SUPERMICRO®

L2/L3 Switches

System

Configuration Guide

Revision 1.0

The information in this USER'S MANUAL 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 gf67cbbwhole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

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

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa 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.

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

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

Manual Revision 1.0

Release Date: August 30, 2013

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2013 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Contents

1 System Configuration Guide

This document describes the system features supported in Supermicro Layer 2/Layer 3 switch products.

This document covers the system configurations for the below listed Supermicro switch products.

Top of Rack Switches	Blade Switches
• SSE-G24-TG4 • SSE-G48-TG4 • SSE-X24S • SSE-X3348S • SSE-X3348T	• SBM-GEM-X2C • SBM-GEM-X2C+ • SBM-GEM-X3S+ • SBM-XEM-X10SM

The majority of this document applies to all the above listed Supermicro switch products. In any particular sub section however, the contents might vary across these switch product models. In those sections the differences are clearly identified with reference to particular switch product models. If any particular switch product model is not referenced, the reader can safely assume that the content is applicable to all the above listed models.

> Throughout this document, the common term "switch" refers to any of the above listed Supermicro switch product models unless a particular switch product model is noted.

1.1 Management IP

Supermicro switches come with a default static management IP address of 192.168.100.102. In TOR switches, the management IP address is assigned to a default VLAN 1 interface. The management IP is accessible through all the switching ports by default.

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

manage blade switches through front panel switching ports, configure a layer 3 VLAN interface with the required IP address.

Defaults – Management IP

Parameter	Default Value
IP Address	192.168.100.102
Broadcast Address	255.255.255.255
Gateway	0.0.0.0

1.1.1 Static Management IP Address Configuration

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>]**	Configures the management interface IP address manually. *ip-address* – A valid IPv4 Address. *ip-address/prefix-length* - A valid IPv4 Address with a prefix length value 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

1.1.2 Management IP Address – DHCP Configuration

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

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 the 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 the start-up configuration.

The **"no ip address dhcp"** command disables the configuring of the management interface IP address through the 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

1.1.3 Default IP Gateway

To configure the default gateway IP address in blade switches, follow the steps below.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ip gateway <ip-address>**	Configures the IP gateway address. *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 the start-up configuration.

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

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

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

In TOR switches, the above "ip gateway" command is not supported. To configure the gateway IP address use the "ip route" command.

To configure default gateway address in TOR switches, follow the steps below.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ip route 0.0.0.0 0.0.0.0 <ip-address>**	Configure the IP gateway address. *ip-address* – IP address of a directly connected gateway.
Step 3	**end**	Exits the configuration mode.
Step 4	**show ip route**	Displays the IP route configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

ⓘ The **"no iproute 0.0.0.0 0.0.0.0 <ip-address>"** command removes the gateway configuration.

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

SMIS# configure terminal
SMIS(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.1**
SMIS(config)# end

1.2 Management Access

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

- User name and password
- Enable password
- Authorized managers

Defaults – Management Access

Parameter	Default Value
User Name/Password/Privilege	ADMIN/ADMIN/15 stackuser/stack123/1
Privilege (for configured users)	1
Enable Password	ADMIN
IP Authorized Managers	None

1.2.1 User Login

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

Users with a 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>]**	Configures the username and password. *user-name*–Alphanumeric with a character length of 1-20 *password* – Alphanumeric with a character length of 1-20 *privilege* - Specify 1-15 for any of the privilege levels
Step 3	**end**	Exits the configuration mode.
Step 4	**list users**	Displays the users available in the switch.
	show users	Displays the users that are currently logged in.

The *username* configuration is saved automatically as part of the start-up configuration. Configured users are not displayed with the '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
stackuser   1
user1   15

SMIS# **show users**

 Line   User   Peer-Address
0 con   user1   Local Peer

1.2.2 Enable

Supermicro switches provide support for configuring access to various CLI commands. This is achieved by *Enable* password and *privilege levels*. A total of 15 privilege levels can be specified.

Follow the steps below to enable a privilege level.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**enable [<1-15> Enable Level]**	Enables a privilege level. *Enable Level* – Specify 1-15 for any of the privilege levels
Step 3	**end**	Exits the configuration mode.

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

SMIS# **enable15**

1.2.3 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>**	Configures password for a particular privilege level. *Level* – Specify 1-15 for 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 the start-up configuration. Enable password configuration is not displayed with 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**

1.2.4 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 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 the 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] [http s] [ssh]] | Configures 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, from 1-32.

interface-type – Specifies the interface type through which the IP authorized manager can access the switch. May be any of the following:
gigabit ethernet – gi
extreme-ethernet – ex
qx-ethernet – qx
vlan

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

vlan -Specifies the vlan id through which the IP authorized manager can access the switch.

service – Specifies 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 the startup configuration.

If IP Authorized Managers are configured in a Supermicro switch, access to switch via telnet, ssh, etc. is possible only by those hosts given access. Other hosts will not be permitted access to the switch.

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

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

SMIS# configure terminal
SMIS(config)# **authorized-manager ip-source 200.200.200.10 service telnet**
SMIS(config)# **authorized-manager ip-source 100.100.100.10 service http**
SMIS(config)# end

SMIS# **show authorized-managers**

IP Authorized Manager Table

IP Address: 100.100.100.10
IP Mask: 255.255.255.255
Services allowed: HTTP
Ports allowed: Gi0/1, Gi0/2, Gi0/3, Gi0/4
        Gi0/5, Gi0/6, Gi0/7, Gi0/8
        Gi0/9, Gi0/10, Gi0/11, Gi0/12
        Gi0/13, Gi0/14, Gi0/15, Gi0/16
        Gi0/17, Gi0/18, Gi0/19, Gi0/20
        Gi0/21, Gi0/22, Gi0/23, Gi0/24
        Ex0/1, Ex0/2, Ex0/3
Vlans allowed: All Available Vlans

IP Address: 200.200.200.10
IP Mask: 255.255.255.255
Services allowed: TELNET
Ports allowed: Gi0/1, Gi0/2, Gi0/3, Gi0/4
        Gi0/5, Gi0/6, Gi0/7, Gi0/8
        Gi0/9, Gi0/10, Gi0/11, Gi0/12
        Gi0/13, Gi0/14, Gi0/15, Gi0/16
        Gi0/17, Gi0/18, Gi0/19, Gi0/20
        Gi0/21, Gi0/22, Gi0/23, Gi0/24
        Ex0/1, Ex0/2, Ex0/3
Vlans allowed: All Available Vlans

1.3 Web Access

Supermicro switches support a Web management interface. Some of the web management interface access configurations are configurable through CLI commands.

Defaults – Web Access

Parameter	Default Value
HTTP	Enabled
HTTP Port	80

WEB Session Timeout	600 seconds
Statistics Refresh Timer	0 seconds

1.3.1 HTTP Enable/Disable

Hyper Text Transfer Protocol (HTTP) is enabled by default in Supermicro switches.

Follow the steps below to disable HTTP.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**set ip http {enable	disable}**	Disables HTTP.
Step 3	**end**	Exits the configuration mode.
Step 4	**show http server status**	Displays the HTTP server configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

> The **"set ip http enable"** command enables HTTP.

The example below shows the commands used to disable HTTP.

SMIS# configure terminal
SMIS(config)# **set ip http disable**
SMIS(config)# end

SMIS# **show http server status**

HTTP server status: Disabled
HTTP port is: 80

When HTTP is enabled, Supermicro switches can be accessed from a web browser by specifying *http:/<management-ip-address>*.

1.3.2 HTTP Port

The default HTTP port is 80. The HTTP port can be modified by the user.

Follow the steps below to configure the HTTP port.

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

Step 2	ip http port <port-number(1-65535)>	Configures the HTTP port. *port-number* – Port number specified as an integer from 1-65535.
Step 3	end	Exits the configuration mode.
Step 4	show http server status	Displays the HTTP server configuration.
Step 5	write startup-config	Optional step – saves this configuration to be part of the startup configuration.

> HTTP status must be disabled before changing the HTTP port configuration.
>
> The "**no ip http port**" command resets the HTTP port to its default value of 80.

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

SMIS# configure terminal
SMIS(config)#**ip http port 500**
SMIS(config)# end

SMIS# **show http server status**

HTTP server status: Enabled
HTTP port is: 500

1.3.3 WEB Session Timeout

When a user session in the web interface is inactive, the user is logged out. In Supermicro switches, the session timeout for inactive WEB access users is configurable. The default web session time out value is 600 seconds.

Follow the steps below to configure the web session timeout.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode.
Step 2	web session-timeout <integer(1-9999)>	Configures the web idle session timeout to between 1-9999 seconds.
Step 3	end	Exits the configuration mode.
Step 4	write startup-config	Optional step – saves this configuration to be part of the startup configuration.

The example below shows the commands used to configure a web session timeout.

SMIS# configure terminal

SMIS(config)# **web session-timeout 500**
SMIS(config)# end

1.3.4 Statistics Refresh Timer

The statistics pages can be configured to automatically refresh periodically. The web statistics refresh timer is configurable through a CLI command.

Follow the steps below to configure the Statistics Refresh Timer.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**statistics refresh-timer <integer(0-9999)>**	Configures the Statistics Refresh Timer to between 1-9999 seconds.
Step 3	**end**	Exits the configuration mode.
Step 4	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The example below shows the commands used to configure the Statistics Refresh Timer.

SMIS# configure terminal
SMIS(config)# **statistics refresh-timer 5000**
SMIS(config)# end

1.4 Interface Properties

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

Defaults – Interface Properties

Parameter	Default Value
MTU	1500 bytes
Speed	For 1 – 1Gbps For 10 – 10Gbps For 40 – 40Gbps
Negotiation	For 1G interfaces – Auto For 10GBaseT interfaces – Auto For all other types of 10G interfaces – No negotiation For 40G interfaces - No negotiation
Storm-control	Disabled
Description	None
Duplex Operation	Full
Flow Control	Off

1.4.1 Description

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

Follow the steps below to configure the interface description string.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**interface *<interface-type><interface-id>*** or **interface range** *<interface-type><interface-id> ….*	Enters the interface configuration mode. *interface-type* – may be any of the following: gigabitethernet – gi extreme-ethernet – ex qx-ethernet – qx vlan *interface-id* is in *slot/port* format for all physical interfaces. It may be the VLAN identifier for VLAN interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20** If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	**description <string>**	Configures the interface description.

		String – alphanumeric with a character length of 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 the startup configuration.

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

SMIS# configure terminal
SMIS(config)# interface Gi 0/22
SMIS(config-if)# **description server1-server2**
SMIS(config-if)# end

SMIS# **show interface description**

```
Interface   Status  Protocol  Description
---------   ------  --------  -----------
Gi0/1     up     down
Gi0/2     up     down
Gi0/3     up     down
Gi0/4     up     down
Gi0/5     up     down
Gi0/6     up     down
Gi0/7     up     down
Gi0/8     up     down
Gi0/9     up     down
Gi0/10    up      down
Gi0/11    up      down
Gi0/12    up      down
Gi0/13    up      down
Gi0/14    up      down
Gi0/15    up      down
Gi0/16    up      down
Gi0/17    up      down
Gi0/18    up      down
Gi0/19    up      down
Gi0/20    up      down
Gi0/21    up      down
Gi0/22    up      up       server1-server2
Gi0/23    up      down
Gi0/24    up      down
Ex0/1     up      down
```

Ex0/2   up   down
Ex0/3   up   down

1.4.2 Negotiation

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

Auto negotiation is enabled by default in all 1Gig interfaces and also on the 10GBaseT interfaces. In other types of 10Gig interfaces and 40Gig interfaces, auto negotiation is not supported.

Follow the steps below to configure Interface Negotiation.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**interface <*interface-type*><*interface-id*>** or **interface range** <*interface-type*><*interface-id*> ….	Enters the interface configuration mode. *interface-type* – may be any of the following: gigabit ethernet – gi extreme-ethernet – ex *interface-id* is in *slot/port* format for all physical interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20**

			If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step3	**negotiation**		Enables 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 the startup configuration.

The **"no negotiation"** command disables interface negotiation.

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

SMIS# configure terminal
SMIS(config)# interface Gi 0/22
SMIS(config-if)# **no negotiation**
SMIS(config-if)# end

SMIS# **show interface status**

```
Port      Status         Duplex  Speed     Negotiation
----      ------         ------  -----     -----------
Gi0/1     not connected  Full    1 Gbps    Auto
Gi0/2     not connected  Full    1 Gbps    Auto
Gi0/3     not connected  Full    1 Gbps    Auto
Gi0/4     not connected  Full    1 Gbps    Auto
Gi0/5     not connected  Full    1 Gbps    Auto
Gi0/6     not connected  Full    1 Gbps    Auto
Gi0/7     not connected  Full    1 Gbps    Auto
Gi0/8     not connected  Full    1 Gbps    Auto
Gi0/9     not connected  Full    1 Gbps    Auto
Gi0/10    not connected  Full    1 Gbps    Auto
Gi0/11    not connected  Full    1 Gbps    Auto
Gi0/12    not connected  Full    1 Gbps    Auto
Gi0/13    not connected  Full    1 Gbps    Auto
Gi0/14    not connected  Full    1 Gbps    Auto
Gi0/15    not connected  Full    1 Gbps    Auto
Gi0/16    not connected  Full    1 Gbps    Auto
Gi0/17    not connected  Full    1 Gbps    Auto
Gi0/18    not connected  Full    1 Gbps    Auto
```

```
Gi0/19    not connected   Full    1 Gbps    Auto
Gi0/20    not connected   Full    1 Gbps    Auto
Gi0/21    not connected   Half    1 Gbps    Auto
Gi0/22    not connected   Full    1 Gbps    No-Negotiation
Gi0/23    not connected   Half    1 Gbps    Auto
Gi0/24    not connected   Half    1 Gbps    Auto
Ex0/1     not connected   Full   10 Gbps    No-Negotiation
Ex0/2     not connected   Full   10 Gbps    No-Negotiation
Ex0/3     not connected   Full   10 Gbps    No-Negotiation
```

1.4.3 Speed

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

1Gb RJ45 interfaces can be configured to operate at 10Mbps, 100Mbps or 1000Mbps speed.

10Gb interfaces in SSE-G24-TG4, SSE-G48-TG4, SBM-GEM-X2C, SBM-GEM-X2C+ and SBM-GEM-X3S+ switches can operate only at the fixed 10Gb speed.

10Gb interfaces in SSE-X24S, SBM-XEM-X10S, SSE-X3348S and SSE-X3348T switches can be configurable to operate at 1Gb or 10Gb speed.

40Gb interfaces are fixed to operate only at the 40Gb speed.

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: gigabitethernet – gi extreme-ethernet – ex *interface-id* is in *slot/port* format for all physical interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-)

		between the start and end interface numbers. E.g.: **int range gi 0/1-10**	
		To provide multiple interfaces or ranges, separate with a comma (,).	
		E.g.: **int range gi 0/1-10, gi 0/20**	
		If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.	
Step 3	**speed { 10 | 100 | 1000 | 10000 }**	Configure the 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 the 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 Gi 0/22
SMIS(config-if)# **speed 10**
SMIS(config-if)# end

SMIS# **show interface status**

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

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

1.4.4 Duplex Operation

Supermicro switches support configuring physical interfaces to full-duplex or half-duplex operation.

Follow the steps below to configure the duplex operation type.

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

			To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10**
			To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20**
			If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	**duplex { full | half }**		Configure as duplex operation.
Step 4	**end**		Exits the configuration mode.
Step 5	**show interface status**		Displays the interface configuration.
Step 6	**write startup-config**		Optional step – saves this configuration to be part of the startup configuration.

The **"no duplex"** command restores the default interface to full duplex operation.

The example below shows the commands used to configure the duplex operation type.

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

SMIS# **show interface status**

```
Port      Status        Duplex  Speed     Negotiation
----      ------        ------  -----     -----------
Gi0/1     not connected Full    1 Gbps    Auto
```

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

1.4.5 MTU

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

Follow the steps below to configure an interface's 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: gigabit ethernet – gi extreme-ethernet – ex qx-ethernet – qx

		vlan port-channel *interface-id* is in *slot/port* format for all physical interfaces. It may be the VLAN identifier for VLAN interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20** If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	**mtu<frame-size(1500-9216)>**	Configure interface MTU to a range of 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 the 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 Gi 0/22
SMIS(config-if)# **mtu 9000**
SMIS(config-if)# end

SMIS# **show interface Gi 0/22**

Gi0/22 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port

Hardware Address is 00:30:48:e3:70:d1
MTU 9000 bytes, Half duplex, 1 Gbps, No Negotiation

HOL Block Prevention enabled.
Input flow-control is off,output flow-control is off

Link Up/Down Trap is enabled

Reception Counters
   Octets: 3549
   Unicast Packets: 0
   Broadcast Packets: 13
   Multicast Packets: 26
   Pause Frames: 0
   Undersize Frames: 0
   Oversize Frames: 0
   CRC Error Frames: 0
   Discarded Packets: 39
   Error Packets: 0
   Unknown Protocol: 0

Transmission Counters
   Octets: 7198
   Unicast Packets: 0
   Non-Unicast Packets: 59
   Pause Frames: 0
   Discarded Packets: 0
   Error Packets: 0

SMIS(config-if)# show interface mtu Gi 0/22

Gi0/22 MTU size is 9000

1.4.6 Flow Control

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

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

Follow the steps below to configure flow control.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**interface *<interface-type><interface-id>*** or **interface range** *<interface-type><interface-id> ….*	Enters the interface configuration mode. *interface-type* – may be any of the following: gigabit ethernet – gi extreme-ethernet – ex qx-ethernet – qx *interface-id* is in *slot/port* format for all physical interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20** If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

Step 3	**flowcontrol { send	receive} { on	off }**	Configure flow control.
		Send – The port can send pause frames but cannot receive pause frames from a connected device.
		Receive – The port cannot send pause frames but can receive pause frames from a connected device.
		On – Enables flow control
		Off - Disables flow control
Step 4	**end**	Exits the configuration mode.
Step 5	**show flow-control [interface <interface-type><interface-id>]**	Displays the Interface Flow control configuration.
Step 6	**write startup-config**	Optional step – saves this configuration to be part of startup configuration.

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

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

SMIS# **show flow-control interface Gi 0/22**
Port   TxFlowControl   Rx FlowControl   Tx Pause   Rx Pause
----   -------------   -------------   --------   --------
Gi0/22   on   off   0   0

1.4.7 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 in the

protocol-stack implementation, 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, then resumes normal forwarding.

Follow the steps below to configure storm control.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**interface** *<interface-type><interface-id>* or **interface range** *<interface-type><interface-id> ….*	Enters the interface configuration mode. *interface-type* – may be any of the following: gigabit ethernet – gi extreme-ethernet – ex qx-ethernet – qx *interface-id* is in *slot/port* format for all physical interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hyphen (-) between the start and end interface numbers. E.g.: **int range gi 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range gi 0/1-10, gi 0/20** If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.

Step 3	storm-control { broadcast	multicast	dlf } level <pps-rate-value (1-10000000)>	Configure storm control for broadcast, multicast or DLF packets.
		Level – threshold level in packets per second from 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 the startup configuration.

> The "no storm-control { broadcast |multicast | dlf } level" command disables storm control.

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

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

SMIS# **show interfaces Gi 0/22 storm-control**

Gi0/22
DLF Storm Control: Disabled
Broadcast Storm Control: Enabled
Broadcast Storm Control: 50000

Multicast Storm Control: Disabled

1.5 Time Management

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

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

Defaults – Time Management

Parameter	Default Value

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

1.5.1 NTP Server

Supermicro switches can synchronize time with a NTP server.

Follow the below steps to configure NTP server parameters.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ntp server <ip_address> [key (1-65535)] [prefer]**	Configure the NTP server. *ip_addr* – IP address of server. *key* – Authentication key for server connectivity in the range of 1-65535. *prefer* –This option can be used to specify a preferred NTP server when multiple NTP servers are configured in the switch. Only one server can be configured as '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 the startup configuration.

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

If the key is configured at a Supermicro switch that's acting as an NTP client, ensure the same key is configured at 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
```

1.5.2 Enable/Disable NTP

NTP is disabled by default in Supermicro switches.

Follow the below steps to enable NTP.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ntp enable**	Enables NTP in the 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 the startup configuration.

i The **"ntp disable"** command disables NTP in the switch. NTP can be enabled in Supermicro switches only after configuring at least 1 NTP server.

The example below shows the commands used to configure NTP.

SMIS# configure terminal
SMIS(config)# **ntp enable**
SMIS(config)#end

SMIS# **show ntp**
[NTP] ntp running unicast mode

```
   Server          Key   Prefer
```

```
============== =====  ======
 200.200.200.10   100   YES
  100.100.100.1   500


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

 Time zone offset not set

1.5.3 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>**	Configures NTP authentication key. *Key-number* –key number in the range of 1-65535, used for MD5. *Key-text* – NTP key text to be used along with the 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 the startup configuration.

The **"no ntp key"** command deletes the NTP authentication key.

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

1.5.4 NTP Broadcast

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

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

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ntp broadcast [authentication]**	Configures the 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 the startup configuration.

i   The **"no ntp broadcast"** command disables the NTP broadcast.

The example below shows the commands used to configure the 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

1.5.5 System Clock

The system clock in Supermicro switches runs from the time the switch starts up and keeps track of the system date and time. The system clock can also be manually configured. System time configured manually will remain accurate until the next restart. Manual configuration of the system clock is useful when the system time cannot be obtained from any other source, such as from 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>**	Configures 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

1.5.6 Timezone

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

Follow the below steps to configure the timezone.

Step	Command	Description

Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**tz offset HH<-12 to 13>:MM<0, 30 or 45>**	Configure the timezone. *HH* – Hour in range -12 to 13. *MM* – Minutes specified as 0, 30 or 45.
Step 3	**end**	Exits the configuration mode.
Step 4	**show system information**	Displays the timezone configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The example below shows the commands used to configure the timezone offset.

SMIS# configure terminal
SMIS(config)# **tz offset 12:30**
SMIS(config)# end

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

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

 Time zone offset value: 12:30

1.6 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

1.6.1 Switch Name

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

Follow the steps below to configure the switch name.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**device name <devname(15)>**	Configures switch name and prompt. *Devname* – Switch name specified with 1-15 alphanumeric characters.
Step 3	**end**	Exits the configuration mode.
Step 4	**show system information**	Displays the system information configuration.

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

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

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

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

[NTP] ntp is disabled

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

 Key #   Key
======= =================================

 Time zone offset not set

1.6.2 Switch Contact

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

Follow the steps below to configure the switch contact.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**system contact <string - to use more than one word, provide the string within double quotes>**	Configures the switch contact.

		String – Contact information entered as a String of maximum length 256.
Step 3	**end**	Exits the configuration mode.
Step 4	**show system information**	Displays the system information configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

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

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

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

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

[NTP] ntp is disabled

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

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

Time zone offset not set

1.6.3 System Location

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

Follow the steps below to configure system location.

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

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

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

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

SMIS# **show system information**
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com
System Location: Santa Clara
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0

Device Up Time: 0 days 0 hrs 51 mins 39 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No

[NTP] ntp is disabled

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

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

 Time zone offset not set

1.6.4 System MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces of the switch is 1500 bytes. MTU size can be increased for all interfaces of the switch at the same time by using 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)>**	Configures system MTU. frame-size – Specifies the MTU of frames from 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 the 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**

Gi0/1   MTU size is 9200

Gi0/2   MTU size is 9200

Gi0/3   MTU size is 9200

Gi0/4   MTU size is 9200

Gi0/5   MTU size is 9200

Gi0/6   MTU size is 9200

Gi0/7   MTU size is 9200

Gi0/8   MTU size is 9200

Gi0/9   MTU size is 9200

Gi0/10 MTU size is 9200

Gi0/11 MTU size is 9200

Gi0/12 MTU size is 9200

Gi0/13 MTU size is 9200

Gi0/14 MTU size is 9200

Gi0/15 MTU size is 9200

Gi0/16 MTU size is 9200

Gi0/17 MTU size is 9200

Gi0/18 MTU size is 9200

Gi0/19 MTU size is 9200

Gi0/20 MTU size is 9200

Gi0/21 MTU size is 9200

Gi0/22 MTU size is 9200

Gi0/23   MTU size is 9200

Gi0/24   MTU size is 9200

Ex0/1   MTU size is 9200

Ex0/2   MTU size is 9200

Ex0/3   MTU size is 9200

1.6.5 Static MAC

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

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

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

Follow the steps below to configure a static MAC address.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**mac-address-table static multicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> interface ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) [forbidden-ports ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]]) [status { permanent	deleteOnReset	deleteOnTimeout }]** **mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)>**	Configures a multicast or unicast static MAC address. *Vlan* – Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are from 1 to 4094. Interface - specifies the interface to which the received packet is forwarded. Valid interfaces include

	interface <interface-type> <iface> [status { permanent | deleteOnReset | deleteOnTimeout }]	physical ports or port channels. *Interface-type* - may be any of the following: gigabit ethernet – gi extreme-ethernet – ex qx-ethernet – qx vlan Port Channel *interface-id* is in *slot/port* format for all physical interfaces. It may be the VLAN identifier for VLAN interfaces. Forbidden-ports - Set of ports forbidden for the VLAN. *Permanent* – Static MAC address is not deleted even after a switch reboot. *deleteOnReset* – Static MAC address is deleted on switch reset/reboot. *deleteOnTimeout* - Static MAC address is deleted along with dynamic MAC entries after the aging time times out.
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 the 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>]** and **no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id(1-4069)> [recv-port <interface-type> <interface-id>]"** commands delete the particular static MAC entry.

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

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

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

SMIS# **show mac-address-table static unicast**

Vlan Mac Address   Status   Ports
---- -----------   ------   -----
1   90:4e:e5:0c:03:75   Permanent   Gi0/14

Total Mac Addresses displayed: 1

1.6.6 MAC Aging

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

Follow the steps below to configure MAC aging.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**mac-address-table aging-time <10-1000000 seconds>**	Configure the MAC Aging time from 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 the startup configuration.

> The **"no mac-address-table aging-time"** command resets the MAC aging to its default value of 300 seconds.

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

SMIS# configure terminal
SMIS(config)# **mac-address-table aging-time 50000**
SMIS(config)# end

SMIS# **show mac-address-table aging-time**

Mac Address Aging Time: 50000

SMIS# **show mac-address-table**

Vlan   Mac Address   Type   Ports
----   -----------   ----   -----
1   90:4c:e5:0b:04:77 Learnt   Gi0/21
1   94:d7:23:94:88:d8 Learnt   Gi0/21

Total Mac Addresses displayed: 2

1.6.7 Port Mirroring

Port mirroring allows network traffic monitoring by copying each incoming and outgoing packet from one port, called the *monitored port,* to another port, called the *monitoring port*. The packets can then be analyzed from the monitoring port.

Supermicro switches support

- only one session of port mirroring at a time
- N:1 source:destination mirroring, i.e. multiple *source ports* can be mirrored by one destination port.

Follow the steps below to configure port mirroring.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**monitor session [session_number 1-1] { destination interface <interface-type> <interface-id>	source interface <interface-type> <interface-id> [{ rx	tx	both }] }**	Configures port mirroring. *session_number* – 1, indicates only one

		session is supported.
		Source – monitored port
		Destination – monitoring port
		interface-type –may be any of the following:
		gigabit ethernet – gi extreme-ethernet – ex qx-ethernet – qx vlan
		interface-id –*i*s in *slot/port* format for all physical interfaces. It may be the VLAN identifier for VLAN interfaces.
		rx – Packets received on source port are monitored (ingress).
		tx – Packets transmitted on source port are monitored (egress).
		both – Packets received and transmitted on source port are monitored.
		NOTE: Source and destination port cannot be the same.
Step 3	**end**	Exits the configuration mode.
Step 4	**show port-monitoring**	Displays the port monitoring configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The **"no monitor session [session_number:1] [{ source interface   <interface-type> <interface-id> |destination interface <interface-type><interface-id > }]"** command deletes port mirroring.

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

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

SMIS# **show port-monitoring**

Port Monitoring is enabled
Monitor Port : Gi0/48

Port	Ingress-Monitoring	Egress-Monitoring
Gi0/1	Disabled	Disabled
Gi0/2	Disabled	Disabled
Gi0/3	Disabled	Disabled
Gi0/4	Disabled	Disabled
Gi0/5	Disabled	Disabled
Gi0/6	Disabled	Disabled
Gi0/7	Disabled	Disabled
Gi0/8	Disabled	Disabled
Gi0/9	Disabled	Disabled
Gi0/10	Disabled	Disabled
Gi0/11	Disabled	Disabled
Gi0/12	Disabled	Disabled
Gi0/13	Disabled	Disabled
Gi0/14	Disabled	Disabled
Gi0/15	Disabled	Disabled
Gi0/16	Disabled	Disabled
Gi0/17	Disabled	Disabled
Gi0/18	Disabled	Disabled
Gi0/19	Disabled	Disabled
Gi0/20	Disabled	Disabled
Gi0/21	Disabled	Disabled
Gi0/22	Enabled	Enabled
Gi0/23	Enabled	Enabled
Gi0/24	Enabled	Enabled

Gi0/25	Enabled	Enabled
Gi0/26	Disabled	Disabled
Gi0/27	Disabled	Disabled
Gi0/28	Disabled	Disabled
Gi0/29	Disabled	Disabled
Gi0/30	Disabled	Disabled
Gi0/31	Disabled	Disabled
Gi0/32	Disabled	Disabled
Gi0/33	Disabled	Disabled
Gi0/34	Disabled	Disabled
Gi0/35	Disabled	Disabled
Gi0/36	Disabled	Disabled
Gi0/37	Disabled	Disabled
Gi0/38	Disabled	Disabled
Gi0/39	Disabled	Disabled
Gi0/40	Disabled	Disabled
Gi0/41	Disabled	Disabled
Gi0/42	Disabled	Disabled
Gi0/43	Disabled	Disabled
Gi0/44	Disabled	Disabled
Gi0/45	Disabled	Disabled
Gi0/46	Disabled	Disabled
Gi0/47	Disabled	Disabled
Gi0/48	Disabled	Disabled
Ex0/1	Disabled	Disabled
Ex0/2	Disabled	Disabled
Ex0/3	Disabled	Disabled
Ex0/4	Disabled	Disabled

1.7 System Logging (Syslog)

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

- Console
- File
- Server

Defaults – Syslog

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

1.7.1 Enable/Disable Syslog

Syslog is enabled by default in Supermicro switches.

Follow the steps below to disable Syslog.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**logging disable**	Disables 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 the 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)

1.7.2 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 the startup configuration.

The **"no logging <ip-address>"** command deletes the Syslog server.

The example below shows the commands used to configure the 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)

1.7.3 Console Log

System Logging messages can be displayed in the 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**	Enables 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 the startup configuration.

The **"no logging console"** command disables console logging.

The example below shows the commands used to enable the 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)

1.7.4 Log File

System Logging messages can be stored as a log file in a switch's 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)>**	Enables storing logs in a file. *Filename* – Specifies a file name of up to 32 characters. *Short* – Specifies entries that can be stored in a file from 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 the startup configuration.

The **"no logging file"** command disables the logging of system messages 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 Gi0/22 status changed to UP
<129> Apr 29 10:11:31 2013:INTF-1:Interface Gi0/22 status changed to UP
SMIS#

SMIS# **show logging**

System Log Information

Syslog logging: enabled(Number of messages 0)
Console logging: disabled(Number of messages 0)

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

LogBuffer(11 Entries)
<135> Apr 29 10:11:05 2013:DHC-7:Exitting DHCPC Task Init

<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCIntSelectTaskMain fn

<135> Apr 29 10:11:05 2013:DHC-7:Entered in DhcpCSocketOpen fn

<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Event 4

<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf2878 type : 1

<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf2890 type : 1

<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Event 4

<135> Apr 29 10:11:06 2013:DHC-7:Rcvd Msg 13cf4448 type : 1

<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Event 4

<135> Apr 29 10:11:07 2013:DHC-7:Rcvd Msg 13cf4908 type : 1

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

LogFile(2 Entries)
<129> Apr 29 10:11:30 2013:INTF-1:Interface Gi0/22 status changed to UP
<129> Apr 29 10:11:31 2013:INTF-1:Interface Gi0/22 status changed to UP

1.7.5 Logging Buffer

The log messages are stored in a circular internal buffer in which older messages are overwritten once the buffer is full. 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)>**	Configures the Syslog buffer with the

		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 the 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 the 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)

1.7.6 Facility

The Syslog Facility provides the approximate details on 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|}	Configures the 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 the startup configuration.

The **"no logging 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)

1.7.7 MAC Table Logging

Supermicro switches support the logging of MAC address table updates.

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

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**logging mac-address-table**	Enables the logging of MAC address table updates.
Step 3	**end**	Exits the configuration mode.
Step 4	**show logging**	Displays the Syslog configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

> The "no **logging mac-address-table**" command disables the logging of MAC address table updates.

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

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

1.7.8 Trap

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

Follow the steps below to configure the logging of 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 }]**	Configures the logging of 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 the startup configuration.

The **"no logging trap"** command resets the trap logging to its default value of 'Critical'.

The example below shows the commands used to configure the logging of 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 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)

1.7.9 Clear Log Buffer

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

Follow the steps below to clear the logging buffer.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**clear log buffer**	Clears the 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 the startup configuration.

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

SMIS# configure terminal
SMIS(config)# **clear log buffer**
SMIS(config)# end

SMIS# **show logging**

System Log Information

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

LogBuffer(0 Entries)

LogFile(0 Entries)

1.7.10   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**	Clears the log 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 the 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)

1.8 Security Features

Supermicro switches support four methods of user authentication:

- **RADIUS** – Remote Authentication Dial-In User Service (RADIUS) uses AAA service for ID verification, granting access and tracking the actions of remote users.
- **TACACS** – *Terminal Access Controller Access Control System (TACACS)* provides accounting information and administrative control for authentication and authorization. RADIUS encrypts only passwords, whereas TACACS encrypts usernames as well, making it more secure.

- **SSH** - *Secure Shell (SSH)* is a protocol for a secure remote connection to a device. SSH provides more security than telnet by encrypting messages during authentication.
- **SSL** –*Secure Socket Layer (SSL)* provides server authentication, encryption and message integrity as well as HTTP client authentication.

1.8.1 Login Authentication Mode

Supermicro switches allow for the configuration of the user login authentication mechanism.

Follow the steps below to configure the login authentication mechanism.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**login authentication { local	radius	tacacs }**	Configures the login authentication mechanism to be used for switch access. Local – Uses the local database in a switch to authenticate users. Radius – Uses a RADUIS server to authenticate users. Tacacs – Uses a TACACS server to authenticate users.
Step 3	**end**	Exits the configuration mode.
Step 4	**show system information**	Displays the login authentication mechanism.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The **"no login authentication"** command resets the login authentication to its default of 'local'.

The example below shows the commands used to configure the login authentication mechanism.

SMIS# configure terminal
SMIS(config)# **login authentication radius**
SMIS(config)# end

SMIS# **show system information**
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc

SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com/support
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: RADIUS
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 15 mins 43 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No

[NTP] ntp is disabled

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

 Key #   Key
======= ===================================

 Time zone offset not set

1.8.2 RADIUS

A sequence of events occurs during RADIUS client-server communication whenever a user logs in.

- The username and password are encrypted by the client and sent to the RADIUS server.
- The client receives a response from the RADIUS server:
  - ACCEPT—User authentication is successful.
  - REJECT—User authentication failed.   User is prompted to re-enter the username/password, or access is denied.
  - CHALLENGE—Additional data is requested from the user.
  - CHALLENGE PASSWORD—User is prompted to select a new password.

Along with ACCEPT or REJECT packets, service options (Telnet, SSH, rlogin, or privileged EXEC services) and connection parameters like user timeouts are sent by the RADIUS server.

Defaults – RADIUS

Parameter	Default Value
Server	None

Timeout	3 seconds
Re-transmit	3 seconds
Key	None

1.8.2.1 RADIUS Server

Supermicro switches function as a RADIUS client. The RADIUS server that is to be contacted for authentication can be configured in the switch.

Follow the steps below to configure the RADIUS server's parameters.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**radius-server host <ip-address> [timeout <1-120>] [retransmit <1-254>] key <secret-key-string> [type {authenticating	accounting	both}]**	Configure the RADIUS server for the purpose of authenticating or accounting or both. *ip-address* – server's IP address. *timeout* – Specifies the RADIUS server timeout, from 1-120 *retransmit* – Specifies the number of retries to attempt to connect to the RADIUS server, from 1-254 *key* – Specifies the authentication key
Step 3	**end**	Exits the configuration mode.
Step 4	**show radius server** **show radius statistics**	Displays the RADIUS configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The **"no radius-server host <ip-address>"** command deletes the RADIUS client.

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

SMIS# configure terminal
SMIS(config)# **radius-server host 200.200.200.1 timeout 50 retransmit 250 key key1**
SMIS(config)# end

SMIS# **show radius server**

Radius Server Host Information

Index: 1
Server address: 200.200.200.1
Shared secret: key1
Radius Server Status: Enabled
Response Time: 50
Maximum Retransmission: 250

SMIS# show radius statistics

Radius Server Statistics

Index: 1
Radius Server Address: 200.200.200.1
UDP port number: 1812
Round trip time: 0
No of request packets: 0
No of retransmitted packets: 0
No of access-accept packets: 0
No of access-reject packets: 0
No of access-challenge packets: 0
No of malformed access responses: 0
No of bad authenticators: 0
No of pending requests: 0
No of time outs: 0
No of unknown types: 0

1.8.3 TACACS

TACACS provides access control to a switch through a client-server model, similar to RADIUS except that it provides enhanced security by encrypting all messages and reliability via TCP.

Defaults – TACACS

Parameter	Default Value
TACACS server	None
TACACS server re-tries	2
TACACS TCP port	49

1.8.3.1 TACACS Server

Supermicro switches allow for the configuration of multiple TACACS servers. One of these servers provides the authentication support.

Follow the steps below to configure a TACACS server.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**tacacs-server host <ip-address> [single-connection] [port <tcp port (1-65535)>] [timeout <time out in seconds>] key <secret key>**	Configures the TACACS server. *ip-address* – TACACS server's IP-address *single-connection* – When this option is specified, only one connection to one of the configured TACACS servers is permitted. *port* – Specifies the TCP port, from 1-65535 *timeout* - Specifies the TACACS server timeout, from 0 – 255 seconds *key* – Authentication key with a maximum length of 64 characters.
Step 3	**end**	Exits the configuration mode.
Step 4	**show tacacs**	Displays the TACACS configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

The **"no tacacs-server host <ip-address>"** command deletes the TACACS server.

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

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

SMIS# **show tacacs**
Server : 1
    Address: 10.10.10.1

Single Connection: no
TCP port: 500
Timeout: 200
Secret Key: key123
Client uses server: 0.0.0.0
Authen. Starts sent: 0
Authen. Continues sent: 0
Authen. Enables sent: 0
Authen. Aborts sent: 0
Authen. Pass rvcd.: 0
Authen. Fails rcvd.: 0
Authen. Get User rcvd.: 0
Authen. Get Pass rcvd.: 0
Authen. Get Data rcvd.: 0
Authen. Errors rcvd.: 0
Authen. Follows rcvd.: 0
Authen. Restart rcvd.: 0
Authen. Sess. timeouts : 0
Author. Requests sent: 0
Author. Pass Add rcvd.: 0
Author. Pass Repl rcvd.: 0
Author. Fails rcvd.: 0
Author. Errors rcvd.: 0
Author Follows rcvd.: 0
Author. Sess. timeouts : 0
Acct. start reqs. sent: 0
Acct. WD reqs. sent: 0
Acct. Stop reqs. sent: 0
Acct. Success rcvd.: 0
Acct. Errors rcvd.: 0
Acct. Follows rcvd.: 0
Acct. Sess. timeouts: 0
Malformed Pkts. rcvd.: 0
Socket failures: 0
Connection failures: 0

1.8.3.2 Server Re-tries

Supermicro switches will retry transmitting messages to the TACACS server if there is no response from the server. This retry count can be configured by the user.

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

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**tacacs-server retransmit <1-100>**	Configures the TACACS server re-tries from 1-100.

Step 3	**end**	Exits the configuration mode.
Step 4	**show tacacs**	Displays the TACACS configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

> ⓘ The **"no tacacs-server retransmit"** command resets the TACACS server re-tries to its default value.

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

SMIS# configure terminal
SMIS(config)# tacacs-server retransmit 5
SMIS(config)# end

1.8.3.3 TACACS Use-server

Supermicro switches provide an option to configure multiple TACACS servers. Users can specify one of these available servers to be used at a time.

Follow the steps below to configure the TACACS server to be used.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**tacacs use-server address\<ip-address\>**	Configures TACACS server to be used.
Step 3	**end**	Exits the configuration mode.
Step 4	**show tacacs**	Displays the TACACS configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

> ⓘ The **"no tacacs use-server address\<ip-address\>"** command deletes the TACACS client.

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

SMIS# configure terminal
SMIS(config)# **tacacs use-server address 10.10.10.1**
SMIS(config)# end

SMIS# **show tacacs**
Server : 1
     Address: 10.10.10.1
     Single Connection: no

TCP port: 49
Timeout: 200
Secret Key: key123
Server : 2
Address: 50.50.50.1
Single Connection: no
TCP port: 49
Timeout: 5
Secret Key: key789
Client uses server: 10.10.10.1
Authen. Starts sent: 0
Authen. Continues sent: 0
Authen. Enables sent: 0
Authen. Aborts sent: 0
Authen. Pass rvcd.: 0
Authen. Fails rcvd.: 0
Authen. Get User rcvd.: 0
Authen. Get Pass rcvd.: 0
Authen. Get Data rcvd.: 0
Authen. Errors rcvd.: 0
Authen. Follows rcvd.: 0
Authen. Restart rcvd.: 0
Authen. Sess. timeouts: 0
Author. Requests sent: 0
Author. Pass Add rcvd.: 0
Author. Pass Repl rcvd: 0
Author. Fails rcvd.: 0
Author. Errors rcvd.: 0
Author Follows rcvd.: 0
Author. Sess. timeouts: 0
Acct. start reqs. sent: 0
Acct. WD reqs. sent: 0
Acct. Stop reqs. sent: 0
Acct. Success rcvd.: 0
Acct. Errors rcvd.: 0
Acct. Follows rcvd.: 0
Acct. Sess. timeouts: 0
Malformed Pkts. rcvd.: 0
Socket failures: 0
Connection failures: 0

1.8.4 SSH

Supermicro switches can act as a SSH client and support both SSH version 1 and SSH version 2.

Defaults – SSH

Parameter	Default Value
SSH status	Enabled
SSH version compatibility	Off
SSH port	22
SSH Key	RSA
Cipher algorithm	3DES-CBC
SSH version	2
Authentication	HMAC-SHA1

Follow the steps below to configure SSH.

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

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

The example below shows the commands used to configure the SSH.

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

SMIS# **show ip ssh**
Version: Both
Cipher Algorithm: 3DES-CBC
Authentication: HMAC-SHA1

Trace Level: None

SMIS# configure terminal
SMIS(config**)# ip ssh cipher des-cbc**
SMIS(config)# end

SMIS# **show ip ssh**

Version: 2
Cipher Algorithm: DES-CBC
Authentication: HMAC-SHA1
Trace Level: None

SMIS# configure terminal
SMIS(config)# **ip ssh auth hmac-md5**
SMIS(config)# end

SMIS# **show ip ssh**

Version: 2
Cipher Algorithm: 3DES-CBC
Authentication: HMAC-MD5
Trace Level: None

1.8.5 SSL

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

Defaults – SSL

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

1.8.5.1 Secure HTTP (https)

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. *HTTP with SSL encryption (HTTPS)* provides a secure connection to allow functions such as configuring a switch from a Web browser.

Follow the steps below to configure Secure HTTP.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] | crypto key rsa [usage-keys (512|1024)] }**	Configures secure HTTP. *server* – Enables an HTTPS server *ciphersuite* – Specifies one or many of the supported encryption algorithms to be used. *crypto key rsa* – Encryption key, either 512 or 1024.
Step 3	**end**	Exits the configuration mode.
Step 4	**show ip http secure server status**	Displays the SSL configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

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

The example below shows the commands used to configure a secure HTTP.

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

SMIS# **show ip http secure server status**
HTTP secure server status: Disabled
HTTP secure server ciphersuite: RSA-DES-SHA:RSA-3DES-SHA:RSA-EXP1024-DES-SHA:
HTTP crypto key rsa 1024

1.8.5.2 Certificate Signing Request (CSR)

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

Supermicro switches create a Certificate Signing Request (CSR) using an RSA key pair and switch identification.

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

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

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

SMIS# **ssl gen cert-req algo rsa sn SMIS**
-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBADAPMQ0wCwYDVQQDEwRTTUlTMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQChj0JzVX1/gZ4SMGekRdrsAnftWnKHG3VypWTtySqkvTwhnZ206Q2o
cBYJNKY4ZCykOXG81mfUhqPfVLyO8sbK+RYzEeTMX9lw9iq9yOySOlvxY6IoYNsg
O++JS02khz0SAbpRkhtGuwmBiZQtSj+8Ea3dG8ReoixpcYDVVdIrDQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAXR8Nz40QeC8wqwzqy+iozT5iUMKOkelXTE8mDydt
AvRyc7a3EPraGjyOL5W1H94z+wW2wkxXTRzKuLzAEYRH9f84XB2uCAdL+jkuSBJc
5qd3j4yBtOIu/pxOsdKKwuq6LWbi44DCXg97SkE+pOYa7nWojVkjc2SbjvK5CTgG
89s=
-----END CERTIFICATE REQUEST-----

SMIS# **show ssl server-cert**

Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 10 (0xa)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=CA, L=SanJose, O=Supermicro, OU=Switch, CN=Switch/Email
=support@supermicro.com
        Validity
            Not Before: Aug 11 22:18:10 2011 GMT
            Not After : Sep 10 22:18:10 2011 GMT
        Subject: CN=SMIS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:a1:8f:42:73:55:7d:7f:81:9e:12:30:67:a4:45:
                    da:ec:02:77:ed:5a:72:87:1b:75:72:a5:64:ed:c9:
                    2a:a4:bd:3c:21:9d:9d:b4:e9:0d:a8:70:16:09:34:
                    a6:38:64:2c:a4:39:71:bc:d6:67:d4:86:a3:df:54:

```
            bc:8e:f2:c6:ca:f9:16:33:11:e4:cc:5f:d9:70:f6:
            2a:bd:c8:ec:92:3a:5b:f1:63:a2:28:60:db:20:3b:
            ef:89:4b:4d:a4:87:3d:12:01:ba:51:92:1b:46:bb:
            09:81:89:94:2d:4a:3f:bc:11:ad:dd:1b:c4:5e:a2:
            2c:69:71:80:d5:55:d2:2b:0d
        Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
      21:bd:73:5e:96:82:89:13:12:a6:69:e8:9c:e6:fb:a5:0f:bc:
      0b:8d:fd:03:25:68:d9:09:73:58:7f:e1:30:64:d9:3a:99:63:
      6b:d2:ec:37:ea:33:1e:28:11:48:26:94:13:36:aa:08:14:5a:
      7a:c4:f2:14:26:54:9e:d4:b5:2d:a2:c1:ab:fe:7a:2f:b8:f6:
      23:08:93:fb:6b:7e:d9:14:da:09:90:50:b4:76:b0:17:e1:5f:
      53:75:ee:7a:5f:85:dd:90:3c:d4:28:18:ee:5c:64:f5:09:52:
      03:25:3e:f1:ed:5d:80:37:4b:ff:ad:fb:54:d0:24:11:a1:cd:
      32:6c
```

1.8.5.3 SSL Certificate

Each SSL Certificate contains:

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

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

Follow the steps below to configure an SSL server certificate.

Step	Command	Description
Step 1	**ip http secure**	Configure the cipher suite and crypto key RSA of your choice using the "**ip http secure"** command.
Step 2	**ssl gen cert-req algo rsa sn**	Enter the subject name and create a certificate request by using the "**ssl gen cert-req algo rsa sn"** command.
Step 3	**show ssl server-cert**	The "**show ssl server-cert**" command will display the certificate request. Copy & paste these contents to a text file, say a.csr.
Step 4	**Linux commands**	To generate an SSL certificate, an openssl application can be used. The following steps can be executed in any Linux machine to generate SSL certificates. For other openssl

| | | implementation, refer to the openssl documentation to find the equivalent steps.

Execute the commands below in the Linux shell.
1. openssl req -x509 -newkey rsa:1024 -keyout cakey.pem -out cacert.pem
2. openssl x509 -req -in a.csr -out cert.pem -CA cacert.pem -CAkey cakey.pem – Cacreateserial

This would generate the certificate file cert.pem. |
|---|---|---|
| Step 5 | **ssl server-cert** | Open the generate certificate file cert.pem. Delete the first line (---BEGIN CERTIFICATE ---) and last line (----END CERTIFICATE--). Join all the remaining lines together as a single line to avoid line breaks from being processed.

Copy & paste these joined texts at the "**Enter Certificate**" prompt. This prompt appears after entering the "**ssl serv-cert**" command in CLI.

This step would configure the certificate and save it to flash. |
| Step 6 | **show ssl server-cert** | Displays the SSL configuration. |

1.9 Configuration Management

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

1.9.1 Save Startup Configuration

Switch configurations can be saved using the command *write startup-config*. A configuration saved as a startup configuration will be loaded automatically when a 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 an existing switch configuration as the startup configuration.

Step	Command	Description
Step 1	**write startup-config**	Configure writing of switch configuration to a file or startup-configuration.
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.

1.9.2 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***|usb:***filename***}**	Configure the writing of the switch configuration to a file in the local flash memory, in a remote TFTP server or in the external USB memory. *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 external USB memory is available only in SSE-X24S, SSE-X3348S and SSE-X3348T switches.

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

1.9.3 Configuring Startup Configuration 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*>**	Configures the startup configuration 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 gi 0/1-48 untagged
ports ex 0/1-4 untagged
exit
snmp view restricted 1 excluded nonvolatile
set ip igmp enable
set ip pim enable
ip pim component 1
exit

1.9.4 Copy Startup Configuration

Supermicro switches can copy a switch's startup configuration to a file in flash or to a remote location.

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

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

The example below shows the commands used to copy from the startup configuration to a file in flash.

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

1.9.5 Copy File

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

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

Step	Command	Description
Step 1	**copy flash:** *filename***tftp://ipaddress/***filename*	Copies a local flash file to a remote TFTP server.

copy tftp://ip-address/*filename* **flash:** *filename*	Copies a remote file to a local flash.
copy flash: *filename* **flash:** *filename*	Makes a copy of the file in the flash memory.
copy usb: *filename***tftp://ipaddress/***filename*	Copies an external USB flash file to a remote TFTP server in SSE-X24S, SSE-X3348S or SSE-X3348T switches.
copy tftp://ip-address/*filename***usb:** *filename*	Copies a remote file to external USB memory in SSE-X24S, SSE-X3348S or SSE-X3348T switches.
copy usb: *filename***usb:** *filename*	Makes a copy of the file in the USB external memory in SSE-X24S, SSE-X3348S or SSE-X3348T switches. *filename* – name of the configuration file.

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

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

1.9.6 Deleting Saved Configurations
Supermicro switches allow users to delete the switch startup configuration and other stored configuration files.

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

Step	Command	Description
Step 1	**erase startup-config**	Removes the startup configuration.
	erase flash:*filename*	
		Deletes the configuration file from a local flash memory.
	erase usb:*filename*	
		Deletes the configuration file from external USB memory in SSE-X24S, SSE-X3348S or SSE-X3348T switches.
		filename – name of the configuration file.

The example below shows the commands used to erase a startup configuration or a file.

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

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

1.9.7 Firmware Upgrades

Supermicro switches support dual firmware images. The default firmware image is referred as "normal" and the backup firmware image is referred as the "fallback" image.

The "firmware upgrade" command is used to update both the normal and the fallback image.

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

Follow the steps below to update the firmware image:

Step	Command	Description
Step 1	**firmware upgrade { tftp://ip-address/filename} [normal	fallback]**	Updates the firmware image from remote a TFTP server.
	**firmware upgrade { usb:filename} [normal	fallback]**	Updates the firmware image from external USB memory in SSE-X24S, SSE-X3348S and SSE-X3348T switches.

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

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

> By default, a switch boots using the normal firmware image. To boot up using the fallback firmware image, use the command "set boot-up {normal | fallback}".

1.9.8 Boot-up Options

Supermicro switches support dual firmware images as "normal" and "fallback". The switch boots up from the normal firmware image by default. Users can also 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}**	Configures the 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

1.9.9 Reset to Factory Defaults

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

Follow the steps below to reset a switch to its factory defaults.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**reset-to-factory-defaults**	Configures the factory defaults.

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

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

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 the factory defaults, a switch will be reloaded immediately.

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