How To Block IPX Traffic Using an Ethertype Filter on Access Point

Document ID: 23306

Introduction

This document explains how to use Ethertype filters to block Internetwork Packet Exchange (IPX) traffic on the Cisco Aironet Access Point. A typical situation in which this is useful is when IPX server broadcasts choke the wireless link, as sometimes happens on a large enterprise network.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document applies to Cisco Aironet Access Points that run either VxWorks or Cisco IOS® Software.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you work in a live network, ensure that you understand the potential impact of any command before you use it.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Connect to the Access Point

You can open the management system of the Access Point through your web browser or through the Access Point serial port with a terminal emulator. If you are unfamiliar with how to connect to an Access Point, refer to Using the Web Browser Interface for directions on how to connect to an Access Point that runs VxWorks, or Using the Web−Browser Interface to connect to an Access Point that runs Cisco IOS Software.

Configuration

Access Points that Run VxWorks

Once you have established a browser connection to the Access Point, perform these steps to configure and apply a filter to block IPX traffic.

Create a Filter

Complete these steps:

1. Under the Setup menu, choose **Ethertype Filters** .
2. In the Set Name field, type a filter name (for example, "BlockIPX") and click **Add New**.
3. On the next page, you see the Default Disposition. The two options are *forward* and *block*. Choose **forward** from the drop−down menu.
4. In the Special Cases field, enter **0x8137** and click **Add New**.
5. A new window is displayed with these options:

   - Disposition
   - Priority
   - Unicast Time−to−Live
   - Multicast Time−to−Live
   - Alert

   For the Disposition, choose **Block**. Leave the other options at their default settings. Click **OK**.

   You are returned to the Ethertype Filter Set screen. Repeat Step 4 and Step 5, and add types **0x8138**, **0x00ff**, and **0x00e0**.

Apply the Filter

Once the filter is created, it must be applied to the interface in order to take effect.

1. Return to the Setup page. Under the Network Ports section on the row marked Ethernet, click **Filters**.
2. You see EtherType with Receive and Forward settings. From each drop−down menu, choose the filter you created in Step 2 of the Create a Filter procedure and click **OK**. This step activates the filter you have created.

Access Points that Run Cisco IOS Software

Create a Filter

Complete these steps:

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.
4. Make sure **NEW** (the default) is selected in the Create/Edit Filter Index menu. If you wish to edit an existing filter, select the filter number from the Create/Edit Filter Index menu.
5. 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.
6. Enter **0x8137** in the Add Ethertype field.

7. Leave the mask for the Ethertype in the Mask field at the default value.
8. Choose **Block** from the Action menu.
9. Click **Add**. The Ethertype appears in the Filters Classes field.
10. In order to remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat Step 6 through Step 9, and add types **0x8138**, **0x00ff**, and **0x00e0** to the filter.
11. Choose **Forward All** from the Default Action menu. Because you block all IPX packets with this filter, you must have a default action that applies to all other packets.
12. Click **Apply**.

Apply the Filter

The filter has, at this point, been saved on the Access Point, but it is not enabled until you apply it on the Apply Filters page.

1. Click the **Apply Filters** tab to return to the Apply Filters page.
2. 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.
3. Click **Apply**. The filter is enabled on the selected ports.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Wireless LAN Product Support**
- **Wireless LAN Technology Support**
- **Wireless LAN Software**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 16, 2007 Document ID: 23306