SSE-X3548S/SSE-X3548SR

System Configuration

User's Guide

Revision 1.14

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

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

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

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

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

Manual Revision 1.14
Release Date: 5/14/2020

Document Revision History

Date	Revision	Description
05/14/2020	1.14	Initial document.

Contents

1 Management IP

The SSE-X3548S/SR comes with DHCP IP settings for default IP management.

1.1 Static Management IP Address

The *IP address* command can be used to manually configure the management interface IP address. Follow the steps below to manually configure the management interface IP address.

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 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 the start-up config.

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

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

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

1.2 DHCP

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

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

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 the management interfaceIP address through DHCP server.

The example below shows the commands used to configure the management interface IP address through DHCP.
SMIS# configure terminal
SMIS(config)#ip address dhcp
SMIS(config)# end

1.3 Default IP Gateway

To configure default gateway on the switch 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 the IP gateway.
SMIS# configure terminal
SMIS(config)# ip gateway 10.1.1.1
SMIS(config)# end

2 Management Access

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

- User name and password
- Enable password

- Authorized Managers

Defaults – Management Access

Parameter	Default Value
Default User Name	ADMIN
Password	Default password is unique for each switch and it can be found on the label stuck on the switch.
Privilege for default user ADMIN. Default privilege for configured users.	15 1
IP Authorized Managers	None

2.1 User Login

User accounts can be configured for switch access. Each username can be associated with a password and privilege level. Users configured with a password are authenticated while accessing the switch to the configured privilege level.
Users with privilege level 1 or above can execute all “show” commands. To execute configuration commands, access with privilege level 15 is required.
Follow the steps below to configure the username.

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
```

2.2 Enable

Supermicro switches provide support for configuring access to various CLI commands. This is achieved by *Enable* password and *privilege levels*. Fifteen privilege levels can be specified.
Follow the steps below to enable a privilege level.

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 command used to enable a particular privilege level.

```
SMIS# enable15
```

2.3 Enable Password

Passwords for different enable levels can be configured by the switch administrator using the *enable password* command.
Follow the steps below to enable password for any privilege level.

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 the 'show running config' command.

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

The example below shows the commands used to configure *enable password*.
SMIS# configure terminal
SMIS(config)# enable password level 10 pwd1

2.4 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* – Manager IP 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: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces.

		vlan -Specify the vlan id through 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 a Supermicro switch, access to the switch via telnet, ssh, etc. is possible only by those hosts allowed to access. Other hosts will not be permitted access.

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

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

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

3 Interface Properties

The SSE-X3548S/R supports the following physical interface types.

25G Fx Ports

The SSE-X3548S/R has 48 Fx ports by default. The Fx ports operate at 25G speed by default and can be configured to operate at 10G or 1G speed.

100G Cx Ports

The SSE-X3548S/R has six 100G capable Cx ports by default.
The Cx ports can also operate at 40G speed.
Additionally, each Cx ports can be split in to four ports that can operate at 25G or 10G speed.
Use the speed command in interface mode to split the ports.
The below table shows the port names in the split cases.

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

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

Parameter	Default Value
MTU	1500 bytes
Negotiation	Enabled
Storm-control	Disabled
Description	None
Duplex Operation	Full
Flow Control	Off
FEC Mode	Enabled

3.1 Description

Supermicro switches allow users to configure a description string to the interfaces. This description string will be useful to identify the interfaces easily.
Follow the steps below to configure interface description string.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <*interface-type*><*interface-id*> or interface range <*interface-type*><*interface-id*> ….	Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	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 Fx 0/22
SMIS(config-if)# description Server_Cluster_0100

```
SMIS(config-if)# end
SMIS
# sh int description

Interface   Status   Protocol  Description
---------   ------   --------  -----------
Fx0/1       up       down
Fx0/2       up       down
Fx0/3       up       down
Fx0/4       up       down
Fx0/5       up       down
Fx0/6       up       down
Fx0/7       up       down
Fx0/8       up       down
Fx0/9       up       down
Fx0/10      up       down
Fx0/11      up       down
Fx0/12      up       down
Fx0/13      up       down
Fx0/14      up       down
Fx0/15      up       down
Fx0/16      up       down
Fx0/17      up       down
Fx0/18      up       down
Fx0/19      up       down
Fx0/20      up       down
Fx0/21      up       down
Fx0/22      up       down     Server_Cluster_0100
Fx0/23      up       down
Fx0/24      up       down
Fx0/25      up       down
Fx0/26      up       down
Fx0/27      up       down
Fx0/28      up       down
Fx0/29      up       down
Fx0/30      up       down
Fx0/31      up       down
Fx0/32      up       down
Fx0/33      up       down
Fx0/34      up       down
Fx0/35      up       down
Fx0/36      up       down
Fx0/37      up       down
Fx0/38      up       down
Fx0/39      up       down
Fx0/40      up       down
Fx0/41      up       down
Fx0/42      up       down
```

```
Fx0/43      up      down
Fx0/44      up      down
Fx0/45      up      down
Fx0/46      up      down
Fx0/47      up      down
Fx0/48      up      down
Cx0/1       up      down
Cx0/2       up      down
Cx0/3       up      down
Cx0/4       up      down
Cx0/5       up      down
Cx0/6       up      down
po1         up      down
po6         up      down
```

3.2 Negotiation

Interface speed can be negotiated between connected devices, if both ends support negotiation. Auto negotiation is enabled by default on all the Fx and Cx ports. It can be disabled if needed by using the 'no negotiation' command. **Auto negotiation is not supported for 40G speeds.** Turn off auto negotiation to set the Cx port speed to 40G.
Follow the steps below to configure Interface Negotiation.

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

Step3	Negotiation	Enable Interface Negotiation
Step 4	End	Exits the configuration mode.
Step 5	show interface status	Displays the interface configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no negotiation” command disables interface negotiation.

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

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

Port      Status        Duplex  Speed     Negotiation
----      ------        ------  -----     -----------
Fx0/1     not connected  Full   25 Gbps   Auto
Fx0/2     not connected  Full   25 Gbps   Auto
Fx0/3     not connected  Full   25 Gbps   Auto
Fx0/4     not connected  Full   25 Gbps   Auto
Fx0/5     not connected  Full   25 Gbps   Auto
Fx0/6     not connected  Full   25 Gbps   Auto
Fx0/7     not connected  Full   25 Gbps   Auto
Fx0/8     not connected  Full   25 Gbps   Auto
Fx0/9     not connected  Full   25 Gbps   Auto
Fx0/10    not connected  Full   25 Gbps   Auto
Fx0/11    not connected  Full   25 Gbps   Auto
Fx0/12    not connected  Full   25 Gbps   Auto
Fx0/13    not connected  Full   25 Gbps   Auto
Fx0/14    not connected  Full   25 Gbps   Auto
Fx0/15    not connected  Full   25 Gbps   Auto
Fx0/16    not connected  Full   25 Gbps   Auto
Fx0/17    not connected  Full   25 Gbps   Auto
Fx0/18    not connected  Full   25 Gbps   Auto
Fx0/19    not connected  Full   25 Gbps   Auto
Fx0/20    not connected  Full   25 Gbps   Auto
Fx0/21    not connected  Full   25 Gbps   Auto
Fx0/22    not connected  Full   25 Gbps   Auto
Fx0/23    not connected  Full   25 Gbps   Auto
Fx0/24    not connected  Full   25 Gbps   Auto
Fx0/25    not connected  Full   25 Gbps   Auto
Fx0/26    not connected  Full   25 Gbps   Auto
```

Fx0/27	not connected	Full	25 Gbps	Auto
Fx0/28	not connected	Full	25 Gbps	Auto
Fx0/29	not connected	Full	25 Gbps	Auto
Fx0/30	not connected	Full	25 Gbps	Auto
Fx0/31	not connected	Full	25 Gbps	Auto
Fx0/32	not connected	Full	25 Gbps	Auto
Fx0/33	not connected	Full	25 Gbps	Auto
Fx0/34	not connected	Full	25 Gbps	Auto
Fx0/35	not connected	Full	25 Gbps	Auto
Fx0/36	not connected	Full	25 Gbps	Auto
Fx0/37	not connected	Full	25 Gbps	Auto
Fx0/38	not connected	Full	25 Gbps	Auto
Fx0/39	not connected	Full	25 Gbps	Auto
Fx0/40	not connected	Full	25 Gbps	Auto
Fx0/41	not connected	Full	25 Gbps	Auto
Fx0/42	not connected	Full	25 Gbps	Auto
Fx0/43	not connected	Full	25 Gbps	Auto
Fx0/44	not connected	Full	25 Gbps	Auto
Fx0/45	not connected	Full	25 Gbps	Auto
Fx0/46	not connected	Full	25 Gbps	Auto
Fx0/47	not connected	Full	25 Gbps	Auto
Fx0/48	not connected	Full	25 Gbps	Auto
Cx0/1	not connected	Full	100 Gbps	Auto
Cx0/2	not connected	Full	100 Gbps	No-Negotiation
Cx0/3	not connected	Full	100 Gbps	Auto
Cx0/4	not connected	Full	100 Gbps	Auto
Cx0/5	not connected	Full	100 Gbps	Auto
Cx0/6	not connected	Full	100 Gbps	Auto

3.3 Speed

Interface speed can be configured for physical interfaces when auto negotiation is disabled.
25G FX ports can be configured to operate at 25G, 10G or 1G speeds.
100G CX ports can be configured to operate at 100G or 40G, or it can be split to operate at 25G/10G. The split can be done using the speed command to set the interface speed to 25G or 10G for the Cx ports.
Follow the steps below to configure the Interface speed.

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

		interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g. int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g. int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	speed { 1000 | 10000 | 25000 | 40000 | 100000 }	Configure interface speed as 10, 100, 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 the interface speed.

```
SMIS# configure terminal
SMIS(config)# interface Fx 0/44
SMIS(config-if)# speed 1000
SMIS(config-if)# end
SMIS# show interface status

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

Fx0/11	not connected	Full	25 Gbps	Auto
Fx0/12	not connected	Full	25 Gbps	Auto
Fx0/13	not connected	Full	25 Gbps	Auto
Fx0/14	not connected	Full	25 Gbps	Auto
Fx0/15	not connected	Full	25 Gbps	Auto
Fx0/16	not connected	Full	25 Gbps	Auto
Fx0/17	not connected	Full	25 Gbps	Auto
Fx0/18	not connected	Full	25 Gbps	Auto
Fx0/19	not connected	Full	25 Gbps	Auto
Fx0/20	not connected	Full	25 Gbps	Auto
Fx0/21	not connected	Full	25 Gbps	Auto
Fx0/22	not connected	Full	25 Gbps	Auto
Fx0/23	not connected	Full	25 Gbps	Auto
Fx0/24	not connected	Full	25 Gbps	Auto
Fx0/25	not connected	Full	25 Gbps	Auto
Fx0/26	not connected	Full	25 Gbps	Auto
Fx0/27	not connected	Full	25 Gbps	Auto
Fx0/28	not connected	Full	25 Gbps	Auto
Fx0/29	not connected	Full	25 Gbps	Auto
Fx0/30	not connected	Full	25 Gbps	Auto
Fx0/31	not connected	Full	25 Gbps	Auto
Fx0/32	not connected	Full	25 Gbps	Auto
Fx0/33	not connected	Full	25 Gbps	Auto
Fx0/34	not connected	Full	25 Gbps	Auto
Fx0/35	not connected	Full	25 Gbps	Auto
Fx0/36	not connected	Full	25 Gbps	Auto
Fx0/37	not connected	Full	25 Gbps	Auto
Fx0/38	not connected	Full	25 Gbps	Auto
Fx0/39	not connected	Full	25 Gbps	Auto
Fx0/40	not connected	Full	25 Gbps	Auto
Fx0/41	not connected	Full	25 Gbps	Auto
Fx0/42	not connected	Full	25 Gbps	Auto
Fx0/43	not connected	Full	25 Gbps	Auto
Fx0/44	not connected	Full	1 Gbps	Auto
Fx0/45	not connected	Full	25 Gbps	Auto
Fx0/46	not connected	Full	25 Gbps	Auto
Fx0/47	not connected	Full	25 Gbps	Auto
Fx0/48	not connected	Full	25 Gbps	Auto
Cx0/1	not connected	Full	100 Gbps	Auto
Cx0/2	not connected	Full	100 Gbps	Auto
Cx0/3	not connected	Full	100 Gbps	Auto
Cx0/4	not connected	Full	100 Gbps	Auto
Cx0/5	not connected	Full	100 Gbps	Auto
Cx0/6	not connected	Full	100 Gbps	Auto

3.4 Duplex Operation

The Supermicro X3548 switch doesn't support half-duplex operation on its physical interfaces.

3.5 MTU

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

Follow the steps below to configure the interface MTU.

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

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

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

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

```
SMIS# configure terminal
SMIS(config)# interface fx 0/22
SMIS(config-if)# mtu 9000
SMIS(config-if)# end
SMIS
# show interface fx 0/22
Fx0/22 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port

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

Link Up/Down Trap is enabled

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

Transmission Counters
  Octets: 0
  Unicast Packets: 0
  Unicast Packets  Rate: 0/Sec
  Broadcast Packets: 0
  Broadcast Packets Rate: 0/Sec
  Multicast Packets: 0
  Multicast Packets Rate: 0/Sec
```

Pause Frames: 0
Discarded Packets: 0
Error Packets: 0# show interface mtu fx-ethernet 0/22

Fx0/22 MTU size is 9000

3.6 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 other ports by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets to prevent any loss of data packets during the congestion period.
Follow the steps below to configure Flow Control.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <*interface-type*><*interface-id*> or interface range <*interface-type*><*interface-id*> ….	Enters the interface configuration mode. interface-type – may be any of the following: fx-ethernet – fx cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	flowcontrol { send | receive} { on | off }	Configure flow control *Send* – The port can send pause frames but cannot receive pause frames from a connected device.

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

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

```
SMIS# configure terminal
SMIS(config)# interface fx 0/22
SMIS(config-if)# flowcontrol send on
SMIS(config-if)# end
SMIS# show flow-control interface fx 0/22
Port    TxFlowControl   Rx FlowControl   Tx Pause   Rx Pause
----    -------------   -------------    --------  --------
Fx0/22  on              off              0         0
```

3.7 Storm Control

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

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

Follow the steps below to configure Storm control.

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

		interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	storm-control { broadcast |multicast | dlf } level <kbps (1-10000000)>	Configure Storm control for broadcast or multicast or DLF packets. Level – Threshold level in kbps, in range 1-10000000.
Step 4	End	Exits the configuration mode.
Step 5	show interfaces storm-control	Displays the interface Storm control configuration.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

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

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

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

SMIS# show interfaces fx 0/22 storm-control
Fx0/22
DLF Storm Control          : Disabled
Broadcast Storm Control    : Enabled
Broadcast Storm Control    : 50000
Multicast Storm Control    : Disabled
```

3.8 Forward Error Correction (FEC) Mode

Supermicro switches allow users to enable or disable the FEC mode on the interfaces configured for 25G and 100G. FEC is not supported for other speed settings. **It is recommended to turn ON FEC for most cables and peer devices.**
FEC is enabled by default in all Fx and Cx ports. This switch supports RS_FEC, which is equivalent to cl91 FEC in some devices.
Follow the steps below to enable FEC mode on the interface.

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

The example below shows the commands used to configure the interface description.
SMIS# configure terminal
SMIS(config)# interface Fx 0/22
SMIS(config-if)# fec-mode

SMIS(config-if)# end
SMIS
SMIS# sh int Fx 0/22

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

3.9 Port Splitting

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

Follow the steps below to split Cx-ethernet ports.

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: cx-ethernet – cx interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: int range cx 0/1-6 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range cx 0/1-2, cx 0/4 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	speed 25000 Or speed 10000	Splits the port into four 25G ports or four 10G ports.

		Note: Fec-mode and negotiation have to be turned off for splitting into 4 x 10G ports.
Step 4	end	Exits the configuration mode.
Step 5	show interface status	Split ports can be viewed in the output.
Step 6	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The example below shows the commands used to split Cx 0/1 interface in SBM-25G-100 into four 25G ports.
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config-if)# speed 25000
SMIS(config-if)# end

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

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

The example below shows the commands used to split Cx 0/1 interface in SBM-25G-100 into four 10G ports.
SMIS# configure terminal
SMIS(config)# interface cx 0/1
SMIS(config)#no fec-mode
SMIS(config)#no negotiation
SMIS(config-if)# speed 10000
SMIS(config-if)# end

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

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

4 Time Management

The system time and date on Supermicro switches can be managed by Network Time Protocol (NTP) or configured manually.
NTP provides synchronization of network resources by a synchronized network timestamp. Supermicro switches can function as an NTP client over UDP and receive the time from an NTP server in the

network.

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

4.1 NTP Server

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

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

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

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

```
[NTP] ntp is disabled
   Server     Key   Prefer
=============== =====  ======
 200.200.200.10   100   YES
  100.100.100.1   500
 Key #    Key
=======  ==================================
 Time zone offset not set
```

4.2 Enable/Disable NTP

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

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

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

The example below shows the commands used to configure NTP.

```
SMIS# configure terminal
SMIS(config)# ntp enable
SMIS(config)#end
SMIS# show ntp
[NTP] ntp running unicast mode
  Server     Key   Prefer
=============== =====  ======
 200.200.200.10   100   YES
  100.100.100.1   500

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

4.3 NTP Authentication

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

key number and text pair.

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
```

4.4 NTP Broadcast

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

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ntp broadcast [authentication]	Configure NTP broadcast. *authentication* – If specified, NTP authentication is enabled for broadcast mode.
Step 3	End	Exits the configuration mode.

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

The "no ntp broadcast" command disables NTP Broadcast.

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

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

4.5 System Clock

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

Step	Command	Description
Step 1	clock set hh:mm:ss day<1-31>month<january|february|march|april|may|june|july|august|september|october|november|december> year<2000 - 2035>	Configure the system clock. *hh:mm:ss* – Time in Hours:Minutes:Seconds format. *day* – Day in 1-31 format. *month* – Month in January-December format. *year* – Year in yyyy format.
Step 2	show clock	Displays the system clock.

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

```
SMIS# clock set 09:26:15 31 august 2013
Wed Aug 31 09:26:15 2013
SMIS# show clock
Wed Aug 31 09:26:20 2013
```

4.6 Time Zone

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

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	tz posix <std><offset>[<dst>]	Configure the time zone. <std> - Standard time text e.g. PST <offset> - Time zone offset in $[+\|-]hh[:mm[:ss]]$ format. This is the value needed to be added to local time to get to UST. This value is positive if the local time zone is in west of the Prime Merdian, otherwise it is negative. <dst> - Day light savings time text e.g. PDT
Step 3	end	Exits the configuration mode.
Step 4	show system information	Displays the time zone 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 time zone offset.
SMIS# configure terminal
SMIS(config)# tz posix PST8
SMIS(config)# end

SMIS# show system information
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 48 mins 5 secs

Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
=============== ===== ======
Key # Key
======= ==========
Time zone offset value: PST8

5 System Management

Supermicro switches can be administered by configuring various operations.

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

Defaults – System Management

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

5.1 Switch Name

Supermicro switches can be assigned a name for identification purpose. The default switch name is SMIS. The switch name is also used as a prompt.
Follow the steps below to configure the Switch Name.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	device name <devname(15)>	Configure Switch Name and prompt. *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 the switch name.

```
SMIS# configure terminal
SMIS(config)# device name switch1
switch1(config)# end
switch1# show system information
Switch Name: switch1
Serial Number: SSC36SR08200014
Switch Management MAC Address: 0c:c4:7a:2c:1f:1d
Switch Base MAC Address: 0c:c4:7a:2c:1f:1e
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
ZTP Config Restore Option: ZTP Enabled
Config Restore Status: Successful
Config Restore Option: Restore
Config Restore ZTP Filename:
Config Restore ZTP TFTP IP Address: 0.0.0.0
Config Restore Local Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 3 hrs 43 mins 6 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No

[NTP] ntp is disabled
   Server      Key   Prefer
=============== =====  ======
 Key #    Key
=======  ==================================
 Time zone offset not set
```

5.2 Switch Contact

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

Follow the steps below to configure the switch contact.

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 64.
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 the startup-config file.

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

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

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

 Key #    Key
=======  ==================================
```

Time zone offset not set

5.3 System Location

Supermicro switches provide option to configure the switch location details.
Follow the steps below to configure the 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 238.
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 the startup-config file.

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

```
SMIS# configure terminal
SMIS(config)# system location "Santa Clara"
SMIS(config)# end
SMIS# show system information
Switch Name: SMIS
Serial Number: SSC36SR08200014
Switch Management MAC Address: 0c:c4:7a:2c:1f:1d
Switch Base MAC Address: 0c:c4:7a:2c:1f:1e
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Santa Clara
Logging Option: Console Logging
Login Authentication Mode: Local
ZTP Config Restore Option: ZTP Enabled
Config Restore Status: Successful
Config Restore Option: Restore
Config Restore ZTP Filename:
Config Restore ZTP TFTP IP Address: 0.0.0.0
Config Restore Local Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 3 hrs 55 mins 33 secs
```

Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
=============== ===== ======
Key # Key
======= ==========
Time zone offset not set

5.4 System MTU

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

Follow the steps below to configure the system MTU.

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 the system MTU.
SMIS# configure terminal
SMIS(config)# system mtu 9200
SMIS(config)# end

SMIS
show interface mtu

Fx0/1 MTU size is 9200

Fx0/2 MTU size is 9200

Fx0/3 MTU size is 9200

Fx0/4 MTU size is 9200

Fx0/5 MTU size is 9200

Fx0/6 MTU size is 9200

Fx0/7 MTU size is 9200

Fx0/8 MTU size is 9200

Fx0/9 MTU size is 9200

Fx0/10 MTU size is 9200

Fx0/11 MTU size is 9200

Fx0/12 MTU size is 9200

Fx0/13 MTU size is 9200

Fx0/14 MTU size is 9200

Fx0/15 MTU size is 9200

Fx0/16 MTU size is 9200

Fx0/17 MTU size is 9200

Fx0/18 MTU size is 9200

Fx0/19 MTU size is 9200

Fx0/20 MTU size is 9200

Fx0/21 MTU size is 9200

Fx0/22 MTU size is 9200

Fx0/23 MTU size is 9200

Fx0/24 MTU size is 9200

Fx0/25 MTU size is 9200

Fx0/26 MTU size is 9200

Fx0/27 MTU size is 9200

Fx0/28 MTU size is 9200

Fx0/29 MTU size is 9200

Fx0/30 MTU size is 9200

Fx0/31 MTU size is 9200

Fx0/32 MTU size is 9200

Fx0/33 MTU size is 9200

Fx0/34 MTU size is 9200

Fx0/35 MTU size is 9200

Fx0/36 MTU size is 9200

Fx0/37 MTU size is 9200

Fx0/38 MTU size is 9200

Fx0/39 MTU size is 9200

Fx0/40 MTU size is 9200

Fx0/41 MTU size is 9200

Fx0/42 MTU size is 9200

Fx0/43 MTU size is 9200

Fx0/44 MTU size is 9200

Fx0/45 MTU size is 9200

Fx0/46 MTU size is 9200

Fx0/47 MTU size is 9200

Fx0/48 MTU size is 9200

Cx0/1   MTU size is 9200

Cx0/2   MTU size is 9200

Cx0/3   MTU size is 9200

Cx0/4 MTU size is 9200

Cx0/5 MTU size is 9200

Cx0/6 MTU size is 9200
SMIS#

5.5 Static MAC

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

Static MAC Characteristics:

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

Forwarding Behavior for Static MAC:

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

Follow the steps below to configure static MAC.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface ([<interface-type><0/a-b,0/c,...>] [<interface-type><0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface <interface-type><iface>	Configure Multicast or unicast static MAC. *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: fx-ethernet – fx cx-ethernet – cx

		interface-id is in slot/port format for all physical interfaces.
Step 3	End	Exits the configuration mode.
Step 4	show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa :aa: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 a static MAC.
SMIS# configure terminal
SMIS(config)# mac-address-table static unicast 90:4e:e5:0c:03:75 vlan 1 interface fx 0/14 status permanent
SMIS(config)# end

SMIS# show mac-address-table static unicast
Vlan Mac Address Status Ports
---- ----------- ------ -----
1 90:4e:e5:0c:03:75 Permanent Fx0/14

Total Mac Addresses displayed: 1

5.6 MAC Aging

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

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 MAC aging to its default value of 300 seconds.

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

```
SMIS# configure terminal
SMIS(config)# mac-address-table aging-time 50000
SMIS(config)# end
SMIS# show mac-address-table aging-time
Mac Address Aging Time: 50000

SMIS# show mac-address-table
Vlan    Mac Address        Type     Ports
----    -----------        ----     -----
1       90:4c:e5:0b:04:77   Learnt   Fx0/21
1       94:d7:23:94:88:d8   Learnt   Fx0/21
Total Mac Addresses displayed: 2
```

6 System Logging (Syslog)

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

- Console
- File
- Server

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

6.1 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)

6.2 Syslog Server

In Supermicro switches, Syslog messages can be re-directed to a Syslog server.
Follow the steps below to configure the Syslog server.

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 a Syslog server.

```
SMIS# configure terminal
SMIS(config)# logging 192.168.1.3
SMIS(config)# end
SMIS# show logging
System Log Information
----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: 192.168.1.3
Facility: Default (local0)
Buffered size: 50 Entries

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

6.3 Console Log

System logging messages can be displayed in switch console.
Follow the steps below to enable the 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)
```

6.4 Log File

System logging messages can be stored as a log file in the switch NVRAM.
Follow the steps below to enable storing logs in a file.

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 the logging of system message in a file.

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

```
SMIS# configure terminal
SMIS(config)#logging file log1
SMIS(config)# end
SMIS# show logging file
LogFile(2 Entries)
<129> Apr 29 10:11:30 2013:INTF-1:Interface Fx0/22 status changed to UP
<129> Apr 29 10:11:31 2013:INTF-1:Interface Fx0/22 status changed to UP
SMIS#
SMIS# show logging
System Log Information
----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: enabled(Number of messages 2)
Log File Name: log1
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: Default (local0)
Buffered size: 50 Entries

LogBuffer: (11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7: Exitting DHCPC Task Init
<135> Apr 29 10:11:05 2013:DHC-7: Entered in DhcpCIntSelectTaskMain fn
<135> Apr 29 10:11:05 2013:DHC-7: Entered in DhcpCSocketOpen fn
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13cf2878 type : 1
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13cf2890 type : 1
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:06 2013:DHC-7: Rcvd Msg 13cf4448 type : 1
<135> Apr 29 10:11:07 2013:DHC-7: Rcvd Event 4
<135> Apr 29 10:11:07 2013:DHC-7: Rcvd Msg 13cf4908 type : 1
<129> Apr 29 10:11:31 2013:INTF-1: Interface Fx0/22 status changed to UP
LogFile(2 Entries)
<129> Apr 29 10:11:30 2013:INTF-1: Interface Fx0/22 status changed to UP
<129> Apr 29 10:11:31 2013:INTF-1: Interface Fx0/22 status changed to UP
```

6.5 Logging Buffer

The log messages are stored in a circular internal buffer in which older messages are overwritten once the buffer is full. The Syslog buffer size is configurable in Supermicro switches.
Follow the steps below to configure the Syslog buffer.

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)
```

6.6 Facility

The Syslog facility provides approximate details regarding which part of the system the Syslog message originated from.
Follow the steps below to configure the Syslog facility.

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 the Syslog facility.

```
SMIS# configure terminal
SMIS(config)#logging facility local5
SMIS(config)# end
SMIS# show logging
System Log Information
----------------------
Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Critical
Log server IP: None
Facility: local5
Buffered size: 50 Entries
LogBuffer: (0 Entries)
LogFile: (0 Entries)
```

6.7 Traps

Supermicro switches provide an option for specifying the type of traps that are to be logged.
Follow the steps below to configure logging traps.

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 traps that can be logged. *Level 0 – Emergencies* Used for logging messages that are equivalent to a panic condition. *Level 1 –Alerts* Used for logging messages that require immediate attention. *Level 2 – Critical* Used for logging critical errors. *Level 3 –Errors* Used for error messages. *Level 4 –Warning* Used for logging warning messages *Level 5 –Notification* Used for logging messages that require attention but are not errors *Level 6 – Informational* Used for logging informational messages. *Level 7 – Debugging* Used for logging debug messages.
Step 3	End	Exits the configuration mode.
Step 4	show logging	Displays the Syslog configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of startup configuration.

The “no logging trap” command resets trap logging to its default value of ‘Critical’.

The example below shows the commands used to configure logging traps.
SMIS# configure terminal
SMIS(config)# logging trap 5
SMIS# end

SMIS(config)# show logging
System Log Information

Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)
File logging: disabled(Number of messages 0)
Log File Name:
File Max Entries: 500
TimeStamp option: enabled
Trap logging: Notification
Log server IP: None
Facility: Default (local0)
Buffered size: 200 Entries
LogBuffer: (11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7: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)

6.8 Clear Log Buffer

The Syslog buffer can be cleared to enable the fresh logging of messages.
Follow the steps below to clear the log buffer.

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 the log buffer.
SMIS# configure terminal
SMIS(config)# clear log buffer
SMIS(config)# end
SMIS# show logging
System Log Information

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

6.8.1 Clear Log File

The Syslog file can be cleared to enable the fresh logging of messages.
Follow the steps below to clear the log file.

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 the log file.
SMIS# configure terminal
SMIS(config)# clear log file
SMIS(config)# end
SMIS# show logging
System Log Information

Syslog logging: enabled(Number of messages 0)
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)

7 Configuration Management

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

7.1 Save Startup-Config

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

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

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

7.2 Save Running Configuration to File

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

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

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

		filename – name of the configuration file.

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

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

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

```
SMIS# show stored-config r1sw1.conf
vlan 1
ports fx 0/1-48 untagged
ports cx 0/1-4 untagged
exit
snmp view restricted 1 excluded nonvolatile
setip igmp enable
setip pim enable
ip pim component 1
exit
```

7.3 Configuring Startup Config File Name

Supermicro switches provide an option to select a file stored in flash memory as the startup configuration file that gets loaded when the switch is powered on or restarted.
Follow the steps below to configure the startup configuration.

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 the switch startup configuration.

```
SMIS# configure terminal
SMIS(config)# set startup-config config2.conf
SMIS(config)# end
SMIS# show startup-config
vlan 1
ports fx 0/1-48 untagged
ports cx 0/1-4 untagged
exit
```

snmp view restricted 1 excluded nonvolatile
setip igmp enable
setip pim enable
ip pim component 1
exit

7.4 Copy Startup-config

Supermicro switches support copying the switch startup configuration to a file in flash or remote location.
Follow the steps below to copy startup-config to a file in a remote location or flash.

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

The example below shows the commands used to copy startup-config to a file in flash.
SMIS# copy startup-config flash:config5.txt
Copied startup-config => flash:/mnt/config5.txt
SMIS#

7.5 Copy File

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

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#

7.6 Deleting a Saved Configuration

Supermicro switches allow for the deletion of the switch startup configuration and other stored configuration files.
Follow the steps below to delete the startup-config file or other configuration files.

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 the startup-config file or another file.

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

7.7 Firmware Upgrade

The switch supports upgrading from both the switch CLI and the ONIE shell. To upgrade from the switch CLI, use the file with the 'swi' extension. To upgrade from the ONIE console, use the file with the 'installer' extension.

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

7.7.1 Firmware Upgrade from Switch CLI

Follow the steps below to update the firmware image from the switch CLI:

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

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

```
SMIS# firmware upgrade tftp://100.100.100.1/SSE-X3548-fw-1.0.1.4.swi
```

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

7.7.2 Firmware Upgrade from ONIE Shell

Follow the steps below to update the firmware image from the ONIE shell:

Step	Command	Description
Step 1	Boot the switch	Boot the switch by powering on. If the switch is already on, use the ‘reload’ command to reboot the switch.
Step 2	From the grub menu, choose the ‘ONIE’ option and press enter.	The grub menu remains for only 4 seconds, after 4 seconds the switch will automatically boot from the ‘Supermicro SSE-X3548 Switch’ option, so, use the down arrow quick enough to move the cursor.
Step 3	From the ONIE menu, choose the ‘ONIE: Install OS’ option and press enter.	After 4 seconds the switch will automatically boot to the ONIE shell from the ‘ONIE: Install OS’ option.
Step 4	onie-discovery-stop	This step stops ONIE from discovering installer files from the network. Stopping the discovery helps stop the discovery messages on the console and prevents the switch from installing from the random ONIE source connected to the network.
Step 5	scp <username>@<hostname>:/<path>/SSE-X3548-fw-x.x.x.x.installer ./	Username is the login user on the remote Linux server. Use the firmware file with the extension ‘installer’.
Step 6	Type ‘y’ and press enter to confirm when the switch prompts “Do you want to continue connecting? (y/n)”.	
Step 7	onie-nos-install ./SSE-X3548-fw-x.x.x.x.installer	The switch will install the firmware and reboot with new firmware.

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

ONIE:/ # onie-discovery-stop
ONIE:/ # scp admin@10.10.10.10:/home/tftp/SSE-X3548-fw-1.0.1.4.installer ./
ONIE:/ # onie-nos-install ./SSE-X3548-fw-1.0.1.4.installer

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

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

7.8 Boot-up Options

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

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 the startup-config file.

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

```
SMIS# configure terminal
SMIS(config)# set boot-up fallback
SMIS(config)# end
SMIS# show system information
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
ConfigSave IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 0 mins 53 secs
Boot-up Flash Area: Fallback
NTP Broadcast Mode: No
[NTP] ntp is disabled
```

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

7.9 Reset to Factory Defaults

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

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 stored configurations, files on the flash memory, user accounts and the management IP address.

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

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

8 Zero Touch Provisioning

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

SSE-X3548S/R switches come with the default management IP address set to DHCP mode. When switches boot up, the management IP address is received from the DHCP server. The DHCP server can also be configured to supply the switch configurations and firmware image when assigning IP addresses to Supermicro switches.

ZTP is enabled by default in Supermicro switches.

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

8.1 ZTP Config Restore

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

8.1.1 DHCP Server Configuration

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

1. Configuration File Name
2. TFTP Server IP Address

Configuration File Name

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

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

TFTP Server IP Address

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

The TFTP server's IP address is sent to switches from the DHCP server using standard DHCP option 66, ***tftp-server-name***. This field needs to be configured in IP address format (e.g. xxx.xxx.xxx.xxx). Switches cannot accept server names, as domain name resolution is not supported.

These options can be added to dhcpd.conf as shown in the example below.

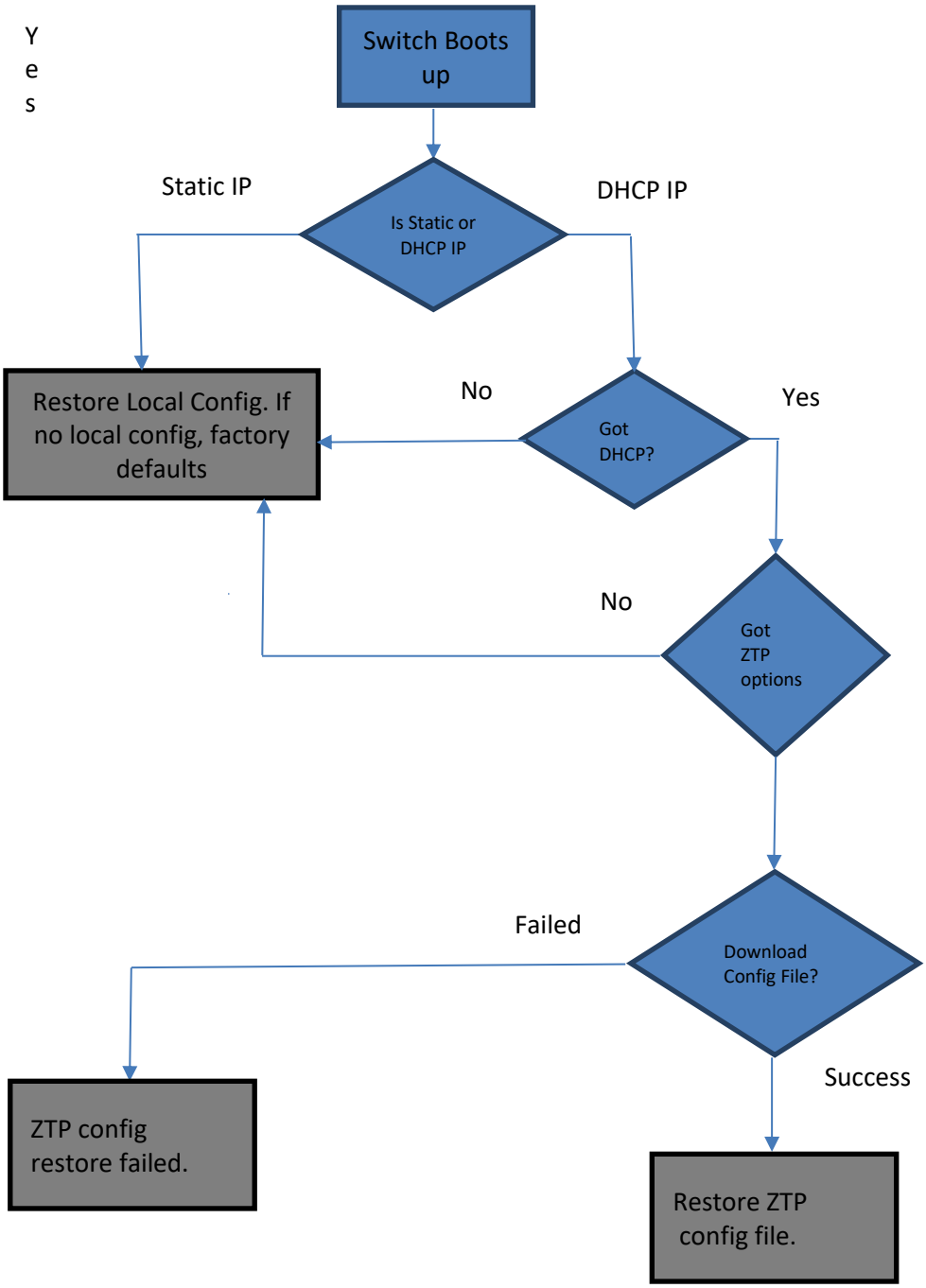
```
option space smc-op;
option smc-op.config-file-name code 1 = text;
option smc-op-encapsulation code 43 = encapsulate smc-op;

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

The lines in **bold** are newly required, other lines are shown for clarity.
Need to add the lines below to define option 43.1 for Supermicro switches.

8.1.2 Switch Configuration Restore

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

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



8.2 ZTP Info

The “show system information” command in CLI displays the ZTP related information, including the following:
ZTP Config Restore Option - Default ZTP Enabled
Config Restore ZTP Filename - The name of the configuration file restored using ZTP. If ZTP restore is not applied, this field will be empty.
Config Restore ZTP TFTP IP Address – The IP address of the TFTP server from where the ZTP config file is downloaded. If ZTP restore is not applied, this field will be empty.
The “Config Restore Option” will also show “ZTP Restore” if a ZTP restore is attempted.
This information can be seen in the web interface on the “system settings” page in the “system management” group.

8.3 ZTP Firmware Upgrade

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

8.3.1 DHCP Server Configuration

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

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

Firmware Image File Name
The firmware image name is sent to switches from the DHCP server using vendor specific option 43 in sub option 04.
This simple text field carries the firmware image file name with the path in respect to the TFTP server root directory. If this file is kept in the TFTP root directory in a TFTP server, this field is a simple file name.

TFTP Server IP Address
The configuration file needs to be available on a TFTP server for the switch to download.
TFTP server IP address is sent to switches from the DHCP server using standard DHCP option 66, ***tftp-server-name***. This field needs to be configured in IP address format (e.g. xxx.xxx.xxx.xxx). Switches cannot accept server names, as domain name resolution is not supported.

These options can added to dhcpd.conf as shown in the below example.

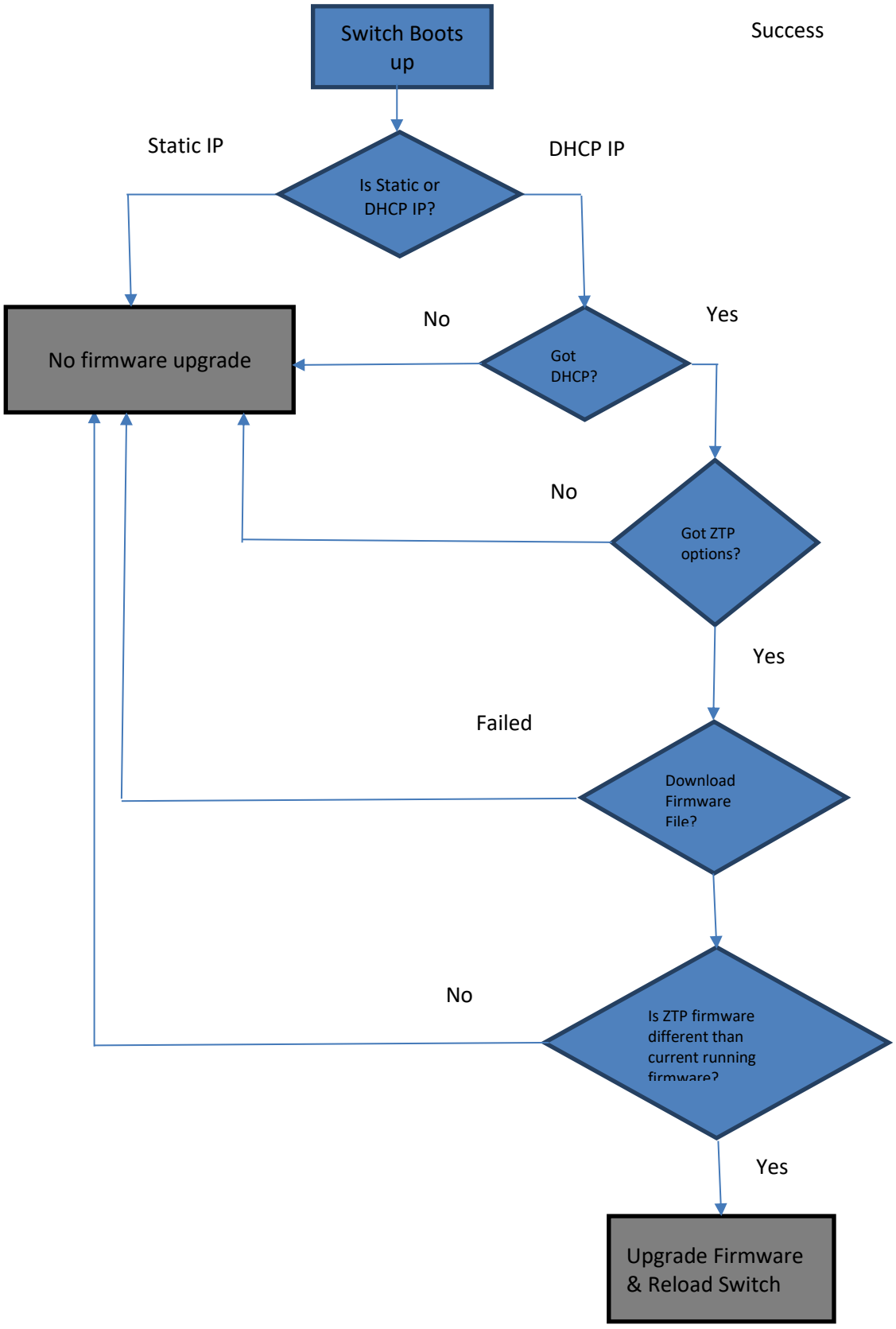
```
option space smc-op;
option smc-op.config-file-name code 1 = text;
option smc-op.fw-img-file-name code 4 = text;
option smc-op-encapsulation code 43 = encapsulate smc-op;

# network for Supermicro switches
subnet 172.31.0.0 netmask 255.255.0.0 {
  range 172.31.30.10 172.31.30.79;
  # the below lines added for automatic restore of configuration
  option smc-op.config-file-name "smcSwitch.conf";
  option tftp-server-name "172.31.43.59";
  option smc-op.fw-img-file-name "SSE-X3548-fw-1.0.1.4.swi";

}
```

The lines in **bold** are newly required, other lines are shown for clarity.
Need to add the below lines to define option 43.1 for Supermicro switches.

8.3.2 Switch Firmware Upgrade

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

The diagram below shows how a switch upgrades the firmware in ZTP.


Switch Boots up
Success
Static IP
DHCP IP
Is Static or DHCP IP?
No
Yes
No firmware upgrade
Got DHCP?
No
Got ZTP options?
Yes
Failed
Download Firmware File?
No
Is ZTP firmware different than current running firmware?
Yes
Upgrade Firmware & Reload Switch

8.4 Disable ZTP

If a customer prefers not to use ZTP and wants to disable ZTP for any reason, it can be done. When ZTP is disabled, a switch always loads the local configuration file. If no local configuration file is available, a switch comes up with a default configuration. Similarly when ZTP is disabled, a switch does not upgrade firmware automatically.
To disable ZTP in CLI, please use the “ztp disable” command in config mode.
To enable ZTP back in CLI, please use the “ztp enable” command in config mode.
This option can be enabled or disabled in the web interface on “system settings” page in the “system management” group.

8.5 DHCP Vendor Class

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

The SSE-X3548S/R switch advertises the vendor class as “SSE-X3548S”.

This vendor class information can be used in DHCP servers to send ZTP options only to the relevant switch models.
The example below shows a DHCP server configuration that uses vendor class information to send ZTP options for Supermicro switch SSE-X3548S/R.

```
class "vendor-class" {
   match option vendor-class-identifier;
}
option space smc-op;
option smc-op.config-file-name code 1 = text;
option smc-op.fw-img-file-name code 4 = text;
option smc-op-encapsulation code 43 = encapsulate smc-op;
subnet 172.31.0.0 netmask 255.255.0.0 {
  range 172.31.30.10 172.31.30.79;
  subclass "vendor-class" "SSE-X3548S" {
    option smc-op.config-file-name "iss-11.conf";
    option smc-op.fw-img-file-name "SSE-X3548-fw-1.0.1.4.swi";
    option tftp-server-name "172.31.33.5";
  }
}
```

9 Tracking Uplink Failures

The Uplink Failure Tracking Feature (ULFT) is useful for Supermicro switches. This helps servers move to down stream Ethernet ports in case any switch uplink fails.
The user can configure one or more groups for ULFT. Each group can have one or more uplinks and one or more downstream ports.

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 fx 0/1 to fx 0/14 when uplink interfaces Cx 0/1 and Cx 0/2 go down:

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

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

10 Loop Protection

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

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

This feature detects networks loops by transmitting Ethernet control packets.

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

10.1 Defaults

Loop Proteciton feature is disabled by default.

10.2 Enable Loop Protection

Loop Protection feature need to be enabled both globally and also on the interface level.
It can be enabled on all the interfaces or on selected interfaces.
Use the below commands to enable loop protection feature.

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

10.3 Disable Loop Protection

Loop Protection feature need to be disabled both globally and also on the interface level.
To disable loop protection on particular interface, use the below commands.

Step	Command	Description

Step 1	**configure terminal**	Enters the configuration mode
Step 2	***interface <ifname> <ifid>***	Enter the interface configuration mode
Step 3	***no loop-protect***	Disabling the loop protection feature on this interface
Step 4	**End**	Exits the configuration mode.
Step 5	***show loop protection***	Displays the loop protection configuration.
Step 6	**write startup-config**	Optional step – saves this configuration to be part of startup configuration.

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

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

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Web Site:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Web Site:	www.supermicro.com.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Web Site:	www.supermicro.com.tw