SSE-X3548S/SSE-X3548SR

VLAN

User's Guide

Revision 1.14

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

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

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

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

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

Manual Revision 1.14
Release Date: 5/14/2020

Document Revision History

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

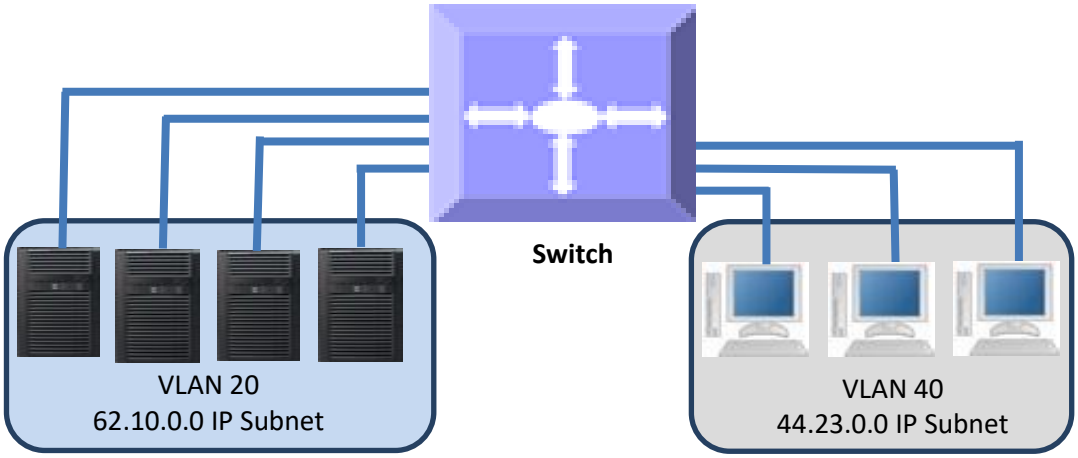
Contents

1 VLAN Basics

A Virtual LAN (VLAN) is a logical switched LAN formed by segmenting physical Local Area Networks (LANs).
Segmenting a switched LAN as one or more VLANs provides the following advantages:

- ⇒ Limits multicast and broadcast floods only to the required segments of the LAN to save LAN bandwidth
- ⇒ Provides secured LAN access by limiting traffic to specific LAN segments
- ⇒ Eases management by logically grouping ports across multiple switches

Figure VLAN-1: VLANs on a Switched LAN



VLANs work in same way as physical LANs. The packets from the end stations of a VLAN are switched only to other end stations or network devices inside that VLAN. To reach devices in another VLAN, the packets have to be routed from one VLAN to another. Supermicro L2/L3 switches support such Inter VLAN routing to route packets across different VLANs. Inter VLAN routing is done by creating “Layer 3 Interface VLANs”.

2 VLAN Support

Supermicro switches support the three types of VLANs: MAC based VLANs, protocol based VLANs and port based VLANs.

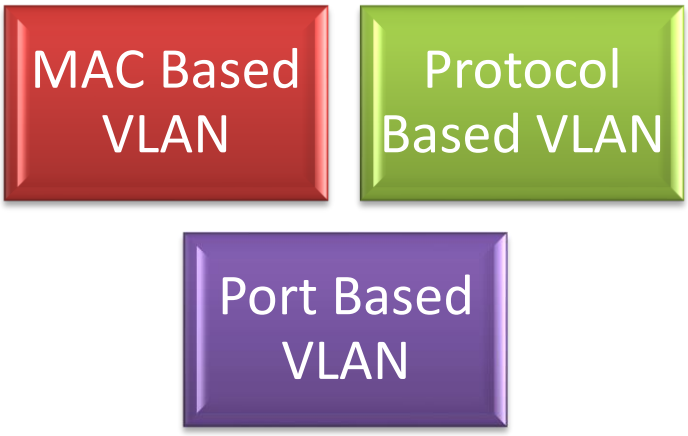
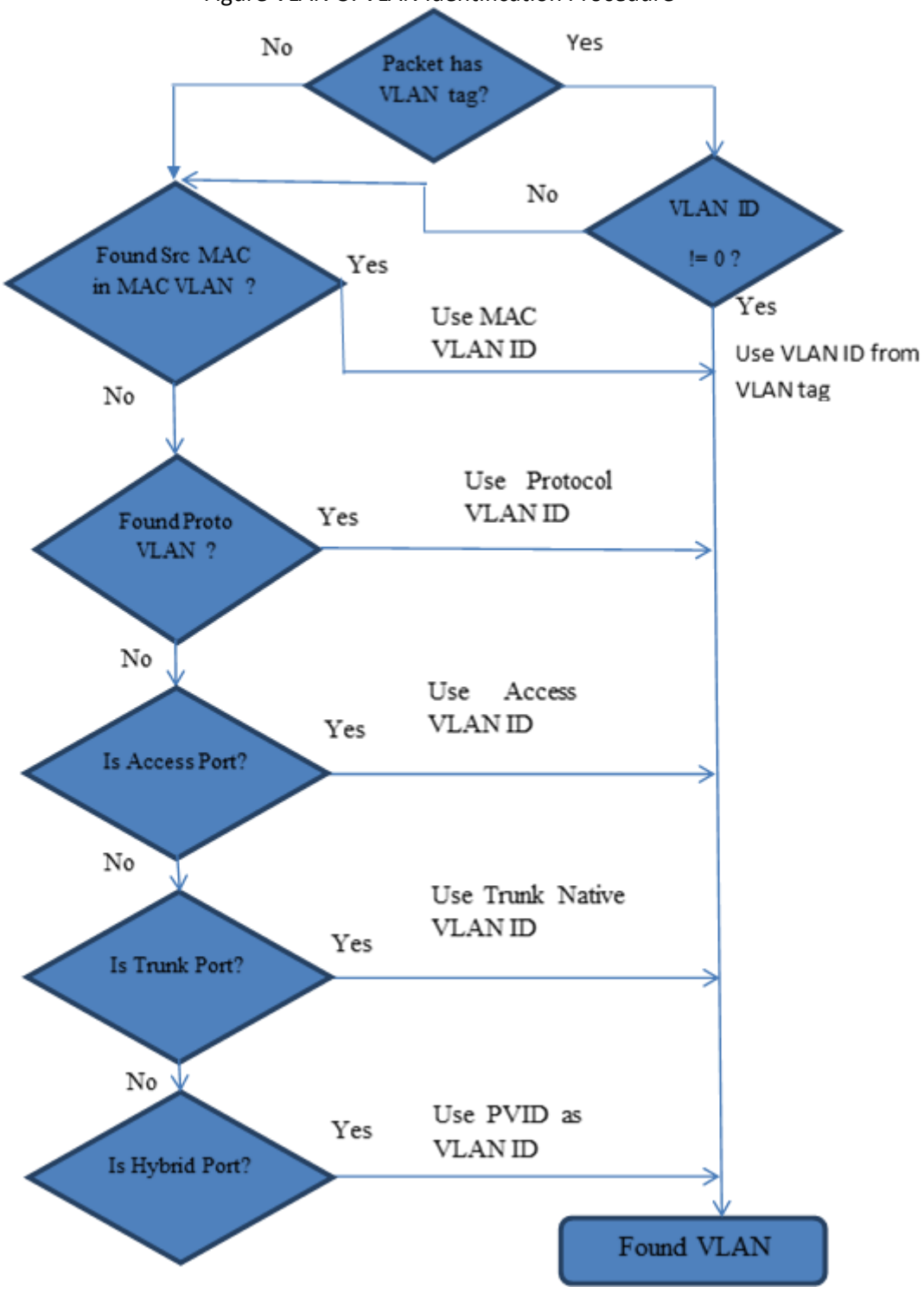


Figure VLAN-2: Types of VLANs Supported

Once a packet is received, a switch tries to identify the VLAN for the received packet. This VLAN identification is done according to the procedure below.
If the incoming packet has a VLAN tag and the VLAN ID in the tag is not equal to zero, then this VLAN ID is used as the VLAN for this packet.
If the incoming packet does not have a VLAN tag (untagged packet) or if the VLAN ID in the VALN tag is equal to zero (priority tagged packet), the packet is considered as untagged/priority tagged and the below steps are used to identify the VLAN for this untagged/priority tagged packet.
Step 1: Use the source MAC of the incoming packet and check the MAC VLAN mapping. If the VLAN is found for this source MAC, that VLAN ID is used as the VLAN for this packet. If the MAC VLAN is not found, proceed to the next step.
Step 2: Use the protocol field from the incoming packet layer 2 header and check the protocol VLAN table. If a protocol VLAN is found, that VLAN ID is used as the VLAN for this packet. If a protocol VLAN is not found, proceed to the next step.
Step 3: This step identifies the VLAN based on a port based VLAN configuration. If the received port is in access mode, the configured access VLAN (default is VLAN 1) is used as the VLAN for this packet. If the received port is in trunk mode, the configured trunk native VLAN (default is VLAN 1) is used as the VLAN for this packet. If the received port is in hybrid mode, the configured PVID (default is VLAN 1) is used as the VLAN for this packet.
This VLAN identification procedure is shown in Figure VLAN-3: VLAN Identification Procedure.
Once the VLAN is identified for the received packet, the switch checks if the received port is a member of this identifier VLAN. If the received is not member of the identified VLAN, the packet is dropped. If the received port is a member of the identified VLAN, then it will be forwarded to other member ports of this VLAN based on the forwarding logic. If there are no other member ports for this VLAN, the packet will most likely be dropped unless it was routed or sent to the CPU or redirected by an ACL rule.

Figure VLAN-3: VLAN Identification Procedure



3 VLAN Numbers

SSE-X3548S/R supports 4K static VLANs.
SSE-X3548S/R switches support VLAN identifiers from 1 to 4069 for user created VLANs. VLAN identifiers 4070 to 4094 are reserved for internal use.

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

SSE-X3548S/R supports 1024 MAC based VLANs.
Supermicro switches support 16 protocol groups for protocol based VLANs. These 16 protocol groups can be mapped to different VLANs in every port. The same protocol group can be associated with different VLANs in different ports.

4 VLAN Defaults

Supermicro switches boot up with VLAN 1, which is a default Layer 2 VLAN. The switchable ports of all switches are added to this default VLAN 1 as hybrid ports. This default setup helps switch forwarding traffic across all the ports without the need of any user configuration.
Users can modify the port members of this VLAN 1 by adding or removing any ports to this VLAN 1 as either tagged or untagged ports. The easier way is to change the port modes to either "Access" or "Trunk" ports and configure the relevant VLANs. The "Access" and "Trunk" modes are described in detail in later sections.

VLAN 1 cannot be deleted by the user. If user wants to prohibit traffic from/to VLAN 1, then remove all the ports from VLAN 1 by using the "**no ports**" command available in the VLAN configuration mode. After removing all the ports, "show vlan id 1" command should display 'none' as shown below.

```
SMIS(config)# show vlan id 1

Vlan database
-------------
Vlan ID                : 1
Member Ports           : None
Hybrid Tagged Ports    : None
Hybrid Untagged Ports  : None
Hybrid Forbidden Ports : None
Access Ports           : None
Trunk Ports            : None
Name                   :
Status                 : Permanent
```

SMIS(config)#

The port based VLAN identifier (PVID) for all the switch ports is set to 1 by default. The PVID is used to associate incoming untagged packets to port based VLANs for the ports in "Hybrid" mode. Users can modify the PVID for switch ports to any VLAN identifier for "Hybrid" ports.
The switch port mode is set to "hybrid" for all switch ports by default. Users can change the port mode as explained in the Port Based VLAN section.
VLAN 1 is configured as the default native VLAN for all trunk interfaces. Users can change the native VLANs for trunk interfaces as explained in the Native VLAN on Trunk section.
Protocol based VLAN is enabled by default.

Supermicro switches do not create VLANs by default except for VLAN 1. Users need to create all the VLANs used on their network in Supermicro switches. Trunk ports will be able to carry only VLANs created in Supermicro switches.

5 Creating VLANs

Follow the steps below to create VLANs in Supermicro switches.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**vlan <***vlan-list***>**	Creates a VLAN using **vlan** command. *vlan-list* – may be any vlan number or list of vlan numbers. Multiple vlan numbers can be provided as comma-separated values. Consecutive vlan numbers can be provided as a range, such as 5-10. User can configure VLANs with identifiers 1 to 4069.
Step 3	**show vlan**	Displays the configured VLANs
Step 4	**write startup-config**	Optional step – Save these VLAN configuration to be part of startup configuration.

The examples below show various ways of creating VLANs.
Create a VLAN with identifier 10
SMIS# **configure terminal**
SMIS(config)# **vlan 10**

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

Create VLANs with identifiers 20 to 30, 50 and 100
SMIS# **configure terminal**
SMIS(config)# **vlan 20-30,50,100**
SMIS(config-vlan)# **exit**

6 Removing VLANs

Follow the steps below to remove VLANs from Supermicro switches.

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

The below examples show ways to remove VLANs.
Delete a VLAN with identifier 10
SMIS# **configure terminal**
SMIS(config)# **no vlan 10**

Delete VLANs with identifier 20 to 30, 50 and 100
SMIS# **configure terminal**
SMIS(config)# **no vlan 20-30,50,100**
SMIS(config-vlan)# **exit**

7 VLAN Name

VLANs can be associated with a label name string for easier configuration and identification. Follow the steps below to add or modify a name string to any VLAN in Supermicro switches.

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

The example below shows the steps necessary to associate a name string to a VLAN.
Associate name main_user_vlan to VLAN 50.
SMIS# **configure terminal**
SMIS(config)# **vlan 50**
SMIS(config-vlan)# **name main_user_vlan**
SMIS(config-vlan)# **exit**

Follow the steps below to remove a name string from any VLAN in a Supermicro switch.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode.
Step 2	**vlan <***vlan-list***>**	Enters the VLAN configuration mode. *vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple

		VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the name string of all these VLANs will be removed by the next step.
Step 3	**no name**	Removes associated name string from this VLAN.
Step 4	**show vlan**	Displays the configured VLANs
Step 5	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

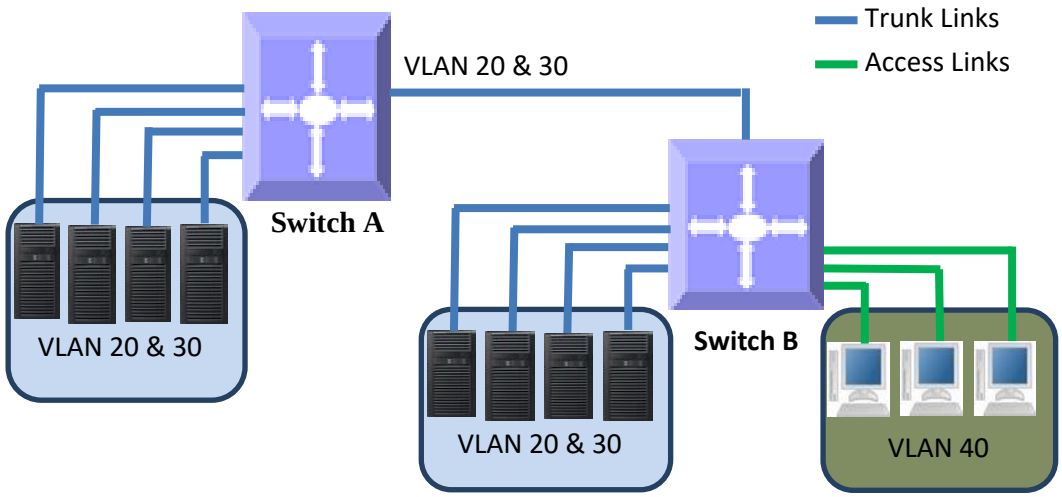
The example below shows steps to remove name string from a VLAN.
Remove name from VLAN 50.
SMIS# **configure terminal**
SMIS(config)# **vlan 50**
SMIS(config-vlan)# **no name**
SMIS(config-vlan)# **exit**

8 Port Based VLANs

Port based VLANs are the simplest and most useful type of VLAN.
In port based VLAN deployment, switch ports are associated with one or more VLANs as member ports. The traffic sent on the ports is decided by the VLAN membership and mode of the ports. Usually ports are associated with VLANs as either “access” port members or “trunk” port members. Supermicro switches support an additional port mode called “hybrid”.

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

Figure VLAN-4: Port Based VLANs



8.1 Access Ports

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

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

Switches will not add VLAN tag headers to all the packets sent out on an access port. Switches expect to receive untagged or priority tagged (VLAN identifier 0) packets only at the access ports. If any tagged packets are received on an access port, the switch will drop them. Follow the below steps to configure any port as the access port of any VLAN.

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

	or **interface range** <*interface-type*> <*interface-id*> ….	*interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range use a hypen (-) between the start and end interface numbers. E.g.: **int range fx 0/1-10** To provide multiple interfaces or ranges, use separate with a comma (,). E.g.: **int range fx 0/1-10, fx 0/20**
Step 3	**switchport mode access**	Sets the port mode as the access port.
Step 4	**switchport access vlan** <*vlan-id*>	Configures the access VLAN for this interface. The VLAN identifiers may be any VLAN number from 1 to 4069. If the given VLAN does not exist, switch will provide a warning message. Only when the VLAN available, the port will operate as an access port for that VLAN.
Step 5	**show vlan port config port** <*iftype*> <*ifnum*>	Displays the configured mode and accesses the VLAN for this interface.
Step 6	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

The "switchport access vlan" command will be accepted only if the port is in access mode.

The "**no switchport mode**" command will change the port mode to the default hybrid mode. For more details about hybrid mode, refer to the Hybrid Ports section.

The "**no switchport access vlan**" command will set the access VLAN as default VLAN 1. The port will continue to be the access port of VLAN 1.

The examples below show various ways to create VLANs with access ports.

Create a VLAN with identifier 50 and configure ports fx 0/2 to fx 0/10 as access ports to this VLAN.

SMIS# **configure terminal**
SMIS(config)# **vlan 50**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface range fx 0/2-10**
SMIS(config-if)# **switchport mode access**
SMIS(config-if)# **switchport access vlan 50**
SMIS(config-if)# **exit**

Create a VLAN with identifier 10 and configure port channel 1 as access port to this VLAN.

SMIS# **configure terminal**
SMIS(config)# **vlan 10**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface po 1**
SMIS(config-if)# **switchport mode access**
SMIS(config-if)# **switchport access vlan 10**
SMIS(config-if)# **exit**

8.2 Trunk Ports

Trunk ports carry the traffic of one or more VLANs. Any switch port can be configured as a trunk port. Usually switch ports connected between switches are configured as trunk ports to carry multiple VLAN traffic across switches. Switch ports connected to end stations (computers / servers) that have multiple VLANs are also configured as trunk ports.

When a switch port is configured as a trunk port, it will be added to all the VLANs in the switch as a tagged port by default. To restrict the VLANs carried in trunk ports, refer to the Allowed VLANs on a Trunk section.

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

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

When a packet is received on a trunk port, the switch identifies the VLAN for the received packet from the packet's VLAN tag header. If the received packet did not have a VLAN identifier and the packet did not match any MAC or protocol VLAN, the native VLAN is used to determine the VLAN for all untagged and priority tagged packets that are received.

If the user has not configured a native VLAN, the default VLAN 1 will be used as native VLAN for the trunk ports.

Follow the steps below to configure any port as a trunk port.

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

	interface range <*interface-type*> <*interface-id*> ….	*interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range fx 0/1-10, fx 0/20**
Step 3	**switchport mode trunk**	Sets the port mode as a trunk port.
Step 4	**show vlan port config port** <*iftype*> <*ifnum*> and **show running-config**	Displays the configured mode for this interface.
Step 5	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

The "**no switchport mode**" command will change the port mode to the default hybrid mode. For more details about hybrid mode, refer to the Hybrid Ports section.

The examples below show various ways to configure trunk ports.

Configure port fx 0/1 and fx 0/2 as trunk ports.

SMIS# **configure terminal**
SMIS(config)# **interface range fx 0/1-2**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **exit**

Configure port channel 1 as a trunk port.

SMIS# **configure terminal**
SMIS(config)# **interface po 1**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **exit**

8.2.1 Allowed VLANs on a Trunk

By default, all the VLANs configured on a switch are allowed on the trunk interfaces. However, there may be some cases where users would like to limit the number of VLANs carried on the trunk ports. This can be configured by following the steps below.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**interface <***interface-type***> <***interface-id***>** or **interface range** <*interface-type*> <*interface-id*> ….	Enters the interface mode. *interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range fx 0/1-10, fx 0/20**
Step 3	**switchport mode trunk**	Sets the port mode as trunk port.
Step 4	Use any one of the below steps 4a to 4f based on the need.	The *vlan-list* parameter used in the below commands could be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.
Step 4a	**switchport trunk allowed vlan** <*vlan-list*>	This command configures the list of allowed VLANs on this trunk. Only the VLANs provided on the *vlan-list* will be carried over the trunk.
Step 4b	**switchport trunk allowed vlan add** <*vlan-list*>	This command adds the given list of VLANS to the existing set of allowed VLANs on this trunk.
Step 4c	**switchport trunk allowed vlan remove** <*vlan-list*>	This command removes the given list of VLANS from the existing set of allowed VLANs on this trunk.

Step 4d	**switchport trunk allowed vlan except** <*vlan-list*>	This command makes all the configured VLANs allowed on this trunk except for the given list of VLANs.
Step 4e	**switchport trunk allowed vlan all**	This command sets the default behavior of allowing all VLANs configured in the switch as allowed VLANs on this trunk.
Step 4f	**switchport trunk allowed vlan none**	This command removes all the allowed VLANs from this trunk.
Step 5	**show vlan port config port** <*iftype*> <*ifnum*> and **show running-config**	Displays the configured, allowed VLANs for this trunk interface.
Step 6	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

The "switchport trunk allowed vlan …" commands will be accepted only if the port is in trunk mode.

A trunk port will not carry traffic for any VLANs that are not configured in the switch. For example, if a user wants to allow traffic for VLANs 1 to 100, VLANs 1 to 100 need to be created in the switch using the "**vlan**" command.

The examples below show examples of configurations to allow VLANs on trunk ports.

Configure to allow only VLANs 2 to 20 on trunk interface fx 0/1.

SMIS# **configure terminal**
SMIS(config)# **vlan 2-20**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface fx 0/1**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **switchport trunk allowed vlan 2-20**
SMIS(config-if)# **exit**

Configure to not to allow VLANs 30 to 50 on trunk interface fx 0/1.

SMIS# **configure terminal**
SMIS(config)# **interface fx 0/1**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **switchport trunk allowed vlan except 30-50**
SMIS(config-if)# **exit**

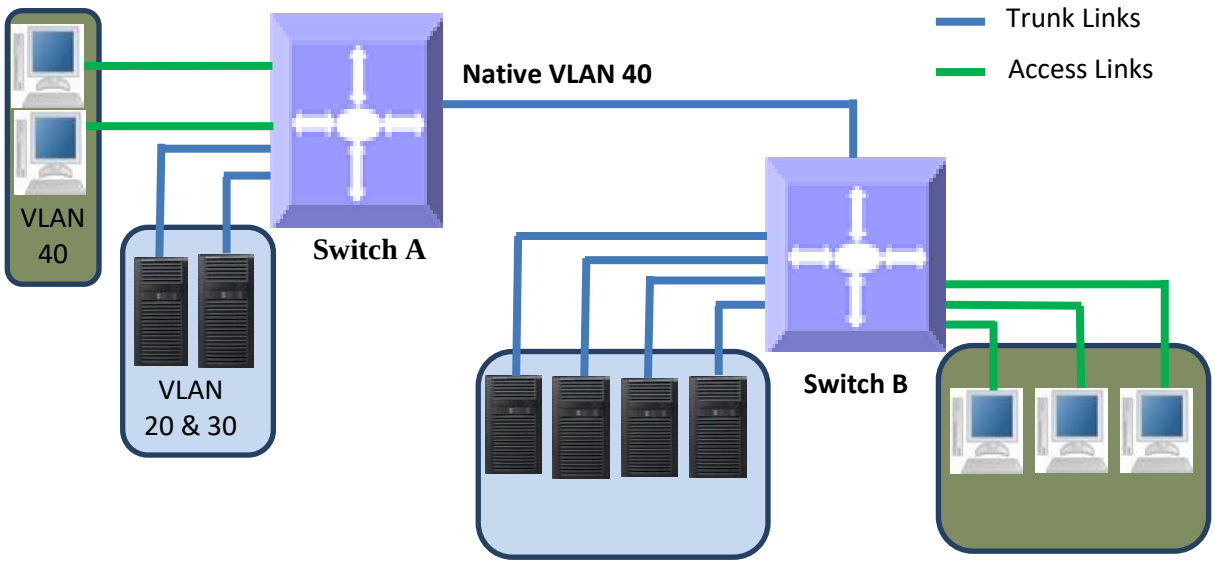
8.2.2 Native VLAN on Trunk

All packets sent out on a trunk interface carry the 802.1Q VLAN tag header. There may be cases in which untagged packets need to be carried over a trunk interface. This is achieved by using the native VLAN feature of the trunk interface.

Any VLAN can be configured on any trunk interface as a native VLAN. Trunk interfaces will send native

VLAN packets as untagged packets without adding the 802.1Q VLAN tag header. Similarly, any untagged packets received on a trunk interface will be considered to be native VLAN packets.
VLAN 1 is the default native VLAN for all trunk interfaces.

Figure VLAN-5: Native VLANs



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

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

Step 4	**switchport trunk native vlan** <*vlan-id* >	*vlan-id* - The VLAN identifiers may be from 1 to 4069. If the given VLAN does not exist, switch will provide a warning message. In this case the native VLAN traffic will be dropped until the VLAN become available. Also, the given VLAN should be part of allowed VLANs in the trunk. If the native VLAN is not member of allowed VLAN list, the native VLAN packets will be dropped.
Step 5	**show vlan port config port** <*iftype*> <*ifnum*> and **show running-config**	Displays the configured native VLAN for this trunk interface.
Step 6	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

The "switchport trunk native vlan" command will be accepted only if the port is in trunk mode.

The "**no switchport trunk native vlan**" command will reset the native VLAN as VLAN 1 for trunk interfaces.

The native VLAN needs to be part of allowed VLANs to pass native VLAN traffic.

The examples below show examples of configuring native VLANs for trunk ports.

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

SMIS# **configure terminal**
SMIS(config)# **vlan 20**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface fx 0/1**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **switchport trunk native vlan 20**
SMIS(config-if)# **exit**

Remove a native VLAN from trunk interface fx 0/1.

SMIS# **configure terminal**
SMIS(config)# **interface fx 0/1**
SMIS(config-if)# **no switchport trunk native vlan**
SMIS(config-if)# **exit**

8.3 Hybrid Ports

Hybrid ports carry both untagged and 802.1Q tagged packets.
Hybrid ports carry the traffic of one or more VLANs. Any switch port can be configured as a hybrid port.
In Supermicro switches, all switch ports by default come up in hybrid mode.
Users need to explicitly add the hybrid ports to all the required VLANs as either tagged or untagged interfaces. A hybrid port could be configured as a tagged or untagged port simultaneously on one or more VLANs.
Users need to configure the PVID for hybrid ports to correctly handle the incoming untagged packets.

It is recommended for users to use hybrid ports only when they thoroughly understand the PVID, tagged and untagged interfaces of their network.

Hybrid ports might cause VLAN packet forwarding drops if the ports are not correctly added to the required VLANs as untagged or tagged interfaces as needed.

Hybrid port functionality can be achieved through trunk ports with allowed VLANs and a native VLAN configuration.

When MAC based VLANs and protocol based VLANs are used, the ports need to be in "Hybrid" mode.

A switch adds the 802.1Q VLAN tag header for VLAN traffic in which the hybrid port is configured as a tagged interface. The switch sends out packets without a VLAN tag header for the VLAN on which the hybrid port is configured as an untagged interface.
When a packet is received on a hybrid port, a switch identifies the VLAN for the received packet from the packet's VLAN tag header. If the received packet did not have a VLAN identifier and the packet did not match any MAC or protocol VLAN, the port PVID is used as the VLAN for all the received untagged and priority tagged packets. If the user has not configured the PVID, VLAN 1 will be used as the default PVID for hybrid ports.
Follow the steps below to configure any port as a hybrid port.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**vlan <***vlan-list***>**	*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma-separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10. If multiple VLANs are provided, the ports configuration provided in the next steps will be applied to all these VLANs.
Step 3	Use steps 3a to 3c below one or more times to configure the required port configurations for the VLANs provided in Step 2 above.	

Step 3a	**ports <***ports-list***> tagged** or **no ports [<***ports-list***>] tagged**	Adds the tagged ports list to this VLAN. *ports-list* – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10. Use the **no** form of this command to remove tagged ports from this VLAN. If *ports-list* is not provided to the **no** command, all the tagged ports are removed from this VLAN.
Step 3b	**ports <***ports-list***> untagged** or **no ports [<***ports-list***>] untagged**	Adds the untagged ports list to this VLAN. *ports-list* – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10. Use the **no** form of this command to remove untagged ports from this VLAN. If *ports-list* is not provided to the **no** command, all the untagged ports are removed from this VLAN.
Step 3c	**ports <***ports-list***> forbidden** or **no ports [<***ports-list***>] forbidden**	Denies traffic from ports given by *ports-list* to this VLAN. *ports-list* – up to three ports or ranges of ports separated by spaces. The range of ports is provided in the format fx 0/1-10, which specifies the ports from fx 0/1 to fx 0/10. Use the **no** form of this command to remove forbidden ports from this VLAN. If *ports-list* is not provided to the **no** command, all the forbidden ports are removed from this VLAN.
Step 4	**Exit**	Exits the VLAN configuration mode.
Step 5	**interface <***interface-type***> <***interface-id***>** or **interface range** <*interface-type*> <*interface-id*> ….	Enters the interface mode. *interface-type* – may be any of the following:

		fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range fx 0/1-10, fx 0/20**
Step 6	**switchport mode hybrid**	Sets the port mode as a hybrid port.
Step 7	**switchport pvid** <*vlan-id*>	Configures the PVID for this interface. The VLANs identifiers could be any VLAN number from 1 to 4069. The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first. This command accepted only when the port is "Hyrbrid" mode.
Step 8	**show vlan port config port** <*iftype*> <*ifnum*> **show running-config** **show vlan**	Displays the configured VLAN and ports information.
Step 9	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

The "ports …" command can be used only for the ports in "hybrid" mode.

The "switchport pvid ..." command will be accepted only when a port is in "hybrid" mode.

A port can be configured as a tagged port for multiple VLANs.

A port can be configured as an untagged port for multiple VLANs. This is useful for MAC based VLANs. For a port based VLAN configuration, having a port as untagged in multiple

VLANs is not a recommended configuration as all the received untagged packets can be associated with only one PVID of that port. In a MAC based VLAN, the received untagged packets will be matched to different VLANs based on the MAC address on the packet.

The examples below show various ways to configure hybrid ports.

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

SMIS# **configure terminal**
SMIS(config)# **vlan 10**
SMIS(config-vlan)# **ports fx 0/1-10 untagged**
SMIS(config-vlan)# **ports cx 0/1 tagged**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface range fx 0/1-10**
SMIS(config-if)# **switchport mode hybrid**
SMIS(config-if)# **switchport pvid 10**
SMIS(config-if**)# exit**

Configure a VLAN 100 with ports fx 0/1, fx 0/10, fx 0/20, fx 0/30, fx 0/40 and cx 0/1-2 as untagged ports and add port channel 1 as a tagged port to this VLAN.

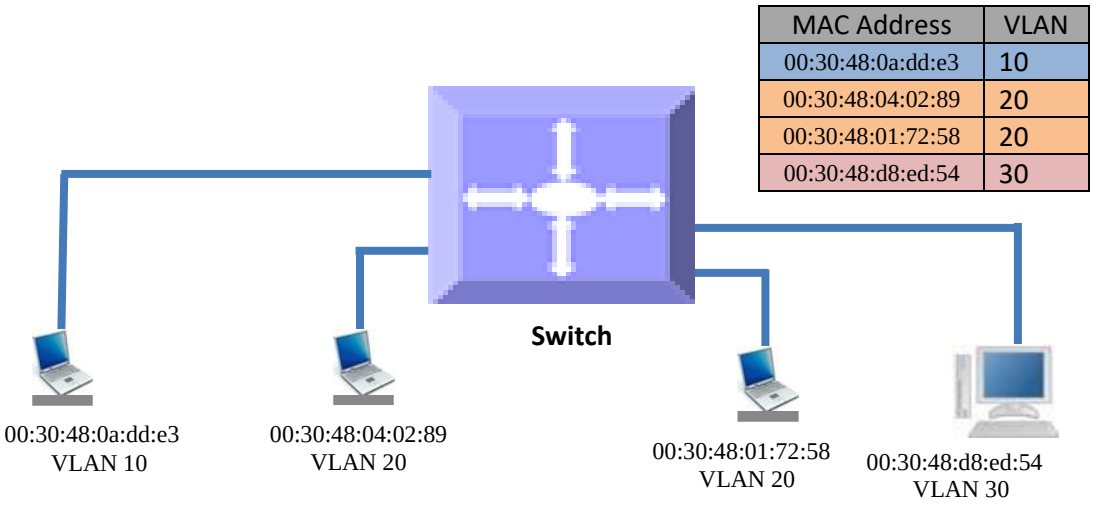
SMIS# **configure terminal**
SMIS(config)# **vlan 100**
SMIS(config-vlan)# **ports fx 0/1 fx 0/10 fx 0/20 untagged**
SMIS(config-vlan)# **ports fx 0/30 fx 0/40 cx 0/1-2 untagged**
SMIS(config-vlan)# **ports po 1 tagged**
SMIS(config-vlan)# **exit**
SMIS(config)# **interface range fx 0/1,fx 0/10, fx 0/20,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

9 MAC Based VLANs

When end users move often from one place to another but remain inside the same LAN, it is difficult to maintain the same VLAN for an end user in a port based VLAN configuration.
MAC based VLAN features are used to provide the same VLAN to any end user irrespective of the switch port the end user is connecting to.
The switch administrator may configure MAC to VLAN mappings for unicast MAC addresses. When a switch receives any untagged packets, the source MAC address of the packet refers to this MAC VLAN mapping to identify the VLAN. If MAC VLAN mapping is not found for the received source MAC address, a protocol based VLAN or port based VLAN is used.

Supermicro switches support 1024 MAC based VLANs.

Figure VLAN-6: MAC Based VLANs



Follow the steps below to configure MAC based VLANs.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**vlan <***vlan-list***>**	Creates the required VLANs. *vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN numbers can be provided as ranges such as 5-10.
Step 3	**ports <***ports-list***> untagged**	Adds the ports given by *ports-list* to this VLAN as untagged ports.

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

User has to create the VLANs using the "**vlan** .." command prior to configuring MAC address VLAN mapping.

The ports required to support MAC VLAN have to be configured as untagged ports in the hybrid mode to those VLANs.

Follow the steps below to remove MAC based VLANs.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**no mac-vlan** <ucast_mac>	Removes MAC VLAN mapping entry. *ucast_mac* – Unicast MAC address for which MAC VLAN mapping is to be removed.
Step 3	**show mac-vlan**	Displays the configured MAC based VLANs.
Step 4	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

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

Create a VLAN 10 and configure MAC address 00:30:40:10:10:10 to VLAN 10 for the ports fx 0/1 to 10
SMIS# **configure terminal**
SMIS(config)# **vlan 10**
SMIS(config-vlan)# ports fx 0/1-10 untagged
SMIS(config-vlan)# **exit**
SMIS(config)# **mac-vlan 00:30:40:10:10:10 vlan 10**

Remove MAC VLAN for MAC address 00:30:40:20:20:20.
SMIS# **configure terminal**
SMIS(config)# **no mac-vlan 00:30:40:20:20:20**

10 Protocol Based VLANs

Protocol based VLAN features help to classify incoming traffic to different VLANs based on the protocol. The protocol or ethertype field in the Layer 2 header is used to classify the packets to different VLANs. Protocol VLAN features are enabled by default in Supermicro switches.
The protocol based VLAN features configuration is a three-step process, as shown in the diagram below.

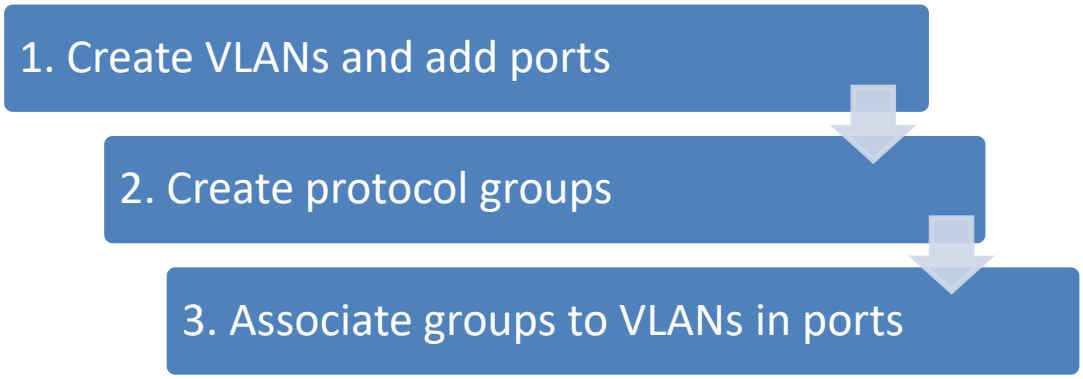


Figure VLAN-7: Protocol Based VLAN Configuration Steps

Follow the steps below to configure protocol based VLANs.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**vlan <***vlan-list***>**	*vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN numbers can be provided as a range, such as 5-10.
Step 3	**ports <***ports-list***> untagged**	Adds the required ports for this VLAN as untagged ports.

		ports-list – up to three ports or three ranges of ports separated by spaces. The range of ports is provided in a format like fx 0/1-10, which refers to ports from fx 0/1 to fx 0/10.
Step 4	**Exit**	Exits the VLAN configuration mode.
Step 5	**map protocol {arp | ip | rarp | ipx | novell | netbios | appletalk | other <***aa:aa or aa:aa:aa:aa:aa***>} {enet-v2 | RFC1042 | llcOther | snap8021H | snapOther} protocols-group <***Group id integer(0-2147483647***) >**	Creates a protocol group. Protocol group creation takes three parameters. First: protocol field as **arp, ip, rarp, ipx,novell, netbios** or **appletalk**. Users can enter any other two-byte protocol fields in hex format as aa:aa. Second: frame type as **enet-v2, llc** or **snap**. Third: protocol group identifier number.
Step 6	**interface <***interface-type***> <***interface-id***>** or **interface range** <*interface-type*> <*interface-id*> ….	Enters the interface mode. *interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It could be the port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g.: **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g.: **int range fx 0/1-10, fx 0/20**
Step 7	**switchport map protocols-group <***Group id integer(0-2147483647***) > vlan <***vlan-id(1-4069***) >**	Associates the group to the VLAN on the above interface. *Group id* – Protocol Group Identifier *vlan-id* – VLAN identifier.

Step 8	**switchport pvid** <*vlan-id*>	Configures the PVID for the default port based VLAN behavior. This will be used for packets that did not match any protocol VLAN map. The VLAN identifiers may be any VLAN number from 1 to 4069. The VLAN provided in this command must exist in the switch. If the VLAN does not exist, create it first.
Step 9	**Exit**	Exits the interface configuration mode.
Step 10	**show vlan protocols-group** **show protocol-vlan**	Displays the configured protocol based VLANs.
Step 11	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

Follow the below steps to remove protocol based VLANs.

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

Step 3	**no switchport map protocols-group <***Group id integer(0-2147483647***) >**	Removes the protocol groups from interface mode. *Group id* – Protocol Group Identifier
Step 4	**Exit**	Exits VLAN configuration mode.
Step 5	**no map protocol {arp | ip | rarp | ipx | novell | netbios | appletalk | other <***aa:aa or aa:aa:aa:aa:aa***>} {enet-v2 | RFC1042 | llcOther | snap8021H | snapOther}**	Removes the protocol group. Before removing any protocol group, it must have been removed from all interfaces.
Step 6	**no vlan <***vlan-list***>** or **vlan <***vlan-list***>** **no ports <***ports-list***> untagged**	Removes the VLANs created for protocol based VLANs. If the VLAN is shared with a MAC or port based VLAN, then remove only the ports added during the protocol based VLAN configuration. To remove the ports use the "no ports" command in the VLAN configuration mode. *vlan-list* – may be any VLAN number or list of VLAN numbers. Multiple VLAN numbers can be provided as comma separated values. Consecutive VLAN numbers may be provided as a range, such as 5-10.
Step 7	**show vlan protocols-group** **show protocol-vlan**	Displays the protocol based VLANs.
Step 8	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

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

Assign all IP traffic to VLAN 20 and all other traffic to VLAN 30 on ports fx 0/1 to fx 0/10.

SMIS# **configure terminal**
SMIS(config)# **vlan 20,30**
SMIS(config-vlan)# **po fx 0/1-10 untagged**
SMIS(config-vlan)# **exit**
SMIS(config)# **map protocol arp enet-v2 protocols-group 1**
SMIS(config)# **map protocol ip enet-v2 protocols-group 2**
SMIS(config)# **int range fx 0/1-10**
SMIS(config-if)# **switchport map protocols-group 1 vlan 20**
SMIS(config-if)# **switchport map protocols-group 2 vlan 20**
SMIS(config-if)# **switchport pvid 30**
SMIS(config-if)# **exit**

Remove protocol VLAN 20.
SMIS# **configure terminal**
SMIS(config)# **int range fx 0/1-10**
SMIS(config-if)# **no switchport map protocols-group 1**
SMIS(config-if)# **no switchport map protocols-group 2**
SMIS(config-if)# **exit**
SMIS(config)# **no map protocol arp enet-v2**
SMIS(config)#**no map protocol ip enet-v2**
SMIS(config)# **no vlan 20**

11 Acceptable Frame Types

By default, Supermicro switch ports accept all frames types – tagged, untagged and priority tagged.

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

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

Users can control this behavior to make switch ports accept either only tagged or untagged and priority tagged packets.
Follow the steps below to configure acceptable frame types for any port or port channel.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**interface <***interface-type***> <***interface-id***>** or **interface range** <*interface-type*> <*interface-id*> ….	Enters the interface mode. *interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers.

		E.g. : **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g. : **int range fx 0/1-10, fx 0/20**
Step 3	Use any of the below steps 3a to 3d to configure acceptable frame types for the ports provided in Step 2 above.	
Step 3a	**switchport acceptable-frame-type tagged**	This command makes only tagged frame types accepted on these ports. Any untagged or priority tagged packets received will be dropped.
Step 3b	**switchport acceptable-frame-type untaggedAndPrioritytagged**	This command makes only untagged and priority tagged frame types accepted on these ports. Any tagged packets received will be dropped.
Step 3c	**switchport acceptable-frame-type all**	This command makes accepting all frame types the default behavior.
Step 3d	**no switchport acceptable-frame-type**	This command makes accepting all frame types the default behavior.
Step 4	**show vlan port config port** <*iftype*> <*ifnum*>	Displays the configured mode and access VLAN for this interface.
Step 5	**write startup-config**	Optional step – saves this VLAN configuration to be part of startup configuration.

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

Configure fx 0/1 to fx 0/10 to accept only untagged and priority tagged packets.

SMIS# **configure terminal**
SMIS(config)# **interface range fx 0/1-10**
SMIS(config-if)# **switchport acceptable-frame-type untaggedAndPrioritytagged**
SMIS(config-if)# **exit**

Configure port channel interface 1 to accept only tagged packets.

SMIS# **configure terminal**
SMIS(config)# **interface po 1**
SMIS(config-if)# **switchport acceptable-frame-type tagged**
SMIS(config-if)# **exit**

12 Ingress Filter

By default, Supermicro switch has the ingress filter enabled. The ingress filter drops packets that do not match the configured VLAN membership.
For example, if the switch has two VLANs configured as 10 and 20, the ports configured with only VLAN 10 can accept packets with the VLAN header having VLAN identifier 20. This is called VLAN hoping. To prevent VLAN hoping, the ingress filter is enabled to drop those packets with a different VLAN identifier than the VLAN configured on the port.
The ingress filter can be disabled to allow VLAN hoping if needed.
Follow the steps below to enable/disable ingress filtering for any port or port channel.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**interface <***interface-type***> <***interface-id***>** or **interface range** <*interface-type*> <*interface-id*> ….	Enters the interface mode. *interface-type* – may be any of the following: fx-ethernet – fx cx-ethernet – cx port-channel – po *interface-id* is in *slot/port* format for all physical interfaces. It may be a port channel identifier for port channel interfaces. To configure multiple interfaces, use the "**interface range** …" command. To provide a range, use a hypen (-) between the start and end interface numbers. E.g. : **int range fx 0/1-10** To provide multiple interfaces or ranges, separate with a comma (,). E.g. : **int range fx 0/1-10, fx 0/20**
Step 3	**switchport ingress-filter** **(or)** **no switchport ingress-filter**	This command enables ingress filtering function. This is the default behavior. The no form of this command disables ingress filtering.
Step 4	**show vlan port config port** <*iftype*> <*ifnum*>	Displays the configured ingress filter mode for this interface.

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

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

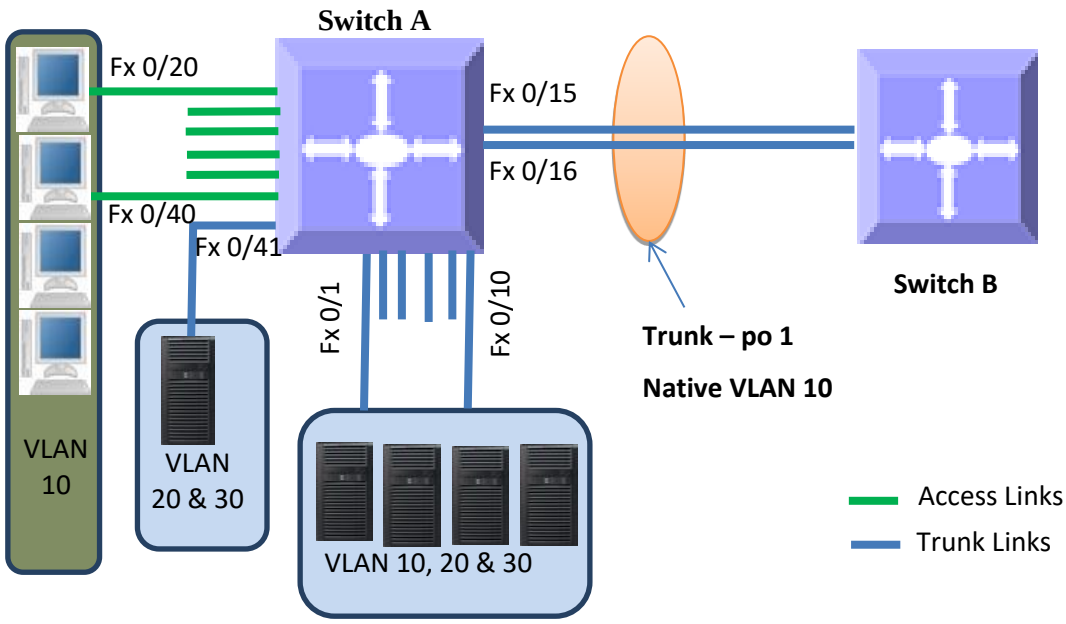
The examples below show how to enable ingress filter on switch ports.
Disable ingress filter for ports fx 0/1 to fx 0/10.
SMIS# **configure terminal**
SMIS(config)# **interface range fx 0/1-10**
SMIS(config-if)# **no switchport ingress-filter**
SMIS(config-if)# **exit**

13 VLAN Configuration Example

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

1. Ports Fx 0/1 to Fx 0/10 are trunk ports connected to servers that have VLANs 10, 20 and 30. Here, VLAN 10 is untagged.
2. Port Fx 0/41 is a trunk port connected to storage, which carries VLAN 20 and 30.
3. Ports Fx 0/20 to Fx 0/40 are access ports for VLAN 10.
4. Ports Fx 0/15 and Fx 0/16 are part of a trunk port channel that carries all the VLANs to other switches with native VLAN 10.

Figure VLAN-8: VLAN Configuration Example



SMIS# **configure terminal**

Create all the VLANs first
SMIS(config)# vlan 10,20,30
SMIS(config-vlan)# exit

Configure VLANs for ports fx 0/1-10
SMIS(config)# **interface range fx 0/1-10**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **switchport trunk native vlan 10**
SMIS(config-if)# **exit**

Configure VLANs for port fx 0/41

SMIS(config)# **int fx 0/41**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **exit**

Configure the access VLAN for ports fx 0/20 to fx 0/40
SMIS(config)# **interface range fx 0/20-40**
SMIS(config-if)# **switchport mode access**
SMIS(config-if)# **switchport access vlan 10**
SMIS(config-if)# **exit**

Configure the port channel trunk interface on fx 0/15 and fx 0/16
SMIS(config)# **interface port-channel 1**
SMIS(config-if)# **exit**
SMIS(config)# **interface range fx 0/15-16**
SMIS(config-if)# **channel-group 1 mode on**
SMIS(config-if)# **exit**
SMIS(config)# **interface port-channel 1**
SMIS(config-if)# **switchport mode trunk**
SMIS(config-if)# **switchport trunk native vlan 10**
SMIS(config-if)# **end**

Check the running-configuration for accuracy
SMIS# show runnning-config

Building configuration...
ID Hardware Version Firmware OS Boot Loader
0 SSE-X3548 1.0.0.0 6 0.0.0.0

ip address 172.31.30.120
interface port-channel 1
exit

Vlans and hybrid mode member ports configurations
vlan 1
ports fx 0/11-14 untagged
ports fx 0/17-19 untagged
ports fx 0/41-48 untagged
ports cx 0/1-6 untagged
exit
vlan 10,20,30
exit

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

```
interface Fx 0/2
 switchport mode trunk
 switchport trunk native vlan 10

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

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

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

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

interface Fx 0/7
 switchport mode trunk
 switchport trunk native vlan 10

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

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

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

interface Fx 0/15
 channel-group 1 mode on

interface Fx 0/16
 channel-group 1 mode on

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

interface Fx 0/21
```

```
 switchport mode access
 switchport access vlan 10

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

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

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

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

interface Fx 0/26
 switchport mode access
 switchport access vlan 10

interface Fx 0/27
 switchport mode access
 switchport access vlan 10

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

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

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

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

interface Fx 0/32
 switchport mode access
 switchport access vlan 10
```

```
interface Fx 0/33
 switchport mode access
 switchport access vlan 10

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

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

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

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

interface Fx 0/38
 switchport mode access
 switchport access vlan 10

interface Fx 0/39
 switchport mode access
 switchport access vlan 10

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

interface po 1
 switchport mode trunk
 switchport trunk native vlan 10

exit
SMIS# show vlan

Vlan database
-------------
Vlan ID: 1
Member Ports: fx 0/1-14 fx 0/17-19 fx 0/41-48 cx 0/1-6 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: fx 0/11-14 fx 0/17-19 fx 0/41-48 cx 0/1-6
Hybrid Forbidden Ports: None
Access Ports: None
```

Trunk Ports: fx 0/1-10 po 1
Name:
Status: Permanent

Vlan ID: 10
Member Ports: fx 0/1-10 fx 0/20-40 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: fx 0/20-40
Trunk Ports: fx 0/1-10 po 1
Name:
Status: Permanent

Vlan ID: 20
Member Ports: fx 0/1-10 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: None
Trunk Ports: fx 0/1-10 po 1
Name:
Status: Permanent

Vlan ID: 30
Member Ports: fx 0/1-10 po 1
Hybrid Tagged Ports: None
Hybrid Untagged Ports: None
Hybrid Forbidden Ports: None
Access Ports: None
Trunk Ports: fx 0/1-10 po 1
Name:
Status: Permanent

SMIS#

14 Private Edge VLAN/Protected Ports

The private edge VLAN (also called the Protected Ports feature) helps to isolate traffic among the same VLAN ports. A protected port cannot forward any traffic to another protected port on the switch even if they are in the same VLAN.
Switch ports can be configured to operate in one of the following three modes.

14.1 Unprotected Port

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

14.2 Protected Port

Protected ports can send and receive traffic only with unprotected ports in the same VLAN. A protected port cannot send or receive traffic with other protected ports or community ports. Protected ports are also called isolated ports.

14.3 Community Port

Community ports can send and receive traffic with unprotected ports and other ports in the same community.

Port Mode	Communicates with
Unprotected Ports	Unprotected Ports Protected Ports Community Ports
Protected Ports	Unprotected Ports
Community Ports	Unprotected Ports Other ports in the same community

15 Unprotected Ports Configuration

By default, all ports are unprotected ports. A protected port or community port can be configured as unprotected port with the below CLI command in interface configuration mode.
noswitchport protected
There is no limit on the number of unprotected ports that can be supported by the switch.

16 Protected Ports Configuration

Any port can be configured as a protected port with the below CLI command in interface configuration mode.
switchport protected
This can be done in the web interface by changing the port mode to "*Protected Port*" on the Protected Ports web configuration page in port manager.
There is no limit on the number of protected ports that can be supported by the switch.

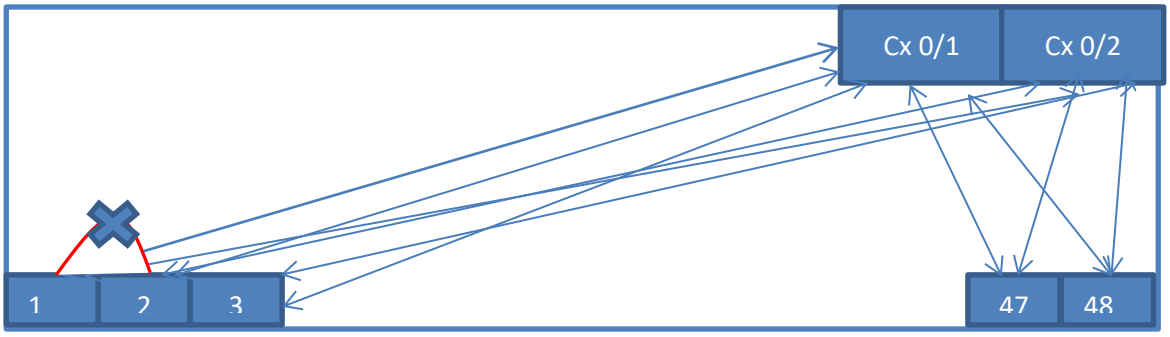
17 Community Ports Configuration

Any port can be configured as a community port with the below CLI command in interface configuration mode.
switchport protected group <group number>
This can be done in the web interface by changing the port mode to "*Protected Port*" and entering the group number on the Protected Ports web configuration page in port manager.
Use the same group number for all the ports in same community. Here, community is identified with the configured group number.
A maximum of 24 different communities can be configured in the switch.

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

17.1 Configuration Example 1

Configure all the 48 downlink Fx ports as isolated (or protected) ports. These 48 ports should not be able to communicate with each other. All these 48 ports should communicate only with the uplink ports cx 0/1 and cx 0/2.



The required configuration for this example is shown below. The uplink ports can be left with their default configuration as unprotected ports. All the downlink 25Gig ports need to be configured as protected ports.

```
SMIS# configure term
SMIS(config)# interface range fx 0/1-48
SMIS(config-if)# switchport protected
SMIS(config-if)# exit
```

17.2 Configuration Example 2

The Fx ports 1 to 24 should be able to communicate among themselves and also should be able to communicate with uplink ports Cx 0/1 and Cx 0/2.
The Fx ports 25 to 48 should be able to communicate among themselves and also should be able to communicate with uplink ports Cx 0/1 and Cx 0/2.
The ports 1 to 24 should not be able to communicate with the ports 25 to 48 and vice versa.
The required configuration for this example is given below. The uplink ports can be left with the default configuration as unprotected ports. The downlink ports 1 to 24 can be configured as one community (group) and ports 25 to 48 can be configured as another community (group).

```
SMIS# configure term
SMIS(config)# interface range fx 0/1-24
SMIS(config-if)# switchport protected group 1
SMIS(config-if)# exit
SMIS(config)# interface range fx 0/25-48
SMIS(config-if)# switchport protected group 2
SMIS(config-if)# exit
```

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