



## Creating and Managing IP Access Control Lists

---

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces. Packet filtering helps to control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices.

You can also apply ACLs to management services such as SNMP, SSH, HTTPS, Telnet, FTP, and TFTP. ACLs can thus be used to control the traffic that these applications provide by restricting the type of traffic that the applications will handle. (Currently the Content Distribution Manager GUI allows you to associate ACLs to SNMP and TFTP applications only.)

This chapter describes the procedure for applying ACLs to devices using the Content Distribution Manager GUI. It contains the following sections:

- [Introducing IP ACLs, page 14-1](#)
- [Creating or Modifying an IP ACL, page 14-2](#)
- [Associating an IP ACL with an Application, page 14-12](#)
- [Applying an IP ACL to an Interface, page 14-13](#)
- [Deleting an IP ACL, page 14-13](#)

### Introducing IP ACLs

In a managed ACNS network environment, administrators need to be able to prevent unauthorized access to various devices and services. ACNS 5.1 software has implemented standard and extended ACLs that allow administrators to restrict access to or through an ACNS network device, such as a Content Engine, Content Router, or Content Distribution Manager. Administrators can thus use ACLs to reduce the infiltration of hackers, worms, and viruses that can harm the corporate network.

ACNS 5.1 software also provides controls that allow various services to be tied to a particular interface. For example, the administrator can use IP ACLs to define a public interface on the Content Engine for content serving and a private interface for management services (for example, Telnet, SSH, SNMP, HTTPS, and software upgrades). A device attempting to access one of the services must be on a list of trusted devices before it is allowed access. The implementation of ACLs for incoming traffic on certain ports for a particular protocol type is similar to the ACL support for the Cisco Global Site Selector and Cisco routers.

To use ACLs, the system administrator must first configure ACLs and then apply them to specific services or interfaces. The following are some examples of how IP ACLs can be used in various enterprise deployments:

- An application layer proxy firewall with a hardened outside interface has no ports exposed. (“Hardened” means that the interface carefully restricts which ports are available for access primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The Content Engine’s outside address is Internet global and inside address is private. The inside interface has an ACL to limit Telnet, SSH, GUI, and Content Distribution Manager traffic.
- A Content Engine is deployed anywhere within the enterprise. Like routers and switches, the administrator wants to limit Telnet, SSH, Content Distribution Manager, and GUI access to the IT source subnets.
- A Content Engine is deployed as a reverse proxy in an untrusted environment, and the administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the backend interface.
- A Content Engine using WCCP is positioned between a firewall and an Internet router or a subnet off the Internet router. Both the Content Engine and the router must have IP ACLs.

**Note**

In the ACNS 5.1 software release, the system administrator must explicitly configure the **ip access-list command** in order to allow or deny access to the user through the TFTP protocol. Unless the ACL is configured for the TFTP service, the security of the content can be at risk and TFTP will not work properly.

In ACNS 5.0 software, TFTP access is denied to the user by default. To allow access to the user, the system administrator must use the **trusted-host** command. The **trusted-host** command, however, is not supported in the ACNS 5.1 software release. If this command is used on Content Engines using ACNS releases earlier than 5.1, and the devices are subsequently upgraded to ACNS 5.1 or later, the command shows up in the CLI, but has no effect on the TFTP protocol. The trusted host configurations can be deleted by using the **no trusted-host** command.

## Creating or Modifying an IP ACL

**Note**

IP ACLs are defined for individual devices only. IP ACLs cannot be managed globally across the ACNS network or through device groups. IP ACLs cannot be defined on IP/TV Program Manager devices.

When you create an IP ACL, you should note the following constraints:

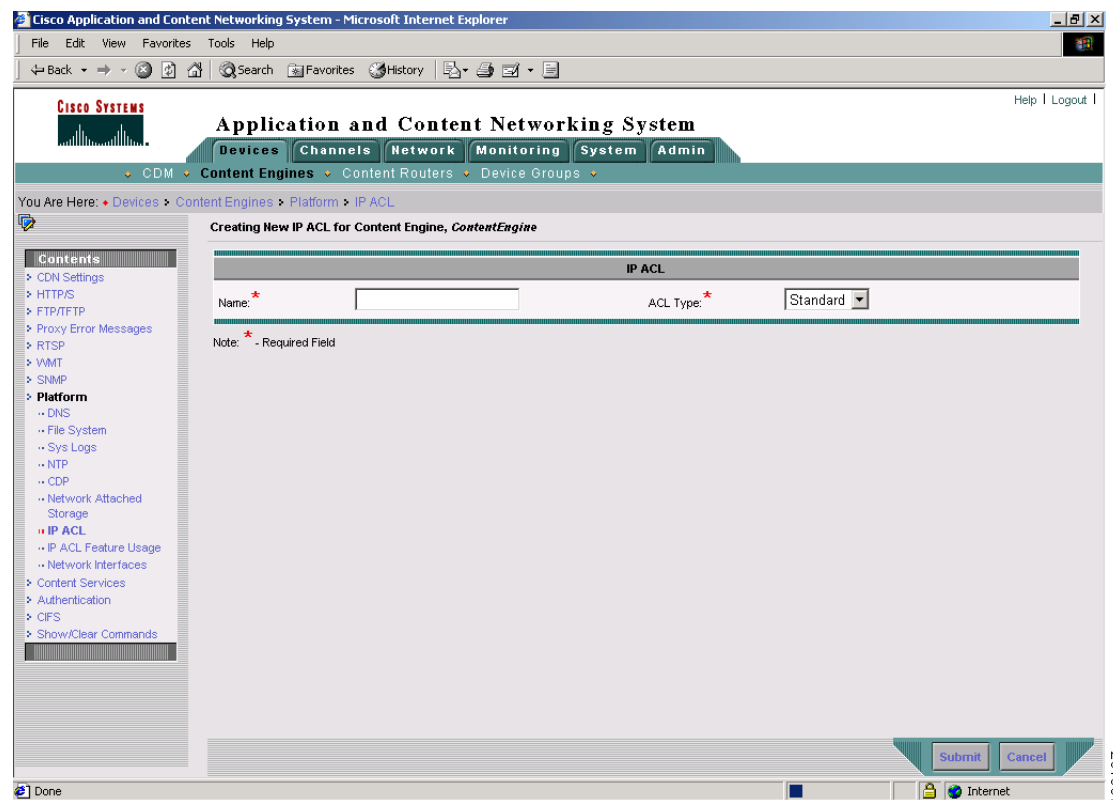
- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no white space or special characters.
- The Content Distribution Manager can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.
- Extended IP ACLs cannot be used with SNMP or TFTP applications in the ACNS 5.1 software release.

## Creating a New IP ACL

To create a new IP ACL using the Content Distribution Manager GUI, follow these steps:

- Step 1** In the Content Distribution Manager GUI, choose **Devices** and then choose **CDM, Content Engines**, or **Content Routers**.
- Step 2** Click the **Edit** icon next to the name of the device for which you want to create an IP ACL.
- Step 3** In the Contents pane, choose **Platform** > **IP ACL**. The IP ACL window appears.
- Step 4** Click the **Create a new IP ACL** icon in the taskbar. The Creating New IP ACL window appears. (See Figure 14-1.)

**Figure 14-1** Creating New IP ACL Window



- Step 5** Enter a name in the Name field, observing the naming rules for IP ACLs.
- Step 6** Choose an IP ACL type from the drop-down list. The choices are Standard or Extended. The default is Standard.
- Step 7** Click **Submit** to save the list.



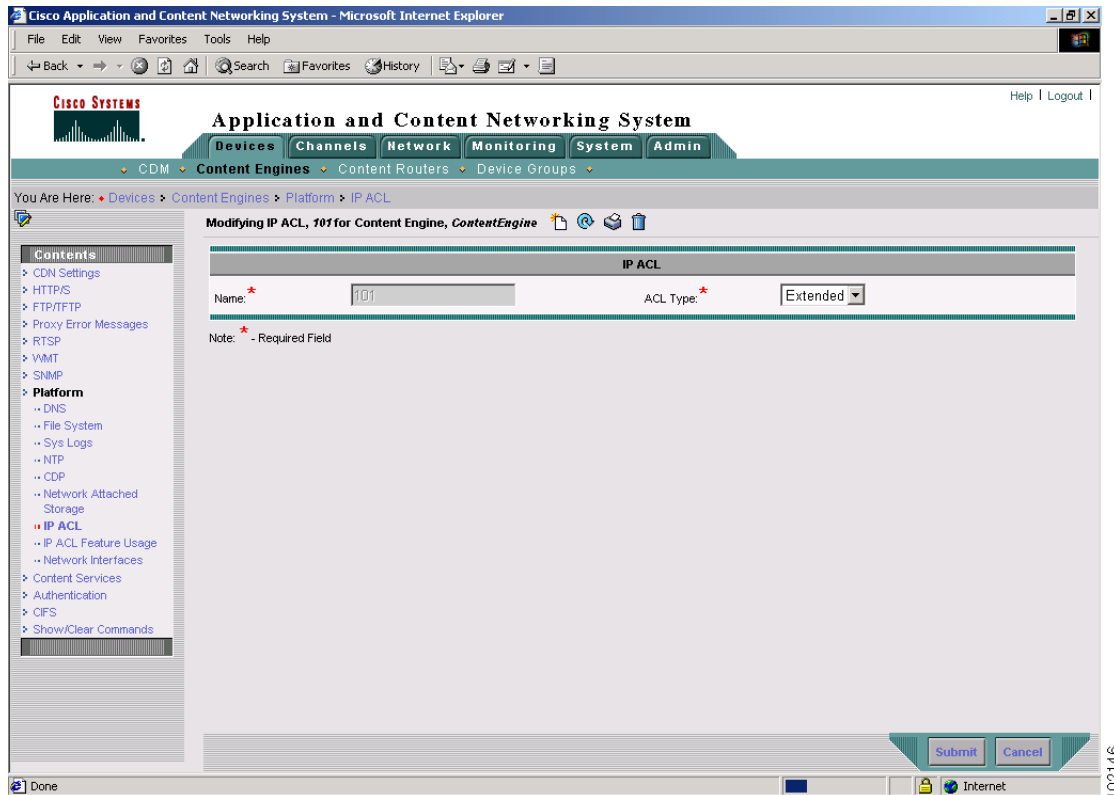
**Note** Clicking **Submit** at this point merely saves the list; IP ACLs without any conditions defined do not appear on the individual devices.

## Adding Conditions to an IP ACL

To add conditions to the IP ACL, follow these steps:

- Step 1** In the Contents pane, click **IP ACL** to return to the list of IP ACLs.
- Step 2** To add conditions to an IP ACL, click the **Edit** icon next to the name of the IP ACL that you created. The Modifying IP ACL window appears. (See [Figure 14-2](#).)

**Figure 14-2** Modifying IP ACL Window



- Step 3** Click the **Create New Condition** icon in the taskbar. The Creating New Condition window appears. (See [Figure 14-3](#).)



**Note** The number of enabled fields for creating IP ACL conditions depends on the type of IP ACL that you have created, either Standard or Extended. You can only fill in the fields that are enabled.

Figure 14-3 Creating New Condition of Extended IP ACL for Content Engine Window

**Step 4** Enter values for the condition properties that are enabled for the type of IP ACL that you are creating.

**Step 5** To set up conditions for a standard IP ACL, follow these steps:

- a. Choose a purpose from the drop-down list. The choices are Permit or Deny.
- b. Enter the source IP address in the Source IP field.
- c. Enter a source IP wildcard address in the Source IP Wildcard field.
- d. Click **Submit** to save the condition. The window refreshes, displaying the condition that you created.

Table 14-1 describes the fields in a standard IP ACL.

**Table 14-1 Standard IP ACL Conditions**

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Source IP*	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard*	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.

1. \* = required field.

- Step 6** To set up conditions for an extended IP ACL, follow these steps:
- Choose a purpose from the drop-down list. The choices are Permit or Deny.
  - Choose an extended type of IP ACL from the drop-down list. (See [Table 14-2](#).)
  - After you choose an extended type of IP ACL, various options become enabled in the GUI, depending on what type you choose.
  - Enter data in the fields that are enabled for the chosen type. (See [Table 14-3](#) through [Table 14-6](#).)

**Table 14-2 Extended IP ACL Conditions**

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type*	Generic	Specifies the Internet protocol to be applied to the condition. When selected, the GUI window refreshes with applicable field options enabled. Choices are: <ul style="list-style-type: none"> <li>Generic (See <a href="#">Table 14-3</a>.)</li> <li>TCP (See <a href="#">Table 14-4</a>.)</li> <li>UDP (See <a href="#">Table 14-5</a>.)</li> <li>ICMP (See <a href="#">Table 14-6</a>.)</li> </ul>

1. \* = required field.

**Table 14-3 Extended IP ACL Generic Condition**

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type*	Generic	Matches any Internet protocol.
Protocol	<b>ip</b>	Name of an Internet protocol. Key words are <b>gre</b> , <b>icmp</b> , <b>ip</b> , <b>tcp</b> , or <b>udp</b> . To match any Internet protocol, use the keyword <b>ip</b> .
Source IP*	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard*	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.

1. \* = required field.

**Table 14-4 Extended IP ACL TCP Condition**

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type*	TCP	Matches the TCP Internet protocol.
Established	Unchecked (False)	Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. A nonmatching case is that of the initial TCP datagram used to form a connection.
Source IP*	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard*	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.
Source Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0 to 65535. Valid TCP port names are: <ul style="list-style-type: none"> <li>- ftp</li> <li>- ftp-data</li> <li>- https</li> <li>- mms</li> <li>- netbios-dgm</li> <li>- netbios-ns</li> <li>- netbios-ss</li> <li>- nfs</li> <li>- rtsp</li> <li>- ssh</li> <li>- telnet</li> <li>- www</li> </ul>
Source Operator	range	Specifies how to compare the source ports. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a TCP port. See Source Port 1.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.

**Table 14-4 Extended IP ACL TCP Condition (continued)**

Field	Default Value	Description
Destination Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0 to 65535. Valid TCP port names are: <ul style="list-style-type: none"> <li>- ftp</li> <li>- ftp-data</li> <li>- https</li> <li>- mms</li> <li>- netbios-dgm</li> <li>- netbios-ns</li> <li>- netbios-ss</li> <li>- nfs</li> <li>- rtsp</li> <li>- ssh</li> <li>- telnet</li> <li>- www</li> </ul>
Destination Operator	range	Specifies how to compare the destination ports. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a TCP port. See Destination Port 1.

1. \* = required field.

**Table 14-5 Extended IP ACL UDP Condition**

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type*	UDP	Matches the UDP Internet protocol.
Established	—	Not available for UDP.
Source IP*	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard*	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.

*Table 14-5 Extended IP ACL UDP Condition (continued)*

Field	Default Value	Description
Source Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0 to 65535. Valid UDP port names are: <ul style="list-style-type: none"> <li>- bootpc</li> <li>- bootps</li> <li>- domain</li> <li>- mms</li> <li>- netbios-dgm</li> <li>- netbios-ns</li> <li>- netbios-ss</li> <li>- nfs</li> <li>- ntp</li> <li>- snmp</li> <li>- snmptrap</li> <li>- tacacs</li> <li>- tftp</li> <li>- wccp</li> </ul>
Source Operator	range	Specifies how to compare the source ports. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a UDP port. See Source Port 1.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.

Table 14-5 Extended IP ACL UDP Condition (continued)

Field	Default Value	Description
Destination Port 1	0	The decimal number or name of a UDP port. Valid port numbers are 0 to 65535. Valid UDP port names are: <ul style="list-style-type: none"> <li>- bootpc</li> <li>- bootps</li> <li>- domain</li> <li>- mms</li> <li>- netbios-dgm</li> <li>- netbios-ns</li> <li>- netbios-ss</li> <li>- nfs</li> <li>- ntp</li> <li>- snmp</li> <li>- snmptrap</li> <li>- tacacs</li> <li>- tftp</li> <li>- wccp</li> </ul>
Destination Operator	range	Specifies how to compare the destination ports. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a UDP port. See Destination Port 1.

1. \* = required field.

Table 14-6 Extended IP ACL ICMP Condition

Field	Default Value	Description
Purpose* <sup>1</sup>	Permit	Specifies whether a packet is to be passed or dropped. Choices are Permit or Deny.
Extended Type*	ICMP	Matches the ICMP Internet protocol.
Source IP*	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard*	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.

Table 14-6 Extended IP ACL ICMP Condition (continued)

Field	Default Value	Description
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify interesting bits with a 0.
ICMP Param Type*	None	<p>Choices are <b>None</b>, <b>Type/Code</b>, or <b>Msg</b>.</p> <p><b>None</b>—Disables the ICMP Type, Code, and Message fields.</p> <p><b>Type/Code</b>—Allows ICMP messages to be filtered by the ICMP message type and code. Also enables the option to set an ICMP message code number.</p> <p><b>Msg</b>—Allows a combination of type and code to be specified using a keyword. Enables the ICMP message drop-down list. Disables the ICMP Type field.</p> <p><b>Note</b> Refer to the <i>Cisco ACNS Software Command Reference, Release 5.1</i> for further explanation of related keywords. (See the <b>ip access-list extended</b> command.)</p>
ICMP Type*	0	Number from 0 to 255. This field is enabled when you choose <b>ICMP Param Type: Type/Code</b> .
Use ICMP Code*	Unchecked	When checked, enables the ICMP Code field.
ICMP Code*	0	Number from 0 to 255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.
ICMP Message*	administratively-prohibited	<p>Allows a combination of ICMP type and code to be easily specified using a keyword. Choose from the drop-down list.</p> <p><b>Note</b> Refer to the <i>Cisco ACNS Software Command Reference, Release 5.1</i> for further explanation of these keywords. (See the <b>ip access-list extended</b> command.)</p>

1. \* = required field.

**Step 7** To add another condition to the IP ACL, repeat [Step 1](#) through [Step 6](#).

**Step 8** To reorder your list of conditions, use the Up or Down Arrows in the Move column.



**Note** The order of the conditions listed in the Content Distribution Manager GUI becomes the IP ACL order applied to the device. The GUI allows sorting by order only.

**Step 9** When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** to commit the IP ACL to the device database.

A green “Change submitted” indicator appears in the lower right corner of the Modifying IP ACL window to indicate that the IP ACL is being submitted to the device database.

---

## Modifying, Deleting, or Reordering a Condition

To modify or delete an individual condition from an IP ACL, follow these steps:

---

- Step 1** In the Content Distribution Manager GUI, choose **Devices > Content Engines**.
  - Step 2** Click the **Edit** icon next to the name of the Content Engine whose IP ACL you want to modify.
  - Step 3** In the Contents pane, choose **Platform > IP ACL**.
  - Step 4** Click the **Edit** icon next to the name of the IP ACL that you want to modify. The Modifying IP ACL window appears listing all the conditions applied to the IP ACL.
  - Step 5** Click the **Edit** icon next the condition that you want to modify or delete. The Modifying Condition window appears.
  - Step 6** To modify the condition, change any allowable field as necessary.
  - Step 7** To delete the condition, click the **Delete IP ACL Condition (Trash)** icon in the taskbar.
  - Step 8** To reorder your list of conditions, use the up or down arrows in the Move column and click **Submit**.
- 

## Associating an IP ACL with an Application

The Content Distribution Manager GUI allows the association of standard IP ACLs with SNMP and TFTP. To associate a standard IP ACL with one of these applications, follow these steps:

---

- Step 1** In the Content Distribution Manager GUI, choose **Devices > CDM, Content Engines, or Content Routers**.
- Step 2** Click the **Edit** icon next to the name of the device for which you have created an IP ACL.
- Step 3** In the Contents pane, choose **Platform > IP ACL Feature Usage**. The IP ACL Feature Settings window appears.
- Step 4** Choose the name of an IP ACL for SNMP and for TFTP from the drop-down list. If you do not want to associate an IP ACL with one of the features, choose **None**.



**Note** The drop-down list contains the names of all your standard IP ACLs. Only standard IP ACLs can be associated with features.

---

- Step 5** Click **Submit**.
-

## Applying an IP ACL to an Interface

ACNS 5.1 software provides controls that allow various services to be tied to a particular interface. To apply an IP ACL to an interface, follow these steps:

- 
- Step 1** In the Content Distribution Manager GUI, choose **Devices > CDM, Content Engine, or Content Routers**.
  - Step 2** Click the **Edit** icon next to the name of the device for which you want to apply an IP ACL to an interface.
  - Step 3** In the Contents pane, choose **Platform > Network Interfaces**.

The Network Interfaces window for the device appears. This window displays all the interfaces available on that device.



---

**Note** The PortChan column refers to the port channel or EtherChannel configuration. EtherChannel for ACNS 5.x software supports the grouping of up to four same-speed network interfaces into one virtual interface. (See the [“Configuring EtherChannel”](#) section on page 3-20.) A negative value in this column indicates that no port channels have been configured for the interface.

---

- Step 4** Choose the name of an IP ACL from the **Inbound ACL** drop-down list.
- Step 5** Choose the name of an ACL from the **Outbound ACL** drop-down list.



---

**Note** The only network interface properties that can be altered from the Content Distribution Manager GUI are the inbound and outbound IP ACLs. All other property values are populated from the device database and are read-only in the Content Distribution Manager GUI.

---

- Step 6** Click **Submit**.
- 

## Deleting an IP ACL

You can delete an IP ACL, including all conditions and associations with network interfaces and applications, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing; however, it is in effect nonexistent.

To delete an IP ACL, follow these steps:

- 
- Step 1** In the Content Distribution Manager GUI, choose **Devices > Content Engines**.
  - Step 2** Click the **Edit** icon next to the name of the Content Engine with the IP ACL configured that you want to delete.
  - Step 3** In the Contents pane, choose **Platform > IP ACL**. The IP ACL for Content Engine window appears.

- Step 4** Click the **Edit** icon next to the name of the IP ACL that you want to delete. The Modifying IP ACL window appears. If you created conditions for the IP ACL, you have two options for deletion:
- **Delete ACL**  
This option removes the IP ACL, including all conditions and associations with network interfaces and applications.
  - **Delete All Conditions**  
This option removes all the conditions, while preserving the IP ACL name.
- Step 5** To delete the entire IP ACL, click the large **Delete ACL** Trash icon in the taskbar. You are prompted to confirm your action. Click **OK**. The record is deleted.
- Step 6** To delete only the conditions, click the small **Delete All Conditions** Trash/List icon in the taskbar. You are prompted to confirm your action. Click **OK**. The window refreshes, conditions are deleted, and the ACL Type field is enabled.
-