SSE-F3548S/SSE-F3548SR

SNMP

User's Guide

Revision 1.0

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

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

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

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

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

Manual Revision 1.0
Release Date: 3/2/2020

Document Revision History

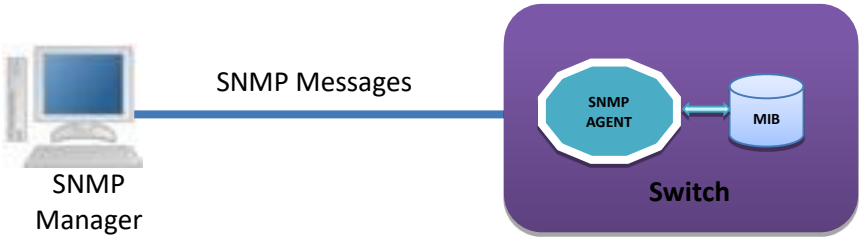
Date	Revision	Description
03/2/2020	1.0	Initial document.

Contents

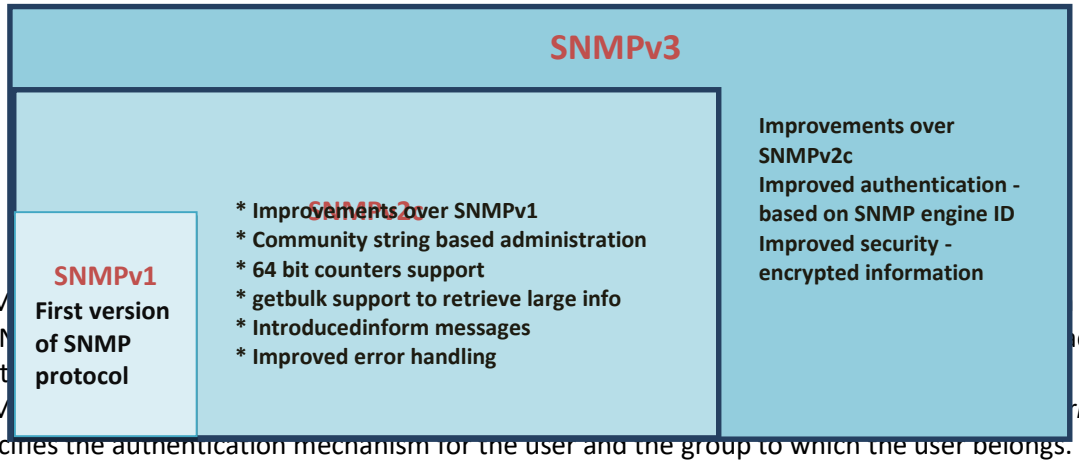
1 SNMP Overview

SNMP helps to monitor and manage the switches from network management systems (NMS). SNMP solutions contain three major components – SNMP manager, SNMP agent and MIB (Management Information Base) as shown in Figure – SNMP-1.
The SNMP MIB contains all the configuration and status information of the switch. MIB is organized in a tree structure with branches and leaf nodes. Each node contains an object of information and is identified with an object identifier (OID). SNMP MIB is stored and maintained in the switch.
The SNMP agent also resides on the switch. It processes the SNMP requests received from the SNMP manager. It sends responses to SNMP managers by retrieving required information from the MIB. It also updates the MIB based on SNMP messages sent by the SNMP managers. SNMP agents also send voluntary traps to SNMP managers. Traps are sent to alert the SNMP managers on events happening on the switch.
The SNMP manager is an NMS application. It monitors and manages switches by communicating to the SNMP agents running on the switch. The SNMP manager application provides command or graphical interfaces to the network administrators to help them manage the networks.

Figure SNMP-1: SNMP Systems



There are three versions of SNMP protocols available.



USM features in SN ccess cont SNM *rity model* specifies the authentication mechanism for the user and the group to which the user belongs. The security models in the Supermicro switch are v1, v2c and v3.
Security level specifies the permitted security within the particular security model. The security levels in Supermicro switches are

- NoAuthNoPriv
- AuthNoPriv

- AuthPriv

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

Security Model	Security Level	Authentication	Encryption	Purpose
V1	noAuthNoPriv	Community string	None	Community string and community user are used to authenticate user login.
V2c	noAuthNoPriv	Community string	None	Community string and community user are used to authenticate user login.
V3	noAuthNoPriv	User name	None	User configuration is used to authenticate user login.
V3	Auth	MD5 or SHA	None	MD5 or SHA algorithm is used to verify user login.
V3	Priv	None	DES	DES is used to encrypt all SNMP messages.

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

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

2 SNMP Support

Supermicro switches support three versions of SNMP:SNMPv1, SNMPv2c and SNMPv3.
A switch supports 50 users, 50 groups, 50 views and 50 views.

3 Interface Numbers

IF-MIB contains information about all the interfaces on the switch. Users can access the interface specific MIB object values using interface index (ifIndex) numbers. The ifIndex numbers are assigned by

switch software for every physical and logical interface. The table below shows ifIndex to interface mapping method.

Interface Type	ifIndex
25 Gig physical interfaces	Starts from 1 and goes up to the maximum number of 25 Gig interfaces available on the switch. 1 to 48
100 Gig physical interfaces	Starts after 1Gig ifIndexes and goes up to the maximum number of 100 Gig interfaces available on the switch. 49 to 54
Port channel interfaces	Starts after 10Gig ifIndexes and goes up to the maximum number of port channel interfaces supported on the switch. 53 to 108
Management IP interfaces	109

4 SNMP Configuration

SNMP Configuration involves configuring user, group, access, view, community etc.

SNMP Users: SNMP users have a specified username, authentication password, privacy password, (if required) and authentication and privacy algorithms to use.

SNMP Groups: When a user is created, it is associated with an SNMP group. SNMPv3 groups are the means by which users are assigned their views and access control policy.

SNMP View: An SNMP MIB view is a defined list of objects within the MIB that can be used to control what parts of the MIB can be accessed by users belonging to the SNMP group that is associated with that particular view. When you want to permit a user to access a MIB view, you include a particular view. When you want to deny a user access to a MIB view, you exclude a particular view.

SNMP Group access: An SNMP group access is essentially an access control policy to which users can be added. Each SNMP group is configured with a security level, and is associated with an SNMP view

There are three possible types of access that can be configured for the users in that SNMP group to have access to an SNMP view.

- ReadView - Specifies Read access for an SNMP view
- WriteView - Specifies Write access for an SNMP view
- NotifyView - Specifies SNMP view for which the group will receive notifications.

The figure below shows the relationship between the various SNMP tables: User, group, access and view.

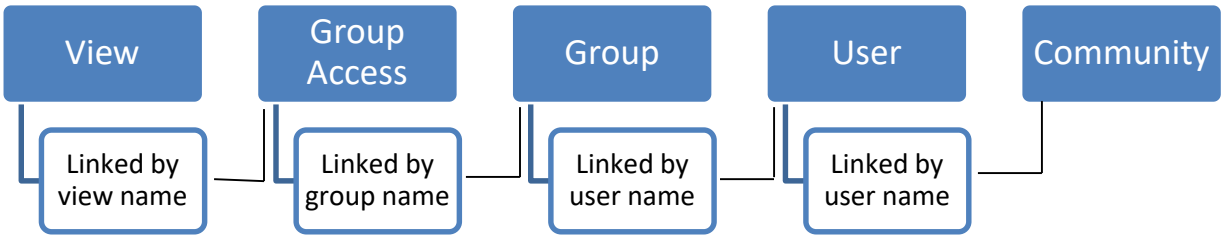


Figure SNMP-2: SNMP - Relationships

The following mapping can exist between the SNMP tables user, group, access and view:

- Multiple users can belong to one group
- An user can belong to multiple groups.
- Multiple groups can be associated with a view.
- Multiple views can be created.
- More than one group can be associated with a particular view.
- More than one view can be associated with a group. For instance, a group can have read access to the entire MIB, but write access only for certain MIB objects.

4.1 Configuration Steps

The sequence of steps for SNMP Configuration in Supermicro switches are:

1. Create a **User** Name
2. Create a **community** name and associate user with the community (Optional).
3. Create a **group** and associate the user name with the group name.
4. The **view** is then defined to include or exclude whole/part MIB sub trees.
5. Define type of **access** for each group for a view.
6. Finally, **traps** can be defined based on the User Name (Optional).

5 SNMP Defaults

Function	Default Value
SNMP Agent Status	Enabled
SNMP Sub-Agent Status	Disabled
Version	3
Engine Id	80.00.08.1c.04.46.53
Communities	PUBLIC, NETMAN
Users	initial, TemplateMD5, TemplateSHA
Authentication (for default users)	initial : none TemplateMD5: MD5 TemplateSHA: SHA
Privacy (for default users)	initial : none TemplateMD5: none TemplateSHA: DES
Groups	iso, initial
Access	iso, initial
View (for default groups)	iso: iso, initial: restricted
Notify View Name	iss, iss1
Read, Write, Notify	Iso
Target Parameters	Internet, test1
Storage Type	Volatile
Context	None
SNMP Port	161
SNMP Trap Port	162
Trap Status	Enabled
Authentication Trap	Disabled
Link-State Trap	Enabled

Switch Name	SMIS
System Contact	http://www.supermicro.com
System Location	Supermicro

6 Enable/Disablethe SNMP Agent

The SNMP Agent is enabled by default in Supermicro switches.
Follow the steps below to **disable** the SNMP agent.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**disable snmpagent**	Disables the SNMP agent
Step 3	**end**	Exits the configuration mode.
Step 4	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

The**"enablesnmpagent"** command enables the SNMP agent.

To enable the SNMP agent, it must be in the disabled state.

The examples below show ways to disable/enable the SNMP agent function on Supermicro switches.
Disable the SNMP agent.
SMIS# **configure terminal**
SMIS(config)# **disable snmpagent**
SMIS(config)# **end**

Enable the SNMP agent.
SMIS# **configure terminal**
SMIS(config)# **enable snmpagent**
SMIS(config)# **end**

6.1 Switch Name

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

Follow the steps below to configure the switch name.

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

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

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

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

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

======= ==========
Time zone offset not set

6.2 Switch Contact

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

Follow the steps below to configure the switch contact.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**system contact <string - to use more than one word, provide the string within double quotes>**	Configures the switch contact. String – Contact information entered as a String of maximum length 256.
Step 3	**End**	Exits the configuration mode.
Step 4	**show system information**	Displays the system information configuration.
Step 5	**write startup-config**	Optional step – saves this configuration to be part of the startup configuration.

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

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

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

SMIS# **show system information**
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: User1 at CA
System Location: Supermicro
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore

Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Device Up Time: 0 days 0 hrs 50 mins 51 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
============== ===== ======
Key # Key
======= ==================================
Time zone offset not set

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

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

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

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

SMIS# **show system information**
Switch Name: SMIS
Switch Base MAC Address: 00:30:48:e3:70:bc
SNMP EngineID: 80.00.08.1c.04.46.53
System Contact: http://www.supermicro.com
System Location: Santa Clara
Logging Option: Console Logging
Login Authentication Mode: Local
Snoop Forward Mode: MAC based
Config Restore Status: Not Initiated
Config Restore Option: No restore
Config Restore Filename: iss.conf
Config Save IP Address: 0.0.0.0
Supermicro L2/L3 Switches Configuration Guide 43
Device Up Time: 0 days 0 hrs 51 mins 39 secs
Boot-up Flash Area: Normal
NTP Broadcast Mode: No
[NTP] ntp is disabled
Server Key Prefer
=============== ===== ======
Key # Key
======= ===================================
Time zone offset not set

7 Access Control

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

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

7.1 Engine Identifier

The SNMP Engine Identifieris a unique identifier for the SNMP agent in a switch. It is used with a hashing function in the agent to generate keys for authentication and encryption. Hence after any change in theEngine Identifier,the following must be re-configured:

- SNMPv3 authentication
- SNMPv3 encryption/privacy
- Community

Follow the steps below to configure the SNMP Engine Identifier.

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

The example below shows the commands used to configure the SNMP Engine Identifier.
SMIS# configure terminal
SMIS(config)# **snmpengineid 80.00.08.1c.44.44**
SMIS(config)# end

SMIS# **show snmpengineid**

EngineId: 80.00.08.1c.44.44

The **"no snmpengineid"** command resets the SNMP engineid to its default value of 80.00.08.1c.04.46.53.

7.2 Community

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.
The SNMP v1/v2 community is also used as a form of security. The community of SNMP managers that can access the agent MIB in the switch is defined by a community string.
Follow the steps below to configure an SNMP community.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp community index <CommunityIndex> name <CommunityName> security <SecurityName>**	Configures the SNMP community.

	[context <name>] [{volatile | nonvolatile}] [transporttag<TransportTagIdentifier | none>]	*CommunityIndex*–Alphanumericvalue with a maximum of 32 characters. *CommunityName*–Alphanumeric value with a maximum of 64 characters. *SecurityName* – This is the user name associated with the community. Alphanumeric value with a maximum of 32 characters. *Name* –Alphanumeric value with a maximum of 32 characters. *TransportTagIdentifier* –Identifies the transport end points between agent and manager. Alphanumeric value with a maximum of 64 characters.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp community**	Displays the SNMP community information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

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

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

The example below shows the commands used to configure the SNMP community.
SMIS(config)# **snmp community index test1 name test1 security user1 nonvolatile**

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

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

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

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

7.3 User

SNMP user configuration is used only for SNMPv3. An SNMP user requests and receives information about switch status and traps.
Follow the steps below to configure an SNMP user.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp user <UserName> [auth {md5 | sha} <passwd>[priv DES <passwd>]] [{volatile | nonvolatile}]**	Configures the SNMP user, authentication and encryption. *UserName* - Alphanumeric value with a maximum of 32 characters. Use **auth**to enable authentication for the user. *Passwd*–Password used for user Authentication. Alphanumeric value with a maximum of 32 characters. Use **priv**toenableencryption of packets. *Passwd*–Password used to generate keys for encryption of messages. Alphanumeric value with a maximum of 40 characters.

		Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp user**	Displays the SNMP user information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

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

The example below shows the commands used to configure the SNMP user.
SMIS# configure terminal
SMIS(config)# **snmp user user5 auth md5 abc123 priv DES xyz123**
SMIS# end

SMIS# **show snmp user**

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

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

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

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

7.4 Group

A group identifies a set of users in SNMPv3.
Follow the steps below to configure an SNMP group.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]**	Configures the SNMP group. *GroupName* – Alphanumeric value with a maximum of 32 characters. *Security-model* – Use v1 or v2c or v3. *UserName* - Alphanumeric value with a maximum of 32 characters. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp group**	Displays the SNMP group information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

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

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

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

SMIS# **show snmp group**

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

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

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

Security Model: v3
Security Name: initial
Group Name: initial
Storage Type: Non-volatile
Row Status: Active

Security Model: v3
Security Name: templateMD5
Group Name: initial
Storage Type: Non-volatile
Row Status: Active

Security Model: v3
Security Name: templateSHA
Group Name: initial
Storage Type: Non-volatile
Row Status: Active

7.5 View

A view specifies limited access to MIBs. A view can be associated with one or many groups.
In an SNMP, parameters are arranged in a tree format. SNMP uses an Object Identifier (OID) to identify the exact parameter in the tree. An OID is a list of numbers separated by periods.
Follow the steps below to configure the SNMP view.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmpview <ViewName><OIDTree> [mask <OIDMask>] {included | excluded}[{volatile | nonvolatile}]**	Configures the SNMP view. *ViewName*- Alphanumeric value with a maximum of 32 characters. *OIDTree*–OID number, with a maximum of 32 numbers. *OIDMask*– OID number, with a maximum of 32 numbers. Use **included**to specifythat the MIB sub-tree is included in the view. Use **excluded**to specify that the MIB sub-tree is excluded from the view. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmpviewtree**	Displays the SNMP view information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

The **"**no snmp view <ViewName><OIDTree> **"**command deletes the specified SNMP view.

The example below shows the commands used to configure the SNMP view.
SMIS(config)# **snmp view view1 1.3.6.1 included**

SMIS(config)# **show snmpviewtree**

View Name: iso
Subtree OID: 1
Subtree Mask: 1
View Type: Included
Storage Type: Non-volatile
Row Status: Active

View Name: view1
Subtree OID: 1.3.6.1
Subtree Mask: 1.1.1.1
View Type: Included
Storage Type: Volatile
Row Status: Active

View Name: Restricted
Subtree OID: 1
Subtree Mask: 1
View Type: Excluded
Storage Type: Non-volatile
Row Status: Active

7.6 Group Access

Group access defines the access policy for a set of users belonging to a particular group. Group access is used only for SNMPv3.
Follow the steps below to configure SNMP group access.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}[read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}]**	Configures the SNMP group access. *GroupName* - Alphanumeric value with a maximum of 40 characters. Security model – Mention one of v1, v2c or v3. Use **auth**to enable authentication for the user. Use **priv**toenableencryption of packets.

		ReadView- View name that specifies read access to particular MIB sub-tree.Alphanumeric value with a maximum of 40 characters. *WriteView*View name that specifies write access to particular MIB sub-tree. Alphanumeric value with a maximum of 40 characters. *NotifyView*View name that specifies a particular MIB sub-tree used in notification. Alphanumeric value with a maximum of 40 characters. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp group access**	Displays the SNMP group access information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of startup configuration.

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

The**"no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}**" commanddeletes the specified SNMP group access.

The sequence of steps to delete a group that is associated with a group access and view:

1. Delete the view
2. Delete the group access.
3. Delete the group.

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

SMIS# configure terminal
SMIS(config)# **snmp access group5 v3 auth read view1 write view2 notify none nonvolatile**
SMIS(config)# end

SMIS# **show snmp group access**

Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Volatile
Row Status: Active

Group Name: iso
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Volatile
Row Status: Active

Group Name: group5
Read View: view1
Write View: view2
Notify View:
Storage Type: Non-volatile
Row Status: Active

Group Name: Initial
Read View: Restricted
Write View: Rrestricted
Notify View: Restricted
Storage Type: Non-volatile
Row Status: Active

Group Name: Initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Non-volatile
Row Status: Active

Group Name: initial
Read View: iso
Write View: iso
Notify View: iso
Storage Type: Non-volatile
Row Status: Active
---

8 Trap

8.1 Target Address

A target is a receiver of SNMP notification(s), which are usually SNMP Managers. The target address defines the transport parameters of the receivers.
Follow the steps below to configure the SNMP Target address.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmptargetaddr<TargetAddressName>param<ParamName> {<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)] [taglist<TagIdentifier | none>] [{volatile | nonvolatile}]**	Configures the SNMP target address information. *TargetAddressName* - Alphanumeric value with a maximum of 32 characters. *ParamName* – The parameter to be notified to the specific target. Alphanumeric value with a maximum of 32 characters. IPAddress– IPv4 address of the target. *IP6Address* – IPv6 address of the target.

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

The "no snmptargetaddr<TargetAddressName> "command deletes the specified SNMP target address information.

The example below shows the commands used to configure the SNMP target address.
SMIS# configure terminal
SMIS(config)# **snmptargetaddr host1 param param1 192.168.1.10 taglist tg1**
SMIS# end

SMIS# **show snmptargetaddr**

Target Address Name: host1
IP Address: 192.168.1.10
Tag List: tg1
Parameters: param1
Storage Type: Volatile
Row Status: Active

8.2 Target Parameters

Target parameters define the MIB objects that should be notified to an SNMP target, usually an SNMP manager.
Follow the steps below to configure SNMP target parameters.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmptargetparams<ParamName> user <UserName>security-model {v1 | v2c | v3 {auth | noauth | priv}}message-processing {v1 | v2c | v3} [{volatile | nonvolatile}]**	Configures the SNMP target parameters. *ParamName*The parameter to be notified. Alphanumeric value with a maximum of 32 characters. *UserName* - Alphanumeric value with a maximum of 32 characters. Security model – Use one of v1, v2c, v3. Use **auth**to enable authentication for the user.

		Use **priv**toenableencryption of packets. Message processing- Specifies the SNMP version for sending/receiving the parameter via a notification message. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmptargetparam**	Displays the SNMP target parameters information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

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

The example below shows the commands used to configure the SNMP target parameters.
SMIS# configure terminal
SMIS(config)# **snmptargetparams param4 user user4 security-model v2c message-processing v2c**
SMIS# end

SMIS# **show snmptargetparam**

Target Parameter Name: Internet
Message Processing Model: v2c
Security Model: v2c
Security Name: None
Security Level: No Authenitcation, No Privacy
Storage Type: Volatile
Row Status: Active

Target Parameter Name: param4
Message Processing Model: v2c

Security Model: v2c
Security Name: user4
Security Level: No Authenitcation, No Privacy
Storage Type: Volatile
Row Status: Active

Target Parameter Name: test1
Message Processing Model: v2c
Security Model: v1
Security Name: None
Security Level: No Authenitcation, No Privacy
Storage Type: Volatile
Row Status: Active

8.3 SNMP Notify

Notify is used to specify the type of notifications to be sent to particular targets that are grouped under a particular tag.
Follow the steps below to configure the SNMP Notification.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp notify <NotifyName> tag <TagName> type {Trap | Inform}[{volatile | nonvolatile}]**	Configures the SNMP Notify information. *NotifyName*- Alphanumeric value with a maximum of 32 characters. *TagName* –Specifies a group of targets identified by this name. Alphanumeric value with a maximum of 32 characters. Type – Notification can be Trap or Inform. Use **volatile**if the value need not be stored in NVRAM. Use **nonvolatile** if the value must be stored in NVRAM and available after restart.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp notify**	Displays the SNMP notification information and Inform statistics.

	show snmp inform statistics	
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

The **"**no snmp notify <NotifyName>**"** command deletes the specified SNMP notification.

The example below shows the commands used to configure the SNMP notification.
SMIS# configure terminal
SMIS(config)# **snmp notify PUBLIC tag tag1 type trap nonvolatile**
SMIS(config)# end

SMIS# **show snmpnotif**

Notify Name: PUBLIC
Notify Tag: tag1
Notify Type: trap
Storage Type: Non-volatile
Row Status: Active

Notify Name: iss
Notify Tag: iss
Notify Type: trap
Storage Type: Volatile
Row Status: Active

Notify Name: iss1
Notify Tag: iss1
Notify Type: trap
Storage Type: Volatile
Row Status: Active

8.4 Trap UDP Port

The default UDP port for traps is 162. Supermicro switches providean option for users to change this trap UDP port.
Follow the steps below to configure the SNMP UDP port for traps.

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

Step 2	**snmp-server trap udp-port <port>**	Configures the SNMP UDP port for traps. *Port*–UDP port for traps in the range 1 – 65535.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp-server traps**	Displays the SNMP traps information.
Step 5	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

The **"no snmp-server trap udp-port"** command resets the SNMP UDP port to its default value of 162.

The example below shows the commands used to configure the SNMP UDP port for traps.
SMIS# configure terminal
SMIS(config)# **snmp-server trap udp-port 170**
SMIS(config)# end

SMIS(config)# **show snmp-server traps**

SNMP Trap Listen Port is 170
Currently enabled traps:
---
linkup,linkdown,
Login Authentication Traps DISABLED.

8.5 Authentication Traps

Traps can be generated when a user login authentication fails at the SNMP agent. In Supermicro switches, authentication traps are disabled by default.
Follow the steps below to enable an SNMP authentication trap.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**snmp-server enable traps snmp authentication**	Enables the SNMP authentication traps.
Step 3	**end**	Exits the configuration mode.
Step 4	**show snmp**	Displays the SNMP information.

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

The **"no snmp-server enable traps snmp authentication"** command disables SNMP authentication traps.

The example below shows the commands used to enable the SNMP authentication traps.
SMIS# configure terminal
SMIS(config)# **snmp-server enable traps snmp authentication**
SMIS# end

SMIS(config)# **show snmp-server traps**

SNMP Trap Listen Port is 162
Currently enabled traps:
---
linkup,linkdown,
Login Authentication Traps ENABLED.

8.6 Link-State Trap

Link-state traps are enabled for all interfaces by default in Supermicro switches. Traps are generated when an interface toggles its state from Up to down or vice-versa.
Follow the steps below to disable SNMP Link-state trap.

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

		interface-id is in slot/port format for all physical interfaces. To configure multiple interfaces, use the “interface range …” command. Toprovide a range, use a hyphen (-) between the start and end interface numbers. E.g.: int range fx 0/1-10 To provide multiple interfaces or ranges, separate with a comma (,). E.g.: int range fx 0/1-10, fx 0/20 If multiple interfaces are provided, the next step will perform the particular configuration on all these interfaces.
Step 3	**no snmp trap link-status**	Disables the SNMP link-state trap on the particular interface.
Step 4	**end**	Exits the configuration mode.
Step 5	**show snmp**	Displays the SNMP information.
Step 6	**write startup-config**	Optional step – saves this SNMP configuration to be part of the startup configuration.

The **“snmp trap link-status”** command enables SNMP link-state traps.

The example below shows the commands used to disable the SNMP Link-state trap.
SMIS# configure terminal
SMIS(config)# interface Fx 0/21
SMIS(config-if)# **no snmp trap link-status**

SMIS(config-if)# end

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

Fx0/21 up, line protocol is up (connected)
Bridge Port Type: Customer Bridge Port

Hardware Address is 00:30:48:e3:04:89
MTU 1500 bytes, Full duplex, 1 Gbps, Auto-Negotiation
HOL Block Prevention enabled.
Input flow-control is off,output flow-control is off

Link Up/Down Trap is disabled

Reception Counters
  Octets : 753
  Unicast Packets : 0
  Broadcast Packets : 0
  Multicast Packets : 9
  Pause Frames : 0
  Undersize Frames : 0
  Oversize Frames : 0
  CRC Error Frames : 0
  Discarded Packets : 0
  Error Packets : 0
  Unknown Protocol : 0

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

9 SNMP Configuration Example

PC – SNMP Manager **Switch - SNMP Agent**

Figure SNMP-2 – SNMP Configuration Example

Configure the following requirements on a switch acting as an SNMP agent as shown above in Figure SNMP-2.

1) Creates SNMP users
    a. Create an SNMP user '*user1*' Specify the authentication and privacy protocol and the authentication and privacy passwords.
    b. Creates an SNMP user '*user2*'. Specify the authentication protocol and password.
2) Creates SNMP groups
    a. Create groupcalled *superusers*and associateuser1 with this group.
    b. Create groupcalled *generalusers* and associate user1 with this group.
3) Create views
    a. Creates an SNMP view '*full*'which will allow access to everything from the specified Object Identifier
    b. Creates an SNMP view '*restricted*'which will allow access to everything from the specified OID onwards, and also adds a restriction to anything on a particular sub-tree.
4) Create group access
    a. Access for *superusers- fullread/write* and notify privilege to the '*full*' view
    b. Access for *generalusers- full* read,notify privilege to the 'full' view and , retricted write
5) Display all configuration

SMIS# configure terminal
SMIS(config)# **snmp user user1 auth md5 pwd1**
SMIS(config)# **snmp user user2 auth sha abcd priv deS 1b12**
SMIS(config)# **snmp group superuser user user1 security-model v3 volatile**
SMIS(config)# **snmp group generalusers user user2 security-model v3 volatile**
SMIS(config)# **snmp view full 1.3.6.1 included volatile**
SMIS(config)# **snmp view restricted 1.3.6.1 included volatile**
SMIS(config)# **snmp view restricted 1.3.6.3.10.2.1 excluded volatile**
SMIS(config)# **snmp access superuser v3 auth read full write full notify full**
SMIS(config)# **snmp access generalusers v3 noauth read full write restricted notify full**
SMIS(config)# end

SMIS# **show snmp user**

Engine ID : 80.00.08.1c.04.46.53

User : user1
Authentication Protocol : MD5
Privacy Protocol : None
Storage Type : Volatile
Row Status : Active

Engine ID : 80.00.08.1c.04.46.53
User : user2
Authentication Protocol : SHA
Privacy Protocol : DES_CBC
Storage Type : Volatile
Row Status : Active

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

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

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

SMIS# **show snmp group**

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

Security Model : v2c
Security Name : none
Group Name : iso
Storage Type : Volatile

Row Status : Active

Security Model : v3
Security Name : user1
Group Name : superuser
Storage Type : Volatile
Row Status : Active

Security Model : v3
Security Name : user2
Group Name : generalusers
Storage Type : Volatile
Row Status : Active

Security Model : v3
Security Name : initial
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

Security Model : v3
Security Name : templateMD5
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

Security Model : v3
Security Name : templateSHA
Group Name : initial
Storage Type : Non-volatile
Row Status : Active

SMIS# **show snmp group access**

Group Name : iso
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Volatile
Row Status : Active

Group Name : iso
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Volatile

Row Status : Active

Group Name : initial
Read View : restricted
Write View : restricted
Notify View : restricted
Storage Type : Non-volatile
Row Status : Active

Group Name : initial
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Non-volatile
Row Status : Active

Group Name : initial
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Non-volatile
Row Status : Active

Group Name : superuser
Read View : full
Write View : full
Notify View : full
Storage Type : Volatile
Row Status : Active

Group Name : generalusers
Read View : full
Write View :
Notify View : full
Storage Type : Volatile
Row Status : Active

SMIS# **show snmp viewtree**

View Name : iso
Subtree OID : 1
Subtree Mask : 1
View Type : Included
Storage Type : Non-volatile
Row Status : Active

View Name   : full
Subtree OID : 1.3.6.1
Subtree Mask : 1.1.1.1
View Type   : Included
Storage Type : Volatile
Row Status   : Active

View Name   : restricted
Subtree OID : 1
Subtree Mask : 1
View Type   : Excluded
Storage Type : Non-volatile
Row Status   : Active

View Name   : restricted
Subtree OID : 1.3.6.1
Subtree Mask : 1.1.1.1
View Type   : Included
Storage Type : Volatile
Row Status   : Active

View Name   : restricted
Subtree OID : 1.3.6.3.10.2.1
Subtree Mask : 1.1.1.1.1.1.1
View Type   : Excluded
Storage Type : Volatile
Row Status   : Active

SMIS# **show running-config**

Building configuration...
ID Hardware Version Firmware OS Boot Loader
0 SSE-F3548 1.0.0.0 6 0.0.0.0
vlan 1
 ports fx 0/1-24 untagged
 ports cx 0/1-3 untagged
exit

snmp user user1 auth md5 AUTH_PASSWD volatile
snmp user user2 auth sha AUTH_PASSWD priv DES DES_CBC volatile
snmp group superuser user user1 security-model v3 volatile
snmp group generalusers user user2 security-model v3 volatile
snmp access superuser v3 auth read full write full notify full volatile
snmp access generalusers v3 noauth read full notify full volatile
snmp view full 1.3.6.1 included volatile
snmp view restricted 1.3.6.1 included volatile

snmp view restricted 1.3.6.3.10.2.1 excluded volatile

Contacting Supermicro

Headquarters

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

Europe

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

Asia-Pacific

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