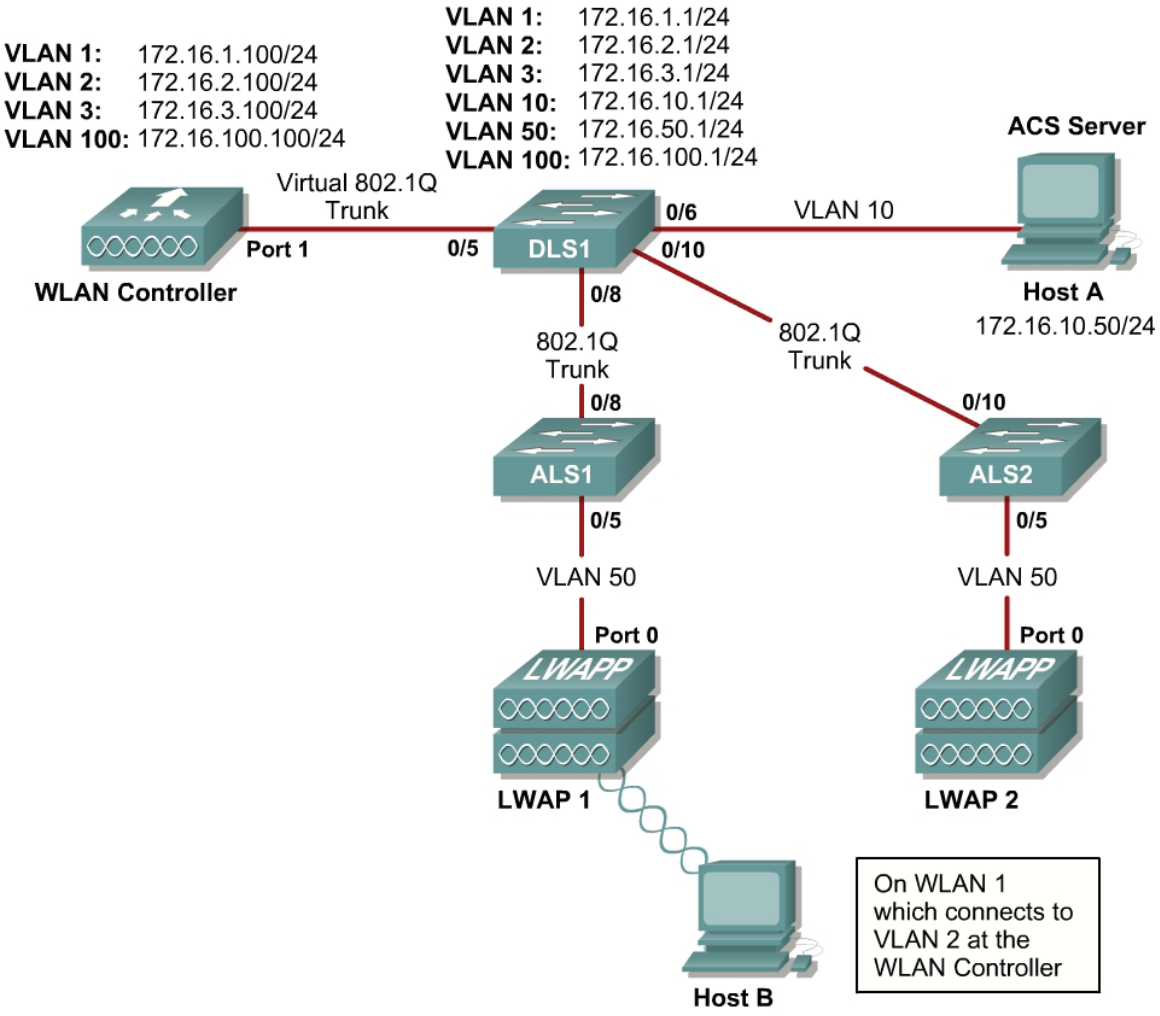
LAB: Configuring LEAP

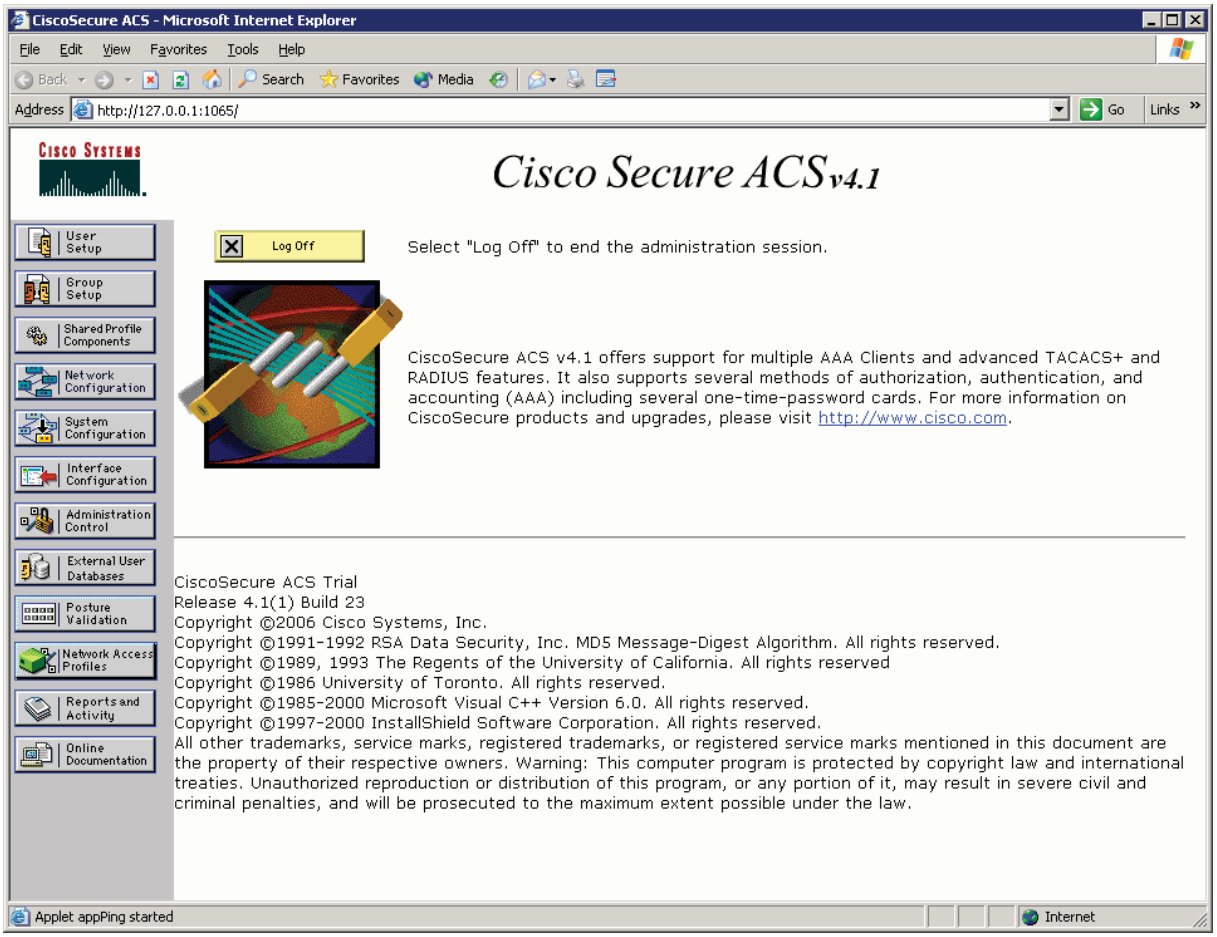
Learning Objectives

Configure Cisco ACS Radius server
Configure a WLAN to use the 802.1X security protocol and LEAP
Authenticate with an access point using 802.1X security and LEAP



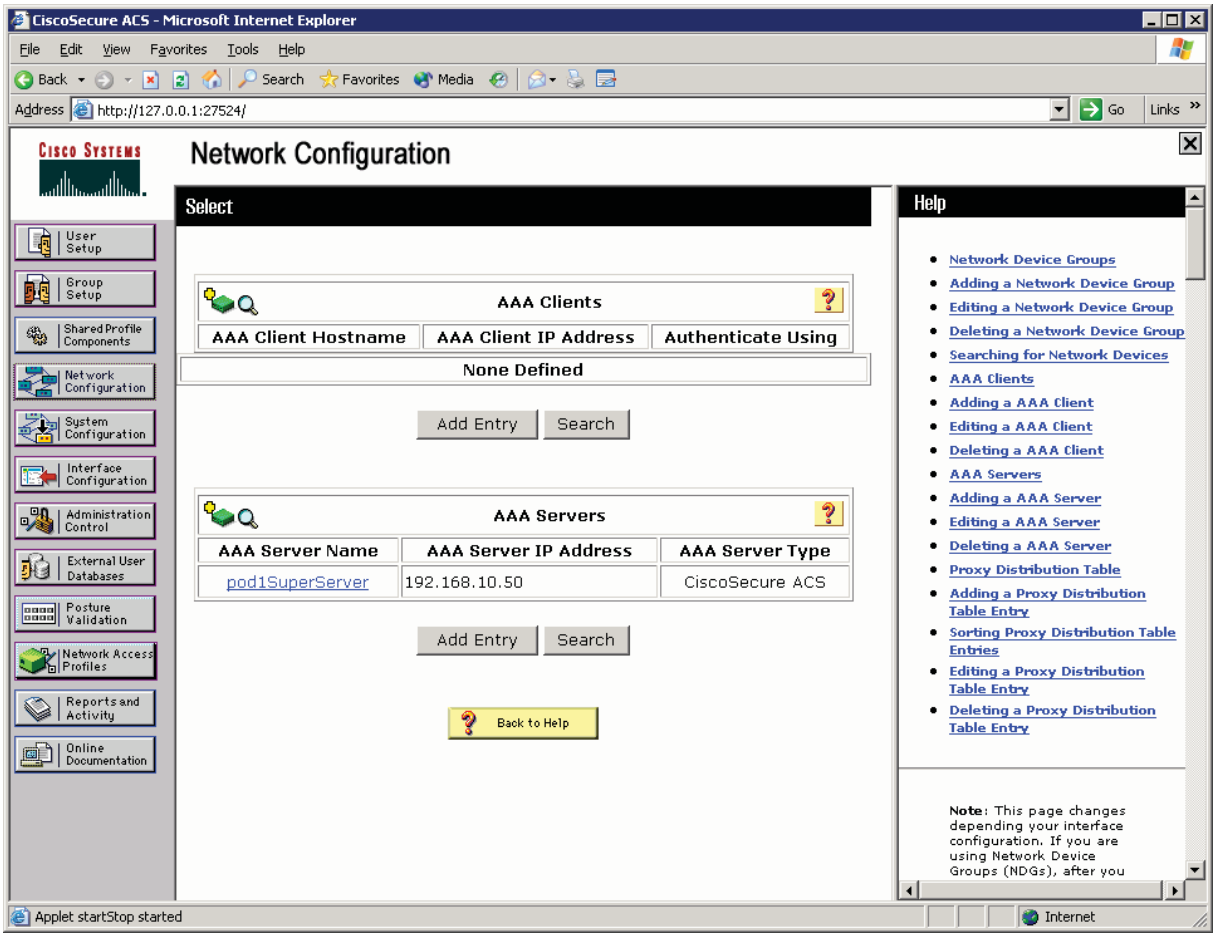
Make sure you have LAB3: Configuring a WLAN Controller finished prior to this lab. For the convenience of this lab, we have already installed Cisco Secure Access Control on Host A.

Set up ACS for LEAP



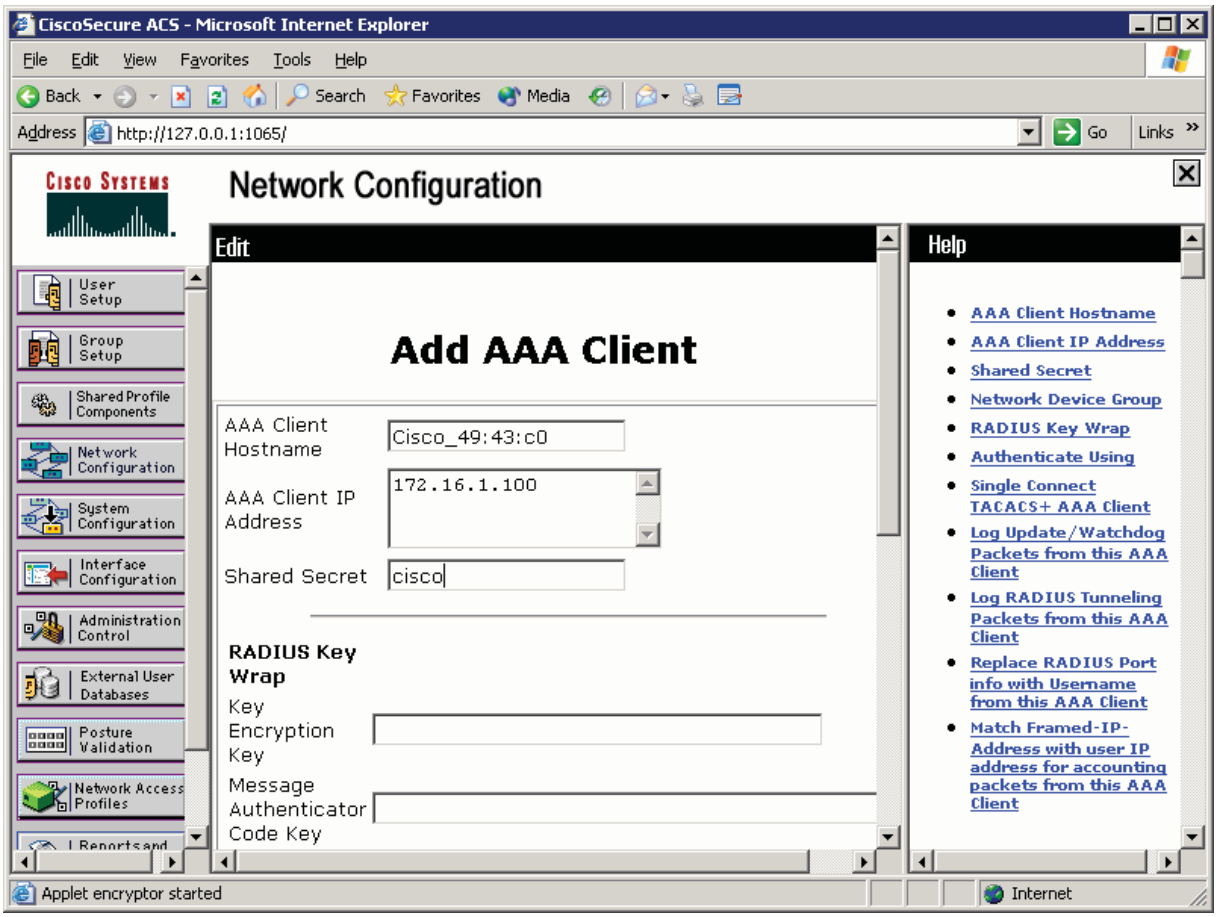
ACS Home Page

In the left pane, click **Network Configuration**. On the Network Configuration screen, you can configure authentication, authorization, accounting (AAA) clients directly. Click the **Add Entry** button under the heading **AAA Clients**.



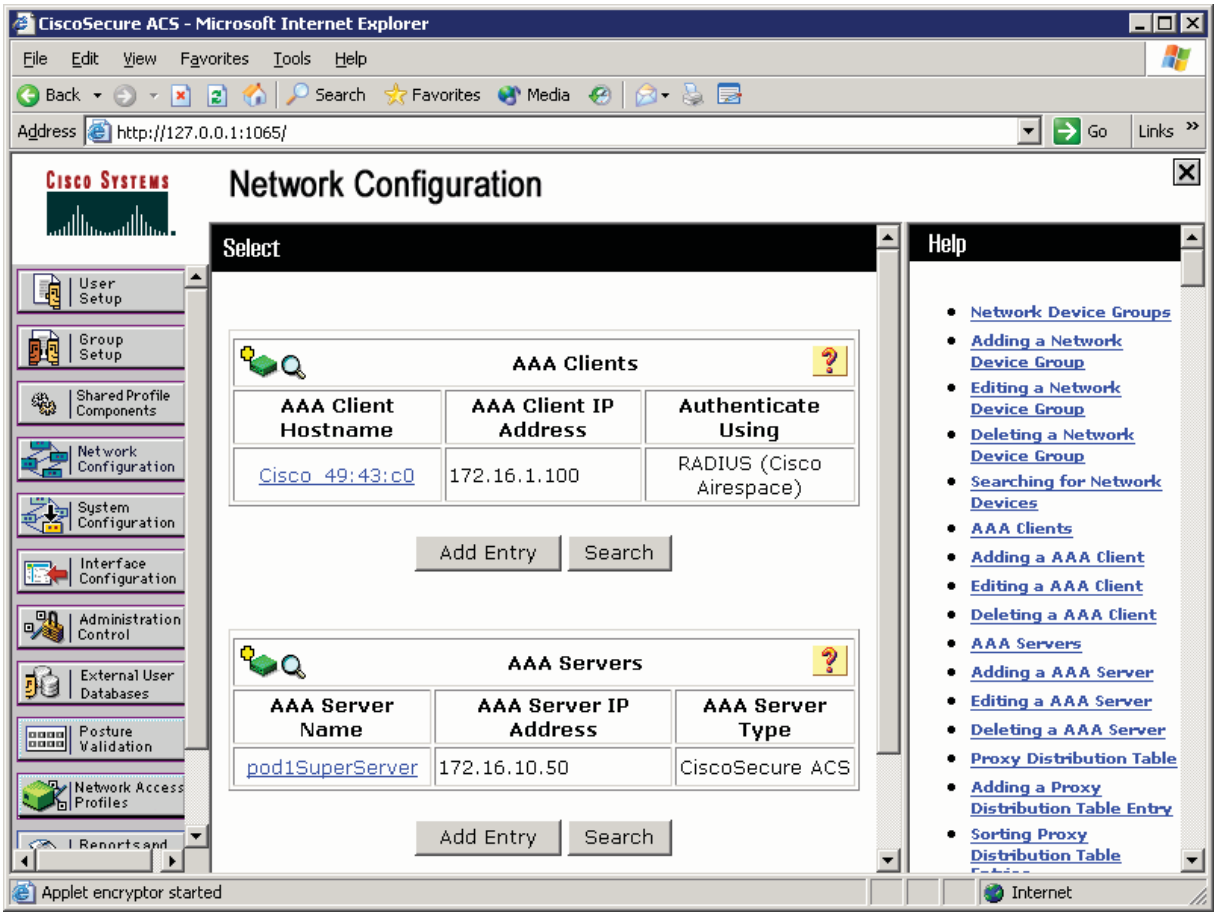
ACS Network Configuration Page

Enter the hostname of the WLC (you can get this from **show run-config** on the WLC command-line interface [CLI] or from its web interface), the management IP address of the WLC, and “cisco” as the shared secret. Change the value of the **Authenticate using:** field to **RADIUS (Cisco Airespace)**. After you have entered in everything, click **Submit + Apply**.



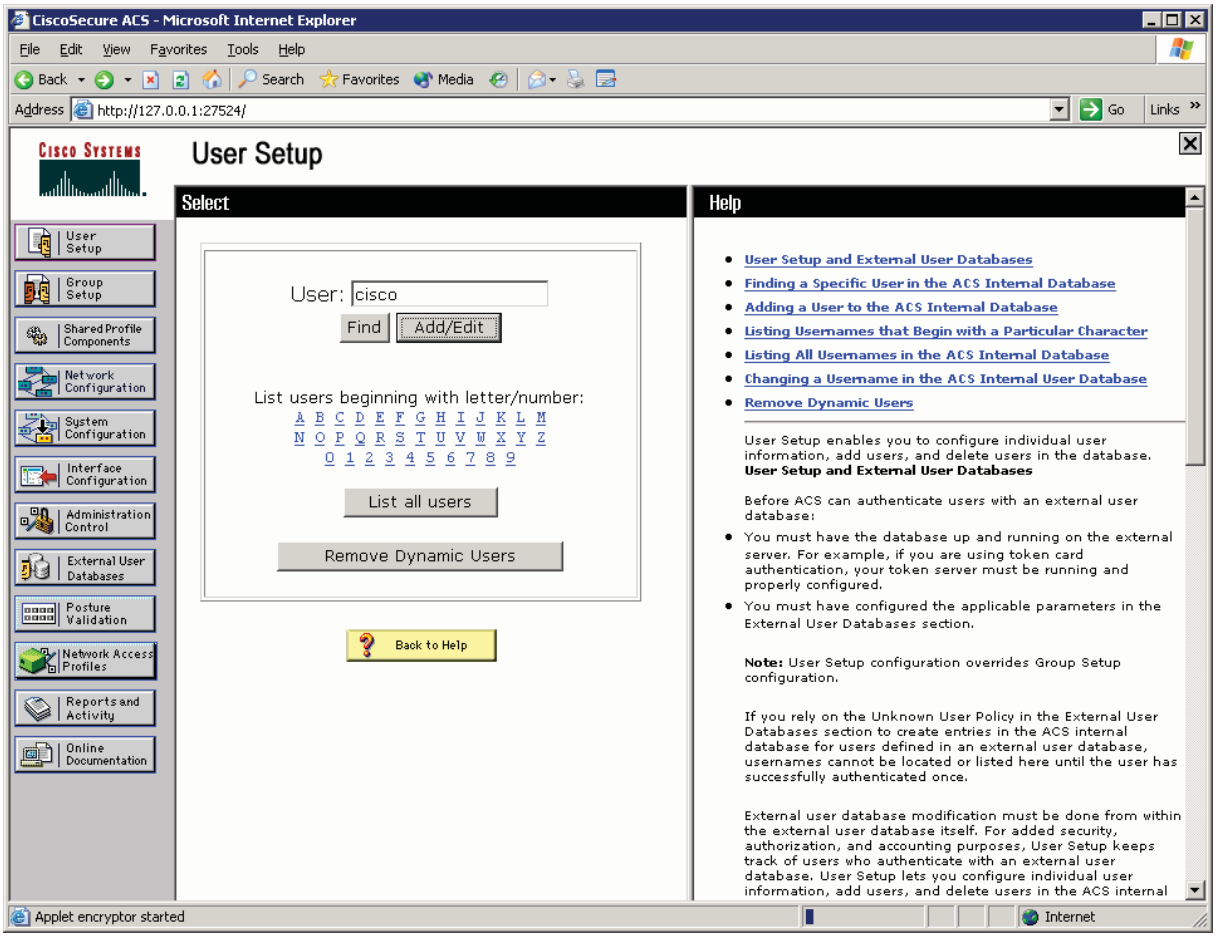
ACS AAA Client Configuration

You should now be able to see the WLC listed as an AAA client on the network configuration screen.



ACS Network Configuration Page, with Changes Applied

On the left pane, click **User Setup**. Add a user named “cisco,” and then click **Add/Edit**.

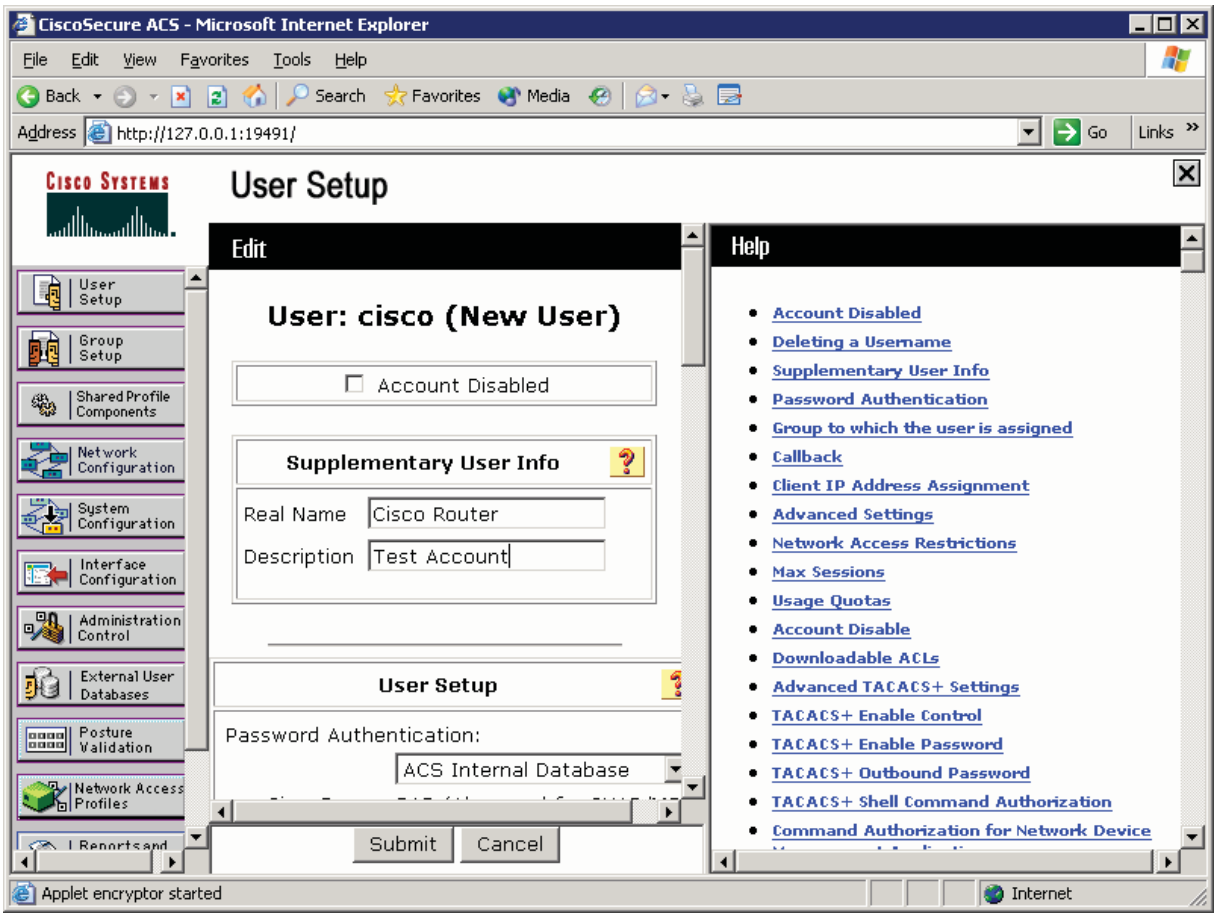


ACS User Configuration Page

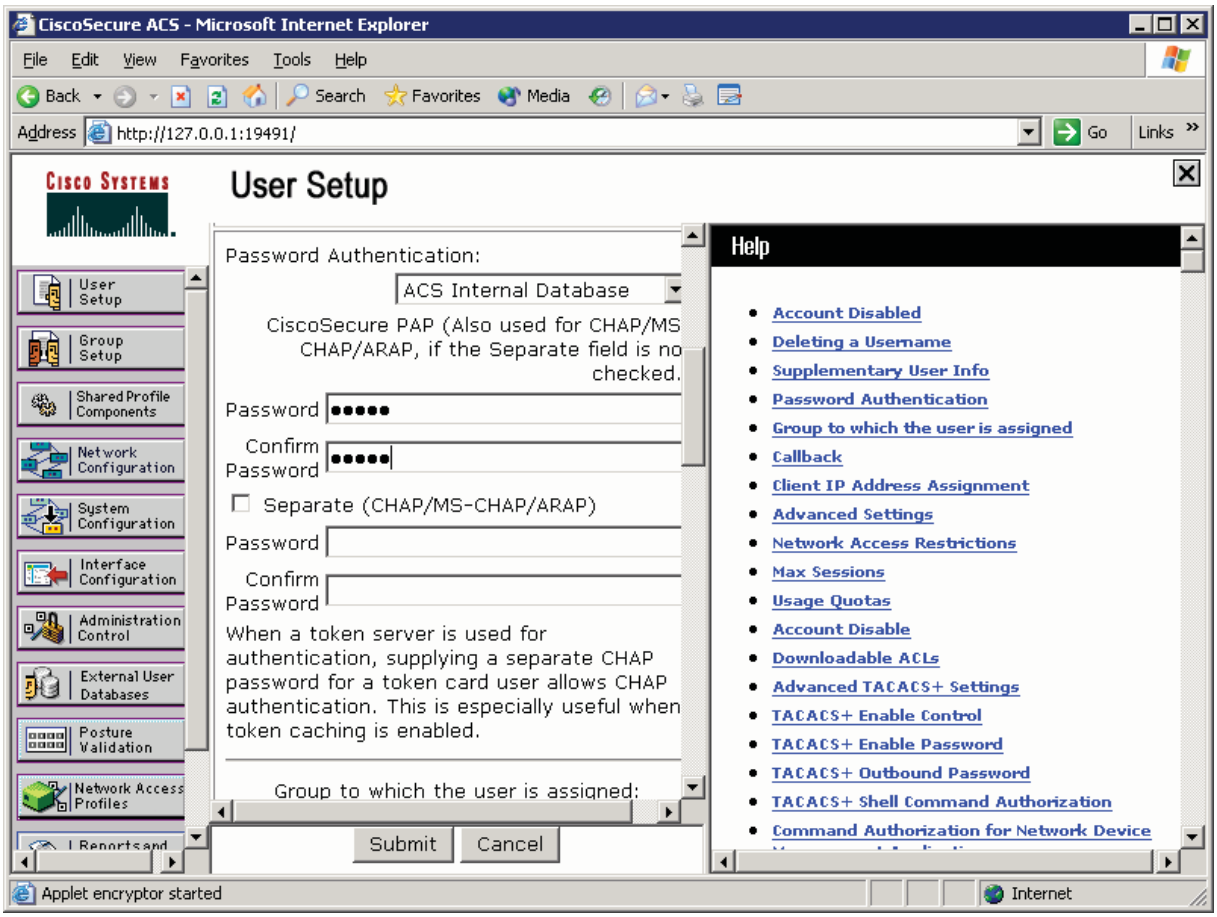
Assign “cisco” as the user name, and set “cisco” as the password. Click **Submit**.

Why is the shared secret configured on a per-client basis?

You should see the WLC listed in the network configuration screen.
On the left pane, click **User Setup**. Type in “cisco” in the user field (this will be the name of the user we are creating), and then click **Add/Edit**.



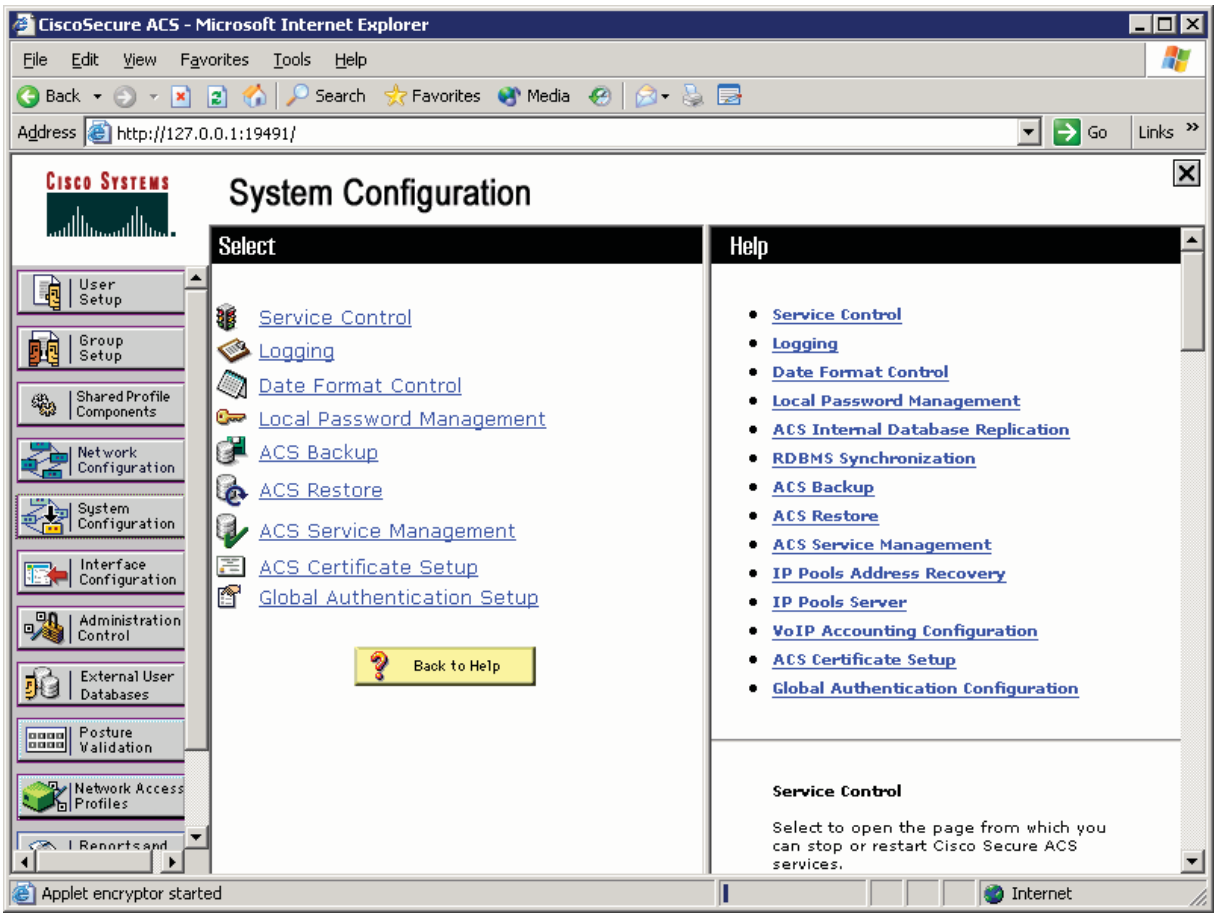
ACS User Configuration



ACS User-level Password and Group Configuration

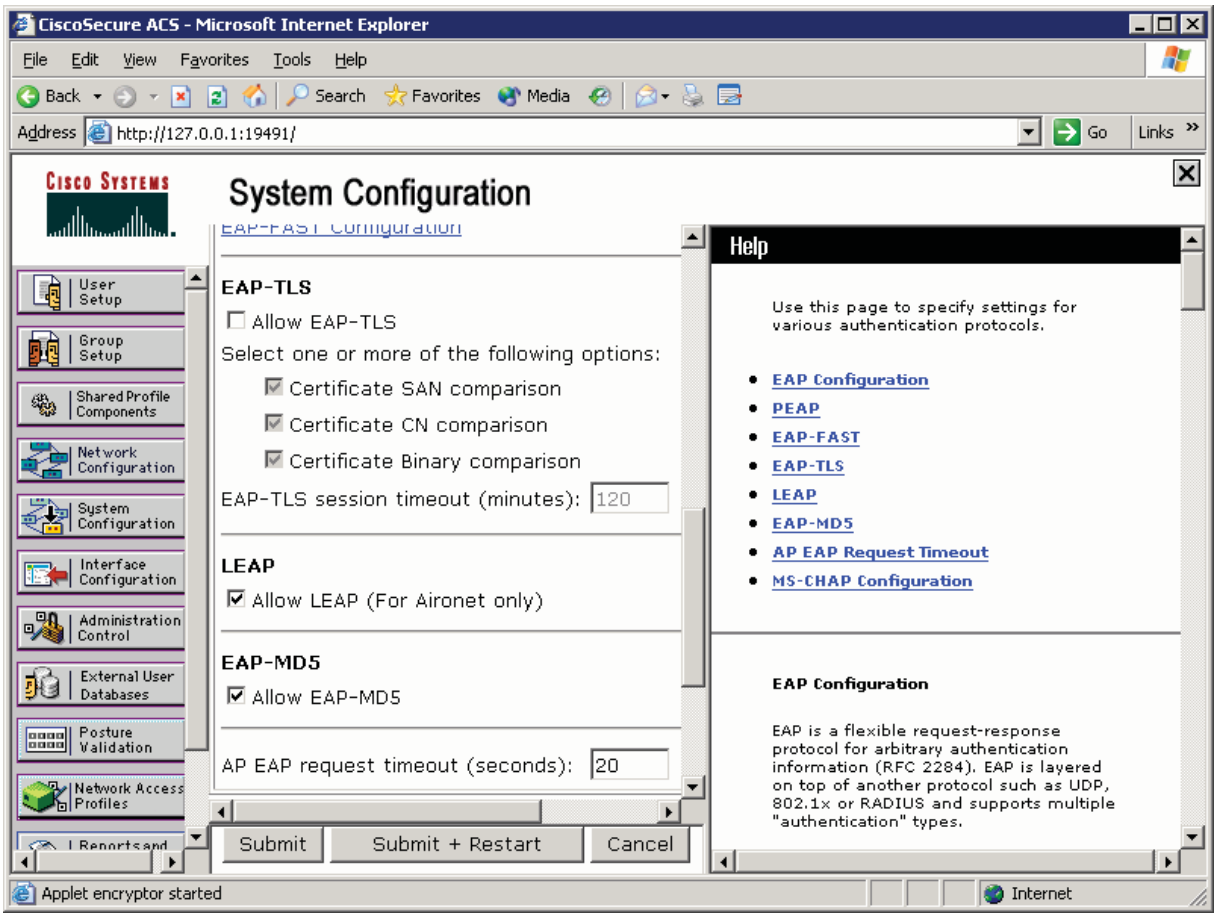
For what purpose will you use this user account?

Although it should be enabled by default, we will make sure that LEAP authentication is enabled in ACS.
Click **System Configuration** on the left pane.



System Configuration Tab

Click **Global Authentication Setup** in the list of options. Scroll down and make sure that **Allow LEAP** is checked.



System Security Protocol Configuration

There are many variants of the Extensible Authentication Protocol.

Lightweight Extensible Authentication Protocol, LEAP, is a Cisco proprietary wireless LAN authentication method. It has some well-known security issues. List a few.

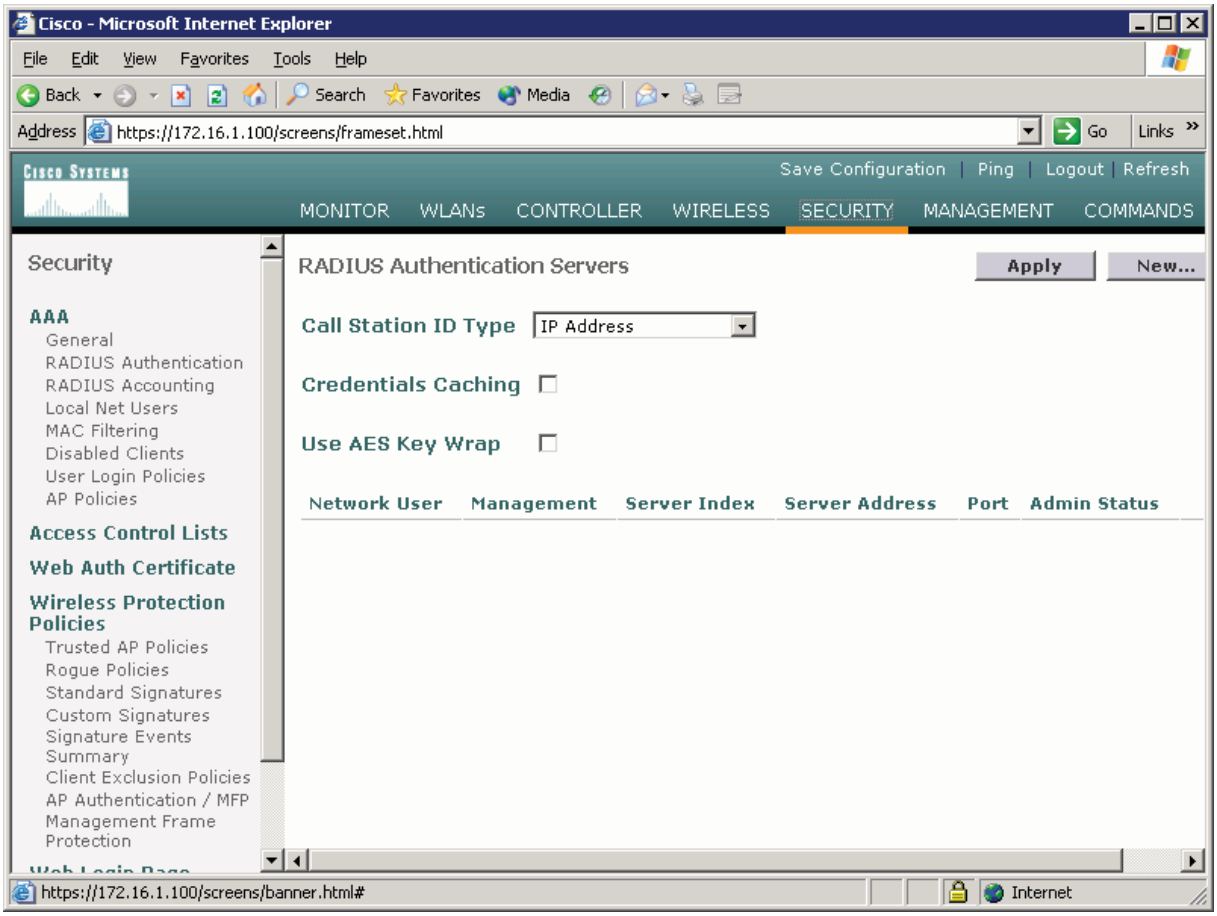
Describe how Protected Extensible Authentication Protocol, PEAP, enhances the EAP protocol.

WLAN Controller Radius Server Configuration

In this step, we will set up a RADIUS server to be used for WLAN authentication.

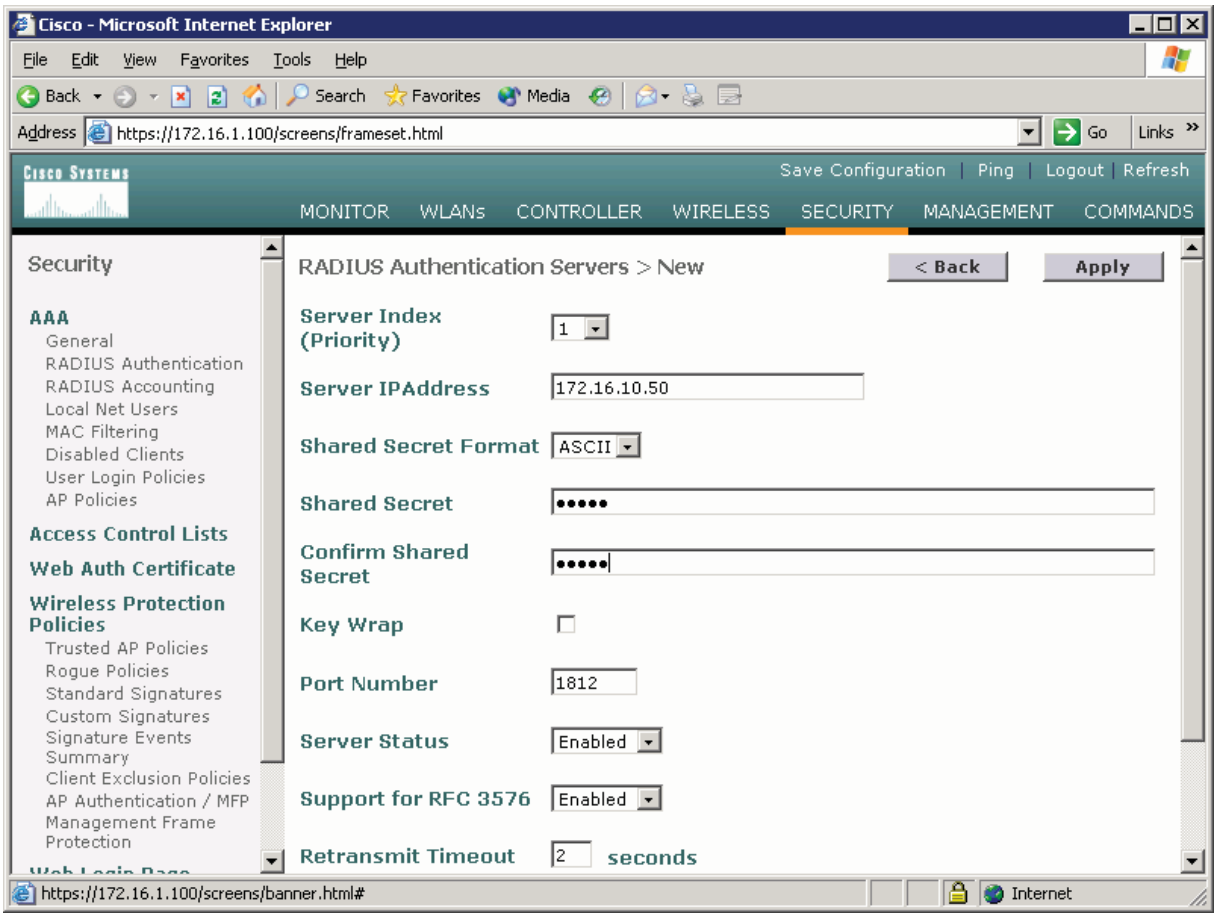
Connect to the WLC from the Management Host

Click the **Security** link at the top of the WLC interface.



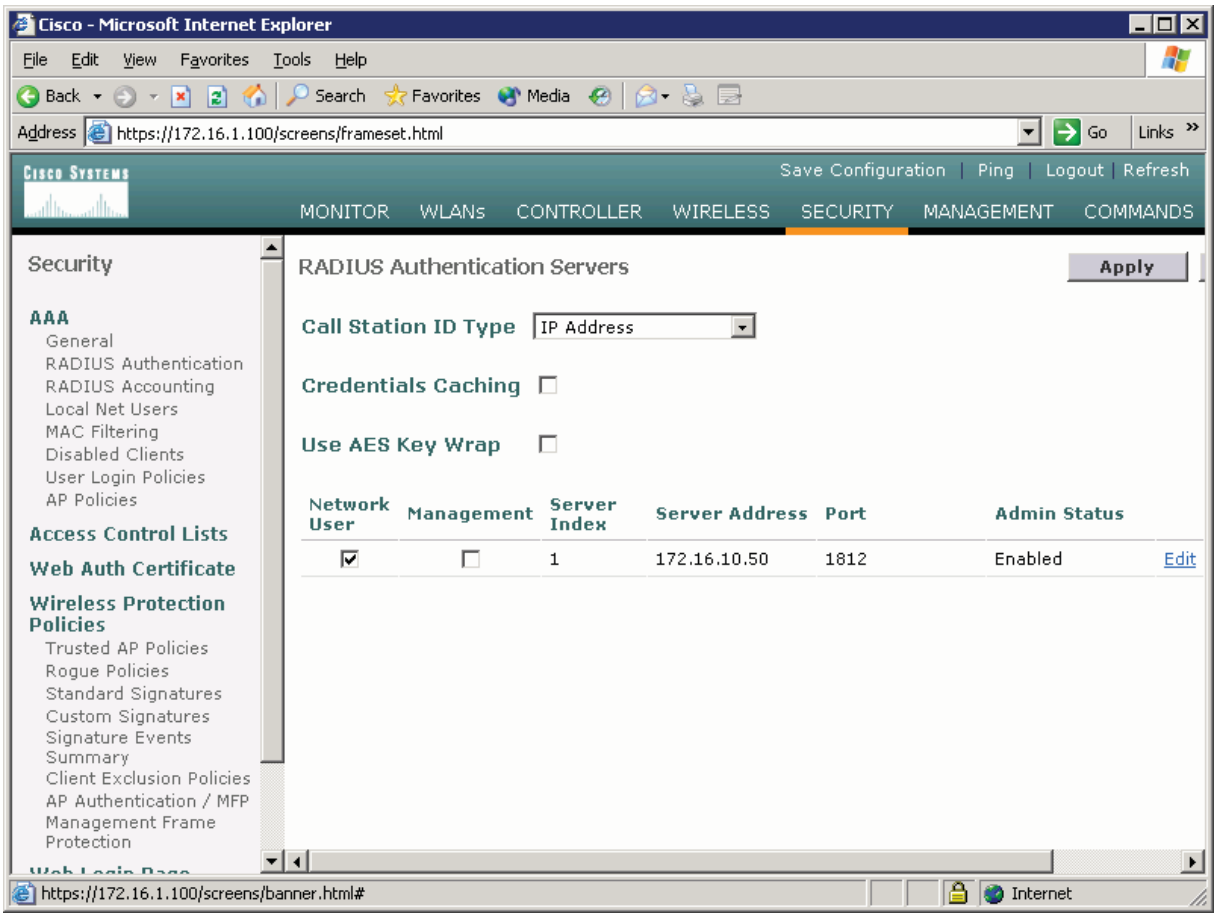
WLC RADIUS Server Configuration

Click **New** to add a new server. Set the IP address to the IP address of the server running ACS, and set the shared secret to “cisco” as configured on the ACS server for this device. Click **Apply** when done.



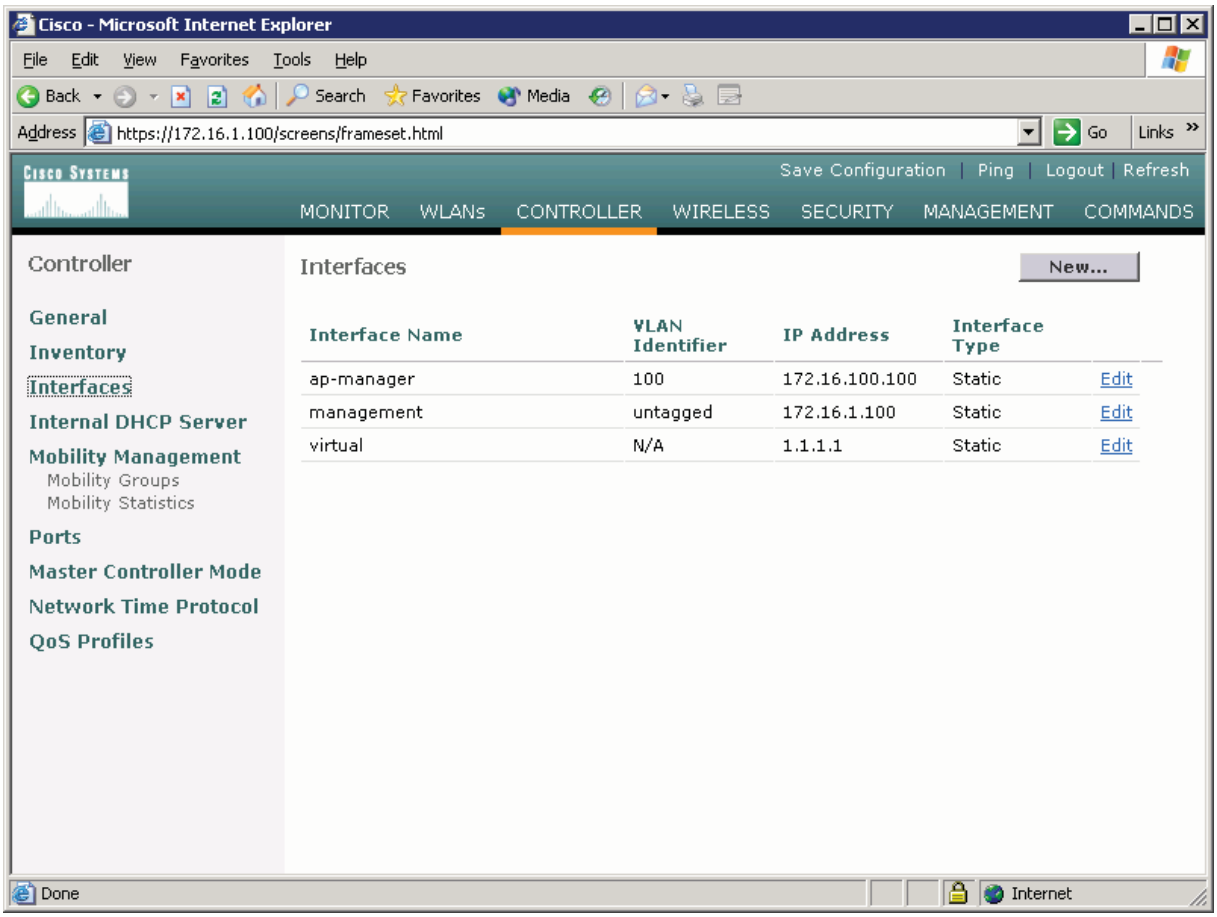
New RADIUS Server Configuration

You should see the new server added to the list. What is the purpose of the shared secret?



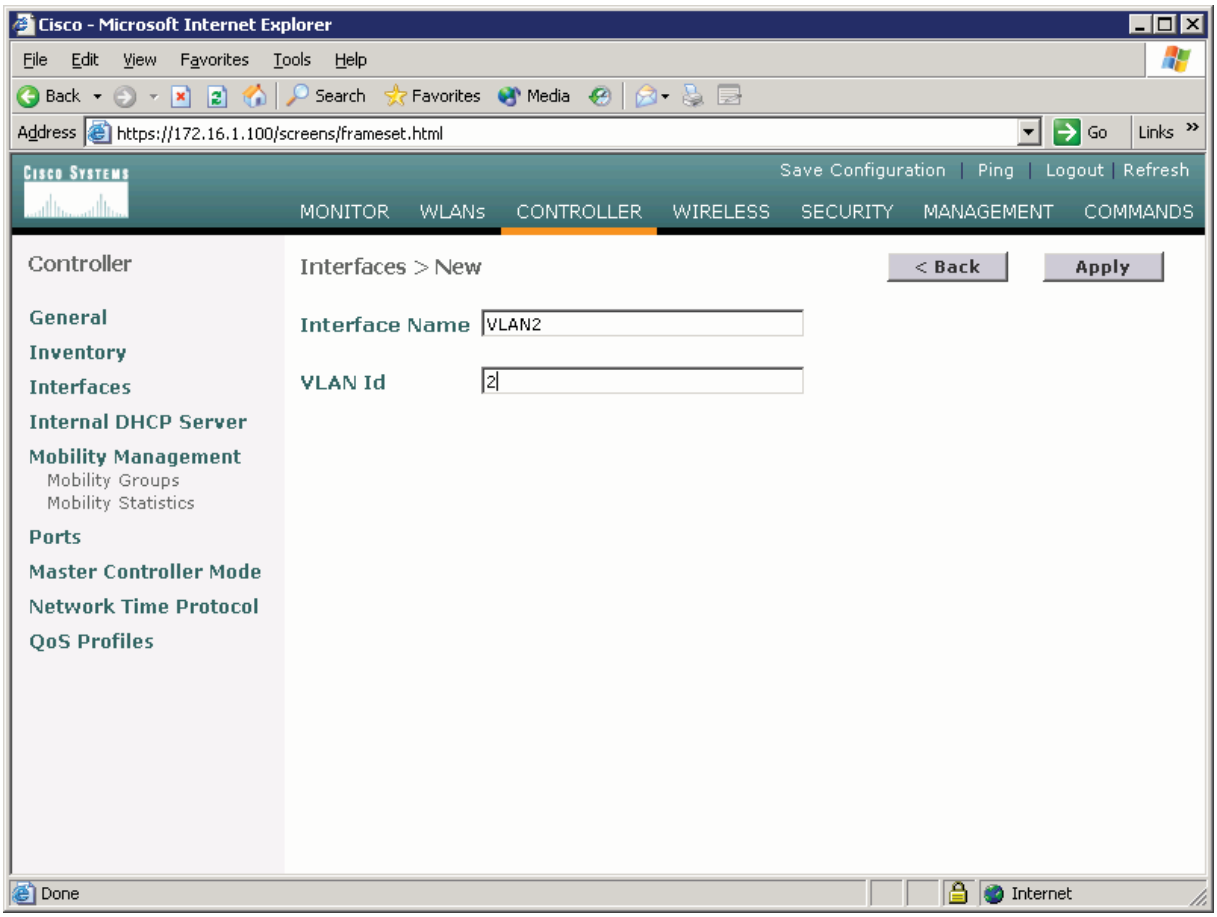
WLC RADIUS Server Configuration with Changes Applied

Click the **Controller** button at the top of the WLC interface. On the left pane, click **Interfaces** to see the current configured IP interfaces on the WLC. Click **New** to create a new interface.



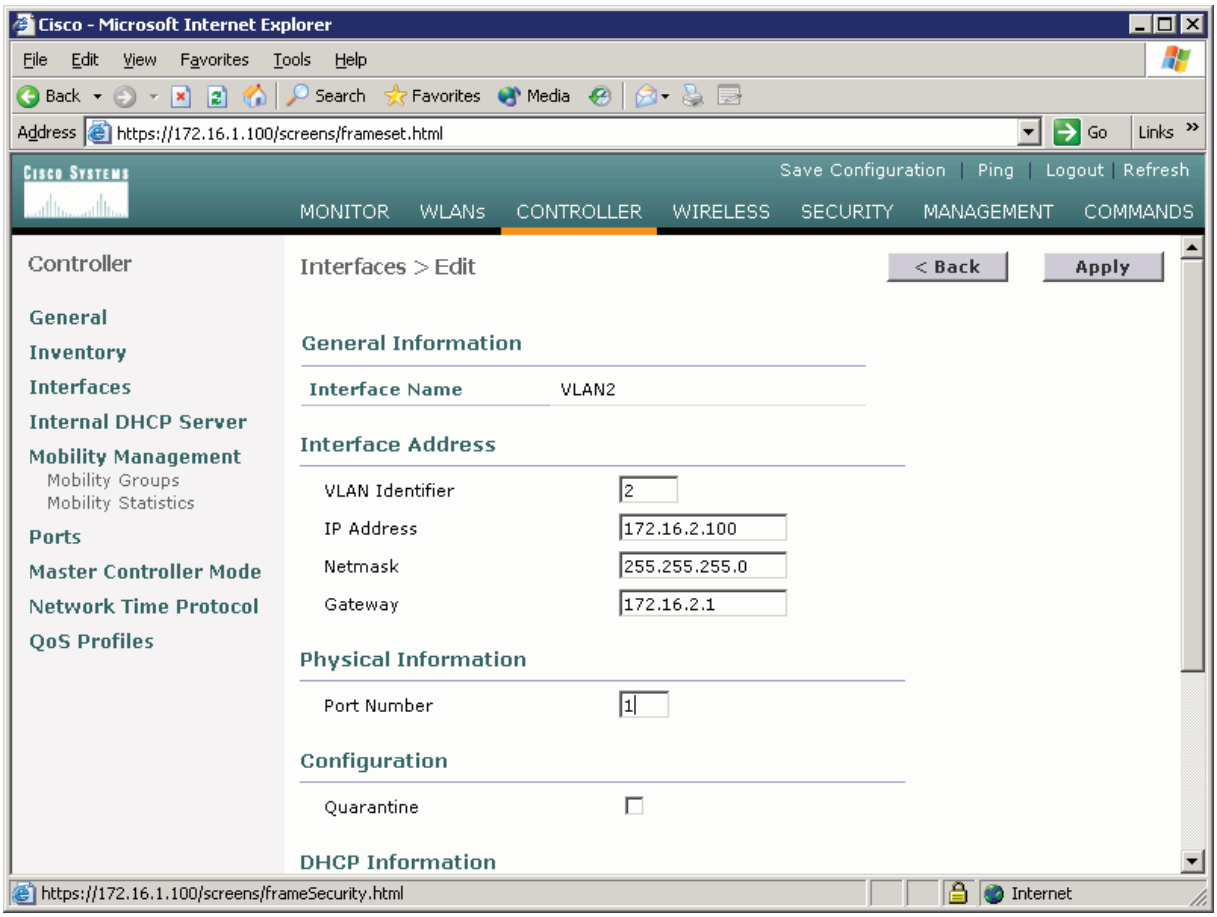
Interface Configuration Page

Name the interface “VLAN2” and assign it to 802.1Q tag 2, just like in Lab 6.2. Click **Apply** when you have completed this.

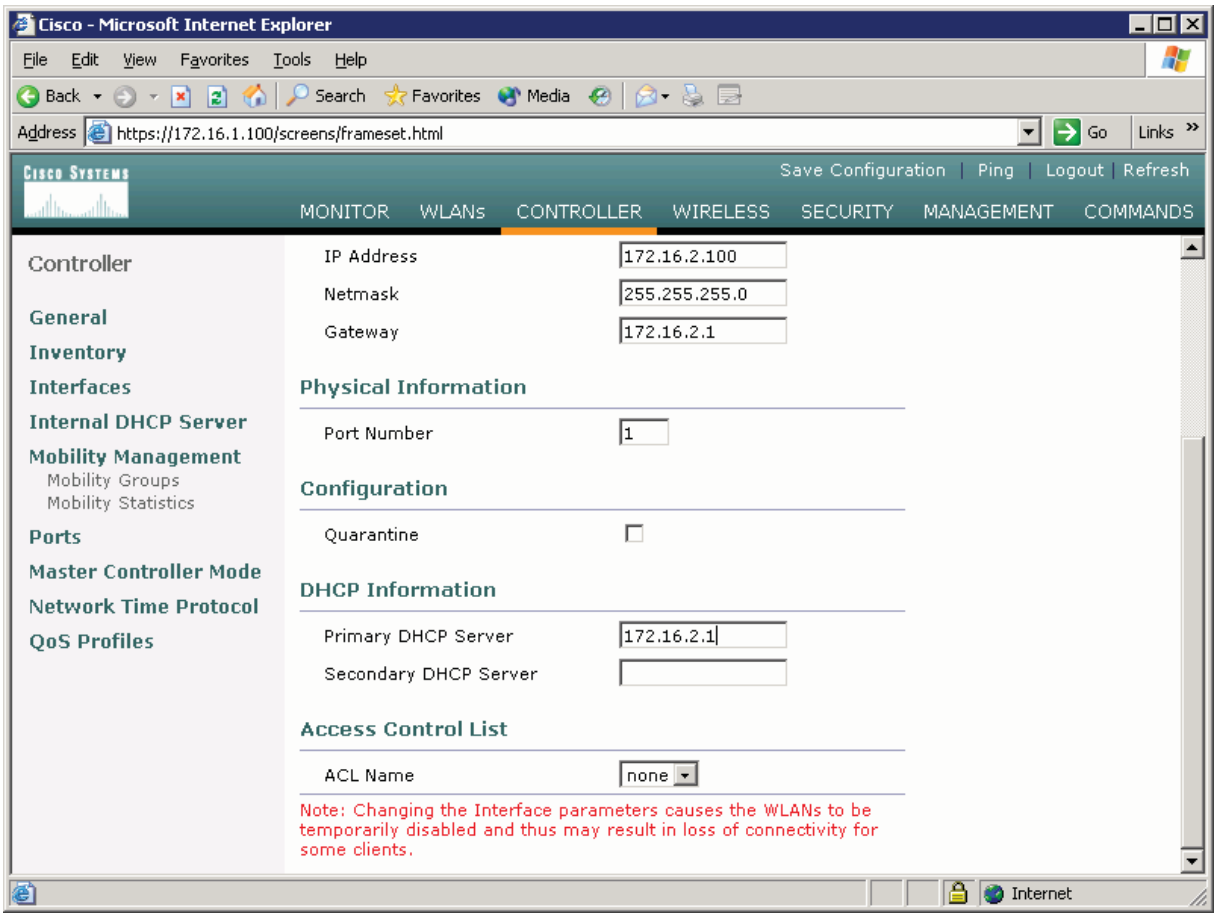


Creating a New VLAN Interface

Configure the IP address, default gateway, port number, and Dynamic Host Configuration Protocol (DHCP) server for this interface as shown in the following figure, and then click **Apply**. Accept the warning that comes up by clicking **OK**.



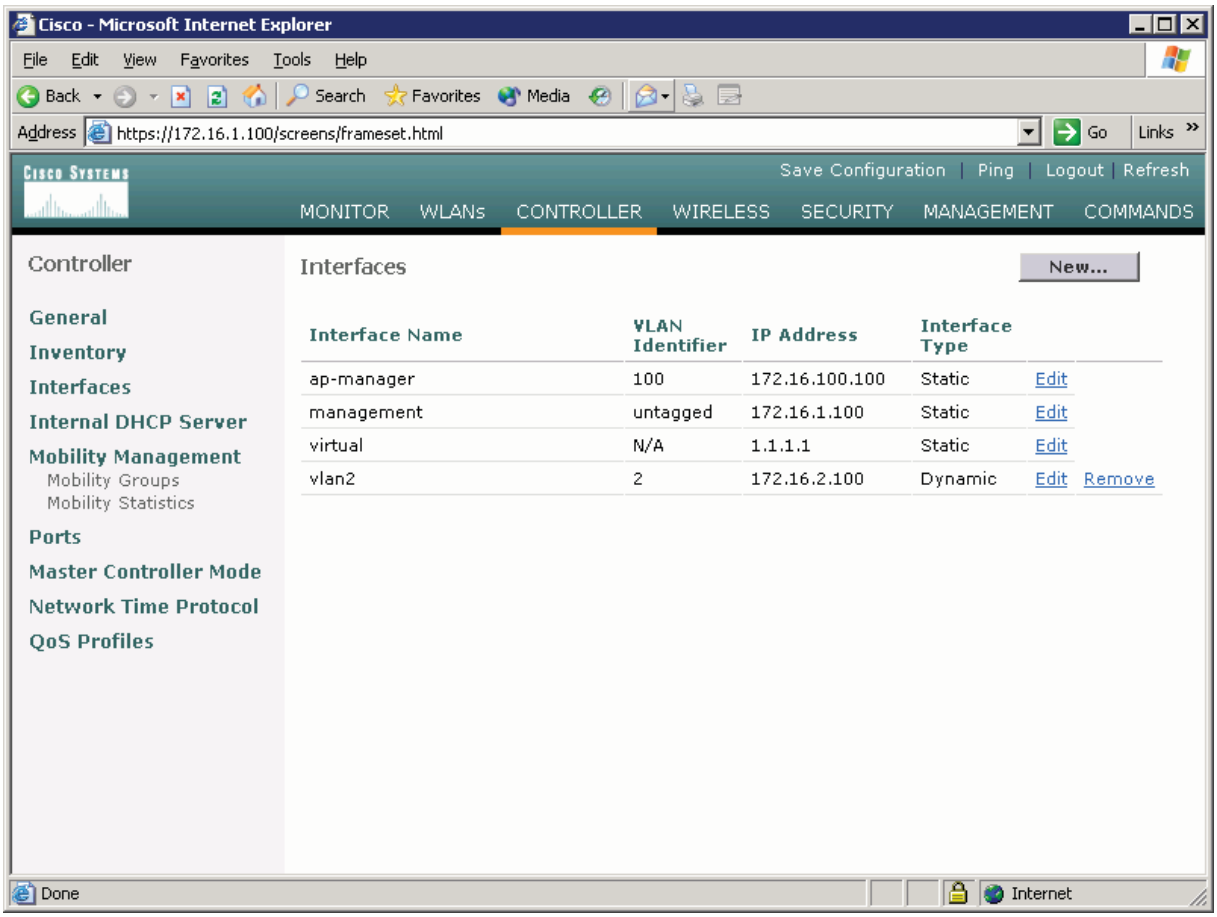
Configuring VLAN Interface Properties



Configuring VLAN Interface Properties, DHCP Options

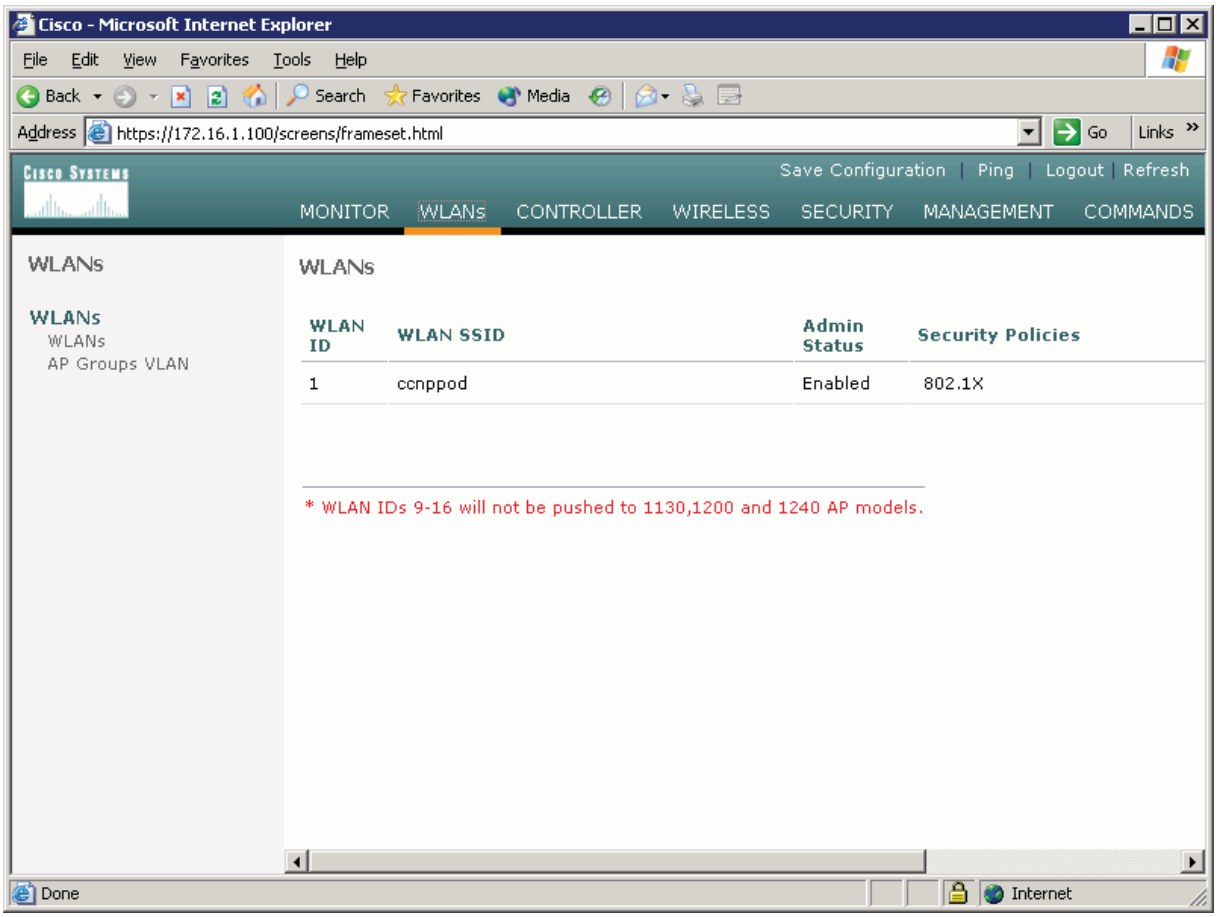
What is a probable IP-address a wireless client will receive?

The new interface should appear in the interfaces list.



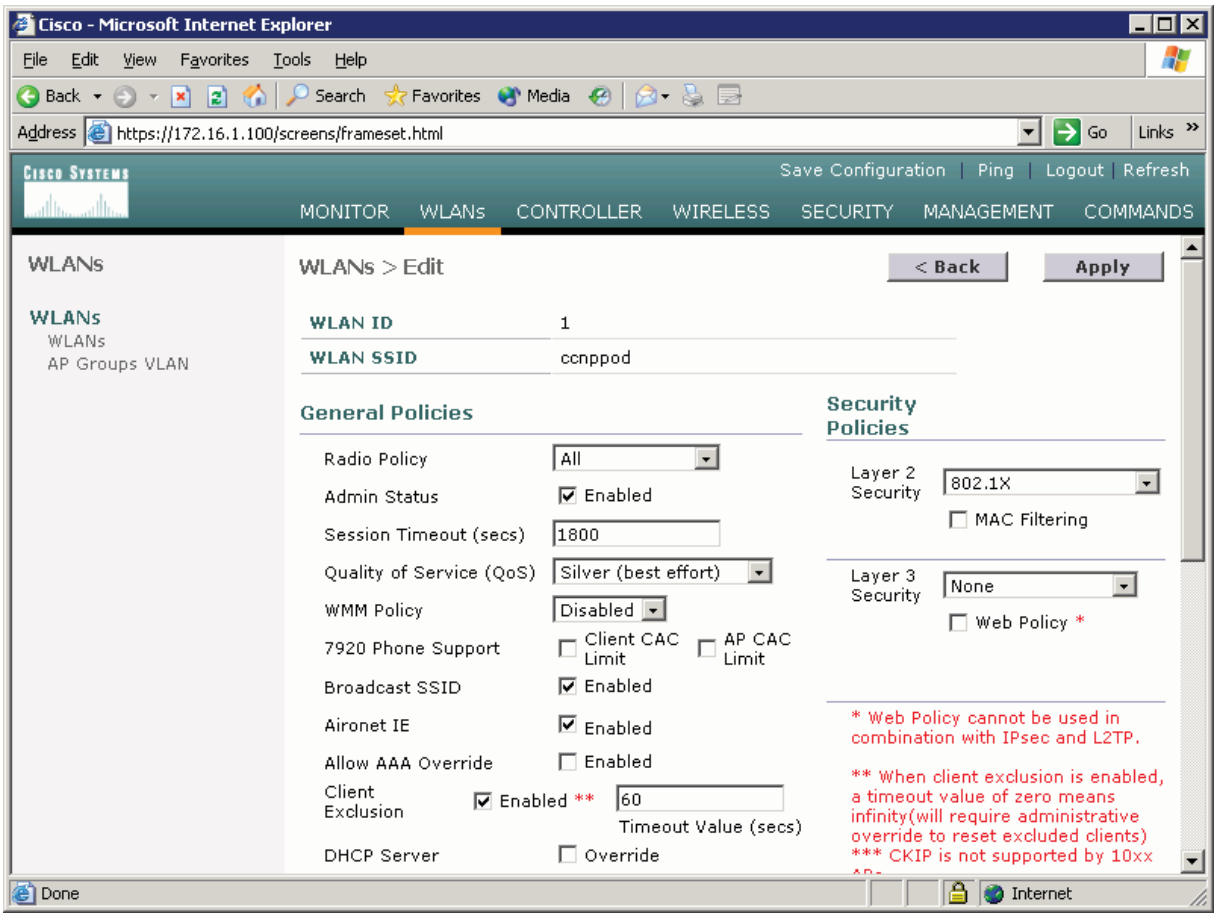
Verify Existing VLAN Interfaces

Click the **WLANs** button at the top of the web interface. This shows you all configured WLANs on the WLC. Currently the only one listed is the one created during the setup wizard.



Viewing Existing WLANs with Security Policies

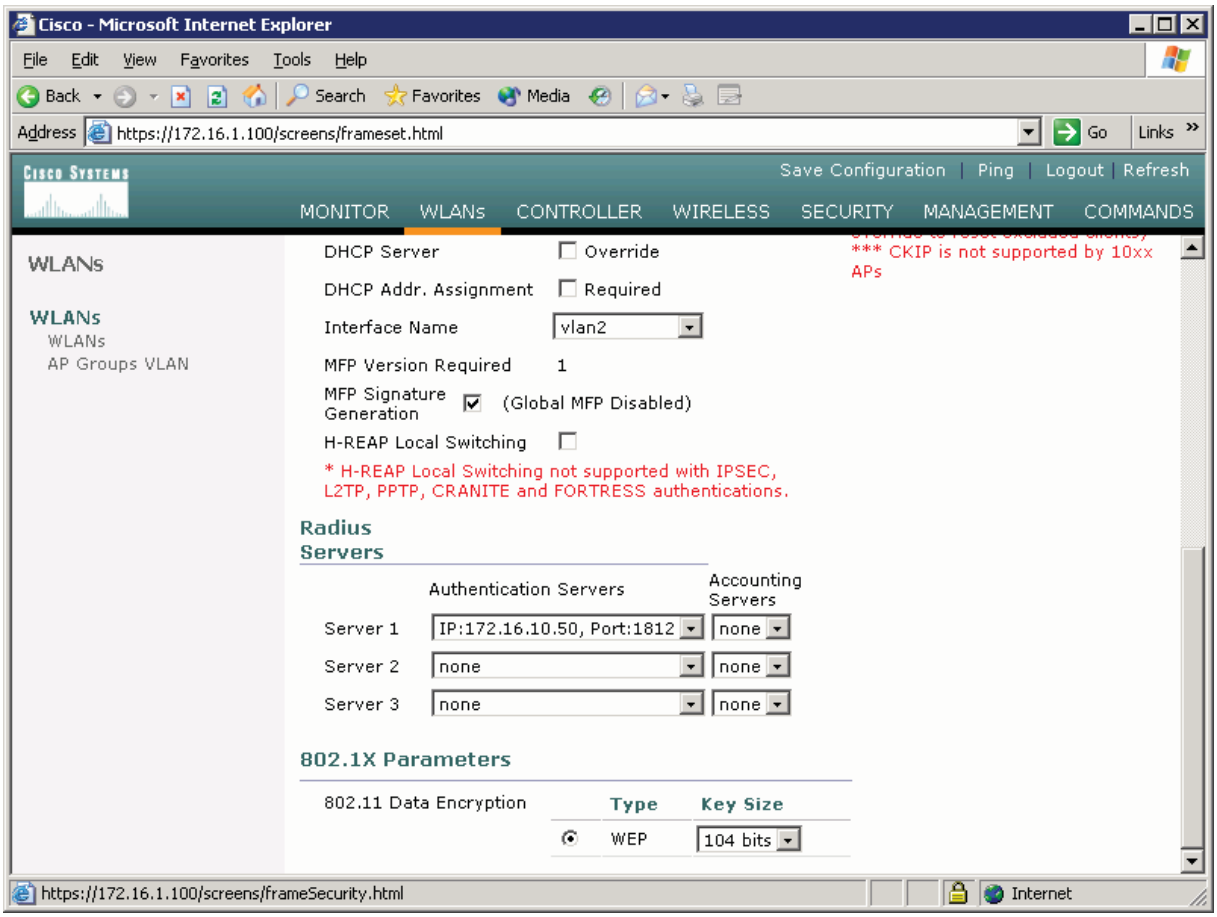
Click **Edit** for the WLAN listed. The default security policy is 802.1X, which is the security policy we want. Make sure that the administrative status of the WLAN is enabled. Change the IP interface of the WLAN to VLAN2, and assign the RADIUS server created earlier. Click **Apply** when all changes are configured. Click **OK** if a warning appears.



Editing the Configuration for WLAN 1

Silver or "best effort" is chosen from the Quality of Service options. What other options are available and what do they support?

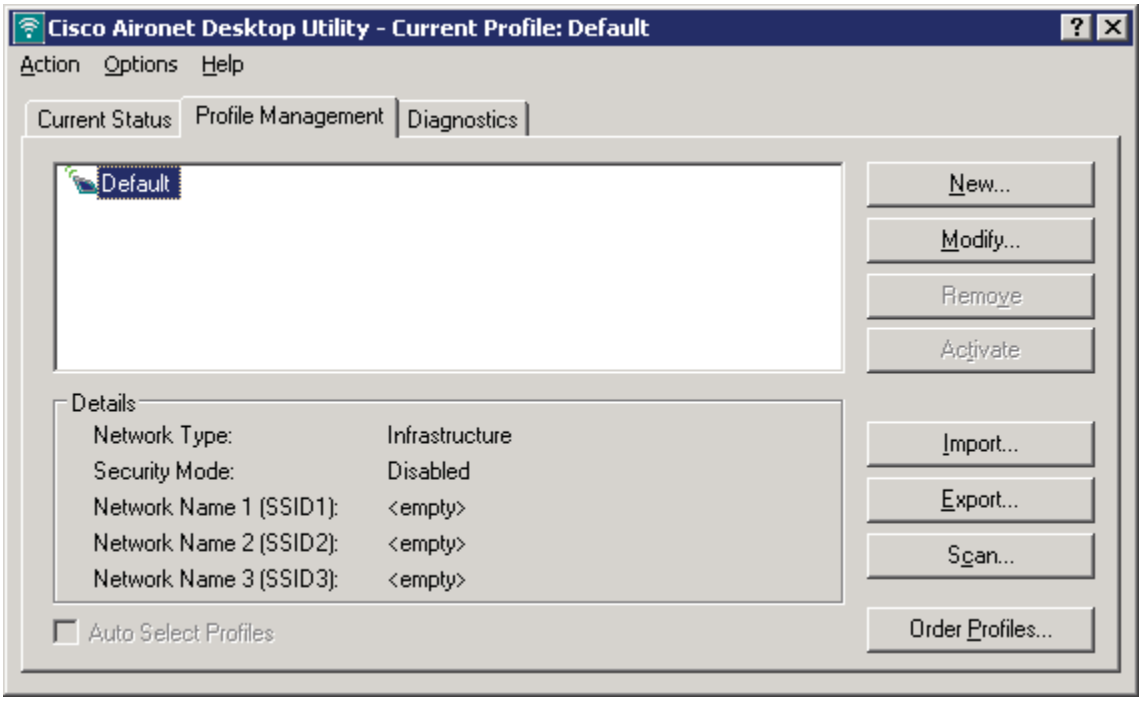
What is the purpose of enabling Aironet IE?



Editing the Configuration for WLAN 1, Security Options

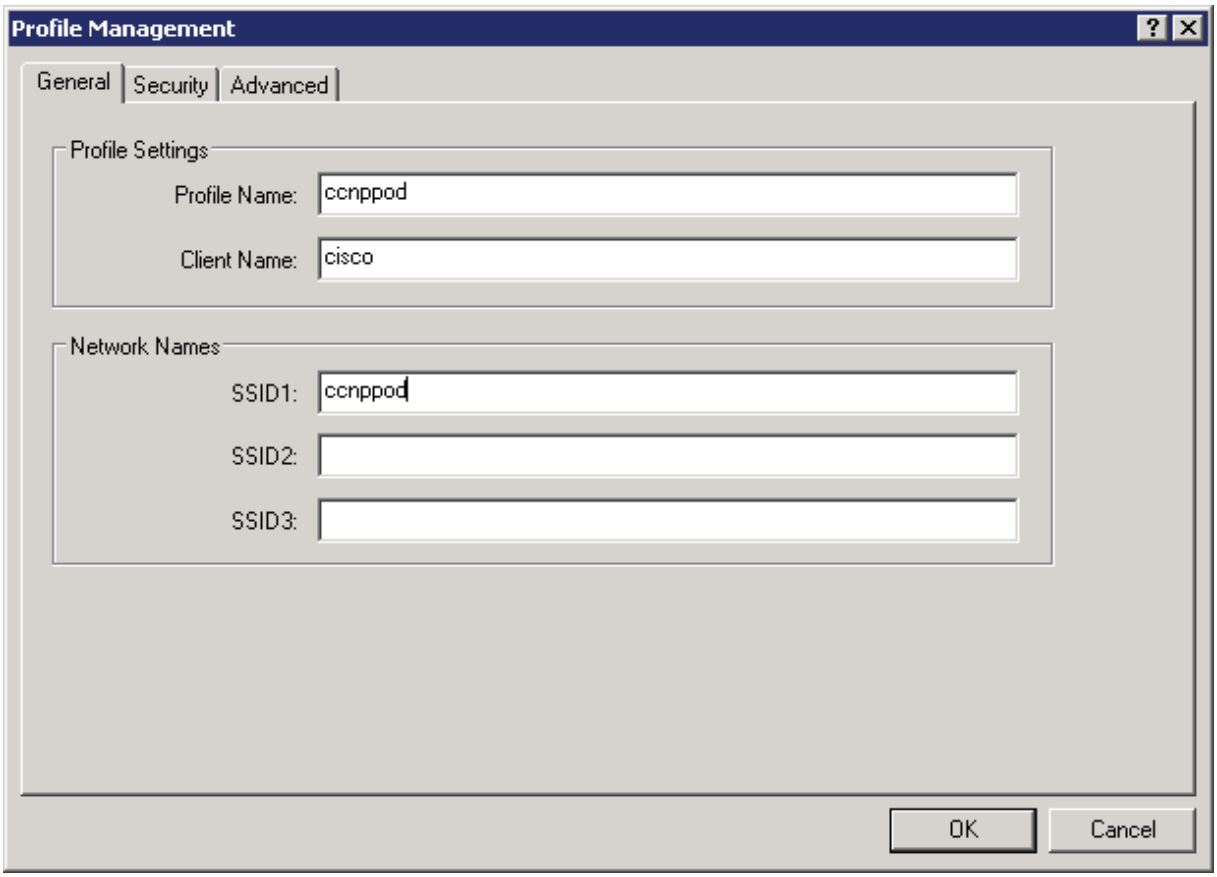
Configure the Wireless Client

On Host B, open up the Cisco Aironet Desktop Utility (ADU) either using the icon on the desktop or the program shortcut in the start menu. If you do not have the Cisco Aironet Desktop Utility installed, consult Lab 6.3: Configuring a Wireless Client. Once in the ADU, click the **Profile Management** tab. Next, click **New** to make a new profile.



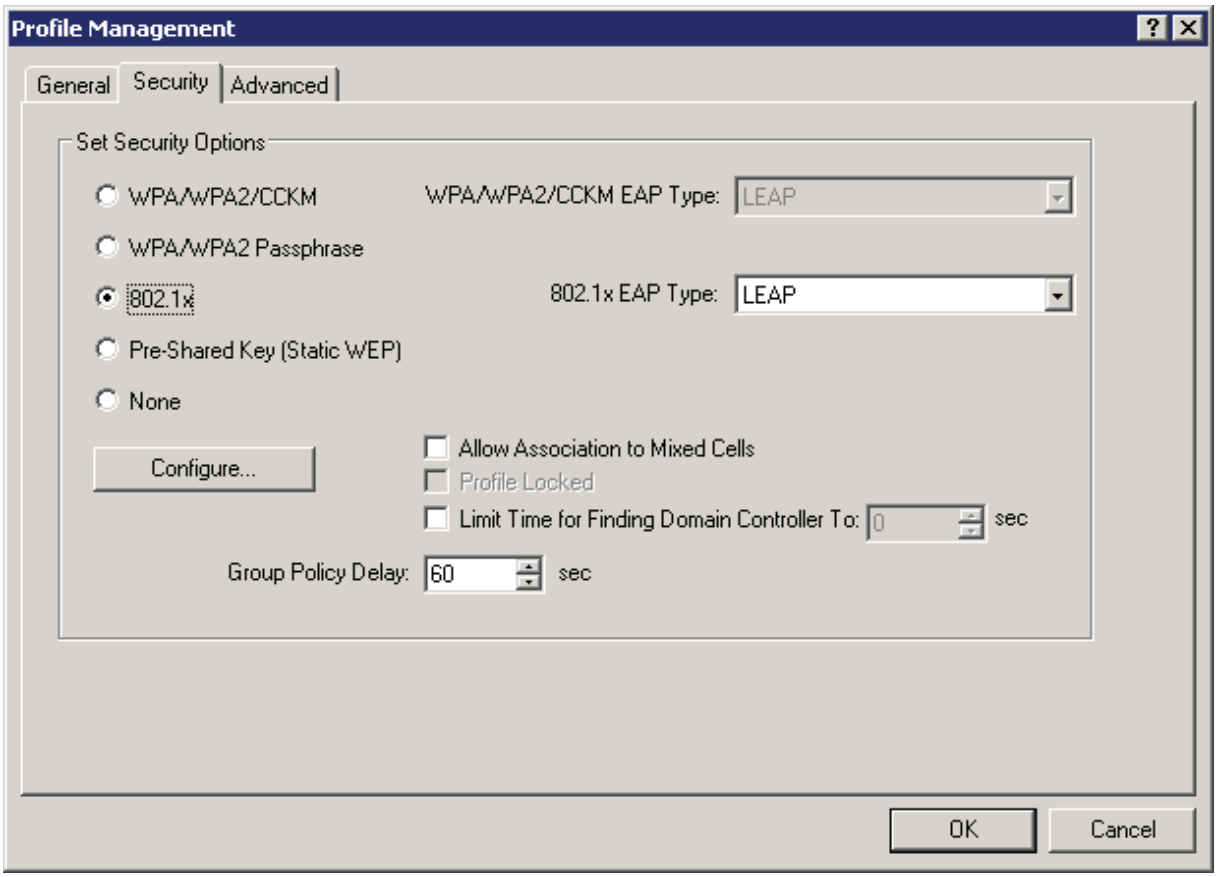
Cisco ADU Profile Management Tab

Use a profile name and service set identifier (SSID) of “ccnppod” since this was the SSID configured earlier. Use any client name desired. Here, “cisco” is the name used.



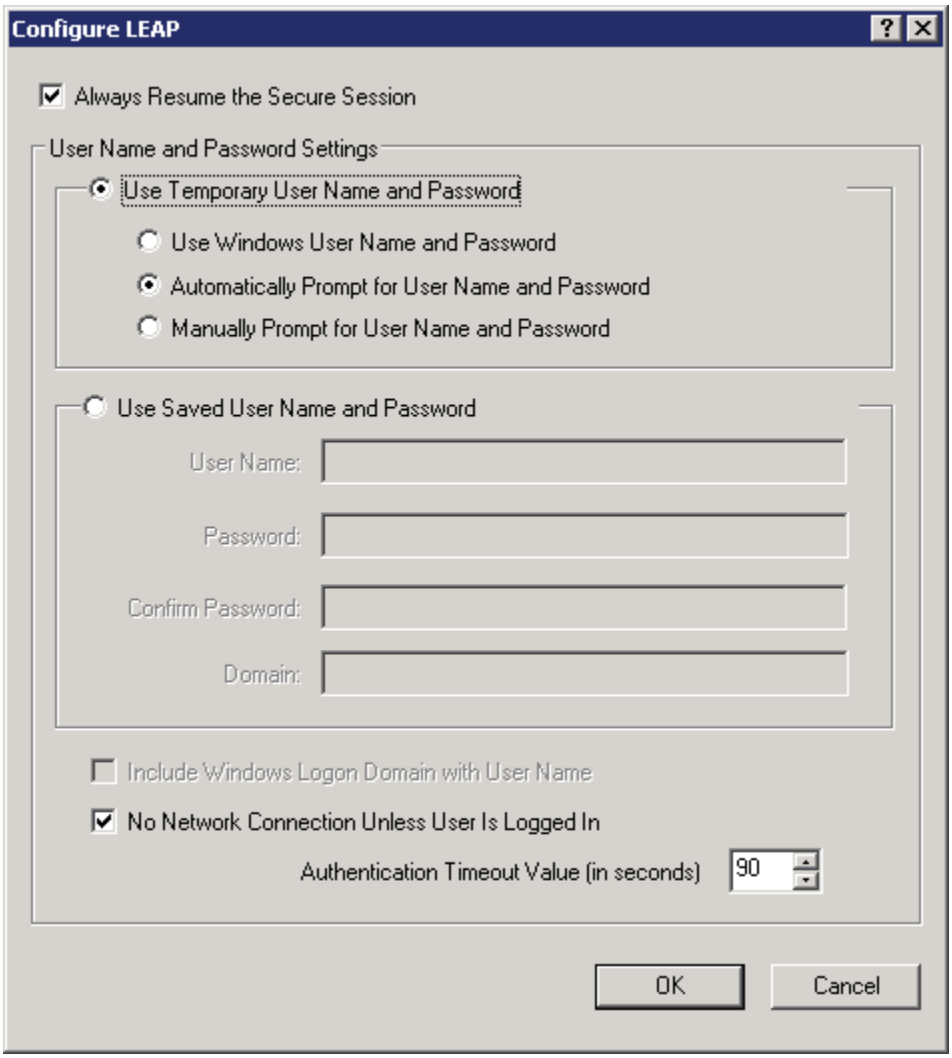
Configuring Profile Options and SSID

Under the **Security** tab, set the security type as **802.1x**. After selecting the security method, click **Configure**.



Wireless Security Options

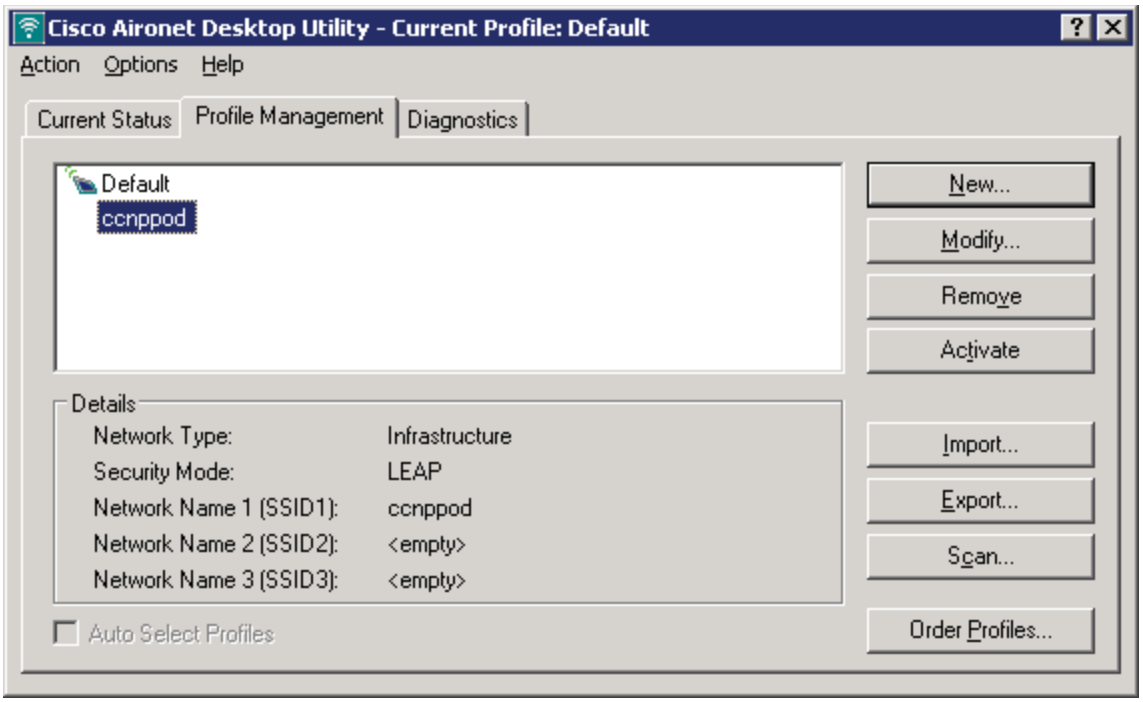
Choose **Automatically Prompt for User Name and Password** as the authentication setting. Click **OK** when done, and then click **OK** again to close the new profile window.



LEAP Configuration Options

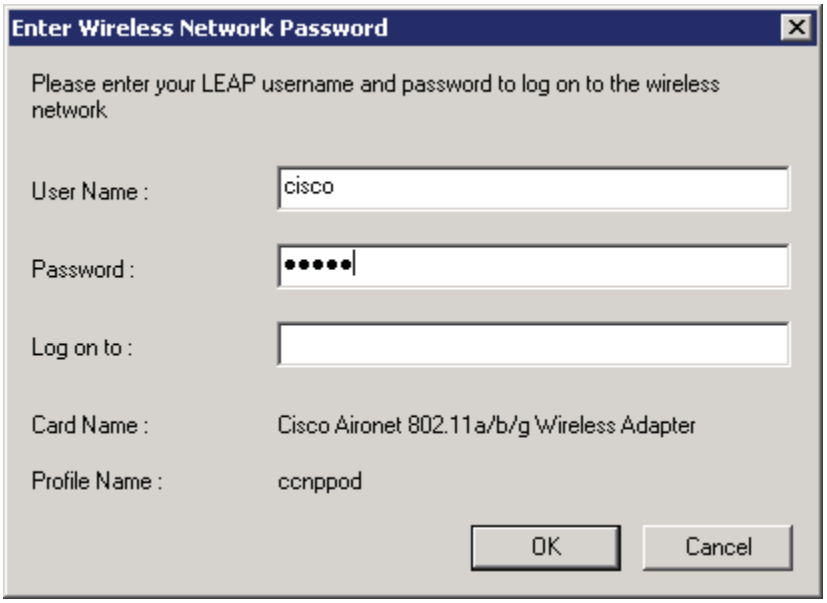
What security benefits are there to always prompt for the username/password?

On the profile list, select the new profile and click **Activate**.



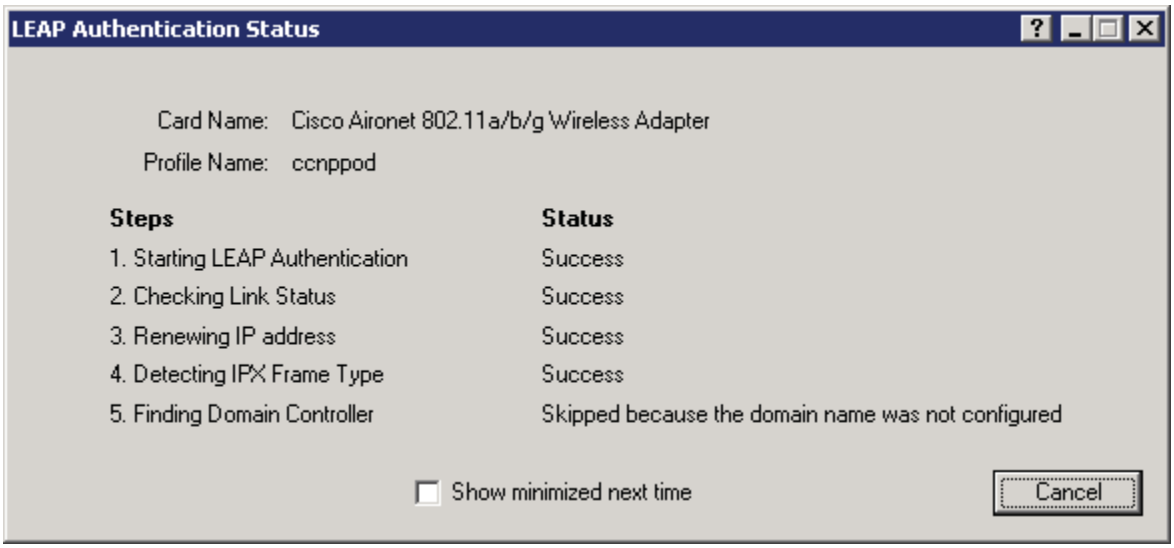
Selecting a Wireless Profile

When prompted to enter a username and password, enter in the credentials created earlier on the ACS server, and then click **OK**. (username and password of “cisco”).



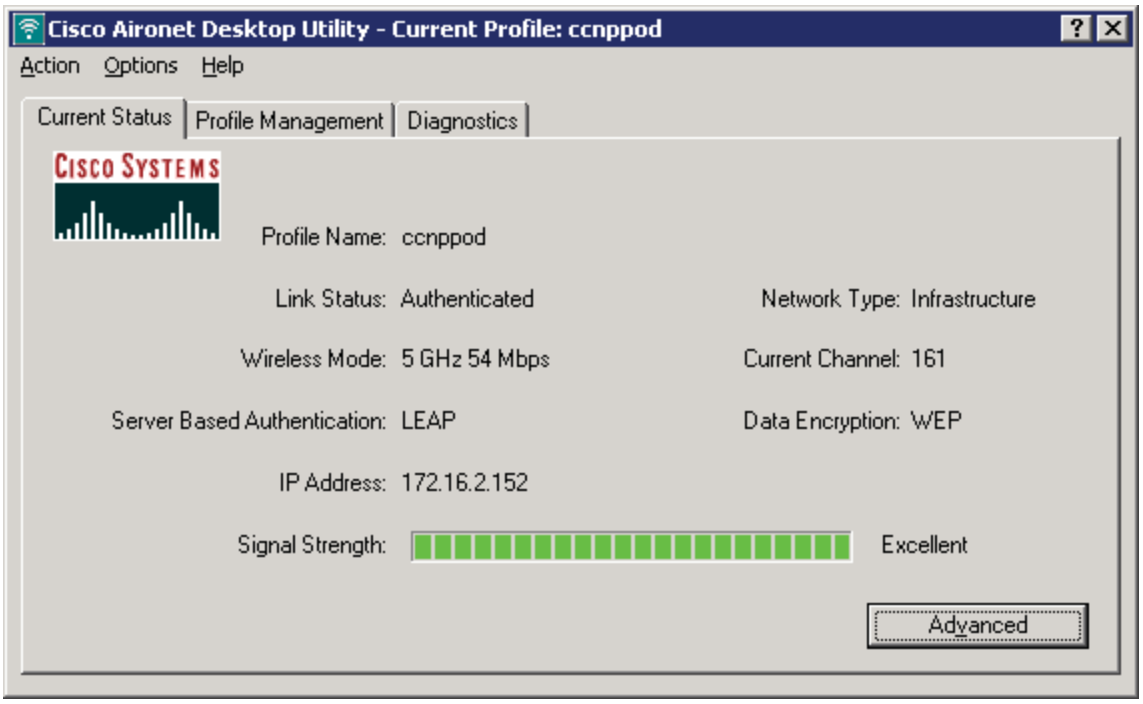
ADU LEAP Authentication Dialog

You should see all authentication steps be successful. If not, troubleshoot.



ADU LEAP Authentication Checklist

Under the **Current Status** tab, make sure you have received a correct IP address for the VLAN and the link is authenticated.



Current Wireless Profile Status

The client received the IP Address: 172.16.2.152. Which addresses in this network-range are excluded?