

# **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 15-2
- Configuring Filters Using the CLI, page 15-2
- Configuring Filters Using the Web-Browser Interface, page 15-3

## **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.

Tin

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.



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.

## **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



Avoid using both the CLI and the web-browser interfaces to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured. For example, if you configure ACLs using the CLI, the web-browser interface might display this message: "Filter 700 was configured on interface Dot11Radio0 using CLI. It must be cleared via CLI to ensure proper operation of the web interface." If you see this message you should use the CLI to delete the ACLs and use the web-browser interface to reconfigure them.

## **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 15-3
- Configuring and Enabling IP Filters, page 15-9
- Configuring and Enabling Ethertype Filters, page 15-12

### **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.



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 15-1 shows the MAC Address Filters page.

Γ

HOME	APPLY FILTERS	MAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
EXPRESS SET-UP				HEIERO	
EXPRESS SECURITY	Hostname ap			ap uptime is 2 days, 21 hours	: 40 minutos
NETWORK MAP +			,	ap apartic is 2 adys, 2 i noars	, <del>40</del> minutes
ASSOCIATION +					
NETWORK +	Services: Filters - I	MAC Address Filters			
INTERFACES +					
SECURITY +	Create/Edit Filter I	ndex: <new></new>			
SERVICES					
Telnet/SSH					
Hot Standby	- Filter Index:		(700-799)		
CDP	-	1	(100-100)		
DNS	-				
Filters	Add MAC Address		Mask: 0000.0000.0000	Action: Forward -	Add
НТТР	- Autu MAC Auturess		Wask: 10000.0000.0000	Action: [Forward]	
	-	(HHHH.HHHH.HHHH)	(HHHH.HHHH.H	HHH)	
Proxy Mobile IP QoS	-				
	_				
SNMP	Default Action:	Block All 🔻			
NTP					
VLAN					
ARP Caching	Filters Classes:				
WIRELESS SERVICES +				_	
SYSTEM SOFTWARE +					
EVENTLOG +					
				Delete Class	
	1				
				Apply Delete	Cancel

Figure 15-1 MAC Address Filters Page

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	v the link path to the MAC Address Filters page.						
Step 2	If you are creating a new MAC address filter, make sure <b><new></new></b> (the default) is selected in the Create/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter In 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		a MAC address in the Add MAC Address field. Enter the address with periods separating the three s 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.

```
\mathcal{P}
```

```
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 15-2 shows the Apply Filters page.

HOME		FILTERS	MAC ADDRESS FILTERS	IP F		ETHERTYPE FILTERS	
EXPRESS SET-UP							
EXPRESS SECURITY	Hostname a	p			ap uptin	ne is 2 days, 2ª	l hours, 50 minutes
NETWORK MAP +		-					•
ASSOCIATION +							
NETWORK +	Services:	Filters - Appl	y Filters				
SECURITY +		Fast	Ethernet	Radio	o0-802.11B	Radio	1-802.11A
SERVICES	Incoming	MAC	<none> -</none>	MAC	< NONE > -	MAC	< NONE > -
Telnet/SSH		101/20		1000		1000	
Hot Standby		EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
CDP							
DNS		IP	< NONE > -	IP	< NONE > -	IP	< NONE > -
Filters							
HTTP	Outgoing	MAC	< NONE > 💌	MAC	< NONE > 💌	MAC	< NONE > 💌
Proxy Mobile IP				<b>FU T</b>		EU T	
QoS		EtherType	< NONE > 💌	EtherType	< NONE > 💌	EtherType	< NONE > 💌
SNMP		IP	< NONE > -	IP	<none> -</none>	IP	< NONE > -
NTP						"	
VLAN							
ARP Caching							
WIRELESS SERVICES +							
SYSTEM SOFTWARE +							
EVENTLOG +							

Figure 15-2 Apply Filters Page

- **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 15-4 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 15-3 shows the Security Summary page.

HOME	Hostname l	JD_AP1230					UD,	_AP1230 upti	me is 3	days, 23	hours, 33 minute
EXPRESS SET-UP											
NETWORK MAP +											
ASSOCIATION	Security S	Summary									
NETWORK +	Administra	tors									
NTERFACES									_		
SECURITY	Username	9			Read-O	nly			R	ead-Wri	te
Admin Access	Cisco				1						
SSID Manager					•						
Encryption Manager	Radio0-802	2.11B SSIDs									
Server Manager	SSID		VI	AN.		pen		Shared		Notw	ork EAP
Local RADIUS Server	3310		VL			hen		Silarea		110.00	OTR EAL
Advanced Security	romeo		1	13		✓					
BERVICES +	Dadio4.001	2.11A SSIDs									
WIRELESS SERVICES +	<u>rtaulu 1-002</u>	<u></u>									
BYSTEM SOFTWARE + EVENT LOG +	SSID		VL	VLAN		Open		Shared		Netw	ork EAP
	romeo		1	4		✓					
	Torrico					•					
	Encryption	Settings									
			W	EP				Cipher			
	VLAN	Encryption Mode	MIC	DDV	TKID	SIZE I	0.401.14	UCD4001.54	CIVID	CHIC	Key Rotation
			MIC	РРК	TKIP	WE	P40bit	WEP128bit	CKIP	CMIC	
	13	WEP-Mandatory									
	14	WEP-Optional									
	Server-Bas	sed Security									
	Server Name/IP Address		Туре	EA	P M.	AC	Proxy	Mobile IP	A	Imin	Accounting
				_							

Figure 15-3 Security Summary Page

**Step 3** Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. Figure 15-4 shows the MAC Address Authentication page.

HOME			
EXPRESS SET-UP			
EXPRESS SECURITY	Hostname ap		ap uptime is 8 minutes
NETWORK MAP +			
ASSOCIATION +	Security: Advanced Security- MAC A	d daaraa Aardhaardhaadhaar	
NETWORK +	Security: Advanced Security- MAC A	uuress Aumenucauon	
SECURITY	MAC Address Authentication		
Admin Access			
Encryption Manager	MAC Addresses Authenticated by:	Content of Content	
SSID Manager		C Authentication Server Only	
Server Manager		-	
Local RADIUS Server		O Authentication Server if no	t found in Local List
Advanced Security			Apply Cancel
SERVICES +			Apply Cancel
WIRELESS SERVICES +			
SYSTEM SOFTWARE +	Local MAC Address List		
EVENT LOG +	Local List:		
	Eucal List.		
			Delete
	New MAC Address:		ІНН.НННН)
			Apply

Figure 15-4 Advanced Security: MAC Address Authentication Page

**Step 4** Click the Association Access List tab to browse to the Association Access List page. Figure 15-5 shows the Association Access List page.

Figure 15-5 Association Access List Page

HOME	
EXPRESS SET-UP	
EXPRESS SECURITY	Hostname ap ap uptime is 11 minutes
NETWORK MAP +	
ASSOCIATION +	
NETWORK	Security: Advanced Security- Association Access List
INTERFACES	
SECURITY	
Admin Access	
Encryption Manager	Filter client association with MAC address access list: <pre></pre>
SSID Manager	Anatal Oracel
Server Manager	Apply Cancel
Local RADIUS Server	
Advanced Security	
SERVICES +	
WIRELESS SERVICES +	
SYSTEM SOFTWARE +	
EVENTLOG +	

**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 15-6:

```
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 15-6 shows the IP Filters page.

Figure	15-6	<b>IP Filters</b>	Page
--------	------	-------------------	------

Impress Ser.uP   Depress Ser.uP   Assocution   Assocution   Assocution   Services: Fitters - IP Fitters   Nitter/Action   Services: Fitters - IP Fitters   Interview   Name:   Interview	LIOME	APPLY FILTERS	MAC ADDRESS FILTERS	IP FILTI	ERS	ETHERTYPE FILTERS	
EXPERSESSECURITY Hostname ap ap uptime is 2 hours, 49 minutes   ASSOCATION ASSOCATION   ASSOCATION Create/Edit Filters. IP Filters   SECURITY Secures   Bame: Image: I			HEIEKO			HEIERO	
NETWORK MAP + REMOKE MAP + REMOK		Hostname an				an untimo is 2	hours 40 minutes
ASSOCUTION *  Services: Filters - IP Filters INTERACES  FilterKSH HITERACES  Filter Name:  Create/Edit Filter Name:  Services:  Filter Name:  Filter State		nostiane ap				ap apartic is 2	nours, 45 minutes
INTERFACES   SERVICTS   Teinet/SSH   Hot Standary   CDP   Default Action:   Block All •   HTTP   PAddress   Destination Address:   0:00   SNMP   NTP   Poxy Mobile P   Ods   Oss   SNMP   NTP   Poxy Mobile P   Ods   SNMP   NTP   Poxy Mobile P   Ods   SNMP   NTP   VLAN   ARP Caching   WRELESS SERVICES +   SYSTEM SOFTWARE +   P Protocol   IP Protocol:   C Custom   (0:255)      UDP/TCP Port   TCP Port:   © Border Gateway Protocol (179)   Action:   Forward • Add   © Custom   (0:45535)   UDP Port:   © Elift (mail notification. comset, 512)   Action:   Forward • Add   © Custom   (0:45535)							
NILTERHACES   SECURITY   SECURITY   SECURITY   Name:   Interfection   Hot Standby   CDP   Diss   Default Action:   Block All •   Prov Mobile IP OoS OoS Source Address: 0.0.0.0 Mask: 0.0.0.0 Mask: 0.0.0.0 Mask: 0.0.0.0 Mask: 255.255.255.255 Mask: Filter Name: Forward • Add Protocol Protocol IP Protocol IP Protocol IP Protocol IDP/TCP Port Custom (0-255) UDP/TCP Port IDP/TCP Port: C Barder Gateway Protocol (179) • Action: Forward • Add C Custom (0-65535) UDP Port: C Barder Gateway Protocol (179) • Action: Forward • Add C Custom (0-65535) IDP Port: Eleft (mail notification, comset 512) • Action: Forward • Add C Custom (0-65535) IDP Port: Eleft Classe Delete Class	NETWORK	Services: Filters - IP F	liters				
SERVICES   TeinetISSH   Hot Standay   CDP   Filter Name:   Default Action:   Block All ▼   HTTP   PAddress   Destination Address:   008   SNMP   NTP   VLAN   ARP Caching   WRELESS SERVICES +   SYSTEM SOFTWARE +   P Protocol   IP Protocol   IP Protocol   Custom   (0-255)   IUDP/TCP Port:    IDP Port:   © Border Gateway Protocol (179)   Action:   Forward ■ Add   Custom   (0-85535)   UDP Port:   © Builder Gateway Protocol (179)   Action:   Forward ■ Add   Custom   (0-85535)   UDP Port:   © Builder Gateway Protocol (179)   Action:   Forward ■ Add   Custom   (0-85535)   UDP Port:   © Builder Gateway Protocol (179)   Action:   Forward ■ Add   Custom   (0-85535)	INTERFACES						
StrivtLS   Name:   FilterSH   HotStandby   COP   DNS   Default Action:   Block All    HTTP   Proxy Mobile IP   GoS   GoS   SNMME   NAN   ARP Caching   WIRELESS SERVICES +   SYSTEM SOFTWARE +   IP Protocol   IP Protocol +   IP Protocol +   IP Protocol +   UDP/TCP Port   TCP Port:   © Custom   (0-255)   Here Classe    Here Class		•	<new></new>				
Hot Standby   CDP   DNS   Defout Action:   Block All ▼   HTTP   Proxy Mobile IP   QoS   SNMP   NNP   VLAN   ARP Caching   WRELESS SERVICES *   SYSTEM SOFTWARE *   EVENT LOG   IP Protocol:   © Custom   (0-255)   UDP/TCP Port Custom Custom (0-2555) Filters Classes Elete Class Delete Class		Name:					
CDP Filter Name:   DN8 Default Action:   Block All ▼   HTTP P Address:   OoS   SNMP   NTP   VLAN   ARP Caching   WIRELESS SERVICE   Protocol   Protocol   Custom   (0-255)   UDP/TCP Port TCP Port: Custom Custom (0-255) UDP/TCP Port: Custom Custom Custom (0-255) Filters Classes LUP Port: Elete Class Detere Class							
DNS   Filters   HTTP   Proxy Mobile IP   GoS   GoS   Source Address:   0.0.0   Mask:   20.0   Mask:   255.255.255.255   VLAN   ARP Caching   WIRELESS SERVICES +   SYSTEM SOFTWARE +   IP Protocol   IP Protocol   IP Protocol:   © Custom   (0-255)   UDP/TCP Port TCP Port: © Border Gateway Protocol (179) Action: Forward • Add © Custom (0-2555) IUDP Port: © Biff (mail notification, comset, 512) Action: Forward • Add © Custom (0-65535) UDP Port: © Biff (mail notification, comset, 512) Action: Forward • Add © Custom @0-65535) UDP Port: © Biff (mail notification, comset, 512) Action: Forward • Add © Custom @0-65535) UDP Port: © Biff (mail notification, comset, 512) Action: Forward • Add © Custom @0-65535) UDP Port: © Biff (mail notification, comset, 512) Action: Forward • Add © Custom @0-65535)		<b>F</b> 114 - N					
Filters Default Action: Elick All    HTTP IP Address: IP Address:   Ox03 Destination Address: Mask:   SNMP Source Address: 0.0.0   NTP VLAN   ARP Caching WIRELESS SERVICES   WIRELESS SERVICES Action:   Forward  Add   Caching IP Protocol   UDP/TCP Port IP Protocol:   Custom 0-255)   UDP/TCP Port Custom		Filter Name:					
HTTP       IP Address         Prow Mobile IP       Oo8         Oo8       Destination Address:       Mask: 00.00         SNMP       Source Address:       0.0.0       Mask: 255.255.255         VLAN       ARP Caching       Action: Forward < Add         WRELESS SERVICES *       IP Protocol       IP Protocol         UDP/TCP Port       Custom (0-255)       Action: Forward < Add         C Custom       (0-255)       Action: Forward < Add         C Custom       (0-65535)       UDP/TCP Port         TCP Port:       © Border Gateway Protocol (179)       Action: Forward < Add         C Custom       (0-65535)       Action: Forward < Add         Delete Class       Delete Class       Action: Forward < Add		Default Action:	Block All 💌				
Proxy Mobile IP IP Address   OoS Destination Address:   NTP Source Address:   VLAN ARP Caching   WRELESS SERVICES +   SYSTEM SOFTWARE +   EVENT LOO   IP Protocol   © Custom   (D-255)   UDP/TCP Port Custom Cu-255) Action: Forward Address: IUDP/TCP Port Custom Custom Cu-255) Action: Forward Address Action: Forward Address Description: Custom Custom Cu-255) Custom Custom Custom Cu-255) Custom </th <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
QoS   SNMP   NTP   VLAN   ARP Caching   WIRELESS SERVICES +   VURN   ARP Caching   WIRELESS SERVICES +   Protocol   IP Protocol   Custom   (0.255)   UDP/TCP Port   TCP Port:   Custom   (0.465535)   UDP Port:   Custom   (0.465535)   Filters Classes   Delete Class		IP Address					
SNMP       Destination Address:       0.0.0         NTP       VLAN       Action:       Forward < Add         ARP Caching       IP Protocol       IP Protocol       IP Protocol         WIRELESS SERVICES *       SySTEM SOFTWARE *       IP Protocol       IP Protocol         UDP/TCP Port       Custom       (0.255)       Action:       Forward < Add         UDP/TCP Port       © Custom       (0.65535)       OUDP/TCP Port       Action:       Forward < Add         © Custom       (0.65535)       UDP Port:       © Biff (mail notification.comsat.512)       Action:       Forward < Add         © Custom       (0.65535)       IDP Port:       © Biff (mail notification.comsat.512)       Action:       Forward < Add         © Custom       (0.65535)       IDP Port:       © Biff (mail notification.comsat.512)       Action:       Forward < Add         © Custom       (0.65535)       IDP Port:       © Biff (mail notification.comsat.512)       IDP Action:       Forward < Add         © Lelete Class       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:         IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:       IDP Port:							
NTP   VLAN   ARP Caching   WIRELESS SERVICES   SYSTEM SOFTWARE   EVENT LOG   IP Protocol   IP Protocol   Custom   (0-255)   UDP/TCP Port Custom (0-255) Action: Forward Add Add Custom (0-65535) UDP Port: © Bird(mail notification, comsat 512) Action: Forward Add Custom Custom (0-65535) Filters Classes Elelete Class		Destination Address:		Mask: 0.0.0.	0		
VLAN ARP Caching   ARTO Caching   WIRELESS SERVICES +   WOTEN SOFTWARE + +   EVENT LOOG +   IP Protocol:   Custom   (0-255)   UDP/TCP Port Custom (0-255) Action: Forward Add Custom (0-65535) UDP Port: E Birlf (mail notification, comsat 512) Action: Forward Add Custom (0-65535) Eilters Classes Delete Class		C 411					
ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + IP Protocol:  Authentication Header Protocol (51) Action: Forward Add C Custom (0-255) UDP/TCP Port TCP Port:  Border Gateway Protocol (179) Action: Forward Add C Custom (0-65535) UDP Port:  Biff (mail notification, comsat 512) Action: Forward Add C Custom (0-65535) Filters Classes Delete Class		Source Address:	0.0.0	Mask: 255.2	55.255.255		
ArP Caching   WRELESS SERVICES *   SYSTEM SOFTWARE +   EVENT LOG +   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						Action: Forv	vard 🔻 Add
SYSTEM SOFTWARE +   EVENT LOG   *     IP Protocol:   © Authentication Header Protocol (51)   • Custom     (0-255)     UDP/TCP Port:   © Border Gateway Protocol (179)   • Action:   Forward • Add   • Custom	-						
EVENT LOG     IP Protocol:        IP Protocol:        IP Protocol:        IP Protocol:        IP Protocol:							
IP Protocol: <ul> <li>Authentication Header Protocol (51)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> </ul> Custom (0-255)   UDP/TCP Port    TCP Port: <ul> <li>Border Gateway Protocol (179)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> <li>Custom</li> <li>(0-65535)</li> </ul> UDP Port: <ul> <li>Biff (mail notification, comsat 512)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> <li>Custom</li> <li>(0-65535)</li> </ul> Filters Classes   Delete Class		IP Protocol					
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	EVENTLUG +						
UDP/TCP Port TCP Port:   Border Gateway Protocol (179)  Custom  Custom  (0-65535)  UDP Port:  Biff (mail notification, comsat 512)  Action: Forward Add  Custom  (0-65535)  Filters Classes  Delete Class		IP Protocol: 💿 Au	thentication Header F	Protocol (51)	-	Action: Forv	vard 💌 🛛 Add
UDP/TCP Port TCP Port:   Border Gateway Protocol (179)  Custom  Custom  (0-65535)  UDP Port:  Biff (mail notification, comsat 512)  Action: Forward Add  Custom  (0-65535)  Filters Classes  Delete Class							
TCP Port: <ul> <li>Border Gateway Protocol (179)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> </ul> Custom (0-65535)   UDP Port:   Biff (mail notification, comsat 512)  Action: Forward Add    Custom (0-65535)   Filters Classes    Delete Class		C Cus	stom	(0-255)			
TCP Port: <ul> <li>Border Gateway Protocol (179)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> </ul> Custom (0-65535)   UDP Port:   Biff (mail notification, comsat 512)  Action: Forward Add    Custom (0-65535)   Filters Classes    Delete Class							
TCP Port: <ul> <li>Border Gateway Protocol (179)</li> <li>Action:</li> <li>Forward</li> <li>Add</li> </ul> Custom (0-65535)   UDP Port:   Biff (mail notification, comsat 512)  Action: Forward Add    Custom (0-65535)   Filters Classes    Delete Class							
C Custom (0-65535) UDP Port: © Biff (mail notification, comsat, 512) • Action: Forward • Add C Custom (0-65535) Filters Classes Delete Class		UDP/TCP PUIL					
Custom (0-65535) UDP Port: © Biff (mail notification, comsat 512)  Action: Forward Add Custom (0-65535) Filters Classes Delete Class		TCP Part: @ Bord	er Gateway Protocol i	(179)	-	Action: For	Add
UDP Port:  Biff (mail notification, comsat 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class				(173)			
UDP Port:  Biff (mail notification, comsat 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class		C Custo	m	(0-65535)			
Custom (0-65535)				· · · ·			
Custom (0-65535)							
Filters Classes  Delete Class		UDP Port: 💿 Biff (r	nail notification, coms	at 512)	•	Action: Forv	vard 💌 Add
Filters Classes  Delete Class						-	
Delete Class		C Custo	m	(0-65535)			
Delete Class							
Delete Class							
		Filters Classes					
		<u> </u>					
		Delete Class					
							9
Apply Delete Cancel						Apply Dr	elete 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 255.255.255.255.255 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 15-7 shows the Apply Filters page.

Figure 15-7 Apply Filters Page

НОМЕ		FILTERS	MAC ADDRESS FILTERS	IP F		ETHERTYPE FILTERS	
EXPRESS SET-UP							
EXPRESS SECURITY	Hostname a	p			ap uptin	ne is 2 days, 21	hours, 50 minutes
NETWORK MAP +							
ASSOCIATION +							
NETWORK +	Services:	Filters - Appl	-				
SECURITY +		Fast	Ethernet	Radio	0-802.11B	Radio	1-802.11A
SERVICES Telnet/SSH	Incoming	MAC	< NONE > -	MAC	< NONE > -	MAC	< NONE > -
Hot Standby CDP		EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
DNS		IP	< NONE > -	IP	< NONE > -	IP	< NONE > -
Filters							
HTTP	Outgoing	MAC	< NONE > 💌	MAC	< NONE > 💌	MAC	< NONE > 💌
Proxy Mobile IP QoS		EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
SNMP		18		18			
NTP		IP	< NONE > 💌	IP	< NONE > 💌	IP	< NONE > 💌
VLAN							
ARP Caching							
WIRELESS SERVICES +							
SYSTEM SOFTWARE +							
EVENT LOG +							
							Apply Cancel

- 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 15-8 shows the Ethertype Filters page.

НОМЕ		IAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
EXPRESS SET-UP EXPRESS SECURITY	Hostname ap			ap uptime is 2 hours,	55 minutes
NETWORK MAP + ASSOCIATION + NETWORK + INTERFACES +	Services: Filters - EtherTyp	e Filters			
SECURITY + SERVICES Telnet/SSH	Create/Edit Filter Index:	<new></new>	•		
Hot Standby CDP DNS	Filter Index:		200-299)		
Filters HTTP	Add EtherType:	M	ask: 0000	Action: Forward -	Add
Proxy Mobile IP QoS SNMP NTP VLAN	(0-FFFF) Default Action: Block All	•	(D-FFFE)		
ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +	Filters Classes:				
				Delete Class	
				Apply Delete	Cancel

Figure 15-8 Ethertype Filters Page

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:

p 1	Follow the link path to the Ethertype Filters page.
p 2	If you are creating a new filter, make sure <b><new></new></b> (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.
p 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.
p 4	Enter an Ethertype number in the Add Ethertype field. See Appendix B, "Protocol Filters," for a list of protocols and their numeric designators.
5	Enter the mask for the Ethertype in the Mask field. If you enter <b>0</b> , the mask requires an exact match of the Ethertype.
;	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 Ethertypes 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 Ethertypes in the filter. For example, if you enter several Ethertypes 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 15-9 shows the Apply Filters page.

НОМЕ		FILTERS	MAC ADDRESS FILTERS	IP F		ETHERTYPE FILTERS	
EXPRESS SET-UP							
EXPRESS SECURITY	Hostname a	p			ap uptin	ne is 2 days, 21	l hours, 50 minutes
NETWORK MAP +		-					
ASSOCIATION +							
NETWORK INTERFACES +	Services:	Filters - Appl	y Filters				
SECURITY +		Fast	Ethernet	Radi	o0-802.11B	Radio	01-802.11A
SERVICES	Incoming	MAC		MAC		MAC	
Telnet/SSH	incoming	MAC	< NONE > 💌	MAC	< NONE > 💌	IVIAC	< NONE > 💌
Hot Standby		EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
CDP		Emerrype		Emeriype		Emerijpe	
DNS		IP	< NONE > -	IP	< NONE > -	IP	< NONE > -
Filters	· ·						
HTTP	Outgoing	MAC	< NONE > 💌	MAC	< NONE > 💌	MAC	< NONE > -
Proxy Mobile IP		E.1. T		<b>EU T</b>		T	
QoS		EtherType	< NONE > 💌	EtherType	< NONE > 💌	EtherType	< NONE > 💌
SNMP		IP	<none> -</none>	IP	< NONE > -	IP	< NONE > -
NTP		"					
VLAN							
ARP Caching	-						
WIRELESS SERVICES +							
SYSTEM SOFTWARE +							
EVENTLOG +							
							Apply Cancel

#### Figure 15-9 Apply Filters Page

**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.