L2 / L3 Switches

Access Control Lists (ACL)

Configuration Guide

Revision 1.1

The information in this USER'S MANUAL has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or 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.

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

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

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

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

Manual Revison 1.1

Release Date: November 6, 2013

Contents

1 ACL Configuration Guide

This document describes the Access Control Lists (ACL) feature supported in Supermicro Layer 2 / Layer 3 switch products.

Access Control List configurations with examples are explained in this document in detail.

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

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

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

In this entire document, the common term “switch” refers to any of the above listed Supermicro switch product models unless another switch product model is named.

ACLs are widely used to provide security and Quality of Service (QoS). This document focuses on ACL configurations only. To learn how to use ACLs for QoS, refer to the QoS Configuration Guide.

1.1 What is ACL

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, Layer 3 IP 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 ACL, that packet will be handled according to the matched ACL configured action.

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**

1.2 How ACL works in Hardware ASIC

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 the ASIC. Layer 2 MAC extended ACL and Layer 3 IP ACL are implemented in two separate hardware tables, which are TCAM tables in the ASIC.

The 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. The ASIC looks up the ACL tables to find a matching ACL rule for the extracted content of the packet. The ASIC compares the values of the configured fields only and it treats all other fields as “do not care”. Once a matching ACL is found, the ASIC stops looking in that ACL table.

The 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 Layer 2 ACL table and Layer 3 ACL table 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.

1.3 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

1.3.1 MAC Extended ACL

A MAC Extended ACL allows users to control the traffic based on fields in Ethernet MAC and VLAN headers.

Users can configure the traffic flow based on 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.

1.3.2 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 source IP address and destination IP address.

Users can choose to deny, redirect or permit the configured traffic flow using an IP Standard ACL.

1.3.3 IP Extended ACL

An IP Extended ACL allows users to control the 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.

1.4 MAC Extended ACL

Supermicro switches support up to 128 MAC Extended ACLs.

Users can define a MAC Extended ACL with a deny, permit, or redirect action rule. A MAC Extended ACL can be defined 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 that the 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 arranged in orderin the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules take precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules created earlier will take precedence over the later ones .

1.4.1 If the user does not specify the priority, by default all rules will have a priority value of 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*> } [**protocol** <*value (1-65535)*>] [**Vlan** <*vlan-id (1-4069)*>] [**priority** <*value (1-255)*>] or **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)*>]	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 **any** is used to refer any MAC addresses. If a source or destination MAC address is configured as **any**, the switch will not 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, 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. Itcan be any value from 1 to 255. The default value is 1. Redirect ACL rule needs additional <*interface-type*> <*interface-id*> parameters to define the 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 the section Applying MAC Extended ACL to Interfaces.

The below examples show various ways of creating 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 00:25:90:01:02:03 going to MAC 00:25:90:01:02:04 to interface gi 0/10.

SMIS# **configure terminal**
SMIS(config)# **mac access-list extended 1**
SMIS(config-ext-macl)# **redirect gi 0/10 host 00:25:90:01:02:03 host 00:25:90:01:02:04**

1.4.2 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**

1.4.3 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**

1.4.4 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.

1.4.4.1 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)>* } **in**	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 gi 0/1 and gi 0/10.

SMIS# **configure terminal**
SMIS(config)# **int gi 0/1**
SMIS(config-if)# **mac access-group 100 in**
SMIS(config-if)# **exit**
SMIS(config)# **int gi 0/10**
SMIS(config-if)# **mac access-group 100 in**

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)>* } **in**	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 gi, ex or qx 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 gi 0/1**
SMIS(config-if)# **no mac access-group 100 in**

1.4.4.2 ACL Egress Port Configuration

User can associate an ACL with only one egress port. Follow the steps below to configure the egress port to an ACL.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**Interface <interface-type> <interface-id>**	The egress port on which this MAC Extended ACL needs to be applied.
Step 3	**mac access-group** { *<short (1-32768)> / <string(32)>* } **out**	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 how to apply a MAC Extended ACL rule 100 to egress port gi 0/1.

SMIS# **configure terminal**
SMIS(config)# **int gi 0/1**
SMIS(config-if)# **mac access-group 100 out**
SMIS(config-if)# **exit**

Removing MAC Extended ACL from egress port

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**Interface <interface-type> <interface-id>**	The egress port from which this MAC Extended ACL needs to be removed.
Step 3	**no mac access-group** { *<short (1-32768)>* | *<string(32)>* } **in**	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 the egress port it was applied to, that ACL will become a switch-wide ACL (applied to all physical ports).
2. MAC Extended ACLs can be configured with only physical egress ports like gi, ex or qx ports. They cannot be configured with port channel interfaces.

The example below shows the commands for removing a MAC Extended ACL from a port.

SMIS# **configure terminal**
SMIS(config)# **int gi 0/1**
SMIS(config-if)# **no mac access-group 100 in**

1.4.5 Displaying MAC Extended ACLs

Step	Command	Description
Step 1	**show access-lists** **or** **show access-lists mac** { *<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 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**.
Out Port	The egress port configured for this ACL. If no egress port has been 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 below example displays a MAC Extended ACL

SMIS# **show access-lists mac 100**
Extended MAC Access List 100

Filter Priority : 1

Protocol Type : 0

Vlan Id :
Destination MAC Address : 00:25:90:01:02:03
Source MAC Address : 00:00:00:00:00:00
In Port List : Gi0/2
Out Port : ALLFilter Action : Deny
Status : Active

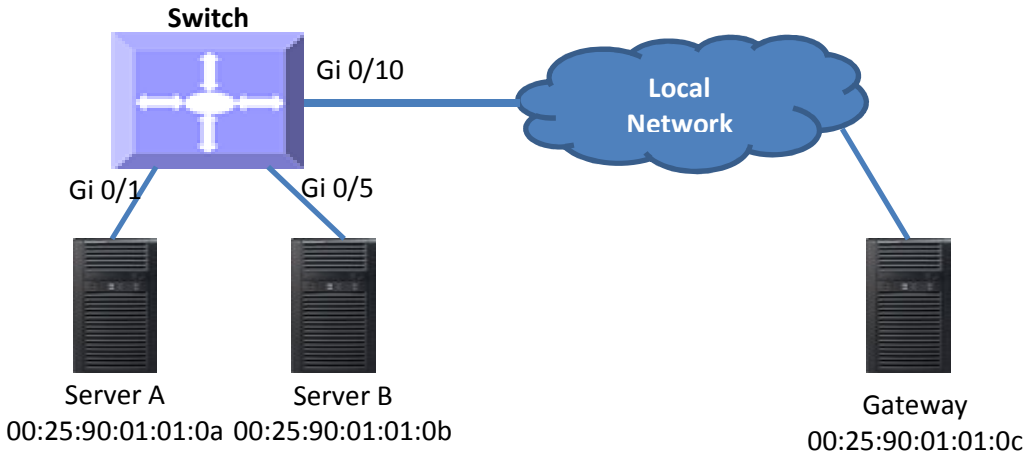
1.4.6 MAC Extended ACL Configuration Example 1

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 gi 0/5 host 00:25:90:01:01:0c any vlan 20**

1.5IP Standard ACLs

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 only with 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 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 an ACL name string.

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 values to IP standard ACL rules. Based on the configured priority, the rules will be arranged in orderon the hardware ACL table. The ACL rules are checked on the incoming packets based on the order of priority. The higher priority ACL rules take precedence over the lower priority rules. In case of multiple rules with the same priority value, the rules 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 of 1.

The priority for the IP standard ACL rule “deny any any” is fixed as 1. Users cannot configure the “deny any any” rule with a different priority value. Since this rule will drop all the IP packets, it 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 with the consideration of both IP standard and

extended ACLs.

1.5.1 Creating IP Standard ACLs

Follow the steps below to create an IP 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-address>* | *<dest-ip-address> <mask>* }] [**priority** *<value (1-255)>*] or **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)>*]	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 **any** is used to refer to any IP addresses. To configure a network IP, address and mask should be provided. A redirect ACL rule needs additional *<interface-type>* *<interface-id>* parameters to define the port to which the packets matching this ACL rule need to be redirected. 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.
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 gi 0/10.

SMIS# **configure terminal**
SMIS(config)# **ip access-list standard 1**
SMIS(config-std-nacl)# **redirect gi 0/10 172.20.20.0 255.255.255.0 host 172.20.0.1**

1.5.2 Modifying IP Standard ACLs

To modify a configured IP Standard ACL, follow the same steps used to create a IP 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 an IP Standard ACL rule 50 being 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**

1.5.3 Removing IP Standard 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 Standard ACL .

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

1.5.4 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.

1.5.4.1 ACL Ingress Port Configuration

Users 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**	Defines the port or port lists on which this IP Standard / Extended ACL needs

	interface range *<interface-type> <interface-id> ….*	to be applied
Step 3	**ip access-group** { *<access-list-number (1-32768)> | <access-list-name> in*	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 an IP Standard ACL rule 100 to ports gi 0/1 and gi 0/10.

SMIS# **configure terminal**
SMIS(config)# **interface gi 0/1**
SMIS(config-if)# **ip access-group 100 in**
SMIS(config-if)# **exit**
SMIS(config)# **int gi 0/10**
SMIS(config-if)# **ip access-group 100 in**

Removing an IP Standard / 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> }*] in	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 gi, ex or qx 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. Same way many IP Standard / Extended ACLs can be applied on a single port.

The example below shows the commands for removing an IP Extended ACL from a port.

SMIS# **configure terminal**
SMIS(config)# **int gi 0/1**
SMIS(config-if)# **no ip access-group 100 in**

1.5.4.2 ACL Egress Port Configuration

User can associate an ACL with only one egress port. Follow the steps below to configure the egress port to an ACL.

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**interface** *<interface-type> <interface-id>*	Defines the egress port on which this IP Standard / Extended ACL needs to be applied
Step 3	**ip access-group** { *<access-list-number (1-32768)> | <access-list-name> out*	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 how to apply an IP Standard ACL rule 100 to egress port gi 0/1.

SMIS# **configure terminal**
SMIS(config)# **interface gi 0/1**
SMIS(config-if)# **ip access-group 100 out**
SMIS(config-if)# **exit**

Removing an IP Standard / Extended ACL from an egress port

Step	Command	Description
Step 1	**configure terminal**	Enters the configuration mode
Step 2	**interface <interface-type> <interface-id>**	The egress port from which this IP Standard or Extended ACL needs to be removed
Step 3	**no ip access-group** [*{ <access-list-number (1-32768)> | <access-list-name> }*] out	Removes the IP Standard / Extended ACL from this egress 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 the egress port 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 gi, ex or qx ports. ACLs cannot be added to Layer 3 vlan interfaces or port channel interfaces.

The example below shows the commands for removing an IP Standard ACL from a port.

SMIS# **configure terminal**
SMIS(config)# **int gi 0/1**
SMIS(config-if)# **no ip access-group 100 out**

1.5.5 Displaying IP Standard ACLs

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

	show access-lists ip { *<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 that needs to be displayed

The **show** 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 IP Standard ACL

SMIS# **show access-lists ip 1**
Standard IP Access List 1

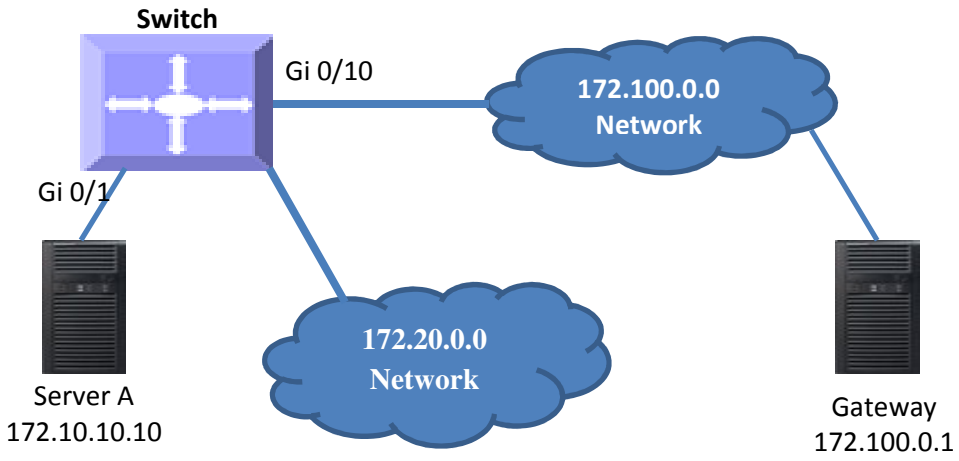
Source IP address:	172.20.20.0
Source IP address mask:	255.255.255.0
Destination IP address:	172.20.0.1
Destination IP address mask:	255.255.255.255
In Port List:	ALL
Out Port:	ALL
Filter Action:	Redirect to Gi0/10
Status:	Active

1.5.6 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 gi 0/1 any 172.10.0.0 255.255.0.0**

1.6 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 numbers can be any number from 1 to 65535. ACL identifier names can 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.

Users can associate priority 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 created earlier will take precedence over the later ones.

If the user does not specify the priority, by default all rules will have the same priority value of 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.

1.6.1 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-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)>*]	Configures a deny, permit or 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 **pim** as needed. The source and destination IP addresses can be provided with the keyword **host**. The keyword **any** may 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. Users can specify any TOS value 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 Extended ACL 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 172.20.0.1 with DSCP value 10 to interface gi 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# redirect gi 0/10 ip 172.20.20.0 255.255.255.0 host 172.20.0.1 dscp 10

1.6.2 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	**deny tcp** {**any** | **host** <*src-ip-address*> | <*src-ip-address*> <*src-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{ **ack** | **rst** }] [{**tos <value (0-255)>** | **dscp** <*value (0-63)*>}] [**priority** <*short(1-255)*>] or **permit tcp** {**any** | **host** <*src-ip-address*> | <*src-ip-address*> <*src-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{ **ack** | **rst** }] [{**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*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*>	Configures a deny, permit or redirect ACL rule. The source and destination IP addresses are provided with the keyword **host**. The keyword **any** may 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, users can configure either the source or destination TCP ports. The specific TCP port is provided with the keyword **eq**. A range of ports is provided with the keyword **range**. Keywords **lt** or **gt** can be used to provide port numbers in less than or greater than conditions. To apply this ACL rule to only TCP ACK packets, the keyword **ack** can be used. Similarly, to apply this ACL rule to only 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. Users can specify any TOS value 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

	| **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{ **ack** | **rst** }] [{**tos <value (0-255)>** | **dscp** <*value (0-63)*>}] [**priority** <*short(1-255)*>]	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 define the 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 to TCP port 23.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny tcp any any eq 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 172.20.0.1 with TCP ports greater than 1000 to interface gi 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 500

SMIS(config-ext-nacl)# redirect gi 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 gt 1000

1.6.3 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	**deny udp** {**any** | **host** <*src-ip-address*> | <*src-ip-address*> <*src-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{**tos <value (0-255)>** | **dscp** <*value (0-63)*>}] [**priority** <*short(1-255)*>] or **permit udp** {**any** | **host** <*src-ip-address*> | <*src-ip-address*> <*src-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{**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 can be provided with keyword **host**. The keyword **any** can 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, users can configure either the source or destination UDP ports. The specific UDP port is provided with the keyword **eq**. A range of ports can be provided with the keyword **range**. Keywords **lt** or **gt** can be used to provide port numbers in less than or greater than conditions. To apply this rule to packets with specific TOS values, use the keyword **tos** and specify the TOS value to be matched. Users 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.

	redirect *<interface-type> <interface-id>* **tcp** {**any** | **host** <*src-ip-address*> | <*src-ip-address*> <*src-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> |**eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] { **any** | **host** <*dest-ip-address*> | <*dest-ip-address*> <*dest-mask*> } [{**gt** <*port-number (0-65535)*> | **lt** <*port-number (1-65535)*> | **eq** <*port-number (0-65535)*> | **range** <*port-number (0-65535)*> <*port-number (0-65535)*>}] [{**tos <value (0-255)>** |**dscp** <*value (0-63)*>}] [**priority** <*short(1-255)*>]	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 define the 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 to UDP port 1350.

SMIS# configure terminal
SMIS(config)# ip access-list extended 100
SMIS(config-ext-nacl)# deny udp any any eq 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 172.20.0.1 with destination UDP ports greater than 1000 to interface gi 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect gi 0/10 udp 172.20.20.0 255.255.255.0 host 172.20.0.1 gt 1000

1.6.4 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 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	**deny 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)>] or **permit 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)>] 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 **any** can 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, users should 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 define the 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 ICMP packets.

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 172.20.0.1 with ICMP message type "Destination Unreachable" to interface gi 0/10.

SMIS# configure terminal
SMIS(config)# ip access-list extended 500
SMIS(config-ext-nacl)# redirect gi 0/10 icmp 172.20.20.0 255.255.255.0 host 172.20.0.1 3

1.6.5 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**

1.6.6 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 the **no ip-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**

1.6.7 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.

1.6.8 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 examples below 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
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 Gi0/1
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

1.6.9 IP Extended ACL Configuration Example 1

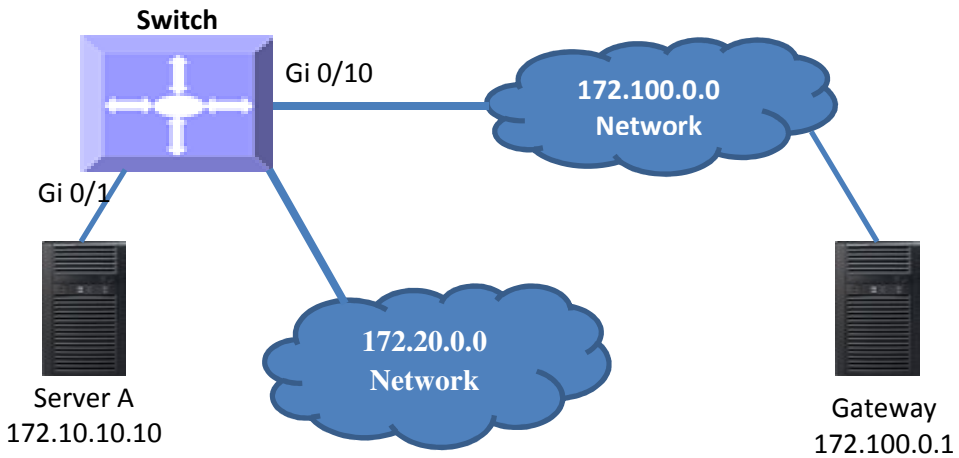
This example describes the commands required to implement the following ACL requirements on the network setup shown in Figure ACL-3.

ACL 1 – Allow SMTP TCP traffic from the 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 gi 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 gt 1000