SSE-F3548S/SSE-F3548SR

ACL

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 ACL Overview

ACL is used to filter or redirect any particular traffic flow on the switch.
ACLs can be configured to match packets based on Layer 2 MAC or Layer3 or Layer 4 TCP/UDP parameters.
Every packet entering the switch is checked for the configured ACLs. If any packet contents match any of the configured ACLs, that packet will be handled according to the matched ACL configured action.
The ACL configuration provides the following actions that can be applied on matched traffic flow.

Deny	• **The switch drops all packets matching this ACL**
Redirect	• **The switch redirects all packets matching this ACL to any configured redirect port**
Permit	• **The switch permits all packets matching this ACL**

Supermicro switches implement ACL in hardware ASIC (Application Specific Integrated Circuit) to provide line rate ACL processing for all incoming traffic.
User configured ACL rules are programmed in an ACL table in ASIC. Layer 2 MAC extended ACLs and Layer 3 IP ACLs are implemented in two separate hardware tables, which are TCAM tables in ASIC.
ASIC analyzes the first 128 bytes of every received packet and extracts the packet contents for key fields in the Layer 2, Layer 3 and Layer 4 headers. ASIC then looks up the ACL tables to find a matching ACL rule for the extracted content of the packet. ASIC compares the values of the configured fields only and treats all other fields as “do not care”. Once a matching ACL is found, ASIC stops looking in that ACL table.
ASIC applies the configured action of the matching ACL rule to the matched packet. This could result in it dropping that packet, redirecting it to any particular port or simply allowing the packet to be forwarded through the switch.
A lookup on the Layer 2 and Layer 3 ACL tables happens simultaneously. If any packet matches the ACL rules of both Layer 2 and Layer 3 ACL tables, the actions configured on both ACL rules will be applied. In this case, conflicting actions configured on Layer 2 and Layer 3 ACL tables for the same traffic could lead to unpredictable behavior. Hence, it is suggested to avoid such ACL use cases.

2 Types of ACLs

Supermicro switches support the following three different types of ACLs.

Three types of ACL	MAC Extended ACL
	IP Standard ACL
	IP Extended ACL

2.1 MAC Extended ACL

A MAC Extended ACL allows users to control the traffic based on the fields in Ethernet MAC and VLAN headers.
Users can configure the traffic flow based on the source MAC address, destination MAC address or Ethernet type field value. Users can also use VLAN identifiers to configure the traffic flow.
Users can choose to deny, redirect or permit the configured traffic flow using a MAC Extended ACL.

2.2 IP Standard ACL

An IP Standard ACL allows users to control the traffic based on the fields in an IP header.
Users can configure the traffic flow based on the source IP address and destination IP address.
Users can choose to deny, redirect or permit the configured traffic flow using an IP Standard ACL.

2.3 IP Extended ACL

An IP Extended ACL allows users to control traffic based on fields in an IP header, ICMP header, TCP header and UDP header.
Users can configure the traffic flow based on source IP address, destination IP address,protocol field in IP header, TOS field in IP header or by using a DSCP priority in an IP header.
Users can also configure the traffic flow based on ICMP message type, ICMP message code, TCP port number or UDP port number.
Users can choose to deny, redirect or permit the configured traffic flow using an IP Extended ACL.

3 MAC Extended ACL

Supermicro switches support up to 128 MAC Extended ACLs.
Users can configure a MAC Extended ACL with a deny, permit or redirect action rule. A MAC Extended ACL can be configured only with one rule. To implement multiple rule ACLs, configure multiple MAC Extended ACLs.

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

The permit rule is widely used for QoS applications. In some cases permit rules are useful when all traffic is denied by a rule and a few specific hosts are to be permitted. In this case, permit rules have to be created before deny rules to make sure switch hardware processes permit rules first.
MAC Extended ACLs allow users to configure the traffic flow with the following fields.

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

MAC Extended ACL rules can be created and identified either with an ACL number such as 1, 2 , 3 or with a name string. An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters No special characters are allowed.
User can associate priority values to MAC extended ACL rules. Based on the configured priority, the rules will be orderly arranged in the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. Higher priority ACL rules take precedence over lower priority rules. In case of multiple rules with the same priority value, rules that were created earlier will take precedence over those created later.
If the user does not specify the priority, all rules will have a priority value of 1 by default.

3.1 Creating MAC Extended ACLs

Follow the steps below to create a MAC Extended ACL.

Step	Command	Description
Step 1	configure terminal	Enter the configuration mode
Step 2	mac access-list extended **{ <access-list-number>| <access-list-name> }**	Creates a MAC Extended ACL using the **mac-access-list extended** command. access-list-number–can be any number from 1 to 65535 access-list-name– any name string up to 32 characters.
Step 3	deny { any | host<src-mac-address>} { any | host<dest-mac-address> }<value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>] or	Configures a deny ACL rule, a permit ACL rule or a redirect ACL rule. The source and destination MAC addresses are provided with the keyword host. The keyword anyis used to refer any MAC addresses. If a source or destination MAC address is configured as any, the switch will not

	permit { any | host<src-mac-address>} { any | host<dest-mac-address> } priority<value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>] or redirect<interface-type><interface-id> { any | host<src-mac-address>} { any | host<dest-mac-address> } priority<value (1-65535)>] [Vlan<vlan-id (1-4069)>] [priority<value (1-255)>]	check that source or destination MAC address to match the packets for this ACL. The protocol keyword can be used to configure the Ethernet header Encap Type field to be matched to apply this ACL rule. This protocol is an optional parameter. If not provided, switch will not check this field while matching packets for this ACL. If this ACL rule is to be applied only to a particular VLAN, user can configure VLAN number using Vlan keyword. This Vlan is an optional parameter. If not provided, the switch will not check VLAN while matching packets for this ACL. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1. Redirect ACL rule needs additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
Step 4	show access-lists	Displays the configured ACL rules
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

Every ACL is applied to all ports by default. Any ACL that needs to be applied only to particular ports needs to be configured as described in section Applying MAC Extended ACL to Interfaces**.**

The below examples show various ways of creatinga a MAC Extended ACL.
Create a deny MAC Extended ACL with ACL number 100 to deny all traffic from MAC 00:25:90:01:02:03
SMIS# configure terminal

SMIS(config)# mac access-list extended 100
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 any
Create a permit MAC Extended ACL with ACL name acl_cw3 to permit all traffic from MAC 00:25:30:01:02:03
SMIS# configure terminal
SMIS(config)# mac access-list extended acl_cw3
SMIS(config-ext-macl)# permit host 00:25:30:01:02:03 any
Create a redirect MAC Extended ACL to redirect all packets from MAC 00:25:90:01:02:03going to MAC 00:25:90:01:02:04 to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# mac access-list extended 1
SMIS(config-ext-macl)# redirect fx 0/10 host 00:25:90:01:02:03 host 00:25:90:01:02:04

3.2 Modifying MAC Extended ACLs

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

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

The below example shows a MAC Extended ACL rule 50 that is created and later modified with different parameters.
SMIS# configure terminal
SMIS(config)# mac access-list extended 50
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 any
SMIS(config-ext-macl)# end
Modify this ACL's rule 50 to deny traffic destined to a particular host MAC instead of any
SMIS# configure terminal
SMIS(config)# mac access-list extended 50
SMIS(config-ext-macl)# deny host 00:25:90:01:02:03 host 00:25:90:01:02:04

3.3 Removing MAC Extended ACLs

Follow the steps below to remove MAC Extended ACLs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no mac access-list extended **{ <access-list-number> | <access-list-name> }**	Deletes a MAC Extended ACL using **no mac-access-list extended** command. access-list-number – the ACL number that needs to be deleted

		access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove a MAC Extended ACL.
SMIS# configure terminal
SMIS(config)# no mac access-list extended 50

3.4 Applying MAC Extended ACLs to Interfaces

MAC Extended ACLs are applied to all physical interfaces by default. If users prefer to apply any MAC Extended ACL only to certain ports, the steps below need to be followed.

3.5 ACL Ingress Port Configuration

User can associate an ACL with multiple ingress ports. Follow the steps below to add ingress port(s) to an ACL.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id> or interface range **<interface-type><interface-id> ….**	The port or port lists on which this MAC Extended ACL needs to be applied.
Step 3	mac access-group { **<short (1-32768)> | <string(32)>**}	Adds the MAC Extended ACL to this port. access-list-number – the ACL number that needs to be added access-list-name – the name of the ACL that needs to be added
Step 4	show access-lists	Displays the configured ACL rules to make sure this port is added to the required ACL.
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows applying a MAC Extended ACL rule 100 to ingress ports fx 0/1 and fx 0/10.
SMIS#configure terminal
SMIS(config)# int fx 0/1

SMIS(config-if)# mac access-group 100
SMIS(config-if)# exit
SMIS(config)# int fx 0/10
SMIS(config-if)# mac access-group 100
Removing MAC Extended ACL from ingress port

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	Interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	The port or port lists from which this MAC Extended ACL needs to be removed.
Step 3	no mac access-group { <short (1-32768)> | <string(32)>}	Removes the MAC Extended ACL from this port. access-list-number – the ACL number that needs to be removed from this interface. access-list-name – the name of the ACL which needs to be removed from this interface.
Step 4	show access-lists	Displays the configured ACL rules to make sure this port is removed from required ACL.
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

1. When a MAC Extended ACL is removed from all the ports it was applied to, that ACL will become a switch-wide ACL (applied to all physical ports).
2. MAC Extended ACLs can be added only to physical ports like fx and cx ports. They cannot be added to Layer 3 vlan interfaces or port channel interfaces.
3. A MAC Extended ACL can be applied to many ports by following the above steps. In the same way, many MAC Extended ACLs can be applied to a single port.

The example below shows the commands for removing a MAC Extended ACL from a port.
SMIS#configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# no mac access-group 100

3.6 Displaying MAC Extended ACLs

Step	Command	Description
Step 1	show access-lists	Enters the configuration mode

	or show access-lists mac { <access-list-number (1-32768)> | <access-list-name>]	access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL which needs to be displayed

The show command displays the following information for every MAC Extended ACL:

Filter Priority	ACL's configured or default priority
Protocol Type	Configured protocol. If not configured, it shall be displayed as zero.
Vlan Id	Configured VLAN identifier.
Destination MAC Address	Configured destination host MAC address. Displays 00:00:00:00:00:00 for any destination MAC address
Source MAC Address	Configured source host MAC address. Displays 00:00:00:00:00:00 for any source MAC address
In Port List	The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.
OutPort	The egress port configured for this ACL. If no egress port configured, this will be ALL.
Filter Action	Configured ACL action rule – deny, permit or redirect
Status	Current status of the ACL. The status should normally be ***active***. In the case of configuration errors, the ACL status may be inactive.

The below example displays a MAC Extended ACL.

```
SMIS#show access-lists mac 100
Extended MAC Access List 100
----------------------------
 Filter Priority              : 1
 Protocol Type                : 0
EncapType                    : 0
Vlan Id                      :
 Destination MAC Address     : 00:25:90:01:02:03
 Source MAC Address          : 00:00:00:00:00:00
 In Port List                : Fx0/2
Out Port                     : ALLFilter Action              : Deny
Status                       : Active
```

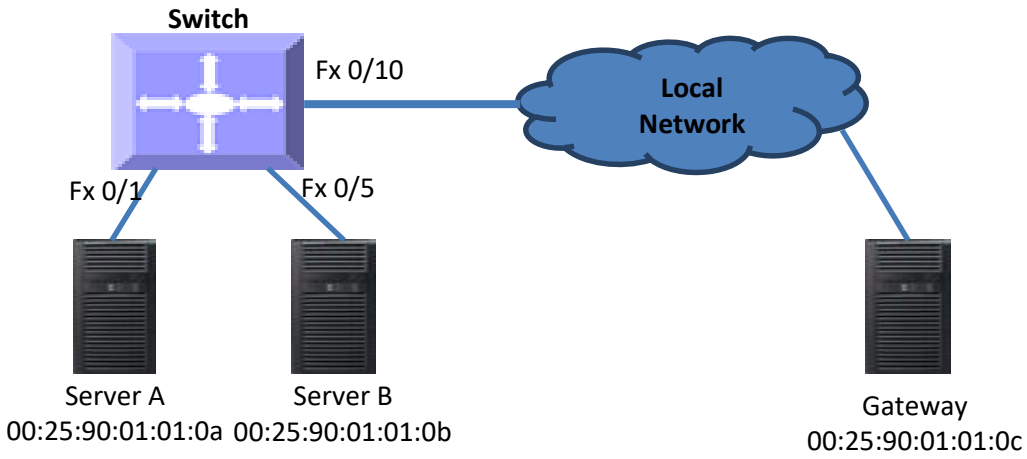
3.7 MAC Extended ACL Configuration

This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-1.

ACL 1 – Deny all traffic going from Server A to the gateway.

ACL 2 – Redirect all vlan 20 traffic coming from the gateway to Server B.

Figure ACL-1: MAC Extended ACL Example 1



ACL 1 Configuration
SMIS# configure terminal
SMIS(config)# mac access-list extended 1
SMIS(config-ext-macl)# deny host 00:25:90:01:01:0a host 00:25:90:01:01:0c
ACL 2 Configuration
SMIS# configure terminal
SMIS(config)# mac access-list extended 2
SMIS(config-ext-macl)# redirect fx 0/5 host 00:25:90:01:01:0c any vlan 20

4 IP Standard ACL

Supermicro switches support 128 IP ACLs, which includes both IP Standard and IP Extended ACLs. Users can define IP Standard ACLs with deny, permit or redirect action rules. An IP Standard ACL can be defined with only one rule. To implement multiple rule ACLs, configure multiple IP Standard ACLs.

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

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

- Source IP Address
- Destination IP Address

IP Standard ACL rules can be created and identified either a with an ACL number as such as 1, 2 or 3 or

with a name string. An ACL identifier number can be any number from 1 to 32768. An ACL identifier name can be any string length not exceeding 32 characters. No special characters are allowed in ACL name strings.

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

Users can associate a priority value to IP standard ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. Higher priority ACL rules take precedence over lower priority rules. In case of multiple rules with the same priority value, the rules that were created earlier will take precedence over those created later.
If the user does not specify the priority, all rules will have a priority value of 1 by default.

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

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

4.1 Creating IP Standard ACLs

Follow the steps below to create anIP Standard ACL.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list standard { <access-list-number(1-32768)> | <access-list-name> }	Creates an IP Standard ACL using ip-access-list standard command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	deny { any | host<ucast_addr> | <ucast_addr><ip_mask> } [{any | host<ip_addr> | <ip_addr><ip_mask> }] [priority<value (1-255)>] or permit { any | host<src-ip-address> | <src-ip-address><mask> } [{ any | host<dest-ip-	Configure a deny ACL rule or permit ACL rule or redirect ACL rule. The source and destination IP addresses are provided with the keyword host. The keyword anyis used to refer to any IP addresses.

	address> | <dest-ip-address><mask> }] [priority<value (1-255)>] or 1. redirect<interface-type><interface-id> { any | host<src-ip-address> | <src-ip-address><mask> } [{ any | host<dest-ip-address> | <dest-ip-address><mask> }] [priority<value (1-255)>]	To configure a network IP, address and mask should be provided. A redirect ACL rule needs additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected. The priority keyword lets user assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

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

The examples below show different ways to create IP Standard ACLs.
Create a deny IP Standard ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 to IP 172.10.10.1
SMIS# configure terminal
SMIS(config)# ip access-list standard 100
SMIS(config-std-nacl)# deny host 172.10.10.10 host 172.10.10.1
Create a permit IP Standard ACL with ACL name acl_cw3 to permit all traffic from IP 172.10.10.1
SMIS# configure terminal
SMIS(config)# ip access-list standard acl_cw3
SMIS(config-std-nacl)# permit host 172.10.10.1 any
Create a redirect IP Standard ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1 to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# ip access-list standard 1
SMIS(config-std-nacl)# redirect fx 0/10 172.20.20.0 255.255.255.0 host 172.20.0.1

4.2 Modifying IP Standard ACLs

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

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

The example below shows anIP Standard ACL rule 50being created and then modified with different parameters.

```
SMIS# configure terminal
SMIS(config)# ip access-list standard 50
SMIS(config-std-nacl)# deny 172.10.0.0 255.255.0.0 any
# Modify this ACL rule 50 to deny traffic destined to a particular host IP instead of to any.
SMIS# configure terminal
SMIS(config)# ip access-list standard 50
SMIS(config-std-nacl)# deny 172.10.0.0 255.255.0.0 host 172.50.0.1
```

4.3 Removing IPStandard ACLs

Follow the below steps to remove IP Standard ACLs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no ip access-list standard { <access-list-number(1-32768)r> | <access-list-name> }	Deletes an IP Standard ACL using no ip-access-list standard command. access-list-number – the ACL number that needs to be deleted access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove an IP StandardACL .

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

4.4 Applying IP ACLs to Interfaces

IP Standard and Extended ACLs are applied to all physical interfaces by default. If users prefer to apply any IP Standard or Extended ACL only to certain ports, the steps below need to be followed.

4.5 ACL Ingress Port Configuration

User can associate an ACL with multiple ingress ports. Follow the steps below to add ingress port(s) to an ACL.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	Defines the port or port lists on which this IP Standard / Extended ACL needs to be applied
Step 3	ip access-group { <access-list -number (1-32768)> | <access-list-name>	Adds the IP Standard / Extended ACL to this ingress port access-list-number – the ACL number that needs to be added access-list-name – the name of the ACL which needs to be added
Step 4	show access-lists	Displays the configured ACL rules to make sure this port has added the required ACL
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration

The example below shows applying anIP Standard ACL rule 100 to ports fx 0/1 and fx 0/10.
SMIS# configure terminal
SMIS(config)# interface fx 0/1
SMIS(config-if)# ip access-group 100
SMIS(config-if)# exit
SMIS(config)# int fx 0/10
SMIS(config-if)# ip access-group 100
Removing anIPStandard / Extended ACL from a port

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	interface <interface-type><interface-id> or interface range <interface-type><interface-id> ….	The port or port lists from which this IP Standard or Extended ACL needs to be removed
Step 3	no ip access-group[{ <access-list-number (1-65535)> | <access-list-name> }]	Removes the IP Standard / Extended ACL from this ingress port access-list-number – the ACL number that needs to be removed from this interface

		access-list-name – the name of the ACL that needs to be removed from this interface
Step 4	show access-lists	Displays the configured ACL rules to make sure this port has been removed from the required ACL
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

1. When an IP Standard/Extended ACL is removed from all the ports it was applied to, that ACL will become a switch wide ACL (applied to all physical ports).
2. IP Standard and Extended ACLs can be added only to physical ports like fx or cx ports. ACLs cannot be added to Layer 3 vlan interfaces or port channel interfaces
3. An IP Standard/Extended ACL can be applied to many ports by following the above steps. In the same way, many IP Standard/Extended ACLs can be applied on a single port.

The example below shows the commands used for removing an IP Extended ACL from a port.
SMIS# configure terminal
SMIS(config)# int fx 0/1
SMIS(config-if)# no ip access-group 100

4.6 Displaying IP Standard ACLs

Step	Command	Description
Step 1	show access-lists or show access-lists ip { <access-list-number (1-32768)> | <access-list-name>]	Enters the configuration mode access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL that needs to be displayed

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

Source IP Address	Configured source host or subnet IP address. Displays 0.0.0.0 for any source IP.
Source IP Address Mask	Configured source subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
Destination IP Address	Configured destination host or subnet IP address. Displays 0.0.0.0 for any destination IP.

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

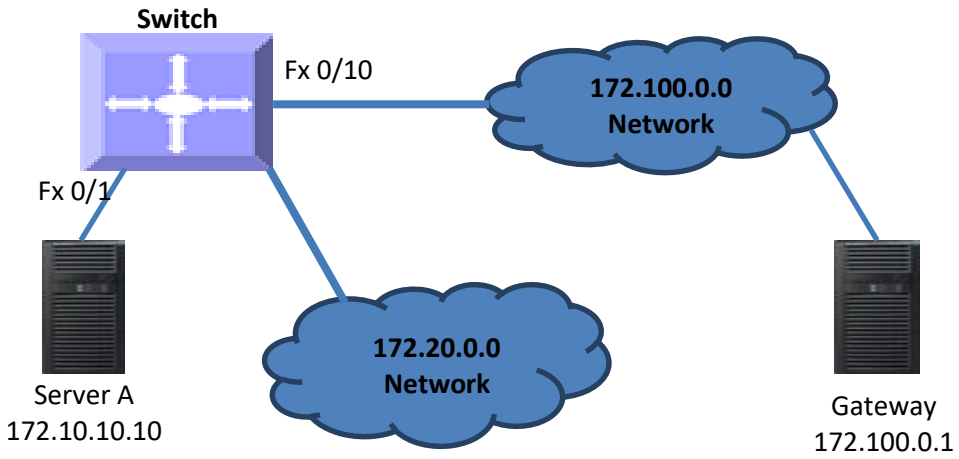
The example below displays an IPStandard ACL
SMIS# show access-lists ip 1
Standard IP Access List 1

Source IP address : 172.20.20.0
Source IP address mask : 255.255.255.0
Destination IP address : 172.20.0.1
Destination IP address mask : 255.255.255.255
In Port List : ALL
Out Port : ALL
Filter Action : Redirect to Fx0/10
Status : Active

4.7 IP Standard ACL Configuration Example 1

This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-2.

ACL 1 – Deny all traffic going from 172.20.0.0 network to 172.100.0.0 network, but allow only server 172.20.20.1 to access the 172.100.0.1 gateway.
ACL 2 – Redirect all traffic destined to IP 172.10.0.0 network to server 172.10.10.10.
Figure ACL-2: IP Standard ACL Example 1



ACL 1 Configuration
This ACL has two rules; one to allow traffic from 172.20.20.1 and the other to deny all traffic from the 172.20.0.0 network.
A permit rule needs to be created first.
SMIS# configure terminal
SMIS(config)# ip access-list standard acl_1a
SMIS(config-std-nacl)# permit host 172.20.20.1 host 172.100.0.1
Then create the deny rule for the subnet 172.20.0.0.
SMIS# configure terminal
SMIS(config)# ip access-list standard acl_1b
SMIS(config-std-nacl)# deny 172.20.0.0 255.255.0.0 172.100.0.0 255.255.0.0
ACL 2 Configuration
SMIS# configure terminal
SMIS(config)# ip access-list standard 2
SMIS(config-std-nacl)# redirect fx 0/1 any 172.10.0.0 255.255.0.0

4.8 IP Extended ACLs

Supermicro switches support 128 IP ACLs, which includes both IP Standard and IP Extended ACLs.
Users can define IP Extended ACLs with deny, permit or redirect action rules. An IP Extended ACL can be defined only with one rule.

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

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

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

- ICMP – Message Type, Message Code

IP Extended ACL rules can be created and identified either a with an ACL number such as 1,2 or 3 or with a name string. ACL identifier numberscan be any number from 1 to 65535. ACL identifier namescan be any string length not exceeding 32 characters.

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

User can associatepriority values to IP Extended ACL rules. Based on the configured priority, the rules will be orderly arranged on the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules takes precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules that created earlier will take precedence over the later ones.
If the user does not specify the priority, by default all rules will have same priority value as 1.

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

4.9 Creating IP Extended ACLs for IP Traffic

Follow the steps below to create an IP Extended ACL for IP, OSPF or PIM traffic.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> | <access-list-name> }	Creates an IP Extended ACL using ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	deny { ip | ospf | pim | <protocol-type (1-255)>} { any | host<src-ip-address> | <src-ip-address><mask> } { any | host<dest-ip-address> | <dest-ip-address><mask> } [{tos<value (0-255)> | dscp<value (0-63)>}] [priority<value (1-255)>] or permit { ip | ospf | pim | <protocol-type (1-255)>} { any | host<src-ip-address> | <src-ip-address><mask> } { any | host<dest-ip-	Configuresa deny, permitor redirect ACL rule. Use the keyword ip to apply this rule to all IP packets. To apply this rule to only OSPF or PIM packets, use the keywords ospf or pimas needed. The source and destination IP addresses can be provided with the keyword host.

	address> | <dest-ip-address><mask> } [{tos<value (0-255)>| dscp<value (0-63)>}] [priority<value (1-255)>] or redirect<interface-type><interface-id> { ip | ospf | pim | <protocol-type (1-255)>} { any | host<src-ip-address> | <src-ip-address><mask> } { any | host<dest-ip-address> | <dest-ip-address><mask> } [{tos<value (0-255)> | dscp<value (0-63)>}] [priority<value (1-255)>]	The keyword anymay be used to refer to any IP addresses. To configure a network IP, address and mask should be provided. To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets.Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP values from 0 to 63. The DSCP configuration is optional. The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It may be any value from 1 to 255. The default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to provide the port to which the packets matching this ACL rule should be redirected.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The examples below show various ways to create an IP Extended ACL for IP traffic.
Create a deny IP Extended ACL with ACL number 100 to deny all traffic from IP 172.10.10.10 with TOS8**.**
SMIS# configure terminal
SMIS(config)# ip access-list extended 100

SMIS(config-ext-nacl)# deny ip host 172.10.10.10 any tos 8
Create a deny IP ExtendedACL with ACL name acl_cw3 to deny all OSPF packets from network 172.20.1.0.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny ospf 172.20.1.0 255.255.255.0 any
Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with DSCP value 10 to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# redirect fx 0/10 ip 172.20.20.0 255.255.255.0 host 172.20.0.1 dscp 10

4.10 Creating IP Extended ACLs for TCP Traffic

Follow the below steps to create an IP Extended ACL for TCP traffic.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> | <access-list-name> }	Creates an IP Extended ACL using the ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	denytcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{ ack | rst }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or permittcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{ ack | rst }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or	Configures a deny, permit or redirect ACL rule. The source and destination IP addresses are provided with the keyword host. The keyword anymay be used to refer to any IP addresses. To configure a network IP, address and mask should be provided. To apply this rule to packets with specific TCP ports, userscan configure either the source or destination TCP ports. The specific TCP port is provided with the keyword eq. To apply this ACL rule to only TCP ACK packets, the keyword ackcan be used. Similarly, to apply this ACL rule to only

	redirect<interface-type><interface-id>tcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{ ack | rst }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>]	TCP RST packets, the keyword rst could be used. To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and specific DSCP values to be matched. Users can specific any DSCP values from 0 to 63. This DSCP configuration is optional. The priority keyword lets users assign a priority to this ACL rule. This priority is an optional parameter. It could be any value from 1 to 255. The default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The examples below show various ways to create IP Extended ACLs for TCP traffic.
Create a deny IP Extended ACL with ACL number 100 to deny all traffic toTCP port 23.
SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny tcp any anyeq 23
Create a deny IP Extended ACL with ACL name acl_cw3 to deny all TCP traffic on 172.20.0.0 network.

SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny tcp any 172.20.0.0 255.255.0.0
Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with TCP ports equal to 1000 to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect fx 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 eq 1000

4.11 Creating IP Extended ACLs for UDP Traffic

Follow the steps below to create an IP Extended ACL for TCP traffic.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended{ <access-list-number(1-32768)> | <access-list-name> }	Creates an IP Extended ACL using the ip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	denyudp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or permitudp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>] or redirect<interface-type><interface-id>tcp {any | host<src-ip-address> | <src-ip-address><src-mask> } [{eq<port-number (0-	Configuresa deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with keyword host. The keyword anycan be used to refer to any IP addresses. To configure a network IP, address and mask should be provided. To apply this rule to packets with specific UDP ports, userscan configure either the source or destination UDP ports. The specific UDP port is provided with the keyword eq. To apply this rule to packets with specific TOS values, use the keyword tos and specify the TOS value to be matched. User can specify any TOS values from 0 to 255. The user provided TOS value will be matched exactly against the type of service byte

	65535)> }] { any | host<dest-ip-address> | <dest-ip-address><dest-mask> } [{eq<port-number (0-65535)> }] [{tos<value (0-255)>|dscp<value (0-63)>}] [priority<short(1-255)>]	on the IPv4 header of the received packets. Hence users have to provide the TOS byte value combining the precedence and type of service fields of IP header. This TOS configuration is optional. To apply this rule to packets with specified DSCP values, use the keyword dscp and the specific DSCP values to be matched. Users can specify any DSCP value from 0 to 63. This DSCP configuration is optional. The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1. A Redirect ACL rule needs additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
Step 4	show access-lists	Displays the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The examples below show various ways to create IP Extended ACLs for TCP traffic.
Create a deny IP Extended ACL with ACL number 100 to deny all traffic toUDP port 1350.
SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny udp any anyeq 1350
Create a deny IP Extended ACL with ACL name acl_cw3 to deny all UDP traffic on 172.20.0.0 network.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny udp any 172.20.0.0 255.255.0.0
Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with destination UDP ports equal to 1000 to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect fx 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 eq 1000

4.12 Creating IP Extended ACLs for ICMP Traffic

Follow the steps below to create an IP Extended ACL for TCP traffic.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	ip access-list extended { <access-list-number(1-32768)> | <access-list-name> }	Creates an IP Extended ACL using theip-access-list extended command. access-list-number – can be any number from 1 to 32768 access-list-name – can be any name string up to 32 characters.
Step 3	denyicmp {any |host<src-ip-address>|<src-ip-address><mask>} {any | host<dest-ip-address> | <dest-ip-address><mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority<(1-255)>] or permiticmp {any |host<src-ip-address>|<src-ip-address><mask>} {any | host<dest-ip-address> | <dest-ip-address><mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority<(1-255)>] or redirect<interface-type><interface-id>icmp {any |host<src-ip-address>|<src-ip-address><mask>} {any | host<dest-ip-address> | <dest-ip-address><mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority<(1-255)>]	Configure a deny, permit or redirect ACL rule. The source and destination IP addresses can be provided with keyword host. The keyword anycan be used to refer to any IP addresses. To configure a network IP, the address and mask should be provided. To apply this rule to ICMP packets with specific message types or message codes, usersshould provide matching values for ICMP message types and ICMP message codes. The priority keyword lets users assign a priority for this ACL rule. This priority is an optional parameter. It can be any value from 1 to 255. The default value is 1. Redirect ACL rules need additional <interface-type><interface-id>parameters to definethe port to which the packets matching this ACL rule need to be redirected.
Step 4	show access-lists	To display the configured ACL rule
Step 5	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The examples below show various ways to create IP Extended ACLs for ICMPpackets.
Create a deny IP Extended ACL with ACL number 100 to deny all ICMP “traceroute” messages.
SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny icmp any any 30
Create a deny IP Extended ACL with ACL name acl_cw3 to deny all ICMP traffic on 172.20.0.0 network.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_cw3
SMIS(config-ext-nacl)# deny icmp any 172.20.0.0 255.255.0.0
Create a redirect IP Extended ACL to redirect all packets from subnet 172.20.20.X going to IP 172.20.0.1with ICMP message type “Destination Unreachable”to interface fx 0/10.
SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect fx 0/10 icmp 172.20.20.0 255.255.255.0 host 172.20.0.1 3

4.13 Modifying IP Extended ACLs

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

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

The example below shows an IP Extended ACL rule 100 being created and then modified with different parameters.
SMIS# configure terminal
SMIS(config)# ip access-list extended 50
SMIS(config-ext-nacl)# deny icmp any 172.10.0.0 255.255.0.0
Modify this ACL rule 50 to deny ICMP redirect messages instead of all ICMP messages
SMIS# configure terminal
SMIS(config)# ip access-list extended 50
SMIS(config-ext-nacl)# deny icmp any 172.10.0.0 255.255.0.0 5

4.14 Removing IP Extended ACLs

Follow the steps below to remove IP Extended ACLs.

Step	Command	Description
Step 1	configure terminal	Enters the configuration mode
Step 2	no ip access-list extended { <access-list-number(1-32768)r> | <access-list-name> }	Deletes an IP Extended ACL using theip-access-list extended command. access-list-number – the ACL number that needs to be deleted

		access-list-name – the name of the ACL that needs to be deleted
Step 3	show access-lists	Displays the configured ACL rules to make sure the deleted ACL is removed properly
Step 4	write startup-config	Optional step – Saves this ACL configuration to be part of startup configuration.

The example below shows how to remove an IP Extended ACL .
SMIS# configure terminal
SMIS(config)# no ip access-list extended 50

4.15 Applying IP Extended ACLs to Interfaces

The procedure to apply IP Extended ACLs to an interface is the same as the procedure used for IP Standard ACLs. Hence, refer to the section Apply IP ACL to Interfaces.

4.16 Displaying IP Extended ACLs

Step	Command	Description
Step 1	show access-lists or show access-lists ext-ip { <access-list-number (1-32768)> | <access-list-name>]	Enters the configuration mode access-list-number – the ACL number that needs to be displayed access-list-name – the name of the ACL that needs to be displayed

This show command displays the following information for every IP Extended ACL.

Filter Priority	Configured or default priority of the ACL
Protocol Type	IP Protocol Type
Source IP Address	Configured source host or subnet IP address. Displays 0.0.0.0 for any source IP.
Source IP Address Mask	Configured source subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.
Destination IP Address	Configured destination host or subnet IP address. Displays 0.0.0.0 for any destination IP.
Destination IP Address Mask	Configured destination subnet IP mask. For host IP address, the mask will be displayed as 255.255.255.255.

In Port List	The list of ports this ACL is applied to. If it is applied to all ports, this will be ALL.
Out Port	The egress port configured for this ACL. If no egress port configured, this will be ALL.
Filter Action	Configured ACL action rule – deny or permit or redirect
Status	Current status of the ACL. The status should normally be ***active*** always. In case of configuration errors, the ACL status may be inactive.
The following fields are displayed for TCP and UDP rules	
Source Ports From	Starting TCP/UDP source port. If the ACL needs to be applied to only one port, the “Ports From” will specify that port. If the ACL needs to be applied to all ports, “Ports From” will be 0.
Source Ports Till	Starting TCP/UDP source port. If the ACL needs to be applied to only one port, the “Ports Till” will specify that port. If this ACL needs to be applied to all ports, “Ports Till” will be 65535.
Destination Ports From	Starting TCP/UDP destination port. If the ACL needs to be applied to only one port, the “Ports From” will specify that port. If the ACL needs to be applied to all ports, “Ports From” will be 0.
Destination Ports Till	Starting TCP/UDP destination port. If the ACL needs to be applied to only one port, the “Ports Till” will specify that port. If the ACL needs to be applied to all ports, “Ports Till” will be 65535.
The following fields are displayed only for TCP rules	
RST bit	If the ACL is applied only to TCP Reset messages
ACK bit	If the ACL is applied only to TCP acknowledgement messages
The following fields are displayed only for ICMP rules	
ICMP type	Displays ICMP types if the ACL is applied only to particular ICMP messages. Displays “No ICMP types to be filtered” if the ACL is applied to all ICMP message types.
ICMP code	Displays ICMP message codes if the ACL is applied only to particular ICMP message codes. Displays “No ICMP codes to be filtered” if the ACL is applied to all ICMP message codes.

The examplesbelow display different IP Extended ACLs.
IP Extended ACLs with IP/OSPF/PIM rules display the following fields:
Filter Priority : 1
Filter Protocol Type : ANY
Source IP address : 172.10.10.10

Source IP address mask : 255.255.255.255
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List : ALL
Out Port : ALL Filter TOS : 0 None
Filter DSCP :
Filter Action : Deny
Status : Active
IP Extended ACLs with TCP rules display the following fields:
SMIS# show access-lists ext-ip 1
Extended IP Access List 1

Filter Priority : 1
Filter Protocol Type : TCP
Source IP address : 172.20.0.0
Source IP address mask : 255.255.0.0
Destination IP address : 0.0.0.0
Destination IP address mask : 0.0.0.0
In Port List : ALL
Out Port : ALL
Filter TOS :
Filter DSCP :
Filter Source Ports From : 0
Filter Source Ports Till : 65535
Filter Destination Ports From : 25
Filter Destination Ports Till : 25
Filter Action : Permit
Status : Active
IP Extended ACLs with ICMP rules display the following fields:
SMIS# show access-lists ext-ip 100
Extended IP Access List 100

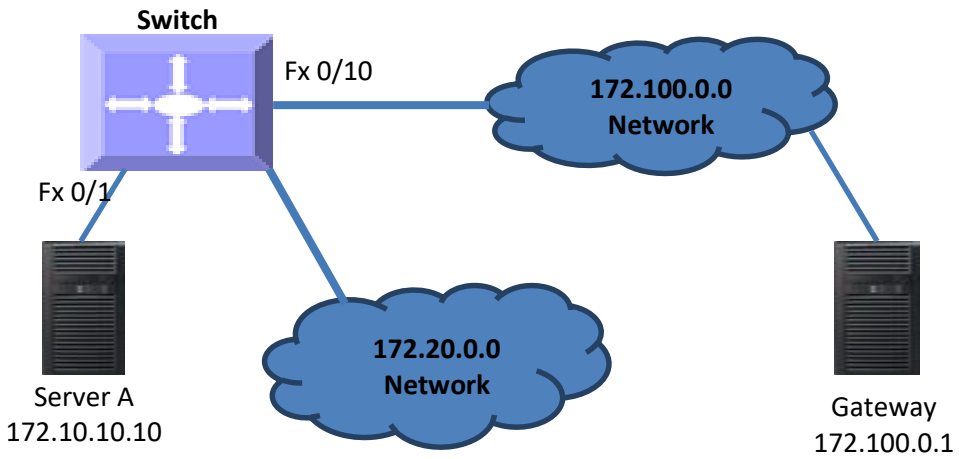
Filter Priority : 1
Filter Protocol Type : ICMP
ICMP type : No ICMP types to be filtered
ICMP code : No ICMP codes to be filtered
Source IP address : 0.0.0.0
Source IP address mask : 0.0.0.0
Destination IP address : 172.10.0.0
Destination IP address mask : 255.255.0.0
In Port List : ALL
Out Port : ALL
Filter Action : Redirect to Fx0/1
Status : Active
SMIS#
IP Extended ACLs with UDP rules display the following fields:
SMIS# show access-lists ext-ip 200

Extended IP Access List 200

Filter Priority : 1
Filter Protocol Type : UDP
Source IP address : 0.0.0.0
Source IP address mask : 0.0.0.0
Destination IP address : 172.100.0.0
Destination IP address mask : 255.255.0.0
In Port List : ALL
Out Port : ALL
Filter TOS :
Filter DSCP :
Filter Source Ports From : 0
Filter Source Ports Till : 65535
Filter Destination Ports From : 1001
Filter Destination Ports Till : 65535
Filter Action : Deny
Status : Active

5 IP Extended ACL Example 1

This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-3.
ACL 1 – Allow SMTP TCP traffic fromthe 172.20.0.0 network and deny all other TCP traffic from this network.
ACL 2 – Redirect all ICMP traffic destined to the IP 172.10.0.0 network to server 172.10.10.10.
ACL 3 –Deny all UDP traffic going to 172.100.0.0 with a destination UDP port greater than 1000.
Figure ACL-3: IP Extended ACL Example 1



ACL 1 Configuration

This ACL has two rules: one to allow traffic from 172.20.20.1 and the other is to deny all traffic from the 172.20.0.0 network.
Create the permit rule first.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_1a
SMIS(config-ext-nacl)# permit tcp 172.20.0.0 255.255.0.0 any eq 25
Then create the deny rule for the subnet 172.20.0.0.
SMIS# configure terminal
SMIS(config)# ip access-list extended acl_1b
SMIS(config-ext-nacl)# deny tcp 172.20.0.0 255.255.0.0 any
ACL 2 Configuration
SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# redirect fx 0/1 icmp any 172.10.0.0 255.255.0.0
ACL 3 Configuration
SMIS# configure terminal
SMIS(config)# ip access-list extended 200
SMIS(config-ext-nacl)# deny udp any 172.100.0.0 255.255.0.0 eq 1000

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