Configuring Your Devices

As a system administrator, you want to use CiscoView to configure your Catalyst 4000 device as well as add IP addresses to allow other management workstations to access the same device. At the same time, you want to limit access to that particular device for other management workstations.

What You Need

Verify these prerequisites *before* starting the procedure for this scenario:

- Read and write community strings are valid.
- Permissions for IP Addresses are enabled.

How To Do It—Procedures

Use the procedures in this section to:

1. Access the Device Configuration Dialog Box.
2. Add IP Addresses for Other Management Workstations.
3. Limit Device Access.

Access the Device Configuration Dialog Box

Access the Device Configuration dialog box to configure your device:

Step 1 Select **Device Manager > CiscoView** from the CiscoWorks navigation tree.

Step 2 Select the device by entering the appropriate device's IP address.

Step 3 Double-click the device chassis area to display the Device Configuration dialog box.

Step 4 From the Device Configuration dialog box, configure your Catalyst 4000 device by entering the required information for that device.

Step 5 Click **OK**.

Add IP Addresses for Other Management Workstations

After you configure your device, add new IP addresses to allow other management workstations to access the same device:

Step 1 From the Device Configuration dialog box, select **IP permit** from the Category list to display the IP Permit window.

Step 2 In the IP Permit window, create an IP address to be included within the IP address list. This list determines which management workstation is permitted or restricted from accessing this particular device.

Note IP addresses allow management workstations to access specific devices for configuration. You can add as many IP addresses to the IP address list as necessary.

Step 3 Click **Create**. The Row Creation dialog box appears.

Step 4 Enter the IP address and the IP mask and click **OK**. The new IP address is added to the IP address list.

Limit Device Access

Limit access privileges for other management workstations and monitor unauthorized attempts to access the device:

Step 1 From the IP Permit window, highlight the IP address to be deleted from the IP address list and click **Delete**. This disables that particular management workstation from accessing the device.

Step 2 To monitor unauthorized attempts to access the device, re-open the IP Permit window to view any access to the device.

Where You Should End Up—Verification

After you configure your device and limit access to the device by other management workstations, verify that there are no unauthorized workstations accessing the device:

Step 1 Go to the bottom of the window to view the Access Attempts from Invalid IP addresses box. This dialog box provides information about which management workstation recently attempted to access the device, the time and date of attempted access, and list of the invalid IP addresses that were deleted from the list.

Step 2 If a deleted IP address is still attempting to access the device, notify the owner of that particular management workstation regarding any recent changes made to the owner's security level.