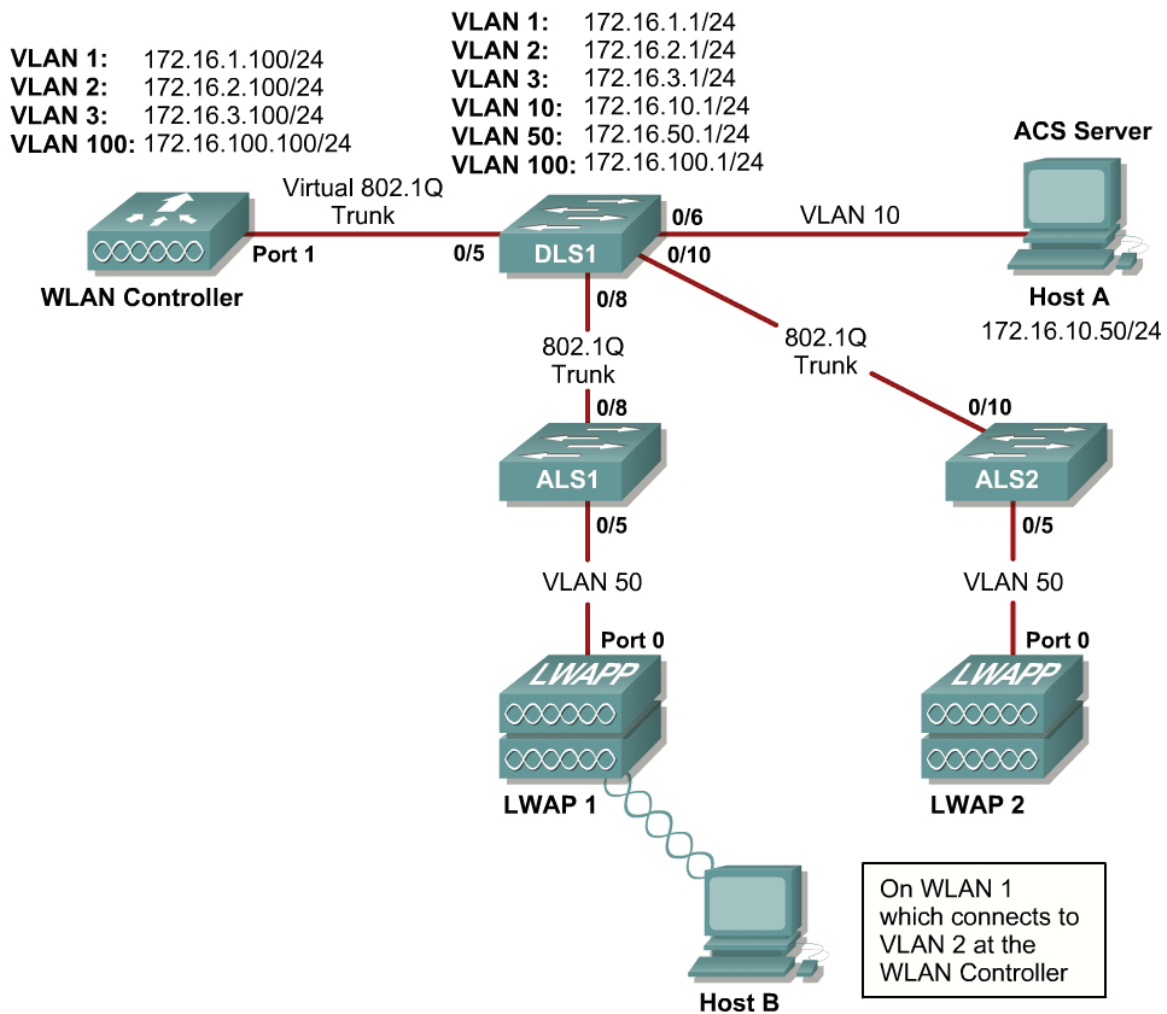


LAB: Configuring LEAP

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

CISCO SYSTEMS

Cisco Secure ACS v4.1

Select "Log Off" to end the administration session.

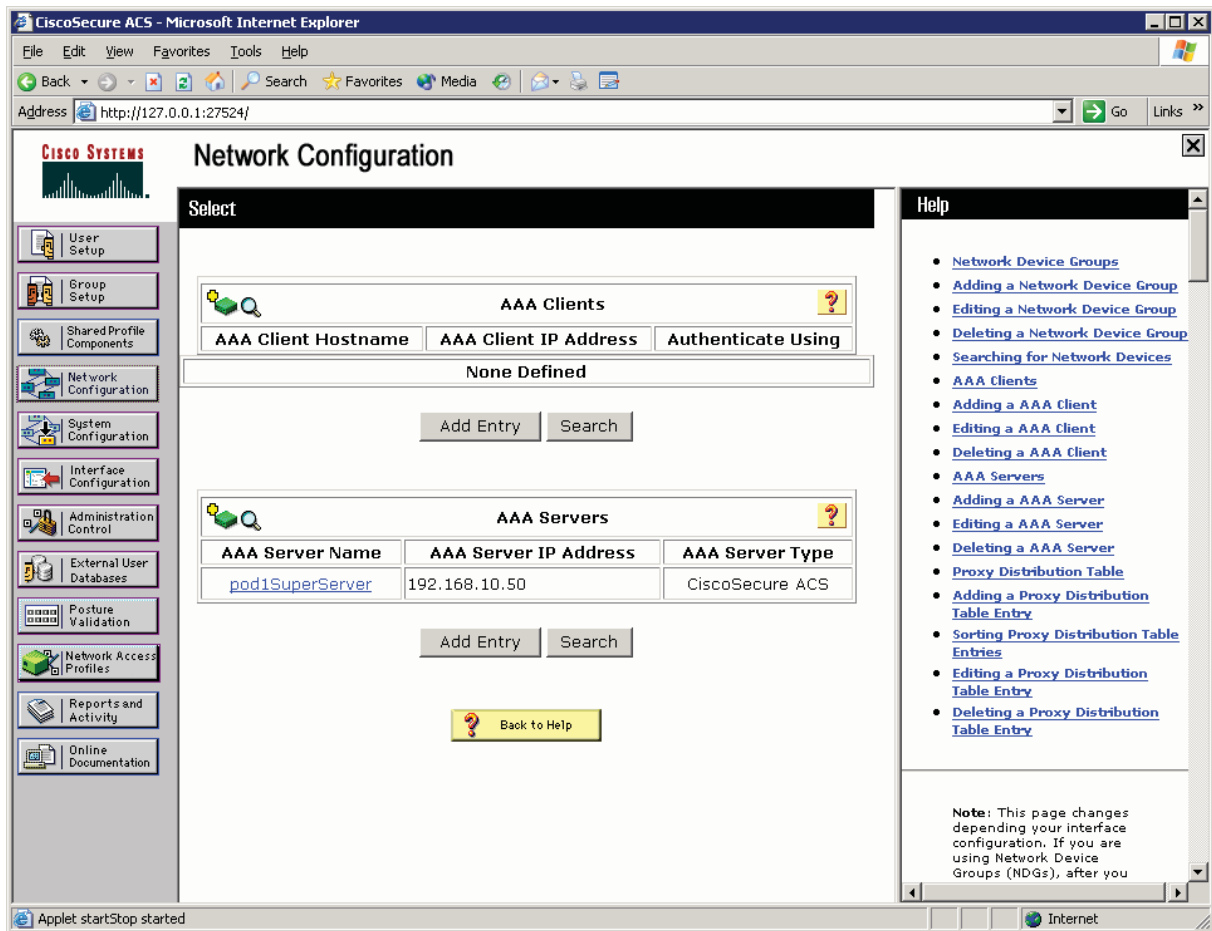
CiscoSecure ACS v4.1 offers support for multiple AAA Clients and advanced TACACS+ and RADIUS features. It also supports several methods of authorization, authentication, and accounting (AAA) including several one-time-password cards. For more information on CiscoSecure products and upgrades, please visit <http://www.cisco.com>.

CiscoSecure ACS Trial
Release 4.1(1) Build 23
Copyright ©2006 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective owners. Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Applet appPing started

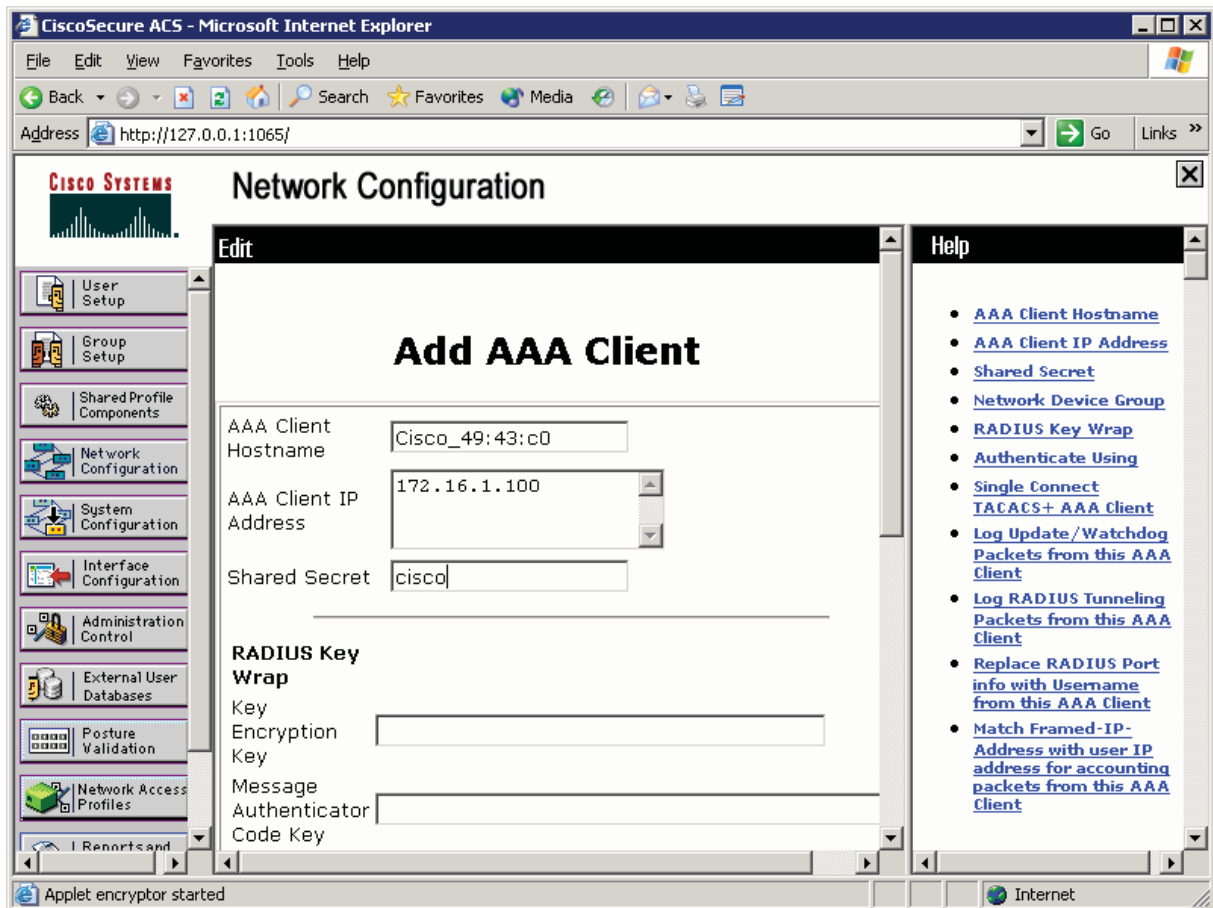
ACS Home Page

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.

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
Cisco 49:43:c0	172.16.1.100	RADIUS (Cisco Airespace)

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
pod1SuperServer	172.16.10.50	CiscoSecure ACS

Add Entry Search

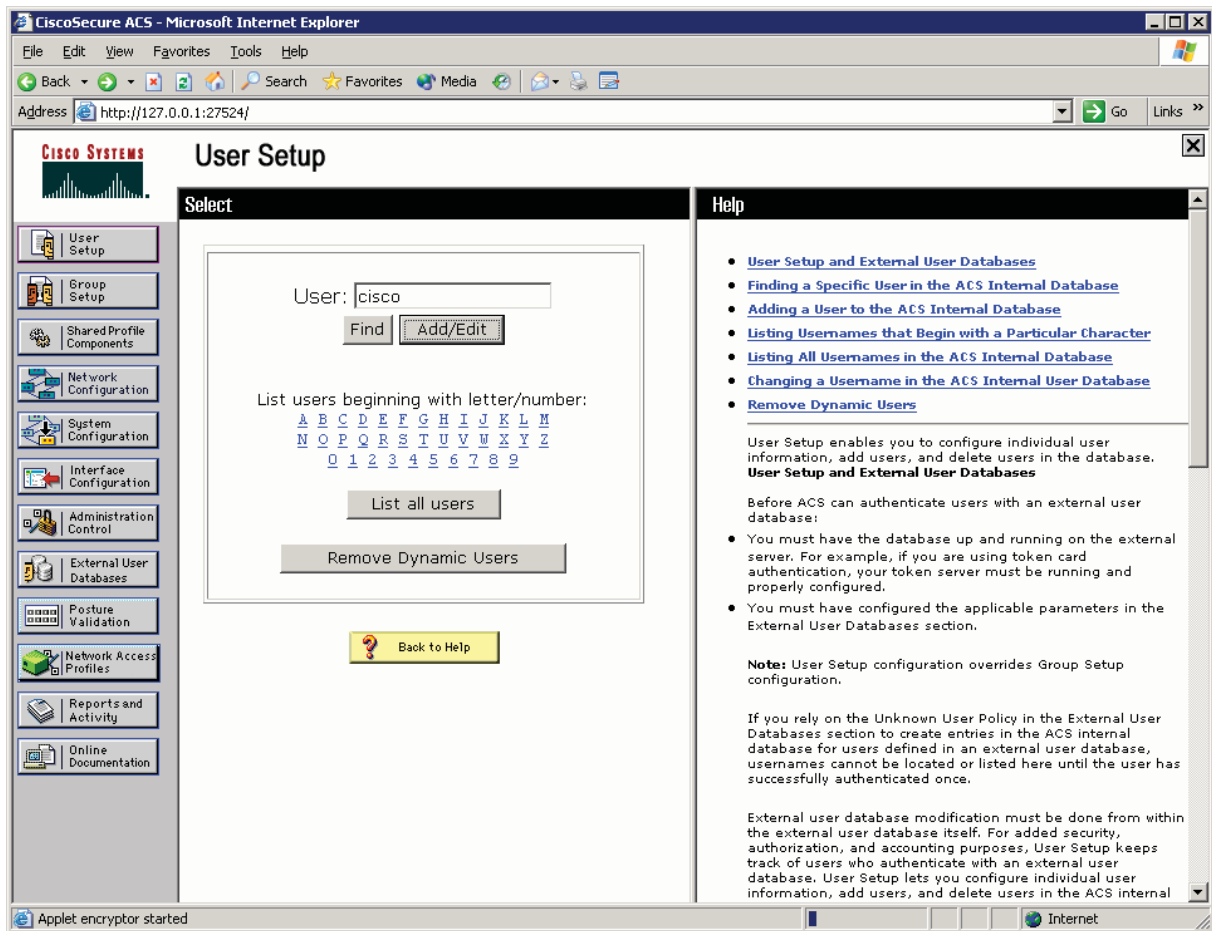
Help

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Editing a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [Searching for Network Devices](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)

Applet encryptor started Internet

ACS Network Configuration Page, with Changes Applied

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

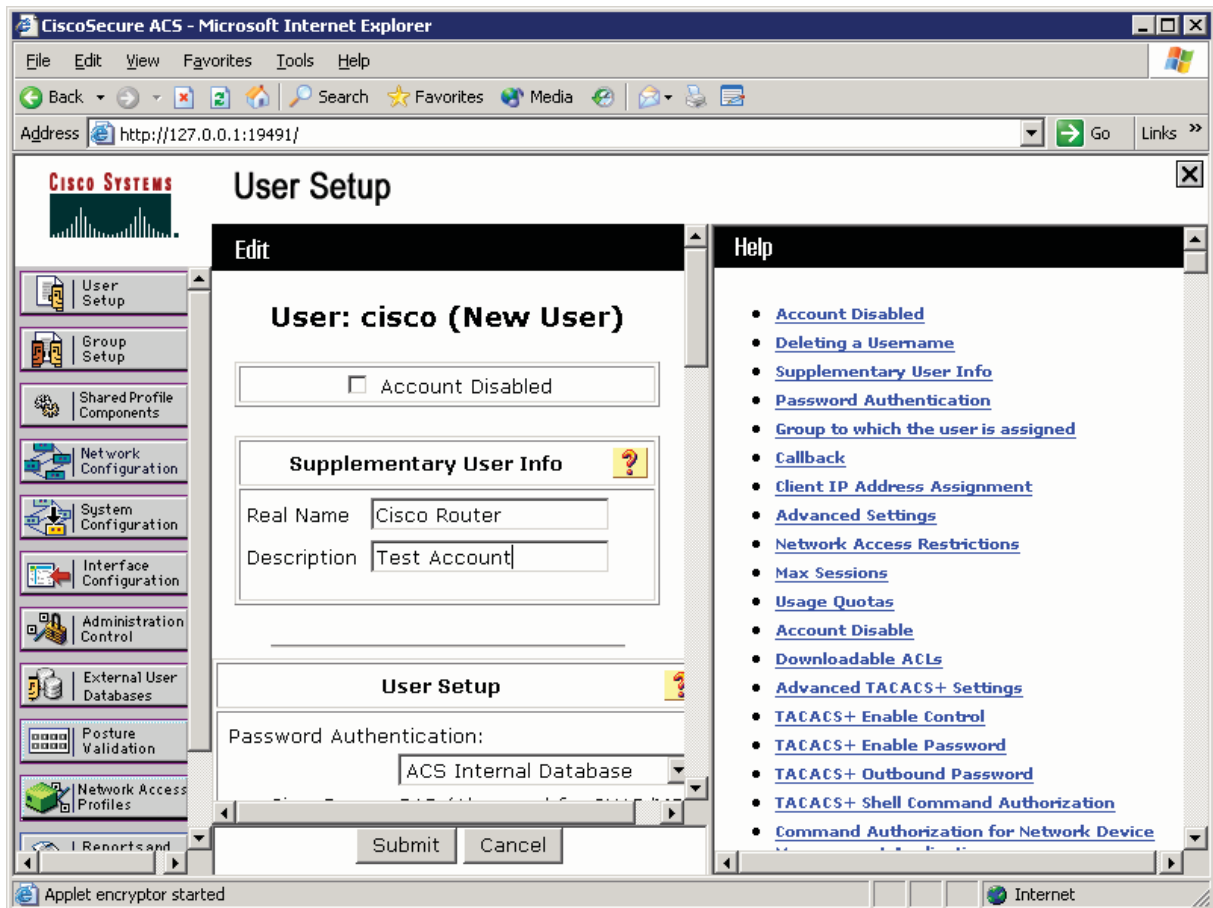


ACS User Configuration Page

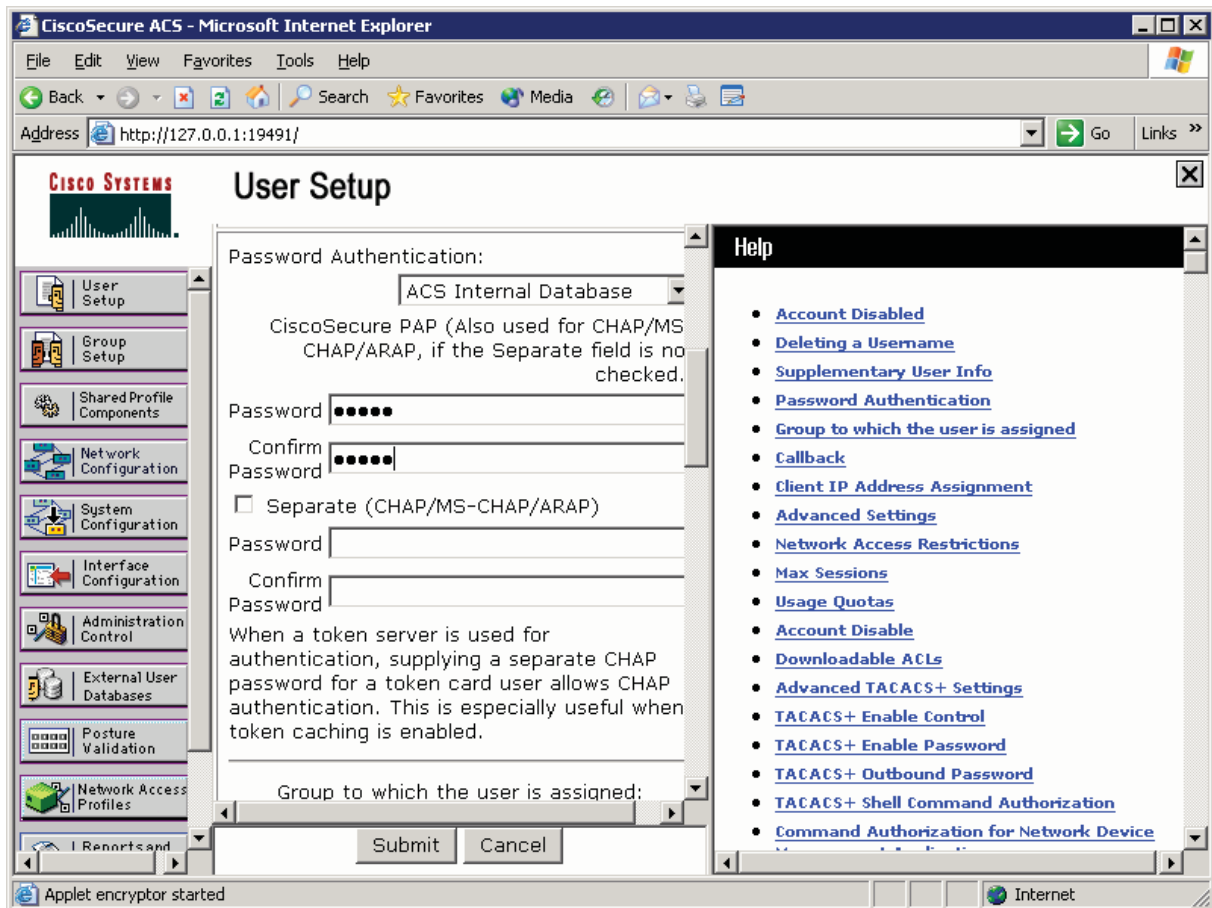
Assign “cisco” as the user name, and set “cisco” as the password. Click **Submit**.

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

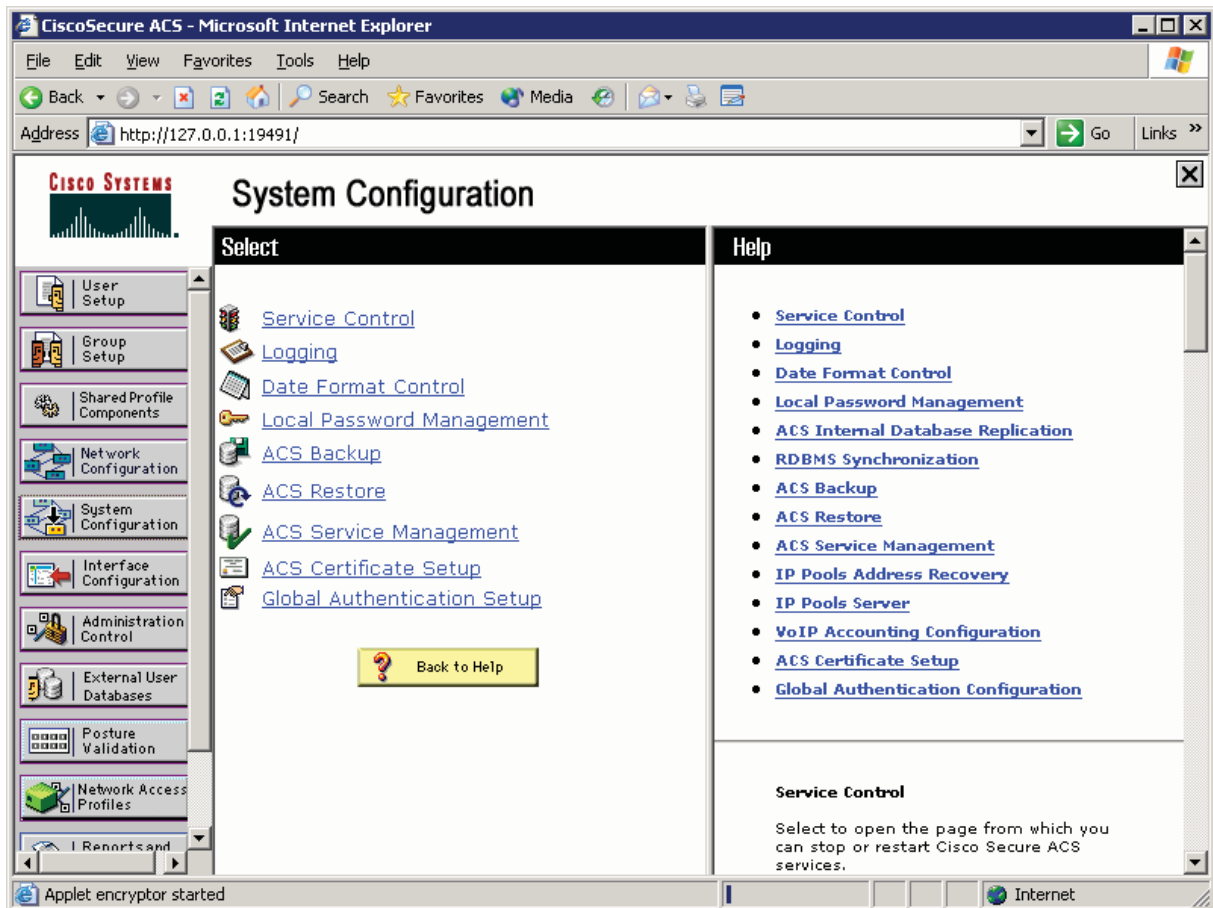


ACS User-level Password and Group Configuration

For what purpose will you use this user account?

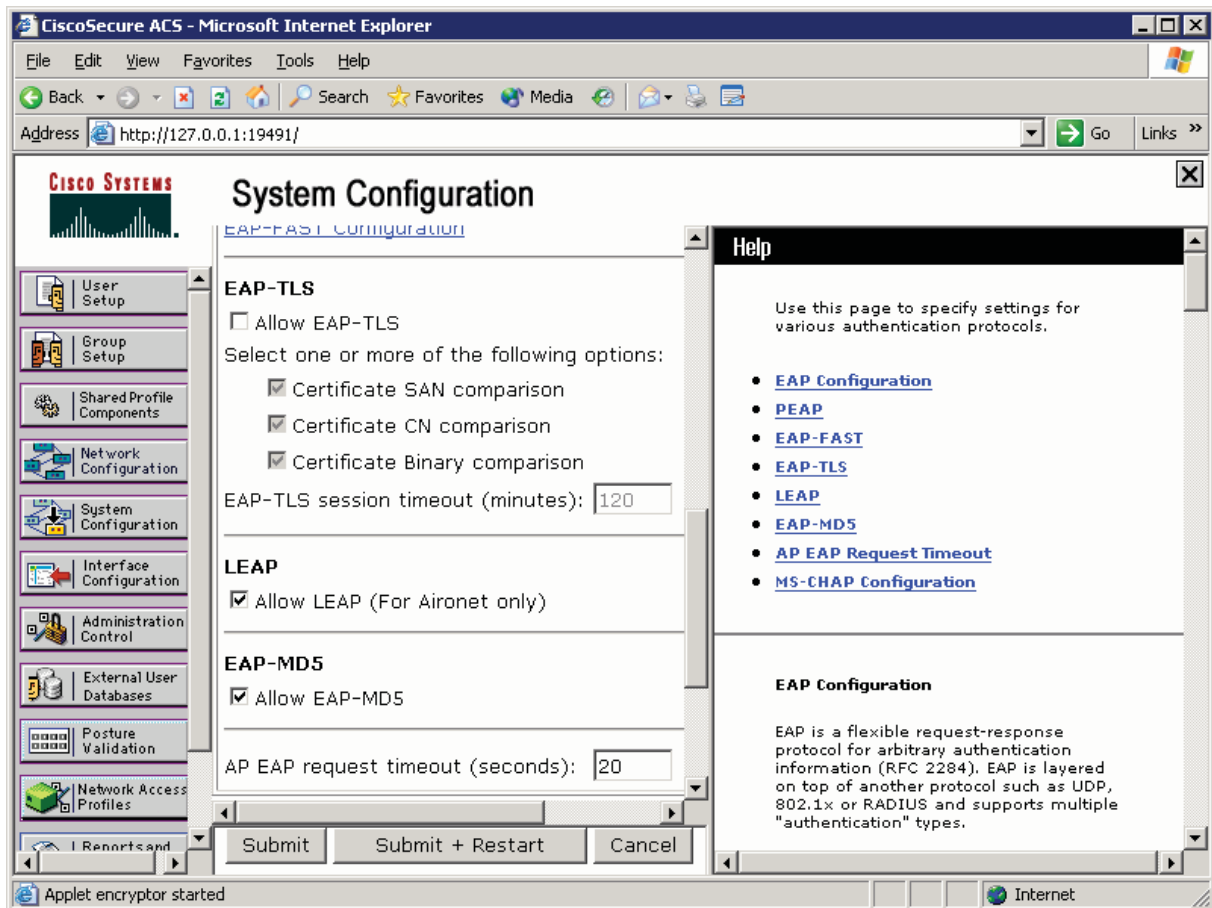
Although it should be enabled by default, we will make sure that LEAP authentication is enabled in ACS.

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.

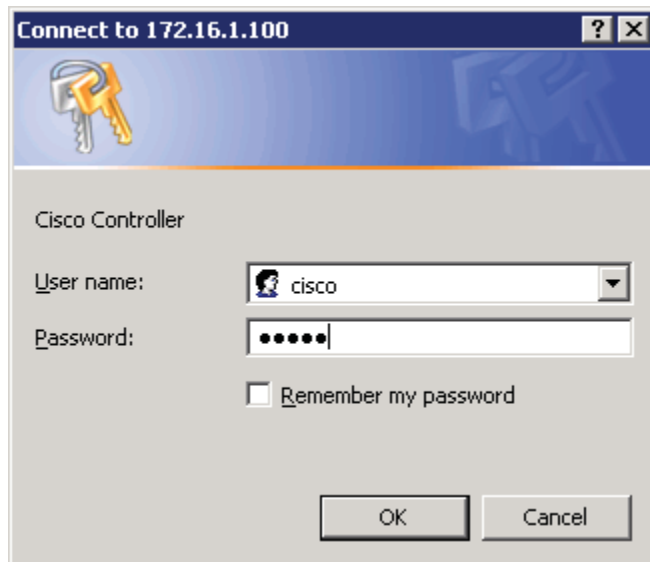
Lightweight Extensible Authentication Protocol, LEAP, is a Cisco proprietary wireless LAN authentication method. It has some well-known security issues. List a few.

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

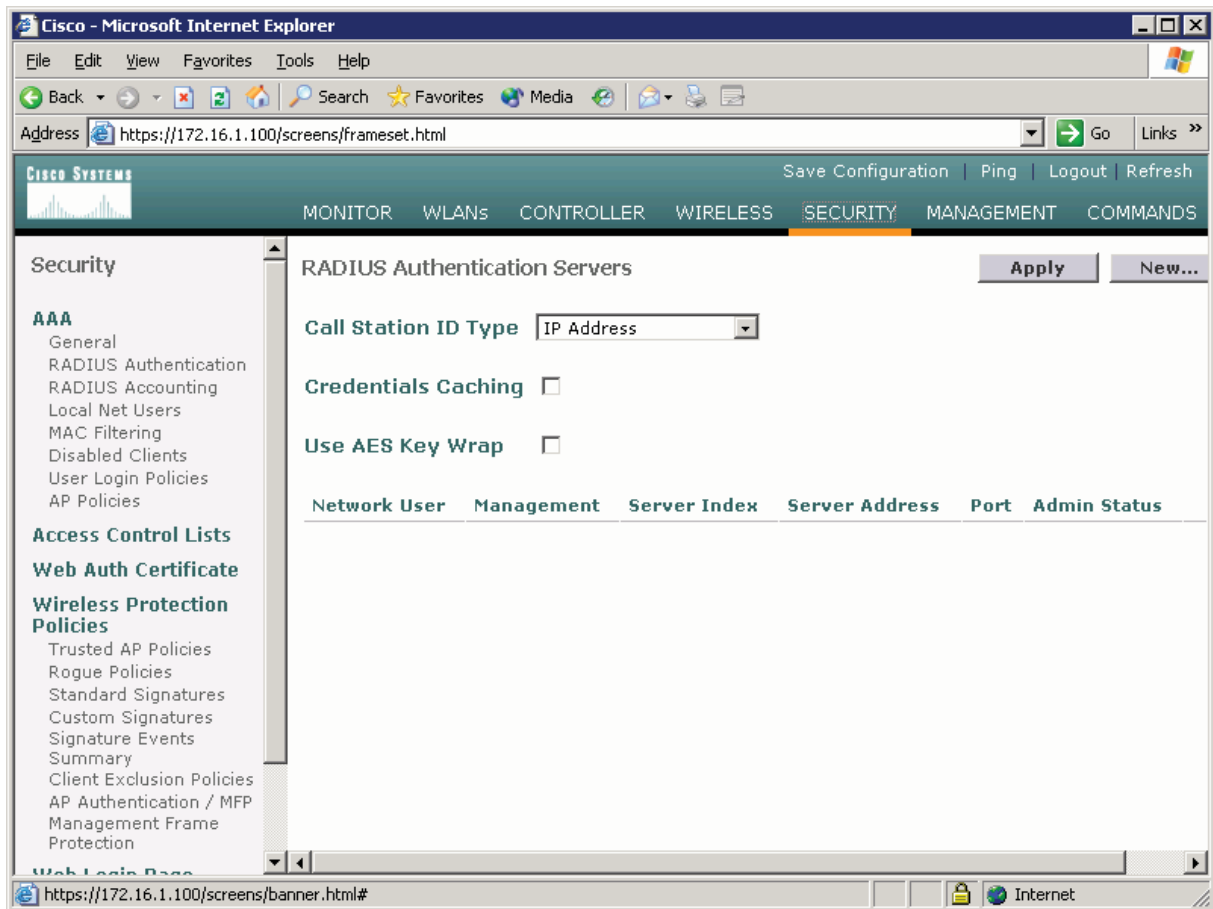
WLAN Controller Radius Server Configuration

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

Connect to the WLC from the Management Host

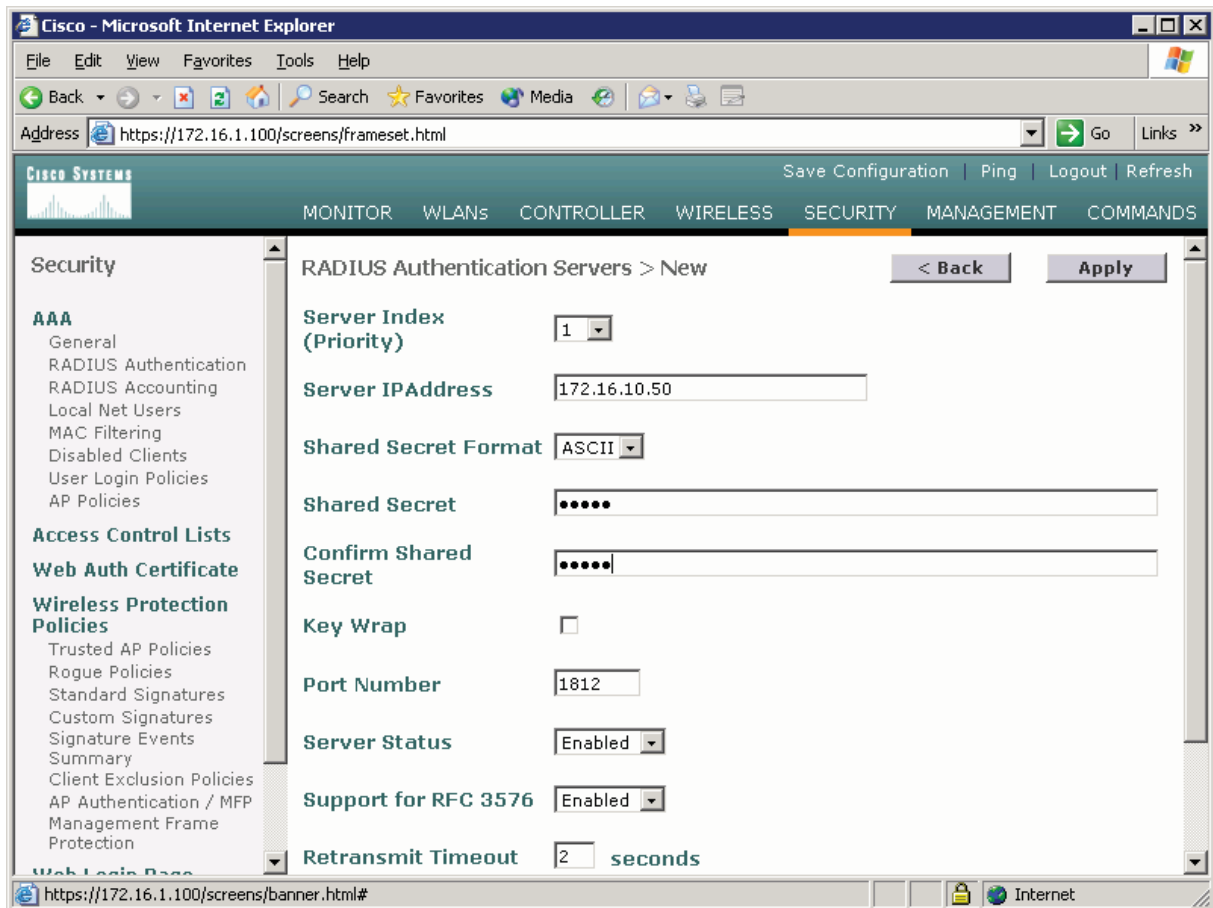


Click the **Security** link at the top of the WLC interface.



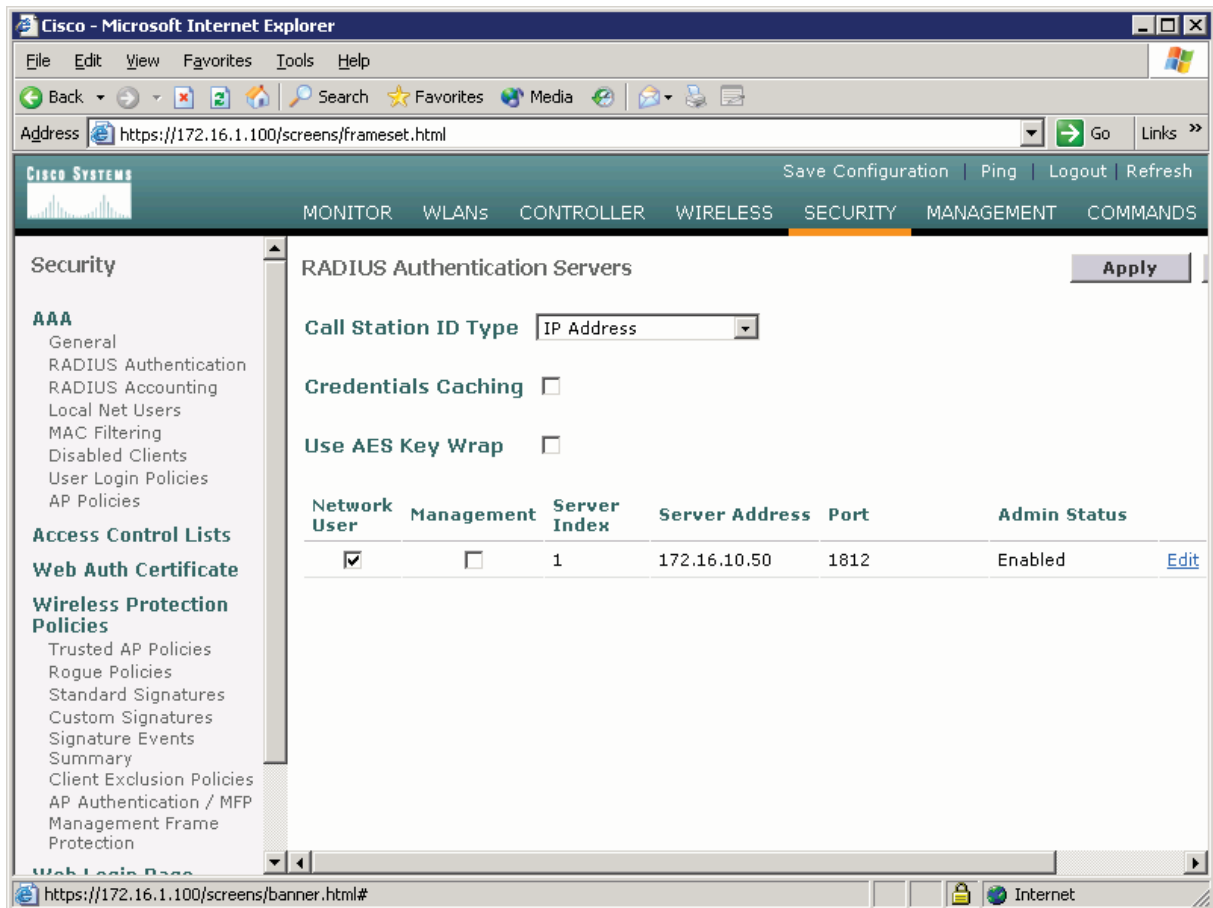
WLC RADIUS Server Configuration

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.

Cisco - Microsoft Internet Explorer

Address <https://172.16.1.100/screens/frameset.html> Go Links >>

CISCO SYSTEMS Save Configuration | Ping | Logout | Refresh

MONITOR WLANS **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS

Controller

General
Inventory
Interfaces
Internal DHCP Server
Mobility Management
 Mobility Groups
 Mobility Statistics
Ports
Master Controller Mode
Network Time Protocol
QoS Profiles

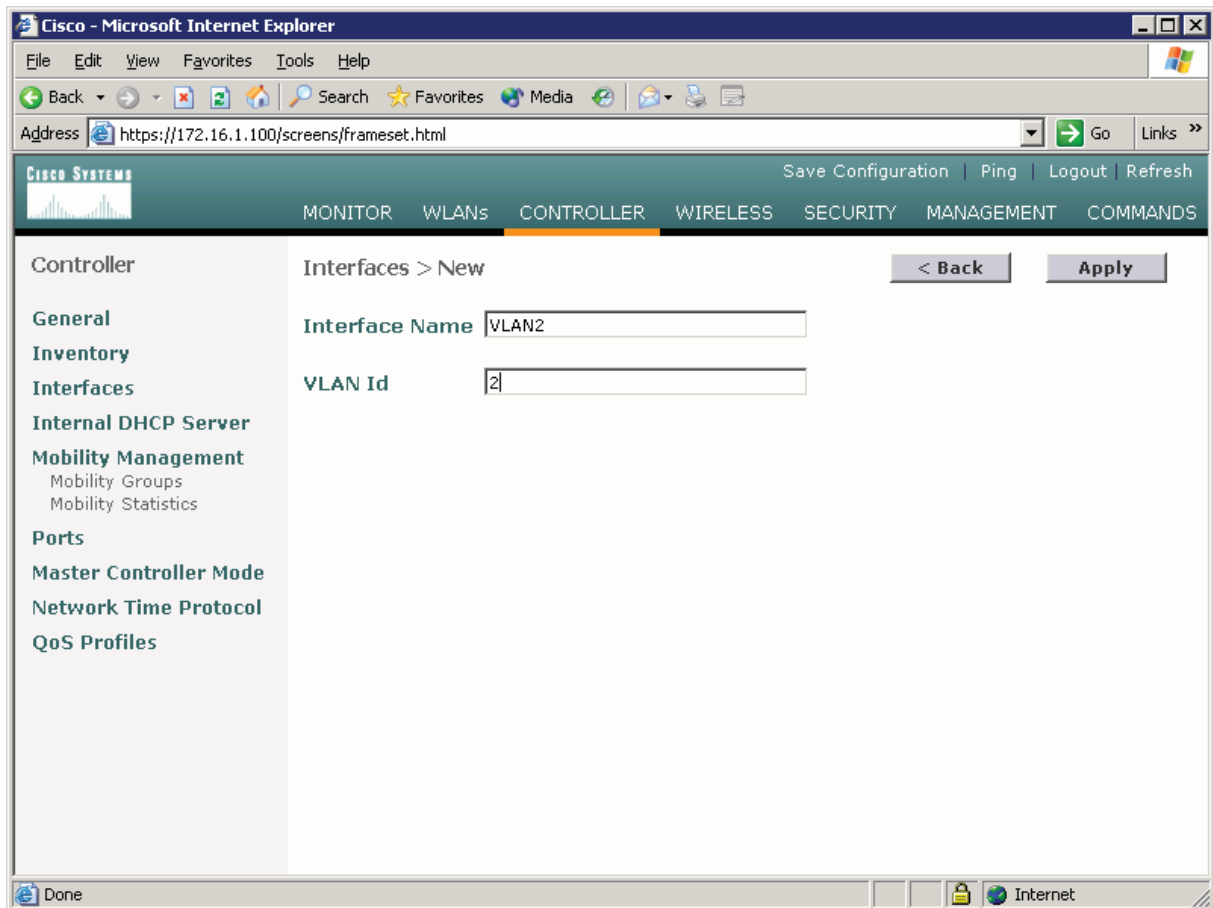
Interfaces New...

Interface Name	VLAN Identifier	IP Address	Interface Type
ap-manager	100	172.16.100.100	Static Edit
management	untagged	172.16.1.100	Static Edit
virtual	N/A	1.1.1.1	Static Edit

Done Internet

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.

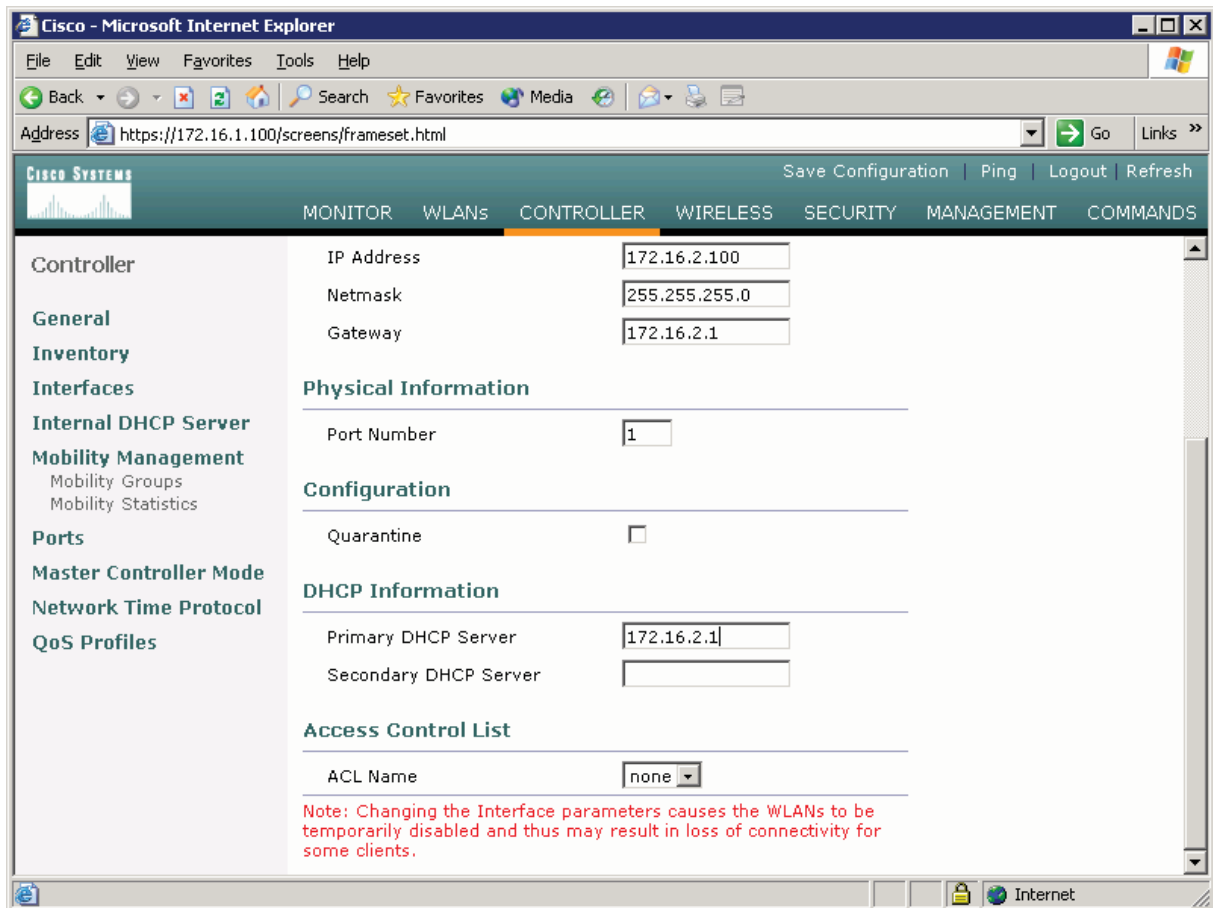


Creating a New VLAN Interface

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**.

The screenshot shows the Cisco Systems Controller configuration interface in Microsoft Internet Explorer. The browser's address bar displays `https://172.16.1.100/screens/frameset.html`. The Cisco Systems logo is in the top left, and navigation links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh' are in the top right. A menu bar contains 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS', with 'CONTROLLER' selected. A left sidebar lists configuration categories: 'Controller', 'General', 'Inventory', 'Interfaces', 'Internal DHCP Server', 'Mobility Management' (with sub-items 'Mobility Groups' and 'Mobility Statistics'), 'Ports', 'Master Controller Mode', 'Network Time Protocol', and 'QoS Profiles'. The main content area is titled 'Interfaces > Edit' and includes '< Back' and 'Apply' buttons. It is divided into sections: 'General Information' (Interface Name: VLAN2), 'Interface Address' (VLAN Identifier: 2, IP Address: 172.16.2.100, Netmask: 255.255.255.0, Gateway: 172.16.2.1), 'Physical Information' (Port Number: 1), 'Configuration' (Quarantine:), and 'DHCP Information'. The browser's status bar at the bottom shows `https://172.16.1.100/screens/frameSecurity.html` and an Internet icon.

Configuring VLAN Interface Properties



Configuring VLAN Interface Properties, DHCP Options

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

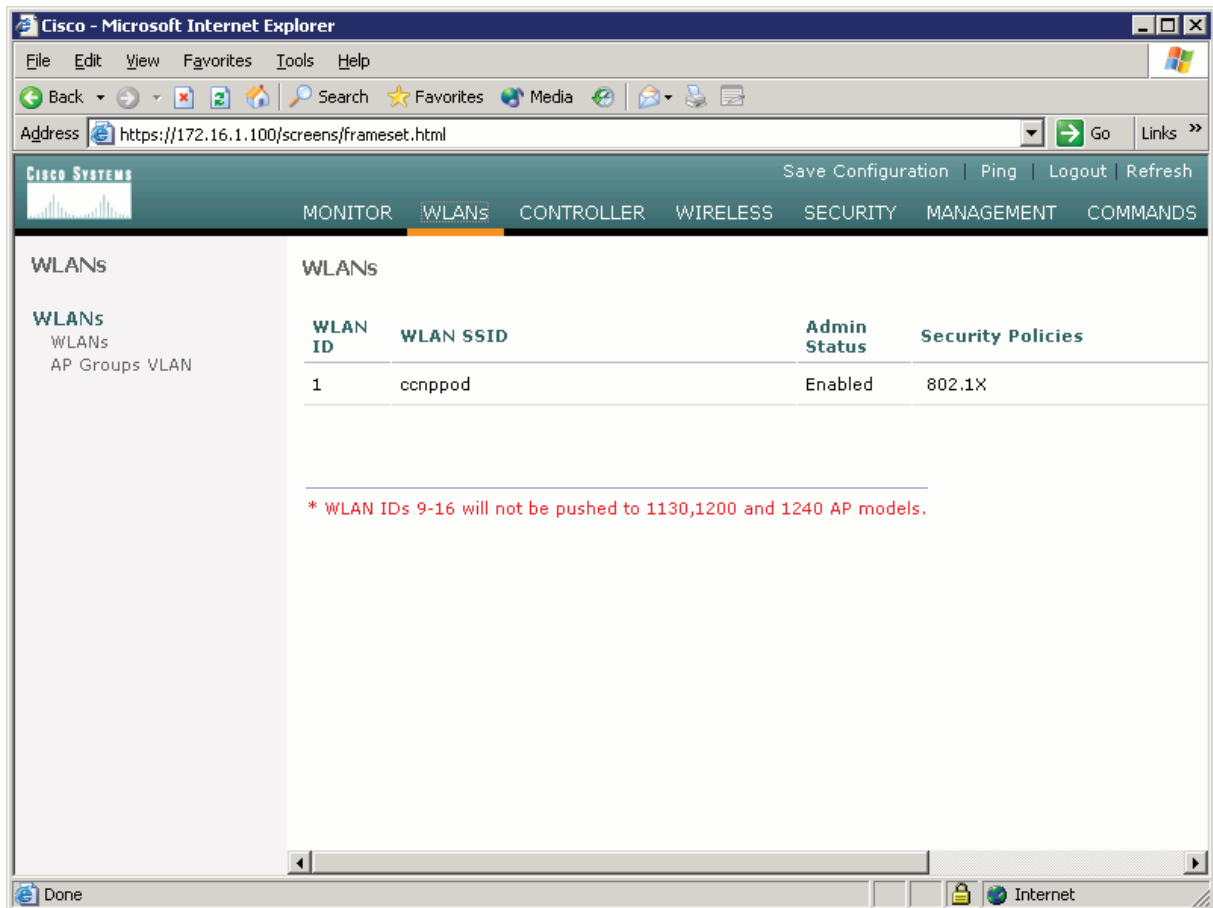
The new interface should appear in the interfaces list.

The screenshot shows the Cisco WLC web interface in Microsoft Internet Explorer. The browser address bar shows `https://172.16.1.100/screens/frameset.html`. The interface has a navigation menu at the top with options: MONITOR, WLANs, CONTROLLER (selected), WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. On the left is a sidebar with menu items: Controller, General, Inventory, Interfaces, Internal DHCP Server, Mobility Management (with sub-items: Mobility Groups, Mobility Statistics), Ports, Master Controller Mode, Network Time Protocol, and QoS Profiles. The main content area is titled 'Interfaces' and includes a 'New...' button. Below the title is a table with the following data:

Interface Name	VLAN Identifier	IP Address	Interface Type	
ap-manager	100	172.16.100.100	Static	Edit
management	untagged	172.16.1.100	Static	Edit
virtual	N/A	1.1.1.1	Static	Edit
vlan2	2	172.16.2.100	Dynamic	Edit Remove

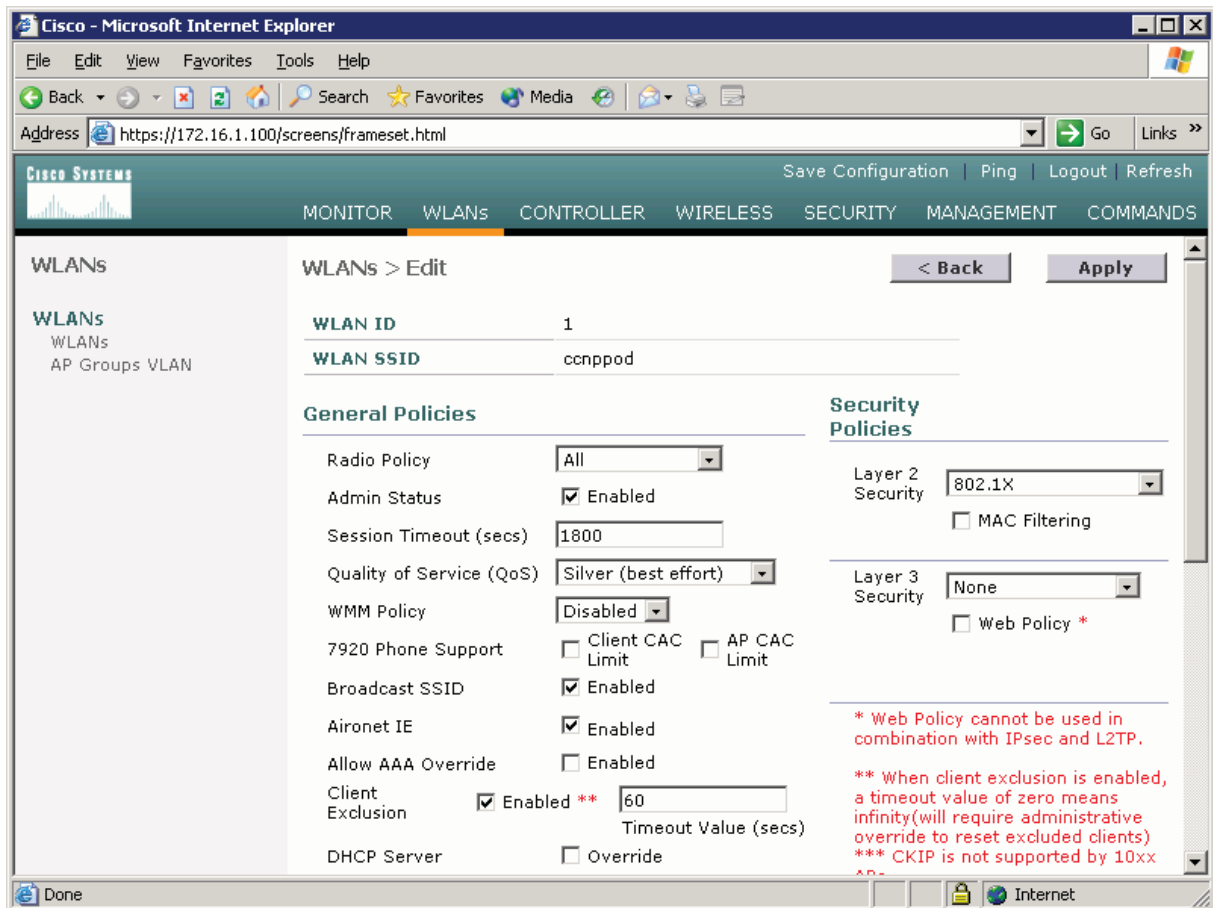
Verify Existing VLAN Interfaces

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?

Cisco - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://172.16.1.100/screens/frameset.html> Go Links >>

CISCO SYSTEMS Save Configuration | Ping | Logout | Refresh

MONITOR **WLANS** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS

WLANS

WLANS
 WLANS
 AP Groups VLAN

DHCP Server Override ***** CKIP is not supported by 10xx APs**

DHCP Addr. Assignment Required

Interface Name

MFP Version Required 1

MFP Signature Generation (Global MFP Disabled)

H-REAP Local Switching

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	<input type="text" value="IP:172.16.10.50, Port:1812"/>	<input type="text" value="none"/>
Server 2	<input type="text" value="none"/>	<input type="text" value="none"/>
Server 3	<input type="text" value="none"/>	<input type="text" value="none"/>

802.1X Parameters

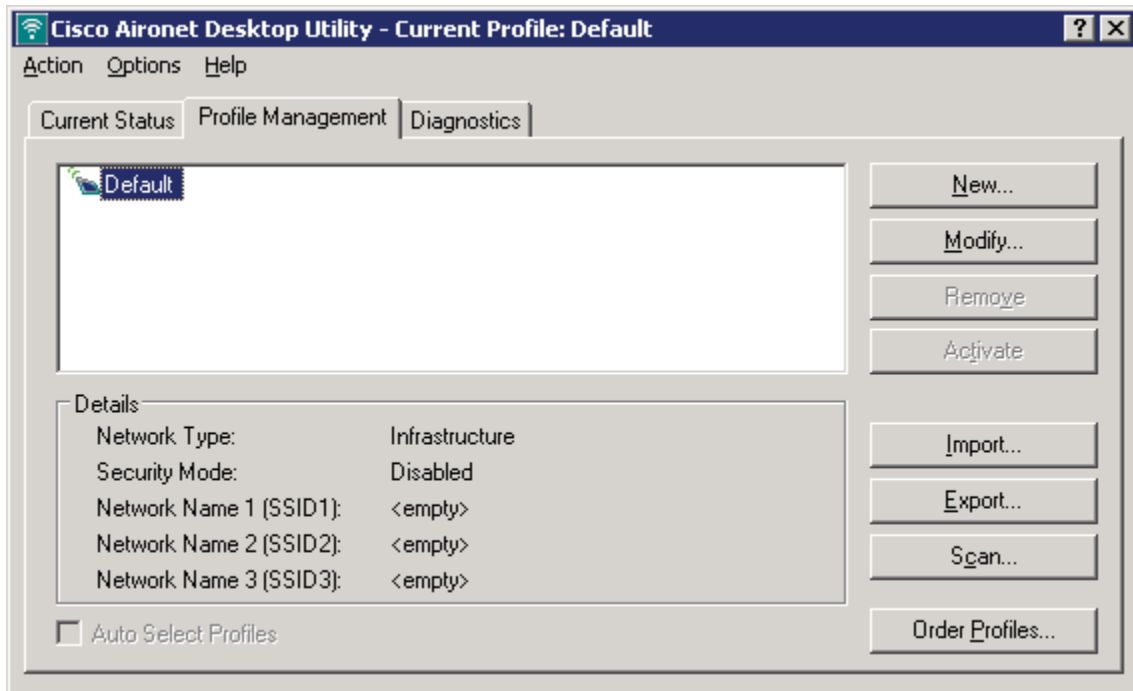
802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	<input type="text" value="104 bits"/>

<https://172.16.1.100/screens/frameSecurity.html> Internet

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.



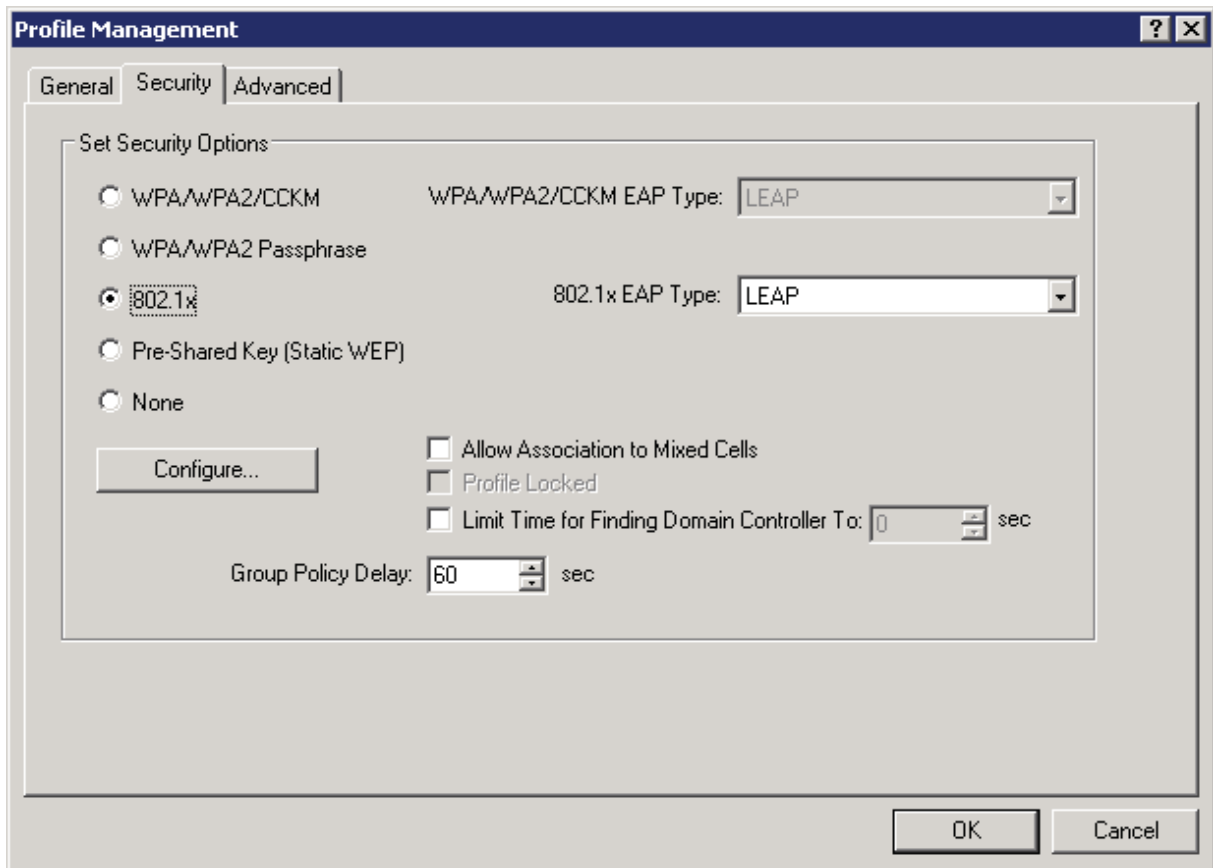
Cisco ADU Profile Management Tab

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.

The image shows a screenshot of a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'Security' tab is selected. The dialog is divided into two main sections: 'Profile Settings' and 'Network Names'. In the 'Profile Settings' section, there are two text input fields: 'Profile Name' containing 'ccnppod' and 'Client Name' containing 'cisco'. In the 'Network Names' section, there are three text input fields: 'SSID1' containing 'ccnppod', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons.

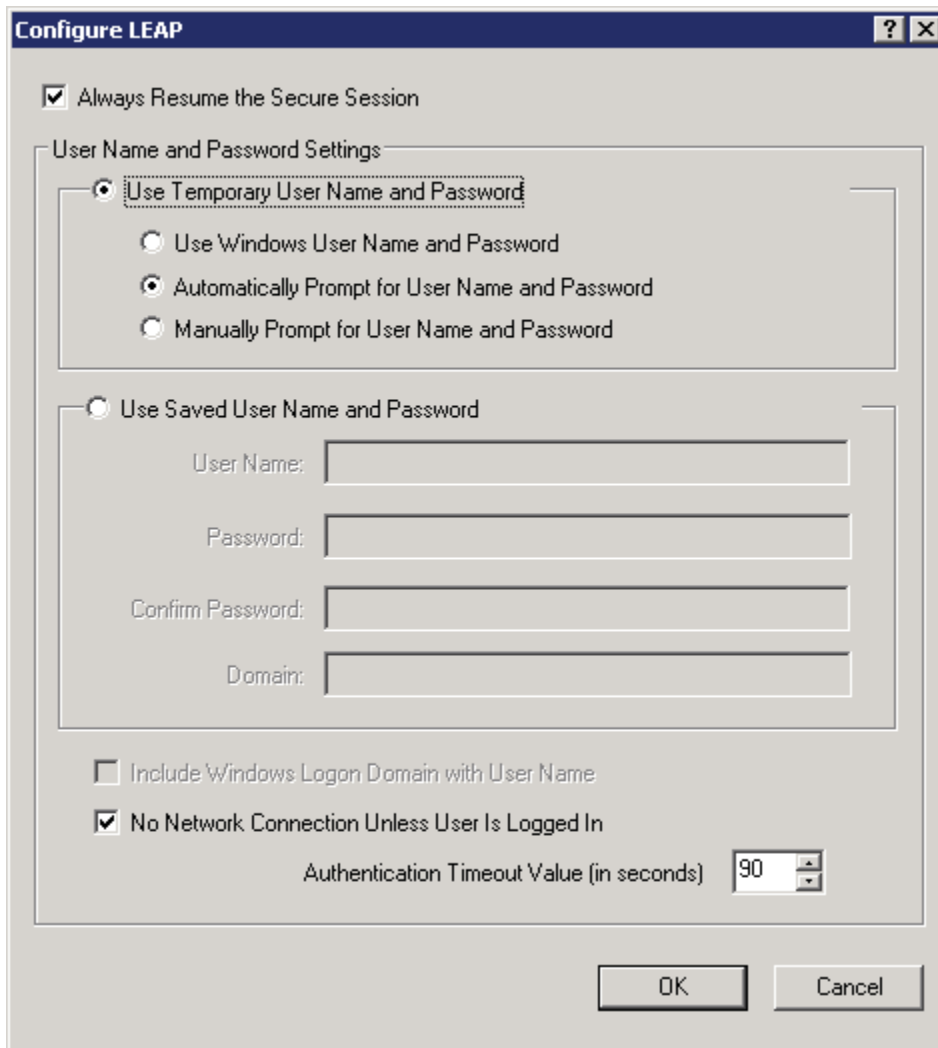
Configuring Profile Options and SSID

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



Wireless Security Options

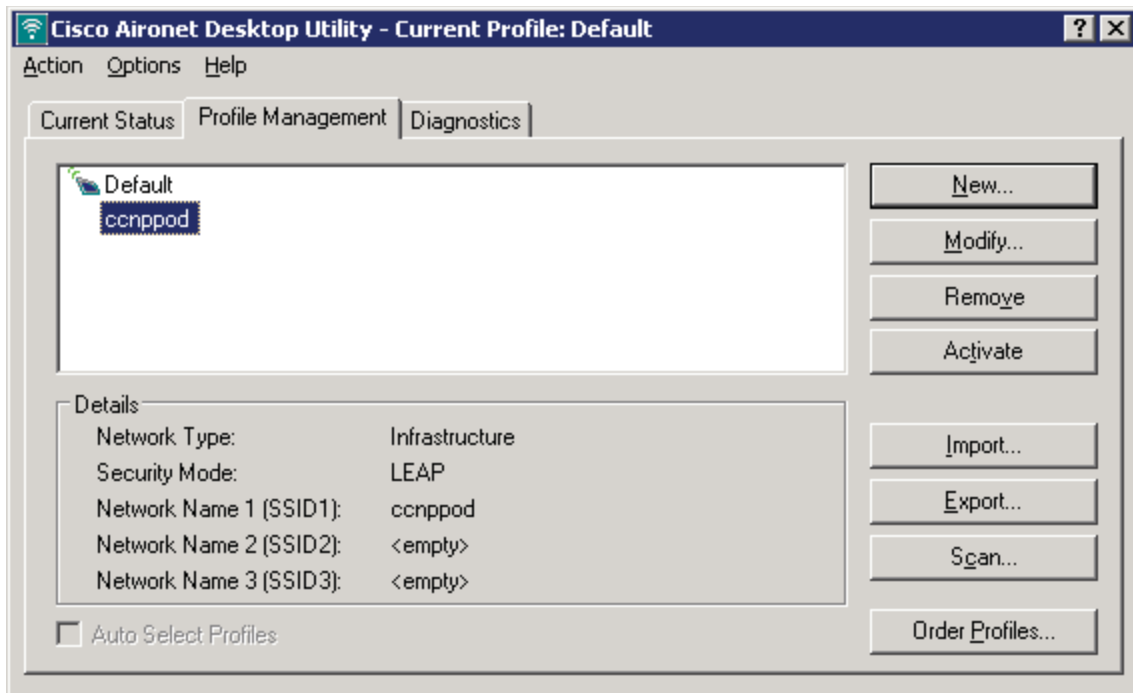
Choose **Automatically Prompt for User Name and Password** as the authentication setting. Click **OK** when done, and then click **OK** again to close the new profile window.



LEAP Configuration Options

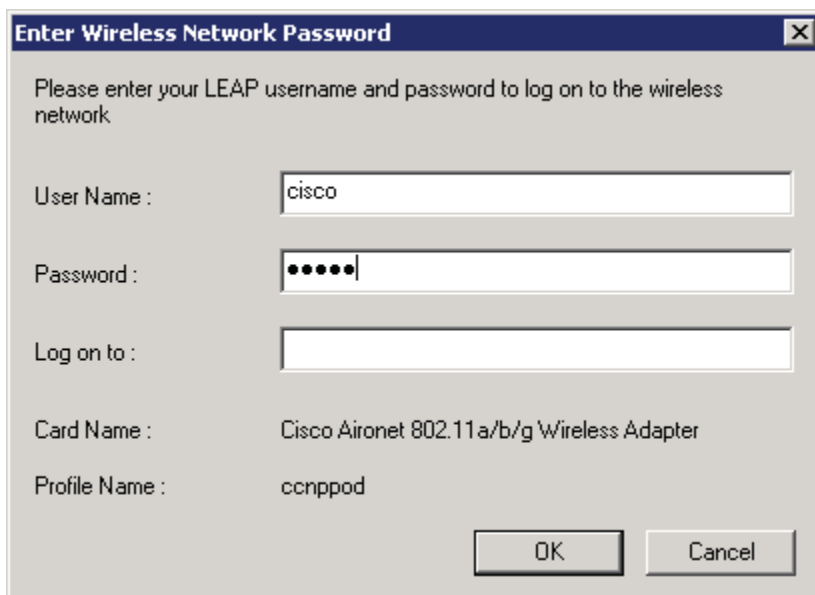
What security benefits are there to always prompt for the username/password?

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



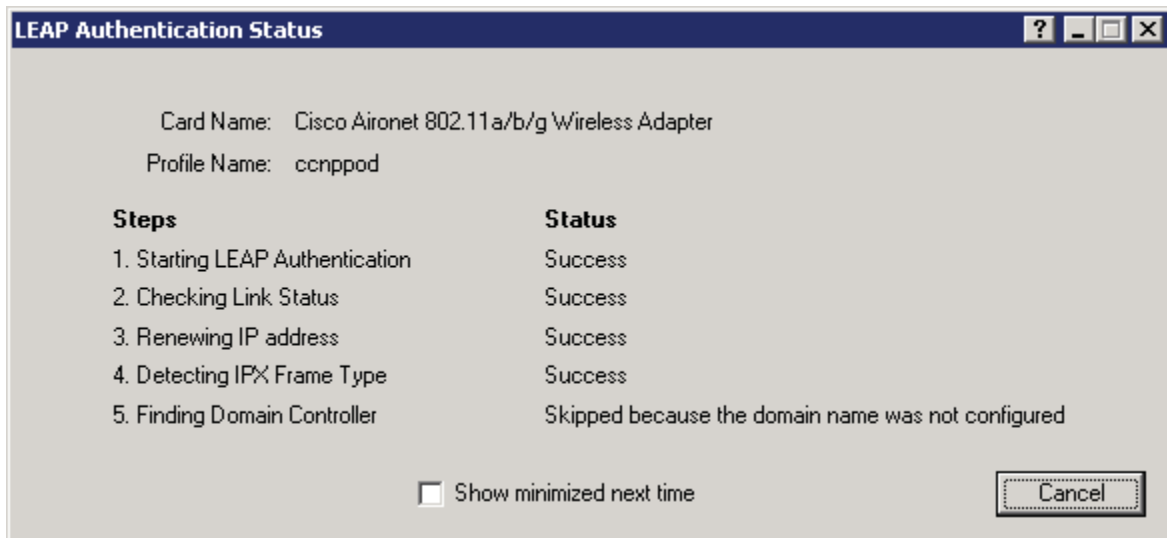
Selecting a Wireless Profile

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”).



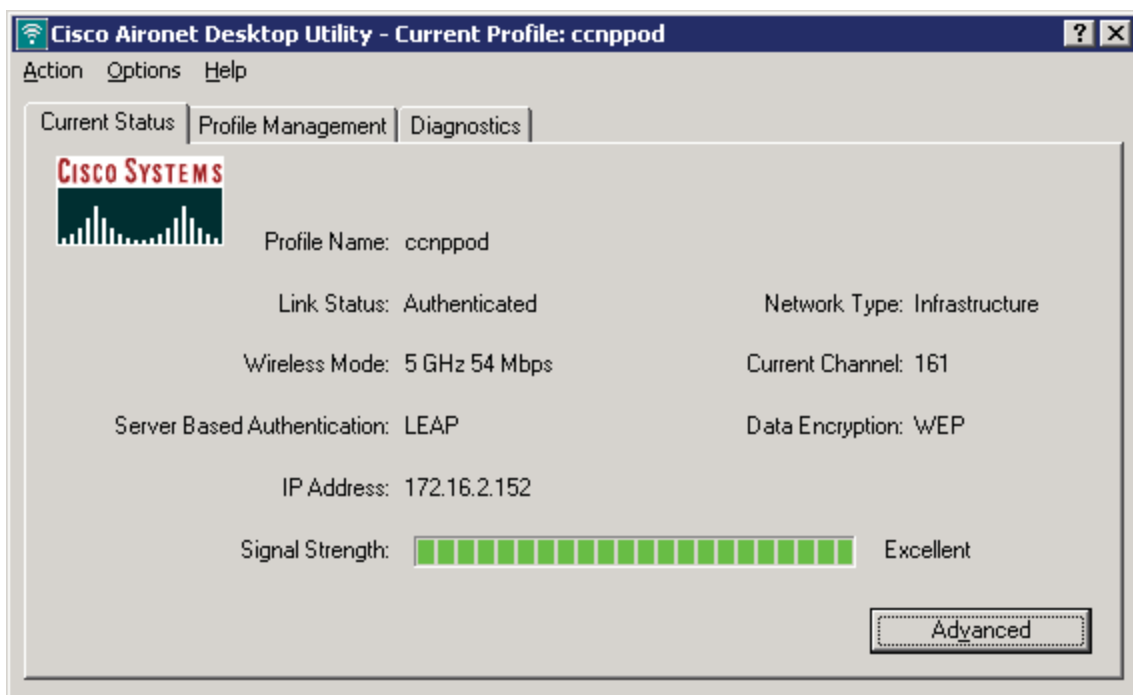
ADU LEAP Authentication Dialog

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?
