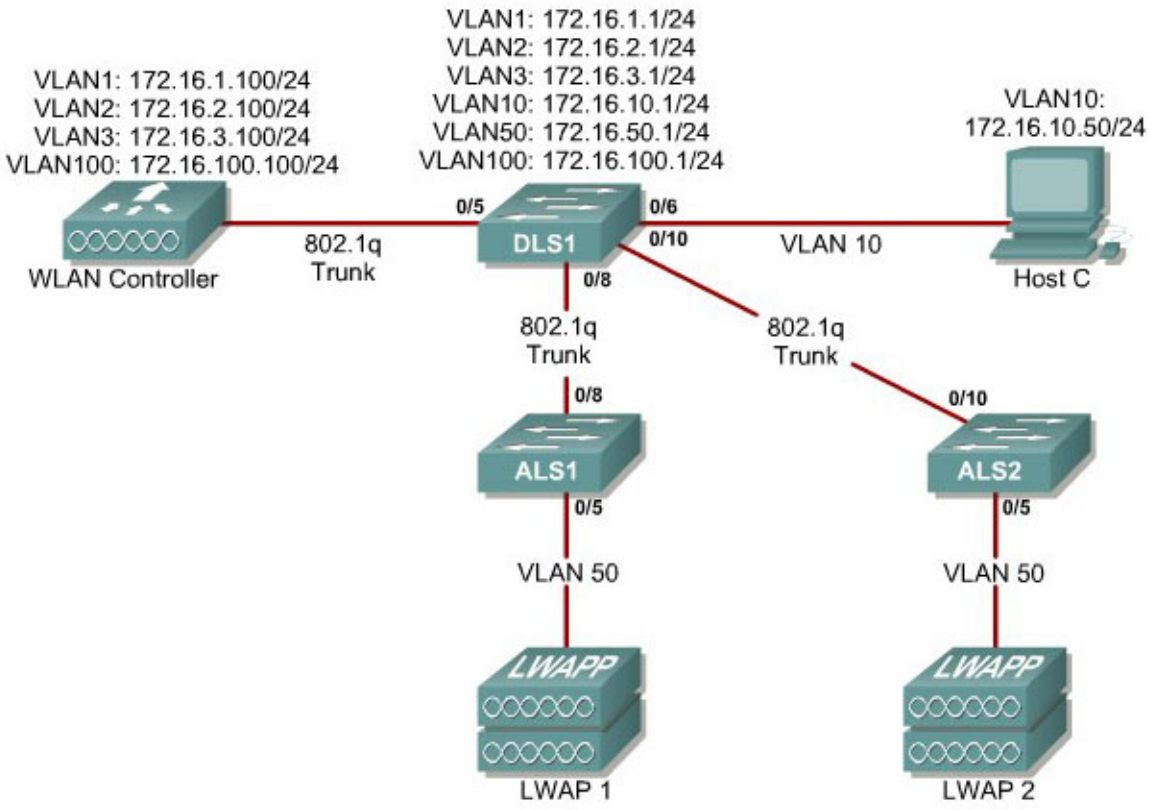
Lab 6-2 Configuring a WLAN Controller via the Web Interface

Topology Diagram



Scenario

Continuing from the previous lab, you will now set up the WLAN controller through its web interface. Previously you configured it through the CLI.

Step 1

Set up all the switches as they were in the previous lab. Make sure that the WLAN controller and host also have the same configuration as before.

Step 2

On the host, open up Internet Explorer and go to the URL “https://172.16.1.100”. This is the secure method of connecting to the management interface of the WLAN controller. You can also use

"http://172.16.1.100" since we previously enabled regular insecure HTTP access in the CLI for Lab 6.1. If you connect to the secure address, you may be prompted with a security warning. Click **Yes** to accept it and you will be presented with the login screen for the WLAN controller. Click **Login** and an authentication dialog box will appear.

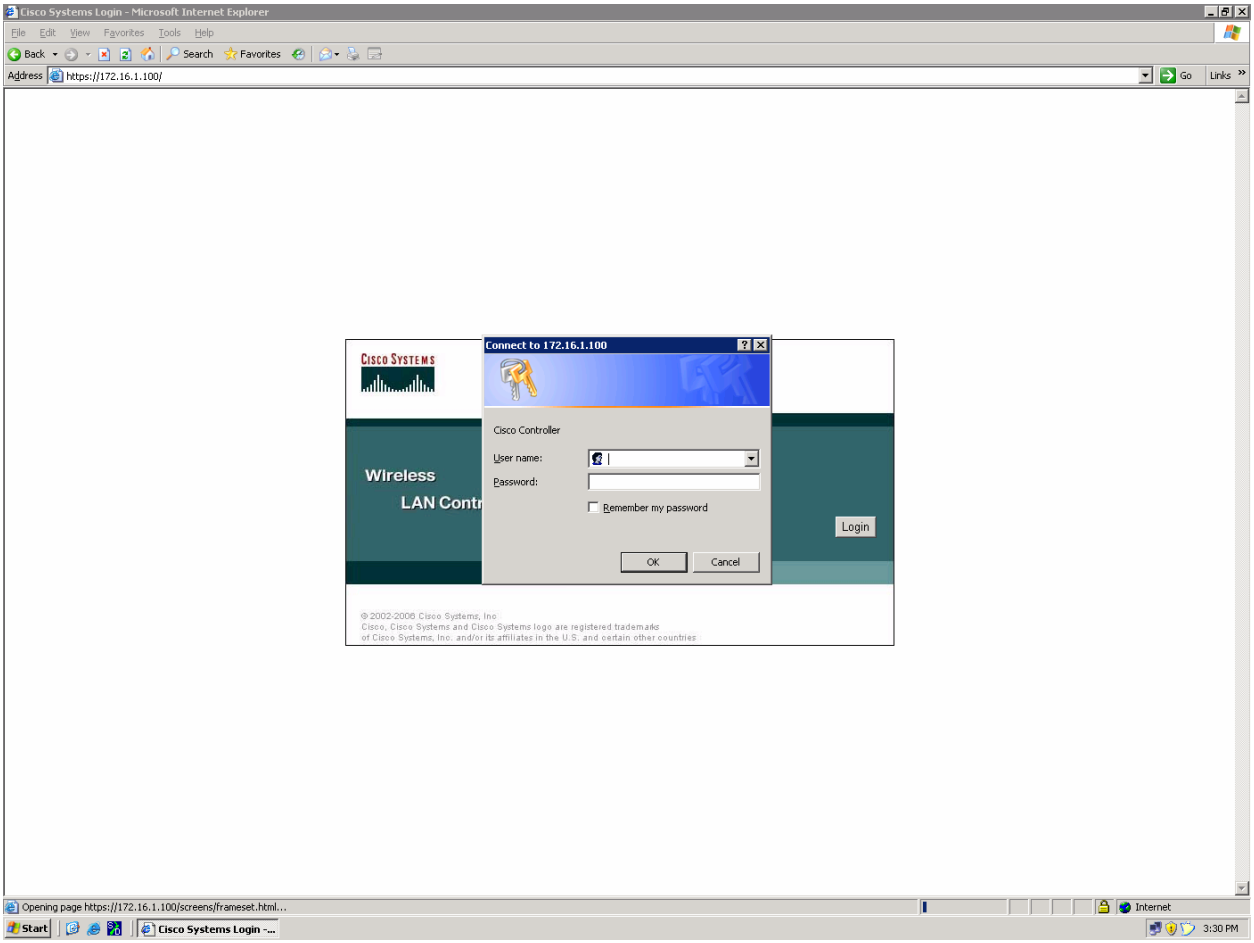


Figure 2-1: Authentication Dialog Box for WLAN Controller Web Access

Use "cisco" as both the username and password. You configured these in the previous lab. Click **OK** to get to the main page of the graphical user interface (GUI). You are then presented with the monitor page for the WLAN controller.

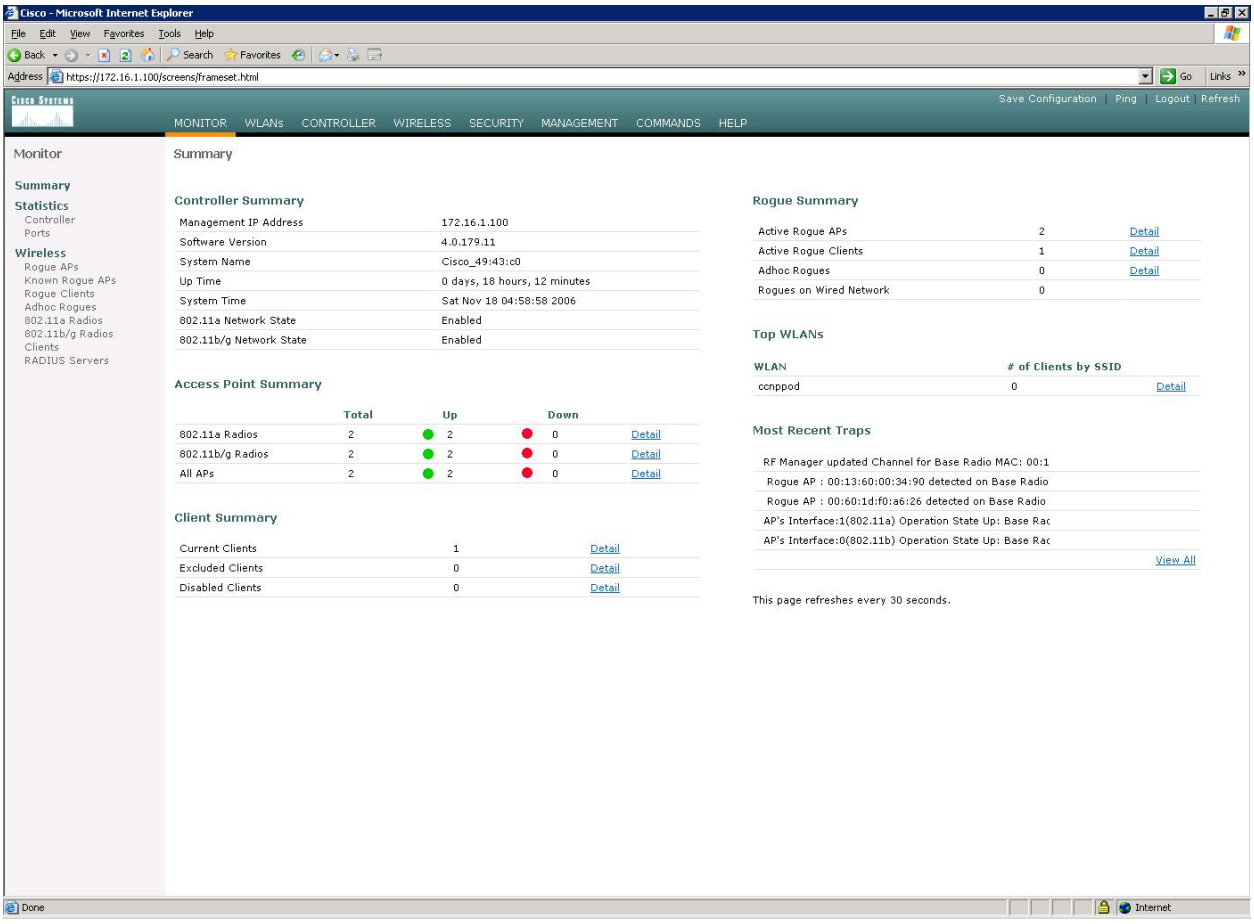


Figure 2-2: WLAN Controller Monitor Page

Make sure you see 2 access points under the “Access Point Summary” part of the page. You may also see it detecting rogue access points if your lab has other wireless networks around it; this behavior is normal. You can also see various port controller and port statistics by clicking their respective links on the left-hand menu on the screen.

Step 3

The next task in configuring WLANs is to add in the logical interfaces on the WLAN controller corresponding to VLANs 2 and 3. To do this, click the **Controller** link on the top of the web interface. Then, click **Interfaces** link on the left side bar.

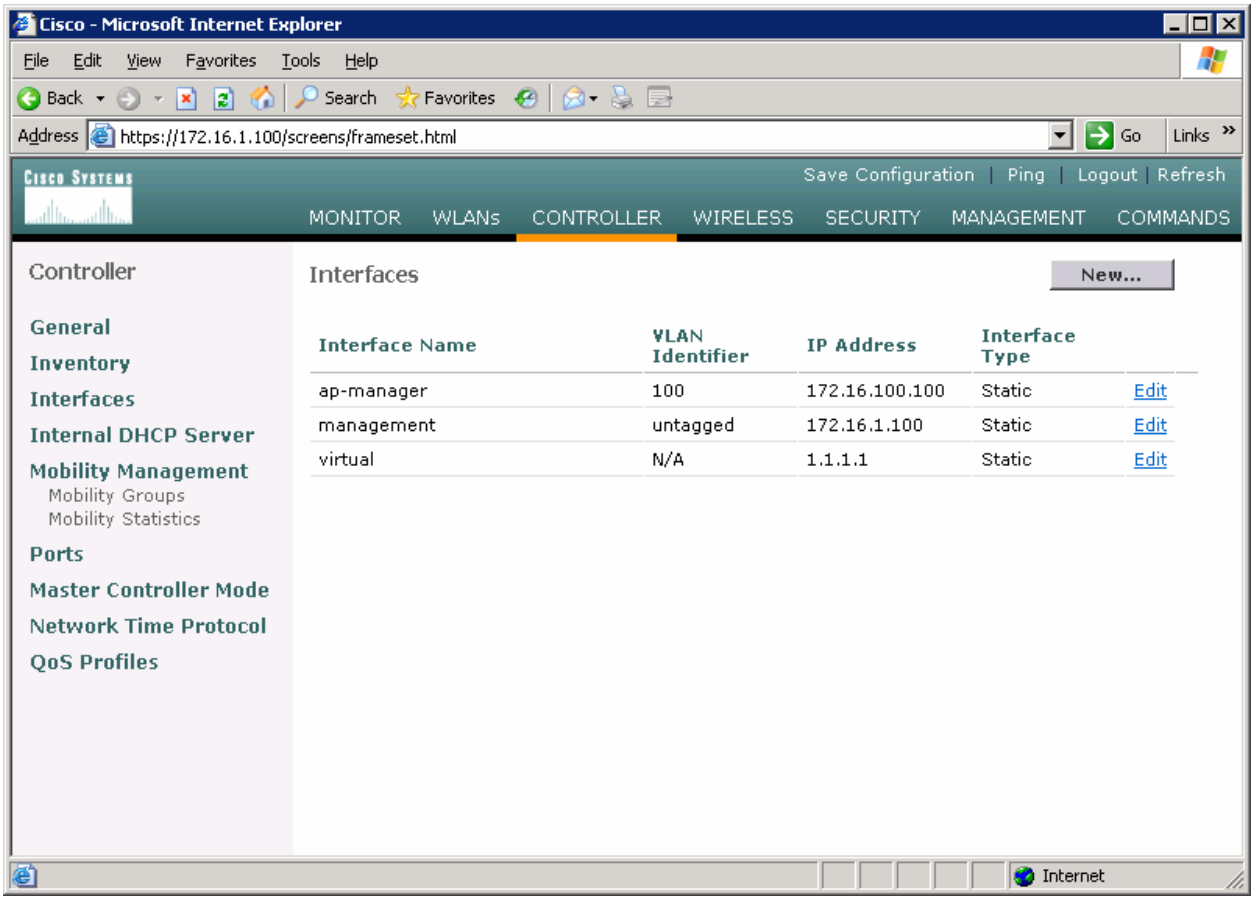


Figure 3-1: Interface Configuration Page

Click the **New...** link to create a new interface. Give the new interface a name of VLAN2 and VLAN number 2. Click **Apply** to submit the parameters.

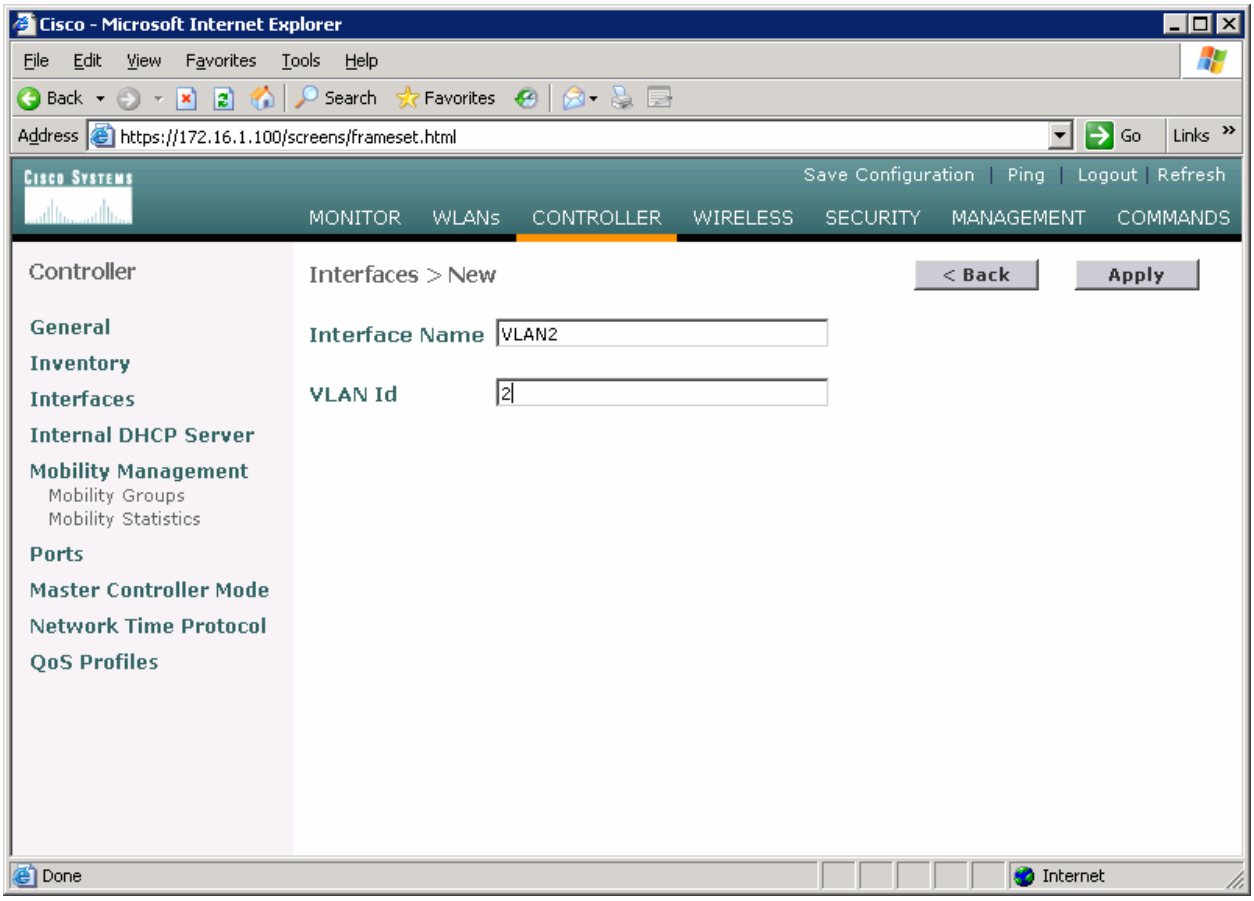


Figure 3-2: Creating a New VLAN Interface

On the next page, configure the IP address shown in the diagram. Also configure this on physical port 1, since that is the port trunked to the switch. After you have entered in all the changes, click **Apply**. Click **OK** to the warning box that comes up. This warning says that there may be a temporary connectivity loss on the APs while changes are applied.

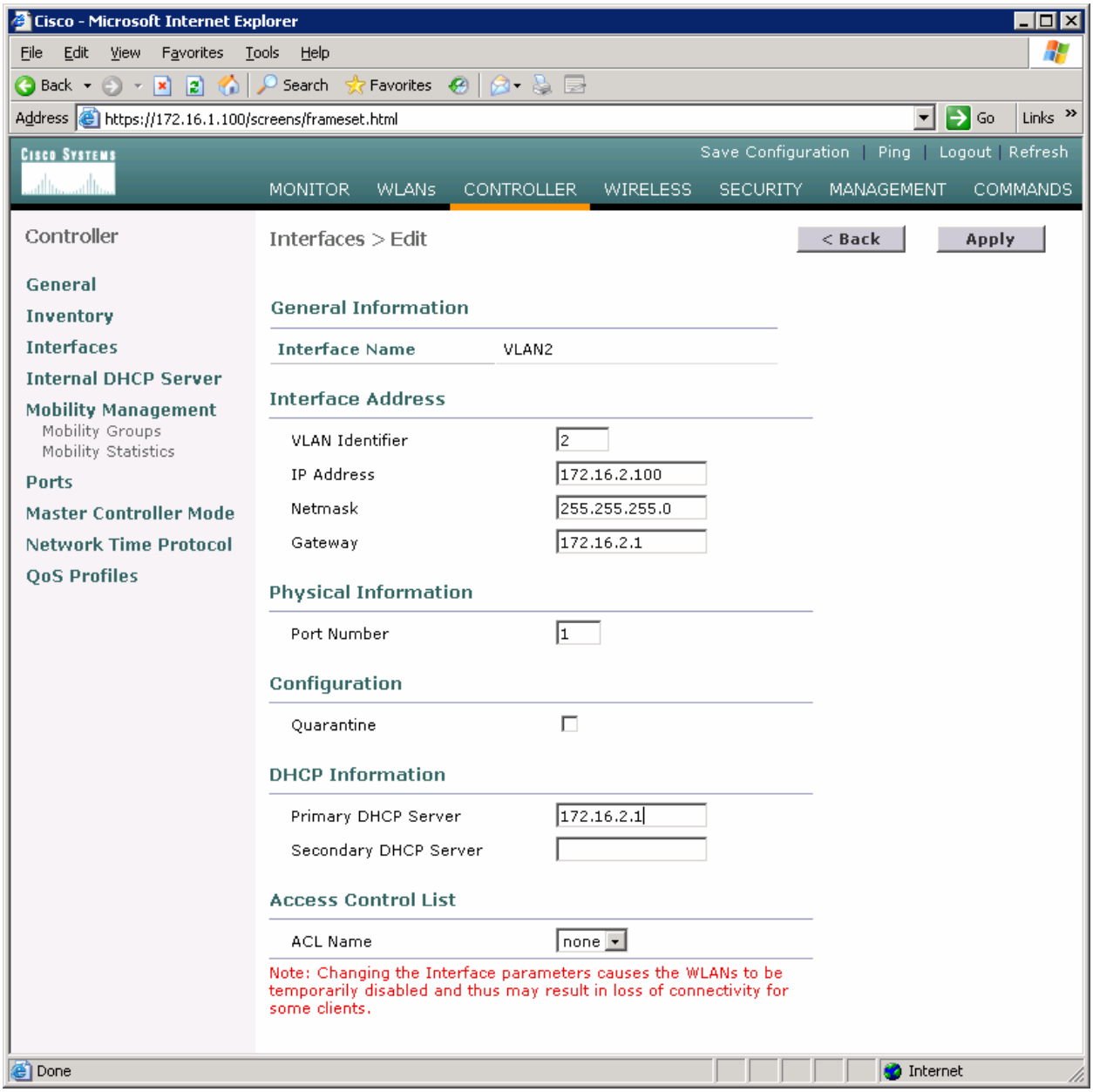


Figure 3-3: Configuring VLAN Interface Properties

The new interface should appear in the interfaces list. Do the same configuration steps for VLAN 3.

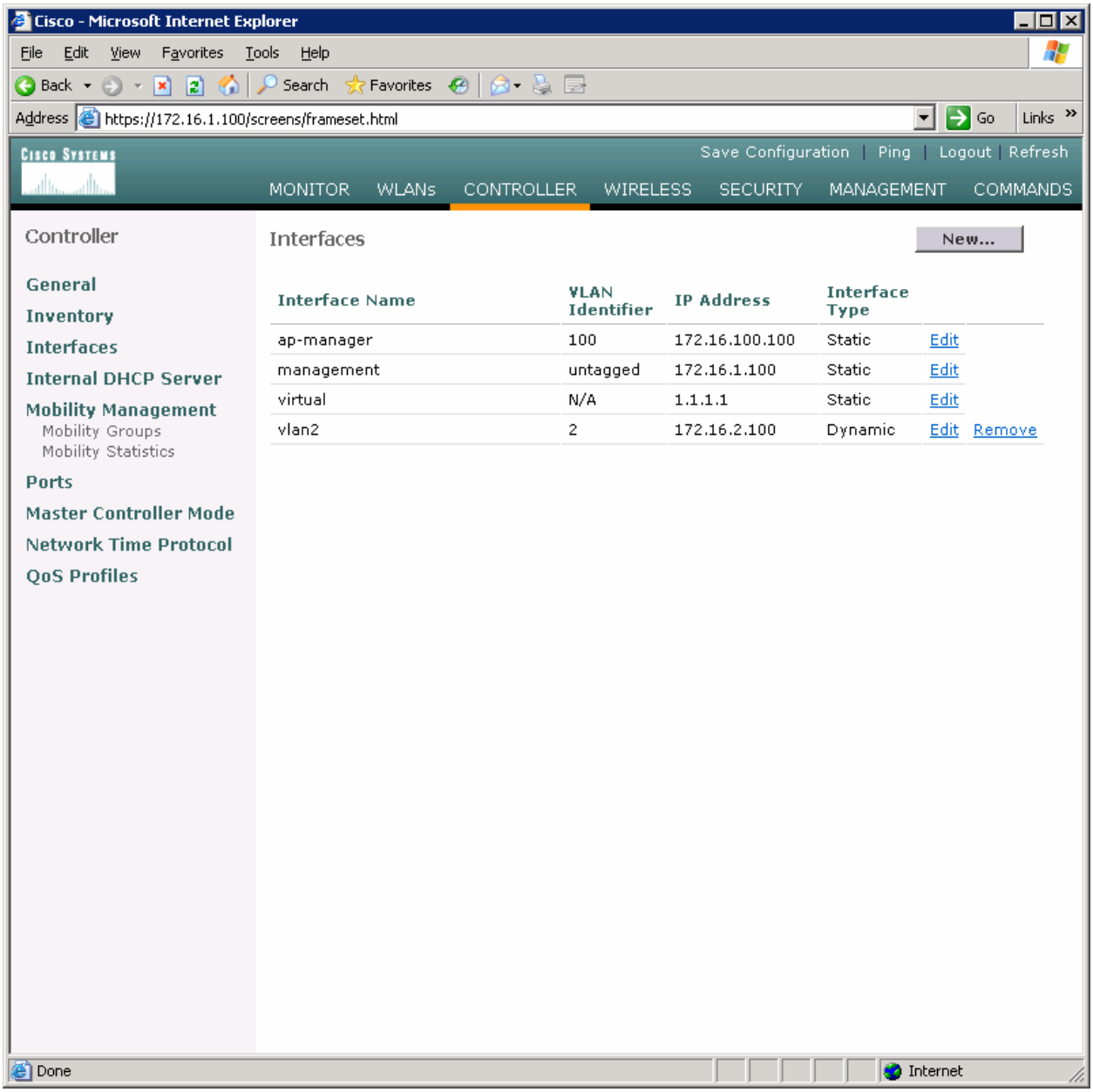


Figure 3-4: Verify Existing VLAN Interfaces

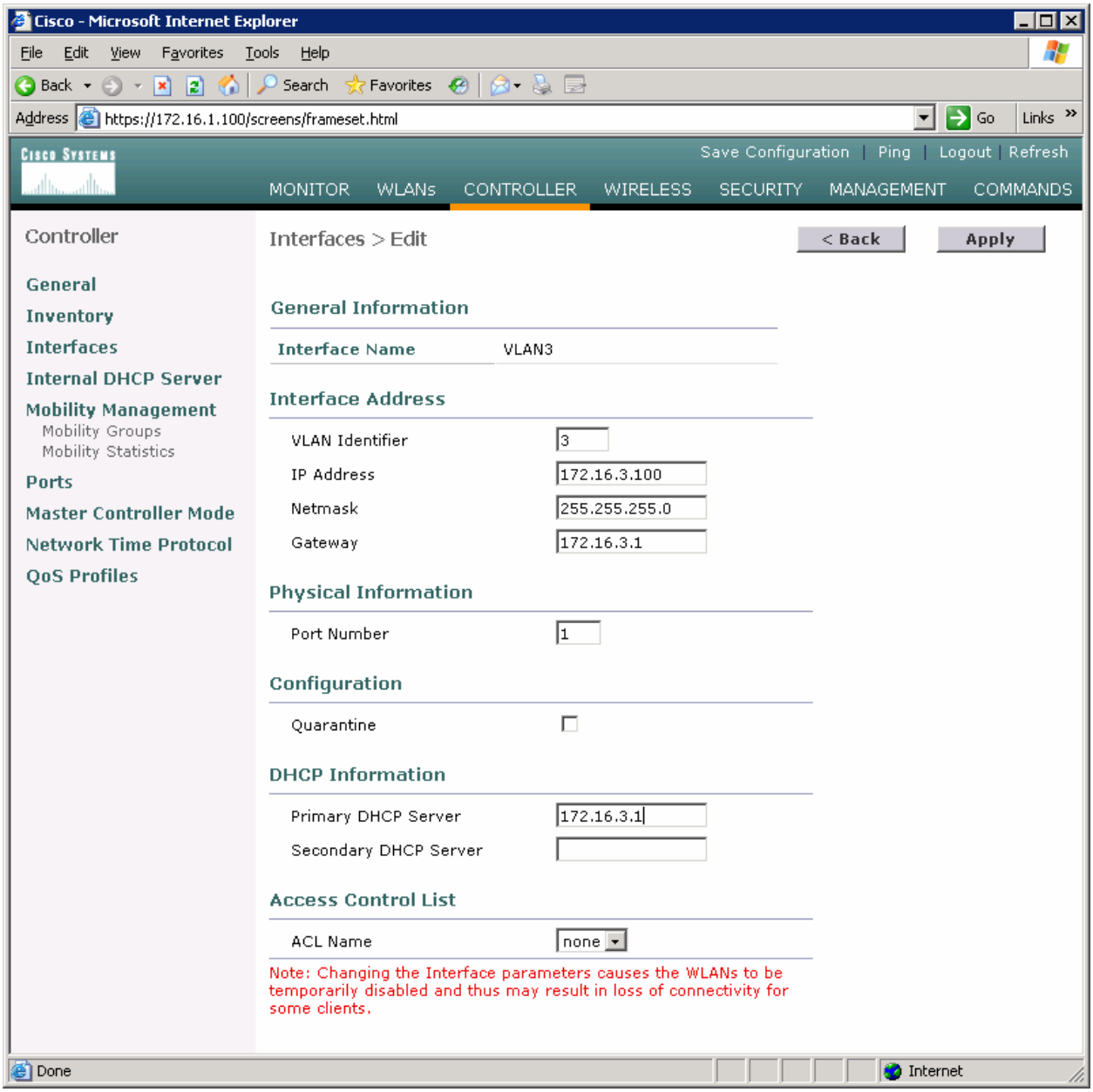


Figure 3-5: Configuring the VLAN 3 Interface

Make sure both interfaces appear in the interface table.

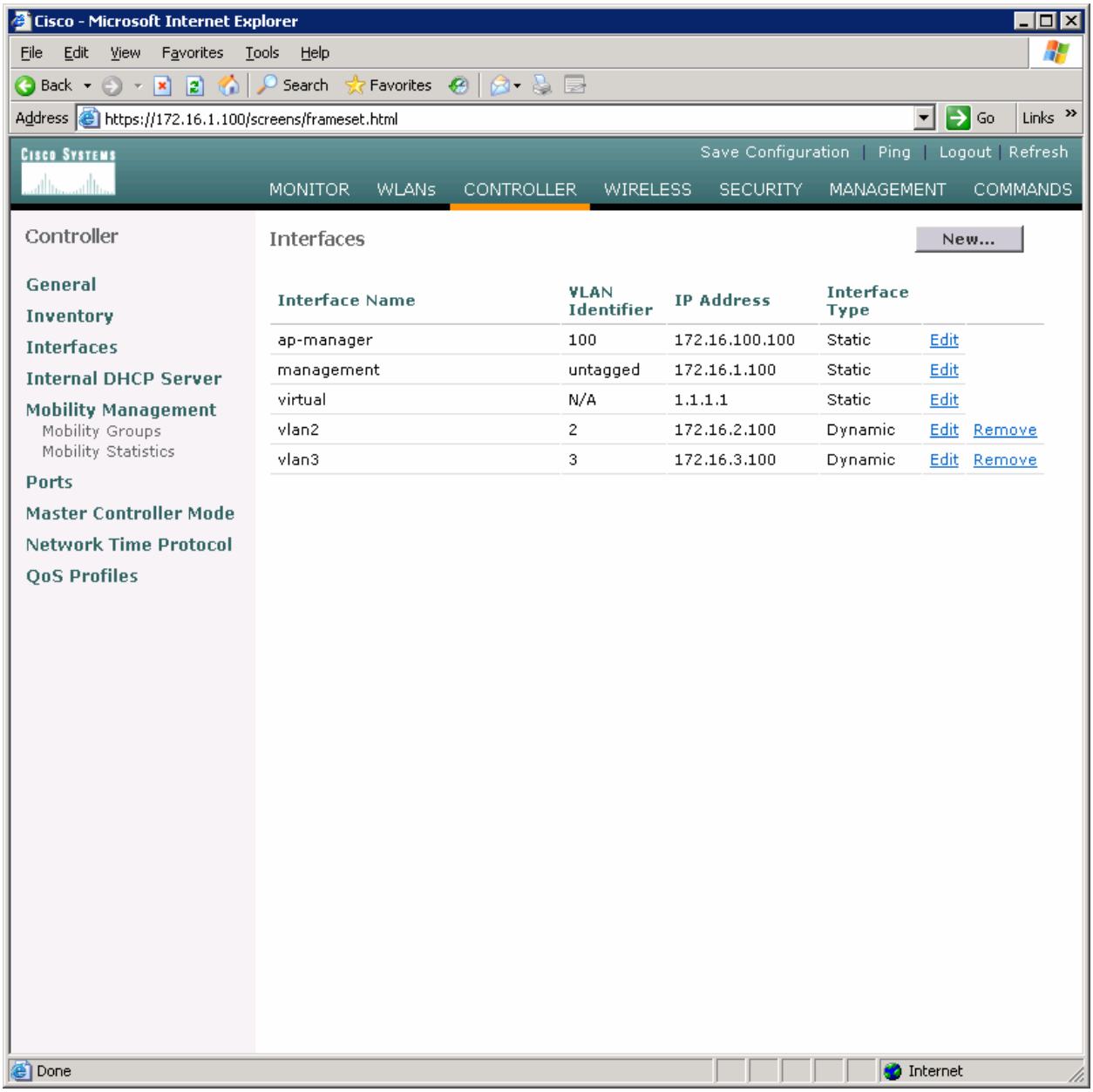


Figure 3-6: Verifying VLAN Interfaces on the WLAN Controller

Step 4

Now, you can configure the WLANs corresponding to these VLANs. To do this, first click the **WLANs** link at the top of the page. This will show you all configured WLANs.

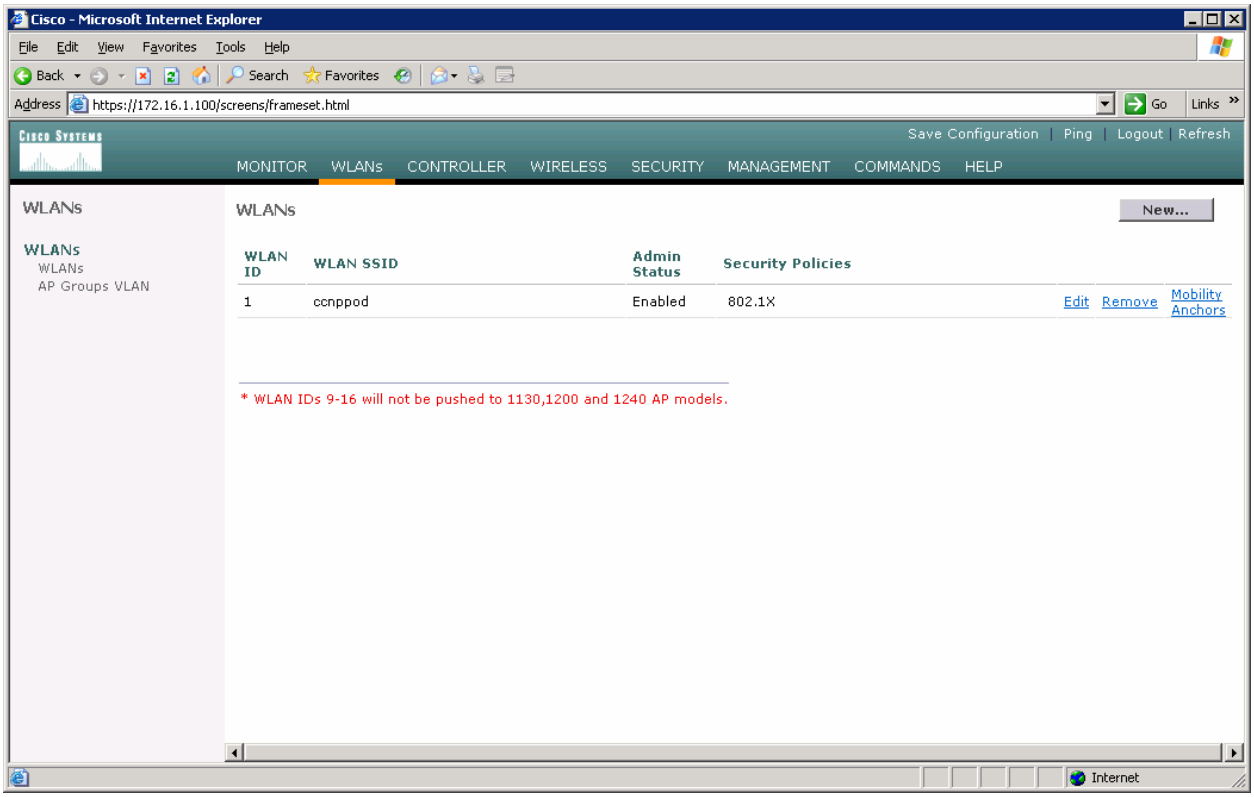


Figure 4-1: Viewing Existing WLANs

On the existing one, click **Edit** on the right of it. Remove the layer 2 security and change the interface to VLAN2. This will associate this WLAN with the correct VLAN.

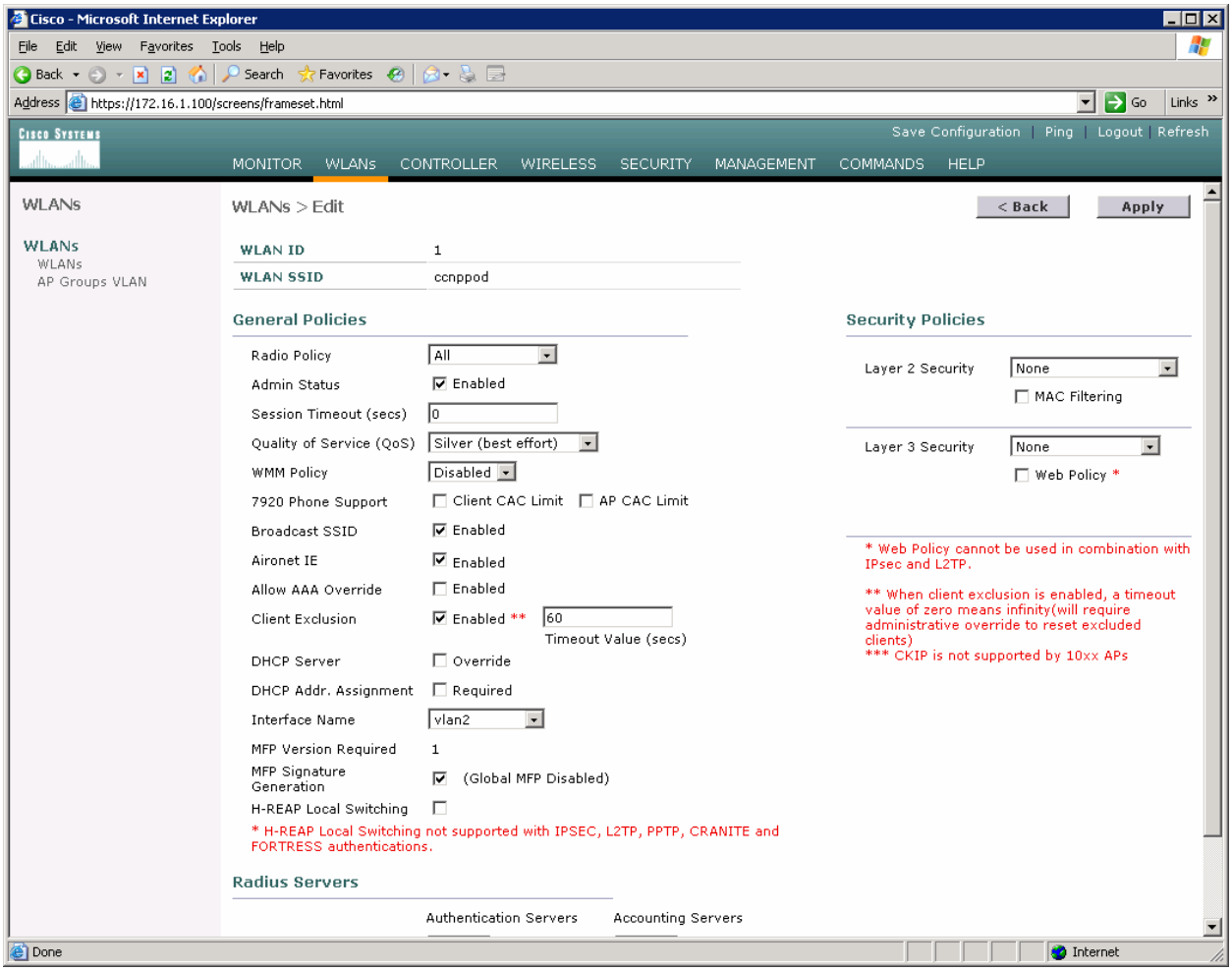


Figure 4-2: Edit the Configuration for WLAN 1

Click **Apply** and click **OK** to the warning box that comes up.

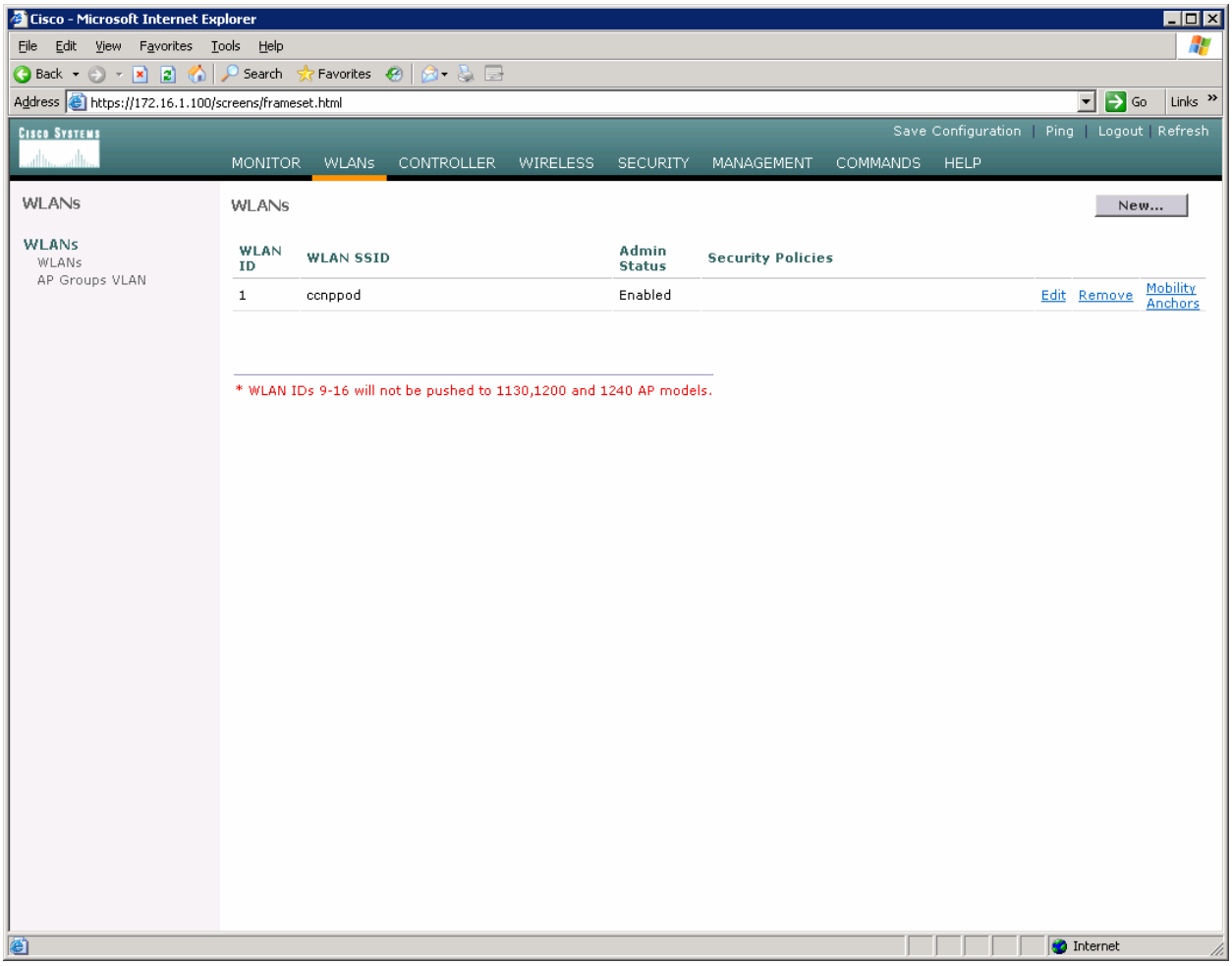


Figure 4-3: WLAN 1 without a Security Policy

Click **New...** and configure a WLAN for VLAN 3. Use the SSID “ccnplab”.

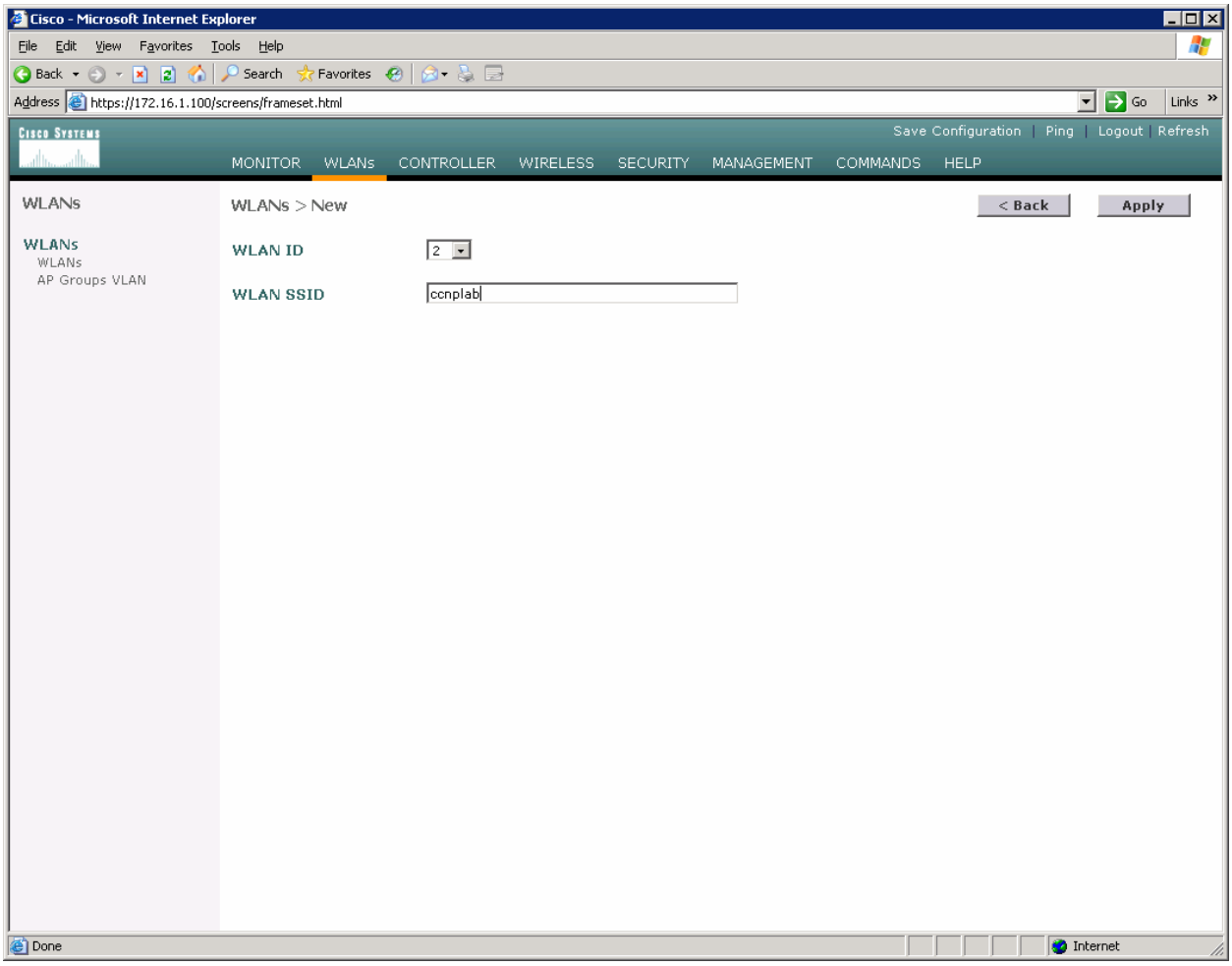


Figure 4-4: Adding a New SSID for WLAN 2

On this WLAN, configure the layer 2 security as Static WEP and use a 40 bit WEP key. Make the key index 2 and use a key of “cisco”. Also, set the administrative status of the WLAN to enabled and change the interface name to VLAN3. When you are done, click **Apply** and you should see both WLANs in the WLAN list.

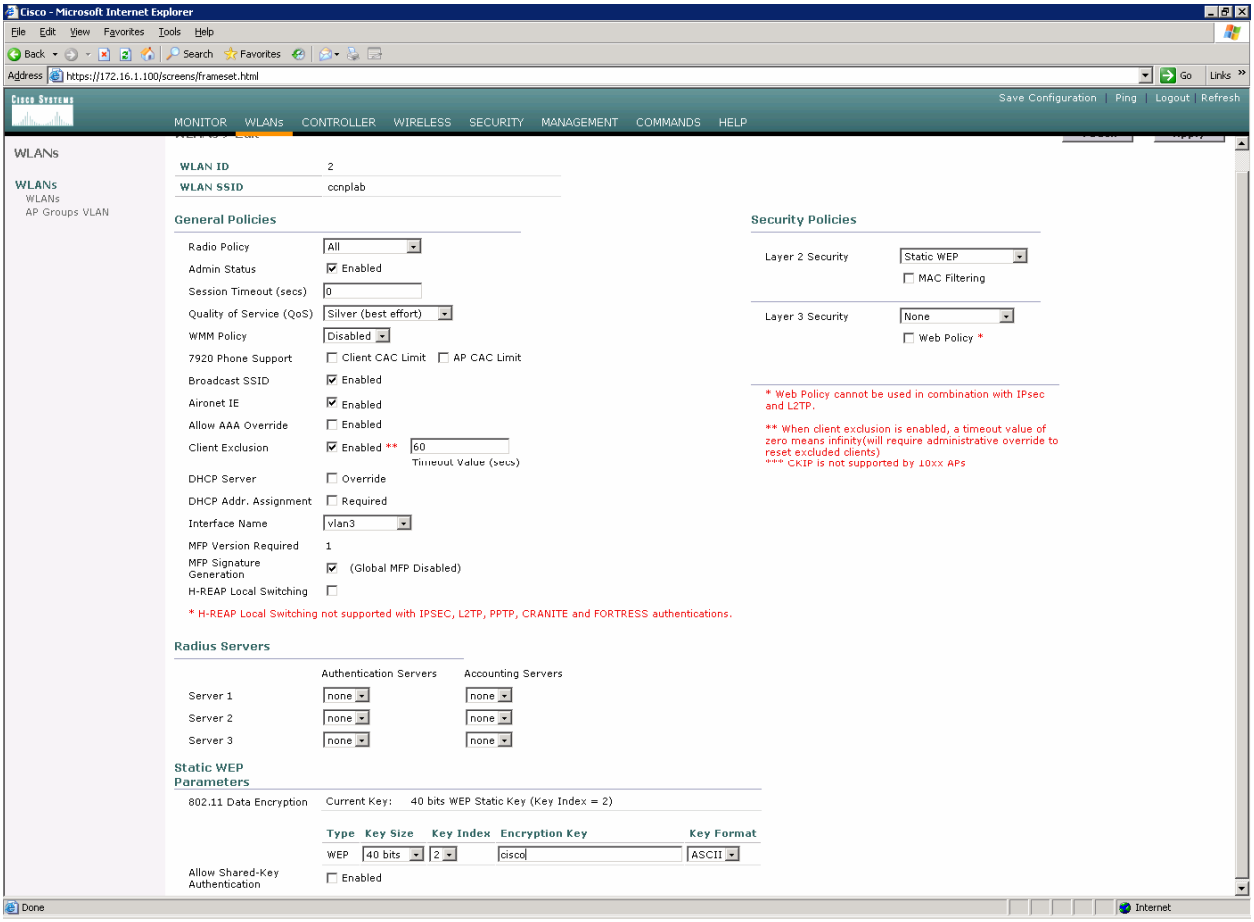


Figure 4-5: Configuring VLAN Association and Authentication for VLAN 3

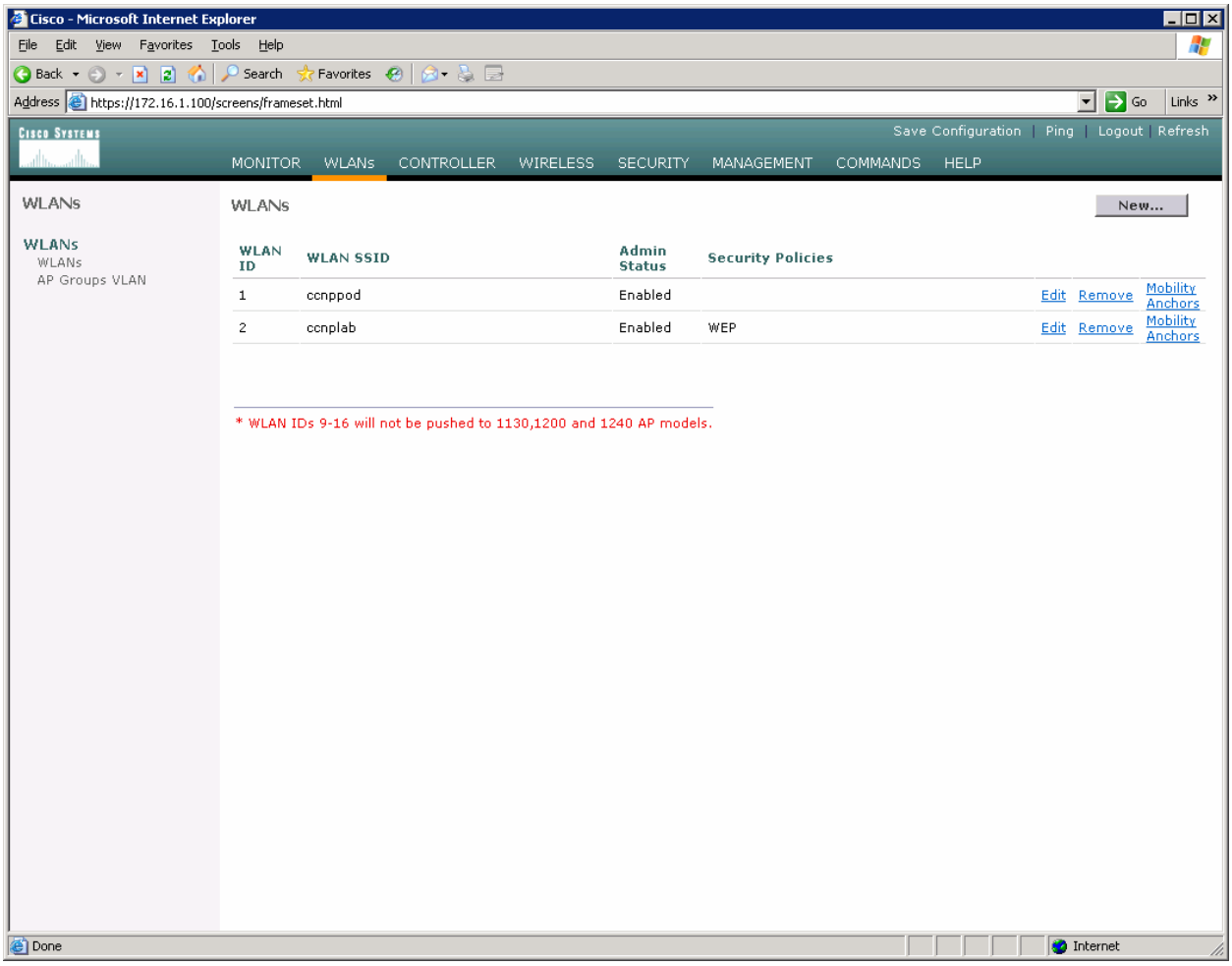


Figure 4-6: Verifying Final WLAN Configuration

At this point, if you have a computer with a wireless card installed you should be able to see both SSIDs and connect to the WLANs/VLANs associated with them. Notice that each WLAN exists in a separate subnet, because each WLAN is in a separate VLAN.

