

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.

HOME	APPLY FILTERS		IP FILTERS		
EXPRESS SET-LIP				HEIERO	
EXPRESS SECURITY	Hostname an			an untimo is 2 davs. 21 hours	: 40 minutos
NETWORK MAP +	nostiane ap		,	ap apartic is 2 adys, 2 i noars	, 40 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 Addroom		Maaka 0000 0000 0000	Action: Forward	Add [
нттр	- Autu MAC Auturess		Mask: 10000.0000.0000	Action: [Forward]	
Dreve Mahila ID	-	(HHHH.HHHH.HHHH)	(HHHH.HHHH.H	HHH)	
	-				
QUS	_				
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 Create menu.	are creating a new MAC address filter, make sure <new></new> (the default) is selected in the e/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter Index							
Step 3	In the an acc	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 group	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.

НОМЕ		FILTERS	MAC ADDRESS FILTERS	IP F		ETHERTYPE FILTERS			
EXPRESS SET-UP					I				
EXPRESS SECURITY Hostname ap ap uptime is 2 days, 21 hours, 50 minutes									
NETWORK MAP +									
ASSOCIATION +									
NETWORK INTERFACES +	Services:	Filters - Appl	ly Filters						
SECURITY +		Fast	tEthernet	Radio	o0-802.11B	Radio	o1-802.11A		
SERVICES Telnet/SSH	Incoming	MAC	< NONE > -	MAC	< NONE > -	MAC	< NONE > -		
Hot Standby		EtherType	<none> -</none>	EtherType	< NONE > -	EtherType	< NONE > -		
DNS	-	IP	<none> -</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 NTP	-	IP	< NONE > -	IP	<none></none>	IP	< NONE > -		
VLAN					,				
ARP Caching									
WIRELESS SERVICES +									
SYSTEM SOFTWARE +									
EVENT LOG +									
							Apply Cancel		

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.

IOME	Hostname I	UD AP1230					UE) AP1230 upti	me is 3	days, 23	hours, 33 minute
EXPRESS SET-UP											,
VETWORK MAP +											
SSOCIATION	Security	Summary									
IETWORK NTERFACES +	Administra	ators									
ECURITY	- Usernam	e			Read-O	nly			R	ead-Wri	te
Admin Access						-					
SSID Manager	Cisco				√						
Encryption Manager	Radio0-80	2.11B SSIDs									
Gerver Manager											
Local RADIUS Server	SSID		VL	.AN	0)pen		Shared		Netw	ork EAP
Advanced Security	romeo			13		✓					
ERVICES +											
IRELESS SERVICES +	Radio1-80	Radio1-802.11A SSIDs									
/STEM SOFTWARE + /ENT LOG +	SSID	SSID		VLAN		Open		Shared		Netw	ork EAP
	romeo		14		✓						
	Encryption	Encryption Settings									
		-	W	ЕР				Cipher			
	VLAN	Encryption Mode	MIC	РРК	ткір	WE	P40bit	WEP128bit	CKIP	CMIC	Key Rotation
	13	WEP-Mandatory									
	14	WEP-Optional									
	Server-Ba	sed Security									
	Server Na	Server Name/IP Address		EA	P M.	AC	Prox	Proxy Mobile IP		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.

	MAC ADDRESS		
HOME			
EXPRESS SET-UP			
EXPRESS SECURITY	Hostname ap		ap uptime is 8 minutes
NETWORK MAP +			
ASSOCIATION +	Convita Advanced Convita MAC	deleges Authoritication	
INTEDEACES +	Security: Advanced Security- MAC /	Autress Autrenucation	
SECURITY	MAC Address Authentication		
Admin Access			
Encryption Manager	MAC Addresses Authenticated by:	Cocal List Only	
SSID Manager		 Authentication Server Only 	,
Server Manager			
Local RADIUS Server		O Authentication Server if not	t found in Local List
Advanced Security			Apply Cancol
SERVICES +			Apply Calicer
WIRELESS SERVICES +			
SYSTEM SOFTWARE +	Local MAC Address List		
EVENT LOG +	Logal List		
	LUCAI LISC		
			Delete
	New MAC Address:		
		(HHHH.HF	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

LIOME	
EXPRESS SET-UP	
EXPRESS SECURITY	Hostname an an untime 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	
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	IP Filters	Page
--------	------	-------------------	------

Provide: Precision EVPRESS SET-UP EVPRESS SET-UP EVPRESS SECURITY Hostname ap ABSOCURITY Hostname ap Services: Filters - IP Filters Tenee2SH Hot Standby ODB DNB Programballe IP Oos Services: Filters: Mask: [0.0.0 Services: III of Address: Mask: [255 255 255 255 Action: Forward ▼ Add WRELESS SERVICES + SYSTEM SOFTWARE + IP Protocol IP Protocol: Prostocol: Outhertication Header Protocol (51) ▼ Action: Forward ▼ Add C Custom (0.255) UDP/TCP Pert TCP Port: © Custom UDP/TCP Pert C Custom Custom (0.65535) UDP Port: © Elifer Classes	LIOME	APPLY FILTERS		IP FILTI	ERS	ETHERTYPE	
BYPESS SECURITY NETWORK MAP NETWORK Preverse Pitter Name: Default Action: Block All * HTTP Proverse Default Action: Block All * HTTP Proverse Oos <			HEIEKO			HEIERO	
Network MAP ABSOCUTOM ABSOCUTOM ABSOCUTOM Services: Fiters - IP Fiters NTER/ACES Fiters Create/Edit Filter Name: Indianday COP DNB Default Action: Block All ♥ HTTP Proy Mobile IP Ox8 SNMP Source Address: MRELESS SERVICES TerretSSH NTF VLN Action: Forward ♥ Ac	EXPRESS SECURITY	Hostname an				an untimo is 2	hours 40 minutes
ASSOCHTON A NTERVORK NTERVORK SECURITY SEC	NETWORK MAP +	nostiane ap				ap apartic is 2	nours, 45 minutes
NETWORK Services: Filters - IP Filters Security Security Security CreaterEdit Filter Name: Intersecurity Filters Cop Filters DN8 Default Action: Block All ▼ HTTP Prowy Mobile P Oos Source Address: 00.0 Services: Mask: 00.0 Services: Oos Source Address: 00.0 Mask: 255.255.255 Action: Forward ▼ ARP Caching WRELEBS SERVICEs VEN ARP Caching WRELEBS SERVICEs UDP/TCP Port IP Protocol IP Protocol: Custom (0-255) UDP/TCP Port TCP Port: © Bird(mail notification, comset, 512) Custom (0-26535) Eiters Classes Eiters Classes Eiters Classes	ASSOCIATION +						
INTERFACES SECURITY Teine055H Hot Standby CDP Default Action: Block All Filter Name: Filter Name: Forward Add Custom Cust	NETWORK _	Services: Filters - IP F	liters				
SECURITY Create/Edit Filter Name: KNEW> Hot Standby CCDP Filter Name: Image: DNS Default Action: Block All Image: HTTP IP Address Doss Source Address: 0.0.0 Mask: 0.0.0 Mask: Source Address: 0.0.0 Source Address: 0.0.0 MREKESS SERVICES Action: Forward Add WIRELESS SERVICES IP Protocol IP Protocol C Custom UDP/TCP Port IDP/TCP Port TCP Port: © Border Gateway Protocol (173) Action: Forward Add C Custom 0.0.65535) UDP Port: IUDP Port: © Biff (mail notification. conset 512) Action: Forward Add Custom (0.65535)	INTERFACES						
SkrVUCS HotStandty COP DNB Default Action: Block All HTTP Proxy Mobile IP GoS GoS Oos SNMP Proxy Mobile IP GoS GoS Os Source Address: D0.0 Mask: 255 255 255 255 VLAN ARP Caching WRELESS SERVICES + VP Protocol Protocol IP Protocol IP Protocol: Custom (0-255) UDP/TCP Port TCP Port: Custom Custom (0-65535) Filters Classes	SECURITY +	Create/Edit Filter	<new> -</new>				
Intervention Intervention <th>SERVICES</th> <th>Name:</th> <th></th> <th></th> <th></th> <th></th> <th></th>	SERVICES	Name:					
Hot Standby CDP Filter Name: Default Action: Block All Filters HTTP Proxy Mobile IP OoS OOS SNMMP Proxy Mobile IP OoS Source Address: 0.0.0 Mask: 0.0.0 Mask: 255.255.255 Action: Forward Add Action: Forward Add Custom 0.255 UDP/TCP Port TCP Port © Border Gateway Protocol (179) Action: Forward Add Custom 0.255 UDP/TCP Port TCP Port: © Border Gateway Protocol (179) Action: Forward Add Custom 0.255 UDP Port: © Biff (mail notification, cornsat 512) Action: Forward Add Custom 0.45535 UDP Port: © Biff (mail notification, cornsat 512) Action: Forward Add Custom 0.45535 UDP Port: © Custom 0.45535 Custom 0.4553	Tellievson						
CUP Filter Name: DNS Default Action: Block All ▼ HTTP Proxy Mobile IP OoS OoS SNMP NNP VLAN ARP Caching WRELESS SERVICES SYSTEM SOFTWARE + EVENT LOG IP Protocol: © Custom (0-255) UDP/TCP Port Custom (0-255) Filters Classes Eiler Class Delete Class	Hot Standby	F 114 - N					
DNS Default Action: Elock All ▼ HTTP IP Address Oo8 SNMP NTP Source Address: 0.0.0 Mask: 255.255.255 VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG IP Protocol IP Protocol IP Protocol UDP/TCP Port TCP Port: © Border Gateway Protocol (179) Action: Forward • Add © Custom (0-255) Filters Classes Default Action: Forward • Add Custom (0-65535) UDP Port: © Biff (mail notification, comsat 512) • Action: Forward • Add Custom (0-65535) UDP Celoci Eilere Class		Filter Name:					
HITTS Proxy Mobile IP OoS OoS ONMP NTP Source Address: 0.0.0 Mask: 255.255.255 VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOO IP Protocol IP Protocol IP Protocol IP Protocol: © Authentication Header Protocol (51) Action: Forward Add © Custom (0-65535) UDP/TCP Port TCP Port: © Border Gateway Protocol (179) Action: Forward Add © Custom (0-65535) UDP Port: © Birl(mail notification. comsat.512) Action: Forward Add © Custom (0-65535) Eilters Classes	DNS Filtere	Default Action:	Block All 💌				
HITP IP Address GoS Destination Address: NMP Source Address: VLAN ARP Caching WRELESS SERVICE + SYSTEM SOFTWARE + EVENT LOG IP Protocol C Custom (C-255) UDP/TCP Port TCP Port: © Border Gateway Protocol (71) Action: Forward Add C Custom (0-65535) UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add C Custom C Custom C-26535) UDP Port: © Custom C-26535) UDP Port: © Custom C-26535) UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add C Custom C-26535) UDP Port: © Custom C-26535) UDP Port: © Custom C-26535) UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add C Custom C-26535) C Custom C-26535) UDP Port: © Custom C-26535) Custom C-26535)	Fifters						
Prox Mobile IP OG8 SNMP NTP VLAN ARP Caching WRELESS SERVICES + SYSTEM SOFTWARE + P Protocol IP Protocol * Portor Custom Delete Class	ние	IP Address					
U03 Destination Address: Mask: 0.0.0 SNMP NTP Source Address: 0.0.0 Mask: VLAN ARP Caching Action: Forward < Add WRELESS SERVICES + P Protocol IP Protocol IP Protocol (51) Action: SYSTEM SOFTWARE + IP Protocol: I Authentication Header Protocol (51) Action: IVDP/TCP Port Custom (0-255) UDP/TCP Port: ICP Port: IVDP Port: Iff(mail notification, comset 512) Action: IVDP Port: Iff(mail notification, comset 512) Action: IVDP Port: Iff(mail notification, comset 512) Action: IVDP I Image: Imag	Proxy Mobile IP						
SNMP VLAN ARP Caching VURN ARP Caching WIRELESS SERVICES System SOFTWARE IP Protocol IP Protocol IP Protocol IDDP/TCP Port Custorn (0-255) IDDP/TCP Port Custorn Close535) IDP Porte Elifers Classes Elifers Classes Delete Class		Destination Address:		Mask: 0.0.0.	0		
NIP VLAN ARP Caching Action: Forward Add WIRELESS SERVICES + IP Protocol WIRELESS SERVICES + IP Protocol IP Protocol + IP Protocol (51) Action: Forward Add UDP/TCP Port Custom (0-255) UDP/TCP Port Custom (0-255) UDP Port: © Birder Gateway Protocol (179) 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 Delete Class Delete Class	SNMP	C 411					
ARP Caching MRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + IP Protocol: © Authentication Header Protocol (51) • Action: Forward • Add © Custom (0-255) UDP/TCP Port: © Custom	NTP	Source Address:	0.0.0	Mask: 255.2	55.255.255		
APP Caching WIRELESS SERVICES YOTEM SOFTWARE EVENT LOG * IP Protocol: © Authentication Header Protocol (51) Action: Forward Add © Custom 00-255) UDP/TCP Port TCP Port: © Border Gateway Protocol (179) Action: Forward Add © Custom 00-65535) UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add © Custom 00-65535) Filters Classes Delete Class	VLAN					Action: Forv	vard 🔻 Add
WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + IP Protocol C 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	ARP Caching						
SYSTEM SOFTWARE + 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	WIRELESS SERVICES +						
EVENT LOG IP Protocol: <pre></pre>	SYSTEM SOFTWARE +	IP Protocol					
IP Protocol: 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	EVENTLUG +						
C 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		IP Protocol: 💿 Au	thentication Header F	Protocol (51)	-	Action: Forv	vard 💌 🛛 Add
UDP/TCP Port TCP Port Custom							
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		C Cus	stom	(0-255)			
UDP/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							
TCP Port: Border Gateway Protocol (179) Custom (0-65535) UDP Port: Biff (mail notification, comsat 512) Action: Forward < Add Custom (0-65535) Filters Classes Delete Class							
TCP Port: Border Gateway Protocol (179) Action: Custom Custom (0-65535) UDP Port: Biff (mail notification, comsat, 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class		UDP/TCP PUIL					
Custom (0-65535) UDP Port: Biff (mail notification, comsat, 512) Custom (0-65535) Filters Classes Delete Class		TCP Part: @ Bord	er Gateway Protocol i	(179)	-	Action: For	Add
Custom (0-65535) UDP Port: Ref (mail notification, comsat, 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class				(173)			
UDP Port: Biff (mail notification, comsat, 512) Custom Custom Custom Co-65535) Filters Classes Delete Class		C Custo	m	(0-65535)			
UDP Port: Biff (mail notification, comsat 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class				· · · ·			
UDP Port: Biff (mail notification, comsat 512) Action: Forward Add Custom (0-65535) Filters Classes Delete Class							
Custom (0-65535)		UDP Port: 💿 Biff (r	nail notification, coms	at 512)	•	Action: Forv	vard 💌 Add
Custom [(0-65535)						-	
Filters Classes Delete Class		C Custo	m	(0-65535)			
Filters Classes Delete Class							
Filters Classes							
Delete Class		Filters Classes					
Delete Class							
Delete Class							
Delete Class							
Delete Class							
Delete Class		<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

INDUC INDUC <td< th=""><th>HOME</th><th></th><th>FILTERS</th><th>MAC ADDRESS</th><th>IP F</th><th></th><th>ETHERTYPE FILTERS</th><th></th></td<>	HOME		FILTERS	MAC ADDRESS	IP F		ETHERTYPE FILTERS	
Restance ap ap uptime is 2 days, 21 hours, 50 mi NETWORK MAP Association Services: Filters - Apply Filters Made Colspan="2">CONNE > Made Colspan="2">CONE > Outgoing MAC CONNE > MAC CNONE > MAC CNONE > Proxy Mobile IP Outgoing QoS MAC SNMP IP NTP IP VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG	EXPRESS SET-UP		L L					
NETWORK MAP + ASSOCIATION + NETWORK + NETWORK + NETWORK + Securices: Filters - Apply Filters Security + Security + FastEthernet Radio0.802.11B Radio1.802.11A Security + FastEthernet Radio1.802.11B Radio1.802.11A Security + FastEthernet Radio0.802.11B Radio1.802.11A Security + FastEthernet Radio1.802.11A Radio1.802.11A Security + FastEthernet Radio1.802.11A Radio1.802.11A Security + FastEthernet Radio1.802.11A Radio1.802.11A Incoming MAC MAC MAC Incoming MAC EtherType NONE > IP DNS IP MAC GDNS IP MAC <	EXPRESS SECURITY	Hostname a	ip .			ap u	ptime is 2 days, 2	1 hours, 50 minutes
ASSOCIATION + NETWORK INTERFACES + SERVICES FastEthernet Radio-802.118 Radio1-802.11A SERVICES Incoming MAC <none> MAC <none> Hot Standby EtherType <none> MAC <none> MAC <none> DNS EtherType <none> IP <none> IP <none> IP <none> Proxy Mobile IP Outgoing MAC <none> MAC <none> MAC <none> NTP IP <none> IP <none> IP <none> IP <none> WIRELESS SERVICES + IP <none> IP <none> <t< td=""><td>NETWORK MAP +</td><td></td><td></td><td></td><td></td><td>•</td><td>• • • •</td><td></td></t<></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>	NETWORK MAP +					•	• • • •	
NETWORK INTERFACES + Services: Filters - Apply Filters SECURITY + FastEthernet Radio-802.11B Radio-802.11A SERVICES Incoming MAC < NONE > MAC < NONE > Telnet/SSH Incoming MAC < NONE > MAC < NONE > MAC < NONE > Hot Standby CDP EtherType < NONE > EtherType < NONE > EtherType < NONE > DNS Fitters IP < NONE > IP < NONE > IP < NONE > IP < NONE > Proxy Mobile IP Quo MAC < NONE > EtherType < NONE > IP	ASSOCIATION +							
SECURITY + FastEthernet Radio-802.11B Radio-802.11A SERVICES Incoming MAC <none> MAC <none> MAC <none> Hot Standby CDP EtherType <none> EtherType <none> EtherType <none> DNS IP <none> IP <none> IP <none> IP <none> Filters Outgoing MAC <none> MAC <none> IP <none> Proxy Mobile IP MAC <none> MAC <none> MAC <none> QoS EtherType <none> EtherType <none> MAC <none> NTP IP <none> IP <none> IP <none> VLAN ARP Caching IP <none> IP <none> IP <none> WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +</none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none></none>	NETWORK INTERFACES +	Services:	Filters - App	ly Filters				
SERVICES Incoming MAC < NONE > MAC < NONE > MAC < NONE > Hot Standby CDP EtherType < NONE > EtherType < NONE > EtherType < NONE > DNS IP EtherType < NONE > IP < NONE > IP < NONE > Filters Outgoing MAC < NONE > IP < NONE > IP < NONE > Proxy Mobile IP Outgoing MAC < NONE > MAC < NONE > MAC < NONE > goS EtherType < NONE > EtherType < NONE > MAC < NONE > NTP EtherType < NONE > IP < NONE > IP < NONE > VLAN ARP Caching # IP < NONE > IP < NONE > IP < NONE > WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +	SECURITY +		Fas	tEthernet	Radio	o0-802.11B	Radi	o1-802.11A
Hot Standby EtherType IP	SERVICES Telnet/SSH	Incoming	MAC	< NONE > -	MAC	< NONE > -	MAC	< NONE > -
DNS IP IP <t< td=""><td>Hot Standby</td><td></td><td>EtherType</td><td>< NONE > -</td><td>EtherType</td><td>< NONE > -</td><td>EtherType</td><td>< NONE > -</td></t<>	Hot Standby		EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
Filters Outgoing MAC Image: None image	DNS		IP	< NONE > -	IP	< NONE > -] IP	< NONE > -
HTTP Outgoing MAC < NONE > MAC < NONE > Proxy Mobile IP GoS EtherType < NONE > EtherType < NONE > QoS EtherType < NONE > EtherType < NONE > EtherType SNMP IP IP < NONE > IP < NONE > IP VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +	Filters						-	
Proxy Mobile IP EtherType NONE > EtherType NONE > QoS EtherType NONE > EtherType NONE > SNMP IP NONE > IP NONE > NTP IP NONE > IP NONE > VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG	HTTP	Outgoing	MAC	< NONE > 🔻	MAC	< NONE > -	MAC	< NONE > 💌
SNMP IP	Proxy Mobile IP QoS	-	EtherType	< NONE > -	EtherType	< NONE > -	EtherType	< NONE > -
VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +	SNMP NTP	_	IP	< NONE > -	IP	< NONE > -] IP	< NONE > -
ARP Caching WIRELESS SERVICES SYSTEM SOFTWARE + EVENT LOG	VLAN							
WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +	ARP Caching							
SYSTEM SOFTWARE + EVENT LOG +	WIRELESS SERVICES +	-						
EVENTLOG +	SYSTEM SOFTWARE +	-						
	EVENTLOG +							

- 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.

HOME	APPLY FILTERS	IP FILTERS	ETHERTYPE FILTERS
EXPRESS SET-UP EXPRESS SECURITY	Hostname ap		ap uptime is 2 hours, 55 minutes
ASSOCIATION + NETWORK + NETWORK +	Services: Filters - EtherType Filters		
SECURITY + SERVICES Telnet/SSH	Create/Edit Filter Index: <pre></pre>	•	
Hot Standby CDP	Filter Index: (20	0-299)	
Filters HTTP	Add EtherType: Mas	sk: 0000	Action: Forward Add
Proxy Mobile IP QoS SNMP NTP VI AN	(U-FFFF) Default Action: Block All	(U-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:

Step 1	Follow the link path to the Ethertype Filters page.
Step 2	If you are creating a new filter, make sure <new></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 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.

HOME		FILTERS	MAC ADDRESS	IP F			
		L	HEIERO			HEIERO	
	Hostnamo				an untin	o ic Cale Ca	houre 50 minutoe
NETWORK MAR +	nosulaine a	h			ah nhuu	ie is z udys, z	nours, so minutes
ASSOCIATION +							
NETWORK +	Services:	Filters - Appl	y Filters			1	
SECURITY +		Fast	Ethernet	Radio	o0-802.11B	Radio	01-802.11A
SERVICES	lu a antina						
Telnet/SSH	Incoming	MAC	< NONE > <	MAC	< NONE > <	MAC	<pre>NONE > _</pre>
Hot Standby		EtherTyne		EtherTyne		EtherTyne	
CDP		Emerijpe		Emerrype		Emerijpe	
DNS		IP	< NONE > -	IP	<none> -</none>	IP	< NONE > -
Filters							
HTTP	Outgoing	MAC	< NONE > 💌	MAC	< NONE > 💌	MAC	< NONE > 💌
Proxy Mobile IP						FU T	
QoS		Etheriype	<pre>NONE > _</pre>	Etheriype	< NONE > <	Etneriype	<pre>NONE > _</pre>
SNMP		IP		IP		IP	
NTP							
VLAN							
ARP Caching							
WIRELESS SERVICES +							
SYSTEM SOFTWARE +							
EVENT LOG +							
							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.