



Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the access point using the web-browser interface. This chapter contains these sections:

- [Understanding Filters, page 16-2](#)
- [Configuring Filters Using the CLI, page 16-2](#)
- [Configuring Filters Using the Web-Browser Interface, page 16-2](#)

Understanding Filters

Protocol filters (IP protocol, IP port, and EtherType) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with the access point but does not block SNMP access from the wired LAN.

IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific IP or MAC addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify.

You can configure filters using the web-browser interface or by entering commands in the CLI.



Note

Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.



Tip

You can include filters in the access point's QoS policies. Refer to [Chapter 14, "Configuring QoS,"](#) for detailed instructions on setting up QoS policies.

Configuring Filters Using the CLI

To configure filters using CLI commands, you use access control lists (ACLs) and bridge groups. You can find explanations of these concepts and instructions for implementing them in these documents:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2.* Click this link to browse to the "Configuring Transparent Bridging" chapter:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm
- *Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide.* Click this link to browse to the "Command Reference" chapter:
http://www.cisco.com/univercd/cc/td/doc/product/13sw/4908g_13/ios_12/10w518e/config/cmd_ref.htm

Configuring Filters Using the Web-Browser Interface

This section describes how to configure and enable filters using the web-browser interface. You complete two steps to configure and enable a filter:

1. Name and configure the filter using the filter setup pages.
2. Enable the filter using the Apply Filters page.

These sections describe setting up and enabling three filter types:

- [Configuring and Enabling MAC Address Filters, page 16-3](#)
- [Configuring and Enabling IP Filters, page 16-8](#)
- [Configuring and Enabling EtherType Filters, page 16-11](#)

Configuring and Enabling MAC Address Filters

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.



Note

Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.



Note

MAC address filters are powerful, and you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, use the CLI to disable the filters.

Use the MAC Address Filters page to create MAC address filters for the access point. [Figure 16-1](#) shows the MAC Address Filters page.

Figure 16-1 MAC Address Filters Page

The screenshot displays the 'MAC Address Filters' configuration page. On the left is a navigation sidebar with categories like 'SERVICES' and 'WIRELESS SERVICES'. The main area has tabs for 'APPLY FILTERS', 'MAC ADDRESS FILTERS', 'IP FILTERS', and 'ETHERTYPE FILTERS'. Below the tabs, it shows 'Hostname ap' and 'ap uptime is 2 days, 21 hours, 40 minutes'. The 'Services: Filters - MAC Address Filters' section contains a 'Create/Edit Filter Index' dropdown set to '< NEW >'. Below that is a 'Filter Index' input field with '(700-799)' next to it. The 'Add MAC Address' section has three input fields: 'Add MAC Address' (with '(HHHH.HHHH.HHHH)' below), 'Mask' (with '0000.0000.0000' and '(HHHH.HHHH.HHHH)' below), and 'Action' (a dropdown set to 'Forward' and an 'Add' button). The 'Default Action' is a dropdown set to 'Block All'. The 'Filters Classes' section has an empty text area and a 'Delete Class' button. At the bottom right are 'Apply', 'Delete', and 'Cancel' buttons. A vertical number '111860' is on the far right edge.

Follow this link path to reach the Address Filters page:

1. Click **Services** in the page navigation bar.

2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

-
- Step 1** Follow the link path to the MAC Address Filters page.
 - Step 2** If you are creating a new MAC address filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter Index menu.
 - Step 3** In the Filter Index field, name the filter with a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.
 - Step 4** Enter a MAC address in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0005.9a39.2110, for example).



Note To make sure the filter operates properly, use lower case for all the letters in the MAC addresses that you enter.

- Step 5** Use the Mask entry field to indicate how many bits, from left to right, the filter checks against the MAC address. For example, to require an exact match with the MAC address (to check all bits) enter **0000.0000.0000**. To check only the first 4 bytes, enter **0.0.FFFF**.
- Step 6** Select **Forward** or **Block** from the Action menu.
- Step 7** Click **Add**. The MAC address appears in the Filters Classes field. To remove the MAC address from the Filters Classes list, select it and click **Delete Class**.
- Step 8** Repeat [Step 4](#) through [Step 7](#) to add addresses to the filter.
- Step 9** Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.



Tip You can create a list of allowed MAC addresses on an authentication server on your network. Consult the [“Configuring Authentication Types” section on page 10-10](#) for instructions on using MAC-based authentication.

- Step 10** Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.
- Step 11** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 16-2](#) shows the Apply Filters page.

Figure 16-2 Apply Filters Page

Services: Filters - Apply Filters						
	FastEthernet		Radio0-802.11B		Radio1-802.11A	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >

- Step 12** Select the filter number from one of the MAC drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.
- Step 13** Click **Apply**. The filter is enabled on the selected ports.

If clients are not filtered immediately, click **Reload** on the System Configuration page to restart the access point. To reach the System Configuration page, click **System Software** on the task menu and then click **System Configuration**.

**Note**

Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point reboots, or when the clients associate to another access point.

Using MAC Address ACLs to Block or Allow Client Association to the Access Point

You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

Follow these steps to use an ACL to filter associations to the access point radio:

- Step 1** Follow Steps 1 through 10 in the “[Creating a MAC Address Filter](#)” section on page 16-4 to create an ACL. For MAC addresses that you want to allow to associate, select **Forward** from the Action menu. Select **Block** for addresses that you want to prevent from associating. Select **Block All** from the Default Action menu.

Step 2 Click **Security** to browse to the Security Summary page. [Figure 16-3](#) shows the Security Summary page.

Figure 16-3 Security Summary Page

HOME	Hostname ap		ap uptime is 6 minutes	
EXPRESS SET-UP				
EXPRESS SECURITY				
NETWORK MAP +				
ASSOCIATION +				
NETWORK INTERFACES +				
SECURITY				
Admin Access				
Encryption Manager				
SSID Manager				
Server Manager				
Local RADIUS Server				
Advanced Security				
SERVICES +				
WIRELESS SERVICES +				
SYSTEM SOFTWARE +				
EVENT LOG +				

Security Summary							
Administrators							
Username	Read-Only			Read-Write			
Cisco	✓						
Radio0-802.11B SSIDs							
SSID	VLAN	Open	Shared	Network EAP			
tsunami	none	no addition					
Radio1-802.11A SSIDs							
SSID	VLAN	Open	Shared	Network EAP			
tsunami	none	no addition					
Radio0-802.11B Encryption Settings							
Encryption Mode	WEP		Cipher				Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	
None							
Radio1-802.11A Encryption Settings							
Encryption Mode	WEP		Cipher				Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	
None							
Server-Based Security							
Server Name/IP Address	Type	EAP	MAC	Proxy Mobile IP	Admin	Accounting	

111868

Step 3 Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. Figure 16-4 shows the MAC Address Authentication page.

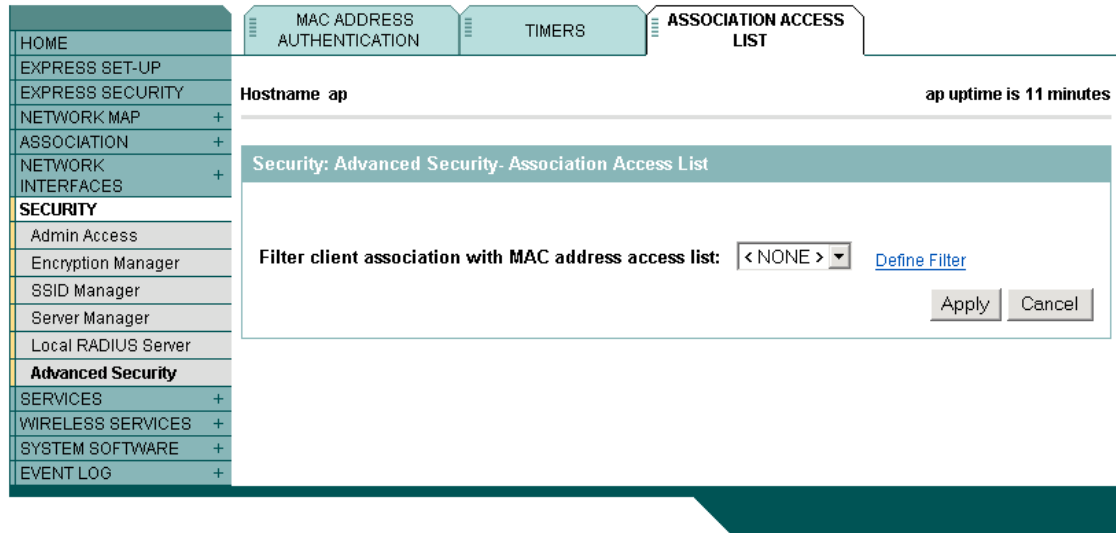
Figure 16-4 Advanced Security: MAC Address Authentication Page

The screenshot displays the configuration page for MAC Address Authentication. On the left is a navigation menu with items like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area has tabs for MAC ADDRESS AUTHENTICATION, TIMERS, and ASSOCIATION ACCESS LIST. The current page shows the hostname 'ap' and 'ap uptime is 8 minutes'. The configuration section is titled 'Security: Advanced Security- MAC Address Authentication' and includes a 'MAC Address Authentication' section with radio buttons for 'Local List Only' (selected), 'Authentication Server Only', and 'Authentication Server if not found in Local List'. Below this is a 'Local MAC Address List' section with a 'Local List' table (currently empty) and a 'Delete' button. At the bottom, there is a 'New MAC Address:' input field with a placeholder '(HHHH.HHHH.HHHH)' and an 'Apply' button.

111859

- Step 4** Click the **Association Access List** tab to browse to the Association Access List page. [Figure 16-5](#) shows the Association Access List page.

Figure 16-5 Association Access List Page



- Step 5** Select your MAC address ACL from the drop-down menu.

- Step 6** Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the “[Using MAC Address ACLs to Block or Allow Client Association to the Access Point](#)” section on page 16-5:

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

In this example, only client devices with MAC addresses listed in access list 777 are allowed to associate to the access point. The access point blocks associations from all other MAC addresses.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring and Enabling IP Filters

IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the access point’s Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the IP Filters page to create IP filters for the access point. Figure 16-6 shows the IP Filters page.

Figure 16-6 IP Filters Page

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES
Telnet/SSH
Hot Standby
CDP
DNS
Filters
HTTP
Proxy Mobile IP
QoS
SNMP
NTP
VLAN
ARP Caching
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

APPLY FILTERS MAC ADDRESS FILTERS **IP FILTERS** ETHERTYPE FILTERS

Hostname **ap** ap uptime is 2 hours, 49 minutes

Services: Filters - IP Filters

Create/Edit Filter Name: <NEW >

Filter Name:

Default Action: Block All

IP Address

Destination Address: Mask: 0.0.0.0

Source Address: 0.0.0.0 Mask: 255.255.255.255

Action: Forward Add

IP Protocol

IP Protocol: Authentication Header Protocol (51) Action: Forward Add

Custom (0-255)

UDP/TCP Port

TCP Port: Border Gateway Protocol (179) Action: Forward Add

Custom (0-65535)

UDP Port: Biff (mail notification, comsat 512) Action: Forward Add

Custom (0-65535)

Filters Classes

Delete Class

Apply Delete Cancel

Follow this link path to reach the IP Filters page:

1. Click **Services** in the page navigation bar.

2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **IP Filters** tab at the top of the page.

Creating an IP Filter

Follow these steps to create an IP filter:

-
- Step 1** Follow the link path to the IP Filters page.
 - Step 2** If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter name from the Create/Edit Filter Index menu.
 - Step 3** Enter a descriptive name for the new filter in the Filter Name field.
 - Step 4** Select **Forward all** or **Block all** as the filter's default action from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an IP port and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.
 - Step 5** To filter an IP address, enter an address in the IP Address field.



Note If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point.

- Step 6** Type the mask for the IP address in the Mask field. Enter the mask with periods separating the groups of characters (112.334.556.778, for example). If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.
- Step 7** Select **Forward** or **Block** from the Action menu.
- Step 8** Click **Add**. The address appears in the Filters Classes field. To remove the address from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 5](#) through [Step 8](#) to add addresses to the filter.
If you do not need to add IP protocol or IP port elements to the filter, skip to [Step 15](#) to save the filter on the access point.
- Step 9** To filter an IP protocol, select one of the common protocols from the IP Protocol drop-down menu, or select the **Custom** radio button and enter the number of an existing ACL in the Custom field. Enter an ACL number from 0 to 255. See [Appendix B, "Protocol Filters,"](#) for a list of IP protocols and their numeric designators.
- Step 10** Select **Forward** or **Block** from the Action menu.
- Step 11** Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 9](#) to [Step 11](#) to add protocols to the filter.
If you do not need to add IP port elements to the filter, skip to [Step 15](#) to save the filter on the access point.
- Step 12** To filter a TCP or UDP port protocol, select one of the common port protocols from the TCP Port or UDP Port drop-down menus, or select the **Custom** radio button and enter the number of an existing protocol in one of the Custom fields. Enter a protocol number from 0 to 65535. See [Appendix B, "Protocol Filters,"](#) for a list of IP port protocols and their numeric designators.
- Step 13** Select **Forward** or **Block** from the Action menu.

- Step 14** Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 12](#) to [Step 14](#) to add protocols to the filter.
- Step 15** When the filter is complete, click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.
- Step 16** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 16-7](#) shows the Apply Filters page.

Figure 16-7 Apply Filters Page

Services: Filters - Apply Filters						
	FastEthernet		Radio0-802.11B		Radio1-802.11A	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >

- Step 17** Select the filter name from one of the IP drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.
- Step 18** Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling Ethertype Filters

Ethertype filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the Ethertype Filters page to create Ethertype filters for the access point. [Figure 16-8](#) shows the Ethertype Filters page.

Figure 16-8 Ethertype Filters Page

HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION + NETWORK INTERFACES + SECURITY + SERVICES Telnet/SSH Hot Standby CDP DNS Filters HTTP Proxy Mobile IP QoS SNMP NTP VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +

APPLY FILTERS MAC ADDRESS FILTERS IP FILTERS ETHERTYPE FILTERS

Hostname ap ap uptime is 2 hours, 55 minutes

Services: Filters - EtherType Filters

Create/Edit Filter Index: <NEW>

Filter Index: (200-299)

Add EtherType: Mask: 0000 Action: Forward Add
(0-FFFF) (0-FFFE)

Default Action: Block All

Filters Classes:

Delete Class

Apply Delete Cancel

Follow this link path to reach the Ethertype Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **Ethertype Filters** tab at the top of the page.

Creating an Ethertype Filter

Follow these steps to create an Ethertype filter:

- Step 1** Follow the link path to the Ethertype Filters page.
- Step 2** If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.
- Step 3** In the Filter Index field, name the filter with a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.
- Step 4** Enter an Ethertype number in the Add EtherType field. See [Appendix B, “Protocol Filters,”](#) for a list of protocols and their numeric designators.
- Step 5** Enter the mask for the Ethertype in the Mask field. If you enter **0**, the mask requires an exact match of the Ethertype.
- Step 6** Select **Forward** or **Block** from the Action menu.

- Step 7** Click **Add**. The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat [Step 4](#) through [Step 7](#) to add Ethernets to the filter.
- Step 8** Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the Ethernets in the filter. For example, if you enter several Ethernets and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.
- Step 9** Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.
- Step 10** Click the **Apply Filters** tab to return to the Apply Filters page. [Figure 16-9](#) shows the Apply Filters page.

Figure 16-9 Apply Filters Page

Services: Filters - Apply Filters						
	FastEthernet		Radio0-802.11B		Radio1-802.11A	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >

- Step 11** Select the filter number from one of the Ethertype drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.
- Step 12** Click **Apply**. The filter is enabled on the selected ports.

