

Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and Ethertype filters on the access point/bridge 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 15-2

Understanding Filters

Protocol filters (IP protocol, IP port, and Ethertype) prevent or allow the use of specific protocols through the access point/bridge'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/bridge's radio port prevents wireless clients from using SNMP with the access point/bridge 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.

 \mathcal{P} Tin

You can include filters in the access point/bridge'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 IOS commands, you use access control lists (ACLs) and access point/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/l3sw/4908g_l3/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 15-3
- Configuring and Enabling IP Filters, page 15-7
- Configuring and Enabling Ethertype Filters, page 15-10

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.

٩, Note

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



MAC address filters are powerful, and you can lock yourself out of the access point/bridge if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point/bridge, use the CLI to disable the filters, or use the Mode button on the access point/bridge power injector to reset the access point/bridge to factory defaults.

Use the MAC Address Filters page to create MAC address filters for the access point/bridge. Figure 15-1 shows the MAC Address Filters page.

	APPLY FILTERS
HOME	
EXPRESS SET-UP	Hostname bridge uptime is 1 day, 23 hours, 26 minutes
EXPRESS SECURITY	······································
NETWORK MAP +	
ASSOCIATION +	Services: Filters - MAC Address Filters
NETWORK +	
INTERFACES	Create/Edit Filter Index: <new></new>
SECURITY +	
SERVICES	
TeinevSSH	Filter Index: (700-799)
CDP	
DNS	
Filters	Add MAC Address: Mask: 0000 0000 Action: Forward Add
HTTP	Add mAc Address. midsk. 5000.0000 Address. rod
Proxy Mobile IP	(НННН. НННН, НННН) (НННН. НННН, НННН)
QoS	
SNMP	
NTP	Default Action: Block All
VLAN	
SIP	Filters Classes:
ARP Caching	
WIRELESS SERVICES +	
SYSTEM SOFTWARE +	
EVENTLOG +	
	Delete Class
	Apply Delete Cancel
	Apply Delete Caliber 4

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 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 (0005.9a39.3456, for example).



Note To make sure the filter operates properly, use lower case for all the letters in the MAC address 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.



You can create a list of allowed MAC addresses on an authentication server on our network.Consult the Chapter 10, "Configuring Authentication Types" for instructions on using MAC based authentication.

- Step 10 Click Apply. The filter is saved on the access point/bridge, 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.

	APPLY FILTERS	MAC ADDRESS		ETHERTYP	E FILTERS
HOME	-		17		
EXPRESS SET-UP	Hostname bridge			bridge upt	ime is 1 day, 23 hours, 30 minutes
EXPRESS SECURITY	-				
NETWORK MAP +					
ASSOCIATION +	Services: Filters - App	ly Filters			
NETWORK +		-			
INTERFACES		Fa	stEthernet	Rac	lio0-802.11G
SECURITY +	Incoming	MAC		MAC	
SERVICES	meening	MAC	KNONE >	MAC	I NONE > •
Telnet/SSH		EthorTupo		EthorTuno	
CDP		Luenype		Luenype	KNONE >
DNS		ID		ID	
Filters		IF		I	
HTTP	Outgoing	MAC	< NONE > -	MAC	<none> •</none>
Proxy Mobile IP					
QoS		EtherType	< NONE > -	EtherType	< NONE > 💌
SNMP					
NTP		IP	< NONE >	IP	< NONE >
VLAN					
STP					
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/bridge. To reach the System Configuration page, click **System Software** on the task menu and then click **System Configuration**.

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.

10		Cisco Airo	onet	1300) Serie	es Wi	irele	ss Bridg	e			12 🖴
E	Hostname ro	ot								root uptii	me is 1 week,	1 hour, 27 minut
RESS SET-UP												
VORK MAP +	Security S	ummary										
CIATION +	Administrat	ors										
VORK +	Hoornamo				D/	ad Onl					Doad Mirito	
RITY	Username				r.t	au-om	У				Redu-wille	
nin Access	Cisco					\checkmark						
ryption Manager	Service Set	Identifiers (SSIDs)										
u manager ver Manager	SSID		VL	AN	Radi	0	BSS	ID/Guest Mo	dev	Onen	Shared	Network FAF
al RADIUS Server					rtuur		000		401		Sharea	Hotwork LA
anced Security	floorine		1	R	adio0-80	2.11G	00	12.433d.f400		no additio	n	
/ICES +	vlan71		7	1 R	adio0-80	2.11G	00	12.433d.f400	 Image: A set of the set of the	no additio	n	
LESS SERVICES +	Encryption	Settings	_									
EM SUFIWARE +			14	/ED				Cinh				
	VLAN	VLAN Encryption Mode		WEP				Cibu	ei			Key Rotation
				PPK	TKIP	WEP4	lObit	WEP128bit	CKI	P CMIC	AES CCM	
	1	None										
	71	None										
	Server-Base	ed Security										
	Server Name/IP Address		Туре		ype EA		۱P	MAC		Admin	Ac	counting
	192.168.17	0.2		RADI	US	*	/					

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.

Figure 15-4 Advanced Security: MAC Address Authentication Page

MAC Address List Mac Address List Mac Address List Mac Address List Cisco Aironet 1300 Series Wireless Bridge Mac Address Servue Mac Address Authentication Mac Address Authenticated by: Cisco Aironet Security Authentication Server Only Authentication Server Only Cisco Aironet Security Authentication Server In of found in Local List Local MAC Address List Local List: Delete New MAC Address: (HHHH.HHHH.HHHH)	ISCO SYSTEMS					
MME MAC ADDRESS AUTHENTICATION TIMERS ASSOCIATION ACCESS LIST PRESS SECURITY PRESS SECURITY TWORK MAP Hostname root root uptime is 1 week, 1 hour, 32 minute Sociation + TWORK * Security: Advanced Security- MAC Address Authentication MAC Address Authenticated by: © Local List Only SID Manager © Authentication Server Only enerr Manager © Authentication Server In to found in Local List RVOCES + VICES + Local MAC Address List	ավիտուսվիտու	Cisco	o Aironet 1300	Series Wireless Brid	ge	12 🛋
IMPE PRESS SET-UP PRESS SET-UP Fostname root TWORK MAP * SOCIATION * YMORK * CURITY Authentication MAC Address Authenticated by: • CURITY • MAC Address Authenticated by: • CURITY • MAC Address Authenticated by: • Cocal MAC Address List • VOCES • STEN SOFTWARE • ENT LOG • New MAC Address: • New MAC Address: • New MAC Address: •		MAC ADDRESS	THERE	ASSOCIATION ACCESS		
PRESS SECURITY PRESS SECURITY PRESS SECURITY Advanced Security: Advanced Security: MAC Address Authentication MAC Address Authentication MAC Address Authenticated by: Caucel List Only Caucel List Only Caucel List Cacel MAC Address List Local MAC Address List Local List: Delete New MAC Address: (HHHH.HHHH.HHHH) Apply Caucel	DME	AUTHENTICATION	I IMERS			
PRESS SECURITY Tototame root root uptime is 1 week, 1 hour, 32 minute TWORK MAP * * SOCIATION * * * TWORK MAP * * CURITY MAC Address Authentication * MAC Address Authenticated by: * Local List Only SID Manager * Authentication Server Only * enerer Manager * Authentication Server only * RELESS SERVICES + * Apply Cancel Local MAC Address List Local List: Delete * New MAC Address: Apply	PRESS SET-UP	F 5		· · ·		
TWORK MAP + SOCIATION + SOCIATION + SOCIATION + SOCIATION + SOCIATION + SOCIATION + SOCIATION + Security: Advanced Security: MAC Address Authentication MAC Address Authentication MAC Address Authenticated by: • Local List Only SID Manager erver Manager erver Manager C Authentication Server Only C Authentication Server In to found in Local List RELESS SERVICES + STEM SOFTWARE + ENTLOG + Local MAC Address List Local List: New MAC Address: New MAC Address: (HHHH.HHHH.HHHH) Apply	PRESS SECURITY	Hostname root			root uptime is	1 week, 1 hour, 32 minute
Sociation + TWORK + TERFACES + CURITY CURITY MAC Address Authentication MAC Address Authenticated by: Cocal List Only MAC Address Authenticated by: Cocal List Only MAC Address Authenticated by: Cocal List Only C Authentication Server Only C Authentication Server if not found in Local List RVICES + RVICES + TERESSERVICES + STEM SOFTWARE + ENT LOG + Local MAC Address List Local List: Delete New MAC Address: (HHHH.HHHH.HHHH)	TWORK MAP +					
CTWORK Security: Advanced Security: MAC Address Authentication MAC Address Authentication MAC Address Authentication MAC Address Authentication MAC Address Authentication MAC Address Authenticated by:	SOCIATION +					
LINENALES MAC Address Authentication dmin Access MAC Address Authenticated by: • Local List Only erver Manager • Authentication Server Only • Authentication Server Integration • Authentication • Apply • Cancel • Cancel • Local MAC Address • Authentication • Delete • New MAC Address: • (HHHH, HHHH, HHHH) • Apply • Authentication	TWORK +	Security: Advanced Sec	urity- MAC Address A	uthentication		
Addrin Access ncryption Manager sito Manager sito Manager werer Manager chanced Security RVICES + RVICES + RUESS SERVICES + STEM SOFTWARE + ENT LOG + Local MAC Address List Local List: Delete New MAC Address: (HHHL,HHHL,HHHL,HHHL) Apply Cancel	CUDITY	MAC Address Authentica	tion			
MAC Addresses Authenticated by: © Local List Only SID Manager errer Manager Authentication Server Only C Authentication Server if not found in Local List Apply Cancel Local MAC Address List Local List: New MAC Address: New MAC Address: New MAC Address: C Authentication Server only C Authentica	dmin Assoc					
Authentication Server Only erver Manager erver Manager dvanced Security RELESS SERVICES + STEM SOFTWARE + ENTLOG + Local MAC Address List Local List: Delete New MAC Address: (HHHH, HHHH, HHHH, HHHH) Apply	Instantion Monogor	MAC Addresses Authen	ticated by:	Local List Only		
Slot Manager dvanced Security RVICES + RVICES + ENT LOG + Local MAC Address List Local List: New MAC Address: New MAC Address: Local MAC Address: (HHHH.HHHH.HHHH) Apply Cancel Delete	OD Manager	-	-			
ever manager (C Authentication Server if not found in Local List RVICES TEM SOFTWARE + ENT LOG Local MAC Address List Local List: Delete New MAC Address: (HHHH.HHHH.HHHH.HHHH) Apoly	ISID Wanager	-		C Authentication Server	Only	
twonces + RELESS SERVICES + STEM SOFTWARE + Local MAC Address List	erver manager	-		O Authentication Server i	if not found in Local List	
NUCES RADEX Apply Cancel RELESS SERVICES + STEM SOFTWARE + Local MAC Address List	avanced Security			 Authentication Server 	ii not iounu in Local List	
New MAC Address:	RVICES +					Apply Cancel
Local MAC Address: CHHHH.HHHH.HHHH.HHHH)	RELESS SERVICES +					
Local List:	ENTLOG +	Local MAC Address List				
Local List: Delete New MAC Address: (HHHH, HHHH, HHHH) Apply	LINI EUO I	•				
New MAC Address: (HHHH.HHHH.HHHH)		Local List:			Delete	
		New MAC Address:		(ннн	1.НННН.НННН)	Apply

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

CISCO SYSTEMS 19 🖻 Cisco Aironet 1300 Series Wireless Bridge MAC ADDRESS AUTHENTICATION ASSOCIATION ACCESS TIMERS LIST EXPRESS SET-UP EXPRESS SECURITY Hostname root root uptime is 1 week, 1 hour, 42 minutes NETWORK MAP ASSOCIATION NETWORK INTERFACES Security: Advanced Security- As ociation Access L SECURITY Admin Access < NONE >
Define Filter Filter client association with MAC address access list: Encryption Manage SSID Manager Apply Cancel Server Manager Local RADIUS Serve Advanced Security SYSTEM SOFTWARE

Figure 15-5 Association List Page

- Step 5 Select your MAC address ACL from the drop down menu.
- Step 6 Click Apply.

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 15-5:

```
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/bridge'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/bridge. Figure 15-6 shows the IP Filters page.

APPL/FILTER MACADDRESS FILTERS IP FILTERS RESS SECURPY Diridge uptime is 1 day, 1 hour, 0 minute RESS SECURPY Output to the state in the sta							_	
He BS SET-UP RESS SET-UP RESS SET-UP RESS SET-UP RESS SET-UP RESS SET-UP RESS SET-UP Sorvices: Filters . IP Filters Create/Edit Filter Name: NCES P Default Action: Bilter Name: 0.0.0.0 Mask: 0.0.0.0 Mask	0.45	APPLY FILTERS	MAC ADDRESS FILTERS) I	IP FILTERS	ETHERTYPE FILTER	RS	
Hestname bridge bridge uptime is 1 day, 1 hour, 0 minut Work MP • Work MP • Work MP • Work MP • Work MCS • Filter Name: • Default Action: • Bis • Default Action: • IP Address • Destination Address: • Mask: 00.0.0 Source Address: 00.0.0 Mask: 00.0.0 P • Cathing • P Protocol • HtsSoftWarff • P Protocol • Action: Forward • Add • Custom (0.255) UDP/TCP Port Custom Custom •<	IUME							
Services: Filters - IP Filters Ocation: P Create/Edit Filter Name: P P Default Action: Block.All • P P Default Action: Block.All • P P Default Action: Block.All • P P Address: Default Action: Block.All • P </td <td>VPRESS SEI-UP</td> <td>Hostname bridge</td> <td></td> <td></td> <td></td> <td>bridge uptime</td> <td>is 1 day, 1 hour,</td> <td>0 minutes</td>	VPRESS SEI-UP	Hostname bridge				bridge uptime	is 1 day, 1 hour,	0 minutes
Nuclear Norman Nuclear Street Nucle								
Solucion Solucion Solucion Solucion: Solucion: Solucion P P S S P Create/Edit Filter Name: P P S S Mais: 0.0.0 Mask: 0.0.0 Source Address: 0.0.0 Mask: 25525525525 Action: Forward Add P P caching ELESS SERVICES + IP Protocol IP Protocol IP Protocol IP Protocol Custom 0(0-255) UDP/TCP Port TCP Port: Classes UDP/TCP Port: Classes Filters Classes Filters Classes Filters Classes Filters Classes Filters Classes Filters Classes Filters Classes								
streAcEs ↑ UITY ↑ VCES TreedSSH P P Filter Name: \[Default Action: Block All ♥ Filter Name: Default Action: Block All ♥ P Default Action: Block All ♥ P Default Action: Block All ♥ P Default Action: Block All ♥ P P Potocol Mask: 255 255 255 255 NU P Caching P P Potocol IP Protocol IP Protocol IP Protocol (1) ♥ Action: Forward ♥ Add C Custom (0.255) UDP/TCP Port TCP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.255) UDP/TCP Port TCP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.65535) UDP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.65535) UDP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.65535) UDP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.65535) UDP Port: C Border Gateway Protocol (179) ♥ Action: Forward ♥ Add C Custom (0.65535)		Services: Filters - IP Filter	\$					
URING Create Call Filter Name: (NEW) Filter Name: Default Action: Block All Filter Name: Default Action: Block All P Address: 0.0.0 Mask: 0.0.0 Source Address: 0.0.0 Mask: 255 255 255 255 P Action: Forward Address: Add P Caching IP Protocol IP Protocol IP Protocol IP Protocol IP Protocol IP Protocol Custom 0.0-255) UDP/TCP Port TCP Port: Blorder Gateway Protocol (179) Action: Forward Add Custom 0.0-255) UDP/TCP Port TCP Port: Blorder Gateway Protocol (179) Action: Forward Add Custom 0.0-255) UDP/TCP Port TCP Port: Blorder Gateway Protocol (179) Action: Forward Add Custom 0.0-255) UDP Port: Blorder Gateway Protocol (179) Action: Forward Add Custom 0.0-255) UDP Port: Blorder Gateway Protocol (179) Action: Forward Add Custom 0.0-255) Filters Classes Filter Class	TERFACES +							
WCCS IP IP IP IP IP IP IP IP P	CURITY +	Create/Edit Fliter Name:	<new></new>					
InterSSH Filter Name: Default Action: Block All Filter Name: Block All Personal Address: Mask: 00.0.0 Source Address: 00.0.0 NN P P P P P P P P P P P P P P P P P	RVICES							
P Filter Name: B Default Action: B Default Action: B IP Address NMP Destination Address: MMP P ANN P ANN P Coshing P	elnet/SSH				-			
B Default Action: Block.All Pr P Source Address: 0.0.0.0 Mask: 255 255 255 255 Source Address: 0.0.0.0 Mask: 255 255 255 255 P Caching Eless services + LESS services + IP Protocol IP Protocol: © Authentication Header Protocol (51) UDP/TCP Port © Custom Custom (0.255) Filters Classes UDP Port: © Biff (mail notification, comsat 512) Custom (0.45535) Filters Classes Eless services + Default Action:	DP	Filter Name:						
ars IP Address Tr my Weight P Source Address: 0.0.0 Mask: 255 255 255 255 Action: Forward • Add P Costing P <td< td=""><td>NS</td><td>Default Actions</td><td>Plook All</td><td></td><td></td><td></td><td></td><td></td></td<>	NS	Default Actions	Plook All					
IP Address Destination Address: MP Source Address: 00.00 MAN P ANN P PCaching IP Protocol IP Protocol: IP Protocol: IP Protocol: IP Protocol: C Custorn (0-255) UDP/TCP Port TCP Port: C Border Gateway Protocol (179) C Custorn (0-65535) UDP Port: C Biff (mail notification, consat, 512) Action: Forward × Add C Custorn (0-65535) IDP Port: Biff (mail notification, consat, 512) Action: Forward × Add C Custorn (0-65535)	ters	Delauti Action.						
IP Address Source Address: Destination Address: NN P P Caching ELESS SERVICES + IP Protocol IP Custom (0.255) UDP/TCP Port Custom Custom (0.65535) UDP Port: Custom (0.65535) UDP Port: Custom (0.65535) Elters Classes Filters Classes Delete Class		ID Address						
Destination Address: Mask: 0.0.0 MP Source Address: 0.0.0 P Action: Forward < Address:		IP Address						
S Destination Address: MP P Source Address: 0.0.0 Mask: 255.255.255 Action: Forward < Add	oxy Mobile IP	Defenden Alle			0.0.0			
MP P NN P Caching LESS SERVCES + IP Protocol IP Protocol: © Authentication Header Protocol (51) • Action: Forward • Add © Custom © Delete Class	18	Destination Address:		Mask:	0.0.0			
P Statute Autilities: p0000 miss: p0000 Action: Forward Add P Protocol P Protocol IP Protocol: C Authentication Header Protocol (51) Action: Forward Add C Custorm (0-255) UDP/TCP Port: C Border Gateway Protocol (173) Action: Forward Add C Custorm (0-255) IUDP/TCP Port: C Border Gateway Protocol (173) Action: Forward Add C Custorm (0-65535) Filters Classes Eless	IMP	Source Address	0.0.0.0	Mack	255 255 255 255			
Action: Forward Add P Caching ELESS SERVICES + TEM SOFTWARE + TILOG + P Protocol IP Protocol: Custom 0.255) UDP/TCP Port TCP Port: Custom 0.255) UDP/TCP Port UDP Port: Custom 0.255) UDP Port: Custom 0.2553) Filters Classes Filters Classes Filters Classes Delete Class	P	Source Address.	0.0.0.0	Wash.	200.200.200.200			
P Caching ELESS SERVICES + IP Protocol IDP/TCP Port Custom	AN					Action:	Forward -	Add
P Caching ELESS SERVICES + TEM SOFTWARE + IP Protocol Custom (0-255) UDP/TCP Port CUstom (0-255) UDP/TCP Port CUstom (0-65535) UDP Port: © Bird(main notification, comset 512) UDP Port: © Custom (0-65535) Ellere Class	P							
IP Protocol IP Protocol IDDP/TCP Port IP Port IDP Port: IP I	P Caching							
LUDDO TIVARE IP Protocol: © Authentication Header Protocol (51) Custom (0-255) UDP/TCP Port Custom © Custom (0-65535) UDP Port: © Biff (mail notification, comsat, 512) Custom © Custom Filters Classes Eithers Classes Delete Class	ELESS SERVICES +	IP Protocol						
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 Filters Classes Delete Class	TEM SOFTWARE +							
UDP/TCP Port C Custom UDP/TCP Port C Custom (0-255) UDP Port: C Custom (0-65535) UDP Port: C Custom (0-65535) Filters Classes Custom Delete Class	NTLOG +	IP Protocol: Auth	entication Header Protoco	1 (51)	•	Action:	Forward -	Add
Custom (0-255) UDP/TCP Port CP Port CCustom (0-255) CCustom (0-65535) UDP Port: Custom (0-65535) Custom (0-65535) Filters Classes Filters Classes Delete Class								
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		C Custo	om 0-2	(55)				
UDP/TCP Port Border Gateway Protocol (179) Custom Cu			(,				
UDP/TCP Port © Border Gateway Protocol (173) Action: Forward Add Custom 0.65535) UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add Custom 0.65535)								
TCP Port: Border Gateway Protocol (173) Custom <li< td=""><td></td><td>UDP/TCP Port</td><td></td><td></td><td></td><td></td><td></td><td></td></li<>		UDP/TCP Port						
TCP Port: © Border Gateway Protocol (179) Custom (0-65535) UDP Port: Biff (mail notification, comsat 512) Custom Custom Filters Classes Eitlers Classes Delete Class								
Custom (0-65535) UDP Port: Biff (mail notification, comset, 512) Custom (0-65535) Filters Classes Delete Class		TCP Port: 💿 Border	Gateway Protocol (179)		•	Action:	Forward 💌	Add
Custom(0-65535) UDP Port: Biff (mail notification, comsat, 512) Custom(0-65535) Filters Classes Delete Class								
UDP Port: © Biff (mail notification, comsat 512) Action: Forward Add C Custom (0-65535) Filters Classes Delete Class		C Custom	(0-655	35)				
UDP Port: Biff (mail notification, comsat, 512) Custom Custom Custom Custom Delete Class 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 (ma	il notification, comsat, 512)		-	Action:	Forward 💌	Add
C Custom (0-65535)		-						
Filters Classes Delete Class		C Custom	(0-655)	35)				
Filters Classes Delete Class								
Filters Classes Delete Class								
Delete Class		Filters Classes						
Delete Class								
Delete Class								
Delete Class								
Delete Class								
Delete Class								
					Delete Class			
		2				-		
								-

Figure 15-6 IP Filters Page

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></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/bridge.
- 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/bridge accepts any IP address. If you enter 0.0.0.0, the access point/bridge 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/bridge.

- 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 A, "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/bridge.

- 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 A, "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/bridge, 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.

	APPLY FILTERS	AC ADDRESS	FILTERS	ETHERTYP	E FILTERS
HOME		-		-	
EXPRESS SET-UP	Hostname bridge			bridge upt	ime is 1 day, 23 hours, 30 minutes
EXPRESS SECURITY	·			• •	
NETWORK MAP +					
ASSOCIATION +	Services: Filters - Ap	ply Filters			
NETWORK INTERFACES +		Fa	stEthernet	Rac	lio0-802.11G
SECURITY +	In a surface				
SERVICES	incoming	MAC	< NONE > -	MAC	<pre>NONE > •</pre>
Telnet/SSH		Ether Torre		Eth a Toura	
CDP		⊏theriype	<pre>I < NUNE > ▼</pre>	Etheriype	KNUNE > •
DNS		IP		IP	
Filters				IF	
HTTP	Outgoing	MAC	< NONE > •	MAC	< NONE > -
Proxy Mobile IP					
QoS		EtherType	< NONE > -	EtherType	< NONE > -
SNMP					
NTP		Ч	< NONE > -	P P	<none> -</none>
VLAN					
STP					
ARP Caching					
WIRELESS SERVICES +					
SYSTEM SOFTWARE +					
EVENT LOG +					

Figure 15-7 Apply Filters Page

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/bridge'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/bridge. Figure 15-8 shows the Ethertype Filters page.

	APPLY FILTERS	E MAC ADDRESS		IP FILTERS		ETHERTYPE FILTERS	
HOME	-	88	-				
EXPRESS SET-UP	Hostname bridge					bridge uptime is 1 da	v, 1 hour, 2 minutes
EXPRESS SECURITY							,, ,
NETWORK MAP +							
ASSOCIATION +	Services: Filters - E	therType Filters					
VETWORK +							
NTERFACES	Create/Edit Filter I	ndex: <ne< td=""><td>W> •</td><td></td><td></td><td></td><td></td></ne<>	W> •				
BECURITY +		1					
SERVICES							
Telnet/SSH							
CDP	Filter Index:		(200-299)				
DNS							
Filters			_				
HTTP	Add EtherType:		Mask:	0000		Action: Forward 💌	Add
Proxy Mobile IP		(O-FFFF)	ſſ	D-FFFE)			
QoS		<u> </u>	v	,			
SNMP							
NTP	Default Action:	Block All					
VLAN							
CTD							
ADD Orobies	Filters Classes:						
ARP Caching							
AURELESS SERVICES +							
SYSTEM SUFTWARE +							
EVENTLUG +							
				Delete	Class		
	<u>J</u>				. 0.000		
						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 A, "Protocol Filters," for a list of protocols and their numeric designators.
Step 5	Enter the mask for the Ethertype in the Mask field.
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/bridge, 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.

APPLY FILTERS MAC ADDRESS FILTERS IP FILTERS ETHERTYPE FILTERS HOME EXPRESS SET-UP bridge uptime is 1 day, 23 hours, 30 minutes Hostname bridge EXPRESS SECURITY NETWORK MAP ASSOCIATION NETWORK INTERFACES FastEthernet Radio0-802.11G SECURITY Incoming MAC (NONE) MAC <NONE> SERVICES Telnet/SSH EtherType <NONE> EtherType <NONE > -CDP DNS IP <NONE> IP <NONE> Filters HTTP Outgoing <NONE> -MAC (NONE) MAC Proxy Mobile IP < NONE > -< NONE > -QoS EtherType EtherType SNMP IP <NONE> IP (NONE) NTP VLAN STP 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.

117023