# Access Control Lists (ACLs)

## Contents

- **Overview** ........................................................................................................... 7-2
- **Stateful ACLs** ..................................................................................................... 7-2
- **ACL Types** ........................................................................................................... 7-3
  - Standard IP ACLs .................................................................................................. 7-3
  - Extended IP ACLs .................................................................................................. 7-3
  - MAC Standard ACLs ............................................................................................. 7-4
  - MAC Extended ACLs ............................................................................................. 7-4
- **ACL Rules** ........................................................................................................... 7-4
  - Precedence ............................................................................................................. 7-5
  - Filters ..................................................................................................................... 7-5
  - Operation ............................................................................................................... 7-6
- **ACL Strategies** .................................................................................................... 7-8
- **Configuring ACLs** .............................................................................................. 7-10
  - Creating ACLs ...................................................................................................... 7-10
  - Configuring Rules for ACLs .................................................................................... 7-13
    - Creating Rules for Standard IP ACLs ................................................................. 7-14
    - Creating Rules for Extended IP ACLs ................................................................. 7-16
    - Creating Rules for MAC Extended ACLs ......................................................... 7-23
  - Modifying ACL Rules ............................................................................................. 7-25
- **Applying ACLs to Interfaces** ............................................................................. 7-26
- **Using ACLs with DHCP Services** ................................................................. 7-28
- **Viewing ACL Statistics** ...................................................................................... 7-28
Access Control Lists (ACLs)
Overview

Overview

You can configure access control lists (ACLs) on the ProCurve Wireless Edge Services xl Module to control traffic to and from wireless stations. An ACL is an ordered list of rules that select packets according to header information and dictate whether the module should permit (forward) or deny (drop) those packets.

ACLs allow you to control wireless users’ network rights. You can configure ACLs for purposes such as:

- limiting certain groups of wireless users to Internet access only
- permitting certain groups of wireless users access to a limited list of network servers
- limiting certain groups of wireless users to certain types of applications
- restricting access to a particular private server to a select group of users only

You can also use ACLs to select traffic for Network Address Translation (NAT). See Chapter 8: Configuring Network Address Translation (NAT) to learn how to configure this feature of the Wireless Edge Services xl Module’s firewall.

Stateful ACLs

The Wireless Edge Services xl Module’s ACLs are stateful. In other words, the module tracks traffic associated with a particular session. Once it has permitted one packet in a session, it permits all packets necessary for that session. For example, if you create a rule to permit traffic from wireless stations to an HTTP server, you do not need to create a rule to permit the HTTP server’s return traffic.
ACL Types

The Wireless Edge Services xl Module supports two basic ACL types:

- **IP ACLs**—based on the IP header (Layer 3)
  
  IP ACLs control traffic *inbound* on an interface. They can apply to the Wireless Edge Services xl Module’s virtual LAN (VLAN) interfaces or to its two physical interfaces: the internal uplink and downlink ports. If applied to a physical port, the IP ACLs control inbound traffic on all VLANs tagged for that interface.

- **MAC ACLs**—based on the Media Access Control (MAC) header (Layer 2)
  
  Standard MAC ACLs are used for MAC authentication. You can apply extended MAC ACLs to the module’s physical interfaces, but not to its VLAN interfaces. Like IP ACLs, the extended MAC ACLs affect *inbound* traffic.

Both types of ACLs include two subtypes: standard and extended.

**Standard IP ACLs**

Standard IP ACLs permit and deny traffic according to source IP addresses. They match inbound traffic based on the following IP header fields:

- **source IP address**—either any IP address, an individual (“host”) IP address, or all IP addresses in a particular subnetwork

- **WLAN index**—the index number (1 through 32) of the WLAN through which the packet arrived (for physical interfaces only)

You can apply a standard IP ACL to inbound traffic on either a logical (VLAN or tunnel) interface or a physical (internal uplink or downlink) interface. When you apply an ACL to a logical interface, the traffic must be routed to be filtered.

**Extended IP ACLs**

Extended IP ACLs can permit and deny traffic according to more sophisticated criteria than standard IP ACLs. They match inbound traffic based on the following IP header fields:

- **source and destination IP address**—either any IP address, an individual (“host”) IP address, or all IP addresses in a particular subnetwork

- **ICMP message type and code**

- **TCP and UDP source and destination ports**

- **WLAN index**—the index number (1 through 32) of the WLAN through which the packet arrived (for physical interfaces only)
Access Control Lists (ACLs)

Overview

You can apply an extended IP ACL to inbound traffic on either a logical (VLAN or tunnel) interface or a physical (internal uplink or downlink) interface. Again, an ACL on a logical interface only affects traffic that the Wireless Edge Services xl Module actually routes.

MAC Standard ACLs

MAC standard ACLs permit and deny traffic according to the source MAC address in the frame. The Wireless Edge Services xl Module uses these ACLs to implement local MAC authentication, restricting access to WLANs according to stations’ MAC addresses. For more information on these ACLs, see “MAC Filters (Local MAC Authentication)” on page 13-74 of Chapter 13: Wireless Network Management.

MAC Extended ACLs

MAC extended ACLs permit and deny traffic according to the source and destination MAC addresses, as well as other information in the MAC header, such as the encapsulated protocol, the VLAN tag, or the 802.1p priority.

You can apply a MAC extended ACL to inbound traffic on a physical (internal uplink or downlink) interface.

When you apply the ACL to the uplink interface, the ACL examines the Ethernet header for traffic that arrives on the uplink port from the wired network.

When you apply the ACL to the downlink interface, the ACL examines the encapsulated 802.11 header for traffic that arrives from RPs on the downlink port. The ACL also examines the Ethernet header after the Wireless Edge Services xl Module bridges the traffic from the WLAN to the VLAN.

ACL Rules

An ACL consists of one or more rules, which the Wireless Edge Services xl Module processes in order. Each rule performs two functions:

- selects traffic according to the filters that you configure
- performs an operation on the selected traffic

For all ACL types, rules include the following specifications:

- **precedence**—the order in which the rule is processed
- **filters**—the criteria by which a rule selects packets
- **operation**—the action that the Wireless Edge Services xl Module takes on traffic selected by a rule
Access Control Lists (ACLs)

Overview

All ACLs include an implicit “deny any” rule at the end. In other words, if traffic does not match any of the ACLs rules, the ACL drops the traffic. MAC standard ACLs, which are configured as filters for local MAC authentication, are the exception. They include an implicit “permit any” rule at the end. See “MAC Filters (Local MAC Authentication)” on page 13-74 of Chapter 13: Wireless Network Management.

Precedence

An ACL’s rules are processed in ascending numeric order until a “match” is found for the packet or frame. When the Wireless Edge Services x1 Module matches traffic to the rule, the rule has “selected” the traffic. The module then performs the operation defined for the rule.

Each ACL has a list of ordered rules separate from all other ACLs. For example, two ACLs can each have one rule with a precedence value of 1.

Filters

Filters specify the information that a packet’s header must match. As discussed in “ACL Types” on page 7-3, valid fields depend on the ACL type. A packet or frame must match every filter that you specify.

Rules for all ACL types can include these filters:

- source address, either IP or MAC address
  The filter can select:
  - all addresses
  - a single address
  - a range of addresses, specified either by subnetwork address and prefix length (for IP ACLs) or by mask (for MAC extended ACLs)

- WLAN index number (from 1 through 32)
  The traffic must arrive from this WLAN to match the rule. This setting is optional and takes effect only for ACLs applied to physical interfaces. You should only use it for the ACLs applied to the downlink port.

Extended IP ACL rules can include these additional filters:

- destination IP address
  The filter can select:
  - all addresses
  - a single address
  - a range of addresses, specified by subnetwork address and a prefix length
Access Control Lists (ACLs)

Overview

- protocol
  By default, a rule matches all IP packets, but you can limit the rule to a specific protocol including:
  - ICMP
  - TCP
  - UDP
- for ICMP packets, ICMP type and ICMP code
- for TCP and UDP packets, source and destination ports

In this way, you can control traffic according to the application. For example, configure a rule to select Web traffic by specifying the TCP protocol and destination port 80.

Extended MAC ACL rules can include these additional filters:
- the destination MAC address, either a single address or a range of addresses (specified by a mask)
- VLAN ID—a specific VLAN ID number
- 802.1p priority—the traffic service class used for quality of service (QoS)
- EtherType—the Layer 3 protocol encapsulated in the frame:
  - IPv4—Internet Protocol, version 4
  - ARP—Address Resolution Protocol
  - RARP—Reverse Address Resolution Protocol
  - AppleTalk
  - AARP—AppleTalk Address Resolution Protocol
  - 802.1q—VLANs
  - IPX—Internetwork Packet Exchange
  - IPv6—Internet Protocol, version 6

Operation

The module takes one of the following actions on packets selected by a rule:
- **deny**—the module drops the selected traffic
- **permit**—the module forwards the selected traffic
- **mark**—the module marks the selected traffic for a certain type of QoS and forwards the traffic
Access Control Lists (ACLs)
Overview

**Permit and Deny.** These operations allow you to control users’ network access.

Remember, the operation only affects traffic that meets *all* of the criteria of the rule. Also, the operation is explicit. That is, the module performs the operation on selected traffic, but *does not* perform the opposite action on traffic that is not selected. Instead, the module attempts to match the traffic against the next rule in order of precedence.

However, all ACLs include an implicit **deny any** rule at the end, which drops all traffic not selected by other rules. In other words, traffic is permitted only if explicitly permitted by one of the ACLs rules. Therefore, whenever you apply an ACL to an interface, make sure that you include a rule to permit all traffic that you want the Wireless Edge Services xl Module to forward.

**Mark.** Besides deny and permit, a third operation is mark, which marks traffic for a particular type of QoS or Type of Service (TOS). Marked traffic is also forwarded. The mark operation only takes effect for ACLs applied to physical interfaces.

Two protocols define QoS classes:

- **802.1p**—a mechanism for implementing QoS at Layer 2

  802.1p divides traffic into different classes and provides expedited service to traffic in higher-priority classes. Eight different classes of service (0 through 7) are available. The class is indicated in three bits of an 802.1Q VLAN tag. Table 7-1 shows the type of service typically associated with each 802.1p class. However, the actual treatment for each class is left to your network implementation. The Wireless Edge Service xl Module simply marks traffic for a particular class.

<table>
<thead>
<tr>
<th>Priority Value</th>
<th>Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 and 2</td>
<td>lowest priority (background)</td>
</tr>
<tr>
<td>0 and 3</td>
<td>default priority (best effort)</td>
</tr>
<tr>
<td>4 and 5</td>
<td>higher priority (video and voice)</td>
</tr>
<tr>
<td>6 and 7</td>
<td>highest priority (network control traffic)</td>
</tr>
</tbody>
</table>
Access Control Lists (ACLs)

Overview

- **TOS**—a mechanism for implementing QoS at Layer 3

  The value for the IP header’s one-byte TOS field can range from 0 through 255. Typically, only values 0 through 63 are used—the six-bit Differential Services (DiffServ) Code Point (DSCP) values. (The other two bits make up the explicit congestion notification field.)

  Again, higher values typically receive higher priority, but the exact handling depends on your network’s implementation.

ACL Strategies

The Wireless Edge Services xl Module’s ACLs can enforce a variety of flexible policies. Within a given rule, or among the rules in a given ACL, you can combine filter criteria—for example, to filter based on a port number and source and destination addresses, or based on an Ethertype and a WLAN index value, and so on.

Example policies include:

- limiting a particular subnetwork to accessing certain servers only

  For example, your Wireless Edge Services xl Module places wireless traffic in VLAN 8 (192.168.8.0/24). You want to limit the wireless users to accessing a Web server. You would create an extended IP ACL and add a permit rule with the destination address of the Web server. The source address would be 192.168.1.0, and the prefix length would be 24.

  You would then apply the ACL to inbound traffic on VLAN 8. The module only forwards traffic matching the permit rule (that is, traffic destined to the Web server).

- marking traffic destined for a particular port (or range of ports) for QoS or TOS

  You may want to mark time-sensitive traffic, which is often destined to one of UDP’s real-time ports, for higher QoS. For example, to mark traffic destined for UDP port 1720 with a TOS value, you would create an extended IP ACL with a rule that includes these specifications:
  - a mark operation and the desired TOS value
  - the UDP protocol
  - the 1720 destination port

  The source and destination wildcard/masks would both be set to “any,” and you would not specify the WLAN index.
Access Control Lists (ACLs)
Overview

- permitting or denying traffic based on the WLAN from which it arrives

Perhaps your Wireless Edge Services xl Module places all wireless traffic in the same VLAN, VLAN 16. However, one WLAN grants guests access, and you want to prohibit guest access to VLAN 2, which include servers holding sensitive information.

When you configure the extended IP ACL to control traffic that arrives on the VLAN 16 interface, add a rule that does the following:

- denies traffic destined to the VLAN 2 subnetwork
- specifically selects traffic from the guest WLAN

Make sure that this rule has a lower precedence order than any rule that permits traffic to VLAN 2.

As you configure ACLs, remember that they always have an implicit "deny any" operation at the end; any traffic not specifically permitted by the rules within an ACL will be denied.
Configuring ACLs

To configure an ACL, you must complete these steps:
1. Create the list and select the ACL type.
2. Create a series of ordered permit, deny, or mark rules.
3. Apply the list to an interface.

Do not complete the final step if you are using a standard IP ACL for a function other than controlling traffic. These functions include:

- **NAT**—The ACL selects traffic for dynamic source NAT; you specify the ACL in the NAT configuration. See Chapter 8: Configuring Network Address Translation (NAT).
- **secure Network Time Protocol (NTP)**—The ACL selects which hosts are allowed to send specific types of NTP communications. See “Applying ACLs to NTP Services” on page 2-146 of Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module.

Creating ACLs

To create an ACL, complete these steps:
1. Select **Security > ACLs > Configuration**.
2. Click the Add button. The Add ACL screen is displayed. (See Figure 7-2.)
3. In the ACL Type field, use the drop-down menu to select either the standard IP, extended IP, or MAC extended ACL type.

4. In the ACL ID field, specify the ACL ID, which uniquely identifies the ACL. ACL IDs can be either an ASCII string or a numeric value. Follow these rules:
   - String names for ACL IDs can contain alphanumeric characters as well as the hyphen ( - ) and underline ( _ ) characters; spaces and other nonalphanumeric characters are not allowed.
   - Valid numeric ACL IDs depend on the ACL type; use the range of values listed in Table 7-2.

Table 7-2. ACL Types and ACL ID Ranges

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>ACL ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard IP access list</td>
<td>1-99 and 1300-1999</td>
</tr>
<tr>
<td>Extended IP access list</td>
<td>100-199 and 2000-2699</td>
</tr>
<tr>
<td>MAC extended access list</td>
<td>Any number outside of the ranges 1-199 and 1300-2699</td>
</tr>
</tbody>
</table>

The numeric value of the ACL ID does not affect the precedence of ACLs. However, precedence is important for the rules inside of a particular ACL; you will set these precedence values later when you configure ACL rules.

5. Click the OK button. The ACL is now listed in the ACLs section of the Security > ACLs > Configuration screen.
After you create an ACL, you must add rules to it. These rules actually select and control the traffic.

For each ACL rule, you must specify the following:

- the rule’s precedence
- the operation (deny, permit, or mark) that the Wireless Edge Services xl Module performs on selected packets
- the filters that select a packet or frame according to fields in the header

You can configure up to 500 rules for each ACL, no matter what its type.
Creating Rules for Standard IP ACLs

The standard IP ACL offers a variety of options for rules. However, some of these options only take effect on certain interfaces. As you create the rule, keep in mind the interface for which you are designing this ACL. In Table 7-3, an X under the interface means that the option is supported for that interface.

Table 7-3. Valid Options for Standard IP ACLs Depending on Interface

<table>
<thead>
<tr>
<th>Option</th>
<th>VLAN/Tunnel Interface</th>
<th>Uplink Port</th>
<th>Downlink Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>permit operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mark operation</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>source IP address and mask</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WLAN index</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

To create a rule for a standard IP ACL, complete these steps:

1. On the Security > ACLs > Configuration screen, in the ACLs section, select a standard IP ACL.
2. Click the Add button under Associated Rules. The Add Rule screen is displayed.
3. In the **Precedence** field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services xl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on), in case you need to insert new rules “between” existing rules later.

4. In the **Operation** field, use the drop-down menu to select the operation (**deny**, **permit**, or **mark**) for the rule.

**Note**

The mark operation *only* takes effect if you apply this ACL to a physical interface.

5. Optionally, check the **Logging** box to allow the module to keep track of the number of packets matched to this rule.

6. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255.

   Standard DSCP values are from 0 through 63.

   Remember that higher values typically mark traffic for better QoS.
In the **Source Wildcard/Mask** field, use the drop-down menu to select one of the following:

- **any**—The rule will apply to traffic from any IP address. (This allows you to filter traffic based on fields other than the source IP address.)
- **host**—The rule will apply specifically to a single source IP address. Enter this address in the **Source Address** field.
- **numbers 1 through 31**—The rule selects traffic from an entire subnetwork with the specified prefix length. Enter the subnetwork’s network address in the **Source Address** field.

For example, you select **24** in the **Source Wildcard/Mask** field and **192.168.8.0** in the **Source Address** field. The rule matches only the first 24 bits (three octets) of source IP addresses against the specified source address. Any packet from the 192.168.8.0/24 subnetwork is selected.

If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the **Wlan Index** field, specify the index number (from 1 through 32) of the WLAN from which traffic must arrive.

If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.

---

**Note**

The WLAN filter *only* takes effect if you apply this ACL to a physical interface. However, you should *never* specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not marked for a WLAN, so the rule will not select any traffic.

---

9. Click the **OK** button to apply the rule.

The rule is now listed in the **Associated Rules** section of the Security > ACLs > Configuration screen (when the corresponding ACL is selected).

Remember to click the **Save** link to preserve the configuration.

**Creating Rules for Extended IP ACLs**

Configuring rules for an extended IP ACL is similar to configuring rules for standard IP ACLs. However, these rules can also select traffic by protocol, application, and destination IP address.

Refer to Table 7-4 to verify that a particular option is supported for the interface to which you plan to apply the ACL. An X under the interface means that the option is supported for that interface.
To create a rule for an extended IP ACL, complete these steps:

1. On the **Security > ACLs > Configuration** screen, in the **ACL** section, select an extended IP ACL.

2. Click the **Add** button under **Associated Rules**. The **Add Rule** screen is displayed.

### Table 7-4. Valid Options for Extended IP ACLs Depending on Interface

<table>
<thead>
<tr>
<th>Option</th>
<th>VLAN/Tunnel Interface</th>
<th>Uplink Port</th>
<th>Downlink Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>permit operation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mark operation</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>source IP address and mask</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>destination IP address and mask</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>protocol</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>protocol options</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>WLAN index</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Access Control Lists (ACLs)
Configuring ACLs

Figure 7-5. Add Rule Screen for Extended IP ACLs

3. In the **Precedence** field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services xl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

   As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on) in case you need to insert new rules in between existing rules later.

4. In the **Operation** field, use the drop-down menu to select the operation (**deny**, **permit**, or **mark**) for the rule.

   **Note**
   
   The mark operation *only* takes effect if you apply this ACL to a physical interface.

5. Optionally, check the **Logging** box to allow the module to keep track of the number of packets matched to this rule.
6. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255. Standard DSCP values are from 0 through 63.

   Remember that higher values typically mark traffic for better QoS.

7. Under **Filter**, use the **Protocol** drop-down menu to select the protocol:
   - `icmp`
   - `ip`
   - `tcp`
   - `udp`

   The ACL rule matches traffic that uses the specified protocol. You can make the filter more specific than the protocol alone. That is, if you choose `icmp`, `tcp`, or `udp`, you should specify protocol options that select certain types of ICMP, TCP, or UDP traffic, based on information in the respective protocol header. If you select `ip`, the rule selects any IP packet that matches other filters, and you cannot specify special protocol options.

8. If you selected `icmp`, `tcp`, or `udp` in step 7, click the **Protocol Options** button.
   a. If you selected the ICMP protocol, the **ICMP Options** screen is displayed. (See step b on page 7-21 if you selected the TCP or UDP protocol.)

![Add Rule > ICMP Options](image)

**Figure 7-6. ICMP Options Screen**

The **ICMP Type** and **ICMP Code** settings are based on the first 16 bits of the 32-bit ICMPv6 message packet, illustrated in Figure 7-7.
In the ICMPv6 message packet:

- The ICMP type value is based on the first eight bits (bits 0 through 7). ICMP type values from 0 through 127 are used for error messages, and ICMP type values from 128 through 255 are used for information messages.
- The ICMP code value is based on the second eight bits (bits 8 through 15). This value depends on the ICMP message type, and specifies the type of packet with more granularity.

Table 7-5 lists common ICMP types and the corresponding ICMP codes. Use this table to find the correct values for the packets that you want to control, and then enter the values in the **ICMP Type** and **ICMP Code** fields of the **ICMP Options** screen.

Click the **OK** button to return to the **Add Rule** screen and finish configuring other filters.

### Table 7-5. ICMP Types and Codes

<table>
<thead>
<tr>
<th>ICMP Type</th>
<th>Type Description</th>
<th>ICMP Code</th>
<th>Code Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination Unreachable message</td>
<td>0</td>
<td>No route to destination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Communication with destination administratively prohibited</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>(Not assigned)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Address unreachable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Port unreachable</td>
</tr>
<tr>
<td>2</td>
<td>Packet Too Big message</td>
<td>0</td>
<td>Set to 0 by the sender and ignored by the receiver</td>
</tr>
<tr>
<td>3</td>
<td>Time Exceeded message</td>
<td>0</td>
<td>Hop limit exceeded in transit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Fragment reassembly time exceeded</td>
</tr>
</tbody>
</table>
b. If you selected the TCP or UDP protocol, the TCP/UDP Options screen is displayed. Specify the source and destination ports for selected traffic in the respective Source Options and Destination Options sections:
   - Use the drop-down menu to select Equals (for one specific port) or Range (for a range of ports).
   - Enter the port number in the field beneath the drop-down menu.

Valid values are from 1 through 65,535. As shown in Figure 7-8, if you select Range, you must enter two port numbers: one for the low end of the range and one for the high end. The range is inclusive.

You do not have to specify both source and destination ports. Set the destination port to control traffic associated with a particular VLAN. For example, set the destination port to 80 to select HTML traffic.
Access Control Lists (ACLs)
Configuring ACLs

Click the OK button to return to the Add Rule screen and finish configuring other filters.

9. In the Source Wildcard/Mask field, use the drop-down menu to select one of the following:
   - **any**—The rule will apply to traffic from any IP address. (This allows you to filter traffic based on fields other than the source IP address.)
   - **host**—The rule will apply specifically to a single source IP address. Enter this address in the Source Address field.
   - **numbers 1 through 31**—The rule selects traffic from an entire subnetwork with the specified prefix length. Enter the subnetwork's network address in the Source Address field.

For example, you select 24 in the Source Wildcard/Mask field and 192.168.8.0 in the Source Address field. The rule matches only the first 24 bits (three octets) of source IP addresses against the specified source address. Any packet from the 192.168.8.0/24 subnetwork is selected.

10. In the Destination Wildcard/Mask and Destination Address fields, specify the destination address for selected traffic in the same way that you specified the source address.

11. If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the Wlan Index field, specify the index number (from 1 through 32) of the WLAN from which traffic must arrive.

If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.

**Note**

The WLAN filter only takes effect if you apply this ACL to a physical interface. You should never specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not marked for a WLAN, so the rule will not select any traffic.

12. Click the OK button to apply the rule.

The rule is now listed in the Associated Rules section of the Security > ACLs > Configuration screen (when the corresponding ACL is selected).

Remember to click the Save link to preserve the configuration.
Creating Rules for MAC Extended ACLs

To create a rule for a MAC extended ACL, complete these steps:

1. On the Security > ACLs > Configuration screen, in the ACL section, select a MAC extended ACL.

2. Click the Add button under Associated Rules. The Add Rule screen is displayed.

3. In the Precedence field, specify the precedence for the rule, from 1 through 5,000. The Wireless Edge Services xl Module processes rules in ascending order (starting at 1, moving to 2, and so on).

   As you assign precedence values to rules for a given ACL, consider using nonconsecutive numbers (for example, 10, 20, 30, and so on) in case you need to insert new rules in between existing rules later.
4. In the **Operation** field, use the drop-down menu to select the operation (deny, permit, or mark) for the rule.

5. If you selected the **mark** operation in step 4, under **Attribute to mark**, select one of the following:
   - **802.1p**—Then specify the traffic service class value, from 0 through 7.
   - **TOS**—Then specify the value for the TOS octet, from 0 through 255. Standard DSCP values are from 0 through 63.

   Remember that higher values typically mark traffic for better QoS.

6. In the **Source Wildcard** field, type one of the following:
   - **any**—The rule will apply to traffic sent from any device. (This allows you to filter traffic based on fields other than the source MAC address.)
   - **host**—The rule will apply to traffic from a specific device only. Enter this device’s MAC address in the **Source Address** field.
   - **MAC address mask**—The rule will apply to a range of MAC addresses. Enter the mask in standard six-octet MAC address format (XX-XX-XX-XX-XX-XX, in which you replace “Xs” with “Fs” to match octets and “0s” to ignore the bit).

   Then enter a MAC address in the **Source Address** field.

   For example, you enter a MAC address mask of FF-FF-FF-00-00-00 and an address of 00:C0:49:00:00:00. The rule matches source MAC addresses to the first three octets and ignores the next three octets.

7. In the **Destination Wildcard** and **Destination Address** fields, specify the destination MAC address or addresses. Use the same rules discussed in the previous step.

8. If you plan to apply this rule to the downlink port, you can optionally specify the WLAN. In the **Wlan Index** field, specify the index number (from 1 through 32) of the WLAN from which traffic must arrive.

   If you do not specify a WLAN index, the rule will apply to any traffic that matches other filters.

---

**Note**

You should *never* specify a WLAN index for an ACL that you apply to the uplink port. Traffic from the uplink port is not marked for a WLAN, so the rule will not select any traffic.
9. Optionally, check the box to filter frames according to the following criteria:
   - **Vlan ID**—Select traffic with the specified VLAN ID
     Valid values range from 1 through 4,095.
   - **802.1p Priority**—Select traffic with the specified QoS class.
     Valid values range from 0 through 7.
   - **Ethertype**—Select traffic according to the encapsulated protocol. Use the drop-down menu to select:
     - **IPv4**—Internet Protocol, version 4
     - **ARP**—Address Resolution Protocol
     - **RARP**—Reverse Address Resolution Protocol
     - **AppleTalk**
     - **AARP**—AppleTalk Address Resolution Protocol
     - **802.1q**—VLANs
     - **IPX**—Internetwork Packet Exchange
     - **IPv6**—Internet Protocol, version 6

10. Click the **OK** button to apply the rule.

### Modifying ACL Rules

You might need to change a rule to fix a mistake or to respond to changing policies. To modify an ACL rule, complete these steps:

1. Select **Security > ACLs > Configuration**.
2. Select the ACL in the **ACLs** section.
3. Select the ACL rule in the **Associated Rules** section.
4. Click the **Edit** button. The **Edit Rule** screen is displayed.
5. Make the necessary changes.
6. Click **OK**.

The edited rule replaces the old rule in the **Associated Rules** section.
Applying ACLs to Interfaces

An ACL does not take effect on the Wireless Edge Services xl Module until you apply it to an interface. Although you can create and configure many ACLs, you are limited in the number of ACLs that you can apply:

- You can apply one IP ACL to each logical (VLAN or tunnel) interface. See “IP Settings” on page 6-3 in Chapter 6: IP Services—IP Settings, DHCP, and DNS to learn how to create a VLAN interface.
- You can apply one IP ACL and one MAC extended ACL to the module’s internal uplink port.
- You can apply one IP ACL and one MAC extended ACL to the module’s internal downlink port.

The Wireless Edge Services xl Module filters all traffic that is inbound to a physical (uplink or downlink) port with the ACLs applied to those ports.

On the other hand, the module filters only traffic that is inbound to a logical (VLAN or tunnel) interface and routed to another interface.

Packets inbound to a VLAN or tunnel interface include:
- packets from the wireless network that have been mapped to that interface
- packets from the wired network that arrive on that interface

The Wireless Edge Services xl Module has already added the Ethernet header to traffic that has been mapped to a logical (VLAN or tunnel) interface. For this reason, the following rules only take effect on ACLs applied to a physical port:
- marking traffic with an 802.1p or DSCP value
- filtering traffic according to WLAN

If you have configured these options in a rule, that portion of the rule does not take effect. Other options in the rule take effect normally.

To associate an ACL with an interface, complete these steps.

1. Select Security > ACLs and click the Attach tab.
2. Click the **Add** button. The **Add ACL Association** screen is displayed.
3. From the **Interface** drop-down menu, select one of the following interfaces:
   - **uplink**—the module’s internal uplink port
   - **downlink**—the module’s internal downlink port
   - an uplink VLAN configured on the module

4. Select the ACL to control incoming traffic on the selected interface. The options available depend on the type of interface:
   - For VLAN interfaces, select an IP-type ACL from the **IP ACL** drop-down menu.
   - For an uplink or downlink port, you can select ACLs from either the **IP ACL** drop-down menu, the **MAC ACL** drop-down menu, or both.

   When you apply both types of ACLs, the Wireless Edge Services xl Module processes the MAC extended ACL first, so a rule in the MAC ACL always takes precedence over a rule in the IP ACL. However, if a frame is not selected by any of a MAC extended ACLs explicit rules, the module sends the frame to be processed by the IP ACL.

5. Click the **OK** button to apply the ACL.

6. Click the **Save** link to preserve your configuration.

### Using ACLs with DHCP Services

An ACL filters all traffic as soon as it arrives on the interface to which the ACL is applied. Remember that most wireless stations have no IP address until they receive one through DHCP. If you have applied an ACL to the VLAN (or tunnel) associated with a WLAN, the module might drop stations’ DHCP requests before they have the chance to receive a valid address.

To avoid problems, check all ACLs that filter traffic on a interface on which DHCP requests might arrive: these ACLs must include a rule that permits those requests. The best way to meet this requirement is to create an extended IP ACL for the VLAN (or tunnel) in question and add a rule that permits any UDP traffic destined to the DHCP server port (67).

### Viewing ACL Statistics

You should check ACLs and verify that they are selecting traffic as they should.

To view statistics for your ACLs, select **Security > ACLs** and click the **Statistics** tab. You can alternatively select **Security > ACL Statistics**.
Figure 7-12. Security > ACLs > Statistics Screen

ACL statistics are displayed on the screen. (If you do not see any statistics, you may need to edit your rules and check the Logging box.)

Each row provides information about one ACL rule:

- **Interface**—the interface to which the ACL rule is applied (uplink, downlink, VLAN, or tunnel interface)
- **Action**—whether the module forwards selected packets or drops them

Refer to Table 7-6 for a key to the action ID.

**Table 7-6. Action IDs for ACL Statistics**

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>drop—a deny rule</td>
</tr>
<tr>
<td>3</td>
<td>forward—a permit or mark rule</td>
</tr>
</tbody>
</table>

- **Protocol**—protocol for selected packets

Table 7-7 provides a key for the protocols.
Table 7-7. Protocol IDs for ACL Statistics

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>IP</td>
</tr>
<tr>
<td>1</td>
<td>ICMP</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
</tr>
</tbody>
</table>

- **Low Source IP** — the lowest source IP address specified for the rule
- **High Source IP** — the highest source IP address specified for the rule
- **Low Destination IP** — the lowest destination IP address specified for the rule (always 0.0.0.0 for standard ACLs)
- **High Destination IP** — the highest destination IP address specified for the rule (always 0.0.0.0 for standard ACLs)
- **Times Used** — the number of times that the Wireless Edge Services xl Module has applied the ACL rule to traffic

The counter increments when the module drops a denied packet or when permits the first packet in a session. The Wireless Edge Services xl Module support stateful ACLs, which means that it automatically allows all traffic in the session.

Check this column periodically to ensure that ACL rules are affecting traffic. If not, you might need to reconfigure ACLs to make them more relevant to your network. You can also check for a deny rule that filters out traffic that should be allowed.

To view detailed statistics for a specific interface, select the interface and click the **Details** button. The **Details** screen is displayed.
In addition to the information that you viewed on the Security > ACLs > Statistics screen, you can monitor the traffic associated with this rule. Total Flows reports the total number of sessions established using this rule and typically matches the value for Times Used. Active Flows shows how many of those sessions are still active. Look at Packets in and Packets out to monitor how much total traffic this rule has permitted.

The Rule Precedence value is based on the precedence value you choose for the rule; however, it is displayed differently. The Wireless Edge Services xl Module processes rules with a high rule presentness first.

Click the Refresh button to update the statistics, and click the Close button to close the window.

On the main Security > ACLs > Statistics screen, you can export statistical information about a specific rule. Select the rule and click the Export button. On the screen that is displayed, specify the destination filename and location.

The logged information is saved to a comma-separated values (CSV) file on your workstation, which lets you monitor activity and looks for signs of possible security issues or problems with traffic flow.
Access Control Lists (ACLs)
Configuring ACLs