Access Control

The Access Control List (ACL) feature is part of the security mechanism. ACL definitions serve as one of the mechanisms to define traffic flows that are given a specific Quality of Service (QoS). For more information, see Quality of Service. ACLs enable network managers to define patterns (filter and actions) for ingress traffic. Packets, entering the device on a port or LAG with an active ACL, are either admitted or denied entry. There are three types of ACLs: Mac ACL, IPv4 ACL and IPv6 ACL. All ACL types can be added to device configuration by user settings. The IPv4 ACL type may also be applied as part of the 802.1x authentication and authorization process, for example via the ISE service.

This chapter contains the following sections:

MAC-Based ACL

MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match. To define a MAC-based ACL follow these steps:

Procedure

Step 1 Click **Access Control** > **MAC-Based ACL**.

This page contains a list of all currently defined MAC-based ACLs.

Step 2 Click **Add**.

Step 3 Enter the name of the new ACL in the ACL Name field. ACL names are case-sensitive.

Step 4 Click **Apply**. The MAC-based ACL is saved to the Running Configuration file. To permanently save the configuration click the **Save** icon.

MAC-based ACE

Note Each MAC-based rule consumes one TCAM rule. The TCAM allocation is performed in couples, such that, for the first ACE, 2 TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add Access Control Entries (ACEs) to an ACL, complete the following steps:

Procedure

Step 1 Click **Access Control** > **Mac-Based ACE**.

Step 2 Select an ACL, and click **Go**. The ACEs in the ACL are listed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

Option	Description
ACL Name	Displays the name of the ACL to which an ACE is being added.
Priority	Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority.
Action	Select the action taken upon a match. The options are: • Permit—Forward packets that meet the ACE criteria. • Deny—Drop packets that meet the ACE criteria. • Shutdown—Drop packets that meet the ACE criteria, and disable the port from where the packets were received.
Logging	Select to enable logging of ACL flows that match the ACL rule.
Time Range	Select to enable limiting the use of the ACL to a specific time range.
Time Range Name	If Time Range is selected, select the time range to be used. Time ranges are defined in the System Time Configuration section.
Destination MAC Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination MAC Address Value	Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant).

Option	Description
Destination MAC Wildcard Mask	Enter the mask to define a range of MAC addresses. This mask is different than in other uses, such as a subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to match that value. **Note** Given a mask of 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there are 0's and ignore the bits where there are 1's): You need to translate the binary value to hexadecimal (four bits per hex digit). In this example, since 1111 1111 = FF, the mask would be written as 00:00:00:00:00:FF.
Source MAC Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
Source MAC Address Value	Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant).

Step 5 Click **Apply**. The MAC-based ACE is saved to the Running Configuration file.

IPv4-based ACL

ACLs can be used as the building elements of the flow definitions for per-flow QoS handling. To check the IPv4 packets, use the IPv4-based ACLs. To define an IPv4-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv4-Based ACL**.

This page contains all currently defined IPv4-based ACLs.

Step 2 Click **Add**.

Step 3 Enter the name of the new ACL in the ACL Name field. The names are case-sensitive.

Step 4 Click **Apply** to save the IPv4-based ACL to the Running Configuration file.
The IPv4-based ACL Table displays the following types of IPv4 ACLs:

a. ACLs added by the user - indicated with a Static value in the Originator column. These ACLs are created and controlled by the user.

b. ACLs added dynamically – ACLs added to a device by an authentication server (such as ISE) as part of the 802.1x authentication process. The user cannot modify or change this type of ACLs.

IPv4-Based ACE

Note Each IPv4-based rule consumes one TCAM rule. The TCAM allocation is performed in couples, such that, for the first ACE. Two TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add rules (ACEs) to an IPv4-based ACL, follow these steps:

Note Rules can be added, removed and edited only for ACLs created by the user. For ACLs created dynamically, the Add and Edit buttons will be grayed out.

Procedure

Step 1 Click **Access Control** > **IPv4-Based ACE**.

Step 2 Select an ACL, and click **Go**. All currently defined IP ACEs for the selected ACL are displayed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

ACL Name	Displays the name of the ACL to which an ACE is being added.
Priority	Enter the priority. ACEs with higher priority are processed first. **Note** One is the highest priority.
Action	Select the action assigned to the packet matching the ACE from the following options: • Permit—Forward packets that meet the ACE criteria. • Deny—Drop packets that meet the ACE criteria. • Shutdown—Drop packets that meet the ACE criteria, and disable the port to which the packets are addressed. Ports are reactivated on the Error Recovery Settings page.
Logging	Select to enable logging of ACL flows that match the ACL rule.
Time Range	Select to enable limiting the use of the ACL to a specific time range
Time Range Name	If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used. Time ranges are described in the System Time section.

Protocol	Select to create an ACE based on a specific protocol or protocol ID. Select Any (IPv4) to accept all IP protocols. Otherwise select one of the following protocols: • ICMP—Internet Control Message Protocol • IGMP—Internet Group Management Protocol • IP in IP—IP in IP encapsulation • TCP—Transmission Control Protocol • EGP—Exterior Gateway Protocol • IGP—Interior Gateway Protocol • UDP—User Datagram Protocol • HMP—Host-Mapping Protocol • RDP—Reliable Datagram Protocol • IDPR—Inter-Domain Policy Routing Protocol • IPV6—IPv6 over IPv4 tunneling • IPV6:ROUT—Matches packets belonging to the IPv6 over IPv4 route through a gateway • IPV6:FRAG—Matches packets belonging to the IPv6 over IPv4 Fragment Header • IDRP—Inter-Domain Routing Protocol • RSVP—ReSerVation Protocol • AH—Authentication Header • IPV6:ICMP—Internet Control Message Protocol • EIGRP—Enhanced Interior Gateway Routing Protocol • OSPF—Open the Shortest Path First • IPIP—IP in IP • PIM—Protocol Independent Multicast • L2TP—Layer 2 Tunneling Protocol • ISIS—IGP-specific protocol • Protocol ID to Match—Instead of selecting the name, enter the protocol ID.
Source IP Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
Source IP Address Value	Enter the IP address to which the source IP address is to be matched and its mask (if relevant).

Source IP Wildcard Mask	Enter the mask to define a range of IP addresses. This mask is different than in other uses, such as a subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value. **Note** Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111, you need to translate the one's to a decimal integer and you write 0 for every four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255.
Destination IP Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination IP Address Value	Enter the IP address to which the destination MAC address is matched and its mask (if relevant).
Destination IP Wildcard Mask	Enter the destination IP wildcard mask.
Source Port	Select one of the following • Any—Match to all source ports. • Single from list—Select a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • Single by number—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • Range—Enter a range 0–65535.
Destination Port	Select one of the available values. They are the same as for the Source Port field described above. **Note** You must specify the IPv4 protocol for the ACL before you can configure the source and/or destination port.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. For each type of flag, select one of the following options: • Set—Match if the flag is SET. • Unset—Match if the flag is Not SET. • Don’t care—Ignore the TCP flag.

Type of Service	The service type of the IP packet. • Any—Any service type • DSCP to match—Differentiated Serves Code Point (DSCP) to match. • IP Precedence to match—IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the three significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
ICMP	If the ACL is based on ICMP, select the ICMP message type that is used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select Any. • Any—All message types are accepted. • Select from list—Select message type by name from the drop-down list. • ICMP Type to match—Number of message types that is to be used for filtering purposes.
ICMP Code	The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options to configure whether to filter on this code: • Any—Accept all codes. • User Defined—Enter an ICMP code for filtering purposes.
IGMP	If the ACL is based on IGMP, select the IGMP message type to be used for filtering purposes. Either select the message type by name or enter the message type number: • Any—All message types are accepted. • Select from list—Select message type by name. • IGMP Type to match—Number of message types that is to be used for filtering purposes.

Step 5 Click **Apply**. The IPv4-based ACE is saved to the Running Configuration file.

IPv6-Based ACL

The IPv6 based ACL check the IPv6-based traffic. ACLs are also used as the building elements of flow definitions for per-flow QoS handling. To define an IPv6-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv6-Based ACL**.

Step 2 Click **Add**.

Step 3 Enter the name of a new ACL in the ACL Name field. The names are case-sensitive.

Step 4 Click **Apply**. The IPv6-based ACL is saved to the Running Configuration file.

IPv6-Based ACE

Note Each IPv6-based rule consumes two TCAM rules.

To define an IPv6-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv6-Based ACE**.

This window contains the ACE (rules) for a specified ACL (group of rules).

Step 2 Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

ACL Name	Displays the name of the ACL to which an ACE is being added.
Priority	Enter the priority. ACEs with higher priority are processed first.
Action	Select the action assigned to the packet matching the ACE from the following options: • Permit—Forward packets that meet the ACE criteria. • Deny—Drop packets that meet the ACE criteria. • Shutdown—Drop packets that meet the ACE criteria, and disable the port to which the packets addressed. Ports are reactivated on the Error Recovery Settings page.
Logging	Select to enable logging ACL flows that match the ACL rule.
Time Range	Select to enable limiting the use of the ACL to a specific time range
Time Range Name	If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used. Time ranges are described in the System Time section.

Protocol	Select to create an ACE based on a specific protocol from the following options:
	• Any (IPv6)—All source IPv6 addresses apply to the ACE
	• Select from list- select from one of the following options:
	  • TCP—Transmission Control Protocol Enables two hosts to communicate and exchange data streams TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they sent.
	  • UDP—User Datagram Protocol Transmits packets but doesn't guarantee their delivery.
	  • ICMP—Matches packets to the Internet Control Message Protocol (ICMP).
	• Protocol ID to match—Enter the ID of the protocol to be matched.

Source IP Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
Source IP Address Value	Enter the IP address to which the source IP address is to be matched and its mask (if relevant).
Source IP Prefix Length	Enter the prefix length of the source IP address.
Destination IP Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination IP Address Value	Enter the IP address to which the destination MAC address is matched and its mask (if relevant).
Destination IP Prefix Length	Enter the prefix length of the IP address.
Source Port	Select one of the following • Any—Match to all source ports. • Select from list—Select a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • By number—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu.
Destination Port	Select one of the available values. They are the same as for the Source Port field described above. **Note** You must specify the IPv6 protocol for the ACL before you can configure the source and/or destination port.
Flow Label	Classifies IPv6 traffic based on a IPv6 Flow label field. This is a 20-bit field that is part of the IPv6 packet header. An IPv6 flow label can be used by a source station to label a set of packets belonging to the same flow. Select Any if all flow labels are acceptable or select User defined and then enter a specific flow label to be accepted by the ACL.

TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. For each type of flag, select one of the following options: • Set—Match if the flag is SET. • Unset—Match if the flag is Not SET. • Don't care—Ignore the TCP flag.
Type of Service	The service type of the IP packet. • Any—Any service type • DSCP to match—Differentiated Serves Code Point (DSCP) to match. • IP Precedence to match—IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
ICMP	If the ACL is based on ICMP, select the ICMP message type that is used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select Any. • Any—All message types are accepted. • Select from list—Select message type by name from the drop-down list. • ICMP Type to match—Number of message types that is to be used for filtering purposes.
ICMP Code	The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options, to configure whether to filter on this code: • Any—Accept all codes. • User Defined—Enter an ICMP code for filtering purposes.

Step 5 Click **Apply**.

ACL Binding (VLAN)

When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that don't match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets. Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy-map, and binding that policy-map to the interface. After an ACL is bound to an interface, it can't be edited, modified, or deleted until it's removed from all the ports to which it's bound or in use.

Note It's possible to bind an interface (port, LAG, or VLAN) to a policy or to an ACL, but they can't be bound to both a policy and an ACL. In the same class map, a MAC ACL can't be used with an IPv6 ACE that has a Destination IPv6 address as a filtering condition.

To bind an ACL to a VLAN, follow these steps:

Procedure

Step 1 Click **Access Control** > **ACL Binding (VLAN)**.

Step 2 To edit a VLAN, select a VLAN and click **Edit**.

If the VLAN you require isn't displayed, add a new one by clicking **Add.** And continue to the next step.

Step 3 Select one of the following:

MAC-Based ACL	Select a MAC-based ACL to be bound to the interface.
IPv4-Based ACL	Select an IPv4-based ACL to be bound to the interface.
IPv6-Based ACL	Select an IPv6-based ACL to be bound to the interface.
Default Action	Select one of the following options: • Deny Any—If a packet doesn't match an ACL, it's denied (dropped). • Permit Any—If a packet doesn't match an ACL, it's permitted (forwarded). **Note** Default Action can be defined only if IP Source Guard isn't activated on the interface.

Step 4 To copy an existing VLAN, click **Copy** (copy icon). If you wish to delete a VLAN from the Binding Table, click **Delete**.

Step 5 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

ACL Binding (Port)

Access Control List (ACL) is a list of permissions applied on a port that filters the stream of packets transmitted to the port. A port is bound with either a policy or an ACL, but not both. The default action is to discard (Deny any) all of the packets that don't meet the rules in an ACL. You can override the default action of an ACL to forward those packets by configuring Permit Any on the desired ports.

To bind an ACL to a port or LAG, follow these steps:

Procedure

Step 1 Click **Access Control** > **ACL Binding (Port)**.

Step 2 Select an interface type Ports/LAGs (Port or LAG).

Step 3 Click **Go**. For each type of interface selected, all interfaces of that type are displayed with a list of their current ACLs (for Input ACLs and Output ACLs):

Interface	Identifier of the interface on which ACL is defined.
MAC ACL	ACLs of type MAC that is bound to the interface (if any).
IPv4 ACL	ACLs of type IPv4 that are bound to the interface (if any).
IPv6 ACL	ACLs of type IPv6 that are bound to the interface (if any).
Default Action	Action of the ACL's rules (drop any/permit any).

Step 4 To edit an interface, select the interface, and click **Edit**.

Step 5 Enter the following for both the Input ACL and Output ACL:

MAC-Based ACL	Select a MAC-based ACL to be bound to the interface.
IPv4-Based ACL	Select an IPv4-based ACL to be bound to the interface.
IPv6-Based ACL	Select an IPv6-based ACL to be bound to the interface.
Default Action	Select one of the following options: • Deny Any—If a packet doesn't match an ACL, it's denied (dropped). • Permit Any—If a packet doesn't match an ACL, it's permitted (forwarded). **Note** Default Action can be defined only if IP Source Guard isn't activated on the interface.

Step 6 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

IPv4 per Interface ACL

To view details about ACLs and ACEs which were applied to a port, complete the following:

Procedure

Step 1 Click **Access Control > IPv4 per Interface ACL** and select the require interface.

Step 2 In the Filter section, select the **Interface** from the drop-down menu and click **Go**. The ACLs are shown according to the interface selected.

Step 3 The ACLs are displayed in the IPv4 per Interface ACL table according to the interface selected. The default values are populated based on the first port. If the value in the Protocol, Source Port, Destination Port or ICMP Type is mapped to a specific protocol, application or ICMP, then the value displayed in the column is the mapped value and not the numerical value received.

Step 4 Click the **Authenticated Sessions** Table button to navigate to **Security > 802.1x Authentication > Authenticated Sessions**.