



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 standard ACLs with SNMP, TFTP, and WCCP 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 15-1](#)
- [Creating or Modifying an IP ACL, page 15-2](#)
- [Associating an IP ACL with an Application, page 15-12](#)
- [Applying an IP ACL to an Interface, page 15-13](#)
- [Deleting an IP ACL, page 15-14](#)

Introducing IP ACLs

In a managed ACNS network environment, administrators need to be able to prevent unauthorized access to various devices and services. ACNS software supports 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 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 globally accessible from the Internet, while its 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**

To allow or deny access to the user through the TFTP protocol, you must explicitly configure the **ip access-list** command. Unless the ACL is explicitly configured for the TFTP service, the security of the content can be at risk, and TFTP will not work properly.

The **ip access-list** command replaces the **trusted-host** command. If the **trusted-host** 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. You can delete trusted host configurations 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:

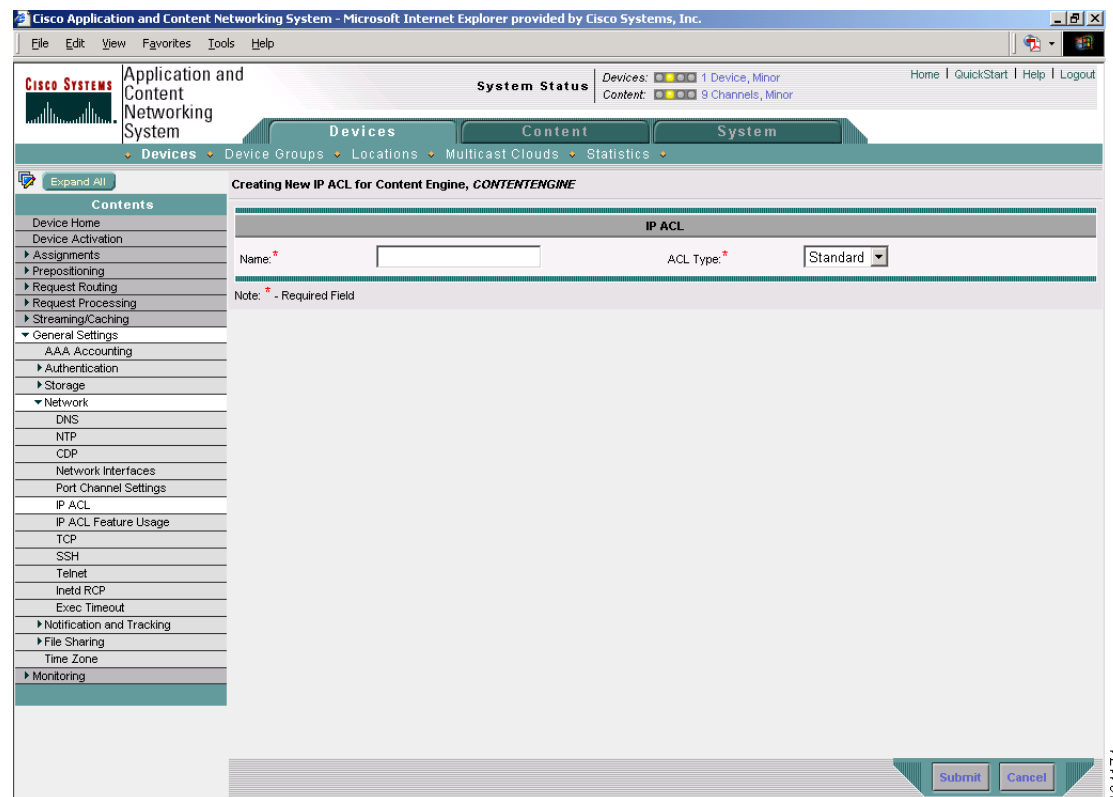
- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no white space or special characters.
- The Content Distribution Manager can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 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, TFTP, or WCCP applications.

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 > Devices**.
- 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 **General Settings > Network > 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 15-1.)

Figure 15-1 Creating a 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 (**Standard** or **Extended**) from the drop-down list. The default is Standard.
- Step 7** Click **Submit** to save the IP ACL. The window refreshes and the Modifying IP ACL window for the newly created IP ACL appears.



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

Adding Conditions to an IP ACL

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

- Step 1** In the Content Distribution Manager GUI, choose **Devices > Devices**.
- 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 **General Settings > Network > IP ACL**. The IP ACL window appears.
- Step 4** Click the **Edit** icon next to the name of the IP ACL for which you want to add conditions. The Modifying IP ACL window appears.
- Step 5** Click the **Create New Condition** icon in the taskbar. The Creating New Condition window appears. (See [Figure 15-2](#).)



Note The number of available fields for creating IP ACL conditions depends on the type of IP ACL that you have created, either standard or extended.

Figure 15-2 Creating a New Condition for an Extended IP ACL Window

The screenshot shows the 'Creating New Condition' window in the Cisco Application and Content Networking System GUI. The window is titled 'Creating New Condition, of Extended IP ACL for Content Engine, CONTENTENGINE'. It contains several fields for configuring the condition:

- Purpose:** Permit
- Extended Type:** Generic
- Protocol:** ip
- Established:**
- Source IP:** 0.0.0.0
- Source IP Wildcard:** 255.255.255.255
- Source Port 1:** 0
- Source Operator:** range
- Source Port 2:** 25535
- Destination IP:** 0.0.0.0
- Destination IP Wildcard:** 255.255.255.255
- Destination Port 1:** 0
- Destination Operator:** range
- Destination Port 2:** 25535
- ICMP Param Type:** None
- ICMP Message:** administratively-prohibited
- ICMP Type:** 0
- Use ICMP Code:**
- ICMP Code:** 0

A note at the bottom indicates that fields with an asterisk are required. The window has 'Submit' and 'Cancel' buttons at the bottom right.

- Step 6** Enter values for the properties that are enabled for the type of IP ACL that you are creating.
 - Go to [Step 7](#) to create a standard IP ACL.
 - Go to [Step 8](#) to create an extended IP ACL.

- Step 7** To set up conditions for a standard IP ACL, follow these steps:
- Choose a purpose (**Permit** or **Deny**) from the drop-down list.
 - Enter the source IP address in the Source IP field.
 - Enter a source IP wildcard address in the Source IP Wildcard field.
 - Click **Submit** to save the condition. The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.
 - To add another condition to the IP ACL, repeat the steps.
 - To reorder your list of conditions from the Modifying IP ACL window, use the Up or Down Arrows in the Move column, or click a column heading to sort by any configured parameter.



Note The order of the conditions listed in the Content Distribution Manager GUI becomes the order in which IP ACLs are applied to the device.

- 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** in the Modifying IP ACL window 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.

Table 15-1 describes the fields in a standard IP ACL.

Table 15-1 Standard IP ACL Conditions

Field	Default Value	Description
Purpose* ¹	Permit	Specifies whether a packet is to be passed (Permit) or dropped (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 bits of interest with a 0.

1. * = required field.

- Step 8** To set up conditions for an extended IP ACL, follow these steps:
- Choose a purpose (**Permit** or **Deny**) from the drop-down list.
 - Choose **Generic**, **TCP**, **UDP**, or **ICMP** from the Extended Type drop-down list. (See Table 15-2.)
After you choose a type of extended IP ACL, various options become available in the GUI, depending on what type you choose.
 - Enter data in the fields that are enabled for the chosen type. (See Table 15-3 through Table 15-6.)
 - Click **Submit** to save the condition. The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.
 - To add another condition to the IP ACL, repeat the steps.
 - To reorder your list of conditions from the Modifying IP ACL window, use the Up or Down Arrows in the Move column, or click a column heading to sort by any configured parameter.



Note The order of the conditions listed in the Content Distribution Manager GUI becomes the order in which IP ACLs are applied to the device.

- g. 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** in the Modifying IP ACL window 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.

Table 15-2 Extended IP ACL Conditions

Field	Default Value	Description
Purpose* ¹	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"> • Generic (see Table 15-3) • TCP (see Table 15-4) • UDP (see Table 15-5) • ICMP (see Table 15-6)

1. * = required field.

Table 15-3 Extended IP ACL Generic Condition

Field	Default Value	Description
Purpose* ¹	Permit	Specifies whether a packet is to be passed (Permit) or dropped (Deny).
Extended Type*	Generic	Matches any Internet protocol.
Protocol	ip	Internet protocol (gre , icmp , ip , tcp , or udp). To match any Internet protocol, use the keyword ip .
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 bits of interest with a 0.

Table 15-3 Extended IP ACL Generic Condition

Field	Default Value	Description
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 bits of interest with a 0.

1. * = required field.

Table 15-4 Extended IP ACL TCP Condition

Field	Default Value	Description
Purpose* ¹	Permit	Specifies whether a packet is to be passed (Permit) or dropped (Deny).
Extended Type*	TCP	Matches the TCP Internet protocol.
Established	Unchecked (false)	When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.
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 bits of interest 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"> • - ftp • - ftp-data • - https • - mms • - netbios-dgm • - netbios-ns • - netbios-ss • - nfs • - rtsp • - ssh • - telnet • - www

Table 15-4 Extended IP ACL TCP Condition (continued)

Field	Default Value	Description
Source Operator	range	Specifies how to compare the source ports against incoming packets. 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 bits of interest with a 0.
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"> • - ftp • - ftp-data • - https • - mms • - netbios-dgm • - netbios-ns • - netbios-ss • - nfs • - rtsp • - ssh • - telnet • - www
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a TCP port. See Destination Port 1.

1. * = required field.

Table 15-5 Extended IP ACL UDP Condition

Field	Default Value	Description
Purpose* ¹	Permit	Specifies whether a packet is to be passed (Permit) or dropped (Deny).
Extended Type*	UDP	Matches the UDP Internet protocol.
Established	—	Not available for UDP.

Table 15-5 Extended IP ACL UDP Condition (continued)

Field	Default Value	Description
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 bits of interest with a 0.
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"> • - bootpc • - bootps • - domain • - mms • - netbios-dgm • - netbios-ns • - netbios-ss • - nfs • - ntp • - snmp • - snmptrap • - tacacs • - tftp • - wccp
Source Operator	range	Specifies how to compare the source ports against incoming packets. 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 bits of interest with a 0.

Table 15-5 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"> • - bootpc • - bootps • - domain • - mms • - netbios-dgm • - netbios-ns • - netbios-ss • - nfs • - ntp • - snmp • - snmptrap • - tacacs • - tftp • - wccp
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a UDP port. See Destination Port 1.

1. * = required field.

Table 15-6 Extended IP ACL ICMP Condition

Field	Default Value	Description
Purpose* ¹	Permit	Specifies whether a packet is to be passed (Permit) or dropped (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 bits of interest 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 15-6 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 bits of interest with a 0.
ICMP Param Type*	None	<p>Choices are None, Type/Code, or Msg.</p> <p>None—Disables the ICMP Type, Code, and Message fields.</p> <p>Type/Code—Allows ICMP messages to be filtered by ICMP message type and code. Also enables the ability to set an ICMP message code number.</p> <p>Msg—Allows a combination of type and code to be specified using a keyword. Activates the ICMP message drop-down list. Disables the ICMP Type field.</p> <p>Note Refer to the <i>Cisco ACNS Software Command Reference, Release 5.2</i> for further explanation of related keywords. (See the ip access-list extended command.)</p>
ICMP Message*	administratively-prohibited	<p>Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.</p> <p>Note Refer to the <i>Cisco ACNS Software Command Reference, Release 5.2</i> for further explanation of these keywords. (See the ip access-list extended command.)</p>
ICMP Type*	0	Number from 0 to 255. This field is enabled when you choose Type/Code .
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.

1. * = required field.

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 > Devices**.
- Step 2** Click the **Edit** icon next to the name of the device whose IP ACL you want to modify.
- Step 3** In the Contents pane, choose **General Settings > Network > 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 Condition** 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 **Trash (Delete IP ACL Condition)** 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, TFTP, and WCCP. Any device that attempts to access one of these applications associated with an access control list (ACL) must be on the list of trusted devices to be allowed access. You can associate any previously configured standard IP ACL with SNMP, TFTP, and WCCP; however, you cannot associate an extended IP ACL with these applications.

To associate a standard IP ACL with one of these applications, follow these steps:

- Step 1** In the Content Distribution Manager GUI, choose **Devices > Devices**.
- 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 **General Settings > Network > IP ACL Feature Usage**. The IP ACL Feature Settings window appears. [Table 15-7](#) describes the fields in this window and provides the corresponding CLI global configuration commands.
- Step 4** Choose the name of an IP ACL for SNMP, TFTP, and WCCP from the drop-down lists. If you do not want to associate an IP ACL with one of the applications, choose **Do Not Set**.



Note The drop-down lists for SNMP and TFTP contain the names of all your standard IP ACLs. Only standard IP ACLs (not extended IP ACLs) can be associated with SNMP and TFTP applications.

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

Table 15-7 IP ACL Feature Settings

GUI Parameter	Function	CLI Command
SNMP	Associates an IP ACL with SNMP.	snmp-server access-list { <i>std_acl_number</i> <i>acl_name</i> }
TFTP	Associates an IP ACL with TFTP.	tftp-server access-list { <i>std_acl_number</i> <i>acl_name</i> }
WCCP	Associates an IP ACL with WCCP.	wccp access-list { <i>std_acl_number</i> <i>ext_acl_number</i> <i>acl_name</i> }

Applying an IP ACL to an Interface

ACNS software allows SNMP, TFTP, and WCCP applications to be applied to a particular interface (such as management services to a private IP address) so that the Content Engine can have one interface in a public IP address space that serves content, and another interface in a private IP address space that the administrator uses for management purposes. This ensures that clients can access the Content Engine only in the public IP address space for serving content and not access it for management purposes. A device attempting to access one of these applications that is associated with an IP ACL must be on the list of trusted devices to be allowed access.

To apply an IP ACL to an interface, follow these steps:

-
- Step 1** In the Content Distribution Manager GUI, choose **Devices > Devices**.
 - 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 **General Settings > Network > Network Interfaces**.

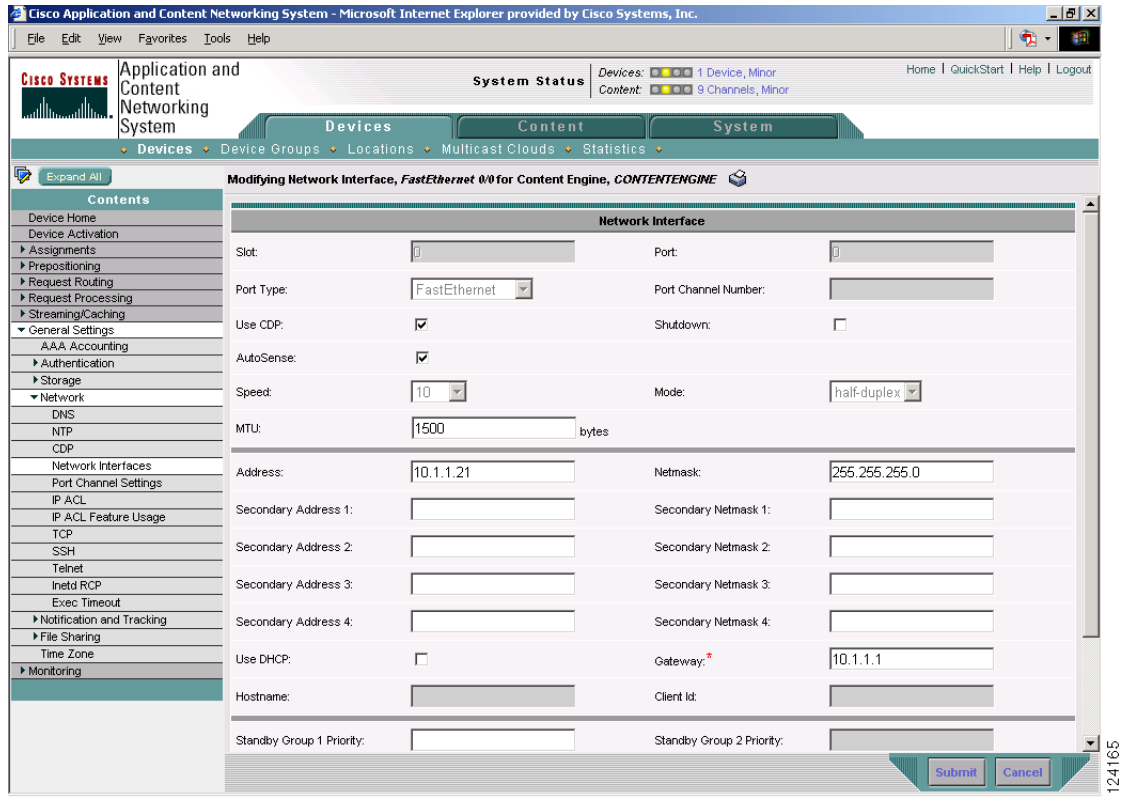
The Network Interfaces window for the device appears. This window displays all the interfaces available on that device.



Note The Port Type column may contain a PortChannel interface indicating an 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 11-11.](#))

- Step 4** Click the **Edit** icon next to the name of the interface to which you want to apply an IP ACL. The Modifying Network Interface window appears. (See figure.)

Figure 15-3 Modifying Network Interface—Applying an IP ACL



Step 5 Scroll to the bottom of the window and choose the name of an IP ACL from the Inbound ACL drop-down list.

Step 6 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 7 Click **Submit**.

To apply an IP ACL to an interface from the CLI, use the following interface configuration command:

```
interface {FastEthernet | GigabitEthernet} slot/port ip access-group {accesslistnumber | accesslistname} {in | out}
```

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 > Devices**.
- Step 2** Click the **Edit** icon next to the name of the device with the IP ACL configured that you want to delete.
- Step 3** In the Contents pane, choose **General Settings > Network > 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 **Trash (Delete ACL)** 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 becomes available.
-

