CHAPTER 16

# Adding an EtherType Access List

This chapter describes how to configure EtherType access lists and includes the following sections:



## Information About EtherType Access Lists

An EtherType access list is made up of one or more Access Control Entries (ACEs) that specify an EtherType. An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number, as well as other traffic types. See the "Supported EtherTypes and Other Traffic" section on page 32-5 for more information.

For information about creating an access rule with the EtherType access list, see Chapter 32, "Configuring Access Rules."

## Licensing Requirements for EtherType Access Lists

The following table shows the licensing requirements for this feature:

| Model | License Requirement |
|---|---|
| All models | Base License. |

# Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

**Context Mode Guidelines**

Available in single and multiple context modes.

**Firewall Mode Guidelines**

Supported in transparent firewall mode only.

**IPv6 Guidelines**

Supports IPv6.

**Additional Guidelines and Limitations**

The following guidelines and limitations apply to EtherType access lists:

- For EtherType access lists, the implicit deny at the end of the access list does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the access list does not now block any IP traffic that you previously allowed with an extended access list (or implicitly allowed from a high security interface to a low security interface). However, if you *explicitly* deny all traffic with an EtherType ACE, then IP and ARP traffic is denied.
- 802.3-formatted frames are not handled by the access list because they use a length field as opposed to a type field.
- See the "Supported EtherTypes and Other Traffic" section on page 32-5 for more information about supported traffic.

# Default Settings

Access list logging generates system log message 106023 for denied packets. Deny packets must be present to log denied packets.

When you configure logging for the access list, the default severity level for system log message 106100 is 6 (informational).

# Configuring EtherType Access Lists

This section includes the following topics:



## Task Flow for Configuring EtherType Access Lists

Use the following guidelines to create and implement an access list:

**Step 1** Create an access list by adding an ACE and applying an access list name, as shown in the "Adding EtherType Access Lists" section on page 16-3.

**Step 2** Apply the access list to an interface. (See the "Configuring Access Rules" section on page 32-7 for more information.)

# Adding EtherType Access Lists

To configure an access list that controls traffic based upon its EtherType, perform the following steps:

### Detailed Steps

| Command | Purpose |
|---|---|
| **access-list** *access_list_name* **ethertype** {**deny** \| **permit**} {**ipx** \| **bpdu** \| **mpls-unicast** \| **mpls-multicast** \| **is-is** \| **any** \| *hex_number*}<br><br>**Example:**<br>`hostname(config)# hostname(config)#`<br>**`access-list ETHER ethertype permit ipx`** | Adds an EtherType ACE.<br><br>The *access_list_name* argument lists the name or number of an access list. When you specify an access list name, the ACE is added to the end of the access list. Enter the *access_list_name* in upper case letters so that the name is easy to see in the configuration. You might want to name the access list for the interface (for example, INSIDE) or for the purpose (for example, MPLS or PIX).<br><br>The **permit** keyword permits access if the conditions are matched.<br><br>The **deny** keyword denies access if the conditions are matched. If an EtherType access list is configured to deny all, all ethernet frames are discarded. Only physical protocol traffic, such as auto-negotiation, is still allowed.<br><br>The **ipx** keyword specifies access to IPX.<br><br>The **bpdu** keyword specifies access to bridge protocol data units, which are allowed by default.<br><br>The **mpls-unicast** keyword specifies access to MPLS unicast.<br><br>The **mpls-multicast** keyword specifies access to MPLS multicast.<br><br>The **is-is** keyword specifies access to IS-IS traffic (Version 8.4(5) only).<br><br>The **any** keyword specifies access for any traffic.<br><br>The *hex_number* argument indicates any EtherType that can be identified by a 16-bit hexadecimal number greater than or equal to 0x600. (See RFC 1700, "Assigned Numbers," at http://www.ietf.org/rfc/rfc1700.txt for a list of EtherTypes.)<br><br>**Note** To remove an EtherType ACE, enter the **no access-list** command with the entire command syntax string as it appears in the configuration. |

### Example

The following sample access list allows common EtherTypes originating on the inside interface:

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

## Adding Remarks to Access Lists

You can include remarks about entries in any access list, including extended, EtherType, IPv6, standard, and Webtype access lists. The remarks make an access list easier to understand.

To add a remark after the last **access-list** command you entered, enter the following command:

| Command | Purpose |
|---|---|
| **access-list** *access_list_name* **remark** *text*<br><br>**Example:**<br>`hostname(config)# access-list OUT remark - this is the inside admin address` | Adds a remark after the last **access-list** command you entered.<br>The text can be up to 100 characters in length. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.<br>If you enter the remark before any **access-list** command, then the remark is the first line in the access list.<br>If you delete an access list using the **no access-list** *access_list_name* command, then all remarks are also removed. |

### Example

You can add remarks before each ACE, and the remarks appear in the access list in these locations. Entering a dash (-) at the beginning of a remark helps to set it apart from the ACE.

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

# What to Do Next

Apply the access list to an interface. (See the "Configuring Access Rules" section on page 32-7 for more information.)

# Monitoring EtherType Access Lists

To monitor EtherType access lists, enter one of the following commands:

| Command | Purpose |
|---|---|
| **show access-list** | Displays the access list entries by number. |
| **show running-config access-list** | Displays the current running access-list configuration. |

# Configuration Examples for EtherType Access Lists

The following example shows how to configure EtherType access lists:

The following access list allows some EtherTypes through the ASA, but it denies IPX:

```
hostname(config)# access-list ETHER ethertype deny ipx
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

The following access list denies traffic with EtherType 0x1256, but it allows all others on both interfaces:

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

# Feature History for EtherType Access Lists

Table 16-1 lists each feature change and the platform release in which it was implemented.

*Table 16-1 Feature History for EtherType Access Lists*

| Feature Name | Releases | Feature Information |
|---|---|---|
| EtherType access lists | 7.0(1) | EtherType access lists control traffic based upon its EtherType.<br>We introduced the feature and the following command: **access-list ethertype**. |