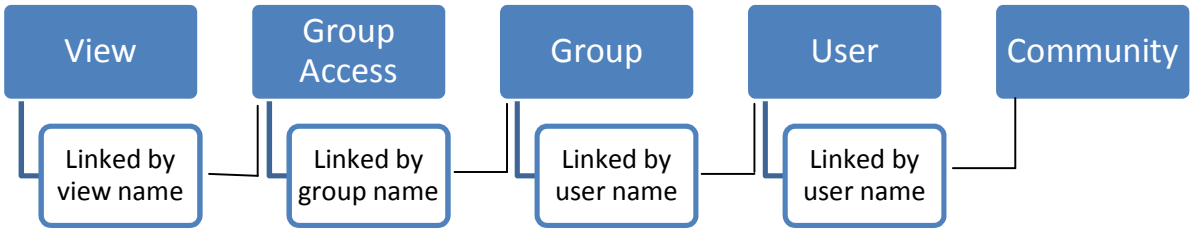


Figure SNMP-2: SNMP - Relationships

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.

10.3.1 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).

10.4 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

10.5 Enable/Disablethe 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.

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**

10.5.1 Switch Name

Supermicro switches can be assigned a name for identification purposes. The default switch name isSMIS. 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 thisconfiguration to be part of the startup configuration.

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

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

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

switch1# **show system information**
Switch Name: switch1
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 1 mins 11 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
=============== ===== ======
Key # Key
======= ====================================
Time zone offset not set

10.5.2 Switch Contact

Supermicro switches provide an option to configure the switch in charge Contact details, usually anemail 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.

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

10.5.3 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

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

10.6 Access Control

There are various parameters that control access to the SNMP Agent.

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

10.6.1 Engine Identifier

The SNMP Engine Identifieris 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 theEngine 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. *EngineIdentifier*-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.

10.6.2 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>]**	Configures the SNMP community. *CommunityIndex*–Alphanumericvalue with a maximum of 32 characters. *CommunityName*–Alphanumeric value with a maximum of 255 characters. *SecurityName* – This is the user name associated with the community. Alphanumeric value with a maximum of 40 characters. *Name* –Alphanumeric value with a maximum of 40 characters. *TransportTagIdentifier* –Identifies the transport end points between agent and manager.Alphanumeric value with a maximum of 255 characters.
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.

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

10.6.3 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
Step 2	**snmp user <UserName> [auth {md5 | sha}**	Configures the SNMP user,

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

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

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

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

SMIS# **show snmp user**

Engine ID: 80.00.08.1c.04.46.53
User: user5
Authentication Protocol: MD5
Privacy Protocol: DES_CBC
Storage Type: Volatile
Row Status: Active

Engine ID: 80.00.08.1c.04.46.53
User: initial
Authentication Protocol: None
Privacy Protocol: None
Storage Type: Volatile
Row Status: Active

Engine ID: 80.00.08.1c.04.46.53
User: templateMD5
Authentication Protocol: MD5
Privacy Protocol: None
Storage Type: Volatile
Row Status: Active

Engine ID: 80.00.08.1c.04.46.53
User: templateSHA
Authentication Protocol: SHA
Privacy Protocol: DES_CBC
Storage Type: Volatile
Row Status: Active

10.6.4 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. *GroupName* – Alphanumeric value with a maximum of 40 characters. *Security-model* – Use v1 or v2c or v3. *UserName* - Alphanumeric value with a maximum of 40 characters. 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
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

10.6.5 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}]**	Configures the SNMP view. *ViewName*- Alphanumeric value with a maximum of 40 characters. *OIDTree*–OID number, with a maximum of 32 numbers. *OIDMask*– OID number, with a maximum of 32 numbers. Use **included**to specifythat the MIB sub-tree is included in the view. Use **excluded**to specify that the MIB sub-tree is excluded from the view. 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 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

10.6.6 Group Access

Group access defines the access policy for a set of users belonging to a particular group. Group access is used only for SNMPv3.

Follow the steps below to configure SNMP group access.

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}]**	Configures the SNMP group access. *GroupName* - Alphanumeric value with a maximum of 40 characters. Security model – Mention one of v1, v2c or v3. Use **auth**to enable authentication for the user. Use **priv**toenableencryption of packets. *ReadView*- View name that specifies read access to particular MIB sub-tree.Alphanumeric value with a maximum of 40 characters. *WriteView*View name that specifies write access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters. *NotifyView*View name that specifies a particular MIB sub-tree used in notification. Alphanumeric value with a maximum of 40 characters. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp group access**	Displays the SNMP group access information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of startup configuration.

Group, user and view should be created before configuring group access.

The**"no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}**" commanddeletes 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

10.7 Trap

10.7.1 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. *TargetAddressName* - Alphanumeric value with a maximum of 40 characters. *ParamName* – The parameter to be notified to the specific target. Alphanumeric value with a maximum of 40 characters. IPAddress– IPv4 address of the target. *IP6Address* – IPv6 address of the target. *Seconds* – Specifies the timeout within which the target should be reachable. *RetryCount* – Specifies the

		number of retries to reach the target. *TagIdentifier*- A set of targets can be grouped under a tag Identifier. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
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

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

The**"no snmptargetparams<ParamName> "**command deletes the specified SNMP target parameters information.

The example below shows the commands used to configure the SNMP target parameters.

SMIS# configure terminal

SMIS(config)# **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 Authenitcation, 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 Authenitcation, 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 Authenitcation, No Privacy
Storage Type: Volatile
Row Status: Active

10.7.3 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
Step 2	**snmp notify <NotifyName> tag <TagName> type {Trap | Inform}[{volatile | nonvolatile}]**	Configures the SNMP Notify information. *NotifyName*- Alphanumeric value with a maximum of 40 characters. *TagName* –Specifies a group of targets identified by this name. Alphanumeric value with a maximum of 255

		characters. Type – Notification can be Trap or Inform. Use **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

10.7.4 Trap UDP Port

The default UDP port for traps is 162. Supermicro switches providean 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. *Port*–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.

10.7.5 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.

10.7.6 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: gigabit ethernet – gi extreme-ethernet – ex port-channel interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. Toprovide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 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 Gi 0/21
SMIS(config-if)# **no snmp trap link-status**
SMIS(config-if)# end

SMIS# **show interface Gi 0/21**

Gi0/21 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

10.8 Sub-Agent

Supermicro switches can act as a Sub-Agent to another SNMP agent. SNMP Agent and Sub-Agent communication is via a protocol called AgentX. The Sub-Agent feature is disabled by default.

Follow the steps below to configure an SNMP Sub-Agent.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**enable snmpsubagent{master { ip4 <ipv4_address> | ip6 <ipv6_address> } [port <number>] }**	Configures the switch as SNMP Sub-Agent. *ipv4_address* – IPv4 address of Sub-Agent *ipv6_address* – IPv6 address of Sub-Agent *number* – UDP port number for SNMP message reception/transmission at Sub-Agent, in the range of 1-65535.
Step 3	**end**	Exits the configuration mode.
Step 4	show snmpagentx information show snmpagentx statistics	Displays the SNMP Sub-Agent information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

An SNMP Agent must be disabled before enabling an SNMP Sub-Agent.

The **"disable snmpsubagent "**command disables the SNMP Sub-Agent.

The example below shows the commands used to enable the SNMP Sub-Agent.

SMIS# configure terminal
SMIS(config)# disable snmpagent
SMIS(config)# **enable snmpsubagent master ip4 192.168.1.80**
SMIS(config)# end

SMIS# **show snmpagentx information**
Agentx Subagent is enabled
TransportDomain:TCP
Master IP Address:192.168.1.80
Master PortNo:705

SMIS(config)# **show snmpagentx statistics**

Tx Statistics
  Transmitted Packets:1
  Open PDU:1
  Index Allocate PDU:0
  Index DeAllocate PDU:0
  Register PDU:0
  Add Agent Capabilities PDU:0
  Notify PDU:0
  Ping PDU:0
  Remove Agent Capabilities PDU:0
UnRegister PDU:0
  Close PDU:0
  Response PDU:0

Rx Statistics
  Rx Packets:0
  Get PDU:0
GetNext PDU:0
GetBulk PDU:0
TestSet PDU:0
  Commit PDU:0
  Cleanup PDU:0
  Undo PDU:0
  Dropped Packets:0
  Parse Drop Errors:0
  Open Fail Errors:0
  Close PDU:0
  Response PDU:0

10.9 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 groupcalled *superusers*and associateuser1 with this group.
    b. Create groupcalled *generalusers* and associate user1 with this group.
3) Create views
    a. Creates an SNMP view '*full'*which will allow access to everything from the specified Object Identifier
    b. Creates an SNMP view '*restricted'*which will allow access to everything from the specified OID onwards, and also adds a restriction to anything on a particular sub-tree.
4) Create group access
    a. Access for *superusers- fullread/write* and notify privilege to the '*full*' view
    b. Access for *generalusers- full* read,notify privilege to the 'full' view and , retricted write
5) Display all configuration

SMIS# configure terminal

SMIS(config)# **snmp user user1 auth md5 pwd1**

SMIS(config)# **snmp user user2 auth sha abcd priv deS 1b12**

SMIS(config)# **snmp group superuser user user1 security-model v3 volatile**

SMIS(config)# **snmp group generalusers user user2 security-model v3 volatile**

SMIS(config)# **snmp view full 1.3.6.1 included volatile**

SMIS(config)# **snmp view restricted 1.3.6.1 included volatile**

SMIS(config)# **snmp view restricted 1.3.6.3.10.2.1 excluded volatile**

SMIS(config)# **snmp access superuser v3 auth read full write full notify full**

SMIS(config)# **snmp access generalusers v3 noauth read full write restricted notify full**

SMIS(config)# end

SMIS# **show snmp user**

Engine ID : 80.00.08.1c.04.46.53

User : user1

Authentication Protocol : MD5

Privacy Protocol : None

Storage Type : Volatile

Row Status : Active

Engine ID : 80.00.08.1c.04.46.53

User : user2

Authentication Protocol : SHA

Privacy Protocol : DES_CBC

Storage Type : Volatile

Row Status : Active

Engine ID : 80.00.08.1c.04.46.53

User : initial

Authentication Protocol : None

Privacy Protocol : None

Storage Type : Volatile

Row Status : Active

Engine ID : 80.00.08.1c.04.46.53

User : templateMD5

Authentication Protocol : MD5

Privacy Protocol : None

Storage Type : Volatile

Row Status : Active

Engine ID : 80.00.08.1c.04.46.53

User : templateSHA

Authentication Protocol : SHA

Privacy Protocol : DES_CBC

Storage Type : Volatile

Row Status : Active

SMIS# **show snmp group**

Security Model : v1

Security Name : none

Group Name : iso

Storage Type : Volatile

Row Status : Active

Security Model : v2c

Security Name : none

Group Name : iso

Storage Type : Volatile

Row Status : Active

Security Model : v3

Security Name : user1

Group Name : superuser

Storage Type : Volatile

Row Status : Active

Security Model : v3

Security Name : user2

Group Name : generalusers

Storage Type : Volatile

Row Status : Active

Security Model : v3

Security Name : initial

Group Name : initial

Storage Type : Non-volatile

Row Status : Active

Security Model : v3

Security Name : templateMD5

Group Name : initial

Storage Type : Non-volatile

Row Status : Active

Security Model : v3

Security Name : templateSHA

Group Name : initial

Storage Type : Non-volatile

Row Status : Active

SMIS# **show snmp group access**

Group Name : iso

Read View : iso

Write View : iso

Notify View : iso

Storage Type : Volatile

Row Status : Active

Group Name : iso

Read View : iso

Write View : iso

Notify View : iso

Storage Type : Volatile

Row Status : Active

Group Name : initial

Read View : restricted

Write View : restricted

Notify View : restricted

Storage Type : Non-volatile

Row Status : Active

Group Name : initial

Read View : iso

Write View : iso

Notify View : iso

Storage Type : Non-volatile

Row Status : Active

Group Name : initial

Read View : iso

Write View : iso

Notify View : iso

Storage Type : Non-volatile

Row Status : Active

Group Name : superuser

Read View : full

Write View : full

Notify View : full

Storage Type : Volatile

Row Status : Active

Group Name : generalusers

Read View : full

Write View :

Notify View : full

Storage Type : Volatile

Row Status : Active

SMIS# **show snmp viewtree**

View Name : iso

Subtree OID : 1

Subtree Mask : 1

View Type : Included

Storage Type : Non-volatile

Row Status : Active

View Name : full

Subtree OID : 1.3.6.1

Subtree Mask : 1.1.1.1

View Type : Included

Storage Type : Volatile

Row Status : Active

View Name : restricted

Subtree OID : 1

Subtree Mask : 1

View Type : Excluded

Storage Type : Non-volatile

Row Status : Active

View Name : restricted

Subtree OID : 1.3.6.1

Subtree Mask : 1.1.1.1

View Type : Included

Storage Type : Volatile

Row Status : Active

View Name : restricted

Subtree OID : 1.3.6.3.10.2.1

Subtree Mask : 1.1.1.1.1.1.1

View Type : Excluded

Storage Type : Volatile

Row Status : Active

SMIS# **show running-config**

Building configuration...

Switch ID	Hardware Version	Firmware Version
0	MBM-GEM-004	1.0.0

vlan 1

ports gi 0/1-24 untagged

ports ex 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

11 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 implementedbasedon 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.

RMON protocol allows multiple monitors or management devices. A monitor provides two ways of data gathering:

- Using RMON probesfrom 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.

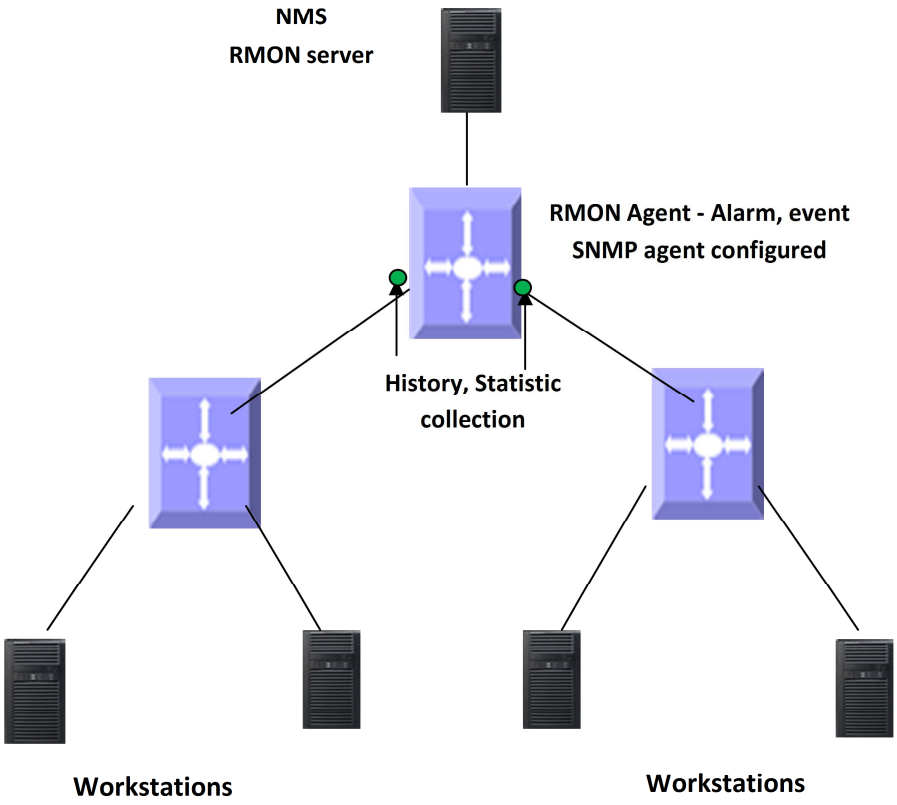


Figure RMON-1: RMON Operation

11.1 RMON Groups

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

11.1.1 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 handledas 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.

11.1.2 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.

11.1.3 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 interfaceas a cumulative sum for a particular period.

11.1.3.1 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.

11.1.3.2 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.

11.2 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

11.2.1 EnablingRMON

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

11.2.2 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 createdfor 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)>]	(Optional) Set an alarm on a MIB object. alarm-number - Alarm Number. This value ranges between 1 and 65535. mib-object-id - The mib object identifier. sample-interval-time - Time in seconds during which the alarm monitors the MIB variable. This value ranges between 1 and 65535 seconds. absolute - Used to test each mib variable directly. delta - Used to test the change between samples of a variable. rising-threshold - A number at which the alarm is triggered. This value ranges

		between 0 and 2147483647. falling-threshold*value* - A number at which the alarm is reset. This value ranges between 0 and 2147483647. NOTE: Falling threshold must be less than rising threshold. rising-event-number - The event number to trigger when the rising threshold exceeds its limit. This value ranges between 1 and 65535. falling-event-number - The event number to trigger when the falling threshold exceeds its limit. This value ranges between 1 and 65535. Owner – Owner of the alarm, string of length 127.
Step 3	rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]	(Optional) Add an event in the RMON event table that is associated with an RMON event number. Number - Event number Description - Description of the event Log - Used to generate a log entry Owner - Owner of the event, , in range 1- 127 characters Trap - Used to generate a trap. The SNMP community string is to be passed for the specifiedtrap. NOTE : When RMON event trap is enabled, SNMP agent must be configured prior to configuring the RMON alarm function as described in SNMP Configuration guide (www.supermicro.com).
Step 4	end	Exit from Configuration mode.
Step 5	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)>” commandsdelete 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, elsethe creation of the alarm entry fails, and no alarm event is triggered.

11.2.3 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 createdper 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: gigabitethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	rmon collection stats <index (1-65535)> [owner <ownername (127)>]	(Optional) Enable RMON statistic collection on the interface

		index - Statistics table index, in range 1-65535 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.

11.2.4 RMON Configuration Example

A sample RMON configuration of alarms, events and collection statistics and History in a Supermicro switch is specified below.

1) Enable RMON
2) Create events for Rising and falling threshold.
3) Create the alarm for the MIB object in 1 1.3.6.1.6.3.16.1.2.1.4table.
4) Create statistics collection on an interface.
5) Display all RMON configurations.

SMIS# configure terminal

SMIS(config)# set rmon enable

SMIS(config)# rmon event 1 description rise log owner smicro1 trap PUBLIC

SMIS(config)# rmon event 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 Gi 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 Gi0/5 is active, and owned by monitor,

Monitors ifEntry.1.5 which has

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

# of packets received of length (in octets):

64: 0, 65-127: 0, 128-255: 0,
256-511: 0, 512-1023: 0, 1024-1518: 0

SMIS# show rmon events

RMON is enabled

Event 1 is active, owned by smicro1

Description is rise

Event firing causes log and trap to community PUBLIC,

Time last sent is Apr 29 10:12:20 2013

Logging Event With Description : rise

Event 2 is active, owned by smicro1

Description is fall

Event firing causes log and trap to community NETMAN,

Time last sent is Apr 29 10:11:01 2013

SMIS# show rmon history

RMON is enabled

Entry 1 is active, and owned by

Monitors ifEntry.1.5 every 20 second(s)

Requested # of time intervals, ie buckets, is 2,

Granted # of time intervals, ie buckets, is 2,

Sample 2 began measuring at Apr 29 10:13:52 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

# of dropped packet events is 0

Network utilization is estimated at 0

Sample 3 began measuring at Apr 29 10:14:12 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

# of dropped packet events is 0

Network utilization is estimated at 0

SMIS# show rmon alarms

RMON is enabled

Alarm 1 is active, owned by smicro1

Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)

Taking absolute samples, last value was 2

Rising threshold is 2, assigned to event 1

Falling threshold is 1, assigned to event 2

On startup enable rising or falling alarm

SMIS# show rmon history overview

RMON is enabled

Entry 1 is active, and owned by

Monitors ifEntry.1.5 every 20 second(s)

Requested # of time intervals, ie buckets, is 2,

Granted # of time intervals, ie buckets, is 2,

SMIS# show rmon statistics 1 alarms events history 1

RMON is enabled

Collection 1 on Gi0/5 is active, and owned by monitor,

Monitors ifEntry.1.5 which has

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

# of packets received of length (in octets):

64: 0, 65-127: 0, 128-255: 0,

256-511: 0, 512-1023: 0, 1024-1518: 0

Alarm 1 is active, owned by smicro1

Monitors 1.3.6.1.6.3.16.1.2.1.4.1.4.110.111.110.101 every 2 second(s)

Taking absolute samples, last value was 2

Rising threshold is 2, assigned to event 1

Falling threshold is 1, assigned to event 2

On startup enable rising or falling alarm

Event 1 is active, owned by smicro1

Description is rise

Event firing causes log and trap to community PUBLIC,

Time last sent is Apr 29 10:12:20 2013

Logging Event With Description : rise

Event 2 is active, owned by smicro1

Description is fall

Event firing causes log and trap to community NETMAN,

Time last sent is Apr 29 10:11:01 2013

Entry 1 is active, and owned by

Monitors ifEntry.1.5 every 20 second(s)

Requested # of time intervals, ie buckets, is 2,

Granted # of time intervals, ie buckets, is 2,

Sample 4 began measuring at Apr 29 10:14:32 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

# of dropped packet events is 0

Network utilization is estimated at 0

Sample 5 began measuring at Apr 29 10:14:52 2013

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions,

# of dropped packet events is 0

Network utilization is estimated at 0

SMIS# write startup-config

Building configuration, Please wait. May take a few minutes ...

[OK]

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

vlan 1

ports gi 0/1-24 untagged

ports ex 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

old 2 1 falling-threshold 1 2 owner smicro1

interface Gi 0/5

rmon collection stats 1 owner monitor

rmon collection history 1 buckets 2 interval 20

exit

11.2.5 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: gigabit-ethernet – gi extreme-ethernet – ex 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 gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 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 of1-10000000.
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 disablesthe ratelimit on a particular interface.

The example below shows the commands used to configure the rate limit.

SMIS# configure terminal
SMIS(config)# interface Gi 0/20
SMIS(config-if)# rate-limit output 500000 4800
SMIS(config-if)# end

SMIS# show interface Gi 0/20 rate-limit

Gi0/20

Rate Limit : 500000 Kbps
Burst Size : 4800 Kbps

11.2.6 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 theinterface configuration.

The “hol blocking prevention” command enables HOLblocking.

The example below shows the commands used to disable HOL blocking.

SMIS# configure terminal
SMIS(config)# interface Gi 0/4
SMIS(config-if)# no hol blocking prevention
SMIS(config-if)# end
SMIS# show interface Gi 0/4

Gi0/4 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port
Hardware Address is 00:30:48:e3:04:78

MTU 1500 bytes, Full duplex, 1 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

12 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.

12.1 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 RADUIS 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
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
```

12.2 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
Key	None

12.2.1 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. *ip-address* – serverIP address. *timeout* – Specify RADIUS server timeout in range 1-120 *retransmit* – Specify number of retries to attempt to connect to RADIUS server in range 1-254 *key* –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

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

12.3 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

12.3.1 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. *ip-address* – TACACS Server IP-address *single-connection* – When this option is specified,only one connection to one of the configured TACACS servers is permitted. *port* – Specify TCP port in range 1-65535 *timeout* - Specify TACACS server timeout in range 0 – 255 seconds *key* – Authentication key of maximum length 64 characters.
Step 3	End	Exits the configuration mode.
Step 4	show tacacs	Displays the TACACS configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no tacacs-server host <ip-address>” command deletes the TACACS server.

The example below shows the commands used to configure TACACS server.

```
SMIS# configure terminal
SMIS(config)# tacacs-server host 10.10.10.1 port 500 timeout 200 key key123

SMIS(config)# end

SMIS# show tacacs

Server : 1
    Address         : 10.10.10.1
```

Single Connection : no

TCP port : 500

Timeout : 200

Secret Key : key123

Client uses server: 0.0.0.0
Authen. Starts sent : 0
Authen. Continues sent : 0
Authen. Enables sent : 0
Authen. Aborts sent : 0
Authen. Pass rvcd. : 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

12.3.2 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
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

12.3.3 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
    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 rvcd.     : 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
```

12.3.4 TACACS Login Authentication Mode

Supermicro switches provide an option to configure TACACS login authentication mode. Users can specify one of the mode PAP or CHAP .

In TACACS+ mode, authentication request is sent to the configured TACACS+ server. The user name and passwords are authenticated using TACACS+ server.

Follow the steps below to configure the TACACS login authentication mode to be used.

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 rvcd.        : 11
Authen. Fails rcvd.       : 3
Authen. Get User rcvd. : 0
Authen. Get Pass rcvd. : 0
Authen. Sess. timeouts    : 0
```

Author. Requests sent : 0
Author. Pass Add rcvd. : 0
Author. Pass Repl rcvd : 0
Author. Fails rcvd. : 0
Author. Errors rcvd. : 0
Author Follows rcvd. : 0
Author. Sess. timeouts : 0
Acct. start reqs. sent : 0
Acct. WD reqs. sent : 0
Acct. Stop reqs. sent : 0
Acct. Success rcvd. : 0
Acct. Errors rcvd. : 0
Acct. Follows rcvd. : 0
Acct. Sess. timeouts : 0
Malformed Pkts. rcvd. : 0
Socket failures : 0
Connection failures : 0

12.3.5 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 rvcd.          : 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
```

12.3.6 TACACS Privilege

Req. #	Description	Comments

1.0	The privilege configured in TACACS+ server should be used while logging in to Supermicro switch using TACACS+ authentication.
	
	There are many types of service used by different vendors on the market. For Supermicro switches the supported service type is 'config'.
	
	E.g. user configuration in TACACS+ server:
	user = test15 {
	name = "Test15 User"
	pap = cleartext "test15"
	service=**config** {
	priv-lvl = 15
		This is an umbrella requirement to cover the functionality.

	} }	

1.1	TACACS+ users without privilege configured also should be able to login to switch with the default privilege level 1.
	
	E.g. user configuration in TACACS+ server:
	user = test1 {
	name = "Test1 User"
	pap = cleartext "test1"
	}	

1.2	This privilege function should be enabled only when user enables it in CLI, Web, and SNMP. Proposed new CLI command to enable: aaa authorization group tacacs In Web, it should be enabled in “Management Security” page. In SNMP, the following OID can be used: 1.3.6.1.4.1.2076.77.1.6.0	For e.g. the new command “aaa authorization
1.3	If this function is not enabled (using the command in Req. 2), switch should behave as before. It means the irrespective of the privilege configured on the TACACS+ server, it will login the users with the default privilege 1.	
1.4	The TACACS+ privilege function should work in telnet, ssh and Web login.	
1.5	The new authorization status configuration (Req. 2) should be saved and restored.	

12.4 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
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 {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>}	*versioncompatibility*- Specify whether switch should process both version 1 and version 2 SSL messages. *cipher* – Specify the encryption algorithm. *auth* –Specify the authentication algorithm. *port* - Specify SSH port in range 1024-65535
Step 3	End	Exits the configuration mode.
Step 4	show ip ssh	Displays the SSH configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc]) | auth ([hmac-md5] [hmac-sha1]) | port <(1024-65535)>}” command disables SSH.

The example below shows the commands used to configure SSH.

SMIS# configure terminal
SMIS(config)# ip ssh version compatibility
SMIS(config)# end
SMIS# show ip ssh

Version : Both

Cipher Algorithm : 3DES-CBC
Authentication : HMAC-SHA1
Trace Level : None
SMIS# configure terminal

SMIS(config)# ip ssh cipher des-cbc

SMIS(config)# end

SMIS# show ip ssh

Version : 2
Cipher Algorithm : DES-CBC

Authentication : HMAC-SHA1
Trace Level : None

SMIS# configure terminal

SMIS(config)# ip ssh auth hmac-md5

SMIS(config)# end

SMIS# show ip ssh

Version : 2
Cipher Algorithm : 3DES-CBC
Authentication : HMAC-MD5

Trace Level : None

12.5 SSL

SSL provides server authentication, encryption, and message integrity, as well asHTTP client authentication, to allow secure HTTP communications.To use this feature, thecryptographic (encrypted) software image must be installed on the switch.

Parameter	Default Value
HTTP Secure server status	Enabled
HTTP Secure server encryption	rsa-null-md5
HTTP Secure server keys	None
SSL Server certificate	None
SSL Server certificate request	None

12.5.1 Secure HTTP (https)

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over theInternet. *HTTP with SSL encryption (HTTPS)*provides a secure connection to allow such functions as configuringa 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	ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }	Configure Secure HTTP. *server* – Enables HTTPS server *ciphersuite* – Specify one or many of the supported encryption algorithm to be used. *crypto key rsa*–Encryption Key, either 512 or 1024.
Step 3	End	Exits the configuration mode.
Step 4	show ip http secure server status	Displays the SSL configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }” command enables the agent.

The example below shows the commands used to configure Secure HTTP.

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

HTTP secure server status : Disabled
HTTP secure server ciphersuite : RSA-DES-SHA:RSA-3DES-SHA:RSA-EXP1024-DES-SHA:
HTTP crypto key rsa 1024

12.5.2 Certificate Signing Request (CSR)

An SSL certificate provides security for online communications. Before requesting an SSL certificate, a Certificate Signing Request (CSR) must be generated and submitted to the Certification Authority (CA).Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. CA servers are called as trustpoints, e.g. thawte.com.

Supermicro switches create a Certificate Signing Request (CSR) using RSA key pair and Switch Identification.

Follow the steps below to configure Certificate Signing Request (CSR).

Step	Command	Description
Step 1	ssl gen cert-req algo rsa sn <SubjectName>	Configure Certificate Signing Request (CSR). *SubjectName* – Switch ID or IP-address.
Step 2	show ssl server-cert	Displays the SSL configuration.
Step 3	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to configure Certificate Signing Request (CSR).

SMIS# ssl gen cert-req algo rsa sn SMIS

-----BEGIN CERTIFICATE REQUEST-----

MIIBTjCBuAIBADAPMQ0wCwYDVQQDEwRTTUlTMIGfMA0GCSqGSIb3DQEBAQUAA4GN

ADCBiQKBgQChj0JzVX1/gZ4SMGekRdrsAnftWnKHG3VypWTtySqkvTwhnZ206Q2o

cBYJNKY4ZCykOXG81mfUhqPfVLyO8sbK+RYzEeTMX9lw9iq9yOySOlvxY6IoYNsg

O++JS02khz0SAbpRkhtGuwmBiZQtSj+8Ea3dG8ReoixpcYDVVdIrDQIDAQABoAAw

```
DQYJKoZIhvcNAQEEBQADgYEAXR8Nz40QeC8wqwzqy+iozT5iUMKOkelXTE8mDydt

AvRyc7a3EPraGjyOL5W1H94z+wW2wkxXTRzKuLzAEYRH9f84XB2uCAdL+jkuSBJc

5qd3j4yBtOIu/pxOsdKKwuq6LWbi44DCXg97SkE+pOYa7nWojVkjc2SbjvK5CTgG

89s=

-----END CERTIFICATE REQUEST-----

SMIS# show ssl server-cert

Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number: 10 (0xa)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=US, ST=CA, L=SanJose, O=Supermicro, OU=Switch, CN=Switch/Email
=support@supermicro.com

      Validity
         Not Before: Aug 11 22:18:10 2011 GMT
         Not After : Sep 10 22:18:10 2011 GMT
      Subject: CN=SMIS
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:a1:8f:42:73:55:7d:7f:81:9e:12:30:67:a4:45:
               da:ec:02:77:ed:5a:72:87:1b:75:72:a5:64:ed:c9:

               2a:a4:bd:3c:21:9d:9d:b4:e9:0d:a8:70:16:09:34:

               a6:38:64:2c:a4:39:71:bc:d6:67:d4:86:a3:df:54:

               bc:8e:f2:c6:ca:f9:16:33:11:e4:cc:5f:d9:70:f6:

               2a:bd:c8:ec:92:3a:5b:f1:63:a2:28:60:db:20:3b:

               ef:89:4b:4d:a4:87:3d:12:01:ba:51:92:1b:46:bb:

               09:81:89:94:2d:4a:3f:bc:11:ad:dd:1b:c4:5e:a2:

               2c:69:71:80:d5:55:d2:2b:0d

            Exponent: 65537 (0x10001)

   Signature Algorithm: md5WithRSAEncryption

      21:bd:73:5e:96:82:89:13:12:a6:69:e8:9c:e6:fb:a5:0f:bc:

      0b:8d:fd:03:25:68:d9:09:73:58:7f:e1:30:64:d9:3a:99:63:

      6b:d2:ec:37:ea:33:1e:28:11:48:26:94:13:36:aa:08:14:5a:
```

7a:c4:f2:14:26:54:9e:d4:b5:2d:a2:c1:ab:fe:7a:2f:b8:f6:
23:08:93:fb:6b:7e:d9:14:da:09:90:50:b4:76:b0:17:e1:5f:
53:75:ee:7a:5f:85:dd:90:3c:d4:28:18:ee:5c:64:f5:09:52:
03:25:3e:f1:ed:5d:80:37:4b:ff:ad:fb:54:d0:24:11:a1:cd:
32:6c

12.5.3 SSL Certificate

Each SSL Certificate contains

- A public/private key pair: a private key with the code and a public key used to decode it. The private key is installed on the server and is not shared with anyone. The public key is incorporated into the SSL certificate and shared with web browsers.
- Identification information. E.g. When you request an SSL certificate, a third party (such as Thawte) verifies your organization's information and issues a unique certificate to you with that information.

SSL Certificate can be configured in Supermicro switches. The certificate should be specified in PEM format.

Follow the steps below to configure SSL server certificate.

Step	Command	Description
Step 1	ip http secure	Configure Cipher Suite and Crypto Key RSA of your choice using "ip http secure" command.
Step 2	ssl gen cert-req algo rsa sn	Enter the subject name and create certificate request by using the "ssl gen cert-req algo rsa sn" command.
Step 3	show ssl server-cert	The "show ssl server-cert" command will display certificate request. Copy paste these contents to a text file, say a.csr.
Step 4	Linux commands	To generate SSL certificate openssl application can be used. The following steps can be executed in any linux machine to generate SSL certificates. For other openssl implementation refer the openssl documentation to find the equivalent steps. Execute the below commands in linux shell. 1. openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem 2. openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CAkey cakey.pem –Cacreateserial This would generate certificate file cert.pem.

Step 5	ssl server-cert	Open the generate certificate file cert.pem. Delete first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--). Join all the remaining lines as single line to avoid line breaks processed. Copy paste these joined texts in “Enter Certificate” prompt– This prompt appears after entering the “ssl serv-cert” command in CLI. This step would configure the certificate and save it to flash.
Step 6	show ssl server-cert	Displays the SSL configuration.

13 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 informationof remote systems.

The LLDP transmit only modesends 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 fromtheir databases.

The LLDP receive only mode receivesaremote 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 avalid 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
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

13.1.1 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.

13.1.2 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
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: gigabit-ethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	lldp {transmit | receive}	(Optional) Sets LLDP admin status on an interface to Transmit or Receive
Step 4	lldp notification [remote-table-chg][mis-configuration]	(Optional) Enables LLDP trap notification on an interface. remote-table-chg - Trap notification for change in neighbor’s table. mis-configuration - Trap notification for mis-configuration.
Step 5	lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }	(Optional) Configures LLDPport IDsubtype and port IDvalue if-alias - interface alias port-comp - port component mac-addr - MAC address if-name - interface name local - locally assigned

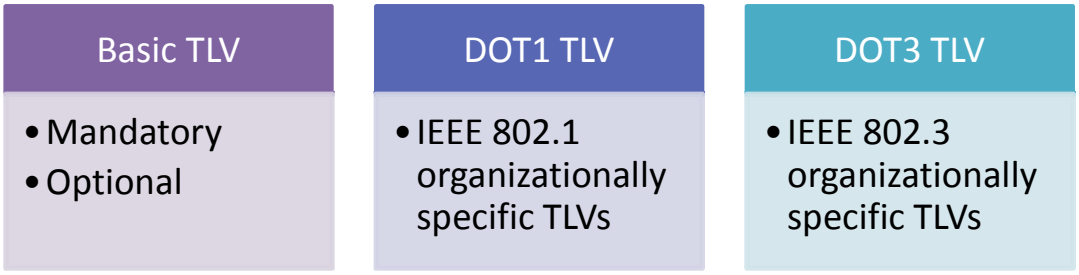
		The default value for port-id-subtype is if-name. Note: The if-alias option can be used only for the interfaces which havevalid description configured.
Step 6	Exit	Exitsinterface configuration mode.
Step 7	lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }	(Optional) Configures LLDPchassis IDsubtype and chassis IDvalue. The chassis identifier value can only be set for the chassis-component and local system subtypes. For all other subtypes, the value is taken from the system automatically. chassis-comp - chassis component if-alias - management interface alias port-comp - port component mac-addr - MAC address nw-addr - network address if-name - interface name local - locally assigned The default value for chassi-id-subtype is mac-addr. Note: To use the if-alias option, the management interface must have been configured with valid description.
Step 8	End	Exits the configuration mode.
Step 9	show lldp interface [<interface-type><interface-id>] show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type><interface-id>][detail] show lldp traffic [<iftype><ifnum>]	Displays LLDP configuration details on a particular interface or all interfaces Displays information about neighbors learned on an interface or all interfaces Displays LLDP counters, including the number of frames sent, received, discarded, etc.

	show lldp errors show lldp statistics	 Displays information about errors such as memory allocation failures, queue overflows, table overflows, etc. Displays the LLDP remote table statistics information
Step 10	clear lldp counters	Clears LLDP transmit and receive statistics
Step 11	clear lldp table	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] }

13.1.2.1 Configuring LLDP TLV

Supermicro switches provide support for user configuration of LLDP TLV's. The TLV types supported by Supermicro switches are: Basic TLV, DOT1 TLV and DOT3 TLV. The figure below displays the TLV types and



their content.

Figure LLDP-1: LLDP TLV Types

The content ofthe various TLVs supported by Supermicro switches are specified in the figurebelow.

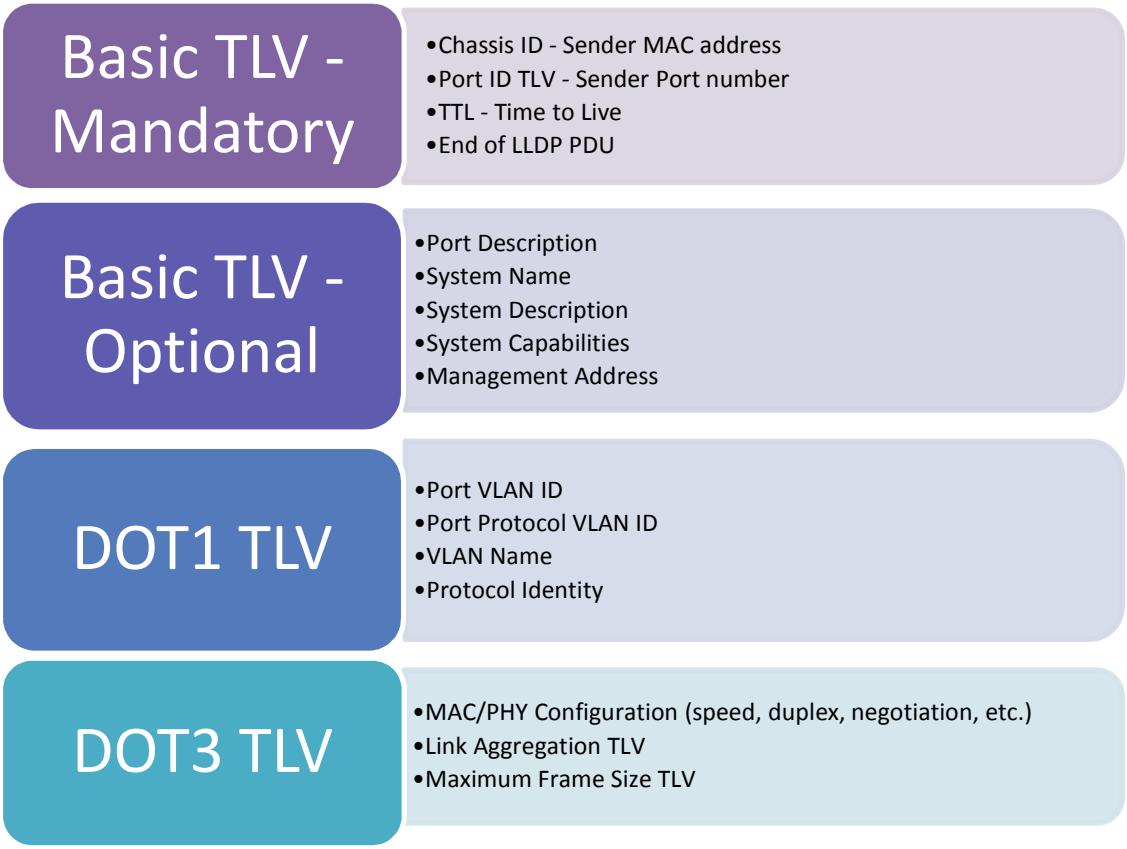


Figure LLDP-2: LLDP TLV Content

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <*interface-type*><*interface-id*> or interfacerange <*interface-type*><*interface-id*> ….	(Optional) Enters the interface configuration mode. interface-type – may be any of the following: gigabit-ethernet – gi extreme-ethernet – ex port-channel – po interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range gi 0/1-10 To provide multiple interfaces or

		ranges, separate with a comma (,). E.g.: int range gi 0/1-10, gi 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	lldptlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr {all | ipv4 <ucast_addr> | ipv6 <ip6_addr>}]}	(Optional) Enables the basic TLV transmission on a given port port-descr - Port description TLV sys-name - System name TLV sys-descr- System description TLV sys-capab - System capabilities TLV mgmt-addr all- Enables the transmission of the management address on the current interface. If no management address is present or configured in the system, the switch'sMAC address will be usedfor transmission. mgmt-addr ipv4 *ucast-addr* - Enables the transmission of a particular ipv4 address on the current interface. mgmt-addr ipv6 *ipv6-addr* - Enables the transmission of a particular ipv6 address on the current interface.
Step 4	lldptlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}]}	(Optional) Configure dot1 TLV types to be transmitted on a port port-vlan-id - Port VLAN identifier TLV. The keyword port-vlan-id keyword is not supported. 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

13.1.3 Configuring LLDP Timers

Supermicro switches allow for user configuration of LLDP timers:

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

13.1.3.1 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) Configuresthe 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 intervalto its default value.

13.1.3.2 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 informsthe receiving LLDP agent of the timeto retain remote LLDP informationif 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 holdtimemultiplier. Follow the steps below to change the message transmit holdtimemultiplier.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	lldpholdtime-multiplier <value(2-10)>	(Optional) Configures the message transmit holdtimemultiplier, range of 2-10.
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information

The “no lldpholdtime-multiplier” command resets the message transmit holdtimemultiplierto its default value.

13.1.3.3 ReinitializationDelay

When LLDP ports are disabled or the link goes down, LLDP is reinitialized on a port. The delay between the port going down and the reinitialization is called the reinitialization delay. When LLDP is reinitialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Supermicro switches allow user configuration of the reinitialization delay. Follow the steps below to change the reinitialization delay.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
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” commandresets the reinitialization delayto its default value.

13.1.3.4 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 themessage transmit delay, range of 1-8192. NOTE: The Txdelay should be less than 0.25 * message Txinterval
Step 3	End	Exits the configuration mode.
Step 4	show lldp	Displays the LLDP global information

The “no lldptx-delay” commandresets the message transmit delayto its default value.

13.1.3.5 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
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.

13.1.4 LLDPConfiguration

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

Figure LLDP-3: LLDP Configuration Example

Switch A

SMIS# configure terminal

SMIS(config)# set lldp enable

SMIS(config)# end

SMIS# show lldp

LLDP is enabled

Transmit Interval : 30

Holdtime Multiplier : 4

Reinitialization Delay : 2

Tx Delay : 2

Notification Interval : 5

Chassis Id SubType : Mac Address

Chassis Id : 00:30:48:e3:04:75

SMIS# show lldp neighbors

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

```
Chassis ID        Local Intf    Hold-time   Capability      Port Id

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

00:30:48:e3:70:bc   Gi0/21        120                 Gi0/22


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 Gi 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

SMIS(config-vlan)# exit

SMIS(config)# interface Gi 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	Gi0/21	120		Gi0/22

Total Entries Displayed : 1

SMIS# show lldp errors

Total Memory Allocation Failures : 0

Total Input Queue Overflows : 0

Total Table Overflows : 0

SMIS# show lldp traffic

Total Frames Out : 71

Total Entries Aged : 0

Total Frames In : 28

Total Frames Received In Error : 0

Total Frames Discarded : 0

Total TLVS Unrecognized : 0

Total TLVs Discarded : 0

SMIS# show lldp interface Gi 0/21

Gi0/21:

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 Gi 0/21

Port Id SubType : Interface Name

Port Id : Slot0/21

Port Description :

Enabled TxTlvs : Port Description, Management Address, Mac Phy

Extended 802.3 TLV Info

-MAC PHY Configuration & Status

Auto-Neg Support & Status : Supported, Enabled

Advertised Capability Bits : 6c11

10base-T(HD)

10base-T(FD)

100base-TX(HD)

100base-TX(FD)

Asym and SymmPAUSE(FD)

1000base-T(FD)

Operational MAU Type : 30

-Link Aggregation

Capability & Status : Not Capable, Not In Aggregation

Aggregated Port Id : 21

-Maximum Frame Size : 1500

Extended 802.1 TLV Info

-Port VLAN Id : 1

-Port & Protocol VLAN Id

Protocol VLAN Id Support Protocol VLAN Status TxStatus

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

0 Supported DisabledDisabled

-Vlan Name

Vlan Id Vlan Name TxStatus

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

1 vlan1 Enabled

SMIS# show running-config

Building configuration...

Switch ID Hardware Version Firmware Version

0 MBM-GEM-004 1.0.0

vlan 1

portsgi 0/1-24 untagged

ports ex 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

interfaceGi 0/21

lldp notification remote-table-chg

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

lldptlv-select dot3tlv macphy-config

lldptlv-select dot1tlv vlan-name 1

exit

Switch B

SMIS# configure terminal

SMIS(config)# set lldp enable

SMIS(config)# end

SMIS# show lldp

LLDP is enabled

Transmit Interval : 30

Holdtime Multiplier : 4

Reinitialization Delay : 2

Tx Delay : 2

Notification Interval : 5

Chassis Id SubType : Mac Address

Chassis Id : 00:30:48:e3:70:bc

SMIS# **show lldp neighbors**

Capability Codes :

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Chassis ID	Local Intf	Hold-time	Capability	Port Id
00:30:48:e3:04:75	Gi0/22	120		Gi0/21

Total Entries Displayed : 1

SMIS# **show lldp statistics**

Remote Table Last Change Time : 80900

Remote Table Inserts : 4

Remote Table Deletes : 3

Remote Table Drops : 0

Remote Table Ageouts : 3

Remote Table Updates : 7

SMIS(config)# show lldp traffic

Total Frames Out : 52

Total Entries Aged : 3

Total Frames In : 144

Total Frames Received In Error : 0

Total Frames Discarded : 0

Total TLVS Unrecognized : 0

Total TLVs Discarded : 0

SMIS(config)# show lldp errors

Total Memory Allocation Failures : 0

Total Input Queue Overflows : 0

Total Table Overflows : 0

SMIS(config)# show lldp interface Gi 0/22

Gi0/22:

Tx State : Enabled

Rx State : Enabled

Tx SEM State : IDLE

Rx SEM State : WAIT FOR FRAME

Notification Status : Disabled

Notification Type : Mis-configuration

SMIS# show lldp local Gi 0/22

Port Id SubType : Interface Alias

Port Id : Gi0/22

Port Description :

Enabled TxTlvs :

Extended 802.3 TLV Info

-MAC PHY Configuration & Status

Auto-Neg Support & Status : Supported, Enabled

Advertised Capability Bits : 6c11

10base-T(HD)

10base-T(FD)

100base-TX(HD)

100base-TX(FD)

Asym and SymmPAUSE(FD)

1000base-T(FD)

Operational MAU Type : 30

-Link Aggregation

Capability & Status : Not Capable, Not In Aggregation

Aggregated Port Id : 22

-Maximum Frame Size : 1500

Extended 802.1 TLV Info

-Port VLAN Id : 1

-Port & Protocol VLAN Id

Protocol VLAN Id	Support	Protocol VLAN Status	TxStatus
0	Supported	Enabled	Disabled

-Vlan Name

Vlan Id	Vlan Name	TxStatus
1		Disabled

SMIS# show running-config

Building configuration...

Switch ID	Hardware Version	Firmware Version
0	MBM-GEM-004	1.0.0

vlan 1

portsgi 0/1-24 untagged

ports ex 0/1-3 untagged

exit

setlldp enable