Lab 8.3.2 Configure Filters on AP

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two.

Objective

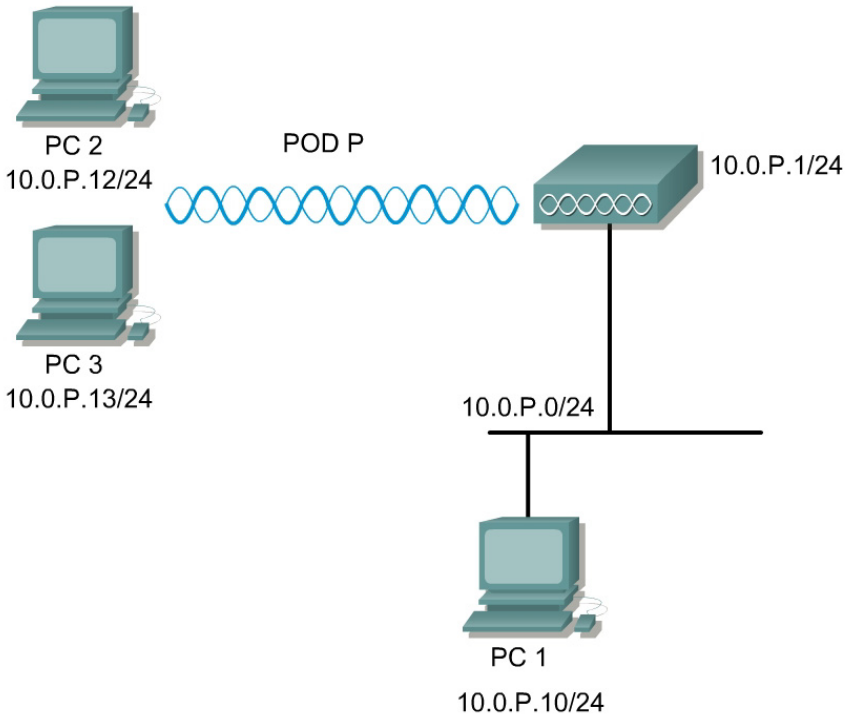
In this lab, the student will learn how to set and enable a protocol filter on the AP and how to set and enable MAC address filters on the AP.

Scenario

Protocol filters prevent or allow the use of specific protocols through the AP. Individual protocol filters or sets of filters can be set up for either the Radio or Ethernet ports. Protocols can be filtered for wireless client devices, users on the wired LAN, or both.

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. A filter can be created that passes traffic to all MAC addresses except those that are specified. A filter can also be created that blocks traffic to all MAC addresses except those that are specified.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

The APs and PC client adapter and utility should be installed and properly configured prior to the lab. The students will also familiarize themselves with the various EtherType, IP, and port filters available on the AP.

Tools and Resources

Each team of students will require the following:

- Cisco Aironet AP
- 1 wired PC or laptop
- 2 wireless PCs with ACU

Step 1 Creating a MAC address filter

Make sure the Topology is cabled and configured according to the Topology.

a. Verify the SSID is configured

b. Verify both PC2 and PC3 are associated and TCP/IP is configured

c. Verify both PC2 and PC3 can ping the AP at 10.0.P.1

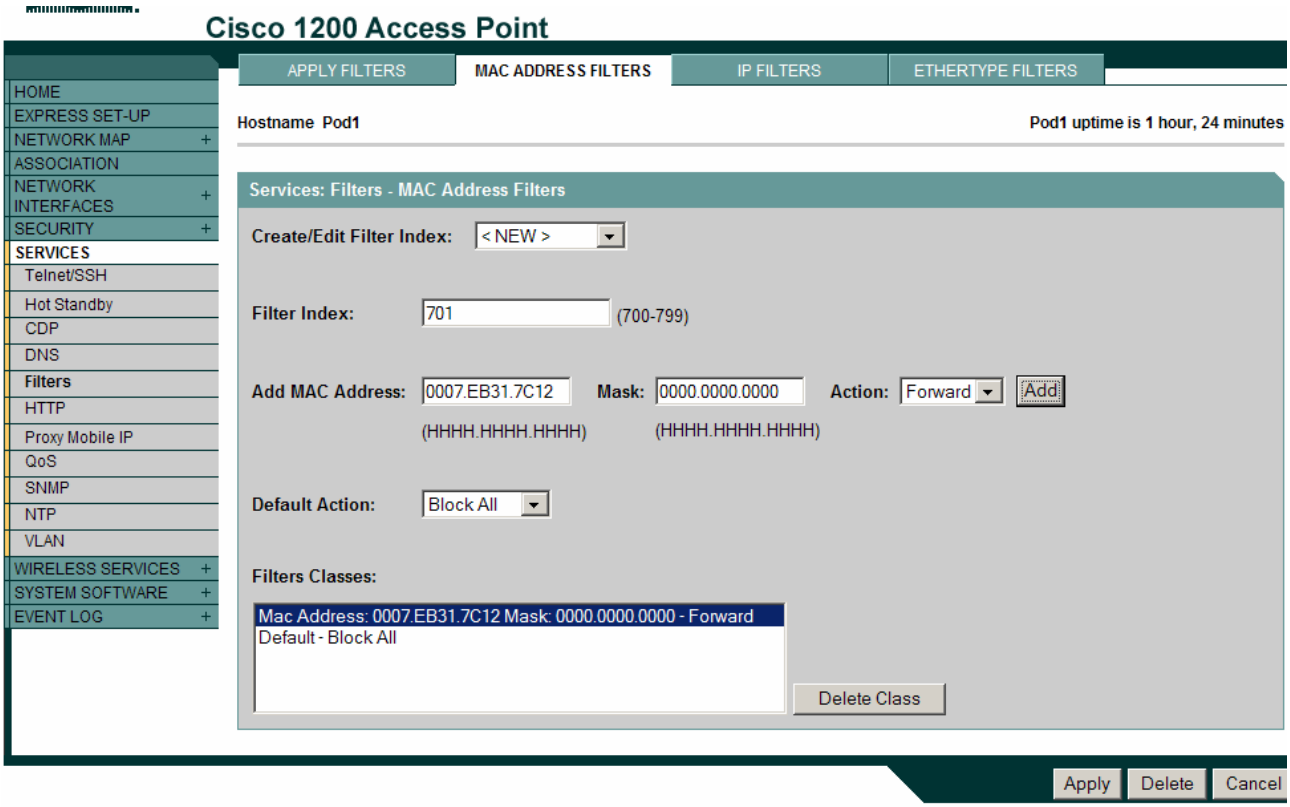
Step 2 Creating a MAC address filter

Follow the path below to reach the Address Filters page:

a. Click **SERVICES** in the page navigation bar.

b. In the Services page list, click **Filters**.

c. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.



d. Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu.

e. In the Filter Index field, name the filter with a number from 701.

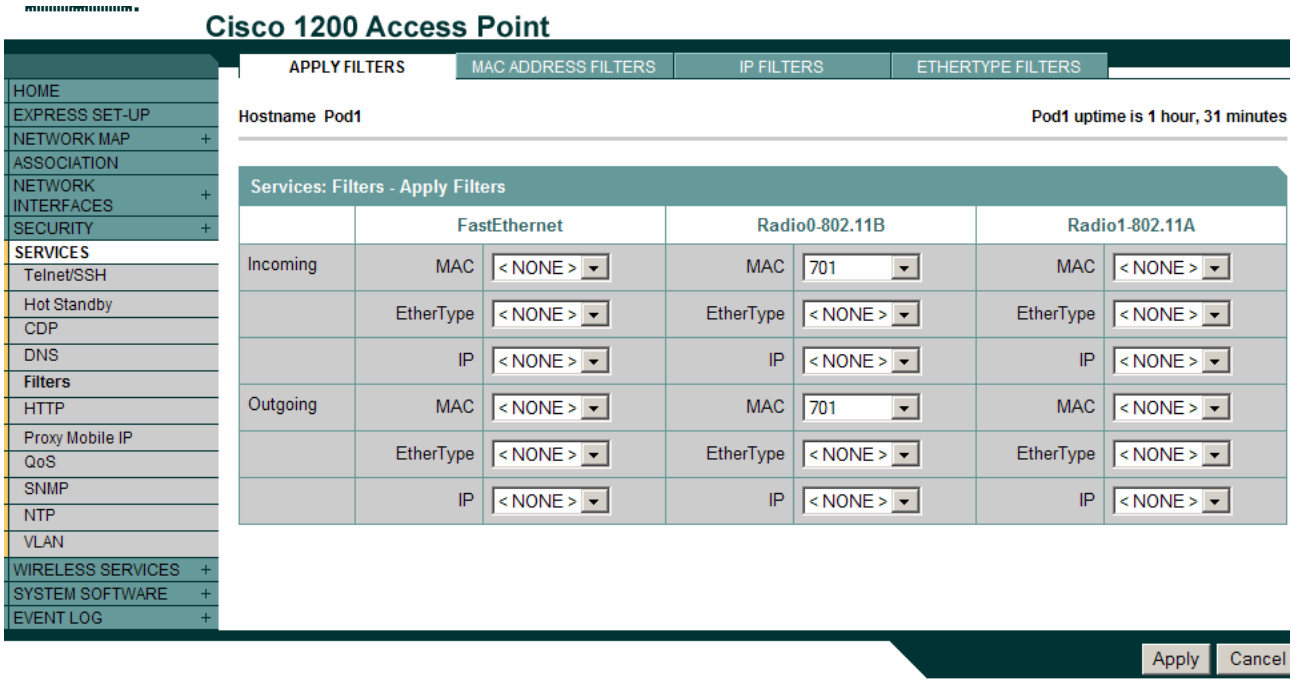
f. Enter a MAC address wireless PC2 in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0007.50CA.E208, for example).

g. Select **Forward** from the Action menu.

h. Click **Add**. The MAC address appears in the Filters Classes field.

i. Click **Apply**. The filter is saved on the AP, but it is not enabled until it is applied on the Apply Filters page.

Step 3 Apply the MAC address filter



a. From the **SERVICES>Filters** Page, go to the APPLY FILTERS tab.

b. Select the filter number 701 from the Radio0-802.11B MAC drop-down menus. Apply the filter to incoming and outgoing packets.

c. Click **Apply**. The filter is enabled on the selected ports.

Note Client devices with blocked MAC addresses cannot send or receive data through the AP, 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 AP stops monitoring them, when the AP reboots, or when the clients associate with another AP.

Step 4 Test the MAC address filter

When applying any security, it is important to test the configuration

a. From PC 3, located at 10.0.P.13, ping the AP at 10.0.P.1.

b. Was this successful? Should it be successful?

_____

_____

c. From PC 2, located at 10.0.P.12, ping the AP at 10.0.P.1

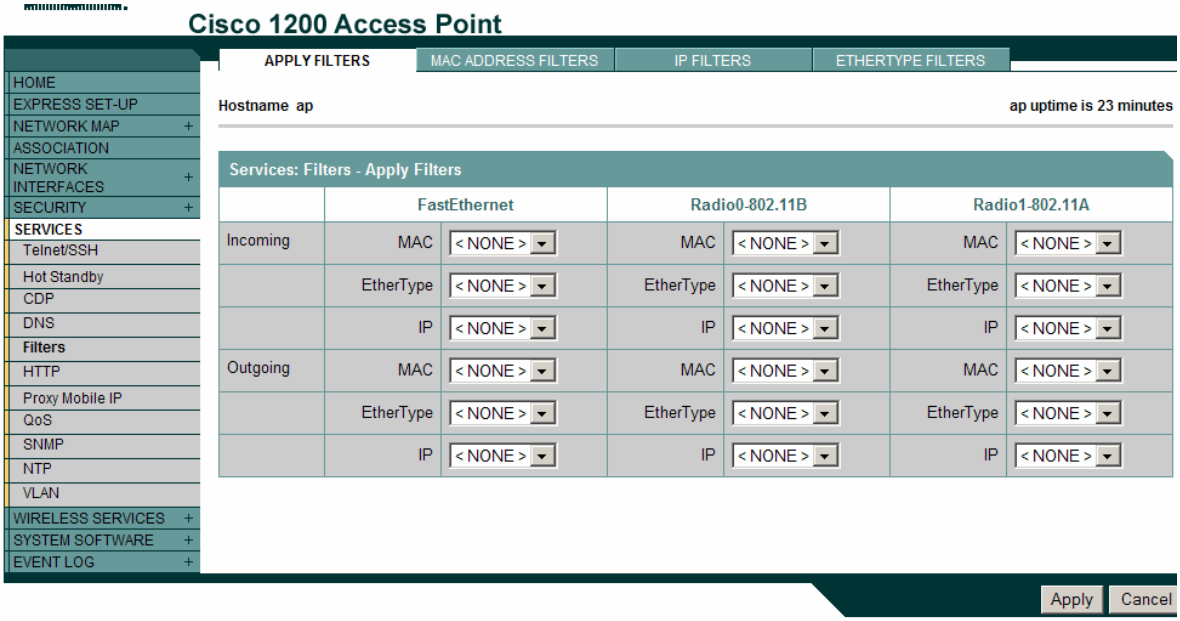
d. Was this successful? Should it be successful?

_____

_____

Step 5 Remove the MAC address filter

Before configuring any IP Filters, delete the existing MAC filter.



a. From the **SERVICES>Filters Page** change the 701 to <NONE> on both Incoming and Outgoing.

b. Click **Apply**.

c. From PC 2 and PC 3, ping the AP at 10.0.P.1.

d. Was this successful? Should it be successful?

_____

_____

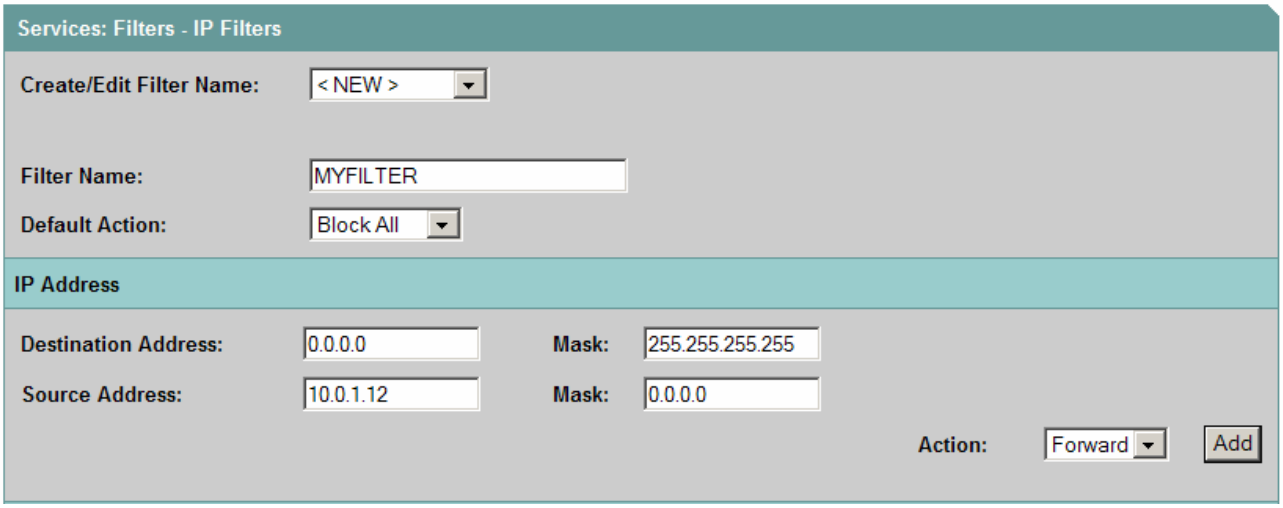
Step 6 Creating an IP filter

Follow this link path to reach the IP Filters page:

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

b. In the Services page list, click **Filters**.

c. On the **Apply Filters** page, click the **IP Filters** tab at the top of the page.



d. Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu, and then click the **Add** button.

e. Enter a descriptive name of **MYFILTER** for the new filter in the Filter Name field.

f. Select **Block all** as the filter's default action from the Default Action menu.

g. Configure the **Destination Address:** of 0.0.0.0 and a **Mask:** of 255.255.255.255.

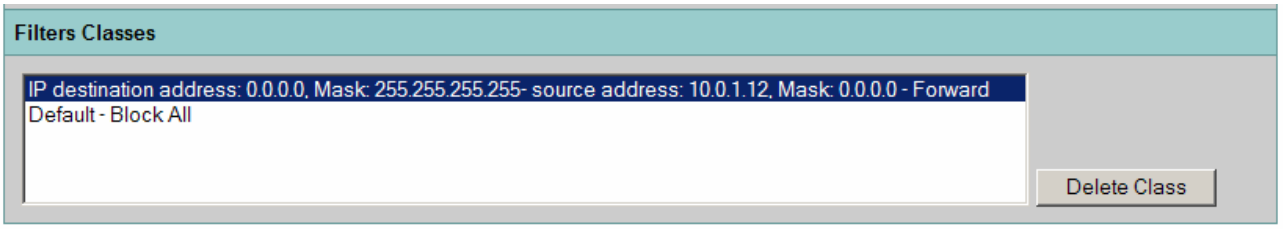
h. Add 10.0.P.12 as the **Source Address:** with a **Mask:** of 0.0.0.0 to permit PC2 traffic.

i. Make sure Forward is selected for the **Action:**

j. Click the **Add** button. The ACL will now appear in the Filters Classes Box at the bottom of the **Filters** page.

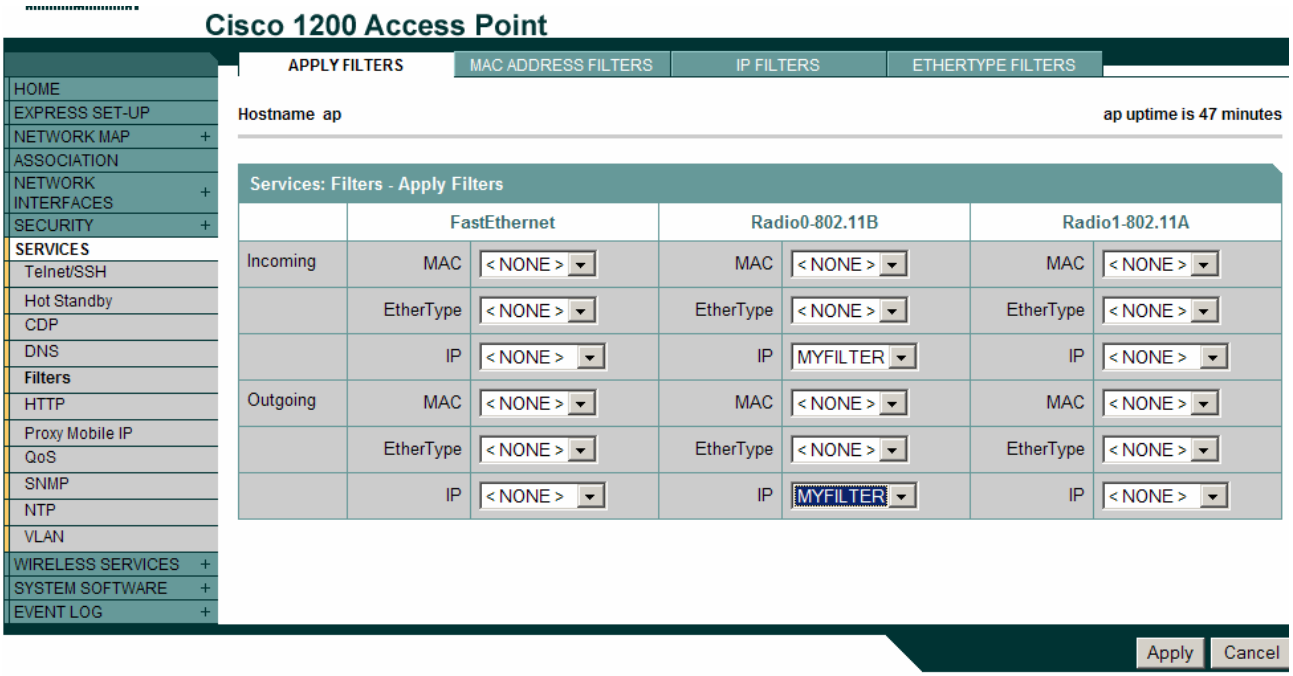
k. Verify the configuration in the Filters Classes box.

.



l. If the configuration is correct, click **Apply**.

Step 7 Apply the IP filter



a. Select **MYFILTER** from the radio ports incoming and outgoing IP fields.

b. Click **Apply**. The filter is now enabled on the selected interface(s).

Step 8 Test the IP filter

When applying any security, it is important to test the configuration

a. From PC 3, located at 10.0.P.13, ping the AP at 10.0.P.1.

b. Was this successful? Should it be successful?

_____

c. From PC 2, located at 10.0.P.12, ping the AP at 10.0.P.1.

d. Was this successful? Should it be successful?

_____

e. List three of the EtherType filters that can be used.

_____

_____

_____

f. List three of the IP filters that can be used.

_____

_____

_____

g. List three of the port filters that can be used.

_____

_____

_____