CHAPTER 8

Creating and Managing IP Access Control Lists for WAAS Devices

This chapter describes how to use the Wide Area Application Services (WAAS) Central Manager GUI to centrally create and manage Internet Protocol (IP) access control lists (ACLs) for your WAAS devices.

This chapter contains the following sections:

- About IP ACLs for WAAS Devices, page 8-1
- Creating and Managing IP ACLs for WAAS Devices, page 8-3
- List of Extended IP ACL Conditions, page 8-8

Note Throughout this chapter, the term WAAS device is used to refer collectively to WAAS Central Managers and Wide Area Application Engine (WAEs) in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

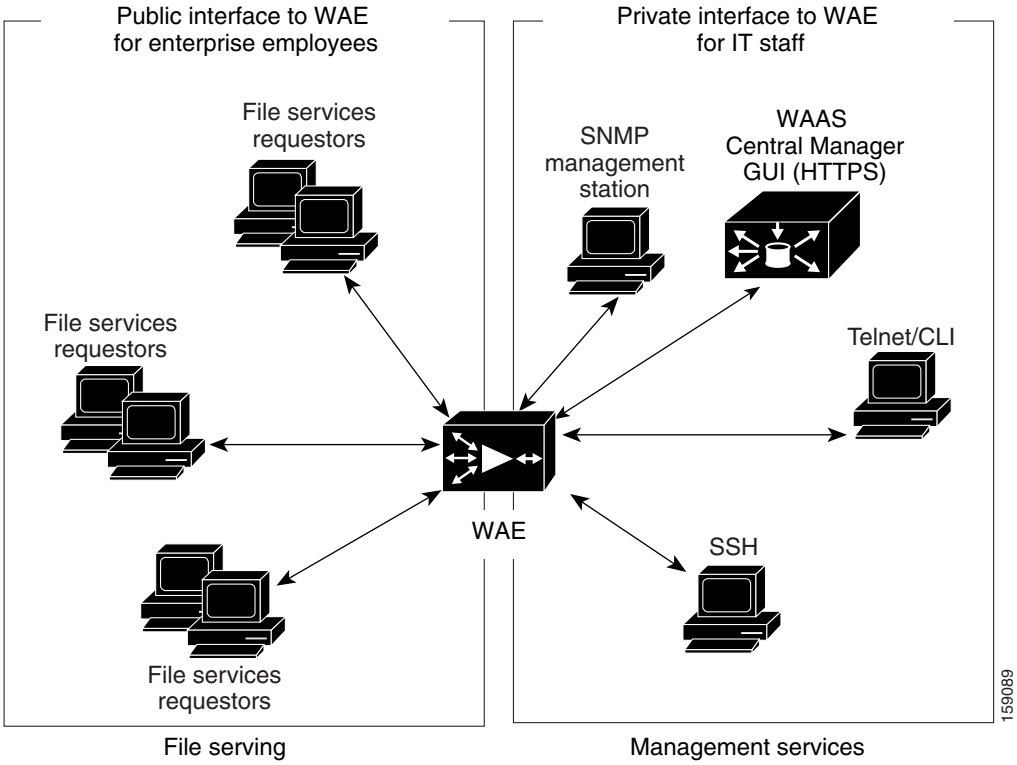
Note ACLs do not apply to the inline interfaces on a Cisco WAE Inline Network Adapter installed in a WAE.

About IP ACLs for WAAS Devices

In a centrally managed WAAS network environment, administrators need to be able to prevent unauthorized access to various devices and services. IP ACLs can filter packets by allowing you to permit or deny IP packets from crossing specified interfaces on a WAAS device. Packet filtering helps to control packet movement through the network. This control can help limit network traffic and restrict network use by specific users or devices.

The WAAS software also provides controls that allow various services to be tied to a particular interface. For example, you can use IP ACLs to define a public interface on the WAE for file serving and a private interface for management services, such as Telnet, Secure Shell (SSH), SNMP, HTTP, and software upgrades. (See Figure 8-1.)

Figure 8-1 Example of How IP ACLs Are Used to Control Access to Specific Interfaces on a WAE



The WAAS software supports standard and extended ACLs that allow you to restrict access to or through a WAAS device. You can use IP ACLs to reduce the infiltration of hackers, worms, and viruses that can harm the corporate network.

The following examples illustrate how IP ACLs can be used in environments that have WAAS devices:

- A WAAS device resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- A WAAS device is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit access to Telnet, SSH, and the WAAS Central Manager GUI to the IT source subnets.

To use ACLs, you must first configure ACLs and then apply them to specific services or interfaces on the WAAS device. 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 WAAS device’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, and GUI access.
- A WAE that is using WCCP is positioned on a subnet off the Internet router. Both the WAE and the router must have IP ACLs. IP access lists on routers have the highest priority followed by IP ACLs that are defined on the WAEs.

Precedence of IP ACLs and Application Definition Policies on WAEs

When the WAE is operating in pass-through mode, all traffic is still subject to IP ACLs that are configured on a WAE because these IP packets are processed by the WAE. The IP ACLs that are configured on the WAE should be used to define the policies that you want to be applied to a WAE's incoming traffic and that are addressed at the IP level.

IP ACLs that are configured on a WAE always take precedence over any WAAS application definition policies that are defined on a WAE. For example, you might define an extended IP ACL that has the following conditions on the Edge WAE in the branch office:

- ip access-list extended DENY_10.56.65.21
- deny ip any host 10.56.65.21
- permit ip any

This extended IP ACL will be applied to the interface on the Edge WAE as follows:

- Interface GigabitEthernet 1/0
- IP address 10.56.64.166 255.255.255.240
- IP access-group DENY_10.56.65.21 out

This interface is the only interface that is up and running on the Edge WAE. In this case, it does not matter what application definition policies have been configured on this Edge WAE because the Edge WAE will drop all the TCP traffic from 10.56.65.21 at IP layer only and will not send the traffic any further (for example, the Edge WAE will drop the traffic and not send the traffic to the Core WAE in the data center).

Note We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI to centrally configure and apply IP ACLs to your WAAS devices. For more information, see the "Creating and Managing IP ACLs for WAAS Devices" section on page 8-3.

Creating and Managing IP ACLs for WAAS Devices

This section provides guidelines and an example of how to use the WAAS Central Manager GUI to create and manage IP ACLs for your WAAS devices.

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

- 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.
- Each WAAS Central Manager device 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.
- The WAAS Central Manager GUI allows the association of standard IP ACLs with SNMP and WCCP. Any device that attempts to access one of these applications associated with an ACL must be on the list of trusted devices to be allowed access.
- You can associate any previously configured standard IP ACL with SNMP and WCCP; however, you can associate an extended IP ACL only with the WCCP application.

- 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 use the WAAS Central Manager GUI to create and modify an IP ACL for a single WAE, associate an IP ACL with an application, and then apply it to an interface on the WAE, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the name of the device (for example, a Core WAE named bd-s14) for which you want to create an IP ACL.

Step 3 Click **Expand All** above the Contents pane.

Step 4 In the Contents pane, choose **General Settings > Network > IP ACL**.

The IP ACL window appears. By default, there are no IP ACLs defined for a WAE. The IP ACL window indicates if there are currently no IP ACLs configured for the WAE.

Step 5 In the taskbar, click the **Create a new IP ACL** icon.

The Creating New IP ACL window appears. Fill in the fields as follows:

- In the Name field, enter a name (for example, test1), observing the naming rules for IP ACLs.

  By default, this new IP ACL is created as a standard ACL.

  Note IP ACL names must be unique within the device, must be limited to 30 characters, and cannot contain any white spaces or special characters.

- If you want to change this default setting and create this new ACL as an extended ACL, choose **Extended** from the ACL Type drop-down list.

Step 6 Click **Submit** to save the IP ACL named test1. IP ACLs without any conditions defined do not appear on the individual devices.

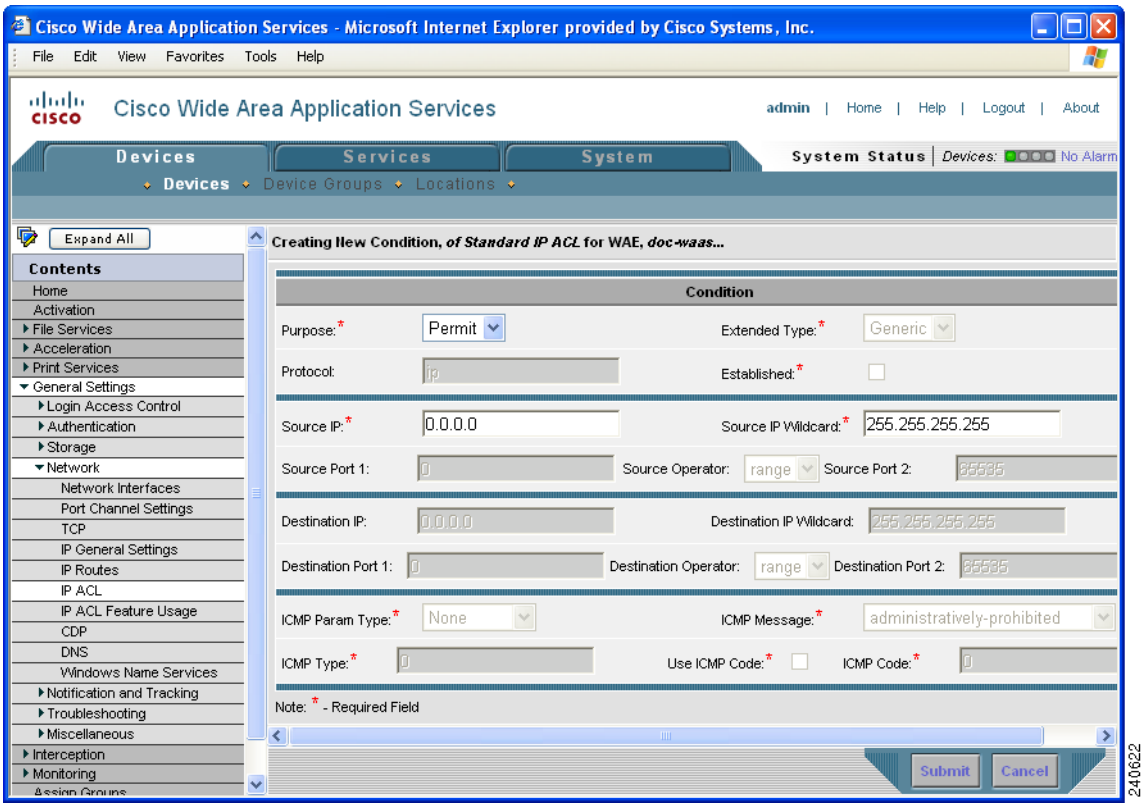
Step 7 Add conditions to the standard IP ACL named test1 that you just created:

a. In the taskbar, click the **Create New Condition** icon.

The Creating New Condition window appears. (See Figure 8-2.)

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 8-2 Creating a New Condition for an Extended IP ACL Window



b. Enter values for the properties that are enabled for the type of IP ACL that you are creating, as follows:

- To set up conditions for a standard IP ACL, go to Step 8.
- To set up conditions for an extended IP ACL, go to Step 9.

Step 8 Set up conditions for a standard IP ACL:

a. From the drop-down list, choose a purpose (**Permit** or **Deny**).

b. In the Source IP field, enter the source IP address.

c. In the Source IP Wildcard field, enter a source IP wildcard address.

d. Click **Submit** to save the condition.

The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.

e. To add another condition to the IP ACL, repeat the steps.

f. 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 WAAS Central 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 8-1 describes the fields in a standard IP ACL.

Table 8-1 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 9 Set up conditions for an extended IP ACL:

a. From the drop-down list, choose a purpose (**Permit** or **Deny**).

b. From the Extended Type drop-down list, choose **Generic**, **TCP**, **UDP**, or **ICMP**. (See Table 8-2.)

Table 8-2 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. The options are generic, TCP, UDP, or ICMP.

1. * = required field.

After you choose a type of extended IP ACL, various options become available in the GUI, depending on what type you choose.

c. In the fields that are enabled for the chosen type, enter the data. (For more information, see Table 8-4 through Table 8-7.)

d. Click **Submit** to save the condition.

The Modifying IP ACL window reappears, displaying the condition and its configured parameters in tabular format.

e. To add another condition to the IP ACL, repeat the steps.

f. 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 WAAS Central 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.

Step 10 Modify or delete an individual condition from an IP ACL:

a. 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 that are currently applied to the IP ACL.

b. Click the **Edit Condition** icon next to the condition that you want to modify or delete. The Modifying Condition window appears.

c. To modify the condition, change any allowable field as necessary.

d. To delete the condition, click the **Trash** (**Delete IP ACL Condition**) icon in the taskbar.

e. To reorder your list of conditions, use the Up or Down arrows in the Move column, and click **Submit**.

Step 11 Associate a standard IP ACL with SNMP or WCCP:

a. Click the **Edit** icon next to the name of the device for which you want to associate a standard IP ACL with SNMP or WCCP.

b. In the Contents pane, choose **General Settings > Network > IP ACL Feature Usage**. The IP ACL Feature Settings window appears.

c. From the drop-down lists, choose the name of an IP ACL for SNMP or WCCP. (For more details, see Table 8-3.) If you do not want to associate an IP ACL with one of the applications, choose **Do Not Set**.

Table 8-3 IP ACL Feature Settings

WAAS Central Manager GUI Parameter	Function
SNMP	Associates a standard IP ACL with SNMP. This option is supported for WAAS devices that are operating as a WAE or a WAAS Central Manager device.
WCCP	Associates any IP ACL with WCCP Version 2. This option is only supported for WAAS devices that are operating as a WAE and not as a WAAS Central Manager device. WCCP is only supported on WAEs; it is not supported on a WAAS Central Manager device.

d. Click **Submit** to save the settings.

Step 12 Apply an IP ACL to an interface:

a. Click the **Edit** icon next to the name of the device for which you want to apply an IP ACL to an interface on the WAE.

b. 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 port-channel interface indicating an EtherChannel configuration. EtherChannel for the WAAS software supports the grouping of up to four same-speed network interfaces into one virtual interface.

c. 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.

d. Scroll to the bottom of the window. From the Inbound ACL drop-down list, choose the name of an IP ACL.

e. From the Outbound ACL drop-down list, choose the name of an ACL.

The only network interface properties that can be altered from the WAAS Central 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 WAAS Central Manager GUI.

Step 13 Click **Submit** to save the settings.

Step 14 (Optional) Delete an IP ACL:

a. Click the **Edit** icon next to the name of the device that has the IP ACL that you want to delete.

b. In the Contents pane, choose **General Settings > Network > IP ACL**.

c. Click the **Edit** icon next to the name of the IP ACL that you want to delete (for example, test1).

The Modifying IP ACL window appears. If you created conditions for the IP ACL, you have two options for deletion:

- **Delete ACL**—Removes the IP ACL, including all conditions and associations with network interfaces and applications.
- **Delete All Conditions**—Removes all the conditions, while preserving the IP ACL name.

d. 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.

e. To delete only the conditions, click the small **Delete All Conditions** Trash/List icon in the taskbar. When you are prompted to confirm your action, click **OK**. The window refreshes, conditions are deleted, and the ACL Type field becomes available.

To define an IP ACL from the CLI, you can use the **ip access-list** global configuration command, and to apply the IP ACL to an interface on the WAAS device, you can use the **ip access-group** interface configuration command. To configure the use of an IP ACL for SNMP, you can use the **snmp-server access-list** global configuration command. To specify an IP ACL that the WAE applies to the inbound WCCP GRE encapsulated traffic that it receives, you can use the **wccp access-list** global configuration command.

List of Extended IP ACL Conditions

When you define a condition for an extended IP ACL, you can specify the Internet protocol to be applied to the condition (as described in Step 9 in the "Creating and Managing IP ACLs for WAAS Devices" section on page 8-3).

The list of extended IP ACL conditions are as follows:

- Generic (See Table 8-4.)
- TCP (See Table 8-5.)
- UDP (See Table 8-6.)
- ICMP (See Table 8-7.)

Table 8-4 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.
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 8-5 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.

Table 8-5 Extended IP ACL TCP Condition (continued)

Field	Default Value	Description
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 as follows: ftp, ftp-data, https, mms, netbios-dgm, netbios-ns, netbios-ss, nfs, rtsp, ssh, telnet, and www.
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 as follows: ftp, ftp-data, https, mms, netbios-dgm, netbios-ns, netbios-ss, nfs, rtsp, ssh, telnet, and 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 8-6 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.
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 8-6 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 as follows: bootpc, bootps, domain, mms, netbios-dgm, netbios-ns, netbios-ss, nfs, ntp, snmp, snmptrap, tacacs, tftp, and 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.
Destination Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0 to 65535. Valid UDP port names are as follows: bootpc, bootps, domain, mms, netbios-dgm, netbios-ns, netbios-ss, nfs, ntp, snmp, snmptrap, tacacs, tftp, and 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 8-7 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 8-7 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	Choices are **None**, **Type/Code**, or **Msg**. **None**—Disables the ICMP Type, Code, and Message fields. **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. **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.
ICMP Message*	administratively-prohibited	Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.
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.