CISCO NETWORKING ACADEMY PROGRAM

Fundamentals of Wireless LANs

Student Lab Manual

Lab 1.2.7 Wireless Component and Media Identification

Estimated Time: 30 Minutes

Number of Team Members: 5 teams with 2 students per team

WLAN Networking Devices

Cisco Aironet 1200 Series Access Point
(802.11a and 802.11b)

Cisco Aironet Client Adapters

Cisco Aironet Antenna

Cisco Aironet 1400 Series
5 GHz Bridge
802.11a

Cisco Aironet 350 Series
2.4 GHz Bridge

802.11b

Objective

The following objectives will be covered in this lab

- Identify the basic media characteristics of wireless LANs
- Identify the components of a Wireless LAN
- Describe the functions of the Wireless components

Scenario

Wireless Local Area Networks (WLANs) have become a popular choice in network installations. Implementing a WLAN is simple because installation is generally limited to installing building mounted antennas and placing the access points (AP).

Local Area Networks (LANs) will quickly become a mixture of wired and wireless systems depending on the network needs and design constraints.

In larger enterprise networks, the core and distribution layers will continue as wired backbone systems. Enterprise systems are typically connected by fiber optics and unshielded twisted pair (UTP) cabling. Even in many smaller networks, there still remains a wired LAN at some level.

Preparation

The instructor will setup 4 equipment stations:

	Wireless	Wired
Station 1	AP(s)	Hub or Switch
Station 2	Bridge(s)	Fiber Optic, modem, WAN Switch
Station 3	Client Adapter(s)	Wired Ethernet NIC
Station 4	Antenna(s)	Ethernet Cable

The instructor will allow the students to examine the equipment and be able to compare the equipment to wired networking equipment.

The following tools and resources will be required to complete the lab:

- A conventional PCI and PCMCIA Network Interface Card(s) for wired networking connections
- Physical media such as UTP
- A conventional wired network hub or switch
- The Cisco Wireless course equipment bundle

Safety

Do not handle any wireless devices while they are powered. A general rule is to not touch or come within several inches of any powered antenna. Also, make sure to power down any device before removing a PCI or PCMCIA card. Most important, do not remove antennas from a Wireless AP or Bridge while powered. This can damage the unit.

Station 1 AP

The AP station contains at least one model of a wireless AP. Depending on the academy equipment inventory, there may be multiple models and vendors. There will also be some wired equivalent devices.

a. What models of Cisco APs are currently listed at cisco.com?

_____

b. What is the model of the AP at the station?

_____

c. What is the frequency range(s) of the AP provided?

_____

d. Does the AP have a detachable antenna or is the antenna built in?

_____

e. What wired ports are available?

_____

f. What is the wired equivalent to the AP that is located at station 1?

_____

g. What are the advantages and disadvantages of the wired and wireless access devices?

Device	Advantage	Disadvantage

h. Draw and label the appropriate icons for the AP, hub, and switch in the space below.

_____

Station 2 bridge

The bridge station contains at least one model of wireless bridge. Depending on the academy equipment inventory, there may be multiple models and vendors. There will also be some wired equivalent devices or media.

a. What models of Cisco bridges are currently listed at cisco.com?

_____

b. What is the model of the bridge at the station?

_____

c. What is the frequency range of the bridge provided?

_____

d. Does the bridge have a detachable antenna or is the antenna built in?

_____

e. What wired ports are available?

_____

f. What is the wired equivalent to the bridge that is located at station 2?

_____

g. What are the advantages and disadvantages of the wired and wireless bridge devices?

Device	**Advantage**	**Disadvantage**

h. Draw and label the appropriate icons for the bridge, modem, and serial line in the space below.

_____

Station 3 client adapters

The client adapter station contains several models of wired and wireless adapters. Depending on the academy equipment inventory, there may be multiple models and vendors. There will also be some wired equivalent devices.

a. What models of client adapters are currently listed at cisco.com?

_____

b. What are the models of the client adapters at the station?

_____

_____

_____

_____

c. Does the client adapter have a detachable antenna or is the antenna built in?

_____

d. What frequency range does the client adapter operate at?

_____

e. What is the wired equivalent to the wireless client adapter that is located at station 3?

_____

f. What are the advantages and disadvantages of the wired and wireless client adapter?

Device	Advantage	Disadvantage

g. Draw and label the appropriate icons for the client adapter in the space below.

_____

Station 4 antenna

The antenna station contains at least one antenna model. Depending on the academy equipment inventory, there may be multiple models and vendors. There will also be some wired equivalent devices or media.

a. What is the model of the antenna?

_____

b. What is the frequency range of the antenna provided?

_____

c. What is the wired equivalent to the antenna that is located at station 4?

_____

d. What are the advantages and disadvantages of the antenna devices?

Device	Advantage	Disadvantage

e. Draw and label the appropriate icons for the antenna, wireless signal, and Ethernet line in the space below.

_____

Lab 1.4.7 Wireless Lab Setup

Estimated Time: 30 minutes

Number of Team Members: Instructor led classroom demonstration

Objective

The following objectives will be covered in this lab:

- Learn the topologies for the basic WLAN design.
- Learn the topology in the basic metropolitan area design.

Scenario

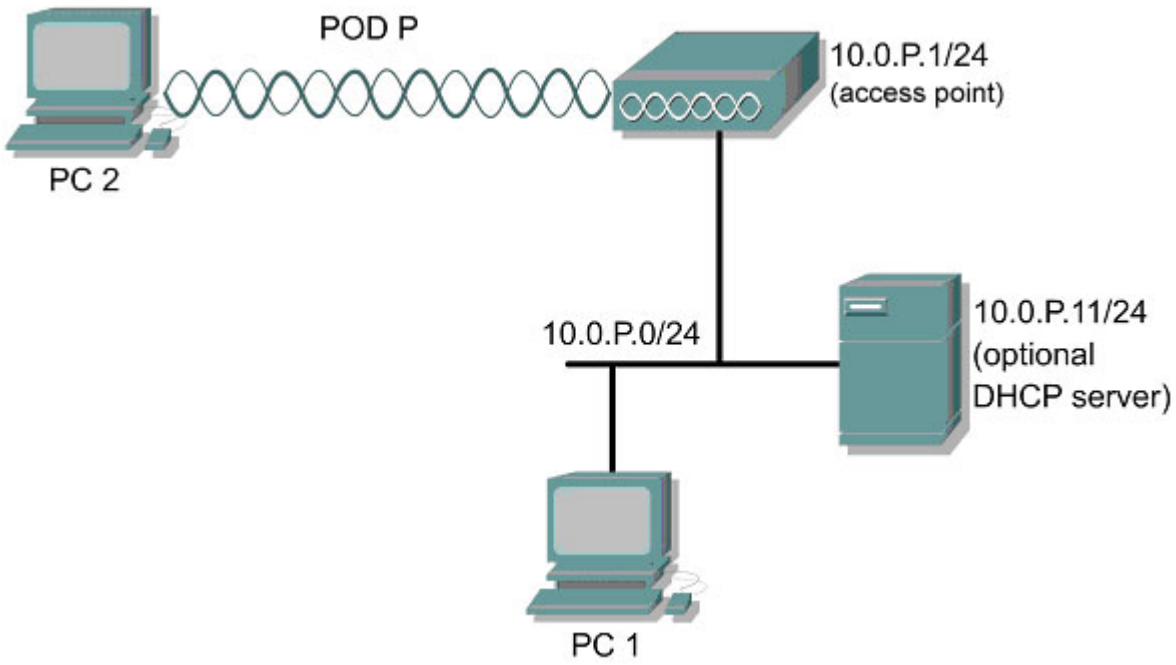
WLAN technology has two functions. First, WLAN can take the place of a traditional wired network. Second, WLAN can extend the reach and capabilities of a traditional wired network.

Much like wired LANs, in-building WLAN equipment consists of a Personal Computer Memory Card International Association (PCMCIA) card, a personal computer interface (PCI) or industry-standard architecture (ISA) client adapters, and wireless APs.

WLANS are also similar to wired LANs for small or temporary installations. A WLAN can be arranged in a peer-to-peer or ad hoc topology using only client adapters. For added functionality and range, APs can be incorporated to act as the center of a star topology or function as a bridge to an Ethernet network.

With a wireless bridge, networks located in buildings miles away from each other can be integrated into a single local-area network.

Topology



Preparation

The instructor will need at least one laptop computer, at least one desktop computer, and the equipment in the wireless course equipment bundle. The instructor should attempt to have as many wireless computers as possible, in order to display the concepts involved in the wireless network.

The following tools and resources will be needed for this lab:

- Wireless networking course equipment bundle
- Laptop computers with the PCMCIA NIC inserted
- Desktop computers with the PCI NIC inserted
- A switch or hub for a wired connection
- A computer to act as a server on the wired network

The instructor may compile any variety of equipment on the wired network to depict the wired network in a more realistic setting.

Step 1 Setup a basic WLAN

1. The instructor will have a variety of PCs or servers cabled into the wired network infrastructure without wireless devices.
2. The instructor will distribute the various computers with the wireless NICs around the classroom in a similar fashion to a basic WLAN topology.
3. The instructor will introduce one AP as the root hub in the classroom.
4. The instructor will introduce a cable from the AP to a switch connected to the wired network. The wired network is now being extended with the wireless AP to the various wireless clients that were assembled.

5. List the devices in this topology:

_____

_____

_____

_____

_____

_____

Step 2 Setup a site-to-site WLAN (Optional)

The instructor will introduce a second AP or bridge into the topology and will introduce the various antennas that can bridge wireless signals across to another building.

a. What type of antenna distributes wireless signals in all directions and can be used in a point–to–multipoint wireless bridge topology?

_____

_____

b. What type of antenna distributes wireless signals in one general direction and can be used in a point-to-point topology?

_____

_____

Lab 1.6.1 Challenges of Wireless Regulations

Estimated Time: 20 minutes

Number of Team Members: Each team will consist of two students

Objective

The student will learn the future direction and technologies associated to wireless regulations.

Scenario

There is continual development in wireless LAN (WLAN) technologies. One primary challenge is to conform to local, state, and national regulations related to wireless LAN emissions. Our focus is on Wireless emissions that occur in the 2.4 GHz and 5 GHz radio frequency spectrums. In this lab, each team will be assigned a topic to investigate.

Preparation

The instructor should compile a list of wireless regulatory bodies.

This lab will require a computer with a connection to the Internet for online research purposes.

The student teams should be encouraged to research resources such as trade publications, magazines, and vendor literature that are applicable to current and future trends in the area of wireless local area networks.

Step 1 Assign each team a regulatory agency to research

The research should include guidelines regulating the operation in both radio frequency spectrums (2.4 GHz and 5 GHz):

- United States (FCC)
- Europe (ETSI)
- Japan (JST)
- Australia/New Zealand (ANZ)
- Other

Team	Agency Assigned:
Team 1	
Team 2	
Team 3	
Team 4	
Team 5	
Team 6	

Step 2 Research sources

a. List at least three different web sites that were visited for the research information:

1. _____
2. _____
3. _____

Step 3 Presentations

a. Give a brief summary of the regulatory agencies researched.

_____

_____

b. What is the future trend of wireless this agency's regulations in the 2.4 GHz RF spectrums?

_____

_____

c. What is the future trend of wireless this agency's regulations in the 5 GHz RF spectrums?

_____

_____

d. How does this body differ from the others?

_____

_____

e. What officials comprise the regulatory agency or body?

_____

_____

f. How do companies comply with the regulations?

_____

_____

g. How do the regulatory agencies police the airwaves?

_____

_____

h. What action(s) do they take for violations?

_____

_____

i. What penalties are imposed for violations?

_____

_____

Lab 1.6.8 Challenges of Wireless Media

Estimated Time: 20 minutes

Number of Team Members: Each team will consist of two students

Objective

The student will research a topic involved with the future direction and technologies associated with wireless networking.

Scenario

There is continual development in the WLAN community. One emerging standard is 802.11g. 802.11g operates at higher speeds than 802.11b in the 2.4-GHz range. 802.11g, like 802.11a, supports Orthogonal Frequency Division Multiplexing (OFDM) modulation with speeds up to 54 Mbps. 802.11g is designed to be backwards compatible with 802.11b clients. If additional speed is needed, 802.11g may become a good choice. If the 2.4-GHz frequency is noisy at a given locale, 802.11a 5-GHz technology may be a better option.

Preparation

The instructor should compile a list of current trends in the area of Wireless Local Area Networking or use the topics given in step 1 of the lab.

This lab will require a computer with a connection to the Internet for online research purposes.

Utilize resources such as trade publications, magazines, and vendor literature that are applicable to current and future trends in the area of wireless local area networks.

Step 1 Assign each group a specific topic from the list below to research

- WLAN security
- WLAN frequency ranges
- WLAN devices
- WLAN connection speeds
- WLAN applications
- WLAN vendors

Team	Topic Assigned:
Team 1	
Team 2	
Team 3	
Team 4	
Team 5	
Team 6	

Step 2 Research sources

1. List at least three different web sites that were visited for the research information:

_____

_____

_____

Step 3 Presentations

a. Give a brief summary of the Wireless Local Area Networking topic researched.

_____

_____

_____

b. What is the future trend of this topic for Wireless Local Area Networking?

_____

_____

_____

c. What companies are involved in the development of the wireless networking topic?

_____

_____

_____

d. Is there an IEEE standard for the topic researched? If so, what is it?

_____

_____

_____

Lab 2.4.3 Install a WLAN Adapter Card

Estimated Time: 15 Minutes

Number of Team Members: six teams with two students per team

Objective

The student will learn the procedures for installing the client adapter in the PC for wireless networking.

Scenario

Install a wireless LAN adapter (WLAN) card in a laptop, desktop, or both.

Preparation

This lab will require the following materials:

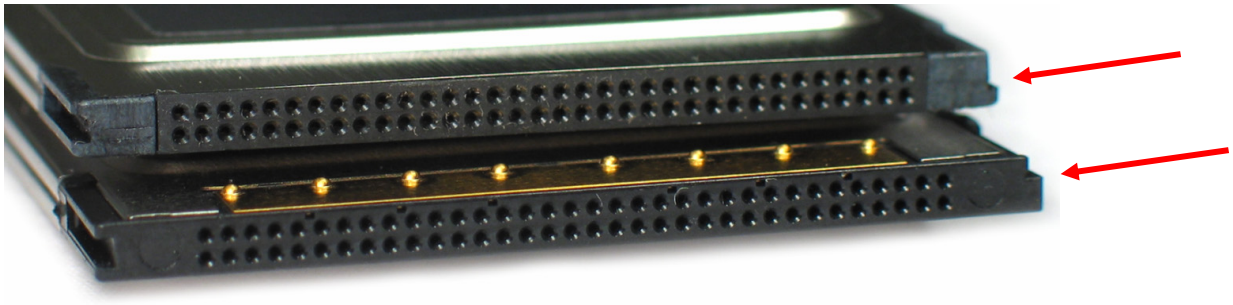
- Desktop or Laptop PC
- One Cisco Aironet PCI352, CB20A, or PCM 352 Client Adapter Network Interface Card.
- One PC installed with a Microsoft Operating System
- One Screwdriver for PCI card installation
- Instructor should preconfigure SSIDs on the APs and determine the IP addresses needed for the PCs or laptop computers that are used in this lab

Step 1 Installing the client adapter card in a laptop

Before installing a new adapter card into the laptop, the laptop may need to have an integrated wireless NIC disabled. To disable an integrated wireless NIC, click on the **Start** button and select the **Control Panel** option. If in Classic View, select **Network Connections** or the appropriate Network Control panel. If in Category View, select the **Network and Internet Connections** category and select **Network Connections**. Right-click on the integrated wireless adapter and select **Disable**.

Note When inserting a wireless NIC into a laptop, the power can be on or off.

Insert the Cisco Aironet PCM 352 Client Adapter into the PCMCIA slot. The CB20A installs into the Laptop PC cardbus slot. A CardBus adapter will not fit completely into a PCMCIA laptop slot. This may be a problem on older laptops. A PCMCIA adapter, however, will fit in a PCMCIA slot or a CardBus slot. Below is a comparison of the cards.



Notice the different shape on the right hand side of the cards.

a. Which card is located in the top of the graphic?

_____

b. Which card is located on bottom?

_____

Step 2 Installing the client adapter card in a desktop

a. Turn off the PC and all the components.

b. Remove the computer cover.

c. Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

d. Examine the client adapter. The antenna connector and the LEDs face out of the computer and are visible when the cover is placed back on. Prior to installing the card, check to make sure the 2-dB dipole 'rubber ducky" antenna has been removed to prevent damage during the card insertion.

e. Tilt the adapter to allow the antenna connector and LEDs to slip through the opening in the CPU back panel.

f. Press the client adapter into the empty slot until the connector is firmly seated. Install the screw.

g. Reinstall the screw on the CPU back panel and replace the computer cover.

h. Attach the 2-dB dipole antenna to the adapter antenna connector until it is finger-tight.

i. For optimal reception, position the antenna so it is straight up.

j. Boot up the computer and proceed to Step 3. Install the drivers for Windows.

Step 3 Install the drivers for Windows

a. After the client adapter is installed into the computer, Windows automatically detects it and briefly opens the Found New Hardware window.

b. The Found New Hardware Wizard window opens and indicates that the wizard will help to install the driver.

c. Click Next. Another window opens and asks what the wizard should do.

d. Select the recommended **Search for a suitable driver for my device** and click **Next**.

e. Select CD-ROM drives. Deselect all other options. Insert the Cisco Aironet Series Wireless LAN Adapters CD into the computer CD-ROM drive. Click **Next**.

f. The wizard finds the installation files on the CD and displays the search results.

g. When the client adapter driver is displayed, click **Next** to copy the required files.

h. When Windows has finished the installation, click **Finish**.

i. Remove the CD from the computer CD-ROM drive.

Step 4 Configure the SSID through Windows

a. Double-click **My Computer**, **Control Panel**, and **System**. For Windows XP, click **Start>My Computer>Control Panel>System**. See your instructor for instructions for other operating systems

b. In the System Properties window, click the **Hardware** tab.

c. Click **Device Manager**.

d. In the Device Manager window, double-click **Network Adapters**.

e. Right-click the **Cisco Systems 350 Series PCMCIA Wireless LAN adapter, or the applicable Aironet Card**.

f. Click **Properties**.

g. In the client adapter Properties window, click the **Advanced** tab.

h. In the Advanced window, select **Client Name**. Type the unique client name of the computer in the Value dialog box.

i. Select **SSID**. Type the RF network SSID, as assigned by the instructor, in the Value dialog box. Remember the SSID is case-sensitive. Click **OK**.

Note The Service Set Identifier (SSID) is a unique identifier that stations must use to be able to communicate with an AP. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

Step 5 Complete the driver installation without a DHCP server

a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. For Windows XP, click **Start>Control Panel** then double-click **Network and Dial-up Connections**. See your instructor for instructions for other operating systems

b. Right-click **Local Area Connection**.

c. Click **Properties**, **Internet Protocol (TCP/IP)**, and **Properties**.

d. Click **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of the computer which can be obtained from the instructor. Click **OK**.

e. In the Local Area Connection Properties window, click **OK**.

f. If prompted to restart the computer, click **Yes**.

g. The driver installation is complete.

Step 6 Verify the TCP/IP settings

a. Select **Start** > **Run** and enter the following:

b. On Win2000 or XP, enter **cmd** to bring up the command prompt. While at the command prompt, type in **ipconfig /all** to verify the IP settings.

c. On Win9x, enter the **winipcfg** command from **Start>Run** and press **Enter**

Step 7 (Optional) Installing on other operating systems

The URLs below provide information for installing the Aironet Client Adapter card on non-Windows Operating Systems:

a. http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

b. http://www.cisco.com/en/US/products/hw/wireless/ps4555/ps448/index.html

Lab 2.5.2.1 Install Aironet Client Utility (ACU)

Estimated Time: 30 Minutes

Number of Team Members: six teams with two students per team

Objective

The student will learn the procedures for installing the Aironet Client Utility (ACU). Also, the student will configure, select, and manage profiles.

Scenario

Install and configure the ACU to allow a user to configure, manage, and monitor wireless connections.

Topology

Preparation

This lab will require the following materials:

- Desktop or Laptop PC
- Appropriate wireless client adapter card
- One Cisco Aironet PCI352, CB20A, or PCM 352 Client Adapter Network Interface Card.
- Aironet Client Utility installer
- 2 configured APs (instructor must setup)
  - Office Profile AP1 – SSID of AP1
  - Home Profile AP2 – SSID of AP2

Resources

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_book09186a0080184b6e.html

Step 1 Configure XP to use the ACU

To configure the client adapter through ACU instead of through Windows XP, follow the steps below:

a. Double-click My Computer, Control Panel, and Network Connections. Click **Start>Control Panel** then double-click **Network Connections**.
For Windows XP, click **Start>My Computer>Control Panel>System**. See your instructor for instructions for other operating systems.

b. Right-click Wireless Network Connection and click Properties.

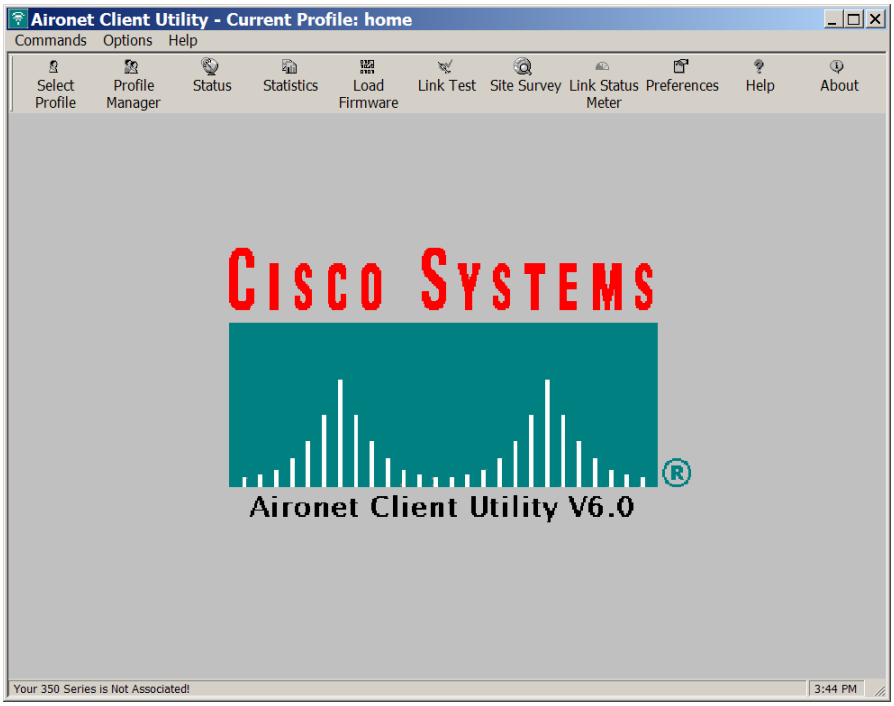
c. Select the Wireless Networks tab.

d. Deselect the Use Windows to configure my wireless network settings check box.

e. Follow the instructions in the "Installing ACU" section to install ACU.

Note If you are planning to configure the client adapter through Windows XP but you want to use ACU's diagnostic tools, then install ACU but do not create any profiles.

Step 2 Install the Aironet Client Utilities (ACU)



After the appropriate driver is installed for the computer's operating system and for the client adapter type, follow the steps below to install the Aironet Client Utility (ACU).

If EAP-TLS, EAP-MD5, PEAP, or EAP-SIM authentication is going to be used on a computer running Windows 2000, Service Pack 3 for Windows 2000 and the Windows 2000 Wireless 802.1X hot fix must be installed before installing ACU.

Follow the procedure below if ACU has never been installed on the computer or if ACU version 4.13 or greater is currently installed. If a version of ACU prior to 4.13 is installed on the computer, uninstall it; then follow the steps below to install the latest version. Cisco does not recommend uninstalling ACU version 4.13 or greater before installing the latest version of ACU.

ACU version 5.05.001 or greater must be used with one of the following software combinations:

- PCM/LMC/PCI card driver version 8.2 or greater and firmware version 4.25.30 or greater
- Mini PCI card driver version 3.4 or greater and firmware version 5.00.03 or greater

- PC-Cardbus card driver version 3.4 or greater and firmware version 4.99 or greater

Note	The most recent version of the ACU can be obtained through the Software Center on the Cisco Connection Online (CCO)

a. To install or use the client utilities on Windows NT or Windows 2000 systems, a user must log onto the system as a user with administrative privileges. The utilities do not install or operate correctly for users not logged in with administrative rights.

b. Select **Start** then **Run** and enter the path for the downloaded ACU setup.exe file.

   To use the CD go to **d:\Utilities\ACU\setup.exe**. “d” is the letter of the CD-ROM drive.

c. Execute the ACU setup.exe file. When the Welcome screen appears, click **Next**.

d. In the Authentication Method screen, select **None,** the default value, for server-based authentication is not enabled for a client adapter and click **Next**.

Note	See the hyperlink in the Resources section to find out more about the Authentication choices.

e. After the client utilities are installed, a user can elect not to implement any security features, or a user can activate some level of security by using WEP keys.

f. In the Select Components screen, make sure the client utilities are selected. Make sure that any undesired utilities are deselected. Click **Next**.

g. In the Select Program Folder screen, click **Next** to allow icons for the client utilities to be placed in the Cisco Systems, Inc. folder.

h. If no server-based authentication was selected in Step 3, select **Launch the Aironet Client Utility** and click **Finish**. The ACU opens so that the client adapter can be configured.

Step 3 Complete the driver installation without a DHCP server

a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.

b. Right-click **Local Area Connection**.

c. Click **Properties**, **Internet Protocol (TCP/IP)**, and **Properties**.

d. Click **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of the computer which can be obtained from the instructor. Click **OK**.

e. In the Local Area Connection Properties window, click **OK**.

f. If prompted to restart the computer, click **Yes**.

g. The driver installation is complete.

Step 4 Verify the TCP/IP settings

a. Select **Start** > **Run** and enter the following:

b. On Win2000 or XP, enter **cmd** to bring up the command prompt. While at the command prompt, type in **ipconfig /all** to verify the IP settings.

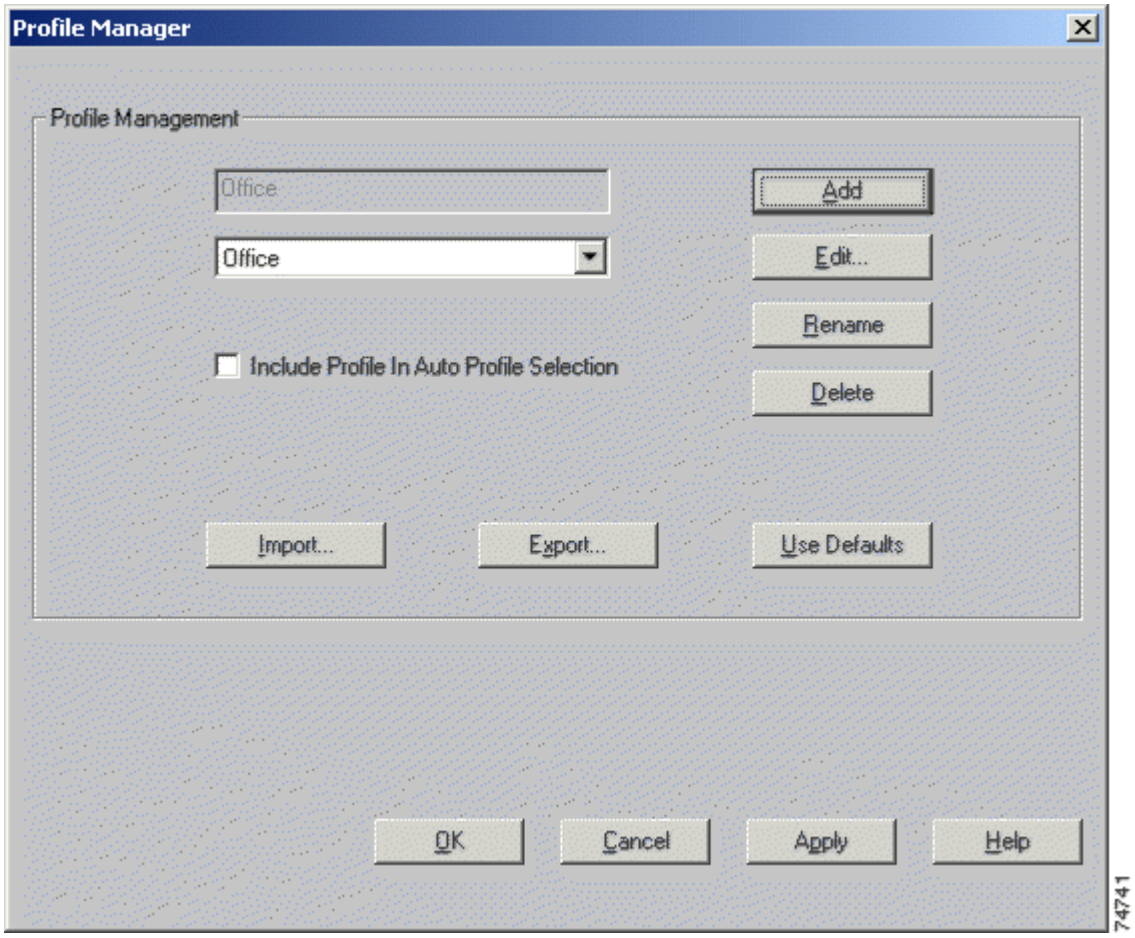
Step 5 (Optional) Installing on other operating systems

The URLs below provide information for installing the Aironet Client Adapter card on non-Windows Operating Systems:

a. http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

b. http://www.cisco.com/en/US/products/hw/wireless/ps4555/ps448/index.html

Step 6 Using the Profile Manager



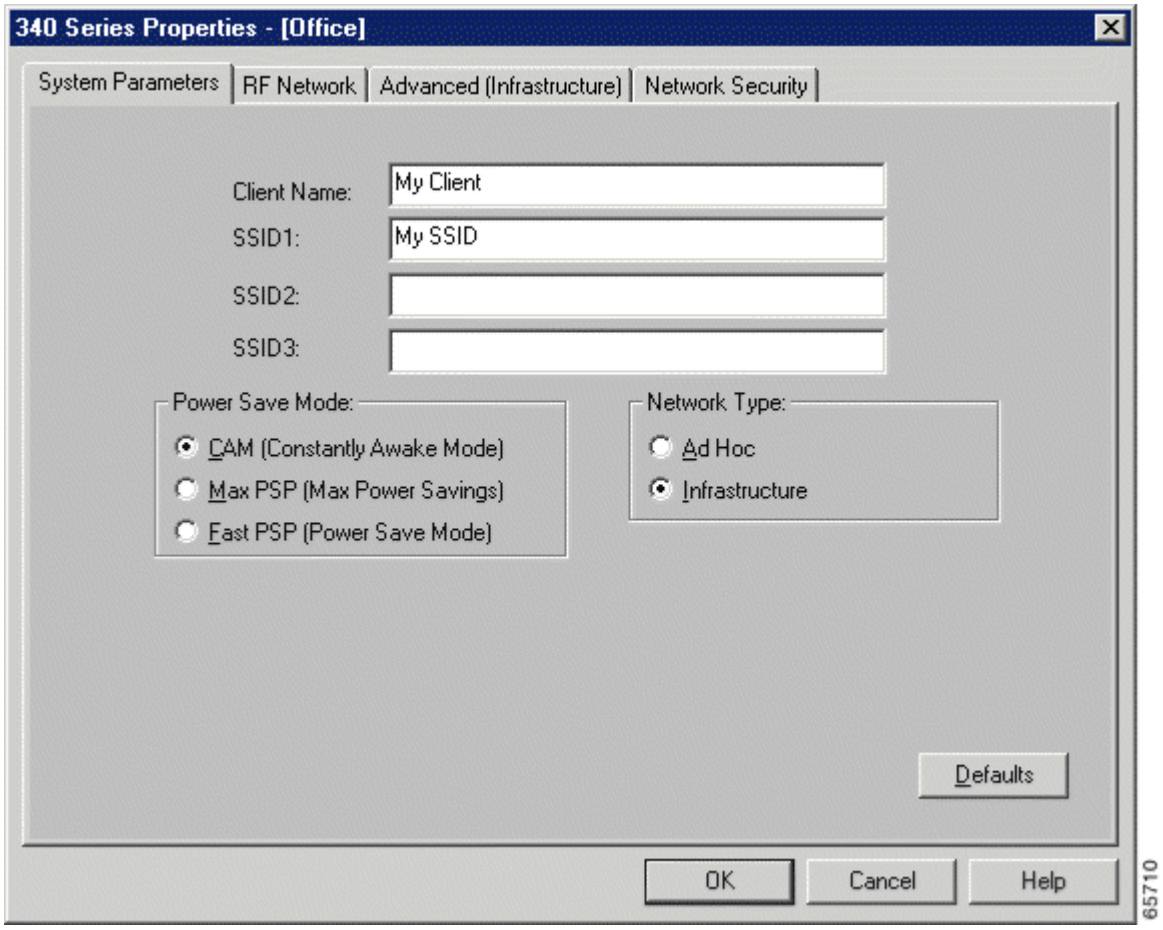
a. Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open the ACU's profile manager.

b. Click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

What tasks does the Profile manager allow?

_____

Step 7 Creating a new profile



Follow the steps below to create a new profile.

a. Click **Add**. A cursor appears in the Profile Management edit box.

b. Enter the name for the first new profiles named “Office”

c. Press **Enter**. The Properties screens appear with the name of the new profile in parentheses.

Note To use the default values, click **OK**. The profile is added to the list of profiles on the Profile Manager screen.

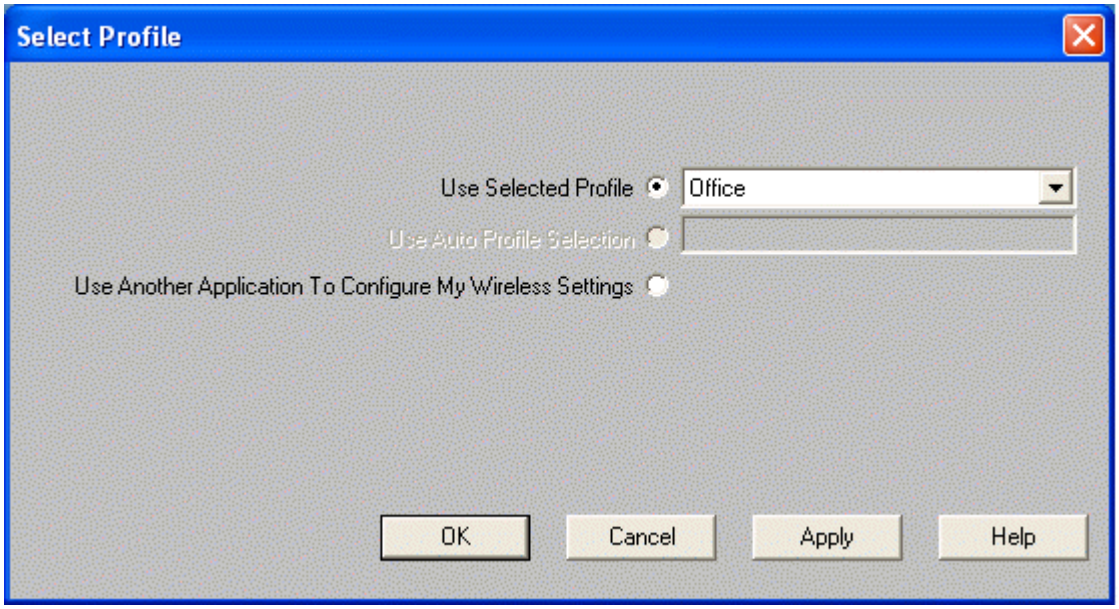
---

d. Configure the Client name and SSID for the Office profile as directed by the instructor in order to connect to the AP.

e. Click **OK** or **Apply** to save your profile.

f. Create profiles named “Home” and “Airport”

Step 8 Selecting the active profile



Follow the steps below to specify the profile that the client adapter is to use.

a. Open ACU; click the **Select Profile** icon or select **Select Profile** from the Commands drop-down menu. The Select Profile screen appears.

b. Select **Use Selected Profile**

c. Now select the Office Profile.

d. Click **OK** or **Apply** to save the selection. The client adapter starts using a profile based on the option selected above.

Note If the client adapter cannot associate to an AP or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, a different profile must be selected or select Use Auto Profile Selection. **Use Auto Profile Selection**—This option causes the client adapter's driver to automatically select a profile from the list of profiles that were set up to be included in auto profile selection. **Use Another Application To Configure My Wireless Settings**—This option allows an application other than ACU to configure the client adapter. Examples of such applications include Windows XP and Boingo. You must select this option if you are configuring your card through Windows XP or 2000 but want to use ACU's diagnostic tools.

Step 9 Using the Aironet Client Monitor (ACM)

ACM is an optional application that provides a small subset of the features available through ACU. Specifically, it enables you to access status information about your client adapter and perform basic tasks. ACM is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use.

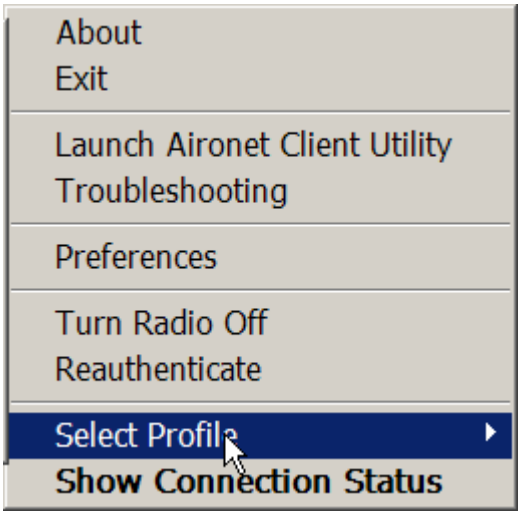
The profile can also be quickly switched through the system tray using ACM.

a. Left click on the ACU icon and go to **Select Profile**, then choose the Home profile.

b. The client will now associate to the second AP. Observe the ACM icon.

c. Now select the Airport profile. Observe the ACM icon turn gray

d. Finally, re-select the Office profile to connect to the first AP. The ACM icon should turn green.



The appearance of the ACM icon indicates the connection status of your client adapter. ACM reads the client adapter status and updates the icon every 2 seconds

Icon	Description
	The client adapter's radio is turned off.
	The client adapter is not associated to an AP.
	The client adapter is associated to an AP, but the user is not authenticated.
	The client adapter is associated to an AP, and the link quality is excellent or good.
	The client adapter is associated to an AP, and the link quality is fair.
	The client adapter is associated to an AP, and the link quality is poor.

e. What is the status of the client adapter?

_____

Step 10 Modifying a Profile (Optional)

This section provides instructions for modifying an existing profile. Follow the steps in the corresponding section below to edit, set to default values, rename, or delete a profile.

Editing a Profile

a. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

b. From the Profile Management drop-down box, select the profile that you want to edit.

c. Click **Edit**. The Properties screens appear with the name of the profile in parentheses.

d. Change any of the configuration parameters for this profile.

e. Click **OK** or **Apply** to save your configuration changes.

Setting a Profile to Default Values

a. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

b. From the Profile Management drop-down box, select the profile that you want to set to default values.

c. Click **Use Defaults**.

d. When prompted, click **Yes** to confirm your decision.

e. Click **OK** or **Apply** to save your change. The profile is saved with default values.

Renaming a Profile

a. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

b. From the Profile Management drop-down box, select the profile that you want to rename.

c. Click **Rename**. The Profile Management edit box becomes enabled.

d. Enter a new name for the profile.

e. Click **OK** or **Apply** to save your change. The profile is renamed and added to the list of profiles.

Deleting a Profile

a. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

b. From the Profile Management drop-down box, select the profile that you want to delete.

c. Click **Delete**.

d. When prompted, click **Yes** to confirm your decision.

e. Click **OK** or **Apply** to save your change. The profile is deleted.

Step 11 Importing and exporting profiles

This section provides instructions for importing and exporting profiles. You may want to use the import/export feature for the following reasons:

- To back up profiles before uninstalling the client adapter driver or changing radio types
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional computers

Follow the steps in the corresponding section below to import or export profiles.

Exporting a Profile

a. Insert a blank floppy disk into your computer's floppy drive, if you wish to export a profile to a floppy disk. Or save the file to the PC hard disk.

b. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears

c. From the Profile Management drop-down box, select the profile that you want to export.

d. Click **Export**. The Save Profile As screen appears. The default filename is *ProfileName*.pro, where *ProfileName* is the name of the selected profile, and the default directory is the directory in which ACU was installed.

e. If you want to change the profile name, enter a new name in the File name edit box.

f. Select a different directory (for example, your computer's floppy disk drive or a location on the network) from the Save in drop-down box.

g. Click **Save**. The profile is exported to the specified location.

Importing a Profile

a. If the profile that you want to import is on a floppy disk, insert the disk into your computer's floppy drive.

b. Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

c. Click **Import**. The Import Profile screen appears.

d. Find the directory where the profile is located.

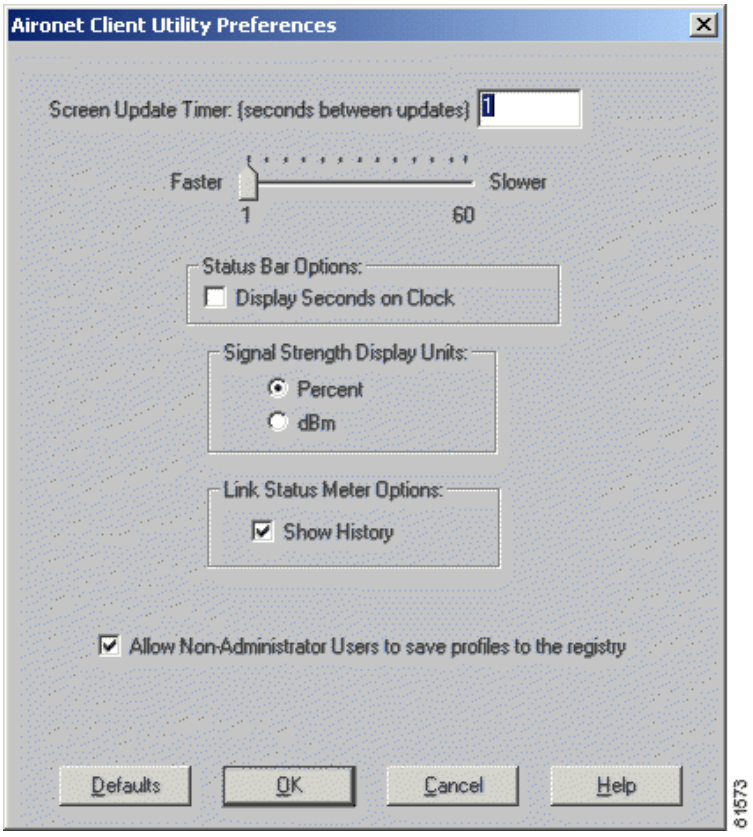
e. Click the profile so it appears in the File name box at the bottom of the Import Profile screen.

f. Click **Open**. The imported profile appears in the list of profiles on the Profile Manager screen.

Step 12 Denying access to non-administrative users

By default, ACU allows regular-class users to modify and save profiles to the registry. However, if you have administrative rights, you can prevent regular-class users from saving profiles on computers running Windows NT, 2000, or XP. (This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.)

Follow the steps below if you wish to prevent users without administrative rights from modifying and saving profiles (or to allow regular-class users to save profiles if permission was denied previously).



a. Open ACU by double-clicking the Aironet Client Utility (ACU) icon on your desktop.

b. Click the Preferences icon or select Preferences from the Options drop-down menu. The Aironet Client Utility Preferences screen appears.

c. Deselect the **Allow Non-Administrator Users to save profiles to the registry** check box (or select this check box if you wish to allow regular-class users to save profiles).

d. Click **OK** to save your changes.

Step 13 Uninstall the Aironet Client Utilities (optional)

Note If this step is performed, the ACU will have to be reinstalled before the next lab.

a. Uninstall the Client Utilities

b. Close any Windows programs that are running.

c. Insert the Cisco Aironet Series Wireless LAN Adapters CD into the computer CD-ROM drive.

d. Select **Start** then **Run** and enter the following path: **d:\Utilities\ACU\setup.exe**. d is the letter of the CD-ROM drive.

e. When the Welcome screen appears, select **Remove** and click **Next**.

f. When asked if selected applications should be completely removed, click **Yes**.

g. If a message appears indicating that a file was detected that may no longer be needed by any application but deleting the file may prevent other applications from running, click **Yes**.

h. If a message is received indicating that locked files were detected, click **Reboot**.

i. In the Maintenance Complete screen, click **Finish**.

j. If prompted to restart the computer, remove the CD from the computer CD-ROM drive and click **Yes**.

Lab 2.5.2.2 Install Aironet Desktop Utility (ADU)

Estimated Time: 30 Minutes

Number of Team Members: six teams with two students per team

Objective

The student will learn the procedures for installing the Aironet Desktop Utility (ADU). Also, the student will configure, select, and manage profiles.

Scenario

Install and configure the ADU to allow a user to configure, manage, and monitor wireless connections when using Cisco® Aironet® IEEE 802.11a/b/g Wireless Adapters.

The Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) are radio modules that provide transparent wireless data communications between fixed, portable, or mobile devices and other wireless devices or a wired network infrastructure. The client adapters are fully compatible when used in devices supporting "plug-and-play" (PnP) technology.

The AIR-CB21AG PC-Cardbus card is an IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with an external 32-bit Cardbus slot. Host devices can include laptops and notebook computers.

The AIR-PI21AG PCI card is an IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop personal computer.

Two client utilities are available for use with the client adapters: Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU). These utilities are optional applications that interact with the client adapter's radio to adjust settings and display information.

ADU enables you to create configuration profiles for your client adapter and perform user-level diagnostics. Because ADU performs a variety of functions, it is documented by function throughout this manual.

ASTU, which is accessible from an icon in the Windows system tray, provides a small subset of the features available through ADU. Specifically, it enables you to view status information about your client adapter and perform basic tasks.

Topology

Preparation

This lab will require the following materials:

- Desktop or Laptop PC
- Appropriate wireless client adapter card
- One Cisco Aironet CB21AG or PI21AG Client Adapter Network Interface Card.
- Aironet Desktop Utility installer
- 2 configured APs (instructor must setup)
    - Office Profile AP1 – SSID of AP1
    - Home Profile AP2 – SSID of AP2

Step 1 Configure XP to use the ADU

To configure the client adapter through ADU instead of through Windows XP, follow the steps below:

a. Open the Control Panel. See the instructor for instructions for other operating systems.

b. Right-click Wireless Network Connection and click Properties.

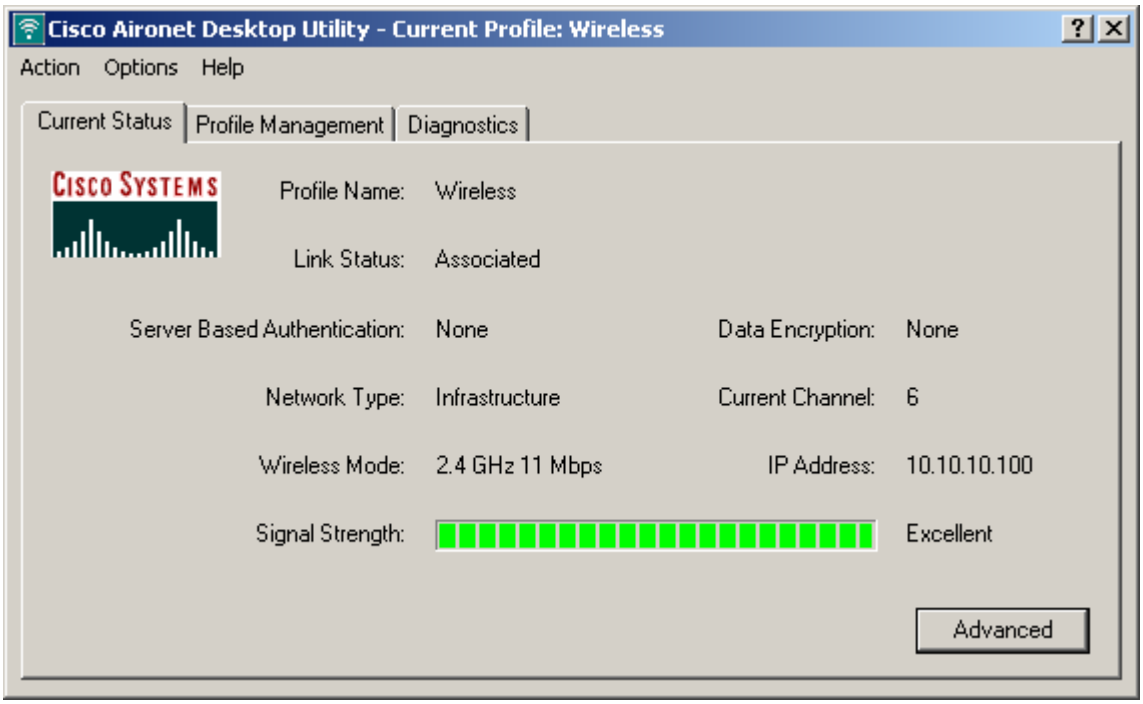
c. Select the Wireless Networks tab.

d. Verify that the Use Windows to configure my wireless network settings check box is deselected.

e. Follow the instructions in the "Installing ADU" section to install ADU.

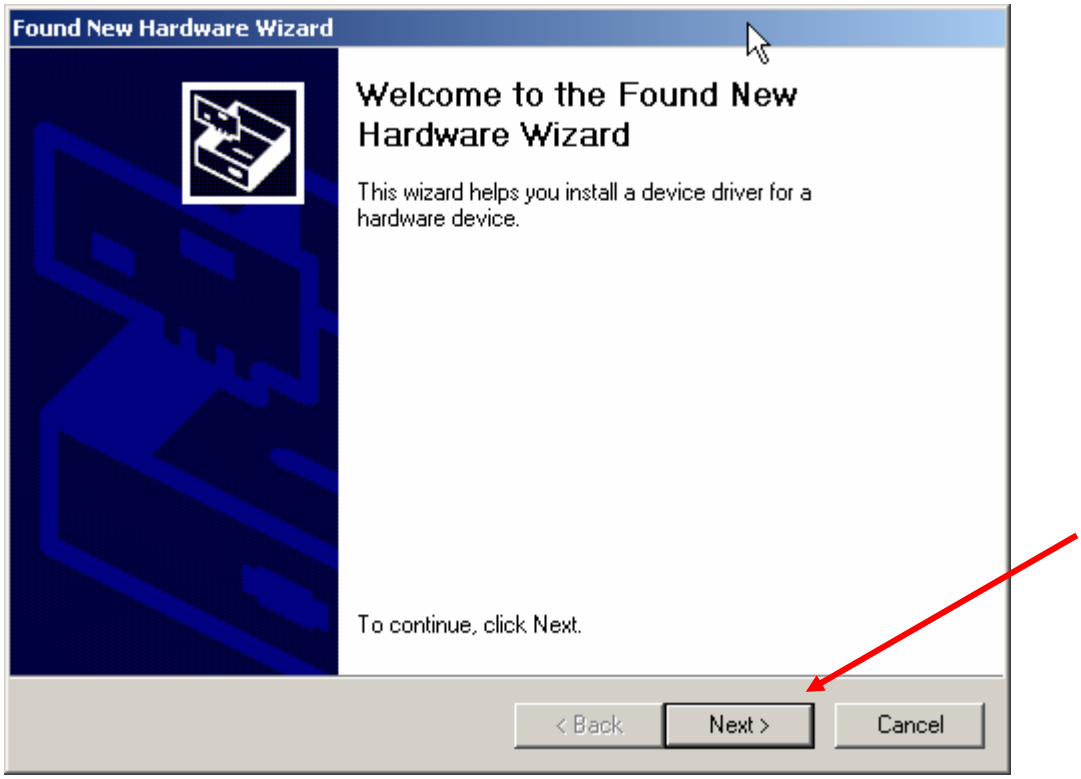
Note If the client adapter will be configured through Windows XP but the ADU's diagnostic tools will be used, then install ADU but do not create any profiles.

Step 2 Install the Aironet Client Utilities (ADU)

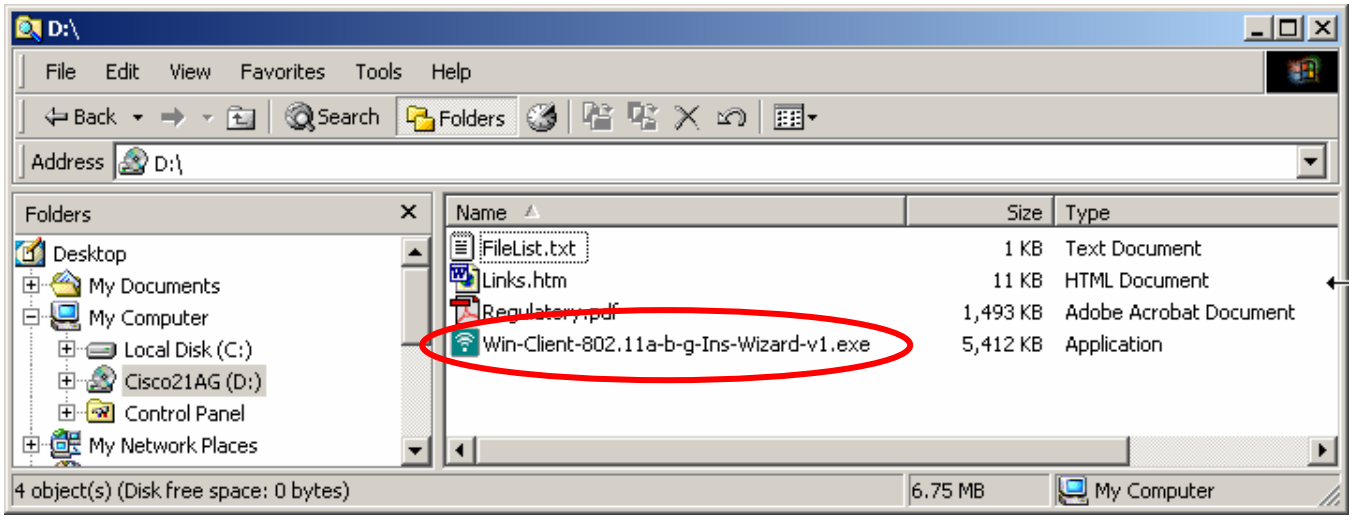


Prior to installing ADU software and card drivers, the client adapter should be installed into the laptop or desktop computer. When the computer reboots, Windows may recognize that hardware has been installed.

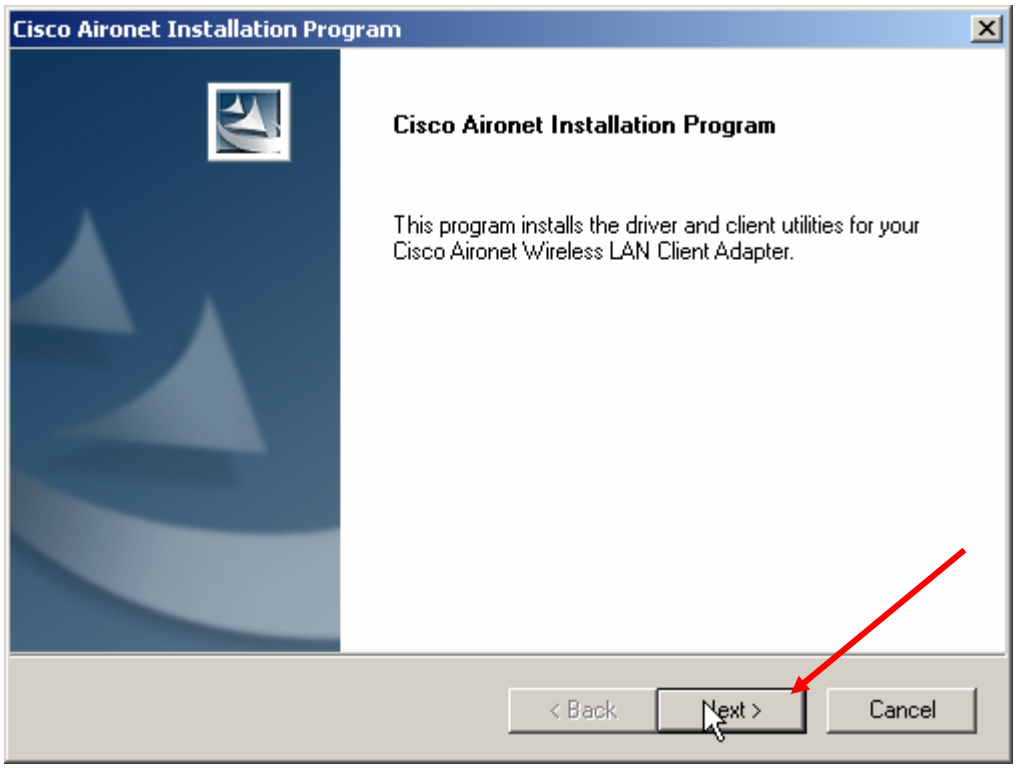
a. Click Cancel on the Windows **Found New Hardware Wizard** to continue.



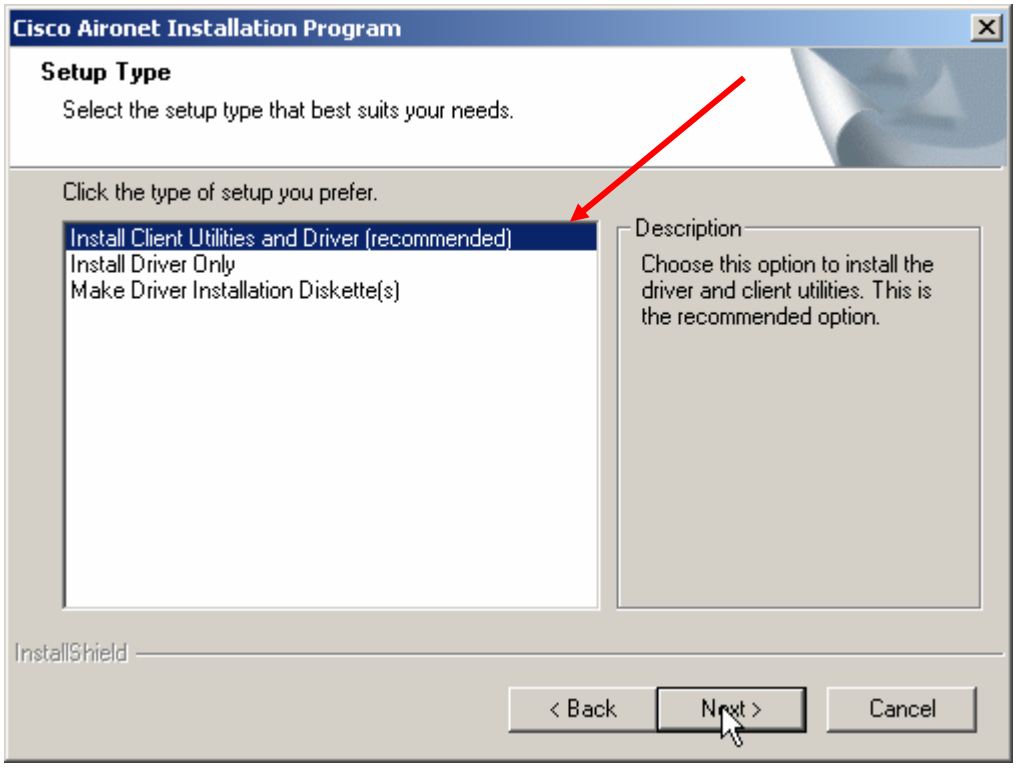
b. Navigate to the installation file for the client adapter. This file can be found either on the CD that came in the package with the CD or on the local PC if this file was downloaded from Cisco.com. Double click the file to begin installation.



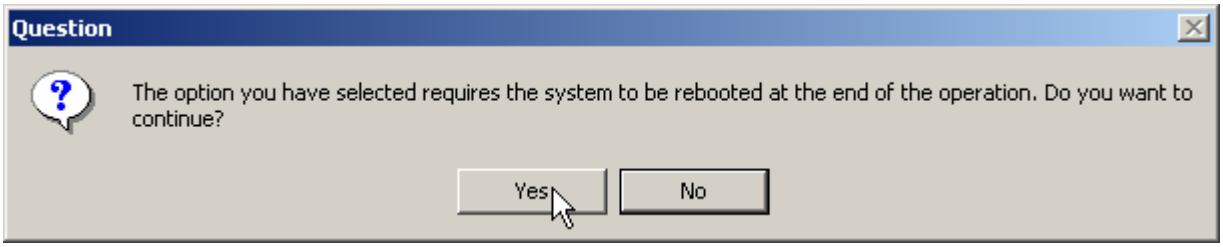
c. The Installation Program will open and prompt for any necessary input. Click **Next** to continue.



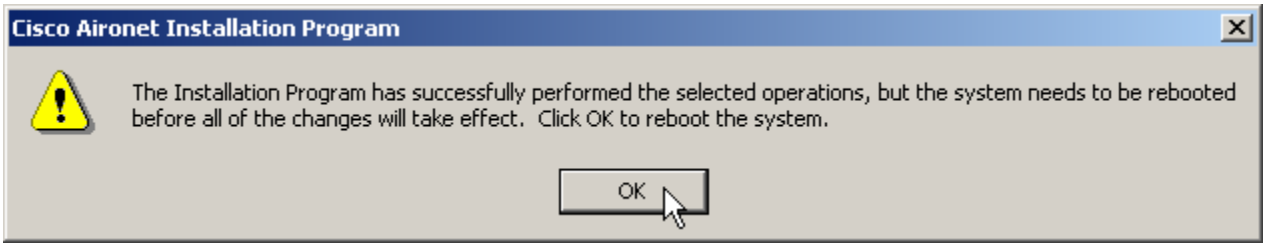
d. From the available Setup types, select the first option: **Install Client Utilities and Driver**. This option will install all of the necessary files for both the client adapter and the desktop utility. Click **Next** to continue.



e. Now there is a prompt to accept a system reboot after installation completes. Click **Yes** to continue installation. Clicking No will cause installation to abort.



f. The default settings can be accepted for the destination folder. Remember to reboot the computer when installation has completed.



Step 3 Complete the driver installation without a DHCP server

a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.

b. Right-click **Local Area Connection**.

c. Click **Properties**, **Internet Protocol (TCP/IP)**, and **Properties**.

d. Click **Use the following IP address** and enter the IP address, subnet mask, and default gateway address obtained from the instructor. Click **OK**.

e. In the Local Area Connection Properties window, click **OK**.

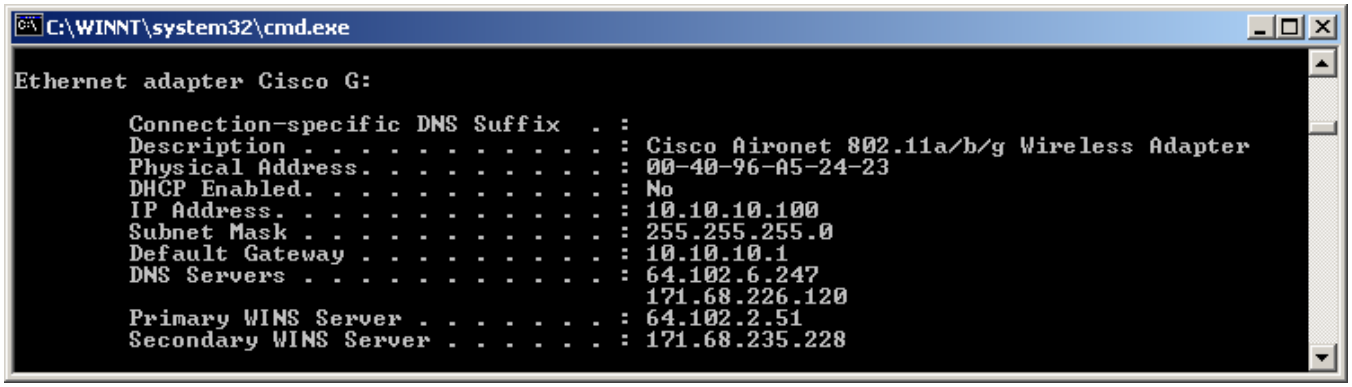
f. If prompted to restart the computer, click **Yes**.

g. The driver installation is complete.

Step 4 Verify the TCP/IP settings

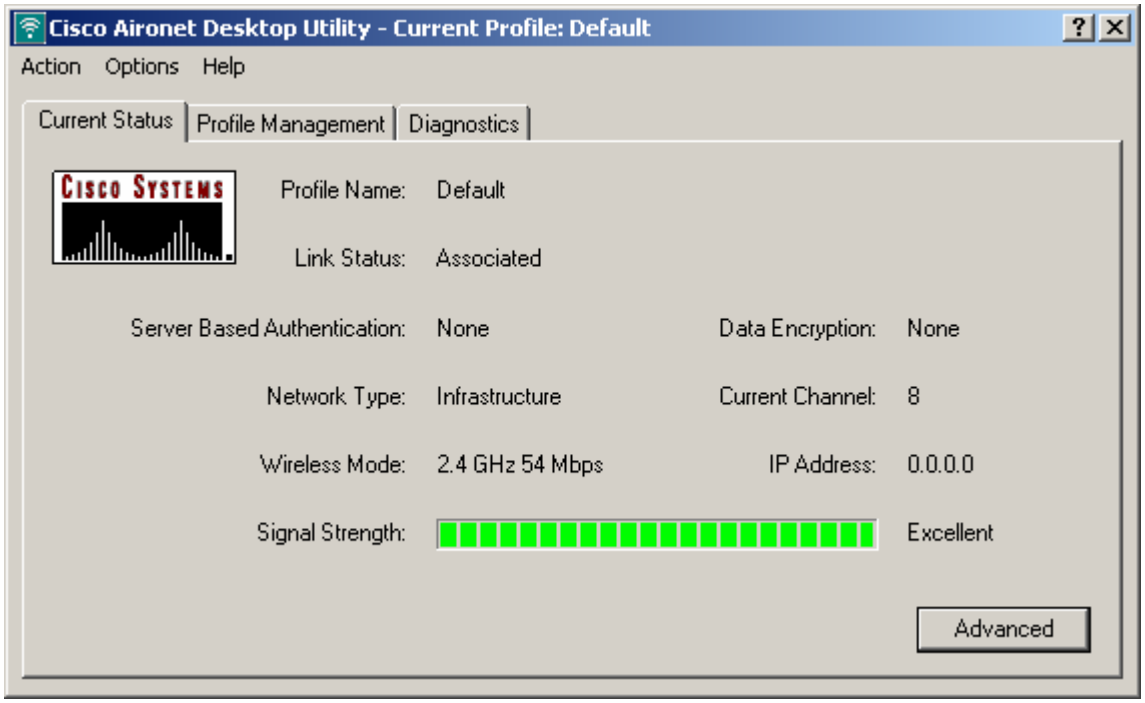
a. Select **Start** > **Run** and enter the following:

b. On Win2000 or XP, enter **cmd** to bring up the command prompt. While at the command prompt, type in **ipconfig /all** to verify the IP settings.



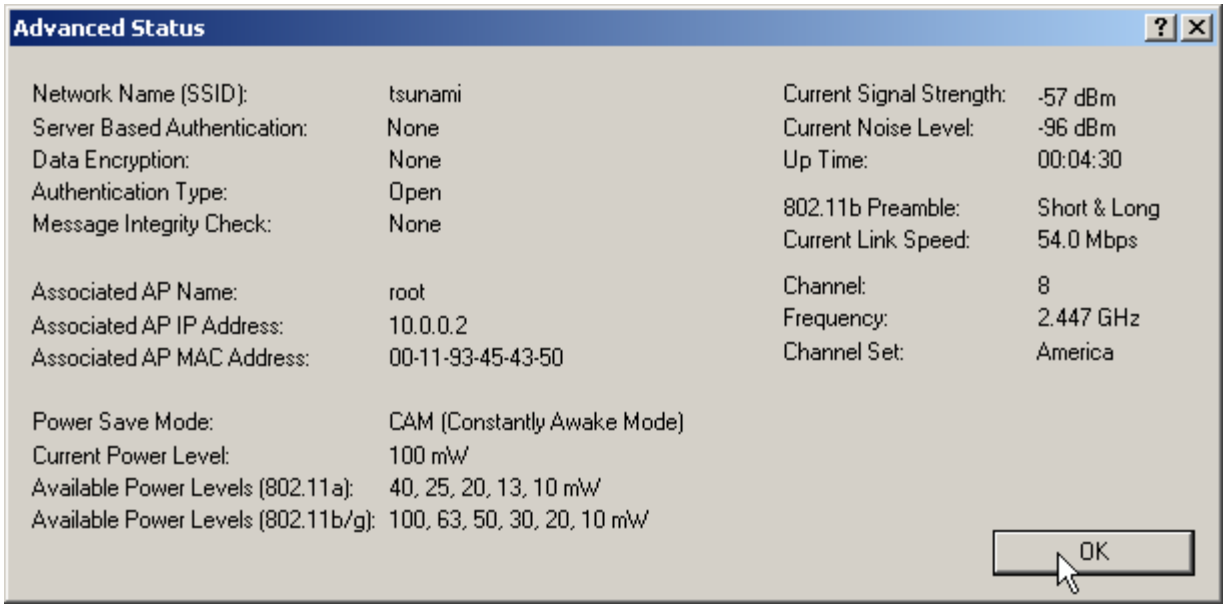
Step 5 Running ADU

To open the ADU double-click the desktop icon or navigate to the program shortcut from the Start button: Start>Programs>Cisco Aironet>Aironet Desktop Utility. Alternately, the System Tray icon can be used to launch the desktop utility.



The tabbed interface of the ADU allows access to each of the necessary tasks to configure and monitor the client adapter.

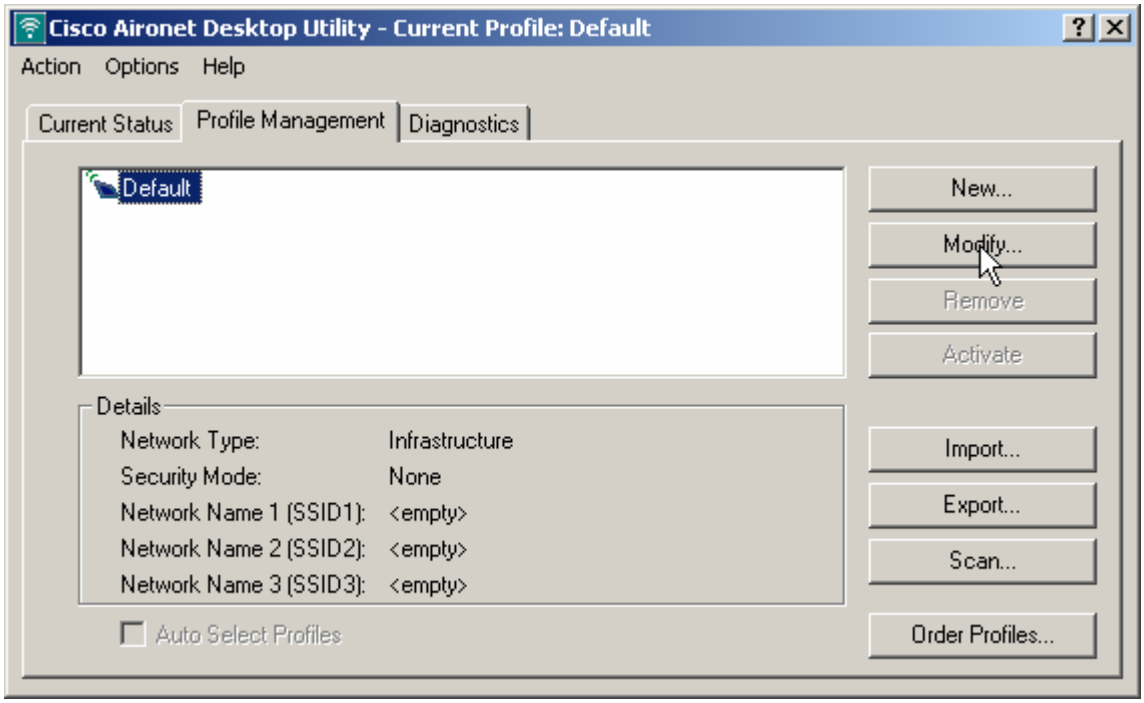
a. Click the Advanced tab to view detailed setting information for the card. The Advanced Status tab can provide useful information about the current SSID as well as association information for the card. Click **OK** to close the window and return.



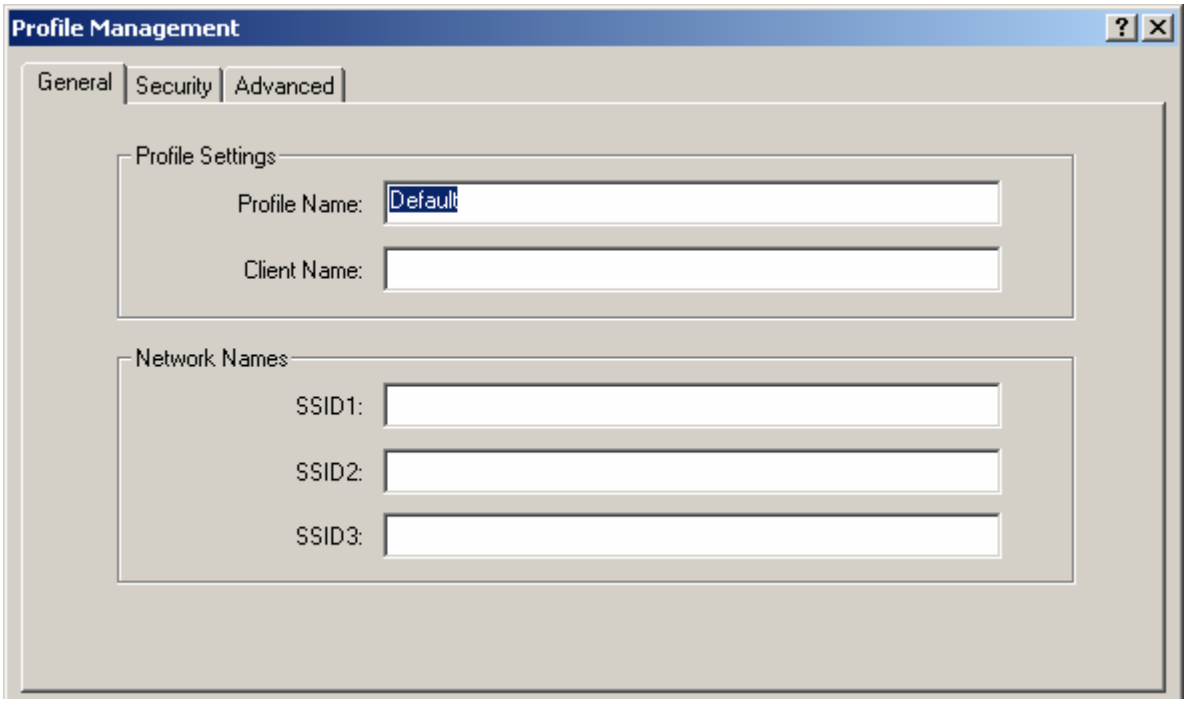
Step 6 Profile Management

The Profile Management tab allows the creation, modification, removal or activation of client adapter profiles. Each profile can contain a unique set of authentication and encryption settings. Using multiple profiles will allow the adapter to work in a variety of settings.

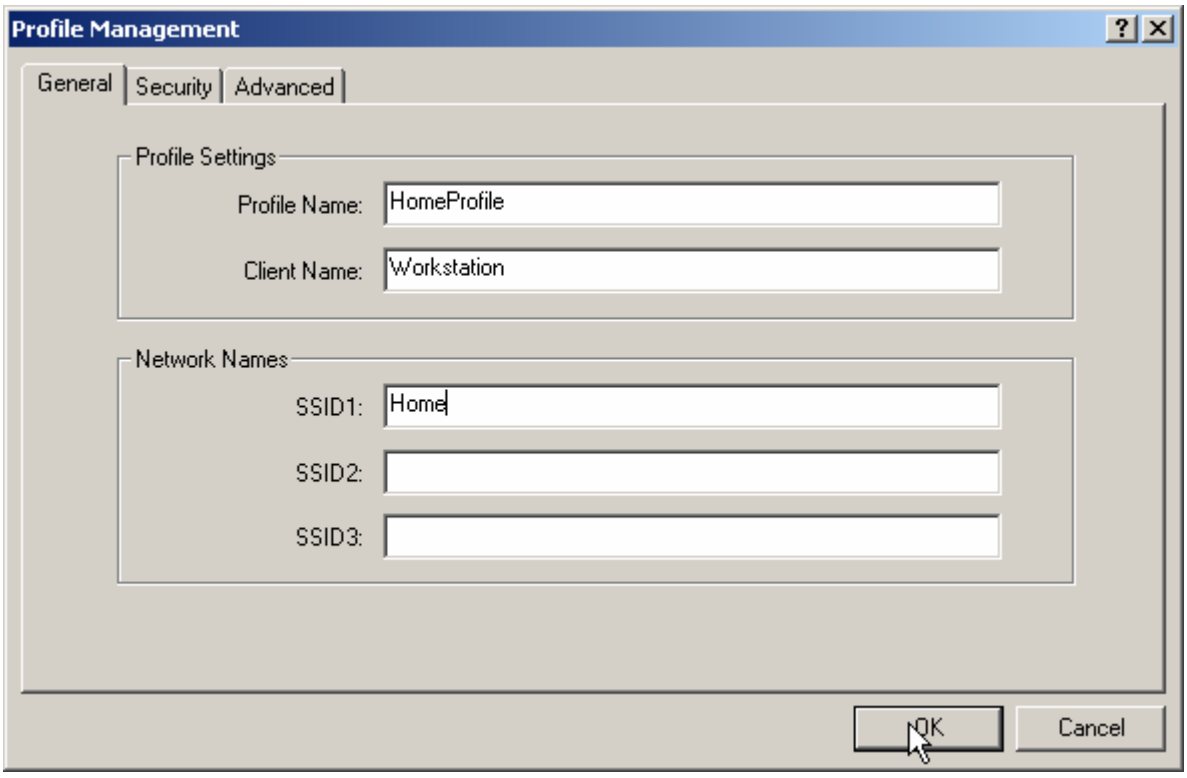
a. The Default profile was created when the adapter was installed. Click the Modify button to view the settings associated with this profile. (If the Default profile has been deleted, click any available profile to modify.)



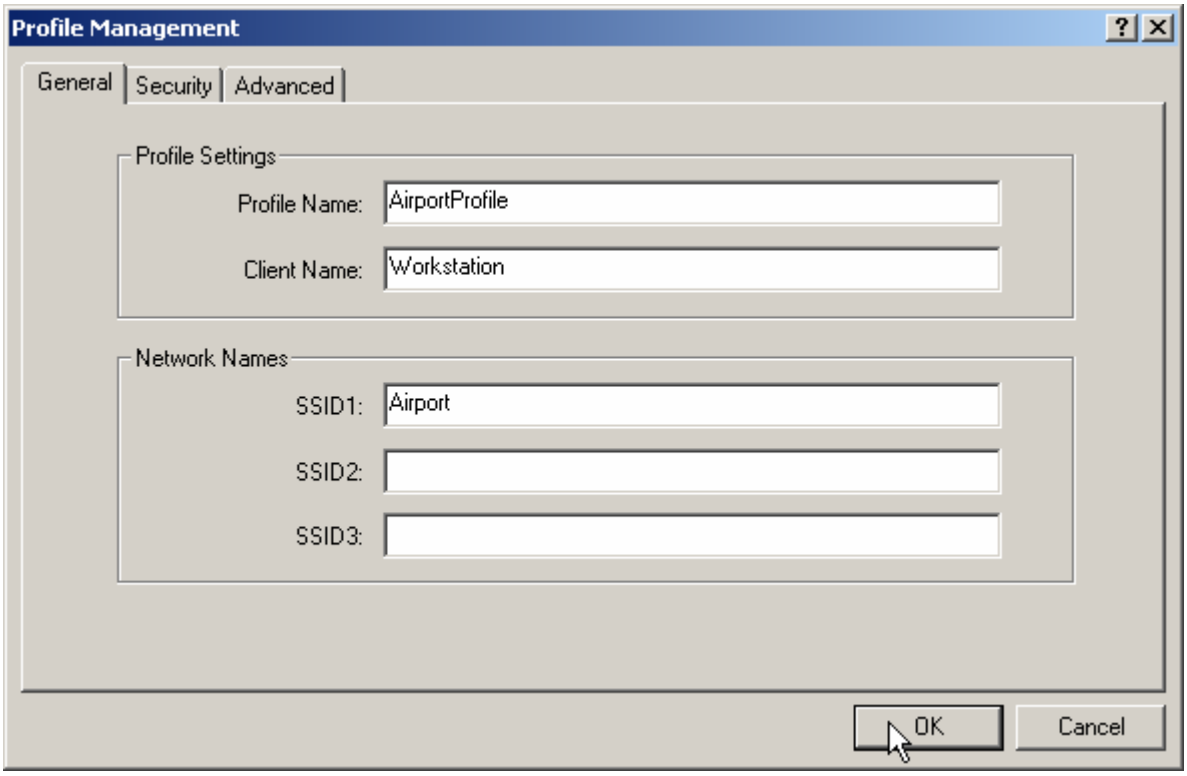
b. View the General, Security and Advanced settings for the profile. Notice that each profile has many configuration options available. Click the **Cancel** button to return to the Profile Management window.



c. To create two new profiles named “Home” and “Airport”, select the **New…** button. First create the Home profile. Use a **Profile Name** that makes it easier to remember where this profile is used. The **Client Name** should be a useful identifier for the computer. In the **SSID1** field, type “Home.” SSIDs are case sensitive and must match the AP or bridge exactly. Click OK to continue.



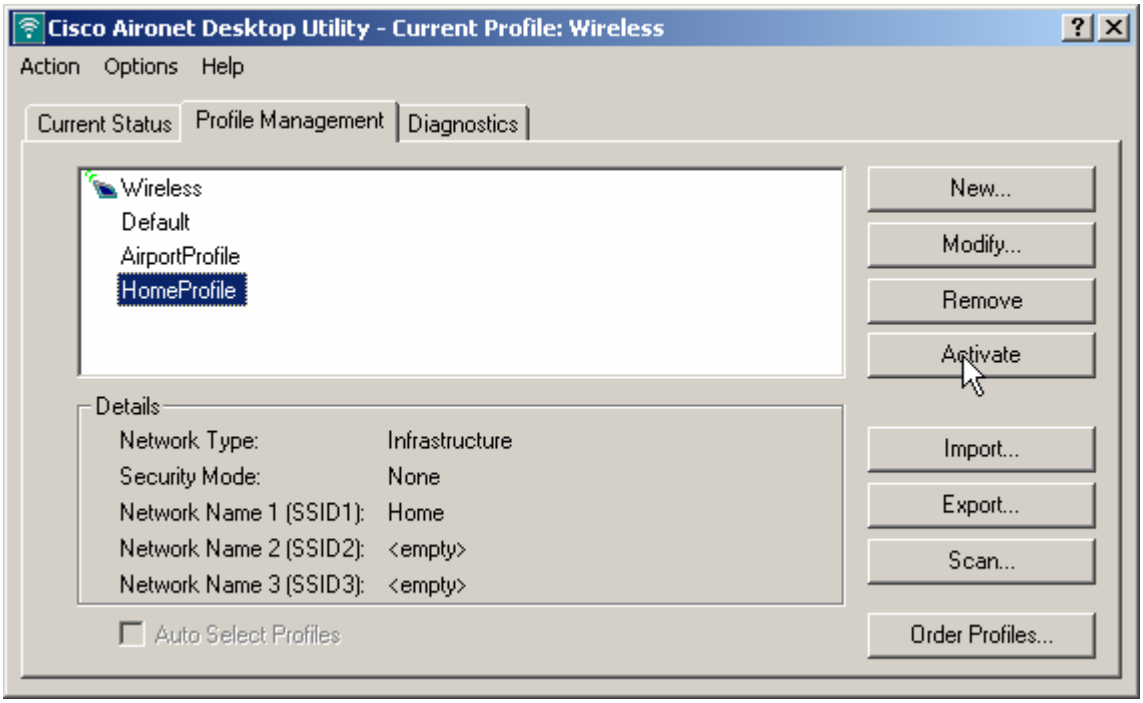
d. Create a second profile for use at the airport.



Step 7 Selecting profiles

With multiple profiles, it is important to know which profile is currently selected for use. From the Profile Management window, any of the listed profiles can be selected. Follow the steps below to specify the profile that the client adapter is to use.

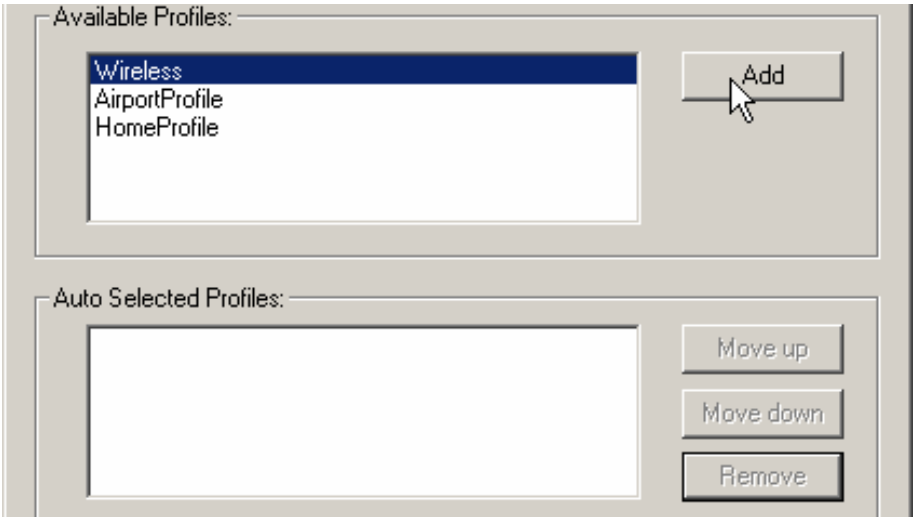
a. From the list of profiles in the Profile Management window, click the **HomeProfile** and then the **Activate** button. If the AP has been configured with the Home SSID, the client should associate. If the client does not associate troubleshoot with your instructor.



Configured profiles can be tried in a specified order. This is useful when a laptop is used in multiple areas consistently. For instance, a laptop might be used daily at work and then at home during the evening. Auto selected profiles in this case would be an easy way to ensure that the laptop associated with the access point at each site.

b. From the Profile Management window, select the **Order Profiles…** button.

c. The configured profiles will appear in the top window as Available Profiles. One or more of these profiles can be added to the Auto Selected Profiles list by selecting the profile and clicking the **Add** button. Once in the list, the profiles can be ordered by preference. The adapter will try each profile in order until one associates with an access point.



Step 8 Using the Aironet Client Monitor (ACM)

The ACM is an optional application that provides a small subset of the features available through ADU. Specifically, it provides access to status information about the client adapter and the ability to perform basic tasks. The ACM is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use.

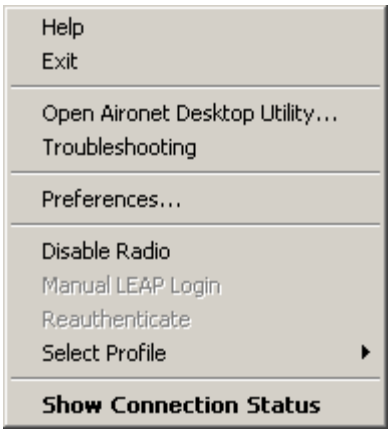
The profile can also be quickly switched through the system tray using ACM.

a. Right click on the ADU icon and go to **Select Profile**, then choose the Home profile.

b. The client will now associate to the second AP. Observe the ACM icon.

c. Now select the Airport profile. Observe the ACM icon turn gray

d. Finally, re-select the Office profile to connect to the first AP. The ACM icon should turn green.



The appearance of the ACM icon indicates the connection status of the client adapter. The ACM reads the client adapter status and updates the icon every 2 seconds

Icon	Description
	The client adapter's radio is turned off.
	The client adapter is not associated to an AP.
	The client adapter is associated to an AP, but the user is not authenticated.
	The client adapter is associated to an AP, and the link quality is excellent or good.
	The client adapter is associated to an AP, and the link quality is fair.
	The client adapter is associated to an AP, and the link quality is poor.

Step 9 Modifying a Profile

Existing profiles may need to be edited to maintain consistency with the access point configuration or if the SSID was misconfigured.

a. Open the ADU, select the profile to modify, and then click the **Modify** button.

b. Change the configured client name for this profile.

c. Click **OK** or **Apply** to save the configuration changes.

Step 10 Removing a Profile

During lab activities, a number of profiles may be created. To ease troubleshooting, profiles may be deleted if they are no longer needed.

a. Click the profile that will be deleted.

b. Click the Remove button. Note that there is no confirmation for this action! Take care when removing profiles from the client adapter.

Step 11 Importing and exporting profiles

This section provides instructions for importing and exporting profiles. YThe import/export feature may be used for the following reasons:

- To back up profiles before uninstalling the client adapter driver or changing radio types
- To set up a computer with a profile from another computer
- To export one of the profiles and use it to set up additional computers

Follow the steps in the corresponding section below to import or export profiles.

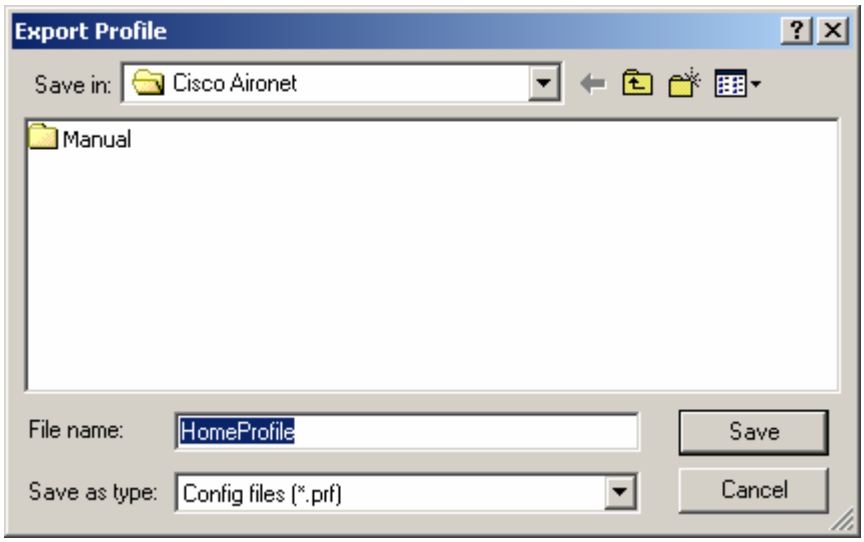
Exporting a Profile

a. Insert a blank floppy disk into the computer's floppy drive, or save the file to the PC hard disk.

b. Open the ADU. From the **Profile Management** tab, select the profile to export. Click the **Export** button.

c. The **Export Profile** screen appears. The filename and directory can be changed.

d. Click **Save** to export the profile.

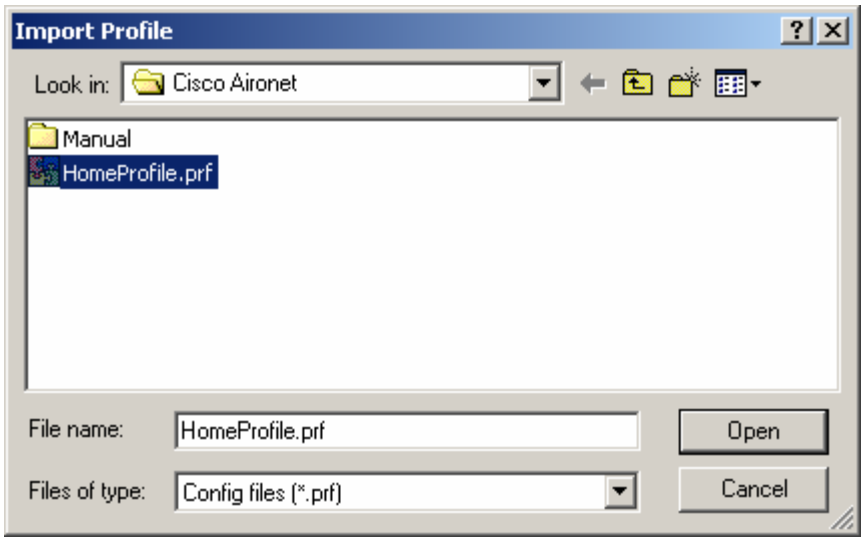


Importing a Profile

a. Open the ADU and click the **Profile Management** tab.

b. Click **Import**. The Import Profile window appears. Navigate to the directory where the profile is located. Click the profile so it appears in the File name box at the bottom of the Import Profile screen.

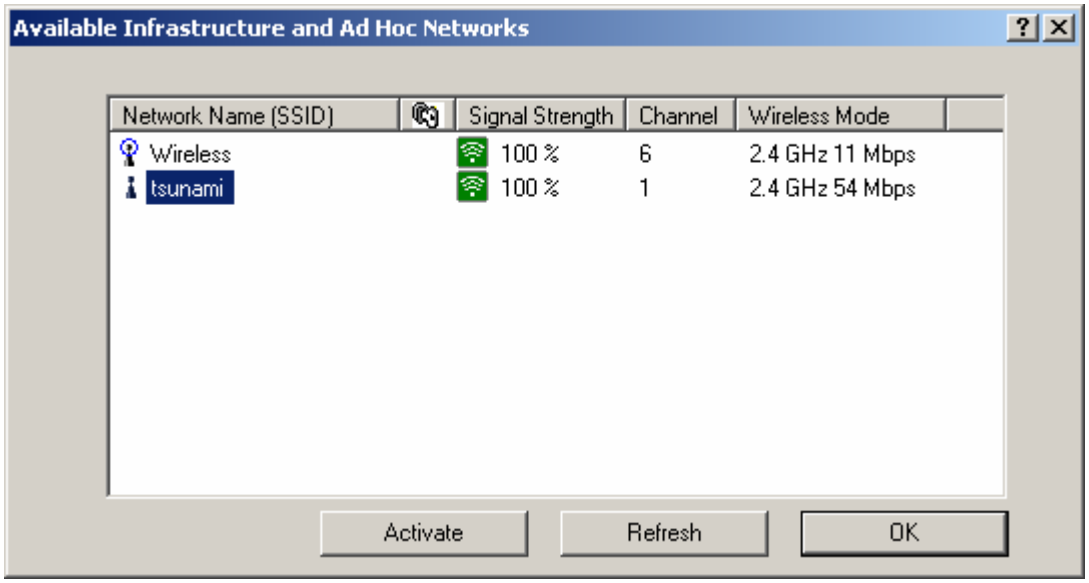
c. Click **Open**. The imported profile appears in the list of profiles on the Profile Manager screen.



Step 12 Scanning for available networks

The Profile Management tab also includes a **Scan** button that displays Available APs and Ad Hoc Networks. Those network names listed with a key icon demonstrate that the network is secured. If no key is displayed, the network is not secured and will likely accept guest associations.

Highlight a network name and click the **Activate** button to connect to an available network. If no configuration profile exists for that network, the Network Configuration Settings window opens to the General tab. Fill in the network name and click OK to create the configuration profile for that network.



Lab 2.5.5.1 Configure Auto Profiles

Estimated Time: 25 Minutes

Number of Team Members: six teams with two students per team

Objective

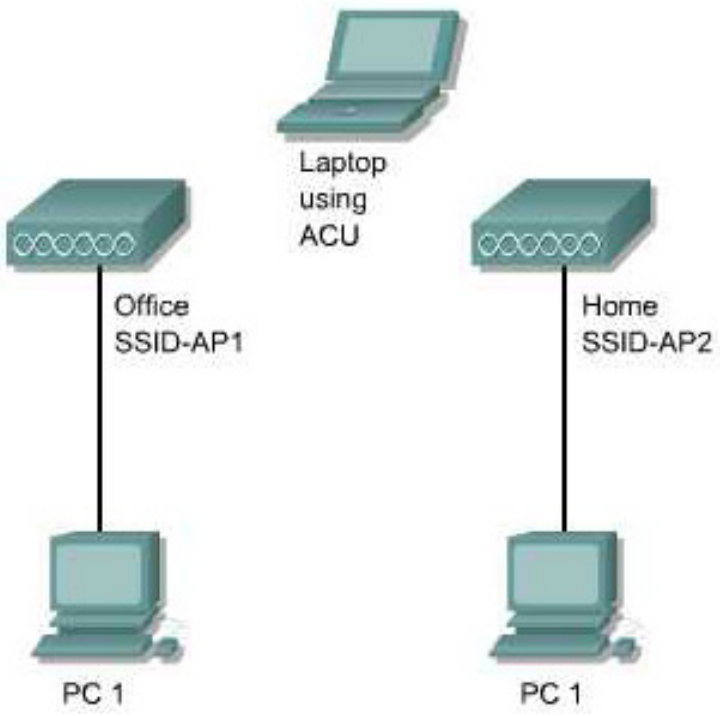
The student will learn the procedures for configuring ACU to use Auto Profiles.

Scenario

The **Use Auto Profile Selection** option causes the driver for the client adapter to automatically select a profile from the list of profiles that were set up to be included in auto profile selection. The name of the profile that is being used appears in the box to the right of the **Use Auto Profile Selection** option.

If the client adapter loses association for more than 10 seconds, the driver switches automatically to another profile that is included in **Auto Profile Selection**. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value). To force the client adapter to associate to a different AP, Auto Profile Selection must be disabled and a new profile must be selected.

Topology



Preparation

This lab will require the following materials:

- 3 Desktop or Laptop PC
- Appropriate wireless client adapter card
- One Cisco Aironet PCI352, CB20A, or PCM 352 Client Adapter Network Interface Card.
- Aironet Client Utility installer
- Two configured AP (instructor must setup)
    - AP1 – SSID of AP1
    - AP2 – SSID of AP2
    - AP3 – SSID of AP3 (optional)

Resources

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_chapter09186a008007f869.html#1091568

Step 1 Creating multiple profiles

a. Remove any existing profiles.

b. Now create 4 profiles based on the following table.

Profile	Profile Name	Client Name	SSID
1	Office1	StudentP1	AP1
2	Home	StudentP2	AP2
3	Office2	StudentP3	AP3
4	Airport	StudentP4	AP4

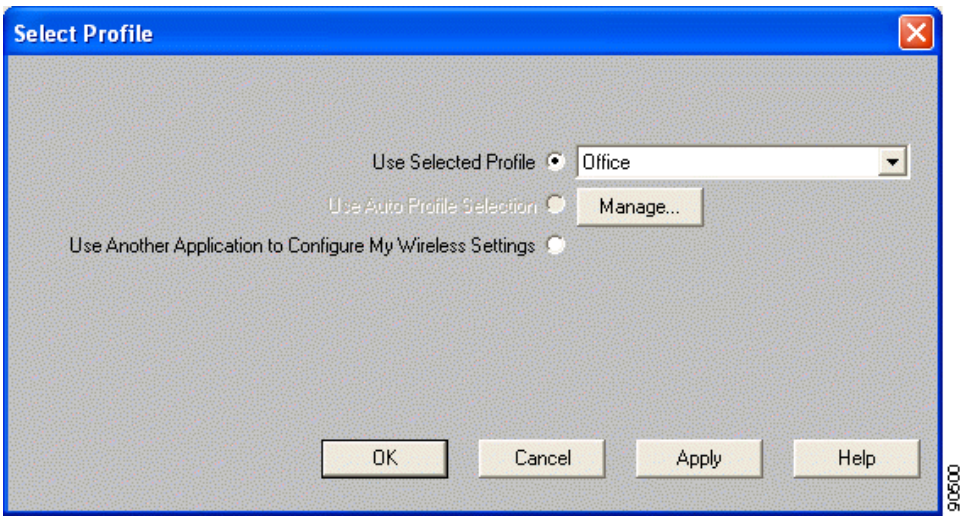
(Where StudentP is the student name)

Step 2 Including a profile in auto profiles selection

After creating the four profiles for the client adapter, the profile manager auto profile selection feature can be used. When auto profile selection is enabled, the client adapter automatically selects a profile from the list of profiles that were included in auto profile selection and uses it to establish a connection to the network.

Follow the steps below to include the profiles in auto profile selection and to establish the order in which the profiles will be selected for use.

a. Open ACU; click the **Select Profile** icon or select **Select Profile** from the Commands drop-down menu. The Select Profile screen appears

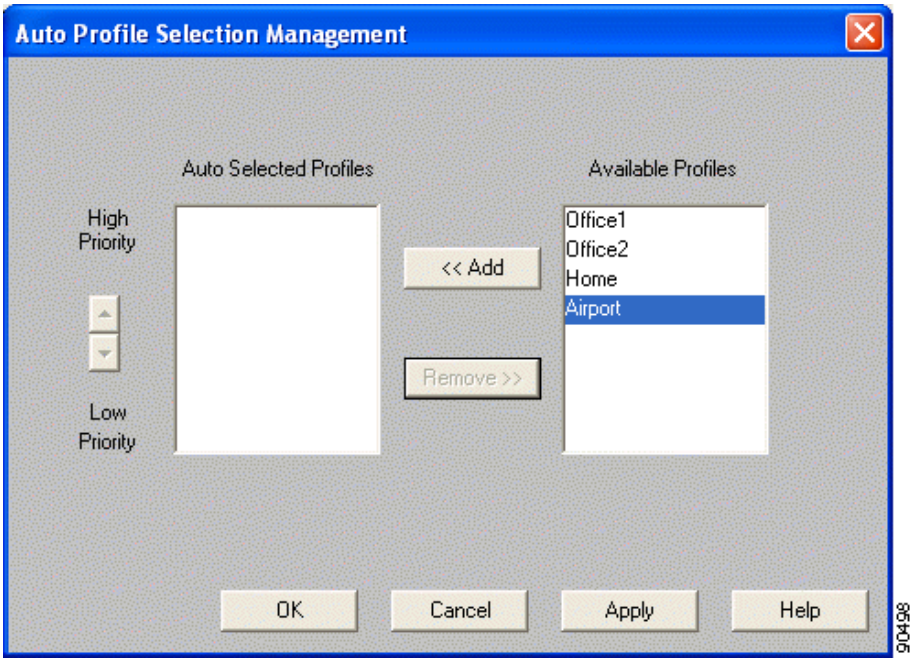


Step 3 Manage and add profiles

The following rules apply to the auto profile selection:

- At least two profiles must be included in the Auto Selected Profiles Box.
- The profiles must specify an SSID; otherwise, they cannot be selected in the Available Profiles box.
- Profiles cannot specify multiple SSIDs; otherwise, they cannot be selected in the Available Profiles box.
- Each profile that is included in auto profile selection must have a unique SSID. For example, if Profile A and Profile B both have "ABCD" as their SSID, only Profile A or Profile B can be included in auto profile selection.

a. Click the **Manage** button next to the Use Auto Profile Selection option. The Auto Profile Selection Management screen appears



b. All the created profiles are listed in the Available Profiles box. Highlight each one to include in auto profile selection and click the **Add** button. The profiles move to the Auto Selected Profiles box.

c. The first profile in the Auto Selected Profiles box has the highest priority while the last profile has the lowest priority. To change the order and priority of the auto-selectable profiles, highlight the profile to be moved and click the **High Priority** or **Low Priority** arrow to move the profile up or down, respectively.

d. Click **OK** to save the changes.

When auto profile selection is enabled, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID and so on.

To remove a profile from auto profile selection, highlight the profile in the Auto Selected Profiles box and click the Remove button. The profile moves to the Available Profiles box.

Step 4 Connect to the highest priority AP

Connecting to APs in various venues becomes very easy. Follow the instructions below to observe the auto profile feature.

a. With the **Select Profile** window open, select the **Use Auto Profile Selection**

b. Click **OK**

c. A connection to the first AP in the list should be established. If not, turn off the client radio and then turn on the radio.

d. After connecting to the highest priority AP, turn off the AP. Observe the ACM icon status.

e. Since the High Priority AP is down, the Auto Profile will attempt to connect to the AP. After an unsuccessful attempt, the Profile Manager will try to connect using the second highest profile in the list.

Lab 2.5.5.2 Configure Auto Profiles using ADU

Estimated Time: 25 Minutes

Number of Team Members: six teams with two students per team

Objective

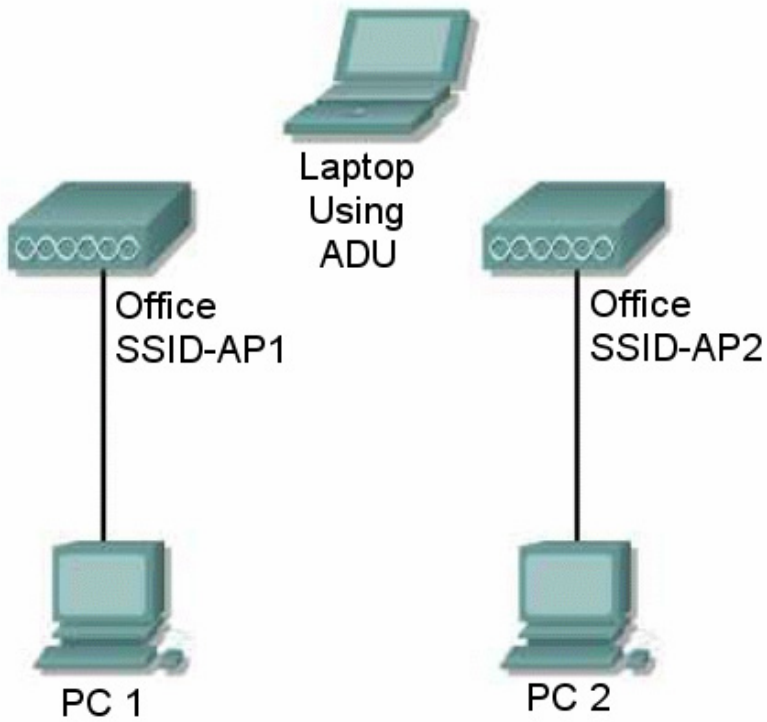
The student will learn the procedures for configuring ADU to use Auto Profiles.

Scenario

The **Auto Selected Profiles** configuration option causes the client adapter to automatically use a profile from the list when attempting to associate with a network.

If the client adapter loses association for more than 10 seconds, the driver switches automatically to another profile that is included in **Auto Selected Profiles** list. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value). To force the client adapter to associate to a different AP, the desired profile must be selected from the **Profile Management** window.

Topology



Preparation

This lab will require the following materials:

- 3 Desktop or Laptop PC
- Appropriate wireless client adapter card
- One Cisco Aironet Client Adapter Network Interface Card.
- Aironet Desktop Utility
- Two configured APs (instructor must setup)
    - AP1 – SSID of AP1
    - AP2 – SSID of AP2
    - AP3 – SSID of AP3 (optional)
    - AP4 – SSID of AP4 (optional)

Step 1 Creating multiple profiles

a. Remove any existing profiles using the Aironet Desktop Utility.

b. Create 4 new profiles based on the following table.

Profile	Profile Name	Client Name	SSID
1	Office1	StudentP1	AP1
2	Home	StudentP2	AP2
3	Office2	StudentP3	AP3
4	Airport	StudentP4	AP4

(Where StudentP is the student name)

Step 2 Including profiles in auto profiles selection

After creating the four profiles for the client adapter, use the Order Profiles button to add profiles to the **Auto Selected Profiles** list.

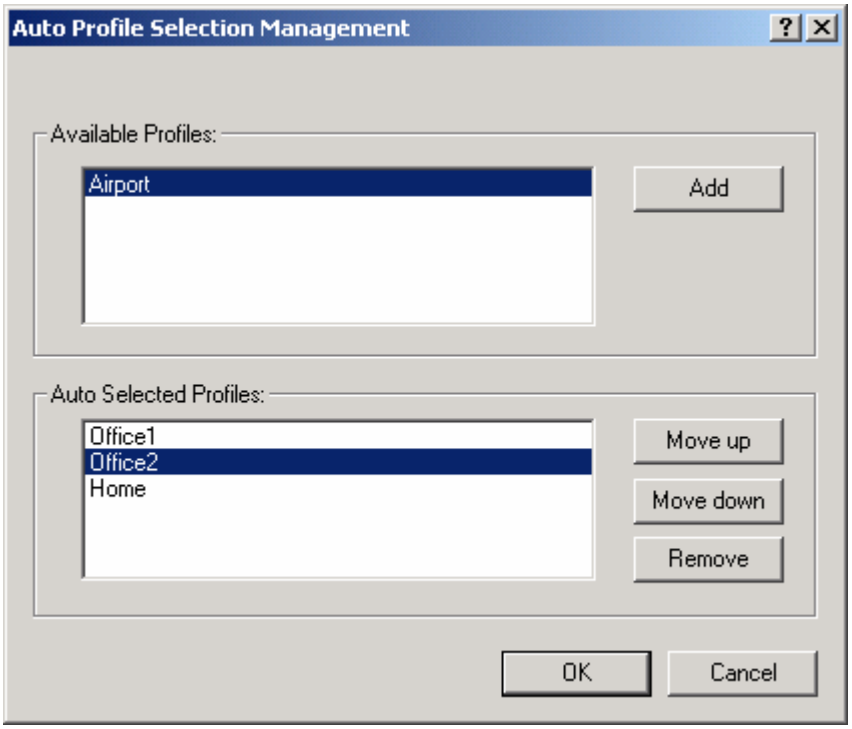
Follow the steps below to include the profiles in auto profile selection and to establish the order in which the profiles will be selected for use.

a. Open the ADU and click the **Order Profiles** button. Add profiles from the **Available Profiles** list to the **Auto Selected Profiles** list.

b. Use the **Move Up** and **Move Down** buttons to rearrange the profiles in the order as listed in the table.

The following rules apply to the auto profile selection:

- The profiles must specify an SSID; otherwise, they cannot be selected in the Available Profiles box.
- Profiles cannot specify multiple SSIDs; otherwise, they cannot be selected in the Available Profiles box.
- Each profile that is included in auto profile selection must have a unique SSID. For example, if Profile A and Profile B both have "ABCD" as their SSID, only Profile A or Profile B can be included in auto profile selection.



When auto profile selection is enabled, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID and so on.

To remove a profile from auto profile selection, highlight the profile in the **Auto Selected Profiles** box and click the **Remove** button. The profile moves to the Available Profiles box.

Step 3 Connect to the highest priority AP

Connecting to APs in various venues becomes very easy. Follow the instructions below to observe the auto profile feature.

a. After connecting to the highest priority AP, turn off the AP. Observe the ACM icon status.

b. Since the High Priority AP is down, the Auto Profile will attempt to reconnect to the AP. After an unsuccessful attempt, the Profile Manager will try to connect using the second highest profile in the list.

c. If the first AP is turned back on and the second AP is now turned off, the client adapter will reconnect to the first.

Lab 2.6.5.1 ACU Utilities

Estimated Time: 10 Minutes

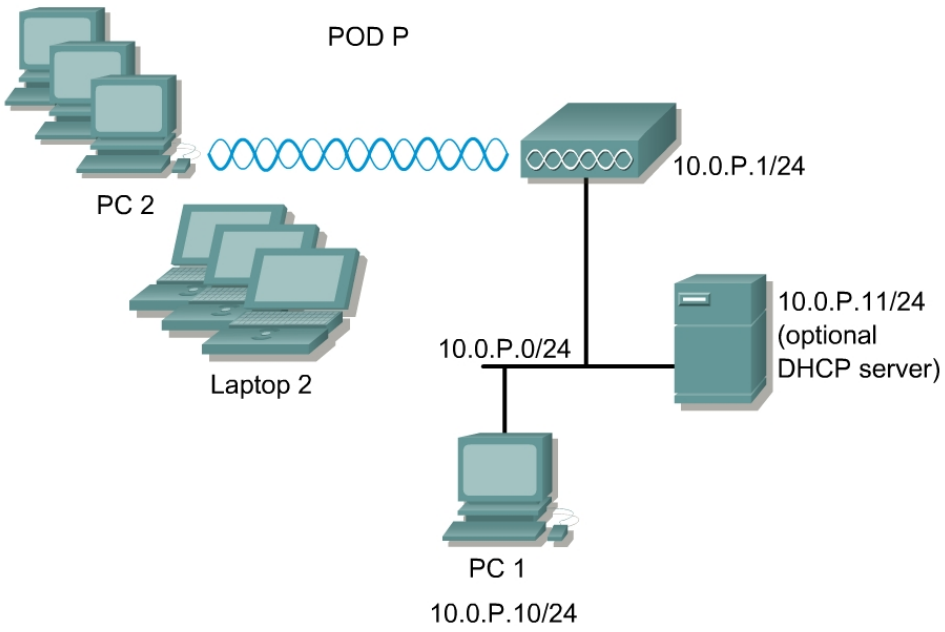
Number of Team Members: 2 students per team

Objective

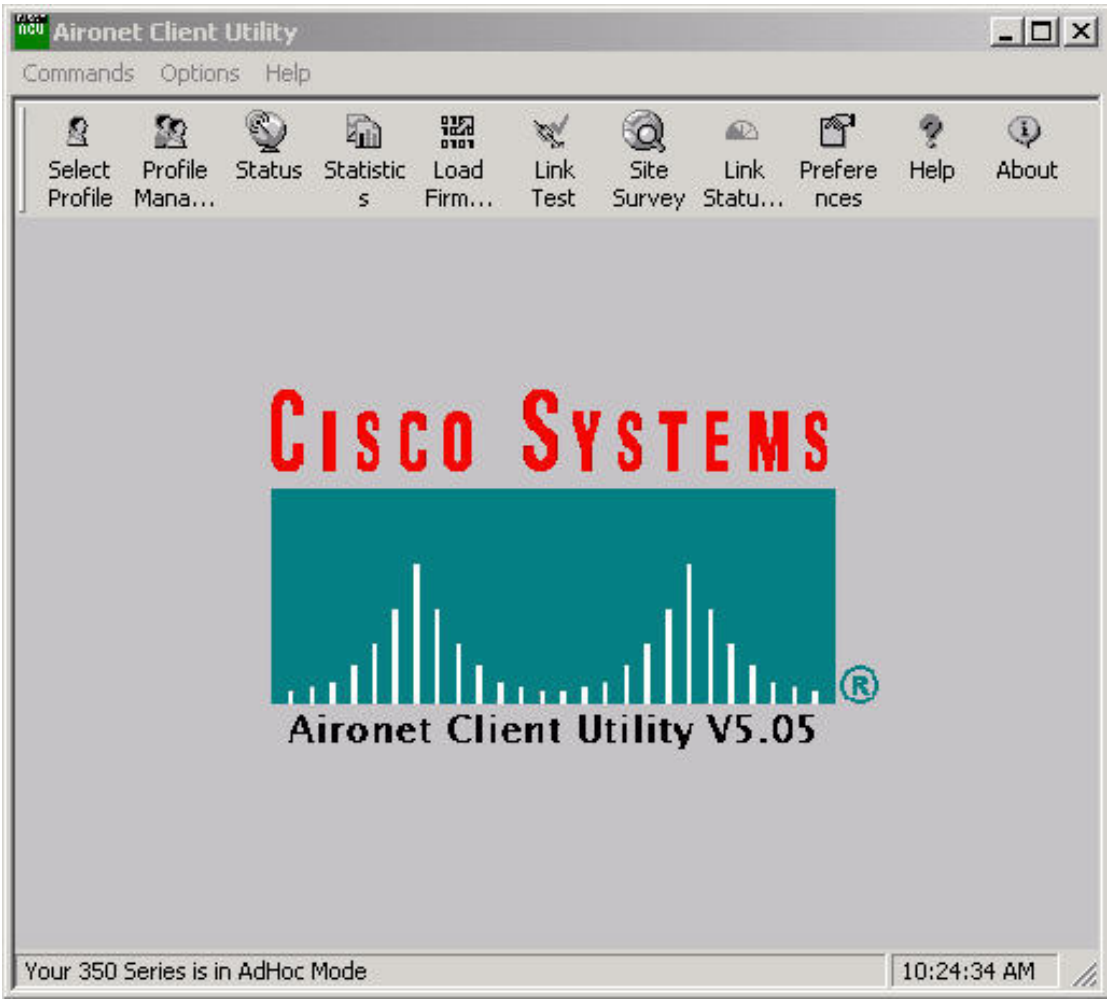
Students will use the Aironet Client Utilities (ACU) to complete the following tasks:

- Assess the performance of the Radio Frequency (RF) link
- View the status of the wireless network
- View the statistics of the wireless network
- View the link status of the wireless network

Topology



Scenario



ACU provides tools that enable a wireless technician to assess the performance of the client adapter and other devices on the wireless network. ACU diagnostic tools perform the following functions:

- Display the current status and configured settings of the client adapter
- Display statistics pertaining to the transmission and reception of data of the client adapter
- Display a graphical image of the client adapter RF link
- Run an RF link test to assess the performance of the RF link between the client adapter and its associated AP.

Preparation

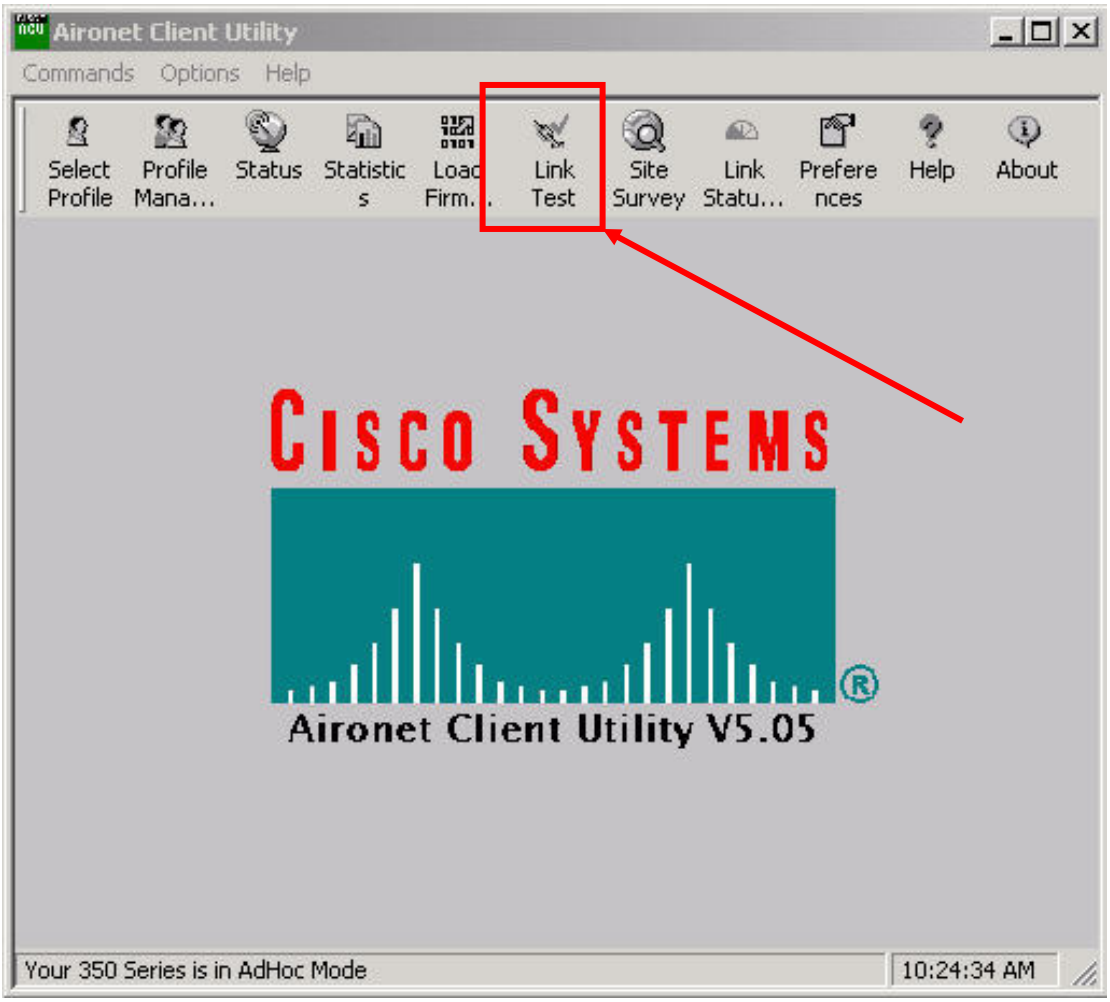
The instructor will prepare one AP that will be used by the whole class to perform this lab exercise. An IP address and SSID must be configured for the AP.

Step 1 Run an RF link test

The ACU link test tool sends out pings to assess the performance of the RF link. The test is performed multiple times at various locations throughout the lab area. The test is designed to run at the data rate set in the Edit Properties - RF Network section of ACU.

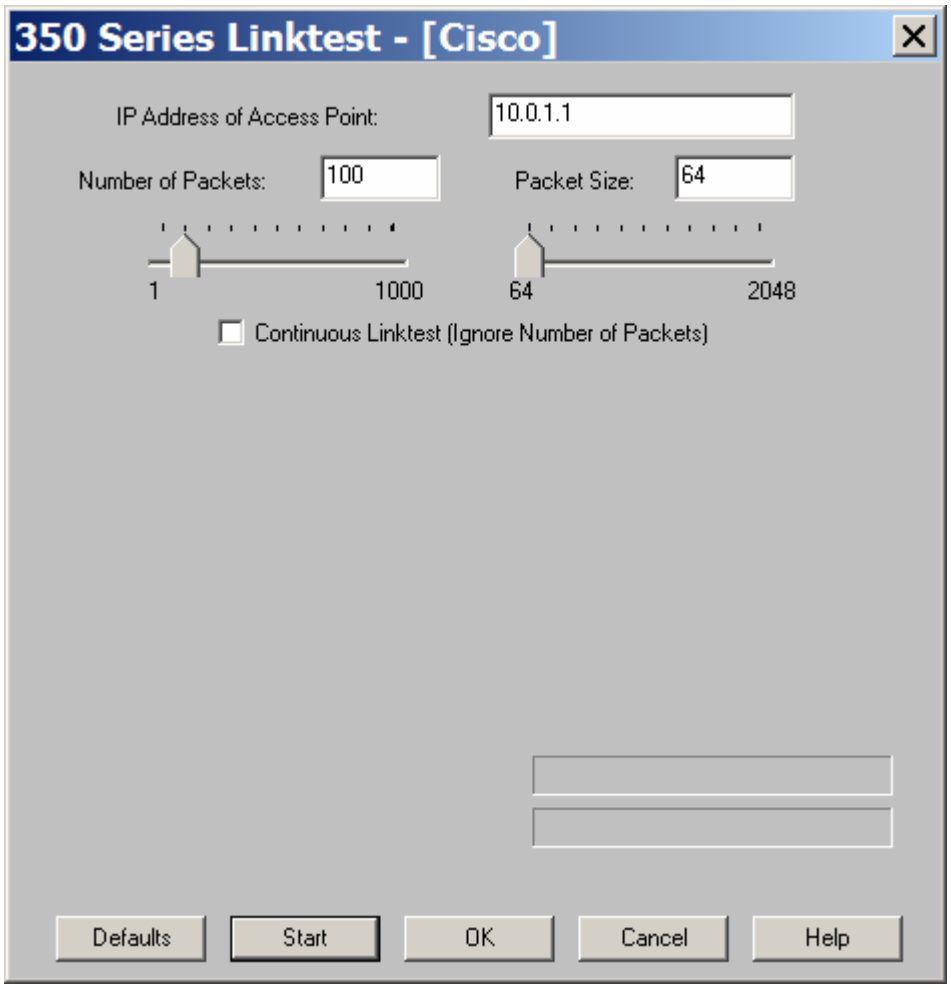
The results of the link test can be used to determine the RF network coverage and ultimately the required number and placement of APs in the network. The test also helps installers avoid areas where performance is weak. Therefore the test helps to eliminate the risk of a lost connection between the client adapter and its associated AP.

Because the link test operates above the RF level, it does more than test the RF link between two network devices. It also checks the status of wired sections of the network and verifies that TCP/IP and the proper drivers have been loaded.



Select the **Link Test** button from the Aironet Client Utility screen. The Link Test Screen will appear on the desktop.

Step 2 Link test screen



In the IP Address of AP field, notice, by default, the IP address is the AP to which the wireless NIC is associated. This IP address could be changed to another wireless device IP address.

The link test can be setup to run until it has attempted to send a specific number of packets or to run until it is stopped. Choose one of the following steps to determine how long the link test will run:

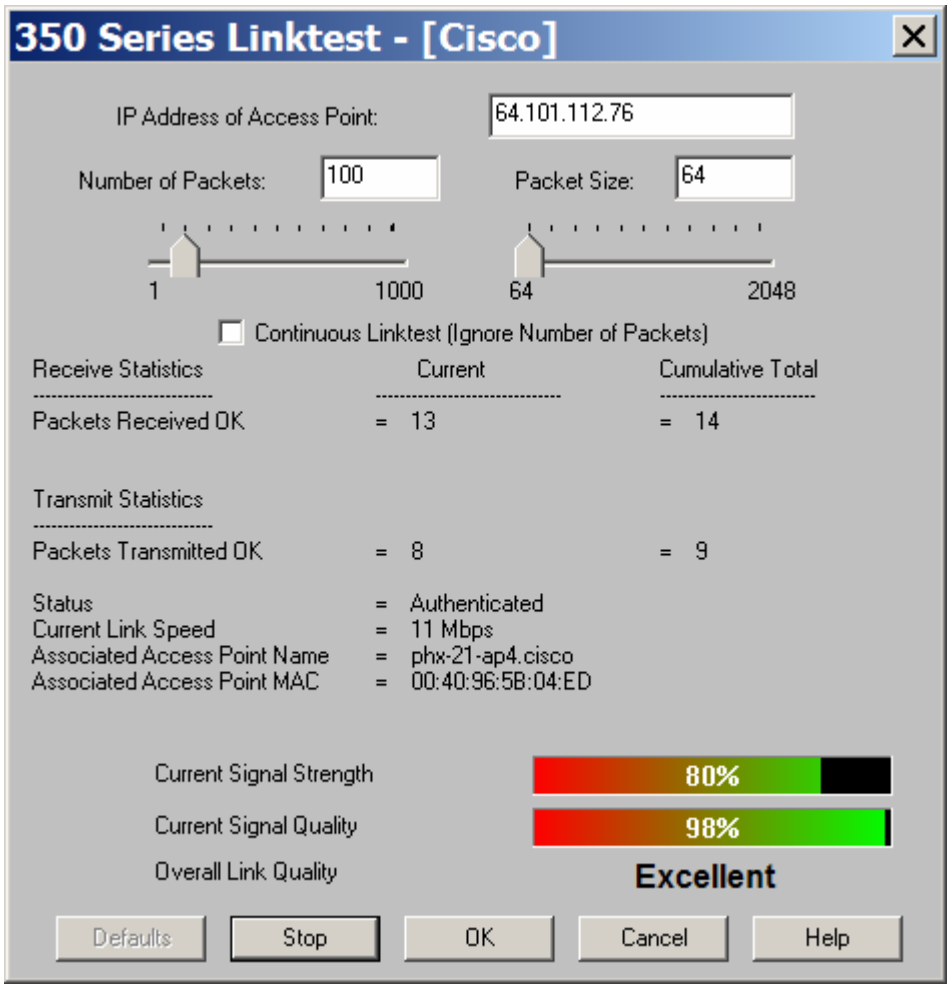
a. Select the number of packets that the link test should attempt to send. A number can be entered in the Number of Packets field or the slider can be used to select this value. (The Number of Packets parameter is ignored if the Continuous Linktest checkbox is selected.)
Range: 1 to 1000
Default: 100

b. Select the Continuous Linktest checkbox to allow the link test to run continuously.
Default: Deselected

c. Select the size of the data packet that is to be sent. Using the ACU, a number can be entered in the Packet Size field or the slider can be used to select this value.
Range: 64 to 2048
Default: 64

d. Leave all options to the default settings.

Step 3 Run the link test



Click the **Start** button to run the link test. While the test is running, statistics are displayed and updated periodically.

a. What is the Cumulative Total of the AP Receive Statistics (Packets)?

_____

b. What is the Cumulative Total of the AP Transmit Statistics (Packets)?

_____

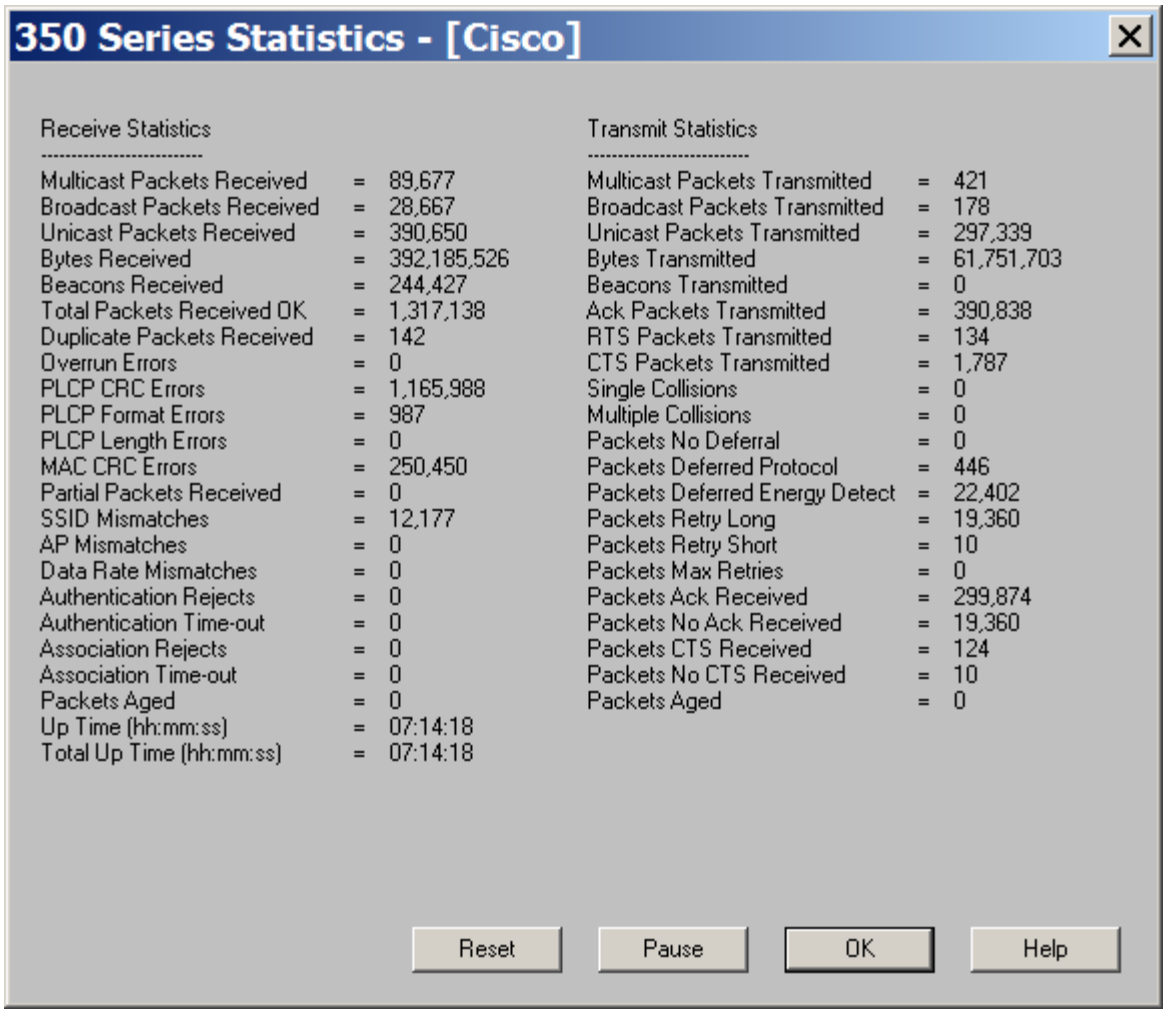
Step 4 Status screen

a. From the Aironet Client Utility screen, select the **Status** button.

b. Complete the following list of information about the Wireless Infrastructure status that is displayed on this page:

1. Firmware version _____
2. Is WEP enabled or disabled _____
3. IP Address _____
4. Current Link Speed _____
5. Current Power Level _____
6. Channel or Frequency _____
7. Status _____
8. SSID _____
9. Power Save Mode _____
10. Associated AP Address _____
11. Associated AP MAC Address _____

Step 5 Statistics screen



From the Aironet Client Utility screen, select the **Statistics** button.

a. Which statistics are incrementing greater, transmit or receive? Why?

_____

_____

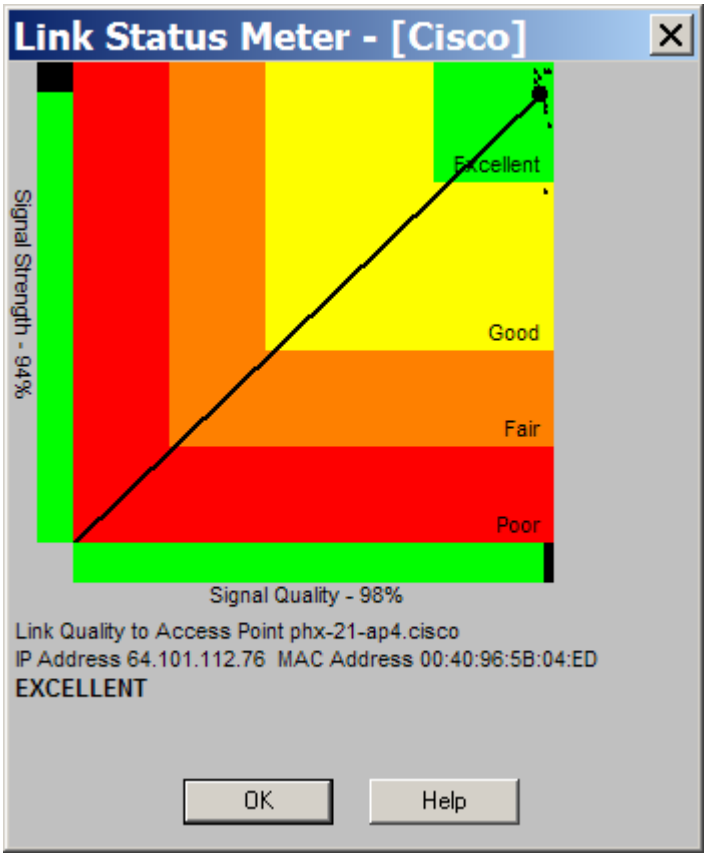
_____

_____

b. Define the following terms from the Statistics screen:

1. **RTS** _____
2. **CTS** _____
3. **ACK** _____

Step 6 Link Status Meter



a. Bring up the Link Status Meter. Click the **Link Status Meter** button on the ACU.

b. Observe the Signal Quality over a period of 30 seconds.

1. What is the Signal Quality of the AP?

_____

2. What is the Signal Strength of the AP?

_____

Lab 2.6.5.2 Using ADU Utilities

Estimated Time: 10 Minutes

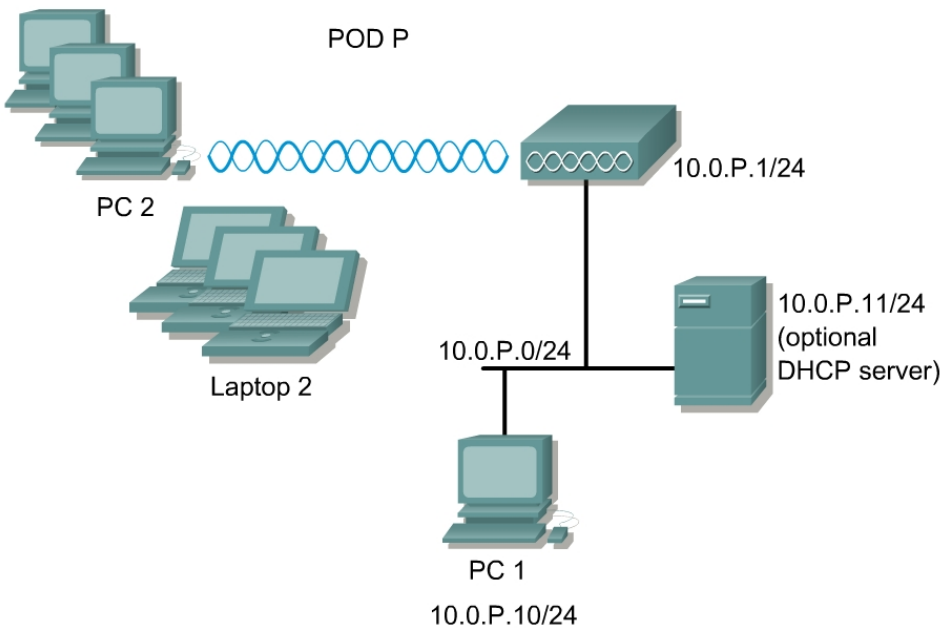
Number of Team Members: 2 students per team

Objective

Students will use the Aironet Desktop Utility (ADU) to complete the following tasks when using a Cisco Aironet IEEE 802.11a/b/g Wireless Adapter:

- Assess the performance of the Radio Frequency (RF) link
- View the general and advanced transmit/receive statistics
- View the adapter information
- Run and analyze troubleshooting reports

Topology



Scenario

The ADU provides tools that enable a wireless technician to assess the performance of the client adapter and other devices on the wireless network. ADU diagnostic tools perform the following functions:

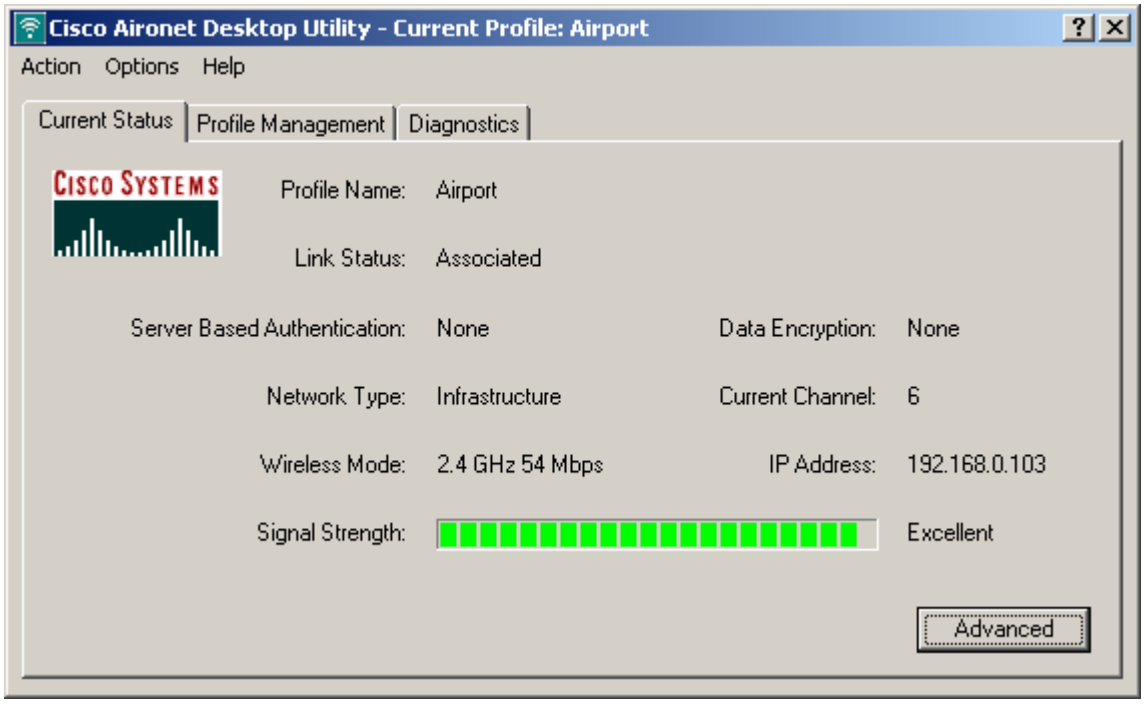
- Display the current status and configured settings of the client adapter
- Display statistics pertaining to the transmission and reception of data of the client adapter
- Display a graphical image of the client adapter RF link
- Run an RF link test to assess the performance of the RF link between the client adapter and its associated AP.

Preparation

The instructor will prepare one AP that will be used by the whole class to perform this lab exercise. An IP address and SSID must be configured for the AP. The instructor must announce or post the AP SSID to which student clients should connect.

Step 1 View the current status of the client adapter

Open the ADU application from either the Start Menu or by right-clicking the client monitor icon from the System Tray. From the **Current Status** tab, a number of useful settings can be seen.



Record the following information from the **Current Status** screen:

1. Profile Name: _____
2. Network Type: _____
3. Data Encryption: _____
4. Adapter IP Address: _____

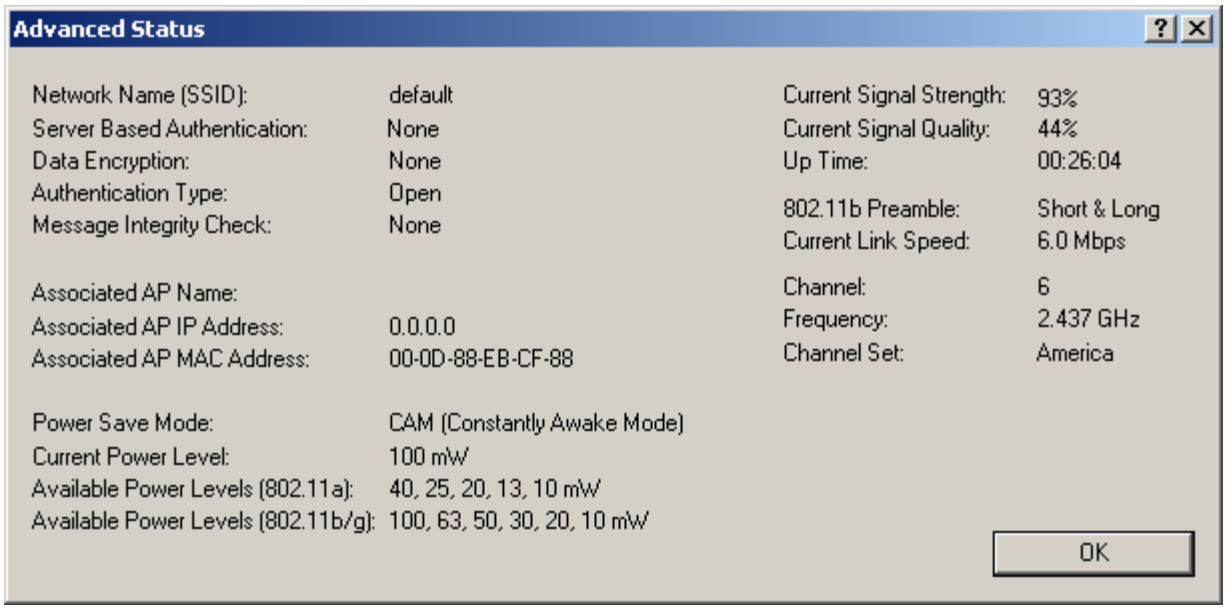
If the connection is made from a laptop computer, move the computer to another part of the room and observe the **Signal Strength**. The graphical display should change as the adapter receives a stronger or weaker signal from the access point.

Step 2 Advanced information

The **Advanced** button can be used to view more detailed statistics for the adapter. Information in the **Advanced Status** window includes settings that have been assigned for SSID, Channel, and Available Power Levels.

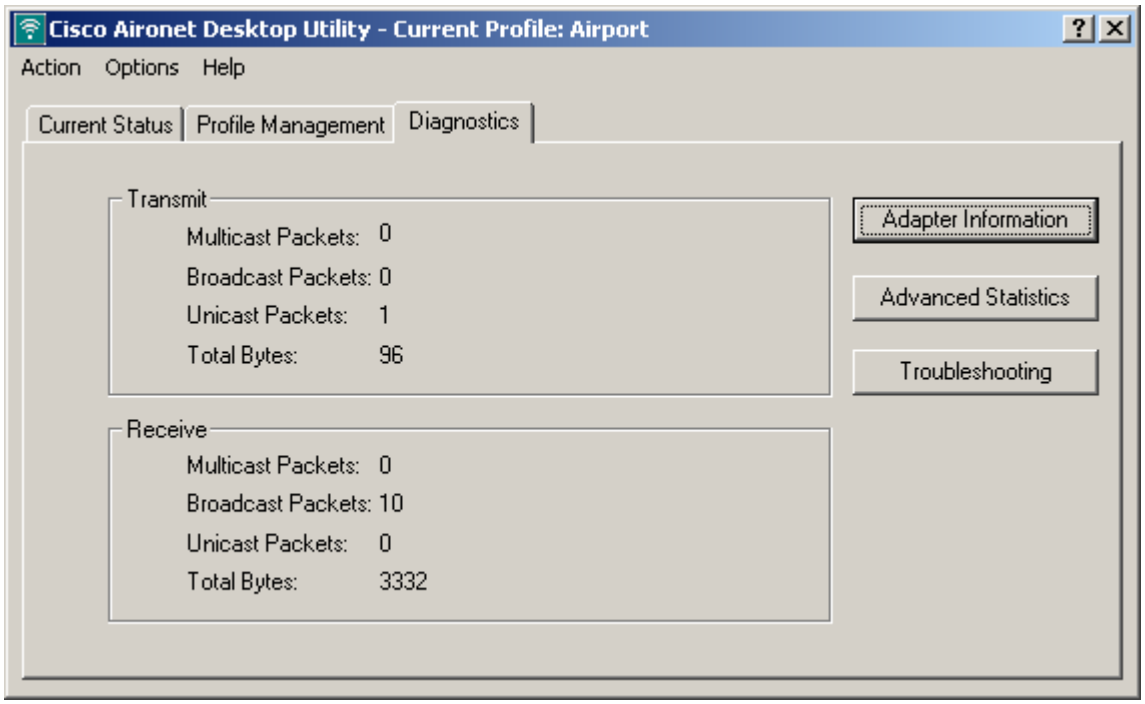
If the access point has been configured to move to the least congested channel, the information in this screen can be used to determine which channel has been selected.

1. Record the current **Channel** from the Advanced Status screen for the adapter: _____
2. Record the current **Link Speed**: _____
3. Record the **Signal Strength** and **Quality**: _____

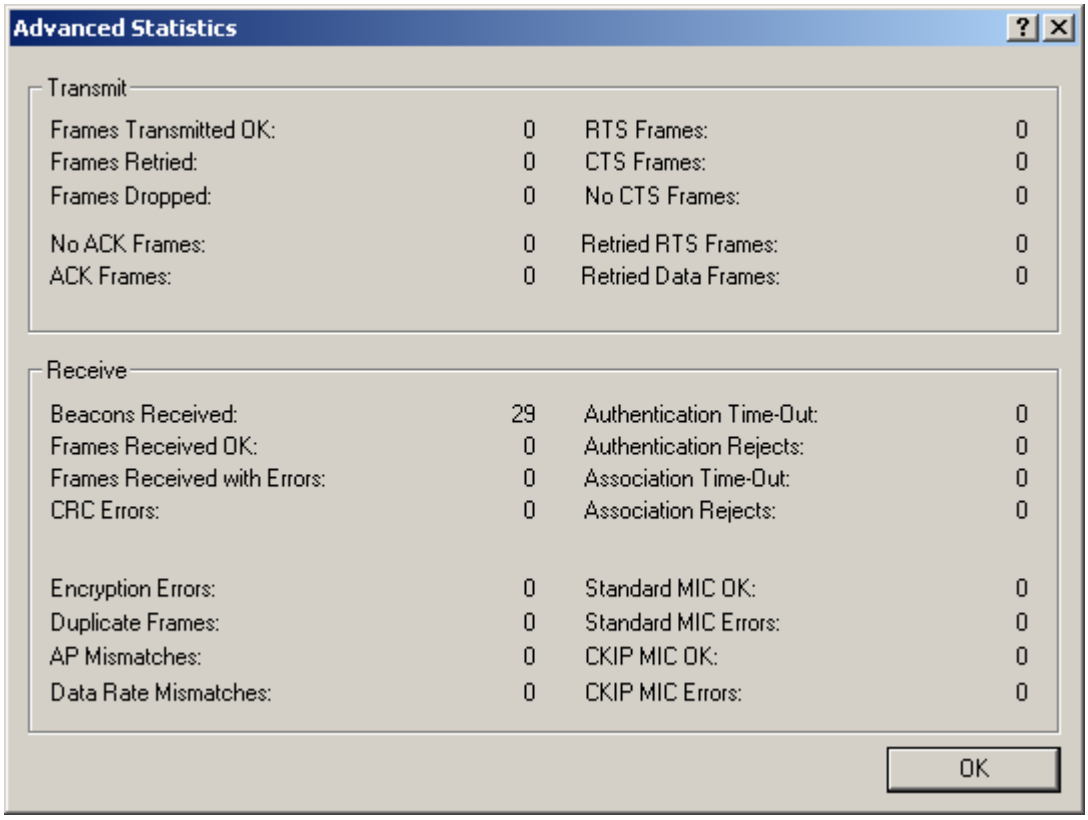


Step 3 Diagnostics

The **Diagnostics** tab has several useful utilities. Basic transmit and receive statistics are presented on the main page. These statistics are useful to determine if the adapter is sending and receiving wireless data.

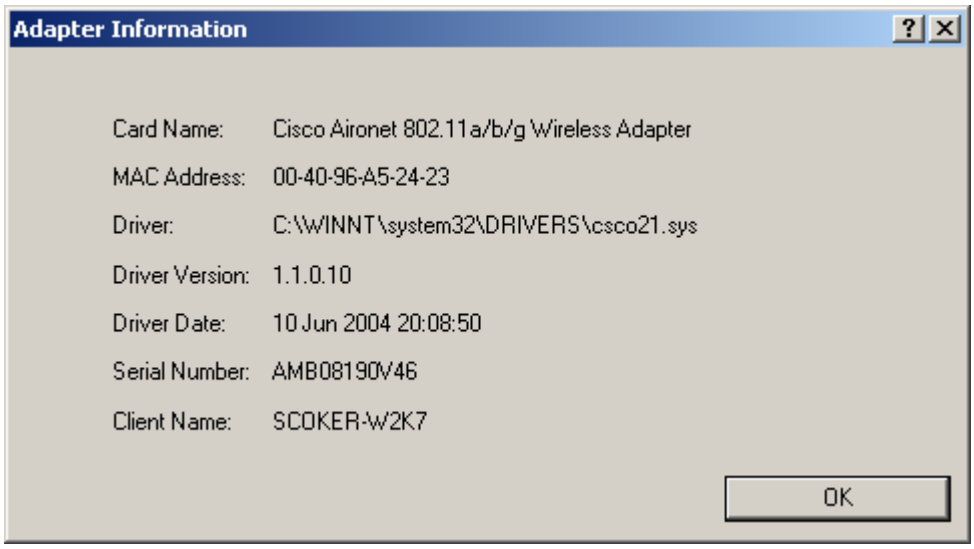


Clicking the **Advanced Statistics** button will open up a window with more detailed information for the wireless connection. Two of the most useful categories of information in this window include authentication statistics and encryption error statistics. When security is applied to the access point, these statistics will be useful to determine if the adapter has had authentication or encryption errors.



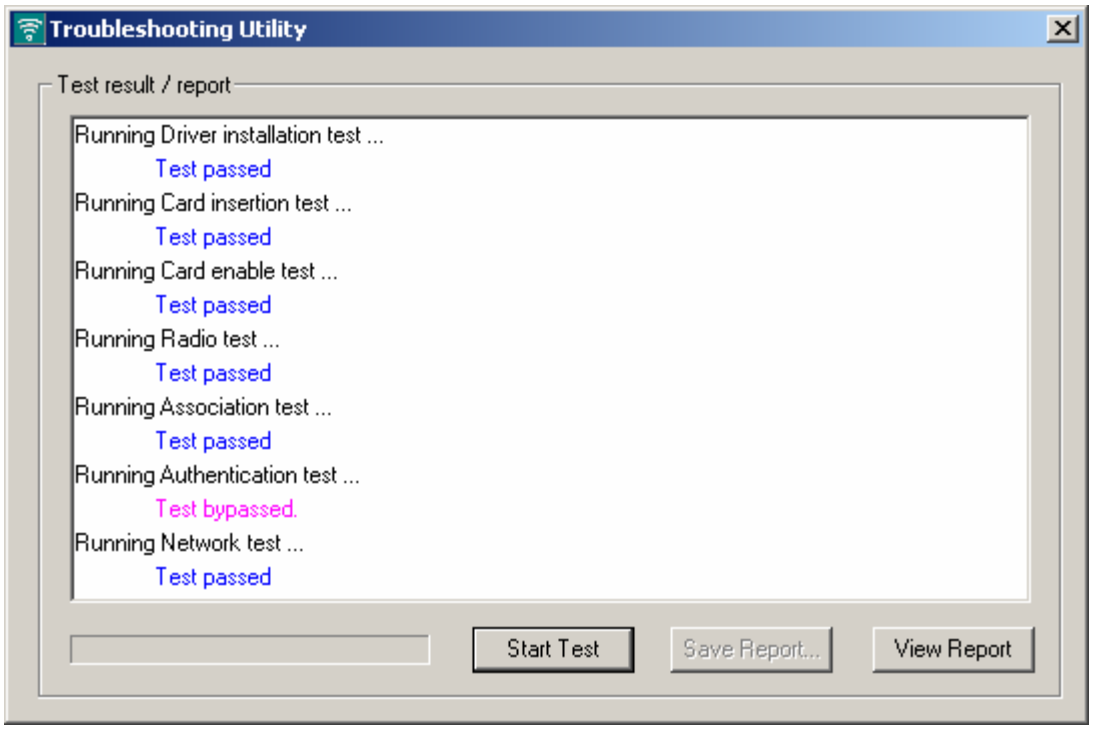
The Adapter Information button opens a window that provides information about the adapter hardware. One very useful parameter displayed is the adapter MAC address.

1. Record the adapter MAC address here: _____

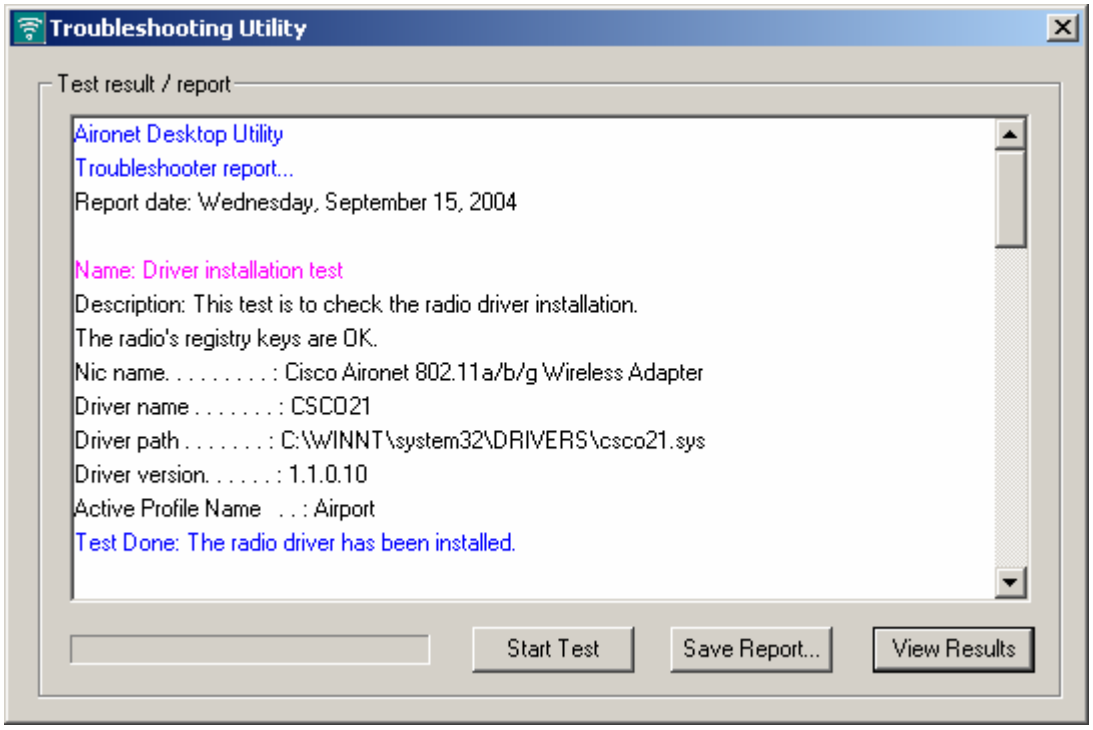


Step 4 Troubleshooting

The **Troubleshooting** button is used to access the built in diagnostic tests. Click the **Start Test** button to begin the diagnostic tests.



Once the tests have completed, a detailed report can be viewed. This report provides useful information for troubleshooting both the hardware and software configuration of the wireless adapter.



Scroll through the test results and record the following information:

1. Active Profile Name: _____
2. AP name: _____
3. AP IP address: _____
4. Default network gateway: _____

Lab 2.6.5.3 Creating an Adhoc Network

Estimated Time: 30 Minutes

Number of Team Members: Students will work in teams of two for this lab process

Objective

Each team will configure several personal computers to communicate with each other without an AP or cables.

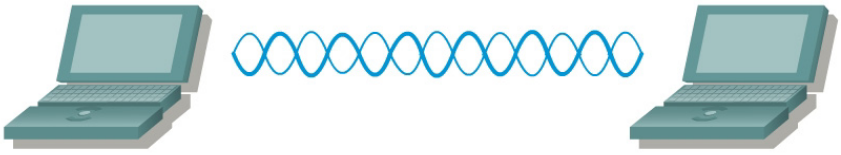
Scenario

Several PCs equipped with Cisco Aironet Client Adapters will be needed. They should be installed and setup. Configure the Aironet Client Utility (ACU) to allow them to connect together as a network without an AP. Perform some of the diagnostics included in the ACU for Ad Hoc mode.

Passive mode differs from active mode in Wireless LANs. The diagnostics tests that are performed in Passive mode can help determine the best placement and coverage for the AP of the network. Instead of using an AP, the other PC becomes the wireless client that can provide similar information.

Active Mode performs these diagnostics with the use of an AP. This lab is an exercise to familiarize the student with how to gather some of this valuable information.

Topology



Preparation

Prior to this lab, all the PCs should be equipped with working Cisco Aironet Client Adapters. The Aironet Client Utility should be installed on the computers.

It is very important for the instructor to assign team numbers. Also, unique IP Addresses should be assigned to each client adapter or personal computer within each team to avoid IP conflicts.

Each team should use the same SSID for each PC in the pod to ensure that the computers associate to each other. The SSID to be used for all PCs is adhocP (where P is the group number assigned by the instructor).

The instructor should help students understand the addressing scheme. Using the information in the following chart, configure the host computers. Note that no default gateway is needed. By assigning unique IP addresses and SSIDs, the students avoid conflict with other teams.

Team	Client Name	SSID	Client Address
1	Client1a	Adhoc1	10.0.1.10/24
	Client1b	Adhoc1	10.0.1.11/24
2	Client2a	Adhoc2	10.0.2.10/24
	Client2b	Adhoc2	10.0.2.11/24
3	Client3a	Adhoc3	10.0.3.10/24
	Client3b	Adhoc3	10.0.3.11/24

The following tools and resources will be required to complete this lab:

Two PCs equipped with the Cisco Aironet Client Adapter per group. One of the computers should be a laptop for mobility purposes.

Step 1 Create a profile named adhocP (where P is the team number)

a. Open the Cisco Aironet Client Utility.

b. Click on the **Profile Manager** icon.

c. Click on the **Add** button.

d. Click on the **OK** button.

e. From the System Parameters tab, type Adhoc# (where # is the group number assigned by the instructor) in the SSID1: box.

f. In the Network Type section, select the **Ad Hoc** radio button.

g. Power Save Mode can be left as the Default Constantly Awake Mode (CAM) setting at this time.

h. Click the **OK** button.

i. Exit Profile Manager by clicking on the **OK** button.

Step 2 Select the profile named adhocP (where P is the team number)

a. From the Aironet Client Utility, click on **Select Profile** icon.

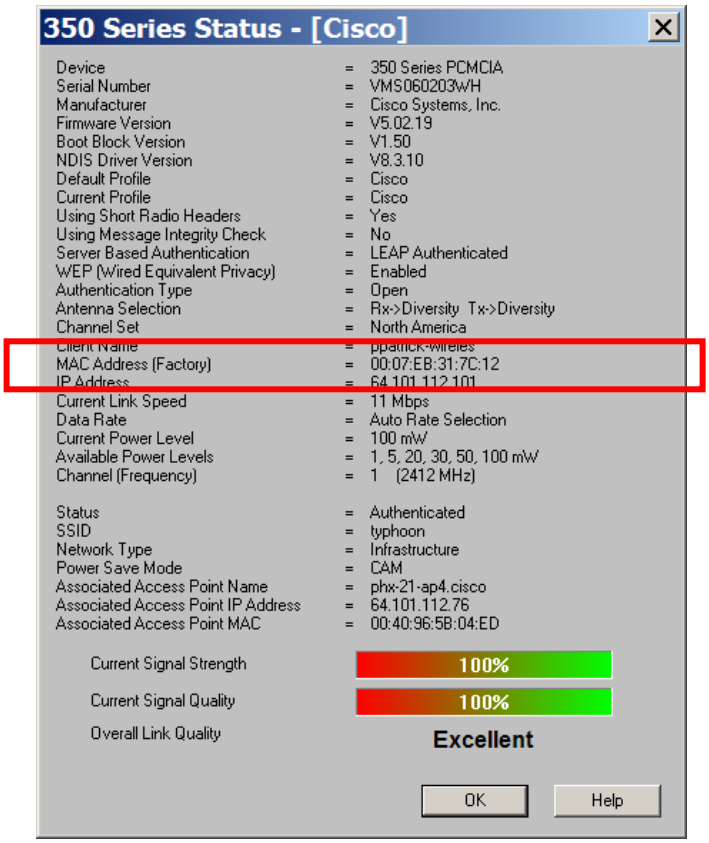
b. From the Use Selected Profile drop down box, select **adhocP**.

c. Click on the **OK** button.

d. Notice that a message appears on the status line at the bottom the Aironet Client Utility that the wireless NIC is in AdHoc Mode.

Step 3 Obtain the MAC address of the PC

a. Click the Status button on the ACU.



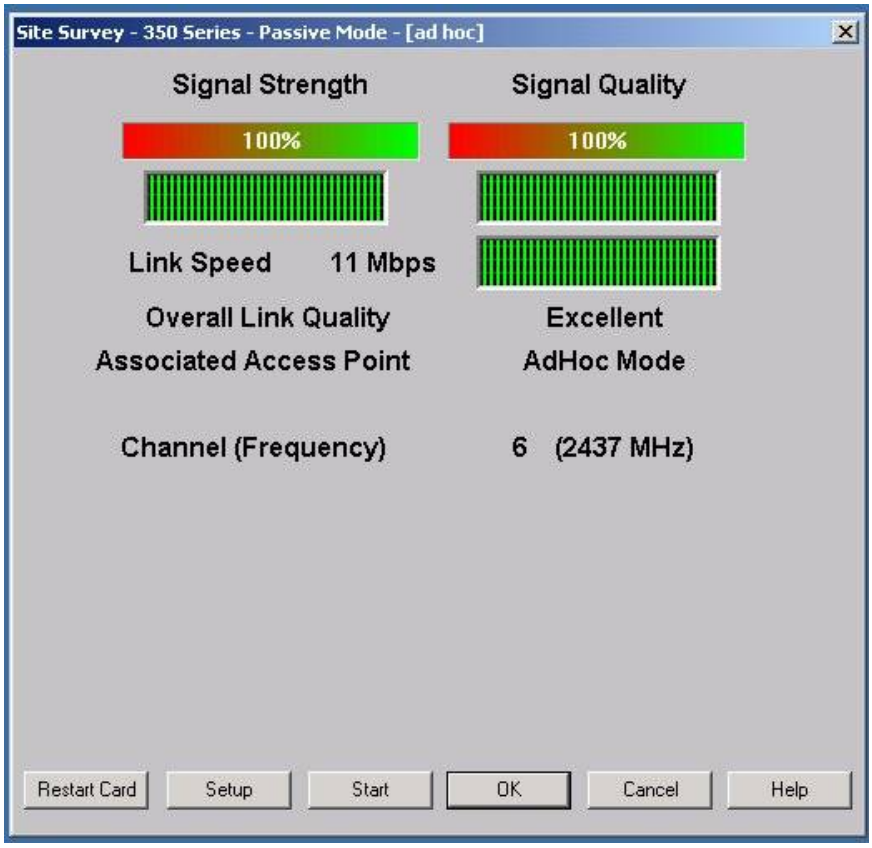
b. What is the MAC address of the computer? Provide this information to your team partner so diagnostics can be performed.

_____

c. Write your partner's MAC address.

_____

Step 4 Ad Hoc Site Survey Passive Mode



a. Click on the **Site Survey** button. This will start the Site Survey Passive mode.

b. Click on the **Setup** button to start the Site Survey Setup mode.

c. Type in the Destination MAC address of your partner's PC that was obtained. That is the PC that will be used for an ad hoc site survey. Try this a few different times with different members of the class.

d. Click the **OK** button to go back to the Ad Hoc Passive Mode Screen.

e. Click the **Start** button to initiate an active mode site survey.

f. What additional information was added to the Ad Hoc Site Survey Screen?

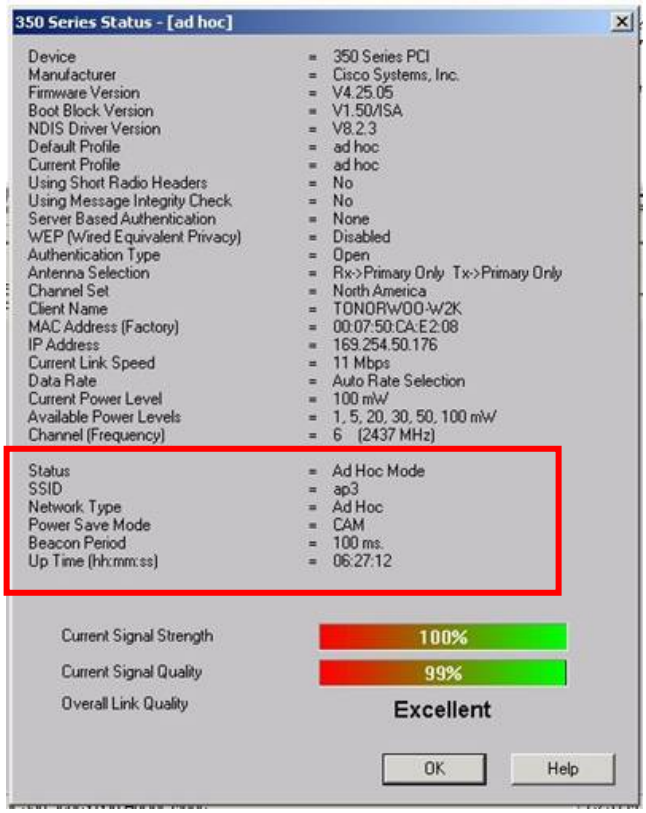
_____

_____

_____

_____

Step 5 Ad Hoc Status screen



1. What is the Status of the PC?

_____

2. What is the SSID of the PC?

_____

3. What is the Network Type of the PC?

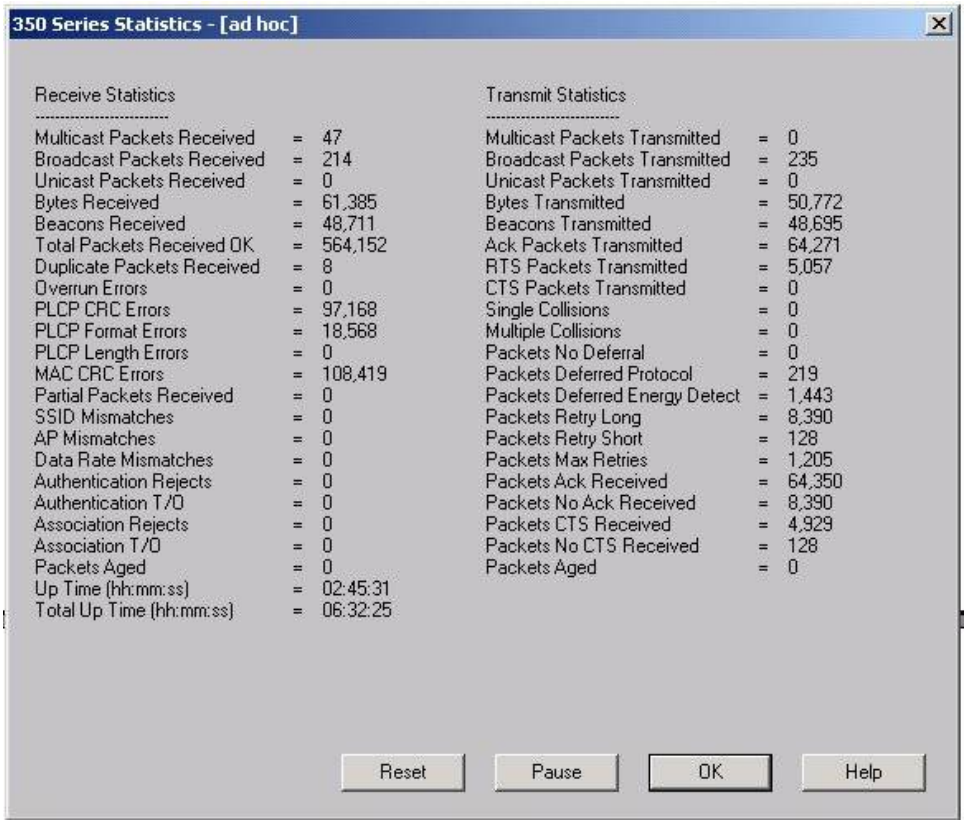
_____

4. What is the Power Save Mode of the PC?

_____

Note	Optional: Walk around the class and note the change in Signal Strength and Signal Quality.

Step 6 Ad Hoc Statistics screen



a. How many Broadcast packets were received?

_____

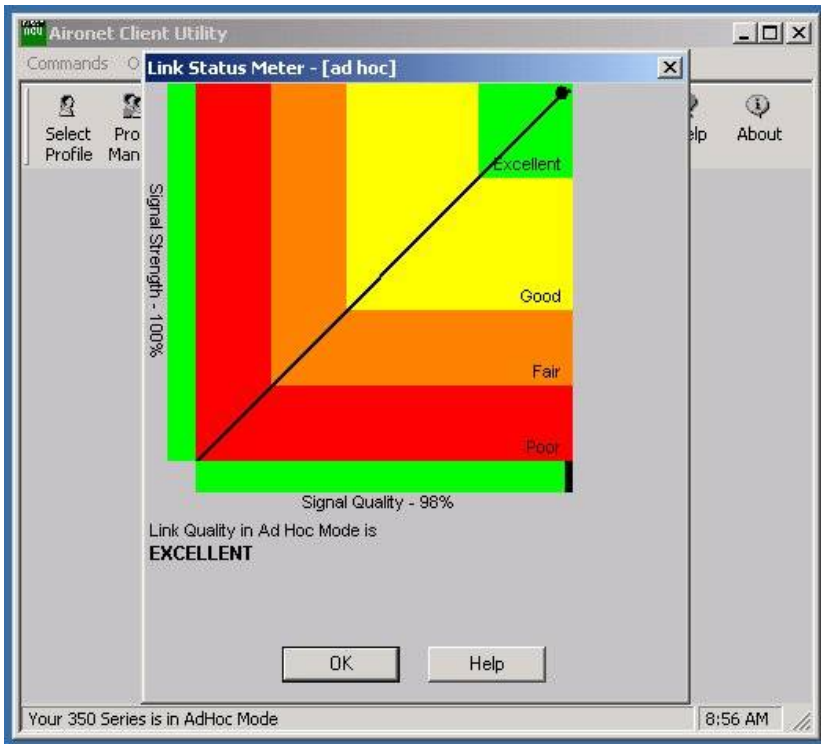
b. How many Broadcast packets were transmitted?

_____

c. Exit from the Ad Hoc Statistics screen by selecting **OK**.

Step 7 Link Status Meter screen

Once Ad Hoc mode is configured properly on the computer, click on the **Link Status Meter** (LSM) icon with the Aironet Client Utility (ACU) to activate the Link Status Meter. Note the position of Signal Strength and Signal Quality indicator line on the meter.



If using a laptop, answer the following questions.

a. Move the laptop around the area. Note how the Link Status Meter behaves. What is the approximate distance that the two computers can be apart before they disassociate?

_____

b. Move one of the computers behind a metal bookcase or file cabinet. Was there a noticeable change in signal quality or signal strength?

_____

c. Try this same experiment with other materials such as the glass window, walls, desks, plastic objects. Which of the materials had the greatest effect on the signal quality or signal strength?

_____

d. If a 2.4 GHZ phone is available, activate the talk button near one of the computers. Note the Link Status Meter. What happens to the signal quality or signal strength?

_____

e. Move the computer behind a wooden door and note the Link Status Meter. Did the wooden door have any effect on the signal quality or signal strength?

_____

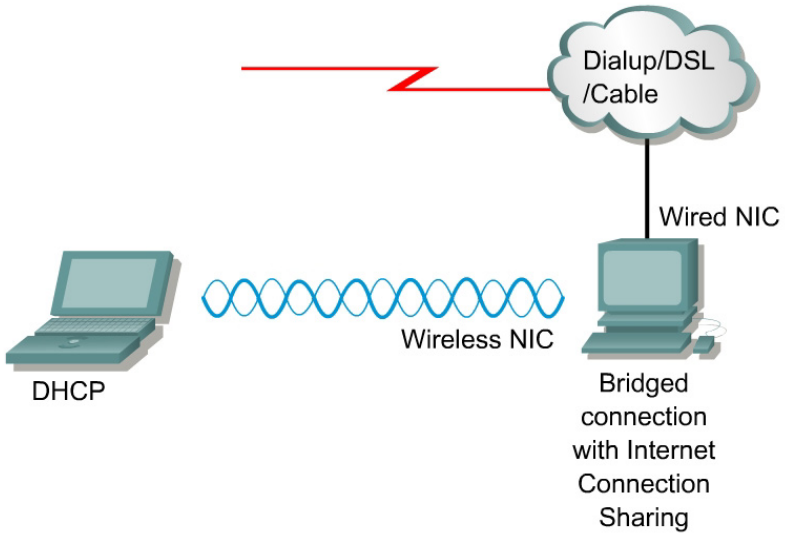
Step 8 File share in Ad Hoc Mode (OPTIONAL LAB)

Scenario 1—Setup a window file share, a web page, or a FTP server program on each PC. Transfer files from one PC to the other. Open a web browser and enter the IP address of the peer team member. If web services are enabled on the peer PC, then a web page should be displayed. Try to transfer a file by FTP between PCs.

Scenario 2—Setup a network game or program that requires network connectivity between PCs. Determine if there are any performance issues. Have other teams change to the adhoc network by matching the SSID and moving into the same IP subnet. Determine if there is a point at which network performance is an issue. Remember that network connectivity is more than ping or telnet traffic. Network application and user demands must always be tested to assure proper network performance after any wireless installation.

Scenario 3—Setup a PC as an mp3 file server and stream music across the wireless adhoc network. Determine if there are any performance issues. Have other teams change to the adhoc network by matching the SSID and moving into the same IP subnet. Determine if there is a point at which network performance is an issue.

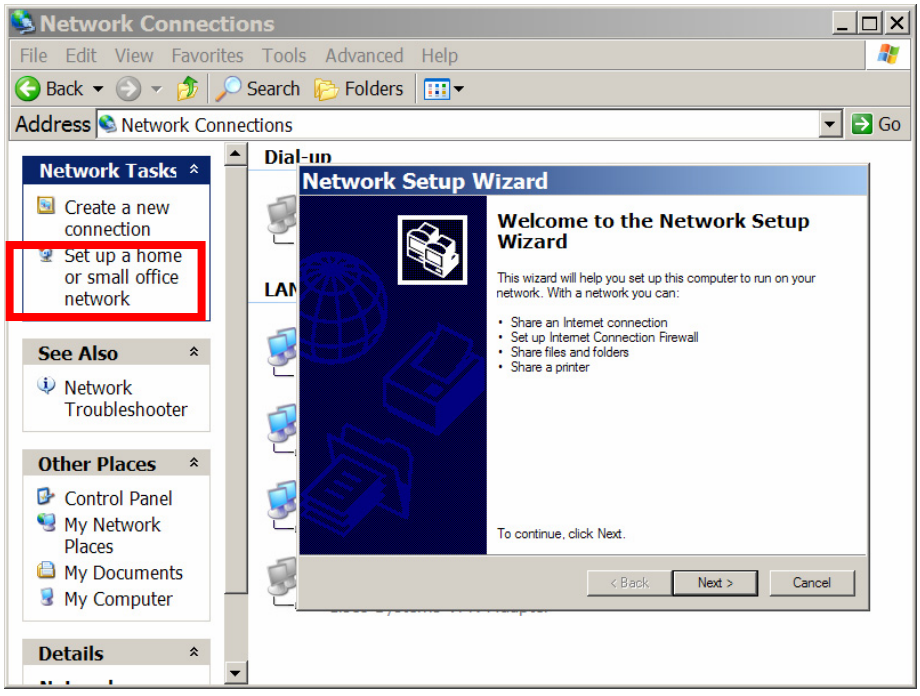
Step 9 Create an AdHoc Network with Internet connection sharing (OPTIONAL LAB)



Is it necessary to purchase an AP in order to share the fast broadband connection at home? This lab is very similar to using a cross-connect cable for a small PC network, but without the use of the router or additional cables.

a. Bridge the connection on the Desktop PC

b. Share an Internet connection



c. Configure Wireless NICs on both PCs in Adhoc mode.

Lab 2.6.5.4 Creating an Ad Hoc Network using ADU

Estimated Time: 30 Minutes

Number of Team Members: Students will work in teams of two for this lab process

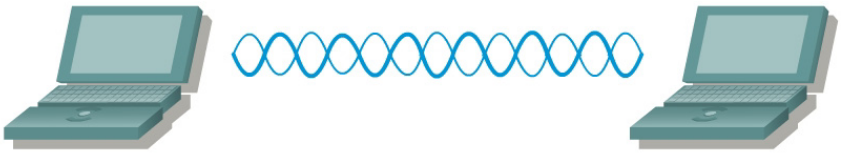
Objective

Each team will configure several personal computers to communicate with each other without an AP or cables.

Scenario

Several PCs equipped with wireless client adapters will be needed. They should be installed and setup. This lab will cover the Cisco® Aironet® IEEE 802.11a/b/g Wireless Adapter and how to configure the associated Aironet Desktop Utility (ADU) to allow them to connect together as a network without an AP. Other Cisco 802.11a and 11b clients, which utilize the Aironet Client Utility (ACU), can be used to create a mixed Ad Hoc environment, however students must follow instructions covered in the appropriate lab or configuration guide. Furthermore, students can utilize other vendor wireless adapters to apply skills learned in this lab.

Topology



Preparation

Prior to this lab, all the PCs should be equipped with working Cisco Aironet Client Adapters. The Aironet Desktop Utility should be installed on the computers.

It is very important for the instructor to assign team numbers. Also, unique IP Addresses should be assigned to each client adapter or personal computer within each team to avoid IP conflicts.

Each team should use the same SSID for each PC in the pod to ensure that the computers associate to each other. The SSID to be used for all PCs is adhocP (where P is the group number assigned by the instructor).

The instructor should help students understand the addressing scheme. Using the information in the following chart, configure the host computers. Note that no default gateway is needed. By assigning unique IP addresses and SSIDs, the students avoid conflict with other teams.

Team	Client Name	Profile Name	SSID	Client Address
1	Client1a	adhocNET	Adhoc1	10.0.1.10/24
	Client1b	adhocNET	Adhoc1	10.0.1.11/24
2	Client2a	adhocNET	Adhoc2	10.0.2.10/24
	Client2b	adhocNET	Adhoc2	10.0.2.11/24
3	Client3a	adhocNET	Adhoc3	10.0.3.10/24
	Client3b	adhocNET	Adhoc3	10.0.3.11/24

The following tools and resources will be required to complete this lab:

Two PCs equipped with the Cisco Aironet Client Adapter per group. One of the computers should be a laptop for mobility purposes.

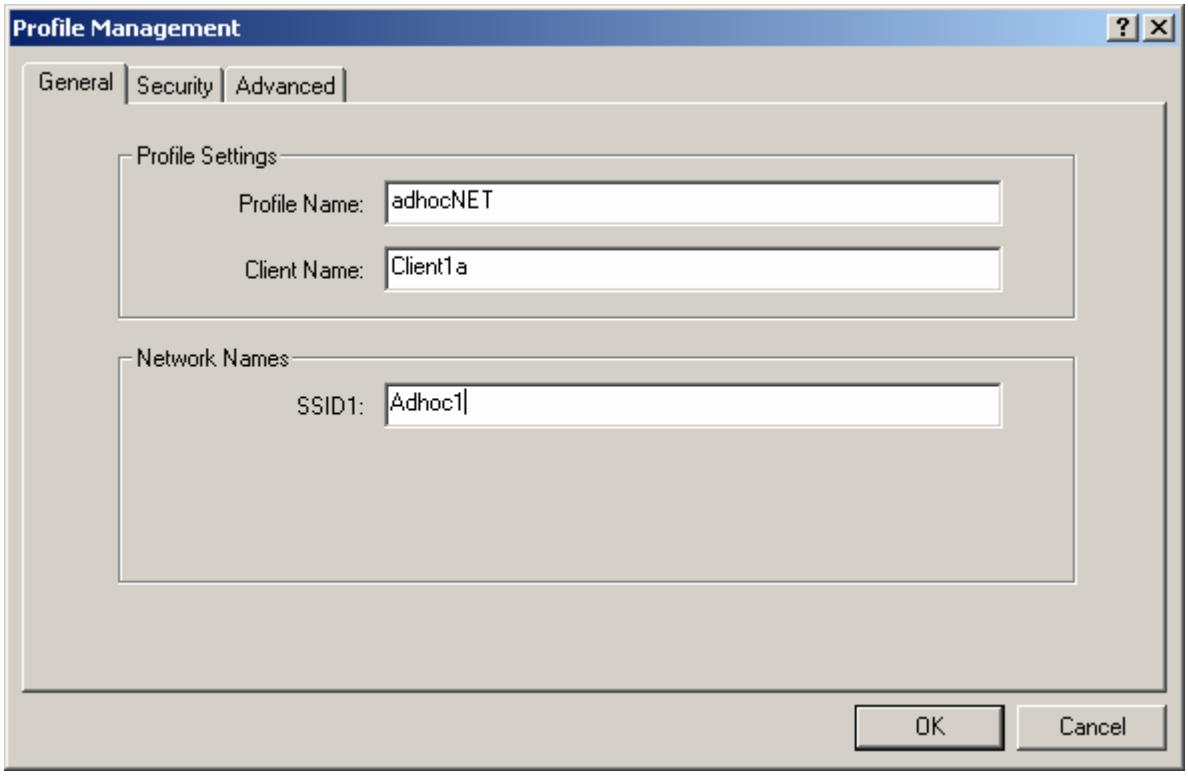
Step 1 Create a profile named adhocP (where P is the team number)

a. Open the Cisco Aironet Desktop Utility.

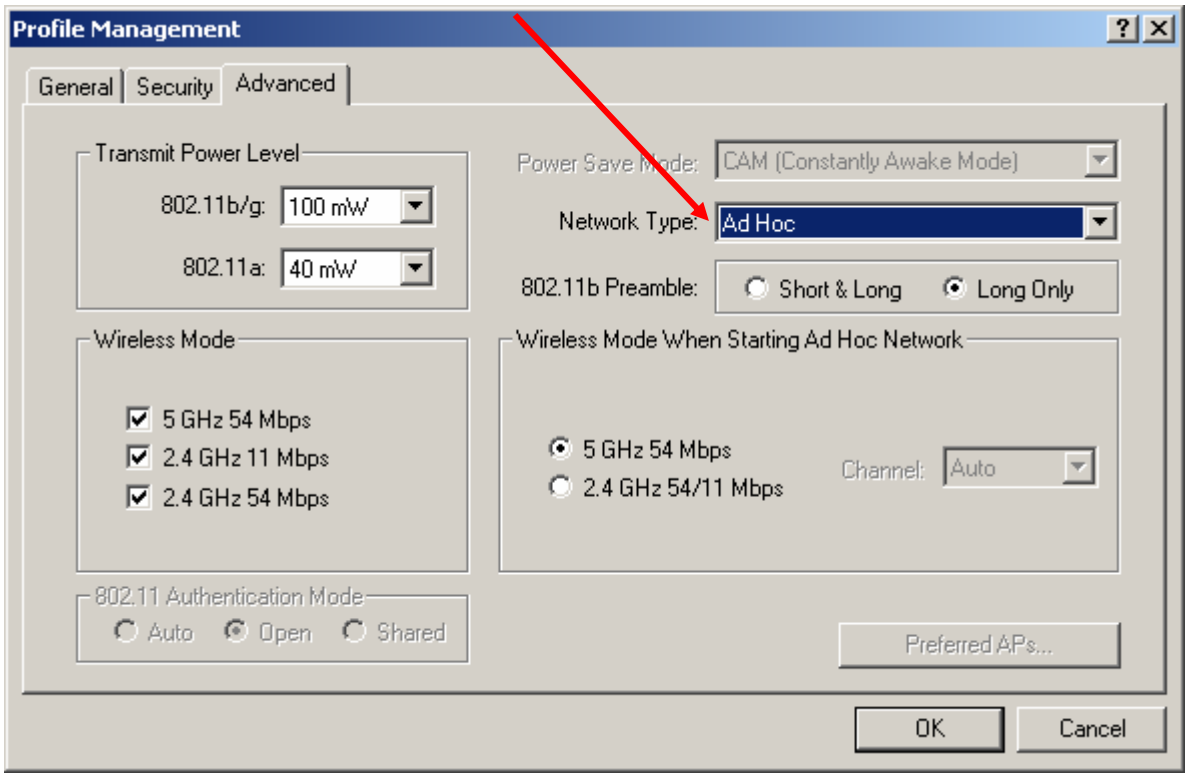
b. Click on the **Profile Management** tab.

c. Click on the **New…** button.

d. Complete the **Profile Name**, **Client Name** and **SSID1** fields with the settings provided in the table.



e. Click the **Advanced** tab to set the Network Type for **Ad Hoc**. The default setting is Infrastructure. Click **OK** to save your settings.

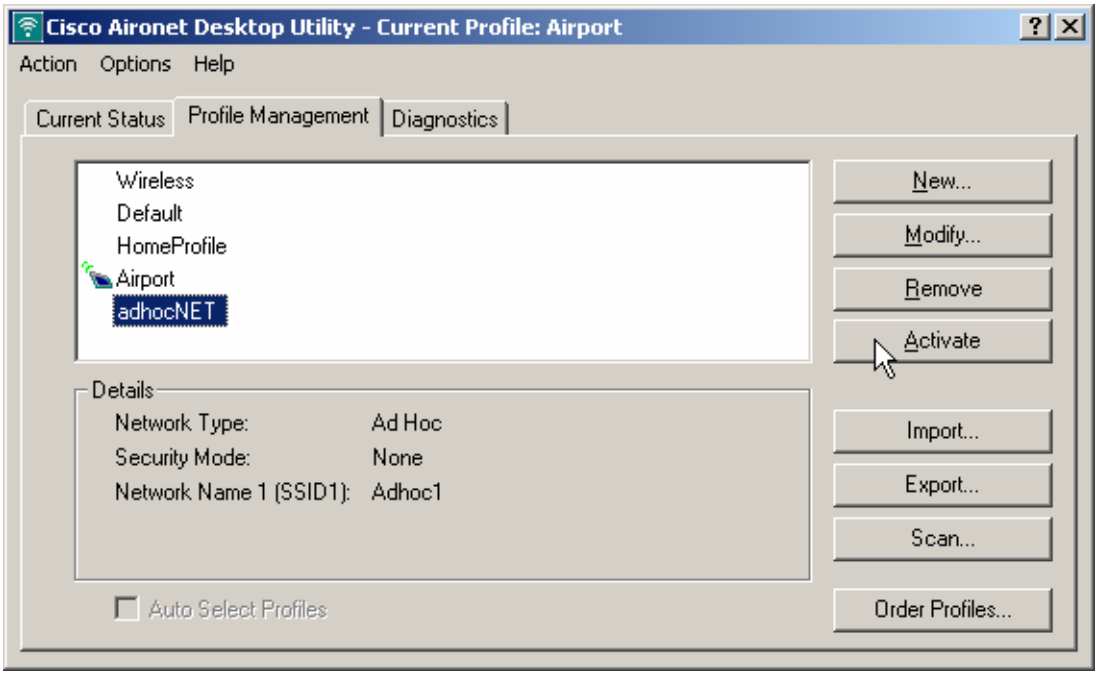


Step 2 Select the profile named adhocP (where P is the team number)

In order to connect to the peer, the ad hoc profile on both computers must be activated.

a. From the **Profile Management** tab, click the adhocNET profile and then click the **Activate** button to use the ad hoc profile.

b. The computers should associate. If association does not occur, troubleshoot as needed.



Step 3 Obtain the MAC address of the PC

Once the computers are associated, you can view information about the peer computer.

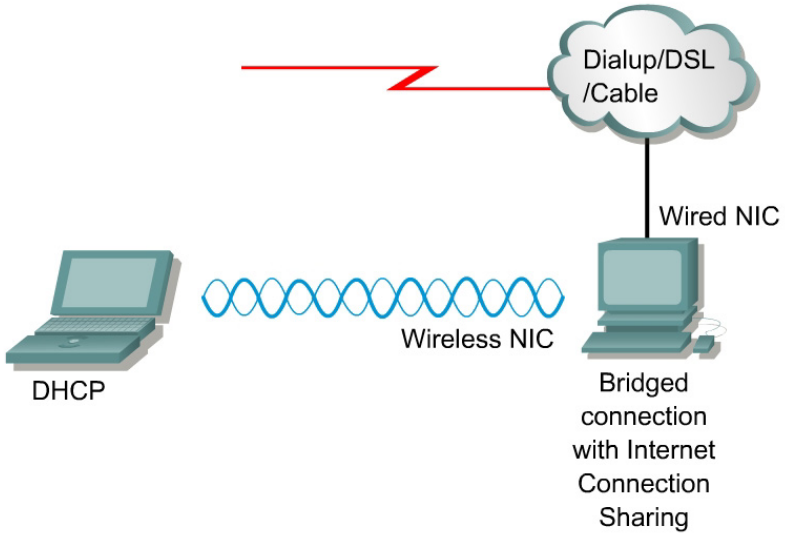
Step 4 File share in Ad Hoc Mode (OPTIONAL LAB)

Scenario 1—Setup a window file share, a web page, or an FTP server program on each PC. Transfer files from one PC to the other. Open a web browser and enter the IP address of the peer team member. If web services are enabled on the peer PC, then a web page should be displayed. Try to transfer a file by FTP between PCs.

Scenario 2—Setup a network game or program that requires network connectivity between PCs. Determine if there are any performance issues. Have other teams change to the adhoc network by matching the SSID and moving into the same IP subnet. Determine if there is a point at which network performance is an issue. Remember that network connectivity is more than ping or telnet traffic. Network application and user demands must always be tested to assure proper network performance after any wireless installation.

Scenario 3—Setup a PC as an mp3 file server and stream music across the wireless adhoc network. Determine if there are any performance issues. Have other teams change to the adhoc network by matching the SSID and moving into the same IP subnet. Determine if there is a point at which network performance is an issue.

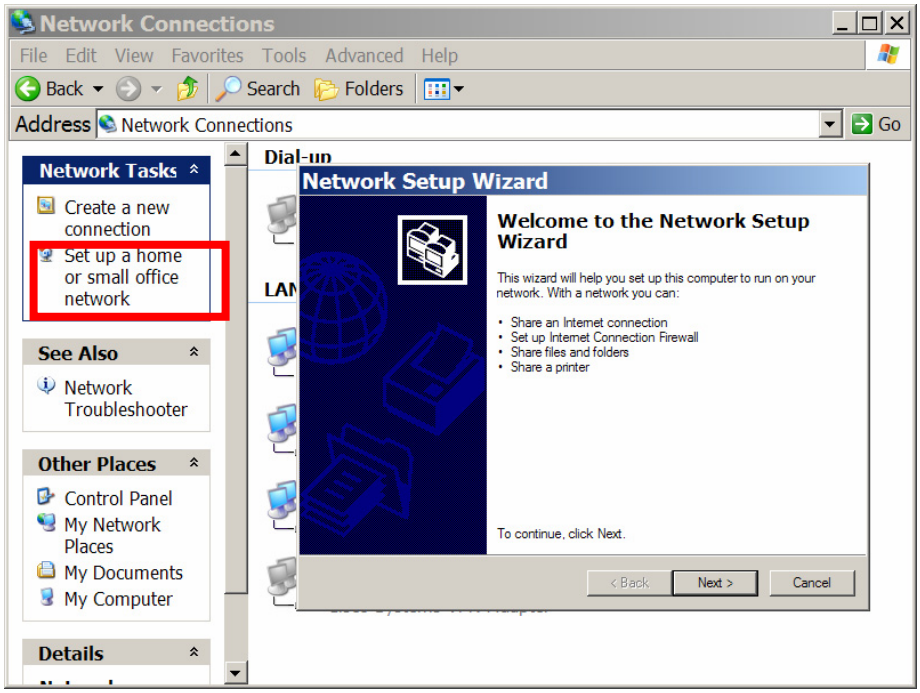
Step 5 Create an AdHoc Network with Windows XP Internet connection sharing (OPTIONAL)



Is it necessary to purchase an AP in order to share the fast broadband connection at home? This lab is very similar to using a cross-connect cable for a small PC network, but without the use of the router or additional cables.

a. Bridge the connection on the Desktop PC

b. Share an Internet connection



c. Configure Wireless NICs on both PCs in Adhoc mode.

Lab 3.2.3 Wireless Mathematics

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two or individually

Objective

In this lab, the student will learn the importance of the output power of the transmitting wireless device. Students will calculate the amount of power actually transmitted from a wireless transmitting device. This will be done through the antenna element, the Effective Isotropic Radiated Power (EIRP) based on the type of antenna, cabling, connectors, and the transmitting device setting being used.

Scenario

Upon completion of this lab, students will calculate potential range of the radiated wave signal transmitted by wireless devices. Students will also convert all radio frequency (RF) signal ratings into a common decibel (dB) unit in order to calculate power gain or loss.

Preparation:

Prior to the lab, students should review the course materials up to 3.2.3.

Tools and Resources:

3.2.3 Interactive Activity: Calculating Decibels
3.2.3 Interactive Activity: Using Decibels

Additional Materials

http://www.zytrax.com/tech/wireless/calc.htm

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml#topic1

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_installation_guide_chapter09186a0080184b5a.html

http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

Students should research the Cisco website for the following information if needed:

- Technical specifications of the power output in decibels (milliwatts) of the wireless devices used. AP and client adapters are examples of these devices.
- Technical specifications of the gain in decibels referenced to an isotropic antenna (dBi) of various wireless device antennas.
- Technical specifications of the gain/loss in decibels (dB) of various wireless device cables
- Technical specifications of the gain/loss in decibels (dB) of various wireless device connectors. These connectors are necessary when cables have to be joined for longer cable lengths.

Maximum Power Levels

ETSI

Band (GHz)	2.4	5.15 – 5.25	5.25 – 5.35	5.470 – 5.725	5.725 – 5.825
EIRP	100 mW 20 dBm	200 mW 22 dBm	200 mW 22 dBm	1000 mW 30 dBm	25 mW 14 dBm

FCC

Band (GHz)	2.4	5.15 – 5.25	5.25 – 5.35	5.470 – 5.725	5.725 – 5.825
Conducted Power EIRP	- 4000 mW 36 dBm	40 mW 200 mW 22 dBm	250 mW 1000 mW 30 dBm	N/A	1000 mW P2MP – 4 W (36 dBm) P2P – 200 W (53 dBm)

Step 1 Calculate the decibel rating

The decibel (dB) measures the power of a signal as a function of its ratio to another standardized value. The symbol is often combined with other symbols to represent what values are being compared. For example: dBm where the decibel value is being compared to 1 milliWatt, and dBw where the decibel value is being compared to 1 Watt. For example:

Power (in dB) = 10 * log10 (Signal/Reference)

Where:

Signal is the power of the signal (for example 50 mW)

Reference is the reference power (for example 1 mW)

In the example:

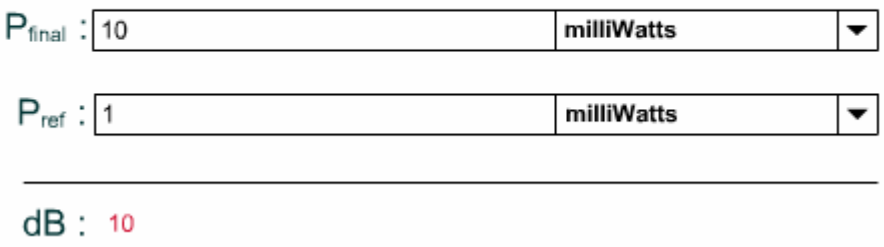
Power (in dB) = 10 * log10 (50/1) = 10 * log10 (50) = 10 * 1,7 = 17 dBm

Since decibels are ratios comparing two power levels, simple math can be used to manipulate them for designing and building networks.

Using the previous example:

Power (in dB) = 10 * log10 (5 * 10) = (10 * log10 (5)) + (10 * log10 (10)) = 7 + 10 = 17 dBm

$$dB = 10 \log_{10} (P_{final} / P_{ref})$$



Complete the missing values below. If help is needed, use the “Calculating Decibels” Interactive Activity.

An increase of:	A decrease of:	Produces:
3dB		Double transmit power
	3dB	Half transmit power
10dB		10 times the transmit power
	10dB	Decreases transmit power 10 times
15dB		32 times the transmit power
	15dB	Decreases transmit power 32 times
20dB		100 times the transmit power
	20dB	Decreases transmit power 100 times
25dB		316 times the transmit power
	25dB	Decreases transmit power 316 times
30dB		1000 times the transmit power
	30dB	Decreases transmit power 1000 times

Additional Practice:

An increase of:	A decrease of:	Produces:
5dB		3 times the transmit power
	5dB	Decreases transmit power 3 times
40dB		10000 times the transmit power
	40dB	Decreases transmit power 10000 times

Step 2 Calculate the delivered power

$$P_{final} = P_{ref} * 10^{(dB/10)}$$

dB : 2.2

P_{ref} : 100 milliWatts

P_{final} : 165.959 milliWatts

Another way to look at this formula is where Pfinal = Pref * 10 (dB/10). In the example above, a 2.4 GHz AP is set to 100mW and has a 2.2 dBi antenna.

Now calculate the following scenarios. Use the “Using Decibels” Interactive Activity

AP Power	Antenna	Power output (in mW)
1 mW	2.2 dBi	1.66
5 mW	6 dBi	20
50 mW	9 dBi	397
100 mW	6 dBi	398
100 mW	22 dBi	15849

1. What is the maximum allowable output power in dBm and Watts for the 2.4 GHz band?

   FCC

   _____

   ETSI

   _____

   _____ (Other Regulatory domain)

   _____

2. What is the maximum allowable output power in dBm and Watts for the 5 GHz band?

   FCC

   _____

   ETSI

   _____

   _____ (Other Regulatory domain)

   _____

3. Why is it necessary for regulatory bodies to define maximum power levels?

   _____

4. What power levels can be set for the 2.4 GHz radio on an AP 1100? 350? 1200?

   _____

5. What power levels can be set for the 2.4 GHz radio on an PCM 350 NICs?

   _____

6. What power levels can be set for the 5 GHz radio on an AP 1200?

   _____

7. What are the approximate dBm values for each of the following power levels?

dBm	mw
___dBm	1mW
___dBm	5mW
___dBm	20mW
___dBm	30mW
___dBm	50mW
___dBm	100mW

Step 3 Calculate the total power output of the wireless device

The radiated (transmitted) power is rated in either dBm or Watts. Power coming off an antenna is measured as Effective Isotropic Radiated Power (EIRP). EIRP is the value that regulatory agencies such as the FCC or European Telecommunications Standards Institute (ETSI) use to determine and measure power limits in applications such as 2.4 GHz wireless equipment. EIRP is calculated by adding the transmitter power (in dBm) to antenna gain (in dBi) and subtracting any cable losses (in dB.)

The dB notation can also be used to describe the power level rating of antennas: dBi for use with isotropic antennas (theoretical antennas that send the same power density in all directions) and dBd when referring to dipole antennas. Antennas are compared to this ideal measurement, and all FCC calculations use this measurement (dBi.) Dipole antennas are more real world antennas. While some antennas are rated in dBd, the majority use dBi. The power rating difference between dBd and dBi is approximately 2.2; that is, 0dBd = 2.2dBi. Therefore, an antenna rated at 3dBd is rated by the FCC (and Cisco) as 5.2dBi.

Example 1:

Description	**Cisco Part Number**	**Power**
AP	AIR-AP1200-A-K9	20 dBm
Antenna gain:	AIR-ANT2012	6 dBi
Antenna Cable loss:	AIR-CAB050LL-R	-3.35 dBi
20dBm + 6dB – 3.35dBi = 34dBm		
		EIRP = 22.65 dBm

Example 2:

Description	**Cisco Part Number**		**Power**
A Cisco Aironet Bridge	AIR-BR350-A-K9		20 dBm
50 foot antenna cable	AIR-CAB050LL-R		3.35 dB loss
solid dish antenna	AIR-ANT3338		21 dBi gain
		EIRP	**37.65 dBm**

a. Which example is permissible according to local regulatory guidelines?

_____

Calculate the EIRP for the following:

AP Output	Antenna Gain	EIRP
20-dBm	12 dBi	
17-dBm	5.2 dBi	
15-dBm	21 dBi	
13-dBm	8.5 dBi	
7-dBm	2.2 dBi	
0 dBm	2.2 dBi	

b. What are the primary hardware factors involved that affect signal distance?

_____

_____

_____

_____

_____

_____

Lab 4.5.3 Topology Design with Cisco Network Designer (CND)

Estimated Time: Sixty minutes

Number of Team Members: Students will work in teams of two or individually.

Objective

Design the following five different network topologies with the Cisco Network Design (CND) software:

- Ad hoc network
- Basic Service Set (BSS) Network
- Extended Service Set (ESS) Network
- Basic home network
- Enterprise network (optional)

Scenario

Network architecture is a roadmap and guide for ongoing network planning, design, and implementation. It provides a logical framework that unifies disparate solutions onto a single foundation.

Once an organization has developed network architecture, they will then have a framework in place for more informed decision-making. This will include appropriate investments in network technologies, products, and services.

Preparation

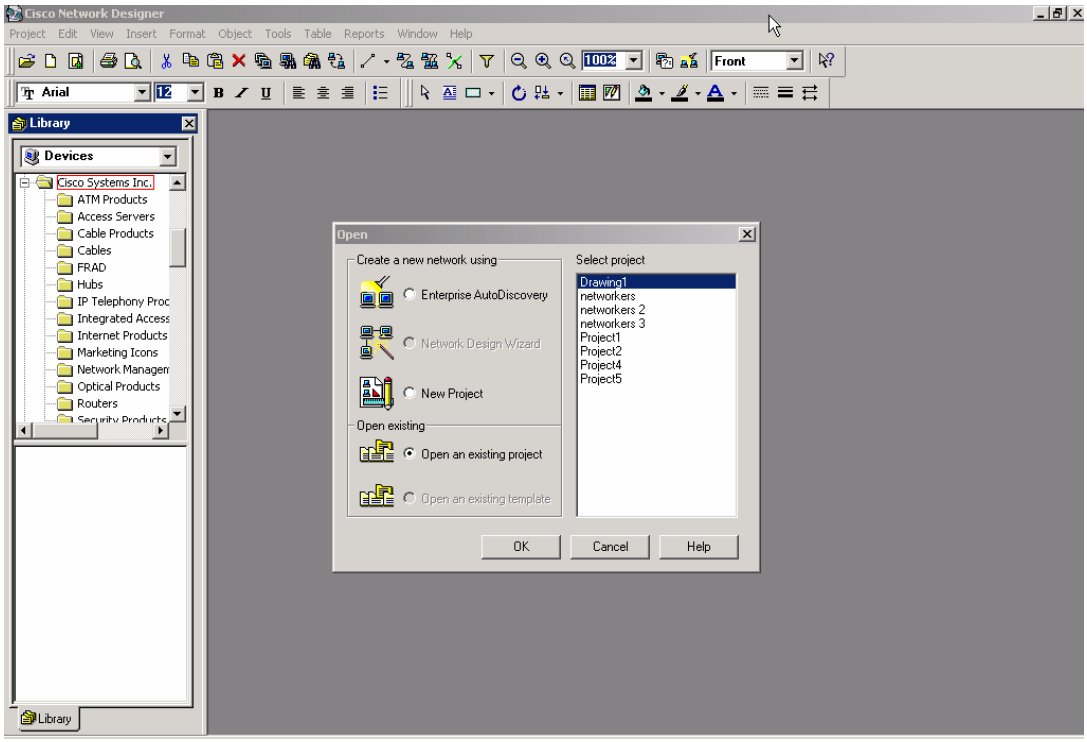
The instructor will provide each student team with a copy of the CND software.

(Optional: This lab can be performed with any other graphical application software or drawing materials the instructor has available.)

The student will review and understand FWL chapter 4 before doing the lab exercise.

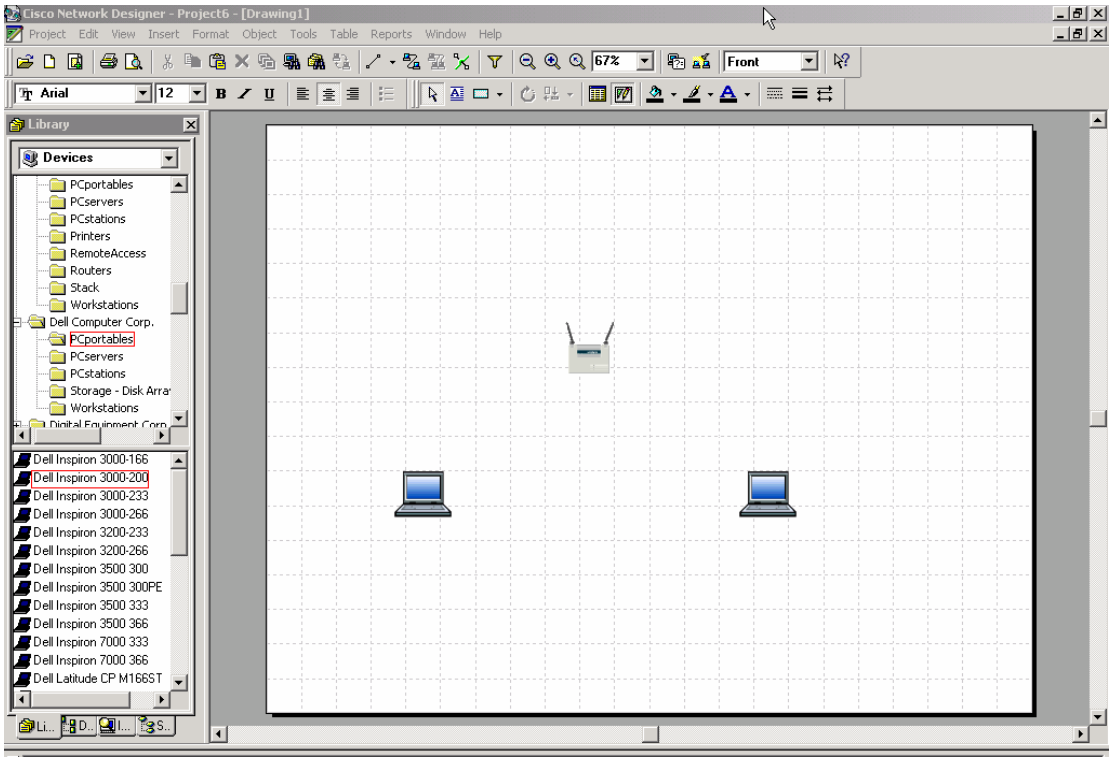
Tools and Resources

- CND Software or Cisco Network Designer Software
- Personal computers for each student or group which are compatible with the CND software.



Step 1 Load the CND or designer software, if it has not been loaded on the PC

Open the Cisco Network Design software. Use the **help** feature to get acquainted with the configuration settings of the software.



Step 2 Design the Ad Hoc topology

Sketch the Ad Hoc design below before creating the design using the software tool. Make sure to show the RF signal from the AP.

Step 3 Design the BSS topology

Sketch the BSS design below before creating the design using the software tool. Make sure to include the following for the BSS topology: one DHCP server, network segments, one wireless AP (show the RF signal), Several wireless clients, two laptops and two desktops.

Step 4 Design the ESS topology

Sketch the ESS design below before creating the design using the software tool. Make sure to include one DHCP server and three wireless APs for the ESS topology. Make sure to indicate the channels of each AP and show the RF signal from the AP.

Step 5 Design a home network topology

Sketch the BSS design below before creating the design using the software tool. Make sure to include the following for the topology:

- One or more PCs
- The network segments
- One wireless AP (show the RF signal)
- Router
- Switch
- One or more laptop(s)
- One handheld (PDA)
- Connection to the Internet through modem (DSL, Cable, Dialup, Wireless ISP)

Step 6 Design an enterprise network topology

Choose a type of enterprise network such as a school, hospital, transportation, manufacturing, etc. Based on the type of business, design a network. Sketch the design below before creating the design using the software tool. Make sure to include the following for the topology: numerous PCs and laptops, workgroups, servers, network segments, numerous wireless access point, router(s), switches, firewalls, IP phones, handheld devices applicable to the business, and so on.

Step 7 Create a PowerPoint show or posters

Assemble all topologies within a PowerPoint show or display posters. Each group or individual can present their topologies to class or create a wall display.

Lab 5.2.2 Configuring Basic AP Settings

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

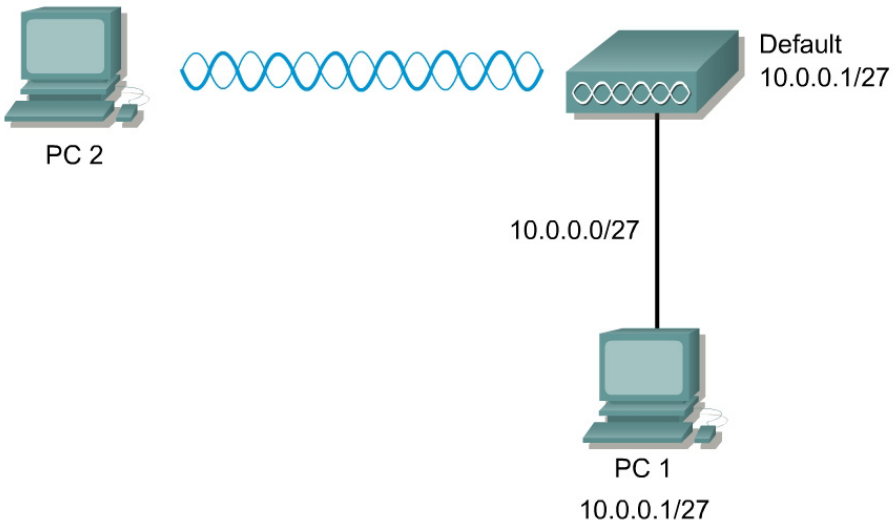
Objective

In this lab, the student will assign basic parameters to the AP using the GUI and IOS CLI. The Express Setup page will also be accessed through a web browser to assign the IP address, subnet mask, default gateway, and SSID to the AP.

Scenario

Basic configuration of an AP can be done through the GUI or IOS CLI.

Topology



Preparation

The student PC should be connected to the AP through an isolated wired network or crossover cable. The AP should be set to factory defaults.

Tools and Resources

Each team will need:

- One AP
- The AP power supply or source
- A PC (PC1) that is connected to the same wired network as the AP
- A wireless PC or laptop (PC2)

Additional Materials

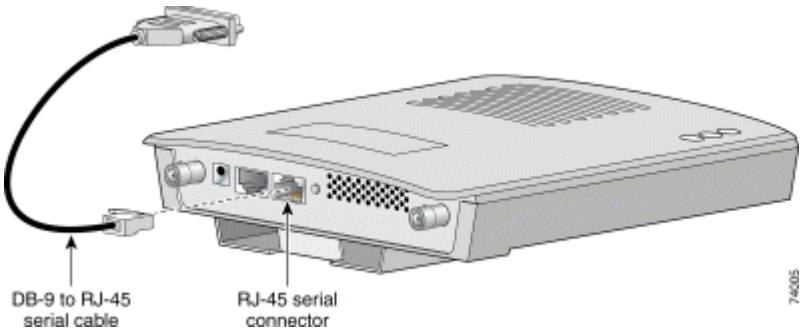
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

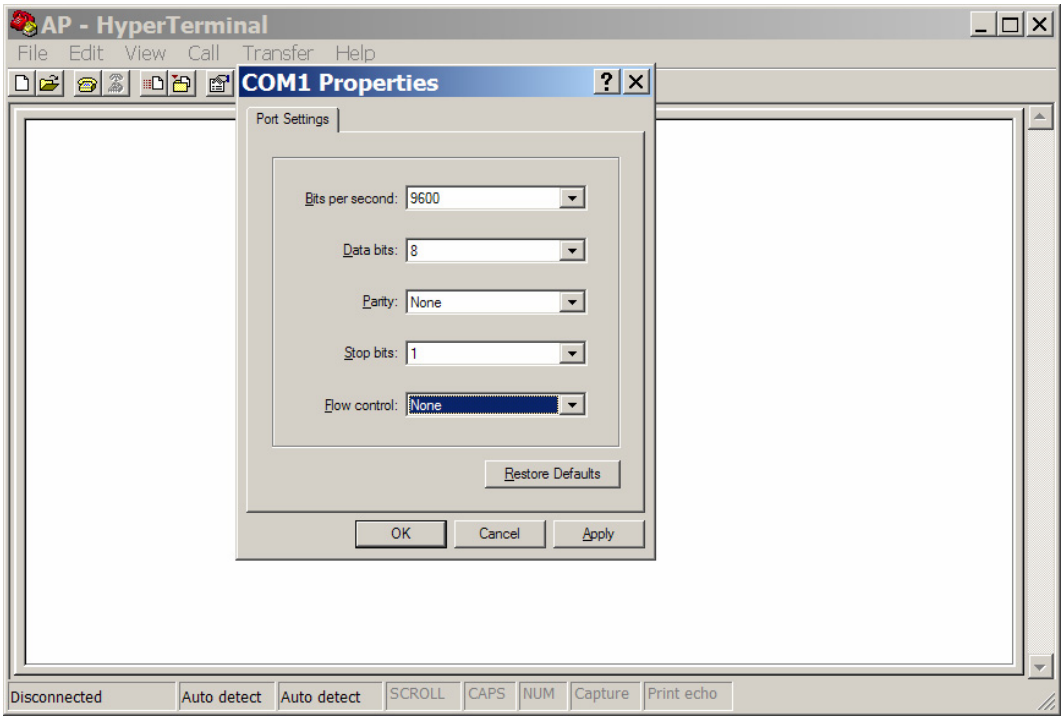
Command	Description
configure terminal	Enter Global configuration mode
hostname	Set the hostname on the device
interface bvi1	Enter the virtual interface for the AP
ip address	Set the IP address and subnet mask on the device
interface dot11radio 0	Enter the device radio interface
station role repeater | root [fallback { shutdown | repeater }]	Set the AP role. Set the role to repeater or root. (Optional) Select the fallback role of the radio. If the Ethernet port of the AP is disabled or disconnected from the wired LAN, the AP can either shut down its radio port or become a repeater AP associated to a nearby root AP.
ssid ssid-string	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note:** Do not include spaces or underscore characters in SSIDs.
enable password *password*	The default password is Cisco. This commands allows an administrator to change the password
enable secret *password*	The default enable password is *Cisco*.
enable password level *level password*	The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
show dot11 associations	View the connected wireless clients
show running-config	Display the current configuration of the device
show startup-config	Display the startup configuration of the device
copy running-config startup-config	Save the entries into the configuration file
show interfaces	Display interface information of the device

Step 1 Connect to the AP using a console



a. Connecting a Cisco rollover cable (console cable) between PC1 and the AP

b. Open a terminal emulator.



c. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

d. Press return to get started

e. Now apply the AP power by plugging in the power supply cable or powered Ethernet cable. Hold the MODE button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button. The AP reboots with the factory default values including the IP address. Without a connected DHCP server, the AP will default to 10.0.0.1/27.

```
flashfs[0]: 141 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 3331584
flashfs[0]: Bytes available: 4409856
flashfs[0]: flashfs fsck took 12 seconds.
Reading cookie from flash parameter block...done.
Base ethernet MAC Address: 00:0b:fd:4a:70:0c
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
ethernet link up, 100 mbps, full-duplex
Ethernet port 0 initialized: link is up
button pressed for 5 seconds
process_config_recovery: set IP address and config to default 10.0.0.1
Loading "flash:/c1200-k9w7-mx.122-11.JA/c1200-k9w7-mx.122-11.JA"...##############
################################
```

Step 2 Configure PC1

Make sure the AP is connected to PC1 by way of a wired connection.

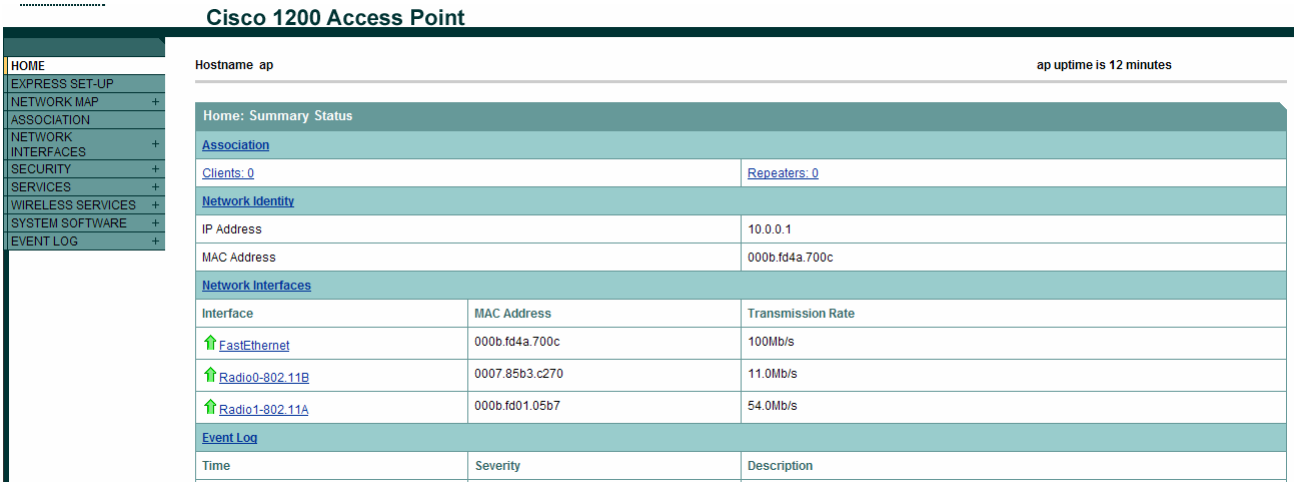
a. Configure the IP address, subnet mask, and gateway on PC1.telent

1. IP address 10.0.0.2
2. Subnet Mask 255.255.255.224
3. Gateway 10.0.0.1

Step 3 Connect to AP using the web browser

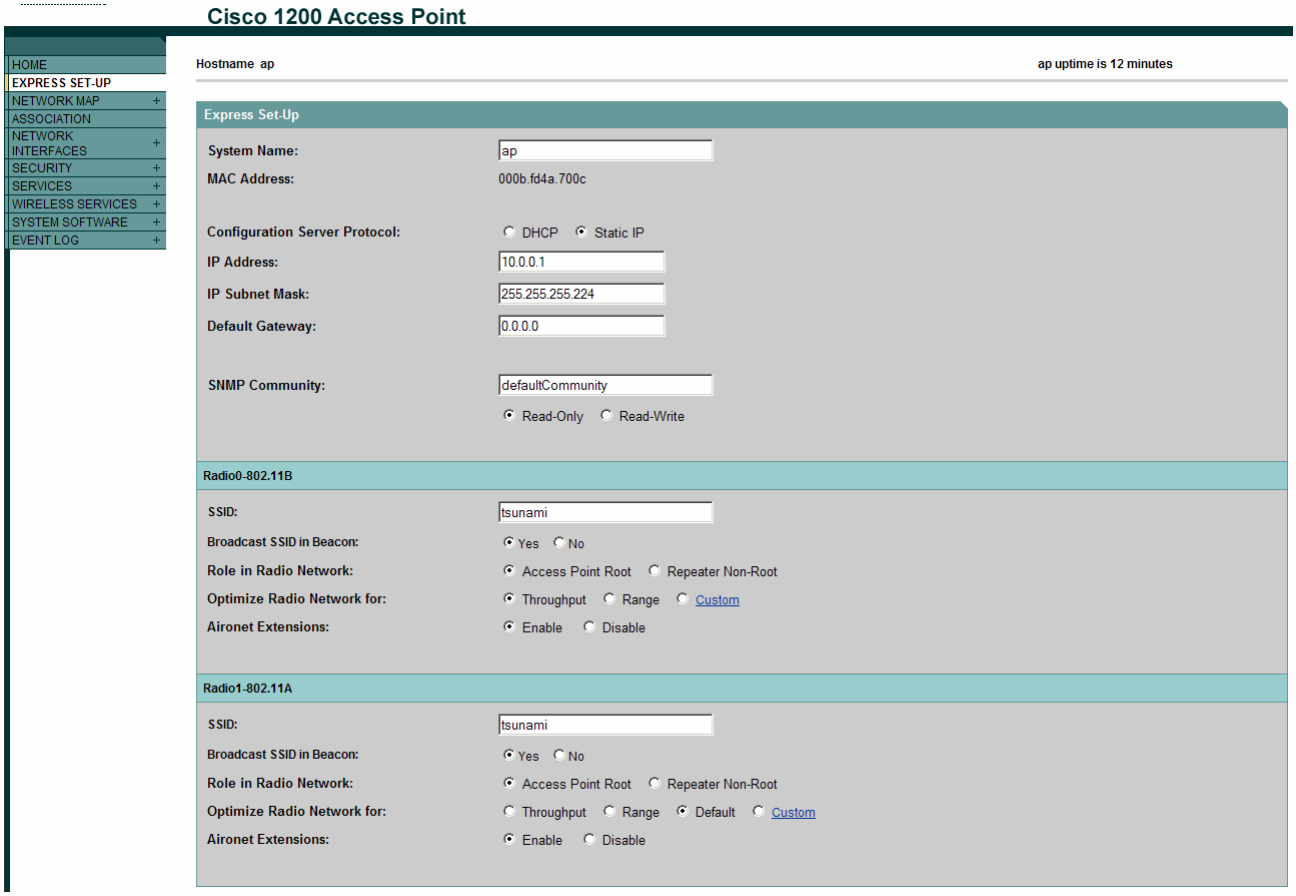
a. Open an Internet browser. The default IP address of an AP from the factory is 10.0.0.1.

b. Type the AP IP address in the browser address location field. Press **Enter**.



c. A log in screen appears. Type in the password of **Cisco** (case sensitive) and click OK.

d. When the AP HOME page appears, click **Express Setup** if the Express Setup does not appear.



e. Type a system name of Pod**P** (where **P** is the Pod or Team number) for the AP in the System Name field.

f. Select **Static IP** as a configuration server protocol from the Configuration Server Protocol selections.

Note If using the BR350 in AP mode, the VxWorks display will be slightly different than the IOS GUI display. These can allow two additional teams to complete the labs. All students should complete the labs with the new 1200 Cisco GUI. If students have available time, then the same labs can be completed using the BR350 in AP mode, remembering the user interface is different. This will allow students to be able to configure legacy Cisco APs such as the AP 340, AP 350, and BR350 in AP mode.

Step 4 Assign the IP address and SSID

Team	AP Name	SSID	AP Address	PC1 Address	PC2 Address
1	Pod1	AP1	10.0.1.1/24	10.0.1.10/24	10.0.1.12/24
2	Pod2	AP2	10.0.2.1/24	10.0.2.10/24	10.0.2.12/24

a. Type the IP address in the **IP Address** field.

What IP address will be assigned to this AP?

_____

b. Enter an IP subnet mask in the **IP Subnet Mask** field.

What Subnet mask will be assigned to this AP? Write the answer in dotted decimal notation.

_____

What Subnet mask in binary.

_____

c. Enter the IP address of the default Internet gateway in the **Default Gateway** field. Assume the router address is 10.0.P.254.

d. Leave the **SNMP Community** field alone at this time.

e. Type an SSID for the AP in the **Radio Service Set ID** (SSID) field.

What SSID will be assigned to this AP?

_____

f. Verify the **AP Root**: as the network role for the AP from the **Role in Radio Network**.

g. Select **Throughput**: as the **Optimize Radio Network**.

h. Click **OK**.

i. The connection will be lost.

j. Reconfigure the IP address, subnet mask and gateway on PC1?

1. IP address 10.0.P.10
2. Subnet Mask 255.255.255.0
3. Gateway 10.0.P.254

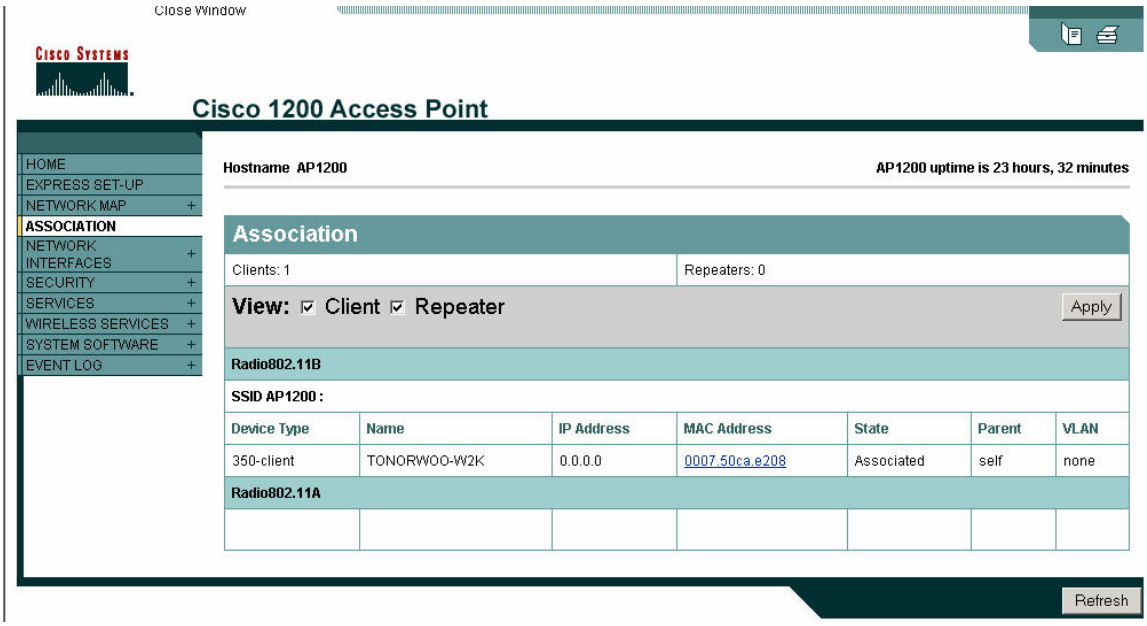
k. Reconnect to the AP from PC1 web browser and verify the settings.

Step 5 Connect to the AP by way of a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct AP. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the AP. Make sure the SSID is configured in the profile to match the AP.
b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members
c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. If a DHCP server is running, configure TCP/IP to receive the address automatically, or configure static IP setting with 10.0.P.12/24.

Step 6 Verify the wireless connection



a. Go to the **ASSOCIATIONS Page** to check the wireless connection.

1. Does the Client Name appear which was previously configured?

2. Record the MAC Addresses of the devices associated to this AP. One of these should be the MAC Address of the laptop or desktop configured in Step 4.

MAC ADDRESS

b. Now check to see if the ACU icon in the system tray is green, which indicates a successful link to the AP. Double click on the icon to verify the correct **AP Name** and **AP IP Address.**

Record the values below.

_____

c. Now check to see if a connection to the AP using a web browser can be achieved from the wireless device. Enter http://10.0.P.1 for the URL within the browser. Did the AP GUI display?

d. Test connectivity to other devices by way of ping, Telnet, http, and ftp. This will vary depending on the devices connected and configured on the wired network.

Step 7 Draw a current topology

a. Using the space below, use the existing Topology and draw an updated Topology with the gateway router and updated IP addresses and subnet masks.

Step 8 Access the AP through IOS CLI

Open the HyperTerminal window on PC1. PC1 should still be connected through the console cable.

Enter privileged mode with the following command. ***Cisco*** is the default password.

```
PodP>enable
Password:
PodP#
```

Step 9 Erase the configuration through CLI

Erase the configuration with the following commands:

```
PodP#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]      (press Enter)
[OK]
Erase of nvram: complete
PodP# reload

System configuration has been modified. Save? [yes/no]:  N
```



```
Proceed with reload? [confirm]   (press Enter)
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:31:09.103: %SYS-5-RELOAD: Reload requested by console.

...
```

Step 10 Configure Hostname

The system name, while not an essential setting, helps identify the AP on your network. The system name appears in the titles of the management system pages.

a. Enter into configuration mode

```
ap>enable
Password:
ap#
ap#configure terminal
ap(config)#
```

b. Now configure the host name with the following command:

```
ap(config)#hostname PodP      (where P is the pod number)
PodP(config)#
```

Step 11 Configure the Bridge Virtual Interface (BVI)

Enter the bvi1 interface mode to configure the ip address, subnet mask settings:

Assign an IP address and address mask to the BVI.

```
PodP(config)#interface bvi1
PodP(config-if)#ip address 10.0.P.1 255.255.255.0
```

Note If you are connected to the AP using a Telnet session, you lose your connection to the AP when you assign a new IP address to the BVI. If you need to continue configuring the AP using Telnet, use the new IP address to open another Telnet session to the AP.

Step 12 Configure passwords

Now configure the enable password to *cisco*. Also, configure the secret password to *class*.The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
PodP(config)#enable password cisco
PodP(config)#enable secret class
```

Use the **level** keyword to define a password for a specific privilege level. After you specify the

level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels.

Now set the **configure** command to privilege level 15 and define *cisco* as the password users must enter to use level 15 commands:

```
PodP(config)#privilege exec level 15 configure
PodP(config)#enable password level 15 cisco
```

Step 13 Configure SSID

Name an SSID and set the maximum number of client devices that can associate using this SSID to 15.

```
PodP(config)#interface dot11radio 0
PodP(config-if)#ssid APP       (where P is the pod number)
PodP(config-if-ssid)#authentication open
PodP(config-if-ssid)#max-associations 15
PodP(config-if-ssid)#end       (or Ctrl-Z)
PodP#
```

Step 14 Check the running configuration and interface status

Display the current configuration of the device

```
PodP#show running-config
```

```
Pod1#show run
Building configuration...

Current configuration : 2660 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PodP
[output omitted]
```

Display the condition and information of the device interfaces.

```
PodP#show interfaces
```

Step 15 Save and verify the configuration is saved to Flash

Save the current configuration of the device into the configuration file.

```
PodP#copy running-config startup-config
```

Verify the startup configuration saved in Flash.

```
PodP#show startup-config
```


Step 16 Connect to the AP using a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct AP. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the AP. Make sure the SSID is configured in the profile to match the AP.
b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members
c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. If a DHCP server is running, configure TCP/IP to receive the address automatically, or configure static IP setting.
d. Now check to see if the ACU icon in the system tray is green, which indicates a successful link to the AP. Double click on the ACU icon to verify the correct **AP Name** and **AP IP Address.**

Record the values below?

_____

Step 17 Verify the Associations

View the current device associations. The wireless device configured in step 11 should appear in the association output.

```
PodP#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [tsunami] :
Others:  (not related to any ssid)
802.11 Client Stations on Dot11Radio1:
SSID [tsunami] :
Others:  (not related to any ssid)
PodP#
```

Step 18 Connect to the AP remotely through Telnet

Follow these steps to open the IOS CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

a. From PC2, Open a Telnet session to the AP located at 10.0.P.1

b. If Telnet is not listed in your Accessories menu, select Start > Run, type Telnet in the entry field, and press Enter.

c. At the username and password prompts, enter your administrator username and password. The default username is Cisco, and the default password is Cisco. The default enable password is also Cisco. The enable secret password is class. Usernames and passwords are case-sensitive.

```
C:\>telnet 10.0.P.1
User Access Verification
Username:
Password:
PodP>
```


Lab 5.2.4 Using features of the Internetworking Operating System (IOS) command line interface (CLI)

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

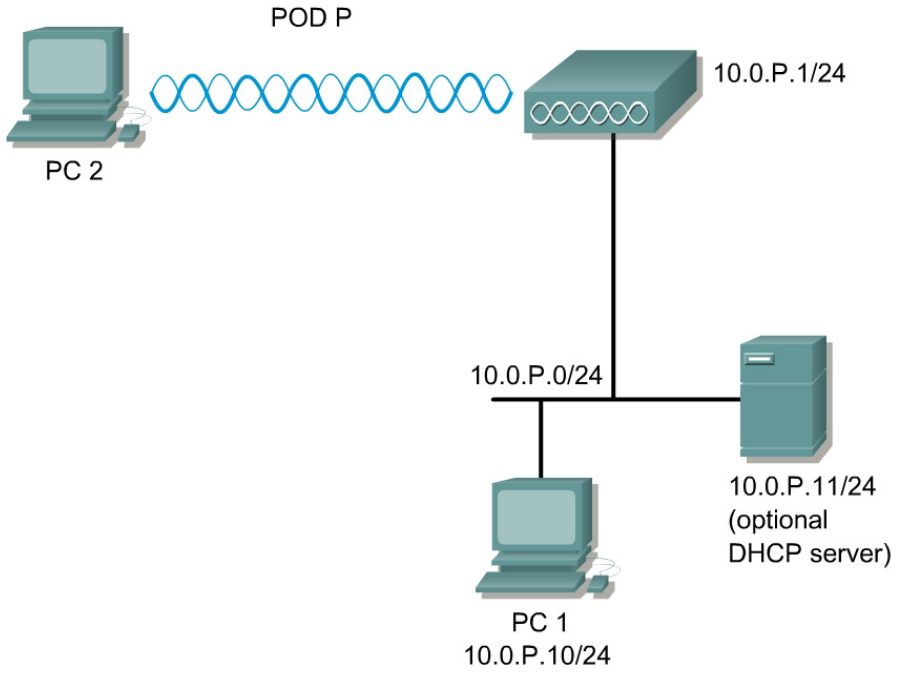
In this lab, the student will learn the following objectives:

- Command Line Interface help features
- Abbreviated commands
- Using the no command to remove config statements
- Command History
- Editing features

Scenario

Students will learn the features of the AP Internetworking operating system (IOS).

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Tools and Resources

Each team will need:

- The AP
- A PC or laptop
- Console cable

Additional Materials:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
help	Obtains a brief description of the help system in any command mode.
?	Lists all commands available for a particular command mode.
command?	Lists the associated keywords for a command.
command keyword ?	Lists the associated arguments for a keyword.
abbreviated-command-entry?	Obtains a list of commands that begin with a particular character string.
no	Use the no form to disable a feature or function or reverse the action of a command
history	The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.
terminal history	The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.
show history	While in privileged EXEC mode, list the last several commands that you just entered.

Press Ctrl-P or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press Ctrl-N or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Step 1 Connect to the AP through the console

a. Connecting a Cisco rollover cable (console cable) between PC1 and the AP

b. Open a terminal emulator.

1. What settings are required?

Bits per second (baud rate):
Data bits:
Parity:
Stop bits:
Flow control:

c. Press return to get started

```
ap>
```

Step 2 Enter into privileged mode

Enter privileged mode. Cisco is the default password. If the password has been changed, reset the AP to factory defaults. If help is needed refer to the previous lab or Cisco online documentation.

```
ap>enable
Password:
ap#
```

Step 3 Erase the existing configuration

If there is an existing configuration on the AP, erase the configuration and reload.

```
ap#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm] Y [OK]
Erase of nvram: complete
ap#
*Mar  1 00:42:37.099: %SYS-7-NV_BLOCK_INIT: Initialized the geometry
of nvram
ap#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]y
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:45:08.446: %SYS-5-RELOAD: Reload requested by console.
```

1. What command is used to check the existing running configuration?

   _____

2. What command is used to check the existing startup configuration?

   _____

Step 4 Configure the AP

a. Enter global configuration mode. Configure the hostname, SSID, and passwords. Use the previous lab for configuration help if needed

```
ap#configure terminal
ap(config)#
ap(config)#hostname PodP
PodP(config)#
…
```

b. Configure the remaining steps

c. Configure a wireless PC or laptop to connect the AP.

d. From PC2 Telnet to the AP to complete the remaining lab.

Step 5 Using the `help` feature of the AP

The AP IOS includes help features. Typing the word help at the command prompt will give you a brief summary of the help usage features. Display the help usage summary by typing the command help at the prompt:

```
PodP#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

PodP#
```

Step 6 Display the available commands of the command mode

To display a list of available commands of the command mode, type the ? character at the command line prompt:

```
PodP#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
```



```
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  dot11            IEEE 802.11 commands
  enable           Turn on privileged commands
  erase            Erase a filesystem
[output omitted]
```

To get help on a specific command, type the command name followed by the ? at the command prompt.

Type **configure ?** at the command prompt to display the available options for the configure command:

```
PodP#configure ?
  memory             Configure from NV memory
  network            Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal           Configure from the terminal
  <cr>

PodP#configure
```

Step 7 Abbreviated commands

The IOS supports the use of abbreviated commands. Type in a partial command at the command prompt and then press the tab button. Pressing the tab button will complete the partial command. Type in show conf rather than show configuration. Press the tab button and it will complete the partial command:

```
PodP#show conf   (press the tab button)
PodP#show configuration
Using 2660 out of 32768 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP1200
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
[output omitted]
```


The Navigation keystrokes below help display the output as needed:

Key	Action
Return	Scroll down one line.
Space	Scroll down one screen.
any other key	Exit the output

Step 8 Command history

The IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

Changing the Command History Buffer Size

By default, the AP records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to set the number of command lines that the AP records during the current terminal session:

```
PodP# terminal history 10
```

(The range is from 0 to 256)

Beginning in line configuration mode, enter this command to configure the number of command lines the AP records for all sessions on a particular line, the example below configures the number of lines to 10:

```
PodP(config)#line console 0
PodP(config-line)# history 10
```

(The range is from 0 to 256)

Step 9 Using `no` Forms of Commands to remove configuration statements

Most configuration commands also have a **`no`** form. In general, use the **`no`** form to disable a feature or function or reverse the action of a command. For example, the **`no shutdown`** interface configuration command reverses the **`shutdown`** of an interface. Use the command without the keyword **`no`** to re-enable a disabled feature or to enable a feature that is disabled by default.

You will perform a **`no`** command in Step 10 below.

Step 10 Enabling and disabling editing features

This section describes the editing features that can help you manipulate the command line. Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
PodP#terminal editing
PodP#
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
PodP(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
PodP(config-line)# no editing
```


Step 11 Editing commands through keystrokes

Use the keystrokes listed below to practice editing command lines. Perform each keystroke starting at the top of the list.

Keystroke1	Purpose
Ctrl-B or the left arrow key	Move the cursor back one character.
Ctrl-F or the right arrow key	Move the cursor forward one character.
Ctrl-A	Move the cursor to the beginning of the command line.
Ctrl-E	Move the cursor to the end of the command line.
Esc B	Move the cursor back one word.
Esc F	Move the cursor forward one word.
Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Delete or Backspace	Erase the character to the left of the cursor.
Ctrl-P (or up arrow)	View the previous command in the command history buffer
Ctrl-N (or down arrow)	View the next command in the command history buffer

Lab 5.2.5 Manage AP Configuration and Image Files

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

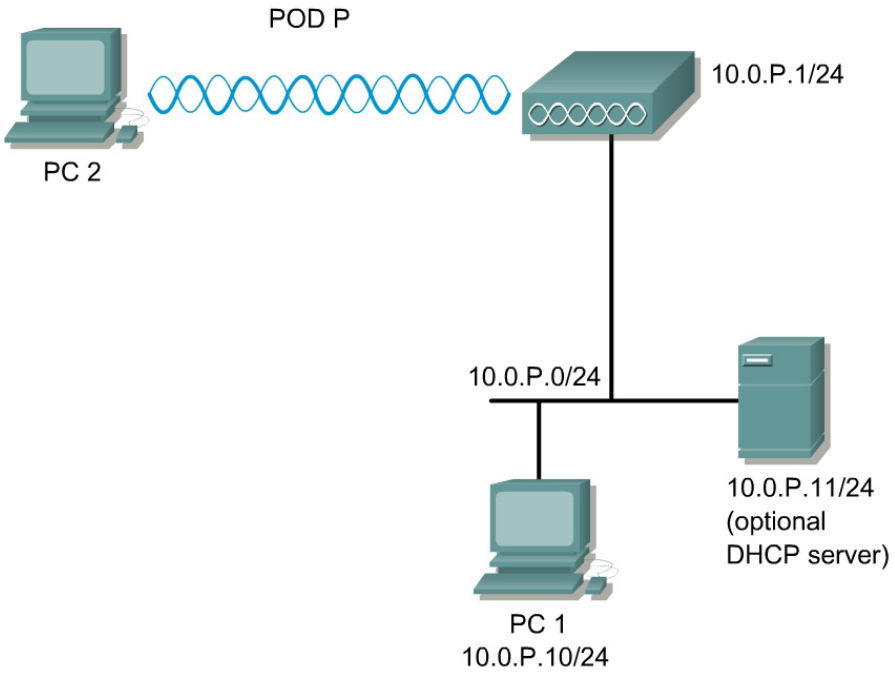
In this lab, the student will learn to manage configuration and image files.

Scenario

Students will learn the file management features of the AP IOS and GUI.

Note The command outputs shown in this lab were produced in IOS version 11.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Download and install TFTP server software on PC1.

Tools and Resources

Each team will need:

- The AP
- A PC or laptop
- Console cable

Additional Materials:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

SolarWinds TFTP

http://www.solarwinds.net/Download-Tools.htm

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
show file systems	Display the available file systems on the AP
dir	View directory information
ping	Ping a IP address to test connectivity
copy	Move files between the AP and a backup server.

Step 1 Erase the existing configuration

a. Enter privileged mode. Cisco is the default password.

```
ap>enable
Password:
ap#
```

b. If there is an existing configuration on the AP, erase the configuration and reload.

```
ap#erase startup-config
ap#reload
```

1. What command is used to check the existing running configuration?

   _____

2. What command is used to check the existing startup configuration?

   _____

c. Configure the AP according to the Preparation table. Also make sure the equipment is cabled and configured as shown in the Topology.

Step 2 Display the AP file system

a. Display the available file systems on the AP.

```
PodP#show file systems
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
*    7741440     4412416     flash     rw   flash:
           -           -    opaque     rw   bs:
     7741440     4412416   unknown     rw   zflash:
       32768       32716     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
```

b. What do the Flags value represent?

   _____

Step 3 Display information on the file system

Display information about files on a file system

a. View the available options for the dir command.

```
PodP#dir ?
  /all             List all files
  /recursive       List files recursively
  all-filesystems  List files on all filesystems
  bs:              Directory or file name
  flash:           Directory or file name
  null:            Directory or file name
  nvram:           Directory or file name
  system:          Directory or file name
  xmodem:          Directory or file name
  ymodem:          Directory or file name
  <cr>
File Systems:
```


b. List all files for the current directory.

```
PodP#dir /all
Directory of flash:/

    2  -rwx         167   Mar 01 1993 00:12:51  env_vars
    4  -rwx           5   Mar 01 1993 00:08:45  private-config
    6  drwx         320   Jan 01 1970 00:07:15  c1200-k9w7-mx.122-
11.JA

7741440 bytes total (4412416 bytes free)
```

c. View the NVRAM files.

```
PodP#dir nvram:
Directory of nvram:/

   30  -rw-           0              <no date>  startup-config
   31  ----           0              <no date>  private-config

32768 bytes total (32716 bytes free)
```

d. View the System files.

```
PodP#dir system:
Directory of system:/

    2  dr-x           0              <no date>  memory
    1  -rw-        1748              <no date>  running-config

No space information available
```

e. View all files in all directories.

```
PodP#dir all- filesystems:
```

Step 4 Backup configurations using TFTP

Backup configurations can save an administrator much time when restoring, deploying, or modifying configurations.

a. First, view the available copy commands.

```
PodP#copy ?
  /erase          Erase destination file system.
  bs:             Copy from bs: file system
  flash:          Copy from flash: file system
  ftp:            Copy from ftp: file system
  null:           Copy from null: file system
  nvram:          Copy from nvram: file system
  rcp:            Copy from rcp: file system
  running-config  Copy from current system configuration
  scp:            Copy from scp: file system
  startup-config  Copy from startup configuration
```



```
system:         Copy from system: file system
tftp:           Copy from tftp: file system
xmodem:         Copy from xmodem: file system
ymodem:         Copy from ymodem: file system
zflash:         Copy from zflash: file system
```

b. Ping the TFTP server to check connectivity. Make sure the TFTP server is enabled and configured properly.

```
PodP#ping 10.0.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

c. Save the current configuration to flash.

```
PodP#copy run start
```

d. Upload a configuration file from the AP running configuration to a TFTP server.

```
PodP#copy running-config tftp://10.0.P.10
```

or

```
PodP#copy run tftp
Address or name of remote host []? 10.0.P.10
Destination filename [PodP-confg]?
```

e. On PC1, verify the file is saved. Open the file with a text editor such as WordPad to verify the configuration.

f. Upload a configuration file from an AP startup configuration to a TFTP server for storage.

```
PodP#copy startup-config tftp://10.0.P.10
```

or

```
PodP#copy start tftp
Address or name of remote host []? 10.0.P.10
Destination filename [Podp-confg]?
```

g. Modify the saved AP configuration on PC1. Change the hostname to PodPrestore

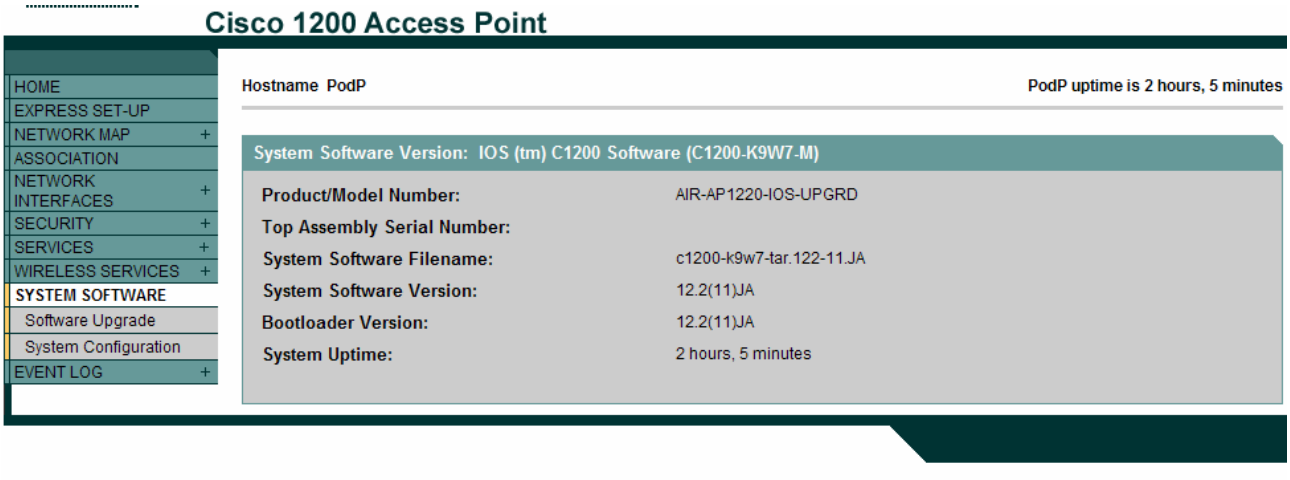
h. Upload a configuration file TFTP server to the AP startup-config.

```
PodP#copy tftp start
Address or name of remote host []? 10.0.P.10
Destination filename [Podp-confg]?
```

i. Verify the uploaded configuration file in NVRAM.

```
PodP#show start
```


Step 5 Manage system image files



Maintaining a record of the AP System Software Version is important for security and operation.

a. Open a browser on PC1. Enter the IP address of the AP in the URL locator. Press Enter.

b. Login to the AP.

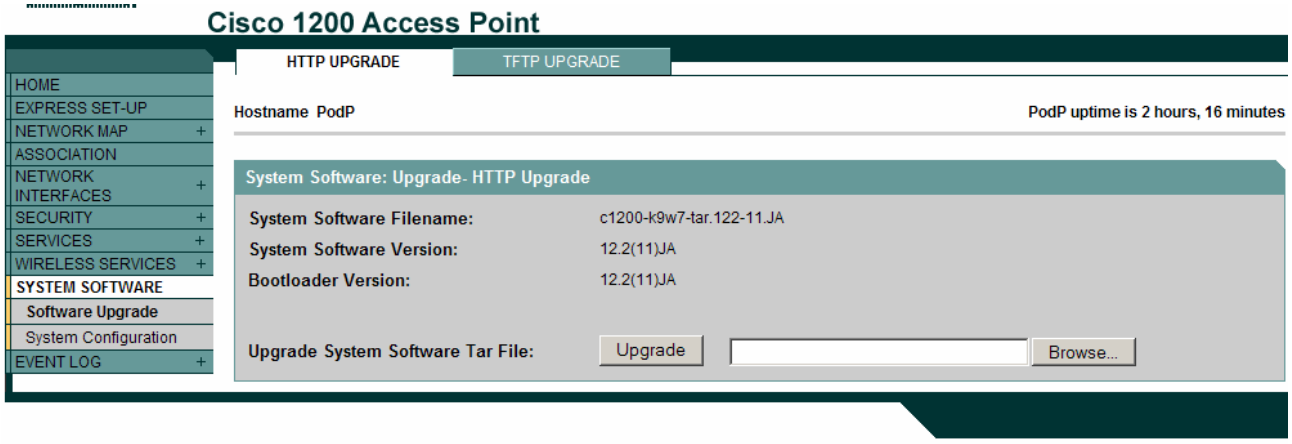
c. From the Home page, go to the **SYSTEM SOFTWARE** Page.

d. What is the Product/Model Number?

_____

e. What is the System Software Filename?

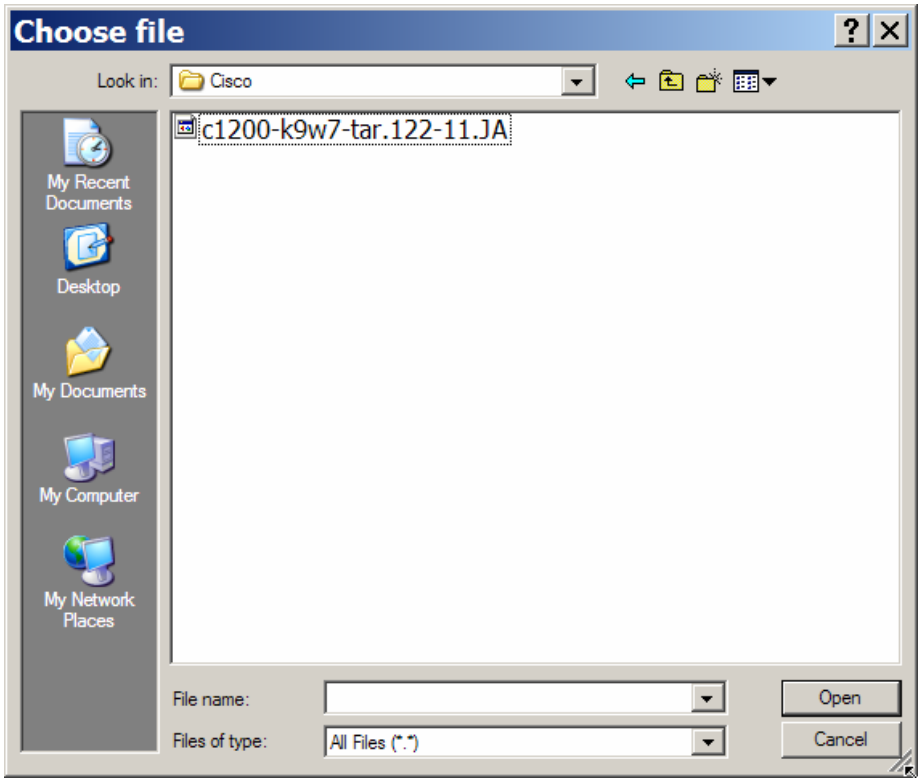
_____



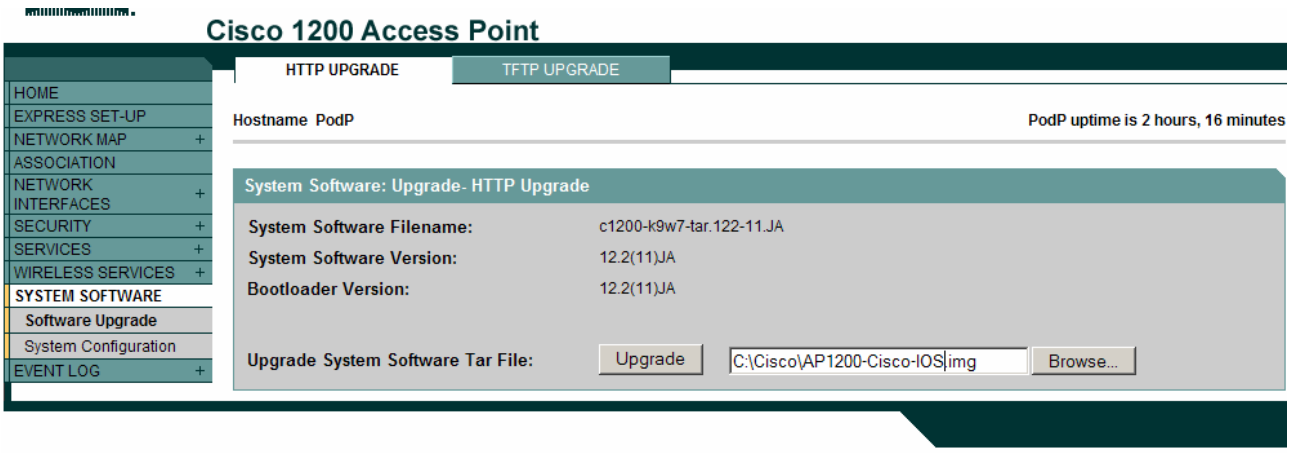
The **SYSTEM SOFTWARE>Software Upgrade** Page provides the easiest method to upgrade a system image.

f. Click on the browse button to locate the desired Tar file located on PC1.

Note The AP image files are available at the following address: http://www.cisco.com/public/sw-center/sw-wireless3.shtml



g. Select the image file and click **Open**.



h. The image will now appear in the File: box.

Note	Before proceeding with Upgrade, get the instructors approval

i. Click the Upgrade button.

j. It is best to maintain a console connection to monitor the upgrade progress.

Note	NEVER reboot once the upgrade process begins! It is a good practice to connect the AP to a UPS.

Step 6 Backup configurations using FTP (Optional challenge)

Download, install and configure a FTP server on PC1. Configure a user of ***netadmin1*** with a password of ***mypass***.

a. From a console or telnet connection to the AP, copy the running-config to a FTP server without configuring the username and password.

```
PodP# copy run ftp://netadmin1:mypass@10.0.P.10/ap1-confg
Write file ap1-confg on host 10.0.P.10?[confirm]
Building configuration...[OK]
Connected to 10.0.P.10
PodP#
```

b. Now, copy the startup-config to a FTP server.

```
PodP(config)#ip ftp username netadmin1
PodP(config)#ip ftp password mypass
PodP(config)#end
PodP#copy start ftp
Remote host[]? 10.0.P.10
Name of configuration file to write [ap1-confg]?
Write file ap1-confg on host 10.0.P.10?[confirm]
![OK]
```

c. Finally, copy a backup configuration to the startup-config.

```
PodP#configure terminal
PodP(config)# ip ftp username netadmin1
PodP(config)# ip ftp password mypass
PodP(config)# end
PodP# copy ftp start
Address of remote host []? 10.0.P.10
Name of configuration file[rtr1-confg]? host1-confg
Configure using host1-confg from 10.0.P.10?[confirm]
Connected to 10.0.P.10
Loading 1112 byte file host1-confg:![OK]
[OK]
```


Lab 5.3.5 Configure Ethernet/FastEthernet Interface

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two.

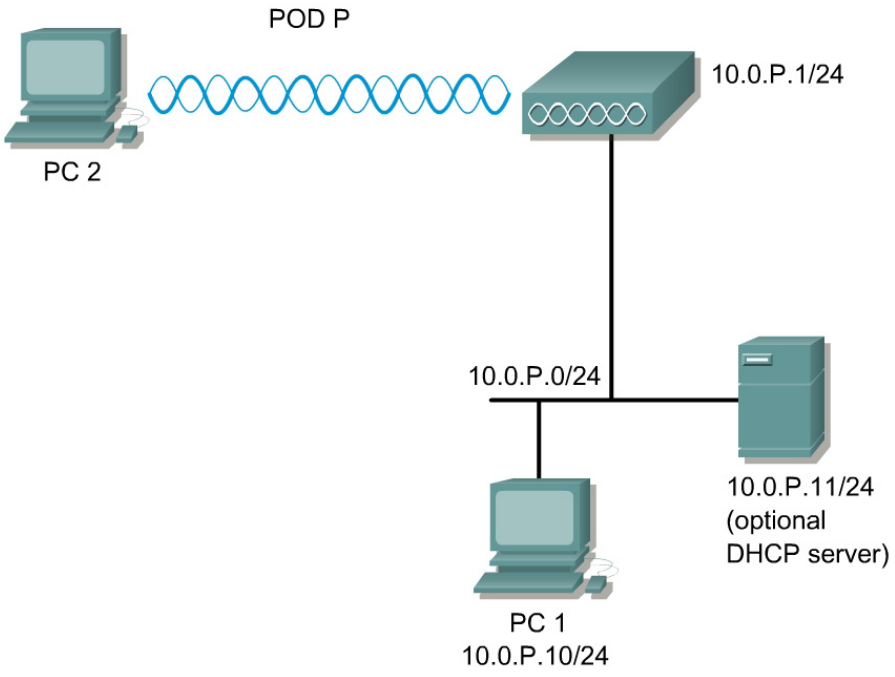
Objective

In this lab, the student will use the AP setting pages to enter speed and duplex information for the AP.

Scenario

This section describes how to configure the AP radio Ethernet and FastEthernet interfaces to lock in speed and duplex settings.

Topology



Preparation

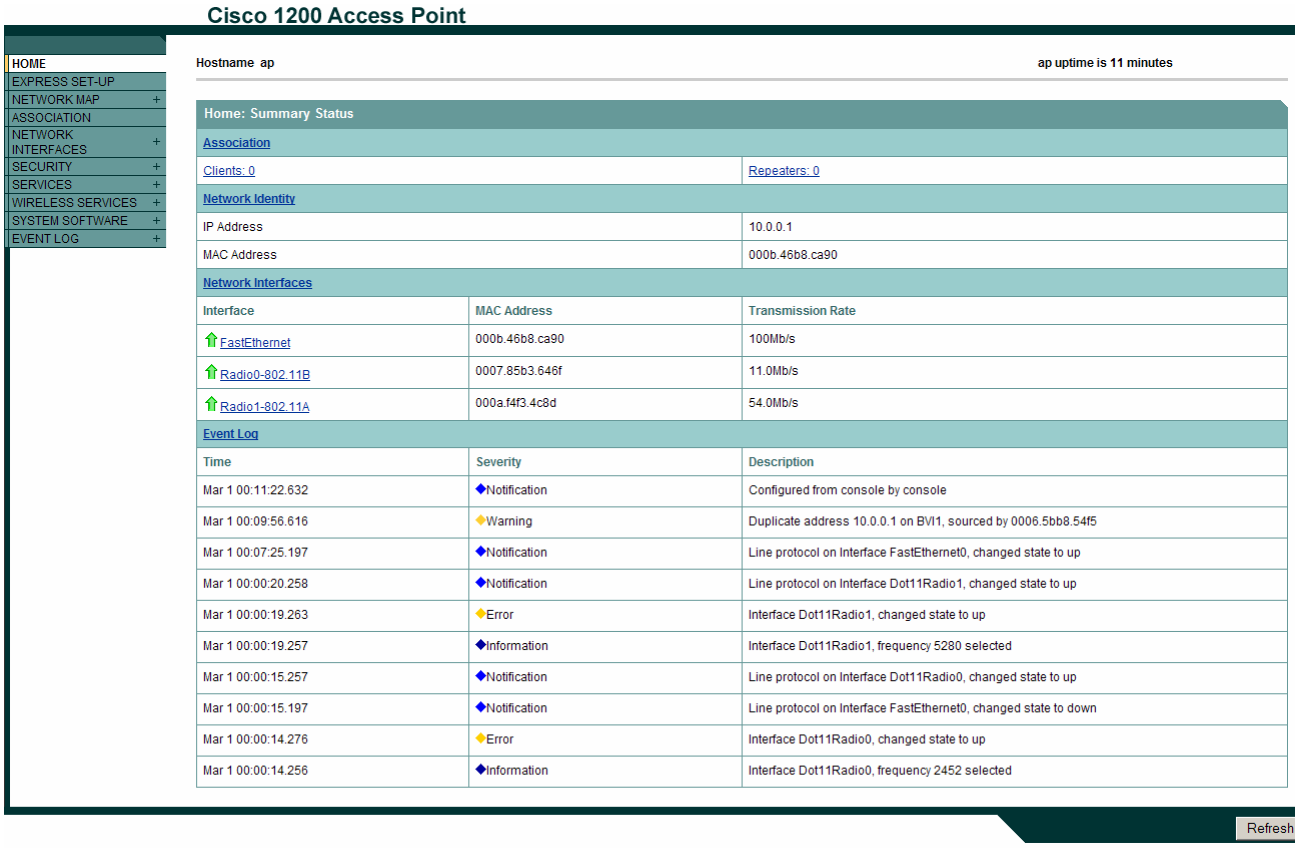
Below are the basic settings to be applied to the AP.

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Tools and Resources

- One Cisco 1200 AP
- PCs with properly installed Cisco wireless client adapters and utility.
- Several PCs on the wired network that can maintain connectivity to the configuration management pages on the AP.

Step 1 Obtaining and Assigning an IP Address



a. If needed, console into the AP and configure the BVI IP address to 10.0.P.1/24. Set the hostname as well according to the Preparation table. Make sure the wired PC TCP/IP settings are configured according to the Topology. A wireless connection to the AP can also be used.

1. Record the configuration commands below needed for Step1a.

_____

_____

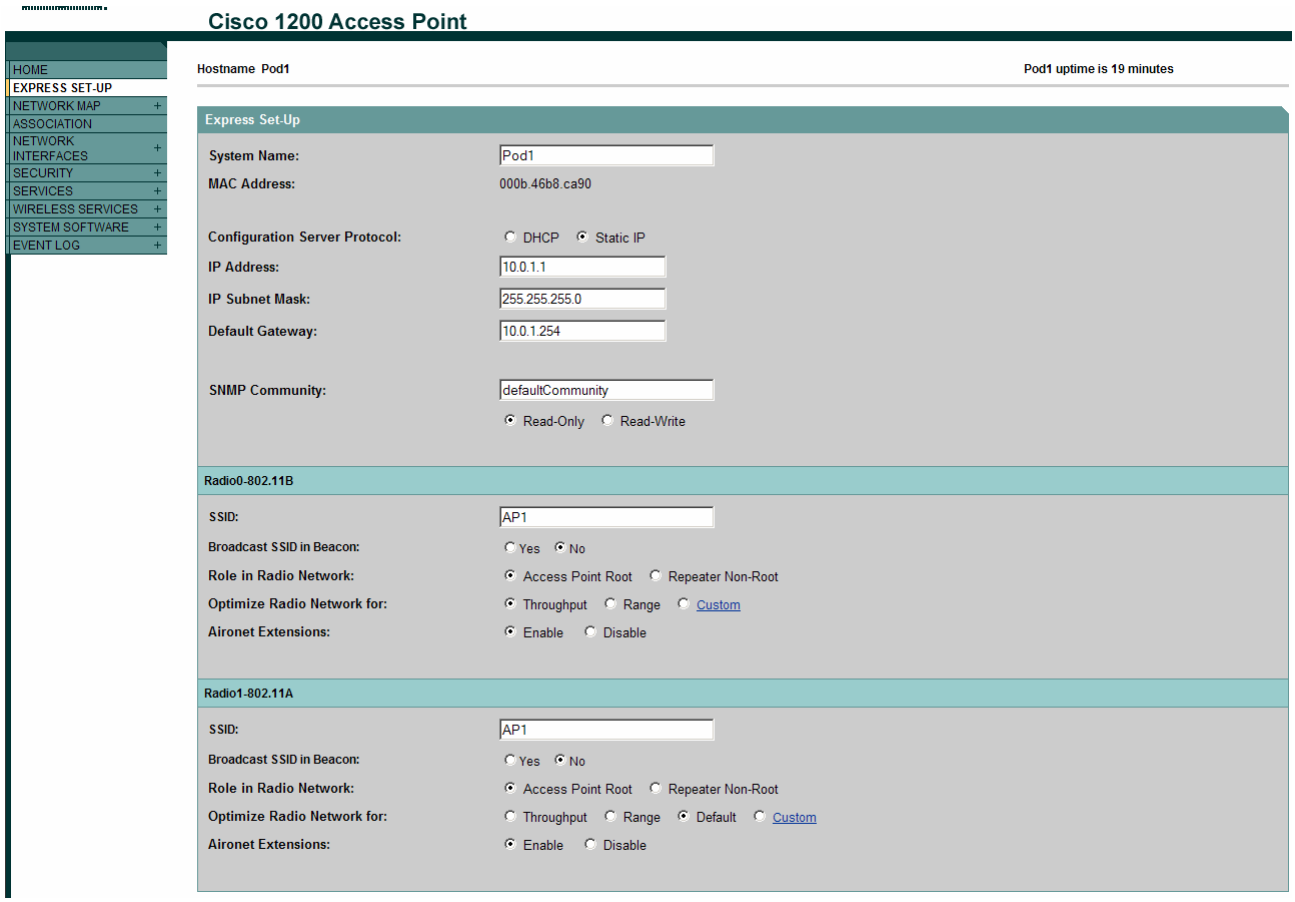
_____

_____

_____

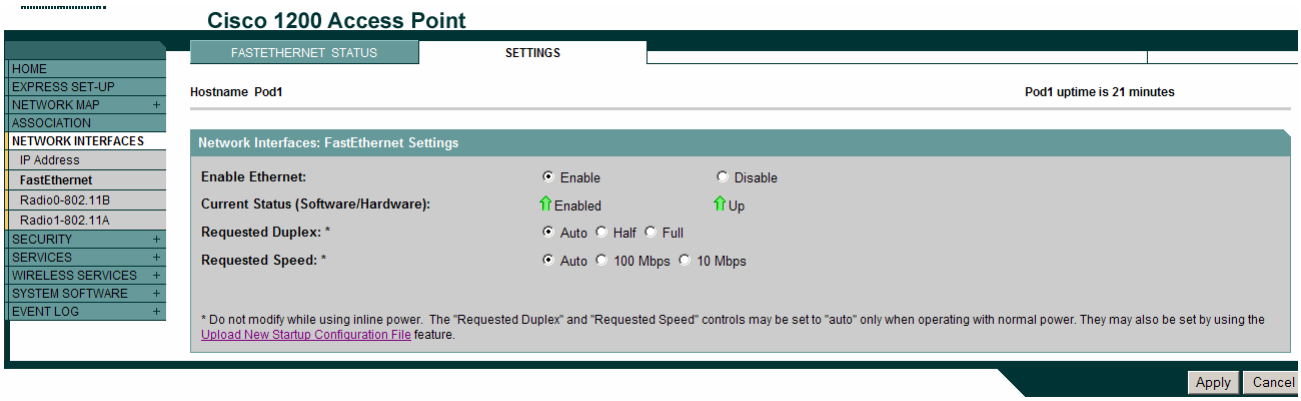
b. Open up a browser on PC1 and browse to the AP's **Home** page

Step 2 Express Setup page



Browse to the **EXPRESS SET-UP** Page and verify the settings configured in Step 1 through GUI.

Step 3 Data rate speed and Duplex of the FastEthernet interface



a. Go to the **NETWORK INTERFACES>FastEthernet** Page and click on the settings tab of the AP.

b. The **Enable Ethernet:** setting should be set to **Enable**.

> **Note** If the FastEthernet settings are modified while connected through the wired network, the connection may be lost. These will actually be modified in Step 4 through the Console. The Requested Duplex Setting should be set to **Auto** by default. In a production environment, the duplex should be locked into the optimum setting of the connected switch.

c. The Requested Speed Setting should be set to **Auto** by default**.** In a production environment, the speed should be locked into the optimum setting of the connected switch.

Step 4 Configure Ethernet/FastEthernet Interfaces through IOS CLI

Typically, an IP address is configured on the BVI interface only. However, there are some other settings which should be set on the FastEthernet interface. Below is a command table which will be used in this step.

Command	Description
configure terminal	enter global configuration mode
interface fastEthernet *interface number*	enter the device Ethernet/fastEthernet interface
duplex *auto|full|half*	set the role of the AP device
show interfaces *<cr>|interface number*	View the interface(s) detailed status
show ip interface brief	View a brief status of IP interfaces
show running-config	View the running configuration
speed *10|100|auto*	set the data rate of the AP

Console into the AP

a. Beginning in configuration mode. Follow these steps to set the AP Ethernet/FastEthernet settings:

```
PodP(config)#interface fastEthernet 0
```


b. Now see what duplex settings are possible.

```
PodP(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
```

c. Set the duplex to full

```
PodP(config-if)#duplex full
```

d. Now see what speed settings are possible.

```
PodP(config-if)# speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

e. Now set the speed to 100 Mbps.

```
PodP(config-if)#speed 100
PodP(config-if)#end
```

f. Check the running configuration.

```
PodP#show running-config
```

g. Display the FastEthernet interface status

```
PodP#show interfaces fastEthernet 0
FastEthernet0 is up, line protocol is up
  Hardware is PowerPC405GP Ethernet, address is 000b.46b8.ca90 (bia 000b.46b8.ca90)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:23:18, output 00:01:54, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1783 packets input, 164809 bytes
     Received 29 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```



```
0 watchdog
0 input packets with dribble condition detected
1141 packets output, 449852 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

h. Quickly verify all the interfaces are up

```
PodP#show ip interface brief
PodP#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
BVI1                       10.0.P.1        YES other  up                    up
Dot11Radio0                unassigned      YES TFTP   up                    up
Dot11Radio1                unassigned      YES TFTP   up                    up
FastEthernet0              unassigned      YES other  up                    up
Virtual-Dot11Radio0        unassigned      YES TFTP   down                  down
Virtual-Dot11Radio1        unassigned      YES TFTP   down                  down
PodP#
```

i. Now check the detailed status of all the interfaces

```
PodP#show interfaces
```

Lab 5.4.4 Configure Radio Interfaces through the GUI

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

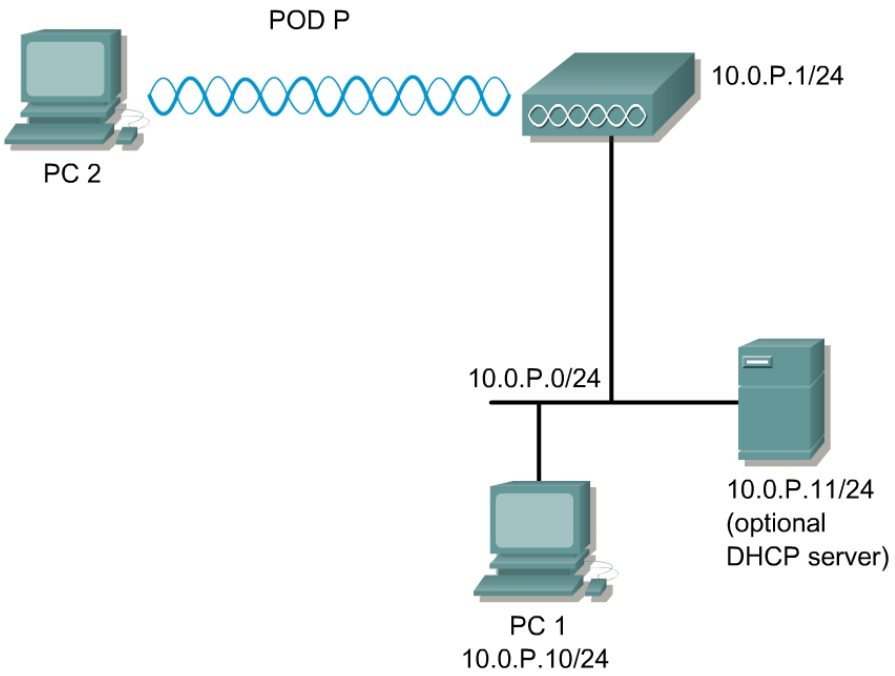
Objective

In this lab, the student will use the Radio 802.11b-setting page to enter basic channel and data rate information for the AP radio. The Radio 802.11b page will also be accessed to enter basic settings for the transmit power, antennas, and operating thresholds on the AP.

Scenario

This section describes how to configure the AP radio. Use the AP Radio interface pages in the management system will be used to set the radio configuration.

Topology



Preparation

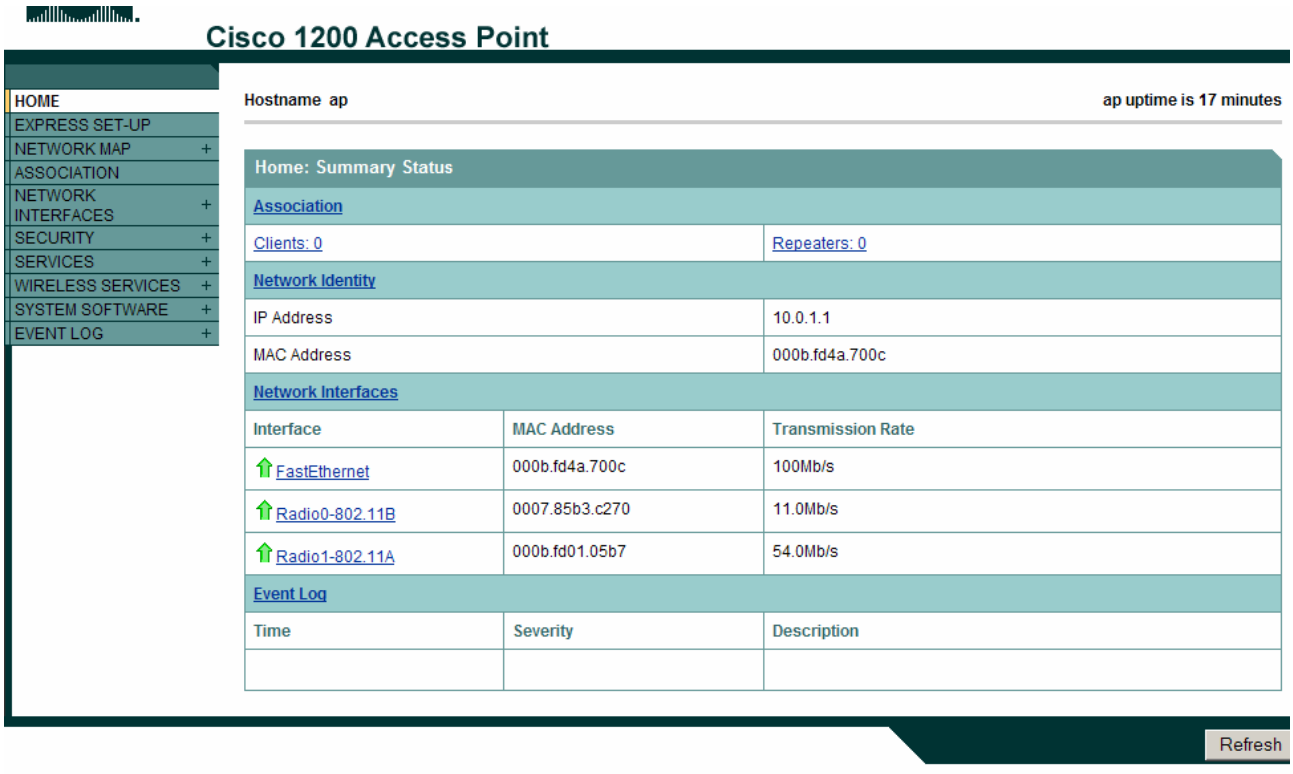
The student PC should be connected to the AP through an isolated wired network or crossover cable. The AP should be set to factory defaults. A DHCP service may be used to assign an address to the AP.

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Tools and Resources

- Cisco APs
- PCs with properly installed Cisco wireless client adapters and utility.
- Several PCs on the wired network that can maintain connectivity to the configuration management pages on the AP.

Step 1 Radio Interface information



a. Open a browser and type in the IP address of the AP that was assigned in the Preparation section of this lab. Log into the AP by pressing TAB while in the username box then type in the default password "Cisco".

Note The password is case sensitive. This should open the AP **HOME** page.

b. Obtain the AP information from this page. It is important for the network administrator to be familiar with the settings on the network equipment.

c. Are there any **Clients** or **Repeaters** connected to the AP? What is the number for each?

_____

d. What is the **IP Address** of the AP?

_____

e. What **Network Interfaces** are available?

_____

_____

_____

f. What is the **Ethernet/FastEthernet** MAC address?

_____

g. If available, what is the Radio 802.11b MAC address?

_____

h. If available, what is the Radio 802.11b Transmission rate?

_____

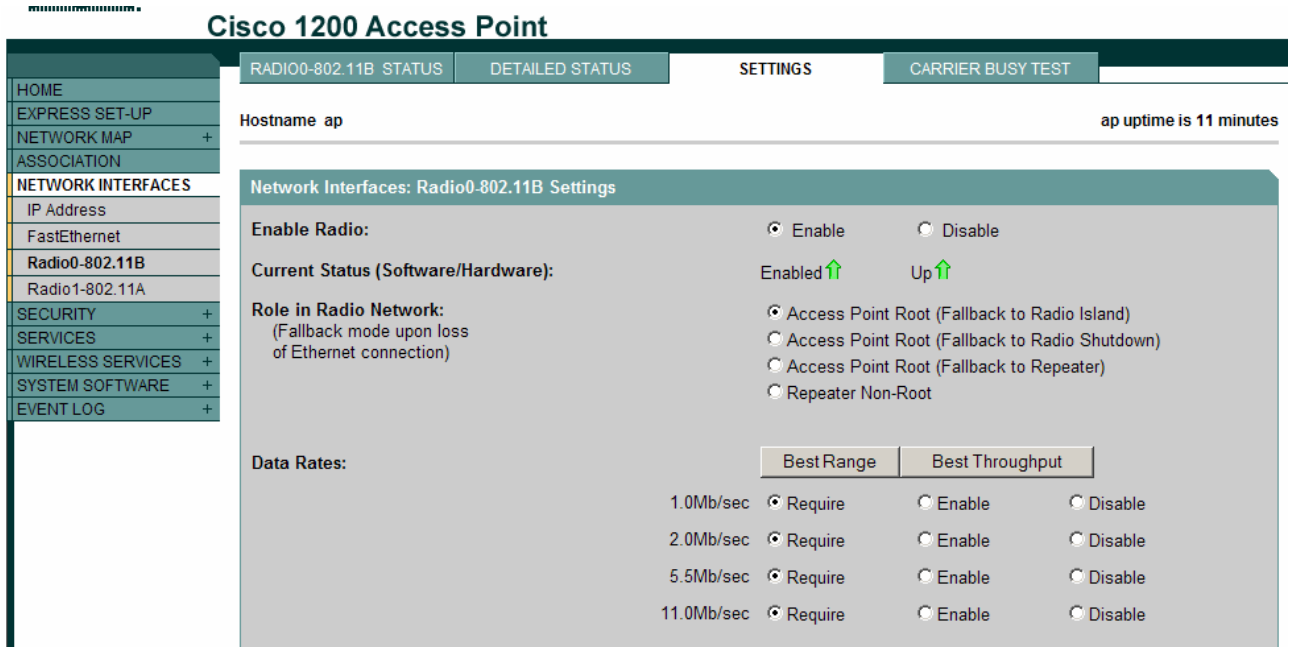
i. If available, what is the Radio 802.11a MAC address?

_____

j. If available, what is the Radio 802.11a Transmission rate?

_____

Step 2 Network Interface settings



If available, click on the **NETWORK INTERFACES>Radio0-802.11B**. Next, click the **SETTINGS** tab. Record the following settings from the Radio Interface page:

a. What is the Enable Radio setting and Current Status?

_____

b. What is the role of this AP?

_____

c. What speeds are configured for the data rates?

_____

d. What is the Enable Radio setting and Current Status?

_____

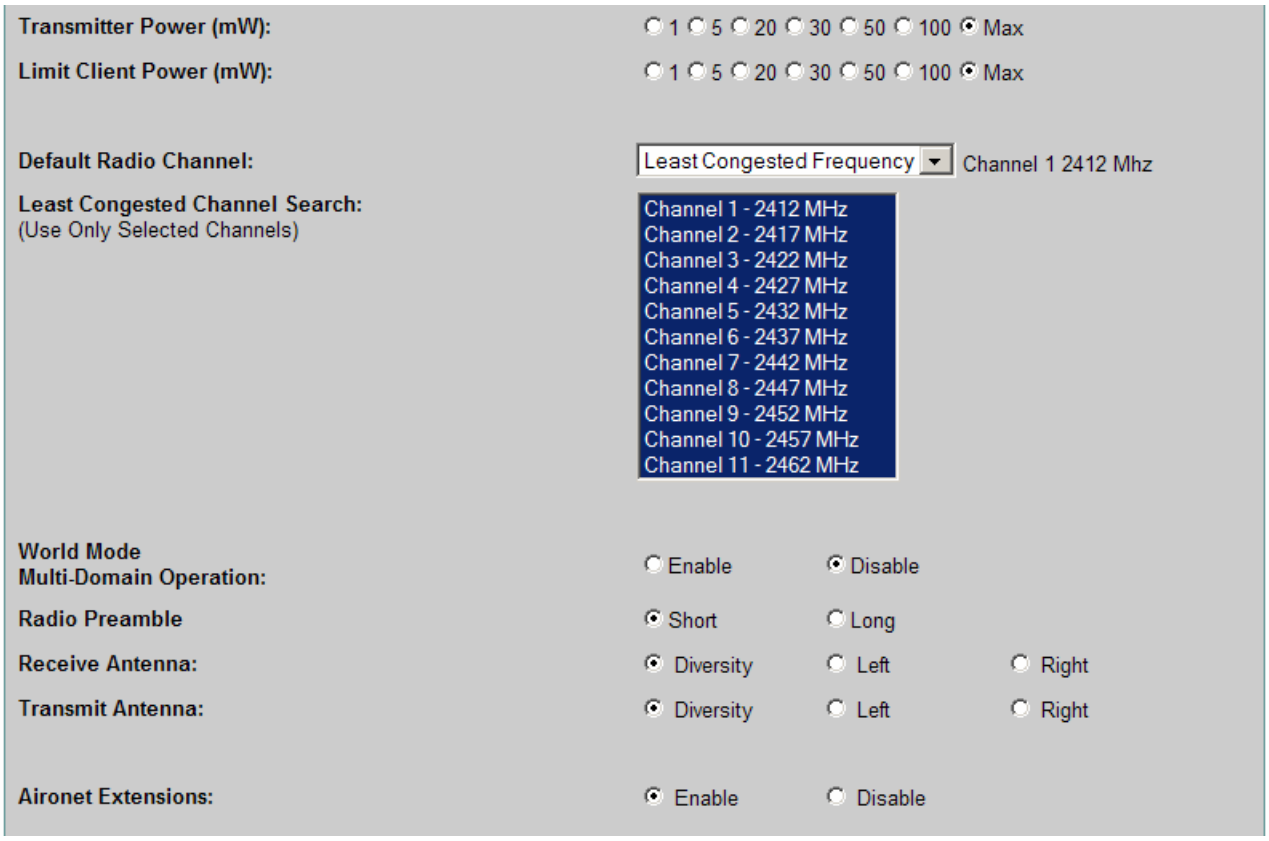
e. What is the role of this AP?

_____

f. What speeds are configured for the data rates?

_____

Scroll down the Network Interface Settings page to view the information displayed in the figure for this step.



g. What is the Transmitter Power setting?

_____

h. What is the Default Radio Channel?

_____

i. What are the other settings on this page? Repeat the **Network Interface Settings** steps for the Radio1-802.11A.

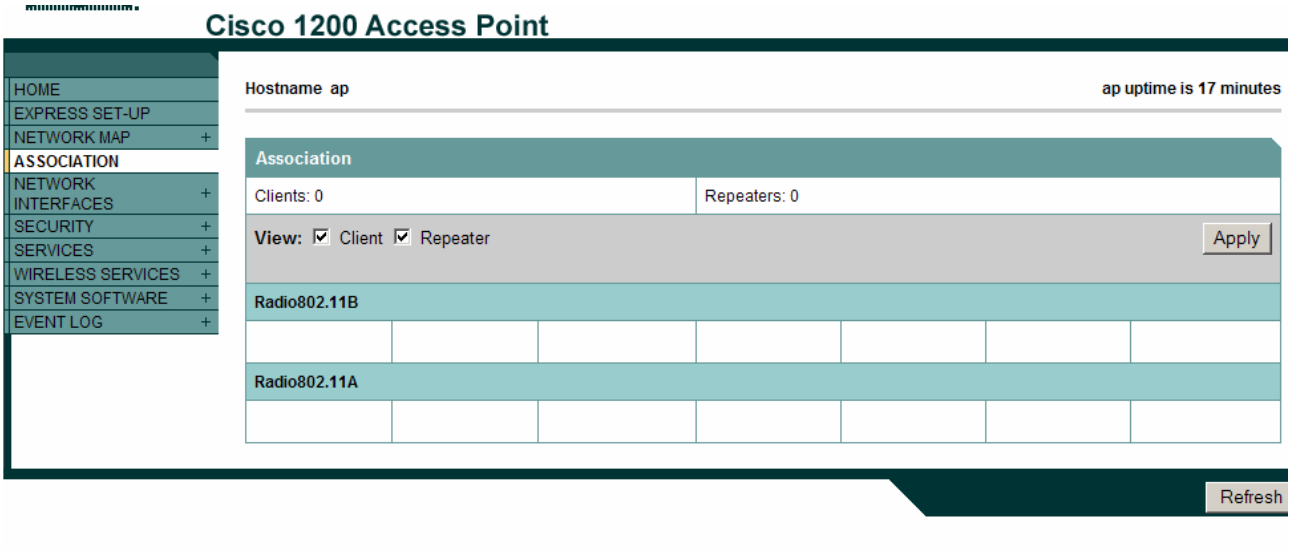
Network Interface Settings

Step 3 Connect to the AP with a wireless PCI NIC

Using a laptop or desktop with a wireless adapter, connect to the correct AP. Make sure the wireless device is not connected by way of the wired network.

a. Configure and select a profile to connect to the AP. Make sure the SSID is configured in the profile to match the AP.
b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members
c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. If a DHCP server is running, configure TCP/IP to receive the address automatically, or configure static IP setting.
d. Now check to see if the ACU icon in the system tray is green, which indicates a successful link to the AP. Double click on the icon to verify the correct **AP Name** and **AP IP Address.**

Step 4 Association page



a. To check which clients are associated to this AP, go to the **ASSOCIATION** page and click on the Association button.

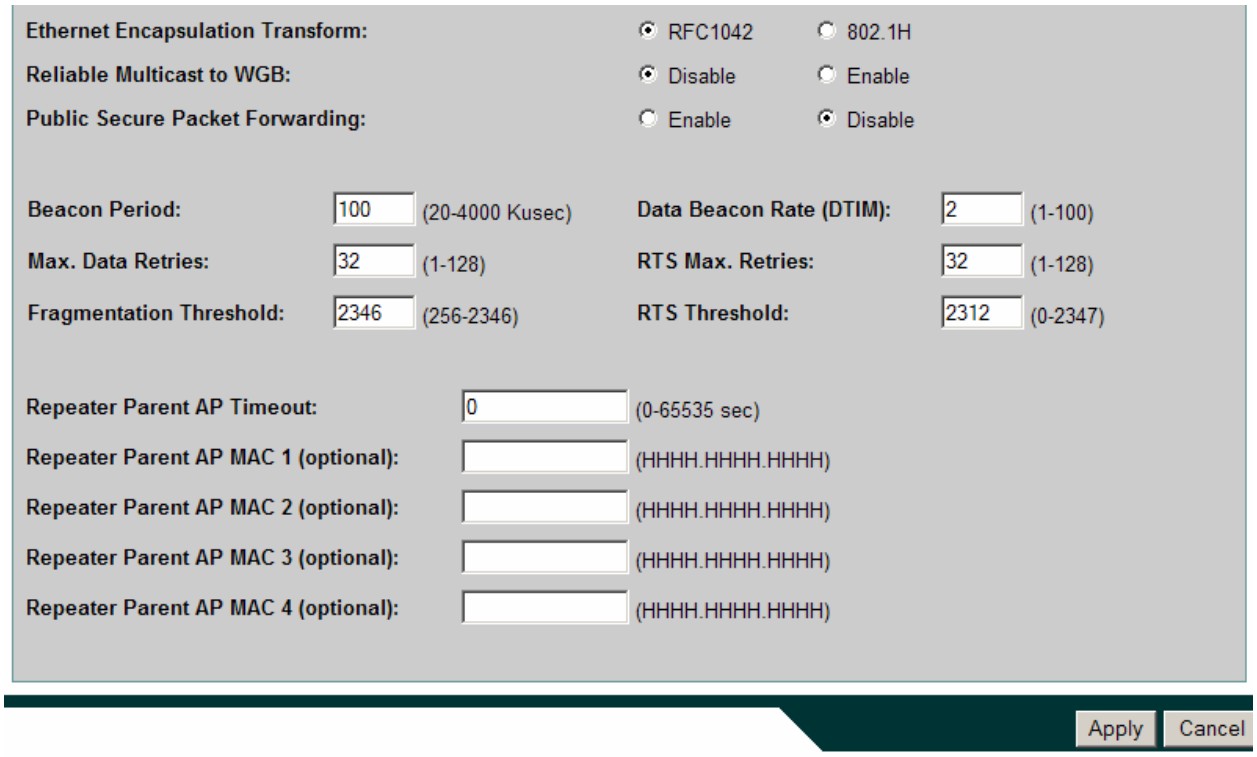
b. Record the MAC Addresses of the devices associated to this AP:

MAC ADDRESS

c. Test connectivity to other devices using ping, Telnet, http, and ftp. This will vary depending on the devices connected and configured on the wired network.

Step 5 Advanced Radio settings

Scroll to the bottom of the Network Interface Settings page to view the information displayed in the figure for this step.



a. What is the Reliable Multicast to WGB setting? What wireless device does this setting pertain to?

_____

b. What is Public Secure Packet Forwarding setting? Why would this be enabled?

_____

c. What is the Beacon Period? What are the advantages and disadvantages of lowering or raising the value?

_____

d. What is the Data Beacon Rate (DTIM)? What are the advantages and disadvantages of lowering or raising the value?

_____

e. What is the Max Data Retries setting? What are the advantages and disadvantages of lowering or raising the value?

_____

f. What is RTS Max Retries setting? What are the advantages and disadvantages of lowering or raising the value?

_____

g. What is the Fragmentation Threshold? What are the units for this value?

_____

h. What is the RTS Threshold setting?

_____

i. What is Repeater Parent AP timeout?

_____

j. What is Repeater Parent AP MAC 1 (optional)?

_____

k. What is Repeater Parent AP MAC 2 (optional)?

_____

l. What is Repeater Parent AP MAC 3 (optional)?

_____

m. What is Repeater Parent AP MAC 4 (optional)?

_____

Step 6 Make changes to the radio interface of the AP (Optional)

Make changes to the radio interface. Perform the setting changes through the web browser interface. As changes are made, use several of the Cisco Aironet client utility tools to test various settings on the radio interface. Take care to make one change at a time and monitor the performance change in either of the site survey or link status meter tools.

Make a change to the APs receive and transmit antenna settings. By default they are set to diversity. Change the setting to left or right. Have your lab partner move about the site with the laptop and see if there is any degradation or improvement in the radio signal.

a. Which antenna setting had the best performance?

_____

b. Which antenna setting had the worst performance?

_____

Note If there is delay caused by congestion, change the channel settings and see if performance is improved. Remember, on the 802.11b, there are only three non-overlapping channels (1, 6, and 11) that can be used in the BSS/ESS topology that this lab is creating. Coordinate channel settings with other team members or set the AP to seek a less congested channel.

c. Which channel setting had the best performance?

_____

d. Which channel setting had the worst performance?

_____

e. Change the Transmitter Power settings and make note of any data rate performance or range. Was there any enhancement or degradation in the performance of the AP? With the instructors permission, see how far the wireless client can roam with the lowest/highest setting.

_____

f. If there was, which Transmitter Power setting gave the furthest range or strongest signal?

_____

g. Which Transmitter Power setting gave the fastest data rate?

_____

Lab 5.4.5 Configure Radio Interface through the IOS CLI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

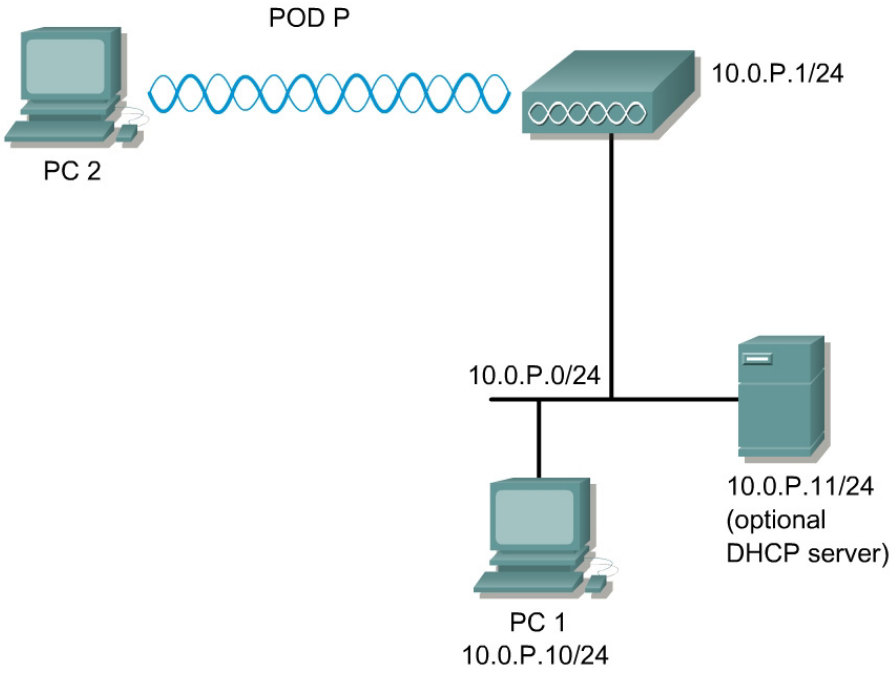
Objective

In this lab, the student will enter basic channel and data rate information for the AP radio.

Scenario

This section describes how to configure the AP radio. Use the AP Radio interface pages in the management system will be used to set the radio configuration.

Topology



Preparation

Configure a PC and AP according to the Topology

Tools and Resources

- One AP
- PCs with properly installed Cisco wireless client adapters and utility.
- Several PCs on the wired network that can maintain connectivity to the configuration management pages on the AP.

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
configure terminal	enter global configuration mode
interface dot11radio *number*	enter the device radio interface. The *number* is 0 for 11b and 1 for 11a. Depending on the installed radio(s), one or both will be available.
station-role	set the role of the AP device
speed basic	set the data rate of the AP
power client	set the power level output of the AP
channel	set the channel of the AP
world-mode	set world-mode on the AP
preamble	set the preamble
antenna	set the receive or transmit antenna

Step 1 Connect to the AP

Connect to the AP using the console or telnet.

Enter global configuration mode with the following command:

```
PodP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PodP(config)#
```

Step 2 View the available 802.11b radio settings

The AP radio has many available settings.

Use the following commands to view the available commands for the 802.11b radio:

```
PodP(config)#interface dot11radio 0
PodP(config-if)#?
  antenna                 dot11 radio antenna setting
  beacon                  dot11 radio beacon
  channel                 Set the radio frequency
  description             Interface specific description
  dot11                   IEEE 802.11 config interface commands
  dot1x                   IEEE 802.1X subsystem
  exit                    Exit from interface configuration mode
  fair-queue              Enable Fair Queuing on an Interface
  mac-address             Manually set interface MAC address
  power                   Set radio transmitter power levels
  preamble-short          Use 802.11 short radio preamble
  rts                     dot11 Request To Send
  shutdown                Shutdown the selected interface
  speed                   Set allowed radio bit rates
  ssid                    Configure radio service set parameters
  station-role            role of the radio
  world-mode              Dot11 radio world mode
```


Notice that there are many more configuration settings available.

Step 3 Configuring the role in radio network

To configure the AP as a root device that is connected to the wired LAN or as a repeater (non-root) device that is not connected to the wired LAN.

View the available station roles. Then configure the AP as a root AP:

```
PodP(config-if)#station-role ?
  repeater  Repeater access point
  root      Root access point

PodP(config-if)#station-role root
```

Step 4 Configuring radio data rates

To use the data rate settings to choose the data rates the AP uses for data transmission. The rates are expressed in megabits per second.

View the available speeds.

```
PodP(config-if)#speed ?
  1.0          Allow 1 Mb/s rate
  11.0         Allow 11 Mb/s rate
  2.0          Allow 2 Mb/s rate
  5.5          Allow 5.5 Mb/s rate
  basic-1.0    Require 1 Mb/s rate
  basic-11.0   Require 11 Mb/s rate
  basic-2.0    Require 2 Mb/s rate
  basic-5.5    Require 5.5 Mb/s rate
  range        Set rates for best range
  throughput   Set rates for best throughput
  <cr>
PodP(config-if)#
```

Use the following commands to set up the AP for 11-Mbps service only:

```
PodP(config-if)#speed basic-11.0 1.0 2.0 5.5
PodP(config-if)#
```

Step 5 Configuring radio transmit power

The power level on client devices that associate to the AP and the AP radio power can be manually set. Use the help to view the power settings which can be configured.

```
PodP(config-if)#power ?
  client  Client radio transmitter power level
  local   Local radio transmitter power level
PodP(config-if)#
```

See which power levels are configurable on the AP.

```
PodP(config-if)#power local ?
```



```
  <1-100>  One of: 1 5 20 30 50 100
  maximum  Set local power to allowed maximum
PodP(config-if)#
```

Configure the AP radio power to 5mW.

```
PodP(config-if)#power local 5
*Mar  1 02:07:19.457: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:07:19.475: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

When a client device associates to the AP, the AP sends the maximum power level setting to the client. Follow these steps to specify a maximum allowed power setting on all client devices that associate to the AP, the example below sets the radio transmit power to 100mW:

```
PodP(config-if)#power client 100
PodP(config-if)#
```

Now lower the setting to 5mw:

```
PodP(config-if)#power client 5
*Mar  1 02:01:42.123: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:01:42.141: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

Step 6 Configuring radio channel settings

The default channel setting for the AP radios is least congested. At startup, the AP scans for and selects the least congested channel. For the most consistent performance after a site survey, it is recommended that a static channel setting for each AP be assigned. The channel settings on your AP correspond to the frequencies available in your regulatory domain.

See what channels are available.

```
PodP(config-if)#channel ?
<1-2462>         One of: 1 2 3 4 5 6 7 8 9 10 11 2412 2417 2422 2427
2432 2437 2442 2447 2452 2457 2462
  least-congested  Scan for best frequency
PodP(config-if)#
```

Follow the steps below to assign a static channel setting for the AP. The example below sets the radio to channel 1:

```
PodP(config-if)#channel 1   (or the channel frequency)
*Mar  1 02:10:46.872: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:10:46.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

Now assign a least congested channel setting for the AP. The example below sets the radio to the least congested channel setting:

```
PodP(config-if)#channel least-congested
*Mar  1 02:12:38.761: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:12:39.760: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio 0, changed state to down
*Mar  1 02:12:43.265: %DOT11-6-FREQ_USED: Interface Dot11Radio0,
frequency 2412 selected
*Mar  1 02:12:43.285: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
*Mar  1 02:12:44.267: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio 0, changed state to up
PodP(config-if)#
```

Notice the output on the console displays the AP selecting the frequency that is least congested at that point and time.

Step 7 Enabling and disabling world-mode

When **world-mode** is enabled, the AP adds channel carrier set information to its beacon. Client devices with **world-mode** enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on **world-mode** to adjust its channel and power settings automatically when it travels to Italy and joins a network there. World mode is disabled by default.

To enable **world-mode** on the AP, follow the steps below:

```
PodP(config-if)#world-mode
*Mar  1 02:14:32.793: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:14:32.811: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

To disable **world-mode** on the AP, follow the steps below:

```
PodP(config-if)#no world-mode
*Mar  1 02:15:00.730: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to down
*Mar  1 02:15:00.732: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:15:00.750: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

Step 8 Disabling and enabling short radio preambles

The radio preamble (sometimes called a *header*) is a section of data at the head of a packet that contains information that the AP and client devices need when sending and receiving packets. The radio preamble can be set to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.

- Long—A long preamble ensures compatibility between the AP and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your APs, you should use short preambles.

Follow these steps to disable short radio preambles:

```
PodP(config-if)#no preamble-short
*Mar  1 02:16:03.156: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:16:03.174: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

Follow these steps to enable short radio preambles:

```
PodP(config-if)#preamble-short
*Mar  1 02:16:24.843: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:16:24.861: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
PodP(config-if)#
```

Step 9 Configuring transmit and receive antennas

The AP can be set to select the antenna the AP uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- Diversity—This default setting tells the AP to use the antenna that receives the best signal. If your AP has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- Right—If your AP has removable antennas and you install a high-gain antenna on the AP's right connector, you should use this setting for both receive and transmit. When you look at the AP's back panel, the right antenna is on the right.
- Left—If your AP has removable antennas and you install a high-gain antenna on the AP's left connector, you should use this setting for both receive and transmit. When you look at the AP's back panel, the left antenna is on the left.

View the available antenna settings

```
PodP(config-if)#antenna ?
  receive   receive antenna setting
  transmit  transmit antenna setting
```

Follow these steps to set the AP receive and transmit to right: (the interfaces will reset after each change.)

```
PodP(config-if)#antenna receive right
PodP(config-if)#antenna transmit right
PodP(config-if)#
```

Follow these steps to set the AP receive and transmit to left:

```
PodP(config-if)#antenna receive left
PodP(config-if)#antenna transmit left
```



```
PodP(config-if)#
```

Follow these steps to set the AP back to receive and transmit to diversity:

```
PodP(config-if)#antenna receive diversity
PodP(config-if)#antenna transmit diversity
PodP(config-if)#
```

Step 10 Disable the radio

If the PC is connected through wireless, it is important to switch to a console connection.

Use the shutdown command to turn off the radio. Afterwards, re-enable the interface.

```
PodP(config-if)#shutdown
*Mar  1 02:27:18.082: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to administratively down
*Mar  1 02:27:18.082: %LINK-5-CHANGED: Interface Virtual-
Dot11Radio0, changed state to administratively down
*Mar  1 02:27:19.083: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio0, changed state to down
PodP(config-if)#
PodP(config-if)#no shutdown
*Mar  1 02:28:00.414: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:28:00.414: %LINK-3-UPDOWN: Interface Virtual-Dot11Radio0,
changed state to down
*Mar  1 02:28:00.433: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
*Mar  1 02:28:01.432: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio 0, changed state to up
```

Optional Steps for 802.11a radio if available

Step 11 View the available 802.11a radio settings

The AP radio has many available settings.

Use the following commands to view the available commands for the 802.11a radio:

```
PodP(config)#interface dot11radio 1
PodP(config-if)#
```

a. What command is needed to see the available commands in the interface mode?

_____

Step 12 Configuring the Role in Radio Network

Configure the AP as a root AP:

a. What command is needed?

_____

Step 13 Configuring Radio Data Rates

View the available data rates for the 11a radio.

a. What command is needed?

_____

b. What speeds are available?

_____

_____

_____

Step 14 Configuring Radio Transmit Power

View the available power settings which can be configured.

a. What command is needed? What power settings are configurable?

_____

See which power levels are configurable on the AP radio.

b. What command is needed? What are the available power levels for the local radio transmitter?

_____

Configure the AP radio power to 10 mW.

c. What command is needed?

_____

Configure the client radio transmit power to 40 mW.

d. What command is needed?

_____

Now lower the setting to 5mw.

e. What command is needed?

_____

Step 15 Configuring Radio Channel Settings

See what 11a channels are available.

a. What command is needed? What channels are available?

_____

_____

_____

_____

Assign static channel 36 to the AP.

b. What command is needed?

_____

Now assign a least congested channel setting for the AP.

c. What command is needed?

_____

Step 16 Configuring Transmit and Receive Antennas

View the available antenna settings.

a. What command is needed? What settings are available?

_____

_____

_____

Configure the AP to receive and transmit to right. (the interfaces will reset after each change.)

b. What commands are needed?

_____

_____

Set the AP to receive and transmit to left.

c. What commands are needed?

_____

_____

Set the AP back to receive and transmit to diversity.

d. What commands are needed?

_____

_____

Step 17 Disable the radio

If the PC is connected through wireless, it is important to switch to a console connection.

Use the shutdown command to turn off the radio. Afterwards, re-enable the interface.

a. What commands are needed?

_____

_____

Lab 5.4.8 Configure an AP as a Repeater through the IOS CLI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

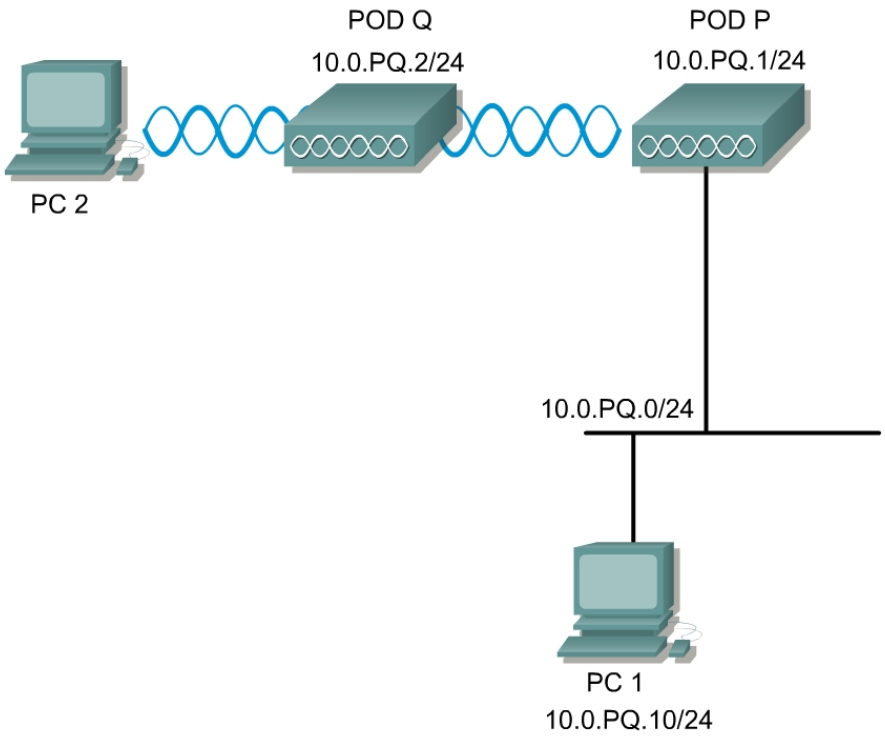
The student will extend the coverage of a basic service set topology by implementing an AP as a repeater.

Scenario

An AP can be configured as a repeater to extend the wireless infrastructure range or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an AP connected to the wired LAN. The data is sent through the route that provides the best performance for the client. In this lab, the Root AP will be Pod***P***. The repeater AP will be Pod***Q***.

A chain of several repeater APs can be setup, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1 (root) P	AP12	10.0.12.1/24
	Pod2 (repeater) Q	AP12	10.0.12.2/24

PC1 should be connected to the wired network. A second team can use the BR350s for the lab, however students must use the VxWorks GUI to configure the steps. It is recommended that students use IOS based APs first.

Tools and Resources

Each team will need:

- 2 APs
- A wired PC (PC1)
- A wireless PC or laptop (PC2)
- Console cable

Additional Materials

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Step 1 Basic AP Configuration to both APs

Console into the AP. Clear the configuration on both of the APs. Then put a basic configuration in the APs.

A sample config is shown using Pod 1.(root AP)

```
ap(config)#hostname Pod1
Pod1(config)#enable secret cisco
Pod1(config)#int bvi 1
Pod1(config-if)#ip address 10.0.12.1 255.255.255.0
Pod1(config-if)#no ssid tsunami
Pod1(config-if)#ssid AP12
Pod1(config-if-ssid)#authentication open
Pod1(config-if-ssid)#infrastructure-ssid
Pod1(config-if-ssid)#end
Pod1#copy run start
```

A sample config is shown using Pod 2. (repeater AP)

```
ap(config)#hostname Pod2
Pod2(config)#enable secret cisco
Pod2(config)#int bvi 1
Pod2(config-if)#ip address 10.0.12.2 255.255.255.0
Pod2(config-if)#no ssid tsunami
Pod2(config-if)#ssid AP12
Pod2(config-if-ssid)#authentication open
Pod2(config-if-ssid)#infrastructure-ssid
Pod2(config-if-ssid)#end
Pod2#copy run start
```

Configure a client and make sure it can associate with the first AP and then the second AP. You will probably have to power off the AP that you are not testing. This will confimed that the APs are configured and operational and clients can connect to the AP***P***.

Step 2 Basic configure the repeater AP

A sample config is shown using Pod 1 as root and Pod 2 as repeater.

a. Pod***P*** will be the root AP and should have a SSID of "AP***PQ***". Pod***Q*** will become the repeater AP. The repeater AP will not require any Ethernet cables when configured in repeater mode. Also, if Aironet extensions are disabled, enable Aironet extensions.

b. Set the AP role in the wireless LAN to repeater.

```
Pod2#config t
Pod2(config)#int Dot11Radio 0
Pod2(config-if)#station-role repeater
Pod2(config-if)#dot11 extension aironet
Pod2(config-if)#end
Pod2# copy run start
```

c. MAC addresses can be entered for up to four parent APs. The repeater attempts to associate to MAC address 1 first; if that AP does not respond, the repeater tries the next AP in its parent list. (Optional) Enter the MAC address for the AP's radio interface to which the repeater should associate.

```
Pod2(config-if)#parent 1 RRRR.RRRR.RRRR
```

(where RRRR.RRRR.RRRR = the MAC address of Pod1 11.b radio [not the fastethernet interface])

d. Verify the configuration

Sample config shown

```
Pod2#show run
   interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid AP12
       authentication open
       infrastructure-ssid
   !
    parent 1 0987.1234.e345 <MAC address will vary>
    speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
    rts threshold 2312
    station-role repeater
```

Step 3 Verify client associates with root

After the repeater is setup, force the client to associate with the repeater and not the root. Make sure the TCP/IP settings and SSID are configured on the laptop. The client may be associated with the repeater or the root. To ensure that the client is associated to the repeater AP:

a. Make sure the configuration on the root AP is saved by using the **`copy run start`** command.

b. Remove the power from the root AP.

c. Verify the client is associated to the repeater using the Aironet Client Utility.

d. When the client is associated with the repeater, re-power the root AP.

e. Once the root AP has booted, ping the root bridge from the client.

Step 4 Verify connections on repeater

After the client is associated with the repeater AP, check the LEDs on top of the repeater AP. If the repeater is functioning correctly, the LEDs on the repeater and the root AP to which it is associated behave like this:

- The status LED on the root AP is steady green, indicating that at least one client device is associated with it (in this case, the repeater).
- The status LED on the repeater AP is steady green when it is associated with the root AP and the repeater has client devices associated to it. The repeater's status LED flashes (steady green for 7/8 of a second and off for 1/8 of a second) when it is associated with the root AP but the repeater has no client devices associated to it.

The repeater AP should also appear as associated with the root AP in the root AP's Association Table. On Pod***P***, verify that Pod***Q*** is connected. There may also be other wireless clients associated.

a. In privilege mode of the repeater, enter the following command to view what information can be displayed

```
Pod2#show dot11 associations ?
```

1. What information is available?

_____

_____

_____

b. Now check the detailed status of all clients

```
Pod2#show dot11 associations all-clients
```

```
Pod2#show dot11 associations all-client
Address           : 0007.85b3.8850     Name             : Pod2
IP Address        : 10.0.12.2          Interface        : Dot11Radio 0
Device            : ap1200-Parent      Software Version :

State             : Assoc              Parent           : Our Parent
SSID              : AP12               VLAN             : 0
Hops to Infra     : 0                  Association Id   : 1
Current Rate      : 11.0               Encryption       : Off
Key Mgmt type     : NONE
Supported Rates   : 1.0 2.0 5.5 11.0
Signal Strength   : -27  dBm           Connected for    : 2541 seconds
Signal Quality    : 80 %               Activity Timeout : 66 seconds
Power-save        : Off                Last Activity    : 0 seconds ago

Packets Input     : 444                Packets Output   : 145
Bytes Input       : 63984              Bytes Output     : 25975
Duplicates Rcvd   : 0                  Data Retries     : 2
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0
MIC Missing       : 0
```


c. In privilege mode of the repeater, verify that the laptop is associated. There may also be other wireless clients associated.

d. Check the detailed status of all clients

```
Pod2#show dot11 associations all-clients
```

```
Pod2#show dot11 associations all-client
Address           : 0007.eb30.a37d     Name             : VIAO
IP Address        : 10.0.12.20         Interface        : Dot11Radio 0
Device            : 350-client         Software Version : 5.20

State             : Assoc              Parent           : self
SSID              : AP12               VLAN             : 0
Hops to Infra     : 1                  Association Id   : 3
Clients Associated: 0                  Repeaters associated: 0
Current Rate      : 11.0               Encryption       : Off
Key Mgmt type     : NONE
Supported Rates   : 1.0 2.0 5.5 11.0
Signal Strength   : -32  dBm           Connected for    : 2866 seconds
Signal Quality    : 88 %               Activity Timeout : 22 seconds
Power-save        : Off                Last Activity    : 3 seconds ago

Packets Input     : 333                Packets Output   : 1
Bytes Input       : 20624              Bytes Output     : 80
Duplicates Rcvd   : 0                  Data Retries     : 0
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0
MIC Missing       : 0

Address           : 000b.be0e.27e5     Name             : AP2
IP Address        : 10.0.12.8          Interface        : Dot11Radio 0
Device            : ap1200-Rptr        Software Version : 12.2

State             : Assoc              Parent           : self
SSID              : AP12               VLAN             : 0
Hops to Infra     : 1                  Association Id   : 2
Clients Associated: 0                  Repeaters associated: 0
Current Rate      : 11.0               Encryption       : Off
Key Mgmt type     : NONE
Supported Rates   : 1.0 2.0 5.5 11.0
Signal Strength   : -25  dBm           Connected for    : 2870 seconds
Signal Quality    : 85 %               Activity Timeout : 43 seconds
Power-save        : Off                Last Activity    : 20 seconds ago

Packets Input     : 155                Packets Output   : 480
Bytes Input       : 29388              Bytes Output     : 69571
Duplicates Rcvd   : 0                  Data Retries     : 4
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0
MIC Missing       : 0
```

1. Is the laptop associated? What information can be used to verify the connection?

_____

_____

_____

Step 5 Configure the 802.11a radio as a repeater (optional)

Erase the configuration on both APs. Return to step 1 and configure the repeater topology using the 801.11a radio instead. In this case, disable the 11b radios.

Lab 6.1.6 Resetting the Bridge

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two

Objective

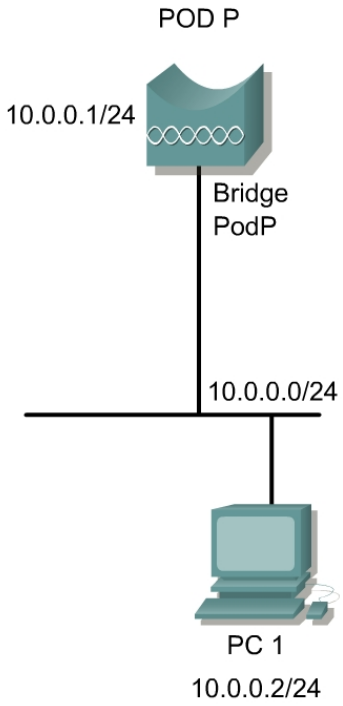
Reset the bridge to factory defaults.

Scenario

You can use the web-browser interface or the CLI to reset the access point/bridge to a factory default configuration. The following steps reset all configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

Note The default username and password are both *Cisco*, which is case-sensitive.

Topology



Preparation

The students will read and familiarize themselves with the concepts in Chapter 6 prior to attempting this lab.

Tools and Resources

Each team will require the following:

- One BR1310
- One PC on the wired LAN and connected via console for bridge configuration

Step 1 Resetting the bridge from the web interface

In order to use the web interface to reset the bridge, the IP address and passwords must be known. The CLI can be used to view the IP address if the passwords are known. If the passwords are not known, the bridge must be reset using the CLI from the console connection.

a. Open a browser and enter the bridge's IP address in the browser address or location line. Press Enter.

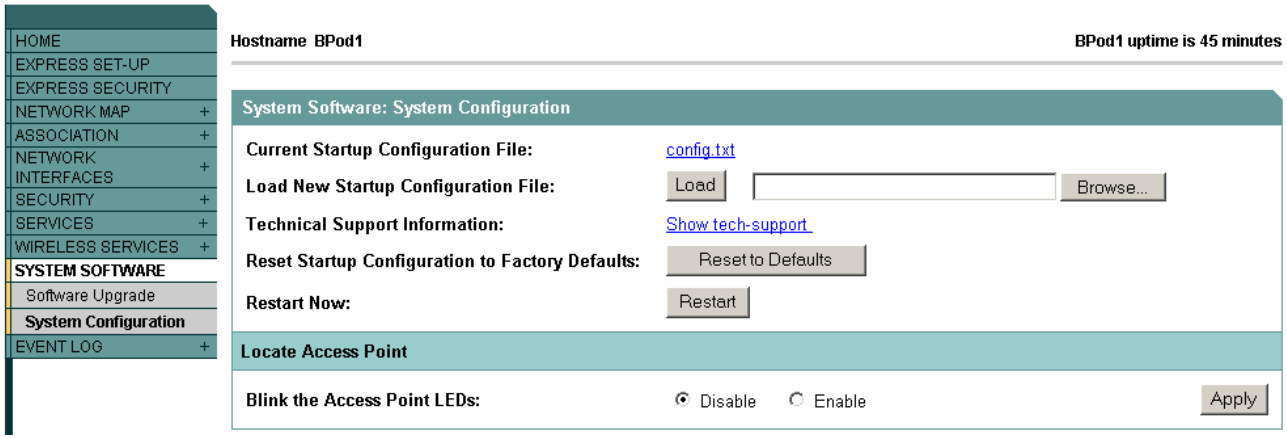
b. When the Enter Network Password screen appears enter a username and password in the appropriate fields. (Defaults for both username and password: *Cisco*)

c. After successful login, the Summary Status page will display.

d. Click **System Software** then **System Configuration** in the left navigation bar. From the System Configuration screen click *Reset to Defaults*. Confirm your choice by clicking the *OK* button in the confirmation window.

e. The bridge will reboot to factory default settings. (Note: If the bridge is configured with a static IP address, the IP address will not change.)

f. After the bridge reboots, it can be configured using either the Web-browser interface or the CLI.



Step 2 Reset the bridge from the CLI

A bridge that has been previously configured may be inaccessible due to a lost or forgotten password. Without the password, the web interface cannot be used to reset the bridge. The CLI provides a method for resetting a bridge when the password is unknown.

a. Open the CLI using a connection to the bridge's console port.

b. Reboot the bridge by removing power and reapplying power.

c. Let the bridge boot until the command prompt appears and the bridge begins to inflate the image. When you see the # symbols on the CLI, press **Esc**:

```
Loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-
mx.v122_15_ja.20040314"...################################## [Esc]
```

Note: Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

d. At the **bridge:** prompt, enter the following command to show a directory of the flash file system similar to the directory shown below:

```
bridge: dir flash:
Directory of flash:/
3    -rwx  1140    <date> config.txt
4    drwx  384     <date> c1310-k9w7-mx.122-15.JA
139  -rwx  5       <date> private-config
140  -rwx  70      <date> env_vars
143  -rwx  3511808 <date> tftp
181248 bytes available (7560192 bytes used)
```

The files **config.txt** and **env_vars** must be deleted or renamed. To keep a copy of the configuration, these files must be renamed. If the files are renamed, they can be used to restore the configuration while allowing you to change the password.

e. Delete both files to restore the bridge to factory defaults.

```
bridge: delete flash:config.txt flash:oldcfg.txt
bridge: delete flash:/env_vars flash:/oldenvars
```

f. Issue the boot command to reboot the bridge.

```
bridge: boot
```

g. The bridge will reboot with factory default values including the IP address (set to receive an IP address using DHCP). To obtain the unit's new IP address, you can use the `show interface bvi1` CLI command. If the unit does not receive an IP address from a DHCP server, the IP address is set to 10.0.0.1.

Note: Do not interrupt the boot process to avoid damaging the configuration file. Wait until the bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished:

```
Line protocol on Interface Dot11Radio0, changed state to up.
```

Lab 6.2.2 Configuring Basic Bridge Settings

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

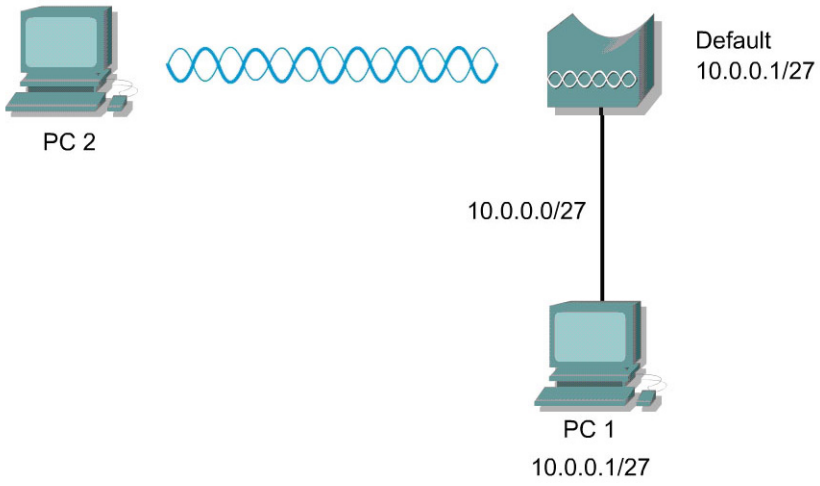
Objective

In this lab, the student will assign basic parameters to the bridge using the GUI and IOS CLI. The Express Setup and Express Security pages will also be accessed through a web browser to assign the IP address, subnet mask, default gateway, and SSID to the bridge.

Scenario

Basic configuration of a bridge can be done through the GUI or IOS CLI.

Topology



Preparation

The student PC should be connected to the bridge through an isolated wired network or crossover cable. The bridge should be set to factory defaults.

Tools and Resources

Each team will need:

- One bridge
- The bridge Power Injector
- A PC (PC1) that is connected to the same wired network as the bridge
- A wireless PC or laptop (PC2)

Command List

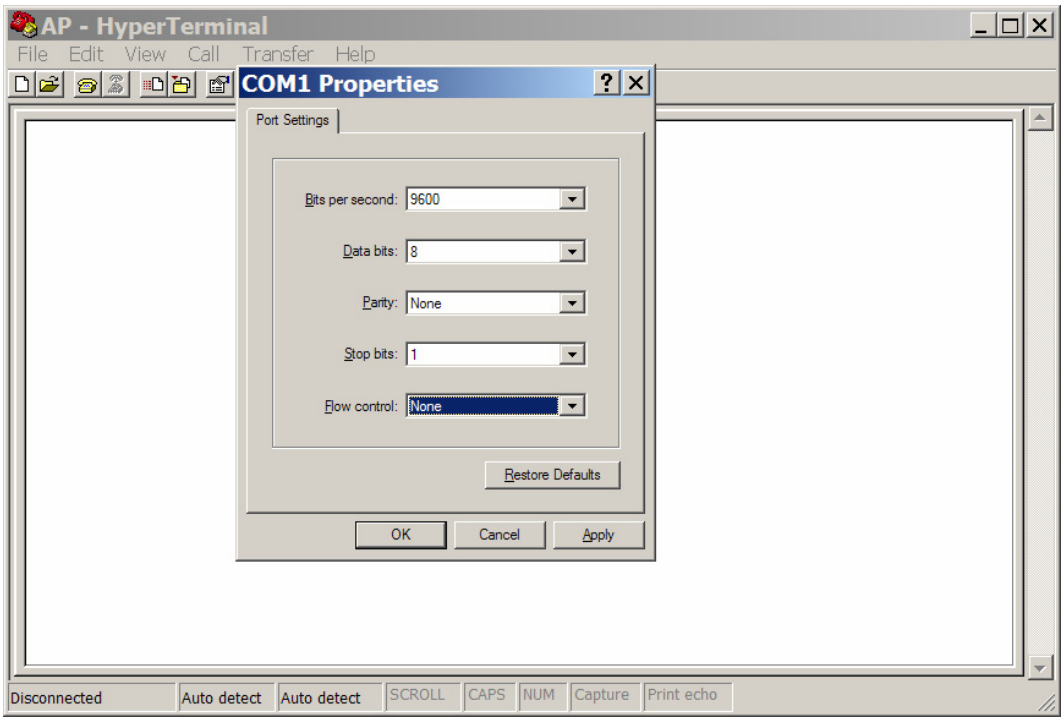
In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
configure terminal	Enter Global configuration mode
hostname	Set the hostname on the device
interface bvi1	Enter the virtual interface for the bridge
ip address	Set the IP address and subnet mask on the device
interface dot11radio 0	Enter the device radio interface
station role install | non-root | root [ap-only] | workgroup-bridge	Set the bridge role. Set the role to install, non-root, root or workgroup bridge. (Optional) If root mode is selected, the bridge can be used as a root bridge or a root AP. When set to ap-only mode, the fallback role of the radio can be selected as repeater or shutdown. If the Ethernet port of the bridge is disabled or disconnected from the wired LAN, the bridge can either shut down its radio port or become a repeater bridge associated to a nearby root bridge.
ssid ssid-string	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note:** Do not include spaces or underscore characters in SSIDs.
enable password *password*	The default password is Cisco. This commands allows an administrator to change the password
enable secret *password*	The default enable password is *Cisco*.
enable password level *level password*	The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
show dot11 associations	View the associated wireless devices
show running-config	Display the current configuration of the device
show startup-config	Display the startup configuration of the device
copy running-config startup-config	Save the entries into the configuration file
show interfaces	Display interface information of the device
logging console 4	Turn off notification logging to avoid interruptions during configuration.

Step 1 Connect to the bridge using a console

a. Connect a PC to the bridge power injector's serial port using a DB-9 to RJ-45 serial cable.

b. Open a terminal emulator.



c. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

d. Press Return to get started

Step 2 Configure PC1

Make sure the bridge is connected to PC1 by way of a wired connection.

a. Configure the IP address, subnet mask, and gateway on PC1

4. IP address 10.0.0.2
5. Subnet Mask 255.255.255.224
6. Gateway 10.0.0.1

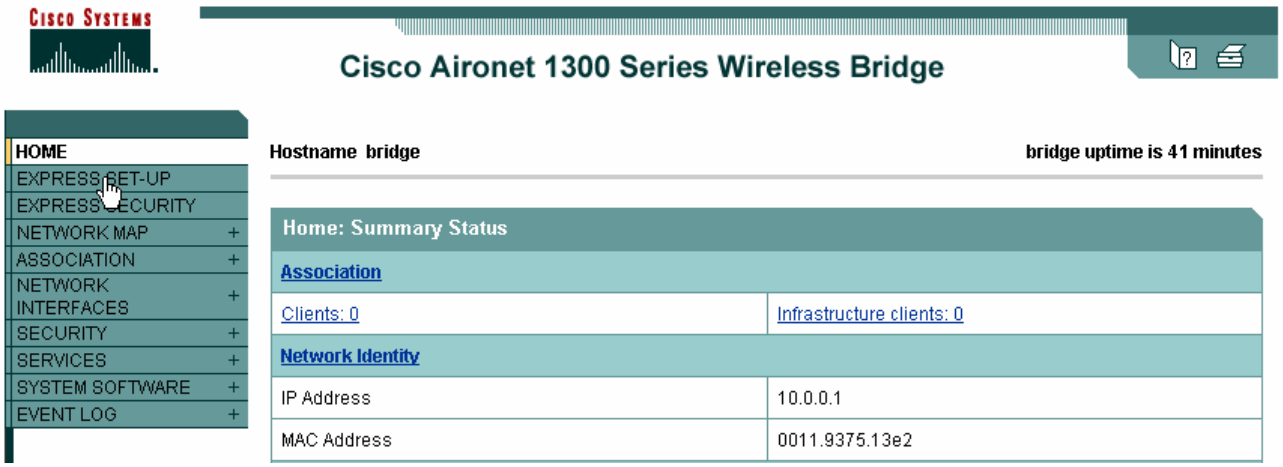
Step 3 Connect to bridge using the web browser

a. Open an Internet browser. The default IP address of a bridge from the factory is 10.0.0.1.

b. Type the bridge IP address in the browser address location field. Press **Enter**.

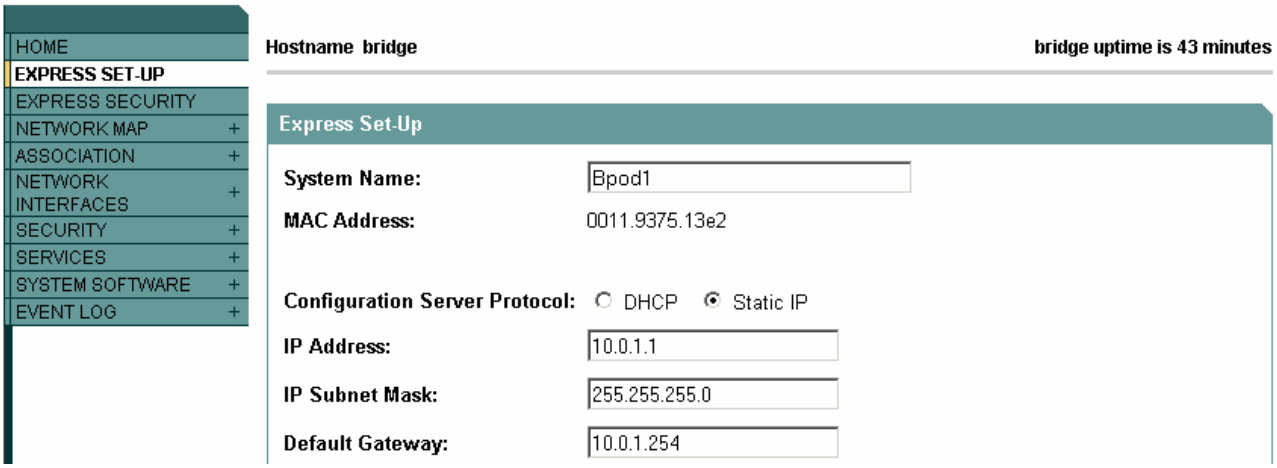
c. A log in screen appears. Type in the password of **Cisco** (case sensitive) and click OK.

d. When the bridge HOME page appears, click **Express Setup** from the left navigation bar.



e. Type a system name of BPod**P** (where **P** is the Pod or Team number) for the bridge in the System Name field.

f. Select **Static IP** as a configuration server protocol from the Configuration Server Protocol selections.



Step 4 Assign the IP address

Use the values in the table to configure the bridge and PC for each team.

Team	bridge Name	bridge Address	PC1 Address	PC2 Address
1	Pod1	10.0.1.1/24	10.0.1.10/24	10.0.1.12/24
2	Pod2	10.0.2.1/24	10.0.2.10/24	10.0.2.12/24

a. Type the IP address in the **IP Address** field.

b. Enter an IP subnet mask in the **IP Subnet Mask** field.

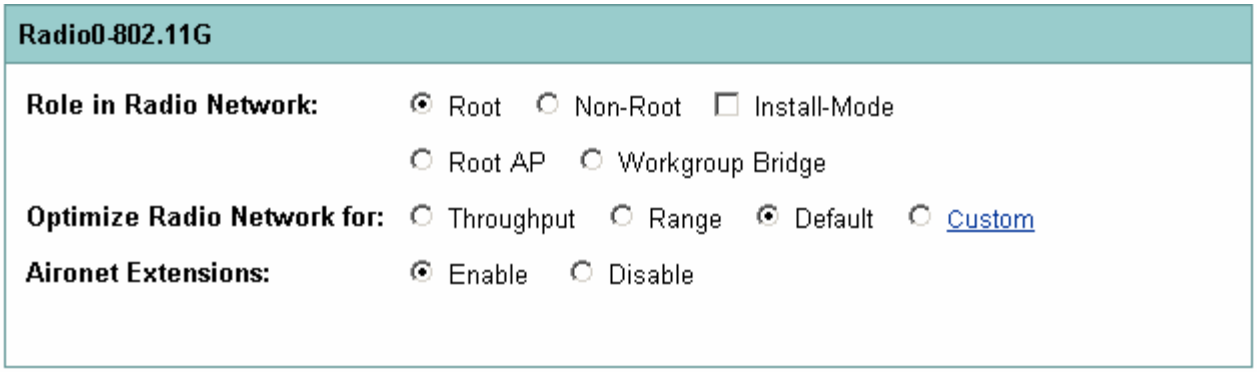
c. Enter the IP address of the default Internet gateway in the **Default Gateway** field. Assume the router address is 10.0.P.254.

d. Leave the **SNMP Community** field at the default value.

e. Set **Role in Radio Network** to Root.

f. Select Throughput for the **Optimize Radio Network** setting. **Note:** This setting will prevent association with 802.11b clients.

g. Click **Apply**.



Once the settings are applied the web connection to the bridge will be lost, since the PC and the bridge are no longer in the same IP subnet.

a. Reconfigure the IP address, subnet mask and gateway on PC1

1. IP address 10.0.P.10
2. Subnet Mask 255.255.255.0
3. Gateway 10.0.P.254

b. Reconnect to the bridge from PC1 web browser and verify the bridge settings from the Express Setup page.

Step 5 Configure SSID

After you assign basic settings to your bridge, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the bridge can communicate beyond the physical boundaries of your worksite. Just as you used the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them.

a. Select the **Express Security** link from the left navigation bar to open the **Express Security Set-Up** page.

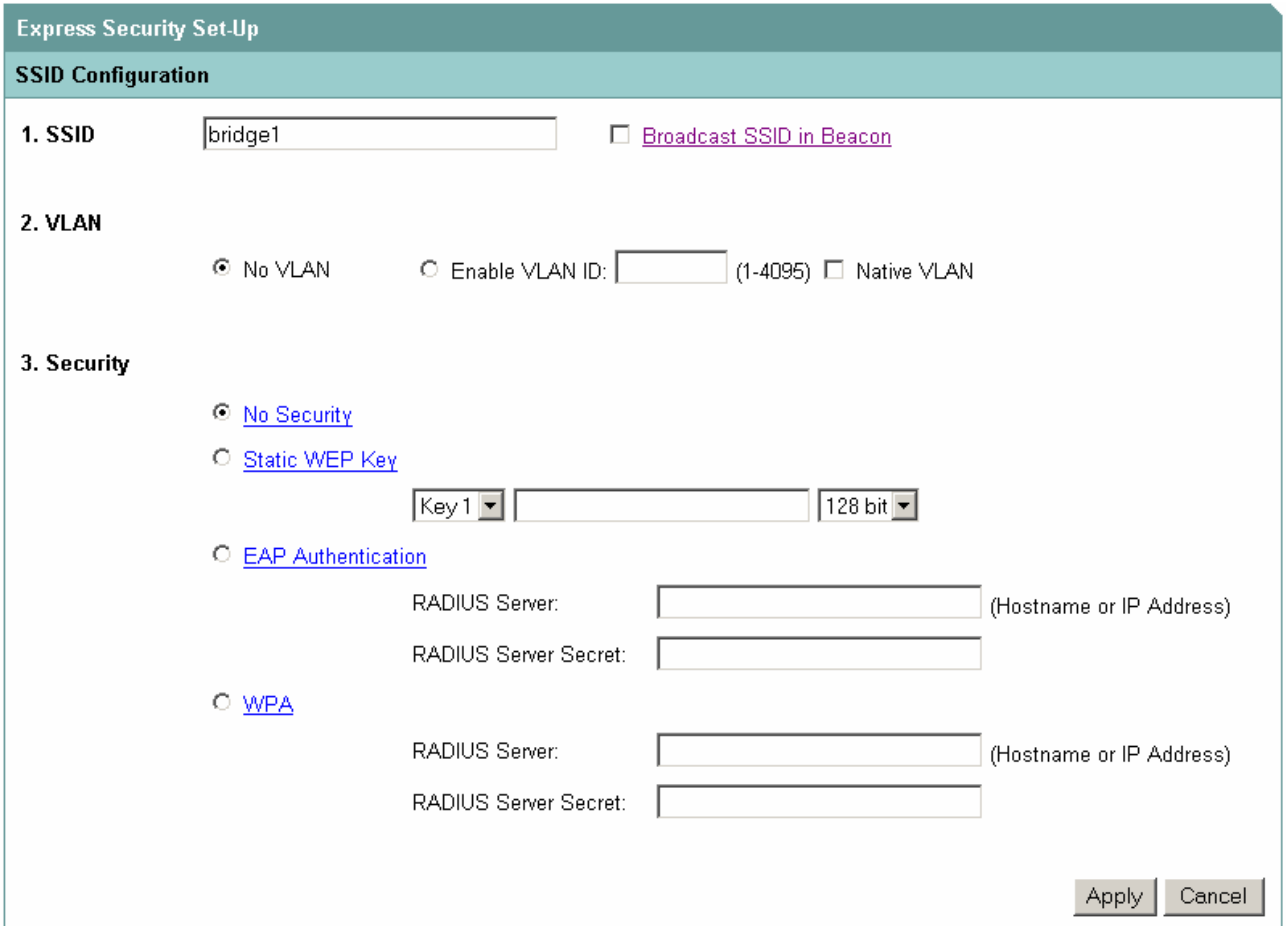
b. In the **SSID** field type the SSID for your pod:

I. Pod 1 SSID: bridge1

II. Pod 2 SSID: bridge2

c. Leave the VLAN and Security settings at their default values. This allows for open authentication.

d. Click **Apply** to save the settings.



Step 6 Connect to the bridge by way of a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct bridge. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the bridge. Make sure the SSID is configured in the profile to match the bridge.

b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members

c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. Configure the wireless adapter with the static IP setting: 10.0.P.12/24.

Step 7 Verify the wireless connection

If the SSID on the bridge and client match, the client should be able to associate with the bridge. The association status can be checked on both the bridge and the PC.

a. From the bridge, navigate to the **Association** page to view all associated devices.

b. Does the wireless PC Client Name appear which was previously configured?

c. Record the MAC Addresses of the devices associated to this bridge. One of these should be the MAC Address of the laptop or desktop configured earlier.

MAC ADDRESS

d. Now check to see if the ACU icon in the system tray is green, which indicates a successful association. Double click on the icon to verify the correct **bridge Name** and **bridge IP Address.**

e. Now check to see if a connection to the bridge using a web browser can be achieved from the wireless device. Enter http://10.0.P.1 for the URL within the browser. Did the bridge GUI display?

f. Test connectivity to other devices by way of ping, Telnet, http, and ftp. This will vary depending on the devices connected and configured on the wired network.

Step 8 Access the bridge through IOS CLI

a. Open the HyperTerminal window on PC1. PC1 should still be connected through the console cable.

b. Enter privileged mode with the following command. ***Cisco*** is the default password.

```
PodP>enable
Password:
PodP#
```

c. Turn off notification logging to avoid interruptions as you enter commands.

```
PodP#configure terminal
PodP(config)#logging console 4
```

Step 9 Erase the configuration through CLI

a. Erase the configuration with the following commands:

```
PodP#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]      (press Enter)
[OK]
Erase of nvram: complete
PodP# reload

System configuration has been modified. Save? [yes/no]:  N
Proceed with reload? [confirm]    (press Enter)
```

Step 10 Configure Hostname

The system name, while not an essential setting, helps identify the bridge on your network. The system name appears in the titles of the management system pages.

a. Enter into configuration mode

```
bridge>enable
Password:Cisco
bridge#
bridge#configure terminal
bridge(config)#
```

b. Turn off notification logging to avoid interruptions as you enter commands.

```
PodP(config)#logging console 4
```

c. Configure the host name with the following command:

```
bridge(config)#hostname PodP  (where P is the pod number)
Pod1(config)#
```

Step 11 Configure the Bridge Virtual Interface (BVI)

When you connect the bridge to the wired LAN, the bridge links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the Ethernet and radio ports, the network uses the BVI.

a. Assign an IP address and address mask to the BVI.

```
PodP(config)#interface bvi1
PodP(config-if)#ip address 10.0.P.1 255.255.255.0
```

Step 12 Configure passwords

a. Configure the enable password to *cisco*. Also, configure the secret password to *class*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
PodP(config)#enable password cisco
PodP(config)#enable secret class
```

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels.

b. Set the **configure** command to privilege level 15 and define *cisco* as the password users must enter to use level 15 commands:

```
PodP(config)#privilege exec level 15 configure
PodP(config)#enable password level 15 cisco
```

Step 13 Configure SSID

a. Configure an SSID with open authentication.

```
PodP(config)#interface dot11radio 0
PodP(config-if)#ssid bridgeP        (where P is the pod number)
PodP(config-if-ssid)#authentication open
PodP(config-if-ssid)#end      (or Ctrl-Z)
PodP#
```

Step 14 Check the running configuration and interface status

a. Display the current configuration of the device

```
PodP#show running-config
Building configuration...
Current configuration : 2660 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PodP
[output omitted]
```

b. Display the condition and information of the device interfaces.

```
PodP#show interfaces
```

Step 15 Save and verify the configuration is saved to Flash

a. Save the current configuration of the device into the configuration file.

```
PodP#copy running-config startup-config
```

b. Verify the startup configuration saved in Flash.

```
PodP#show startup-config
```

Step 16 Connect to the bridge using a wireless PC

Using a laptop or desktop with a wireless adapter, connect to the correct bridge. Make sure the wireless device is not connected through the wired network.

a. Configure and select a profile to connect to the bridge. Make sure the SSID is configured in the profile to match the bridge.

b. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members

c. Make sure to check or configure the TCP/IP settings of the laptop or desktop to connect to the proper IP network. Configure the wireless adapter with the static IP setting: 10.0.P.12/24.

d. Now check to see if the ACU icon in the system tray is green, which indicates a successful association. Double click on the ACU icon to verify the correct **bridge Name** and **bridge IP Address.**

Step 17 Verify the Associations

View the current device associations from the bridge CLI. The wireless device configured should appear in the association output.

```
PodP#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [tsunami] :
SSID [bridgeP] :
Others:  (not related to any ssid)
PodP#
```

Step 18 Connect to the bridge remotely through Telnet

Follow these steps to open the IOS CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

a. From PC2, Open a Telnet session to the bridge located at 10.0.P.1

b. If Telnet is not listed in your Accessories menu, select Start > Run, type Telnet in the entry field, and press Enter.

c. At the username and password prompts, enter your administrator username and password. The default username is *Cisco*, and the default password is *Cisco*. The default enable password is also *Cisco*. The enable secret password is class. Usernames and passwords are case-sensitive.

```
C:\>telnet 10.0.P.1
User Access Verification
Username:
Password:
PodP>
```

Lab 6.2.4 Using Features of the Internetworking Operating System (IOS) command line interface (CLI)

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

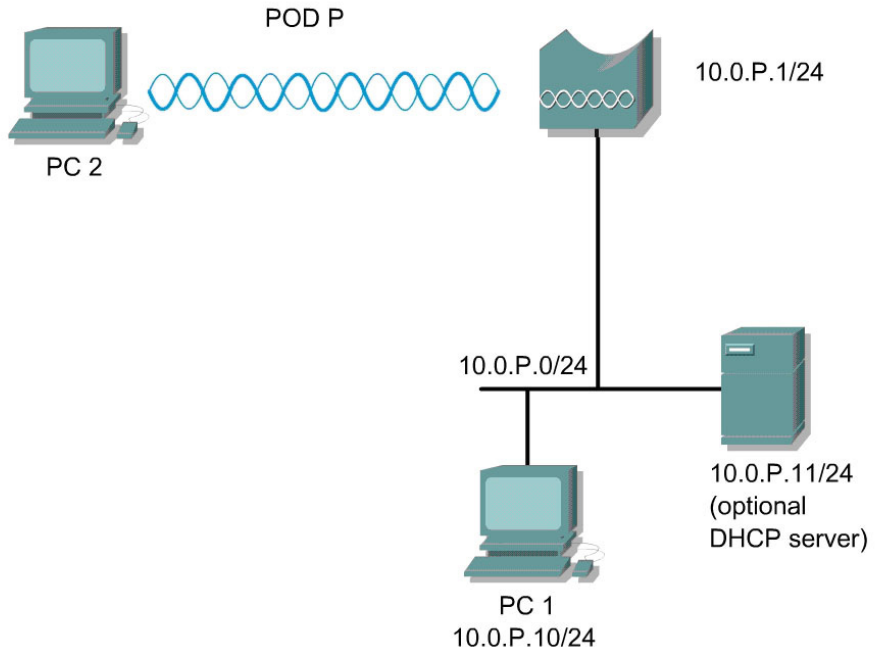
In this lab, the student will learn the following objectives:

- Command Line Interface help features
- Abbreviated commands
- Using the no command to remove config statements
- Command History
- Editing features

Scenario

Students will learn the features of the bridge Internetworking operating system (IOS).

Topology



Preparation

Team	System Name	SSID	Address
1	Pod1	bridge1	10.0.1.1/24
2	Pod2	bridge2	10.0.2.1/24

Tools and Resources

Each team will need:

- The bridge
- The bridge power injector
- A PC or laptop
- Console cable

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
help	Obtains a brief description of the help system in any command mode.
?	Lists all commands available for a particular command mode.
command?	Lists the associated keywords for a command.
command keyword ?	Lists the associated arguments for a keyword.
abbreviated-command-entry?	Obtains a list of commands that begin with a particular character string.
no	Use the no form to disable a feature or function or reverse the action of a command
History size	The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.
terminal history size	The number of commands that are displayed is determined by the setting of the terminal history global configuration command and history line configuration command.
show history	While in privileged EXEC mode, list the last several commands that you just entered.
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Step 1 Connect to the bridge through the console

a. Connecting a Cisco rollover cable (console cable) between PC1 and the bridge

b. Open a terminal emulator.

1. What settings are required?

Bits per second (baud rate):
Data bits:
Parity:
Stop bits:
Flow control:

c. Press return to get started

```
bridge>
```

Step 2 Enter into privileged mode

Enter privileged mode. *Cisco* is the default password. If the password has been changed, reset the bridge to factory defaults. If help is needed refer to a previous lab or Cisco online documentation.

```
bridge>enable
Password:
bridge#
```

Step 3 Erase the existing configuration

If there is an existing configuration on the bridge, erase the configuration and reload.

```
bridge#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm] Y [OK]
Erase of nvram: complete
bridge#
*Mar  1 00:42:37.099: %SYS-7-NV_BLOCK_INIT: Initialized the geometry
of nvram
bridge#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]y
Radio system is preparing for reload...
Radio system is ready for reload.
*Mar  1 00:45:08.446: %SYS-5-RELOAD: Reload requested by console.
```

1. What command is used to check the existing running configuration?

_____

2. What command is used to check the existing startup configuration?

_____

Step 4 Configure the bridge

a. Enter global configuration mode. Configure the hostname, SSID, and passwords. Use the previous lab for configuration help if needed

```
bridge#configure terminal
bridge(config)#
bridge(config)#hostname PodP
PodP(config)#
…
```

b. Configure the remaining steps

c. Configure a wireless PC or laptop to connect the bridge.

d. From PC2 Telnet to the bridge to complete the remaining lab.

Step 5 Using the `help` feature of the bridge

The bridge IOS includes help features. Typing the word `help` at the command prompt will give you a brief summary of the help usage features. Display the help usage summary by typing the command **`help`** at the prompt:

```
PodP#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

PodP#
```

Step 6 Display the available commands of the command mode

To display a list of available commands of the command mode, type the ? character at the command line prompt:

```
PodP#?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
```



```
  dot11             IEEE 802.11 commands
  enable            Turn on privileged commands
  erase             Erase a filesystem
[output omitted]
```

To get help on a specific command, type the command name followed by the ? at the command prompt.

Type **configure ?** at the command prompt to display the available options for the configure command:

```
PodP#configure ?
  memory              Configure from NV memory
  network             Configure from a TFTP network host
  overwrite-network   Overwrite NV memory from TFTP network host
  terminal            Configure from the terminal
  <cr>

PodP#configure
```

Step 7 Abbreviated commands

The IOS supports the use of abbreviated commands. Type in a partial command at the command prompt and then press the tab button. Pressing the tab button will complete the partial command. Type in show conf rather than show configuration. Press the tab button and it will complete the partial command:

```
PodP#show conf   (press the tab button)
PodP#show configuration
Using 2660 out of 32768 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname bridge
!
[output omitted]
```

The Navigation keystrokes below help display the output as needed:

Key	Action
Return	Scroll down one line.
Space	Scroll down one screen.
any other key	Exit the output

Step 8 Command history

The IOS provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

Changing the Command History Buffer Size

By default, the bridge records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to set the number of command lines that the bridge records during the current terminal session:

```
PodP# terminal history size 10
```

(The range is from 0 to 256)

Beginning in line configuration mode, enter this command to configure the number of command lines the bridge records for all sessions on a particular line, the example below configures the number of lines to 10:

```
PodP(config)#line console 0
PodP(config-line)# history size 10
```

(The range is from 0 to 256)

Step 9 Using `no` Forms of Commands to remove configuration statements

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the **shutdown** of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

You will perform a **no** command in Step 10 below.

Step 10 Enabling and disabling editing features

This section describes the editing features that can help you manipulate the command line. Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
PodP#terminal editing
PodP#
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
PodP(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
PodP(config-line)# no editing
```

Step 11 Editing commands through keystrokes

Use the keystrokes listed below to practice editing command lines. Perform each keystroke starting at the top of the list.

Keystroke1	Purpose
Ctrl-B or the left arrow key	Move the cursor back one character.
Ctrl-F or the right arrow key	Move the cursor forward one character.
Ctrl-A	Move the cursor to the beginning of the command line.
Ctrl-E	Move the cursor to the end of the command line.
Esc B	Move the cursor back one word.
Esc F	Move the cursor forward one word.
Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Delete or Backspace	Erase the character to the left of the cursor.
Ctrl-P (or up arrow)	View the previous command in the command history buffer
Ctrl-N (or down arrow)	View the next command in the command history buffer

Lab 6.3.2 Configure Radio Interface through the IOS CLI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

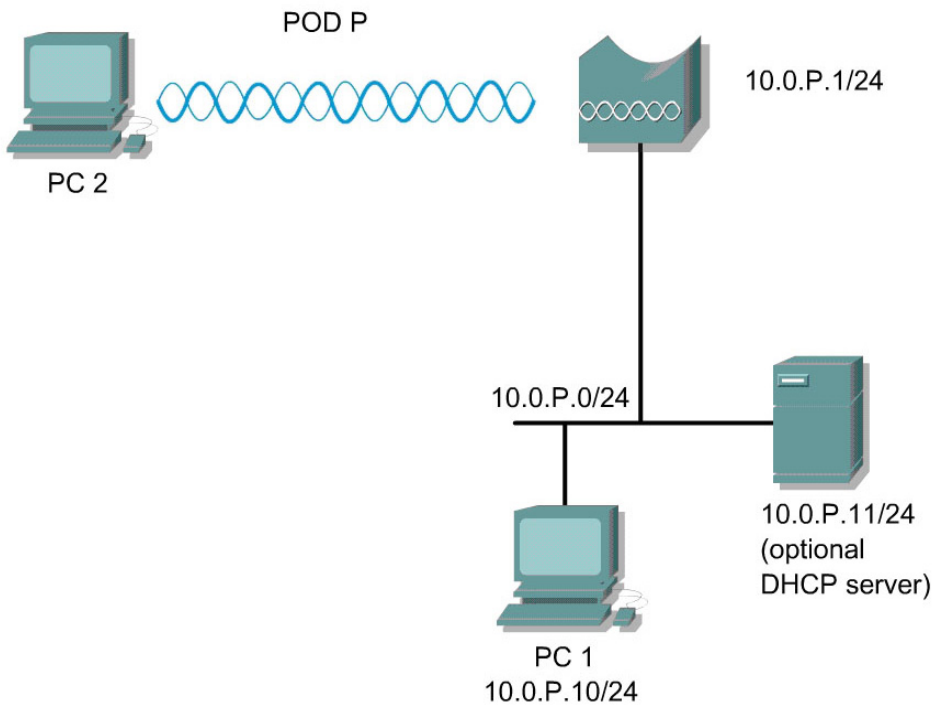
Objective

In this lab, the student will enter basic channel and data rate information for the bridge radio.

Scenario

This section describes how to configure the bridge radio. Use the bridge Radio interface pages in the management system will be used to set the radio configuration.

Topology



Preparation

Configure a PC and bridge according to the Topology

Tools and Resources

- One bridge
- PCs with properly installed Cisco wireless client adapters and utility.
- Several PCs on the wired network that can maintain connectivity to the configuration management pages on the bridge.

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
configure terminal	enter global configuration mode
interface dot11radio *number*	enter the device radio interface. The *number* is 0 for 11g.
station-role	set the role of the bridge device
speed basic	set the data rate of the bridge
power client	set the power level output of the bridge
channel	set the channel of the bridge
world-mode	set world-mode on the bridge
preamble	set the preamble
antenna	set the receive or transmit antenna

Step 1 Connect to the bridge

Connect to the bridge using the console or telnet.

Enter global configuration mode with the following command:

```
PodP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PodP(config)#
```

Step 2 View the available 802.11g radio settings

The bridge radio has many available settings.

Use the following commands to view the available commands for the 802.11g radio:

```
PodP(config)#interface dot11radio 0
PodP(config-if)#?
Interface configuration commands:
  access-expression       Build a bridge boolean access expression
  antenna                 dot11 radio antenna setting
  arp                     Set arp type (arpa, probe, snap) or timeout
  bandwidth               Set bandwidth informational parameter
  bridge-group            Transparent bridging interface parameters
  carrier-delay           Specify delay for interface transitions
  cca                     Clear channel assessment threshold
  cdp                     CDP interface subcommands
  concatenation           dot11 packet concatenation
  countermeasure          countermeasure

[output omitted]
```


Note that there are many other commands available.

Step 3 Configuring the role in radio network

The bridge can be configured in a number of station roles to reflect how it is connected to the wired network or the type of clients it is designed to support.

View the available station roles. Then configure the bridge as a root bridge:

```
PodP(config-if)#station-role ?
  install           Install Mode for Antenna Alignment
  non-root          Bridge non-root
  root              Bridge root
  workgroup-bridge  Workgroup Bridge
PodP(config-if)#station-role root
```

Step 4 Configuring radio data rates

To use the data rate settings to choose the data rates the bridge uses for data transmission. The rates are expressed in megabits per second.

View the available speeds.

```
PodP(config-if)#speed ?
  1.0          Allow 1 Mb/s rate
  11.0         Allow 11 Mb/s rate
  12.0         Allow 12 Mb/s rate
  18.0         Allow 18 Mb/s rate
  2.0          Allow 2 Mb/s rate
  24.0         Allow 24 Mb/s rate
  36.0         Allow 36 Mb/s rate
  48.0         Allow 48 Mb/s rate
  5.5          Allow 5.5 Mb/s rate
  54.0         Allow 54 Mb/s rate
  6.0          Allow 6 Mb/s rate
  9.0          Allow 9 Mb/s rate
  basic-1.0    Require 1 Mb/s rate
  basic-11.0   Require 11 Mb/s rate
  basic-12.0   Require 12 Mb/s rate
  basic-18.0   Require 18 Mb/s rate
  basic-2.0    Require 2 Mb/s rate
  basic-24.0   Require 24 Mb/s rate
  basic-36.0   Require 36 Mb/s rate
  basic-48.0   Require 48 Mb/s rate
  basic-5.5    Require 5.5 Mb/s rate
  basic-54.0   Require 54 Mb/s rate
  basic-6.0    Require 6 Mb/s rate
  basic-9.0    Require 9 Mb/s rate
  default      Set default rates
  range        Set rates for best range
  throughput   Set rates for best throughput
  <cr>
PodP(config-if)#
```

Use the following commands to set up the bridge for 54-Mbps service only:

```
PodP(config-if)#speed basic-54.0
PodP(config-if)#
```

Step 5 Configuring radio transmit power

The power level on client devices that associate to the bridge and the bridge radio power can be manually set. Set the transmit power for the 802.11g radio to one of the power levels allowed in your regulatory domain. All settings are in mW.

Use the help to view the power settings which can be configured.

```
PodP(config-if)#power ?
  client  Client radio transmitter power level
  local   Local radio transmitter power level
PodP(config-if)#
```

See which power levels are configurable on the bridge.

```
PodP(config-if)#power local ?
  cck   Set local power for CCK rates
  ofdm  Set local power for OFDM rates
PodP(config-if)#
```

You can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices.

Note The settings allowed in your regulatory domain might differ from the settings listed here.

Configure the bridge radio power to 5mW.

```
PodP(config-if)#power local cck 5
PodP(config-if)#
```

Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.

When a client device associates to the bridge, the bridge sends the maximum power level setting to the client. Follow these steps to specify a maximum allowed power setting on all client devices that associate to the bridge, the example below sets the radio transmit power to 100mW:

```
PodP(config-if)#power client 100
PodP(config-if)#
```

Now lower the setting to 5mw:

```
PodP(config-if)#power client 5
PodP(config-if)#
```

Step 6 Configuring radio channel settings

The default channel setting for the bridge radios is least congested. At startup, the bridge scans for and selects the least congested channel. For the most consistent performance after a site survey, it is recommended that a static channel setting for each bridge be assigned. The channel settings on your bridge correspond to the frequencies available in your regulatory domain. Only a bridge running in root mode will allow configuration of a static channel.

See what channels are available

```
PodP(config-if)#channel ?
<1-2462>         One of: 1 2 3 4 5 6 7 8 9 10 11 2412 2417 2422 2427
2432 2437 2442 2447 2452 2457 2462
  least-congested  Scan for best frequency
PodP(config-if)#
```


Follow the steps below to assign a static channel setting for the bridge. The example below sets the radio to channel 1:

```
PodP(config-if)#channel 1    (or the channel frequency)
PodP(config-if)#
```

Now assign a least congested channel setting for the bridge. The example below sets the radio to the least congested channel setting:

```
PodP(config-if)#channel least-congested
PodP(config-if)#
```

Step 7 Enabling and disabling world-mode

When **world-mode** is enabled, the bridge adds channel carrier set information to its beacon. Client devices with **world-mode** enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on **world-mode** to adjust its channel and power settings automatically when it travels to Italy and joins a network there. World mode is disabled by default.

To view **world-mode** options on the bridge, use the help feature.

```
PodP(config-if)#world-mode ?
  dot11d  802.11d World Mode advertise country
  legacy  Legacy World Mode advertize country
PodP(config-if)#
```

When you enter the dot11d option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website. After the country code, you must enter indoor, outdoor, or both to indicate the placement of the bridge. Enter the legacy option to enable Cisco legacy world mode.

To enable legacy **world-mode** on the bridge, follow the steps below:

```
PodP(config-if)#world-mode legacy
PodP(config-if)#
```

Step 8 Disabling and enabling short radio preambles

The radio preamble (sometimes called a *header*) is a section of data at the head of a packet that contains information that the bridge and client devices need when sending and receiving packets. The radio preamble can be set to long or short, and is set to short by default.

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.
- Long—A long preamble ensures compatibility between the bridge and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your bridges, you should use short preambles.

Follow these steps to disable short radio preambles:

```
PodP(config-if)#no preamble-short
PodP(config-if)#
```

Follow these steps to enable short radio preambles:

```
PodP(config-if)#preamble-short
PodP(config-if)#
```


Step 9 Configuring transmit and receive antennas

The bridge can be set to select the antenna the bridge uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- Diversity—This default setting tells the bridge to use the antenna that receives the best signal. If your bridge has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- Right—If your bridge has removable antennas and you install a high-gain antenna on the bridge's right connector, you should use this setting for both receive and transmit. When you look at the bridge's back panel, the right antenna is on the right.
- Left—If your bridge has removable antennas and you install a high-gain antenna on the bridge's left connector, you should use this setting for both receive and transmit. When you look at the bridge's back panel, the left antenna is on the left.

View the available antenna settings

```
PodP(config-if)#antenna ?
  gain      Configure Resultant Antenna Gain
  receive   receive antenna setting
  transmit  transmit antenna setting
```

View the available receive options:

```
PodP(config-if)#antenna receive?
  diversity  antenna diversity
  left       antenna left
  right      antenna right
```

Follow these steps to set the bridge receive and transmit to right: (the interfaces will reset after each change.)

```
PodP(config-if)#antenna receive right
PodP(config-if)#antenna transmit right
PodP(config-if)#
```

Follow these steps to set the bridge receive and transmit to left:

```
PodP(config-if)#antenna receive left
PodP(config-if)#antenna transmit left
PodP(config-if)#
```

Follow these steps to set the bridge back to receive and transmit to diversity:

```
PodP(config-if)#antenna receive diversity
PodP(config-if)#antenna transmit diversity
PodP(config-if)#
```

Step 10 Disable the radio

If the PC is connected through wireless, it is important to switch to a console connection.

Use the shutdown command to turn off the radio. Afterwards, re-enable the interface.

```
PodP(config-if)#shutdown
*Mar  1 02:27:18.082: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to administratively down
*Mar  1 02:27:18.082: %LINK-5-CHANGED: Interface Virtual-
Dot11Radio0, changed state to administratively down
*Mar  1 02:27:19.083: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio0, changed state to down
PodP(config-if)#
PodP(config-if)#no shutdown
```

```
*Mar  1 02:28:00.414: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 02:28:00.414: %LINK-3-UPDOWN: Interface Virtual-Dot11Radio0,
changed state to down
*Mar  1 02:28:00.433: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
*Mar  1 02:28:01.432: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Dot11Radio 0, changed state to up
```

Lab 6.3.5 Configure Ethernet/FastEthernet Interface

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two.

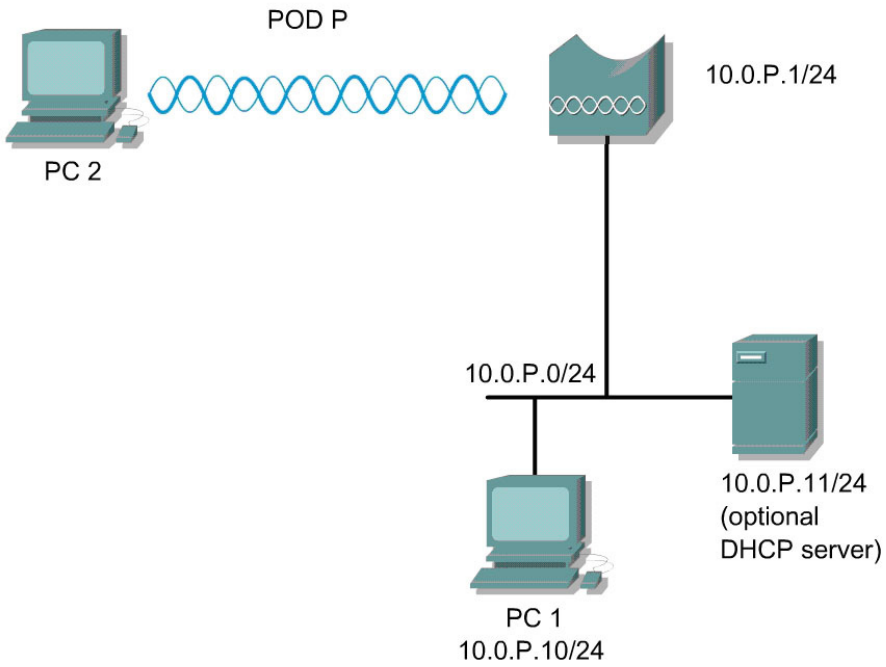
Objective

In this lab, the student will use the bridge setting pages to enter speed and duplex information for the bridge Ethernet interface.

Scenario

This section describes how to configure the bridge radio Ethernet and FastEthernet interfaces to lock in speed and duplex settings.

Topology



Preparation

Below are the basic settings to be applied to the bridge.

Team	bridge Name	SSID	Address
1	Pod1	bridge1	10.0.1.1/24
2	Pod2	bridge2	10.0.2.1/24

Tools and Resources

- Cisco 1310 bridge
- Bridge power injector
- PCs with properly installed Cisco wireless client adapters and utility.
- PCs on the wired network that can maintain connectivity to the configuration management pages on the bridge.

Step 1 Configuring the bridge IP Address

In order to access the web interface of the bridge for configuration, the IP address of the bridge BVI must be known. The default IP address for the bridge is 10.0.0.1/27. If this IP address has been changed from previous configurations, it will be necessary to connect to the bridge via a console cable to configure the bridge with a known IP address.

a. If needed, console into the bridge and configure the BVI IP address to 10.0.P.1/24. Set the hostname as well according to the Preparation table. Configure the wired PC with the correct TCP/IP settings as indicated by the lab Topology. A wireless connection to the bridge can also be used if the bridge configuration is known.

   1. Record the configuration commands below needed for Step1a.

      _____

      _____

      _____

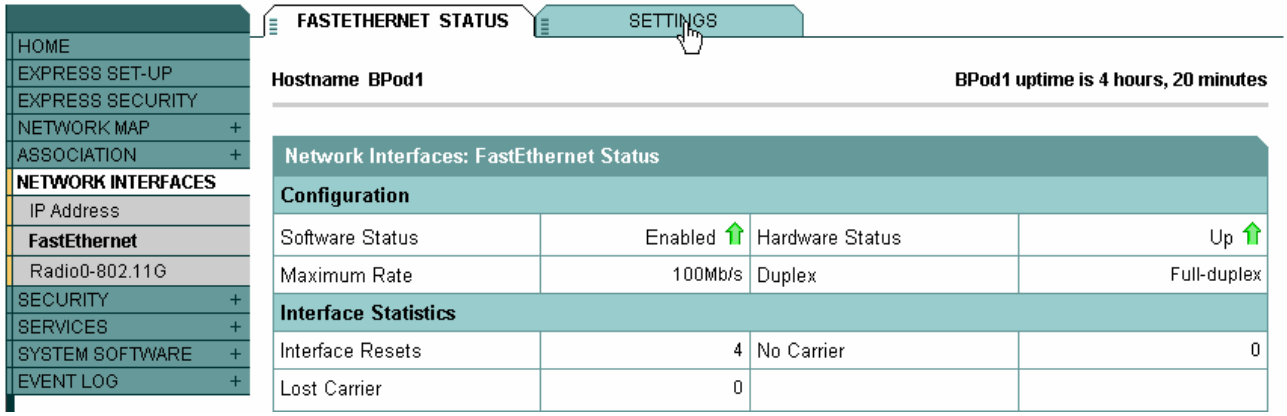
      _____

      _____

b. After the hostname and BVI interface have been configured, navigate to the bridge web interface using the wired or wireless PC. The default username is *Cisco*. The default password is also *Cisco*. Both username and password are case sensitive.

Step 2 Configure data rate speed and Duplex of the FastEthernet interface

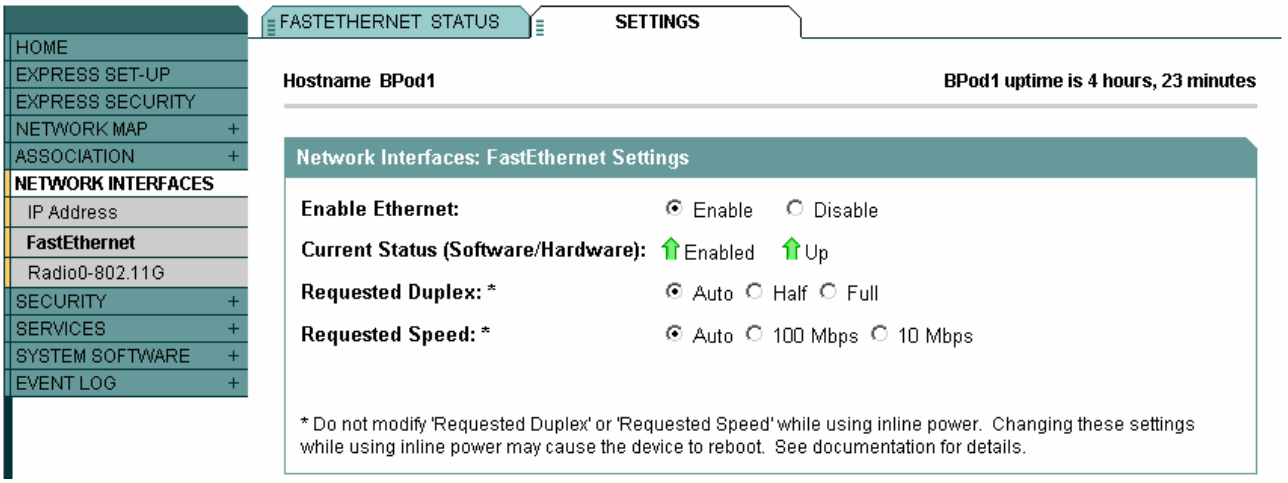
a. Go to the **NETWORK INTERFACES>FastEthernet** Page and click on the settings tab of the bridge.



b. The **Enable Ethernet:** setting should be set to **Enable**.

Note	If the FastEthernet settings are modified while connected through the wired network, the connection may be lost. These will actually be modified in Step 4 through the Console. The Requested Duplex Setting should be set to **Auto** by default.

c. The Requested Speed and Duplex settings should be set to **Auto** by default**.** In a production environment, the speed should be locked into the optimum setting of the connected switch.



Step 4 Configure Ethernet/FastEthernet Interfaces through IOS CLI

Parameters can be configured via the CLI if the web interface is inaccessible or if HTTP access has been disabled for security reasons.

Console into the bridge. Beginning in configuration mode. Follow these steps to set the bridge Ethernet/FastEthernet settings.

a. Enter interface configuration mode:

```
PodP(config)#interface fastEthernet 0
```


b. Now see what duplex settings are possible.

```
PodP(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
```

c. Set the duplex to full

```
PodP(config-if)#duplex full
```

d. View possible speed settings:

```
PodP(config-if)# speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

e. Configure the speed to 100 Mbps.

```
PodP(config-if)#speed 100
PodP(config-if)#end
```

f. Check the running configuration.

```
PodP#show running-config
```

g. Display the FastEthernet interface status

```
PodP#show interfaces fastEthernet 0
FastEthernet0 is up, line protocol is up
  Hardware is PowerPC405GP Ethernet, address is 000b.46b8.ca90 (bia 000b.46b8.ca90)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:23:18, output 00:01:54, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1783 packets input, 164809 bytes
     Received 29 broadcasts, 0 runts, 0 giants, 0 throttles
```



```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
1141 packets output, 449852 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

h. Quickly verify all the interfaces are up

```
PodP#show ip interface brief
PodP#show ip interface brief
Interface                  IP-Address      OK? Method Status
   Protocol
BVI1                       10.0.P.1        YES other  up             up
Dot11Radio0                unassigned      YES TFTP   up             up
Dot11Radio1                unassigned      YES TFTP   up             up
FastEthernet0              unassigned      YES other  up             up
Virtual-Dot11Radio0        unassigned      YES TFTP   down
   down
Virtual-Dot11Radio1        unassigned      YES TFTP   down
   down
PodP#
```

i. Now check the detailed status of all the interfaces

```
PodP#show interfaces
```


Lab 6.3.6.1 Configure Site-to-Site Wireless Link

Estimated Time: 60 minutes

Number of Team Members: Students will work in teams of two

Objective

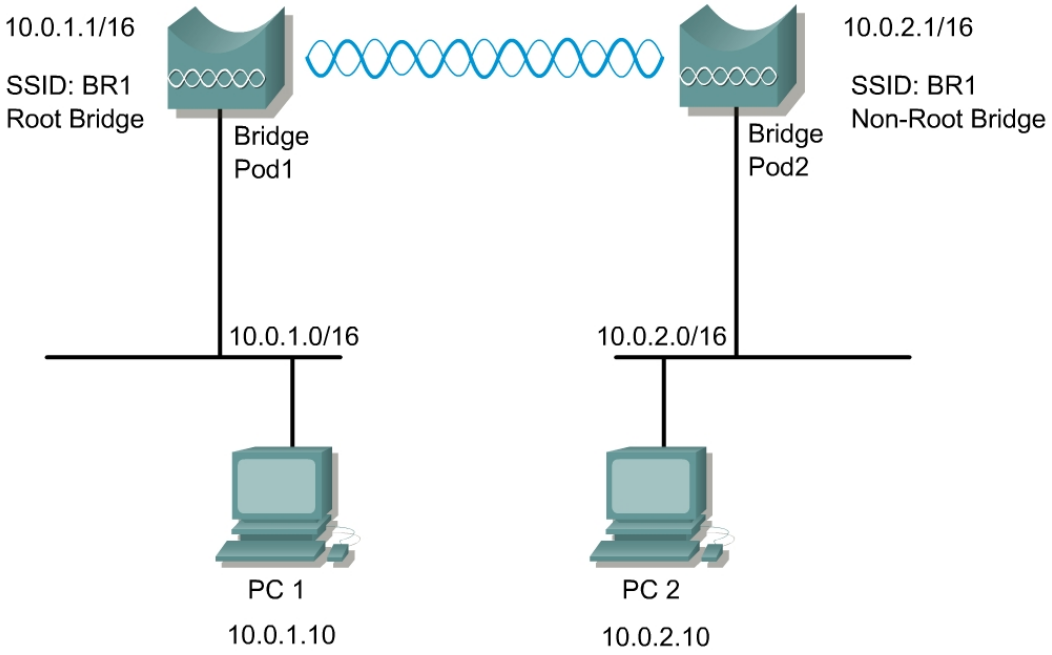
Configure a site-to-site bridged network.

Scenario

A remote location several miles away requires connectivity to the existing wired network. The two LAN segments will use a wireless bridge for their physical layer connection using two Cisco Aironet Bridges (BR350s).

Note This lab uses a different subnet mask to identify the two segments of the same network. These two segments, although separated by distance, remain part of the same LAN through the use of a Wireless physical layer link.

Topology



Preparation

In this lab, the following will be configured.

Device Name	Label	SSID	Address
BPod1	BR1	BR1	10.0.1.1/16
BPod2	BR2	BR1	10.0.2.1/16

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco BR350
- PC with FTP server loaded and a file to transfer in the root directory of the FTP server

Note This lab uses a FTP client/server functionality. Download an evaluation version or freeware/shareware version to accomplish this lab. Use a search engine using the keywords 'ftp server downloads' as a start.

Step 1 Cable and power the bridge

a. First, attach two rubber duck antennas to the RP-TNC connectors.

b. Plug the RJ-45 Ethernet cable into the Ethernet port on the back of the bridge. Plug the other end of the Ethernet cable into the Cisco Aironet power injector TO AP/BRIDGE end.

c. Connect the power cable into the inline power injector and to the receptacle.

Step 2 Connect to the bridge

Connect a nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the bridge. (This cable ships with the bridge)

a. Open a terminal emulator.

b. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: Xon/Xoff

c. Press = to display the home page of the bridge. If the bridge has not been configured before, the Express Setup page appears as the home page. If this is the case, go to Step 3.

d. If the bridge is already configured, the Summary Status page appears as the home page. When Summary Status screen appears, type :**resetall**, and press **Enter**.

```
Enter "YES" to confirm Resetting All parameters to factory defaults:
YES
00:02:12 (FATAL): Rebooting System due to Resetting Factory Defaults
*** Restarting System in 5 seconds...
```

e. Type **yes**, and press **Enter** to confirm the command.

f. Power cycle the bridge by removing the power.

Note **:resetall** can only be issued within the first 2 minutes after power on.

Step 3 Connect to the BR350 using Express Setup

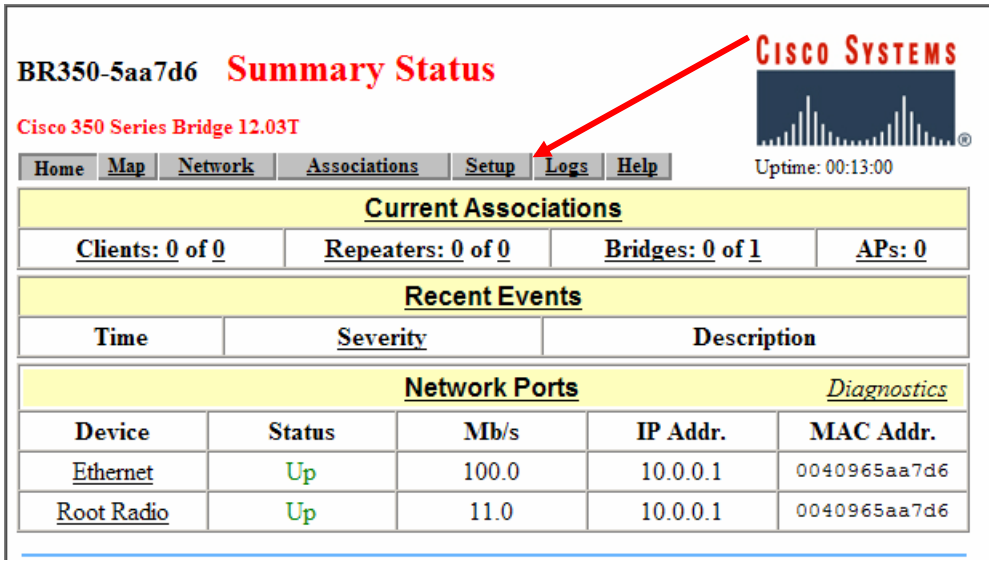
a. Plug a second RJ-45 Ethernet cable into the power injector end labeled TO NETWORK. Plug the other end of the Ethernet cable into the Ethernet port on a switch or hub. Then connect PC1 to the switch. A crossover cable can be used to connect directly from the inline power injector to PC1/PC2.

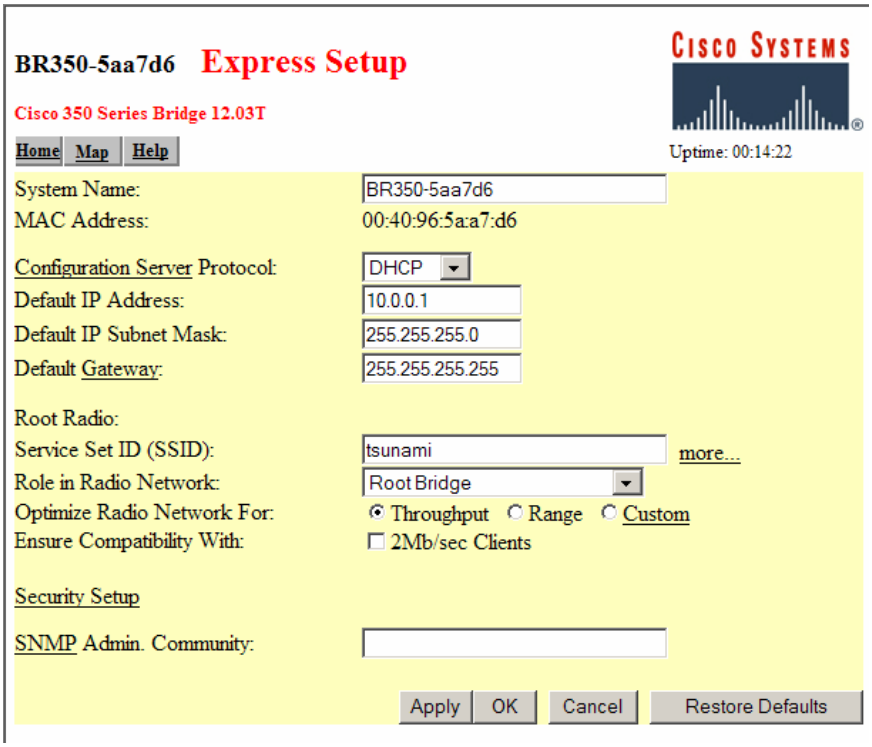
b. Configure PC1 to 10.0.0.2/24

c. Open a web browser, type the default bridge address http://10.0.0.1, and press Enter.

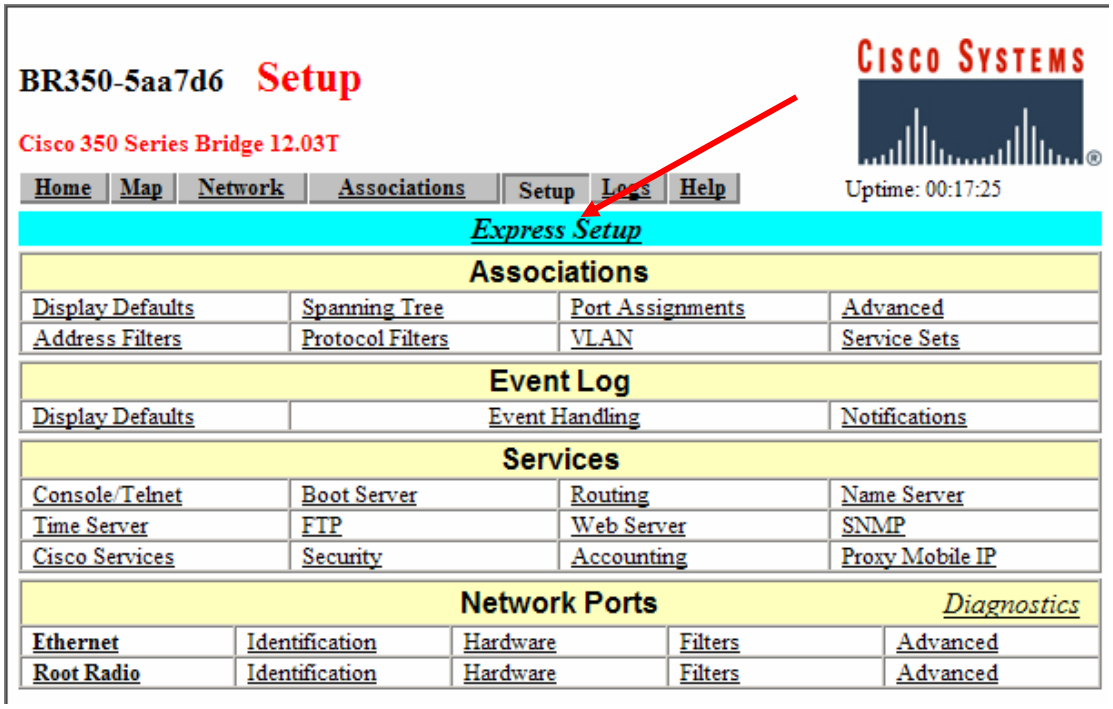
d. Either of the following pages will appear:

1. The **Summary Status** Page, also known as the **Home** Page
2. The **Express Setup** Page



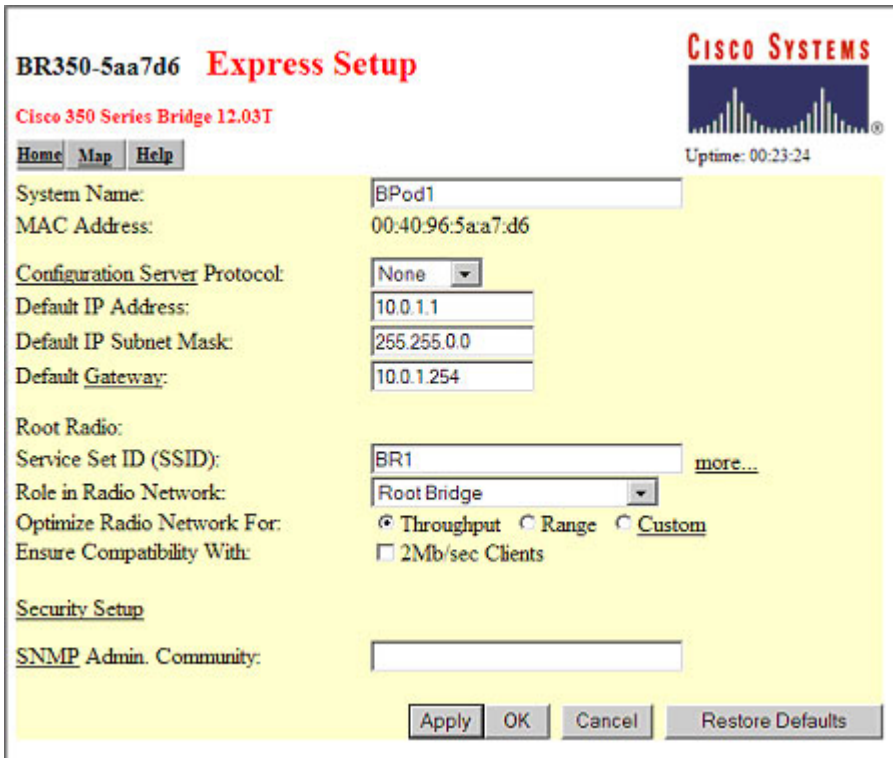


e. If the Express Setup Page does not appear, from the Summary Status Page click on the **Setup** hyperlink. This will bring up the Setup Page.



f. Now click on the ***Express Setup*** link. This will now bring up the Express Setup Page.

Step 4 Configure the bridge settings



Configure the following settings:

	Parameter	BPod1	BPod2
a.	System Name:	***BPod1***	***BPod2***
b.	Configuration Server Protocol:	***None***	***None***
c.	Default IP address:	***10.0.1.1***	***10.0.2.1***
d.	Default Gateway:	***10.0.1.254***	***10.0.1.254***
e.	Service Set ID:	***BR1***	***BR1***
f.	Role in Radio Network:	***Root Bridge***	***Non-Root Bridge w/o Clients***

g. Click Apply. The connection will drop.

h. Configure the PCs

- PC1 with an IP address of 10.0.1.10/16
- PC2 with an IP address of 10.0.2.10/16

i. Reconnect to the using the browser. Enter 10.0.P.1 and connect.

j. Verify the settings.

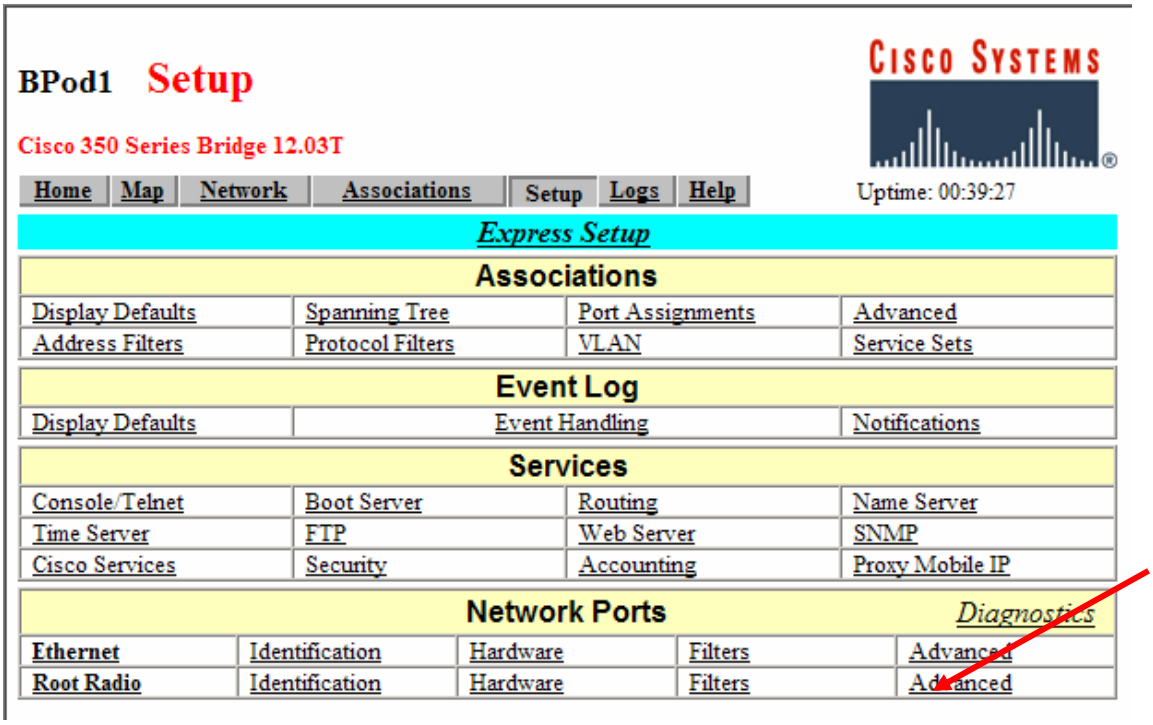
1. What roles can the bridge serve in the network?

_____

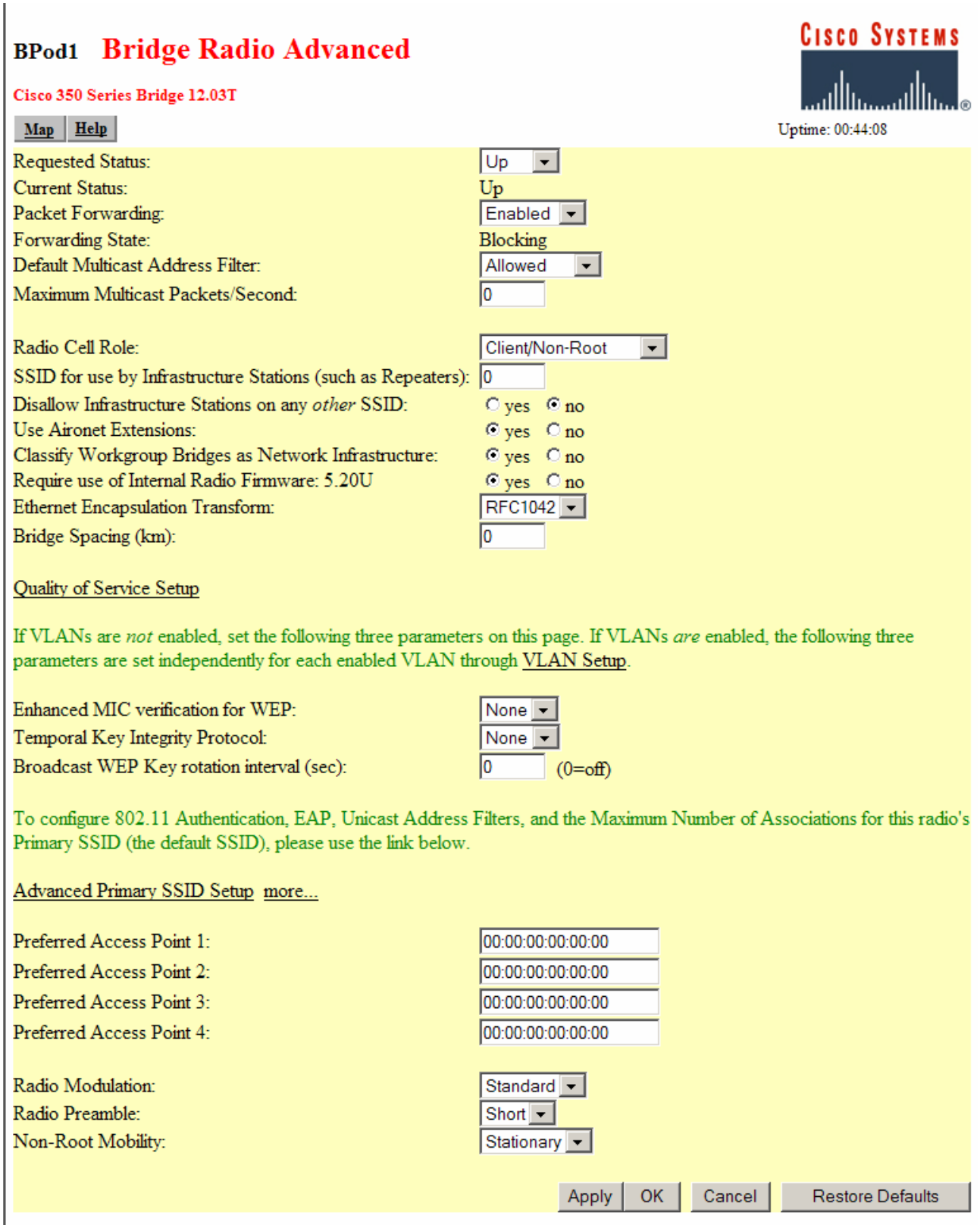
_____

_____

Step 5 Advanced radio settings for the non-root bridge

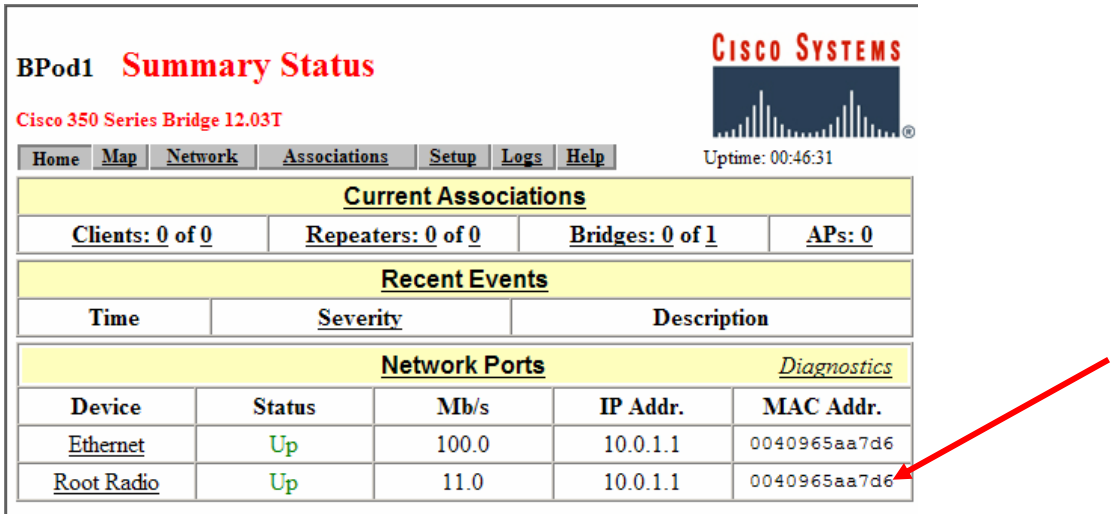


a. From the **Setup** Page, Click on the Root Radio>Advanced link to go to the **Radio Advanced** page of the Non-Root Bridge.

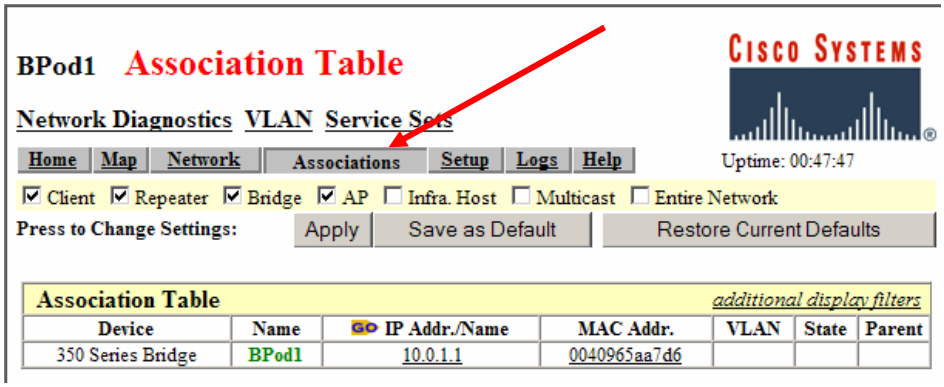


b. Enter the MAC address of the Root Bridge into the **Preferred AP 1:** field.

This can be found on the bottom of the Root Bridge or from the Root Bridge **Home** Page.



c. Click the **Apply** button to apply the settings.



d. Go to the **Associations** page of the Root Bridge. Is the Non-Root Bridge in the Association table?

_____

Step 7 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices on this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, ping from PC1 to BPod2. Then ping from PC1 to PC2.

1. Were these successful?

_____

b. Test layer 7 connectivity by browsing to BPod2 from PC1.

c. Configure FTP or Web services on PC1 and PC2. Transfer a files from PC1 to PC2 and vice versa. Calculate the download performance across the wireless link.

1. What was the download speed in Mbps?

_____

2. How was this calculated?

_____

3. What is the speed limitation?

_____

Lab 6.3.6.2 Configure Site-to-Site Wireless Link

Estimated Time: 60 minutes

Number of Team Members: Students will work in teams of two

Objective

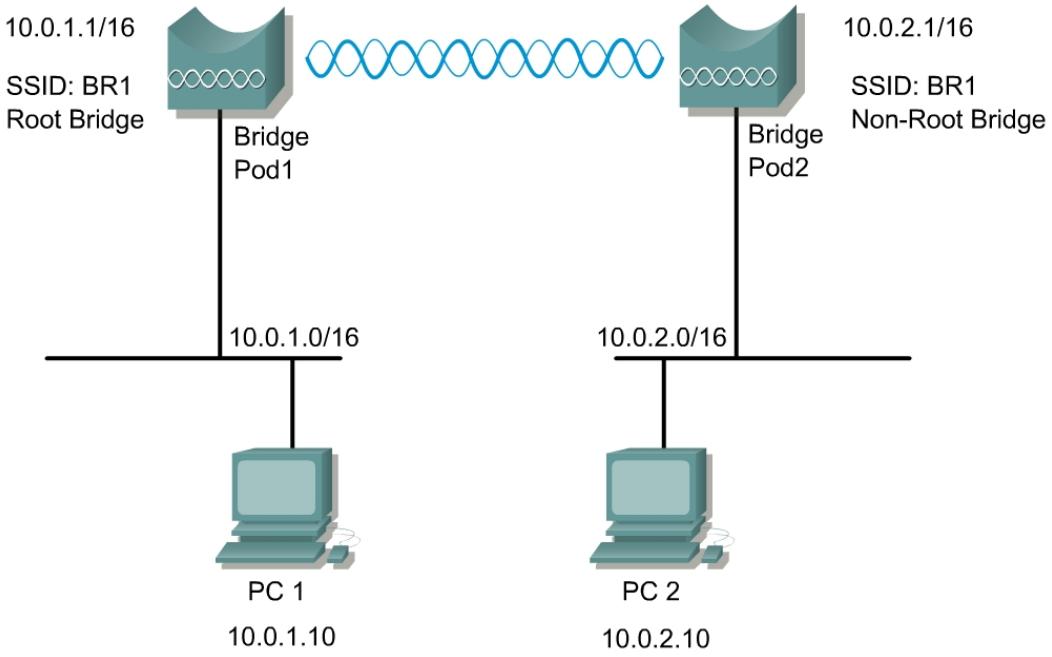
Configure a site-to-site bridged network.

Scenario

A remote location several miles away requires connectivity to the existing wired network. The two LAN segments will use a wireless bridge for their physical layer connection using two Cisco Aironet Bridges (BR1310s).

Note This lab uses a different subnet mask to identify the two segments of the same network. These two segments, although separated by distance, remain part of the same LAN through the use of a Wireless physical layer link.

Topology



Preparation

In this lab, the following will be configured.

Device Name	SSID	Address
BPod1	BR1	10.0.1.1/16
BPod2	BR1	10.0.2.1/16

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together.
- Two Cisco BR1310
- PC with FTP server loaded and a file to transfer in the root directory of the FTP server

Step 1 Cable and power the bridge

a. First, attach two rubber duck antennas to the RP-TNC connectors.

b. Connect the Power Injector to the BR1310 using the RG-59 coax cables.

c. Connect the power cord to the Power Injector.

Step 2 Connect to the bridge CLI

Using a standard console cable, you can connect to the bridge via a terminal emulator application such as HyperTerminal. Follow these steps to open the CLI.

a. Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the power injector and to the COM port on your PC.

b. Open a terminal emulator.

c. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: None

d. When the terminal emulator is activated, press **Enter**. An Enter Network Password window appears. The default username is *Cisco*. The default password is *Cisco*. Both the username and password are case sensitive.

e. Upon a success login, the bridge will display the user mode prompt.

f. Enter the enabled mode by typing the `enable` command and providing the default password: *Cisco*.

```
br>enable
Password:*****
br#
```

g. Reset the bridge to factory defaults by entering the `erase nvram` command and confirming.

```
br#erase nvram
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
```

Step 3 Connect to the BR1310 using Express Setup

a. Connect an RJ-45 Ethernet cable into the power injector Ethernet LAN port. Connect the other end of the Ethernet cable into an Ethernet port on a switch or hub. Then connect PC1 to the switch. (NOTE: A crossover cable can be used to connect directly from the power injector to PC1/PC2.)

b. Configure PC1 to 10.0.0.2/24

c. Open a web browser, type the default bridge address http://10.0.0.1, and press Enter.

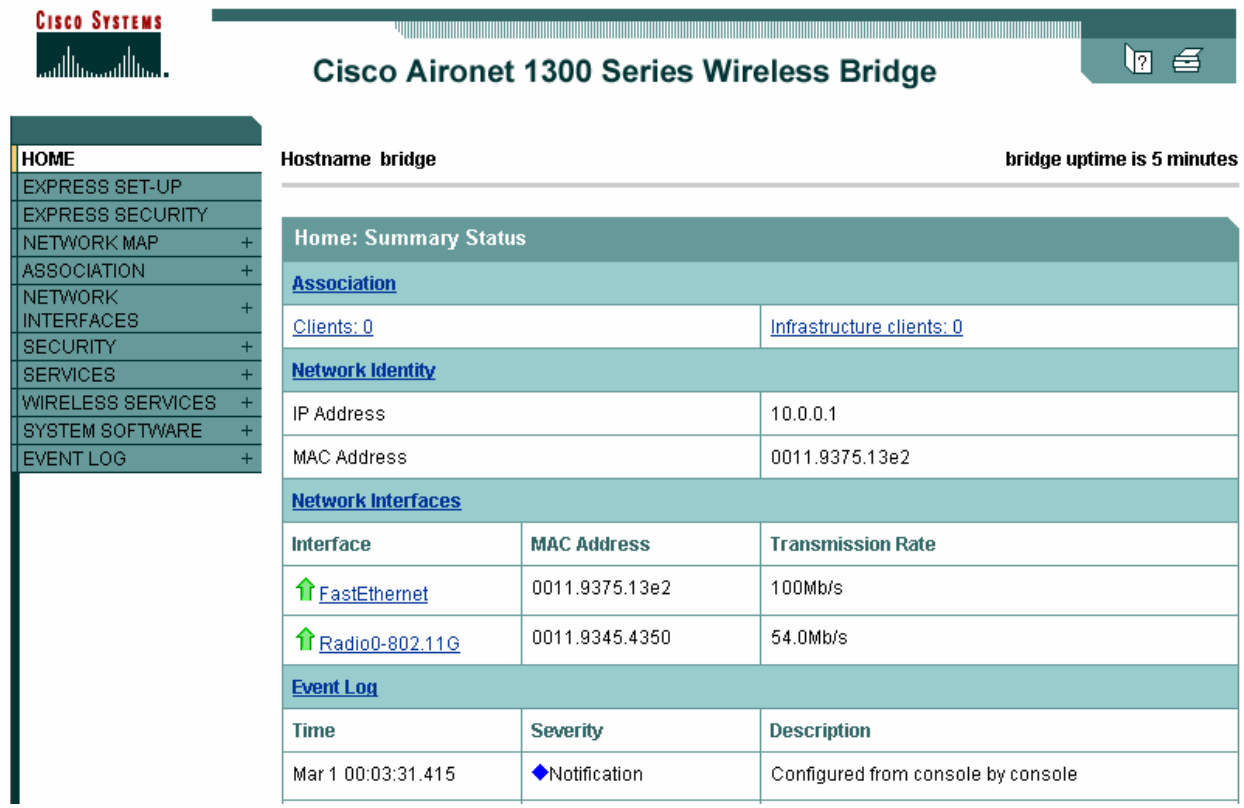
d. When prompted for the username and password, enter the case-sensitive default values:

i. Username: Cisco

ii. Password: Cisco

e. The bridge Home page will open displaying the Summary Status of the bridge.

f. Navigate to the Express setup page by selecting the ***Express Setup*** link from the left navigation bar. The Express Setup page will allow configuration of some basis settings.



Step 4 Configure the bridge settings

Using the Express Setup page, configure the bridge with the appropriate settings as indicated in the table below. Remember to choose the correct parameters for your pod.

Configure the following settings:

	Parameter	BPod1	BPod2
a.	System Name:	***BPod1***	***BPod2***
b.	Configuration Server Protocol:	***Static IP***	***Static IP***
c.	Default IP address:	***10.0.1.1/16***	***10.0.2.1/16***
d.	Default Gateway:	***10.0.1.254***	***10.0.1.254***
e.	Role in Radio Network:	***Root***	***Non-Root***

f. Click Apply. The connection will drop. Reestablish the connection by changing the configuration of the PC to match the bridge.

- PC1 with an IP address of 10.0.**1**.10/16
- PC2 with an IP address of 10.0.**2**.10/16

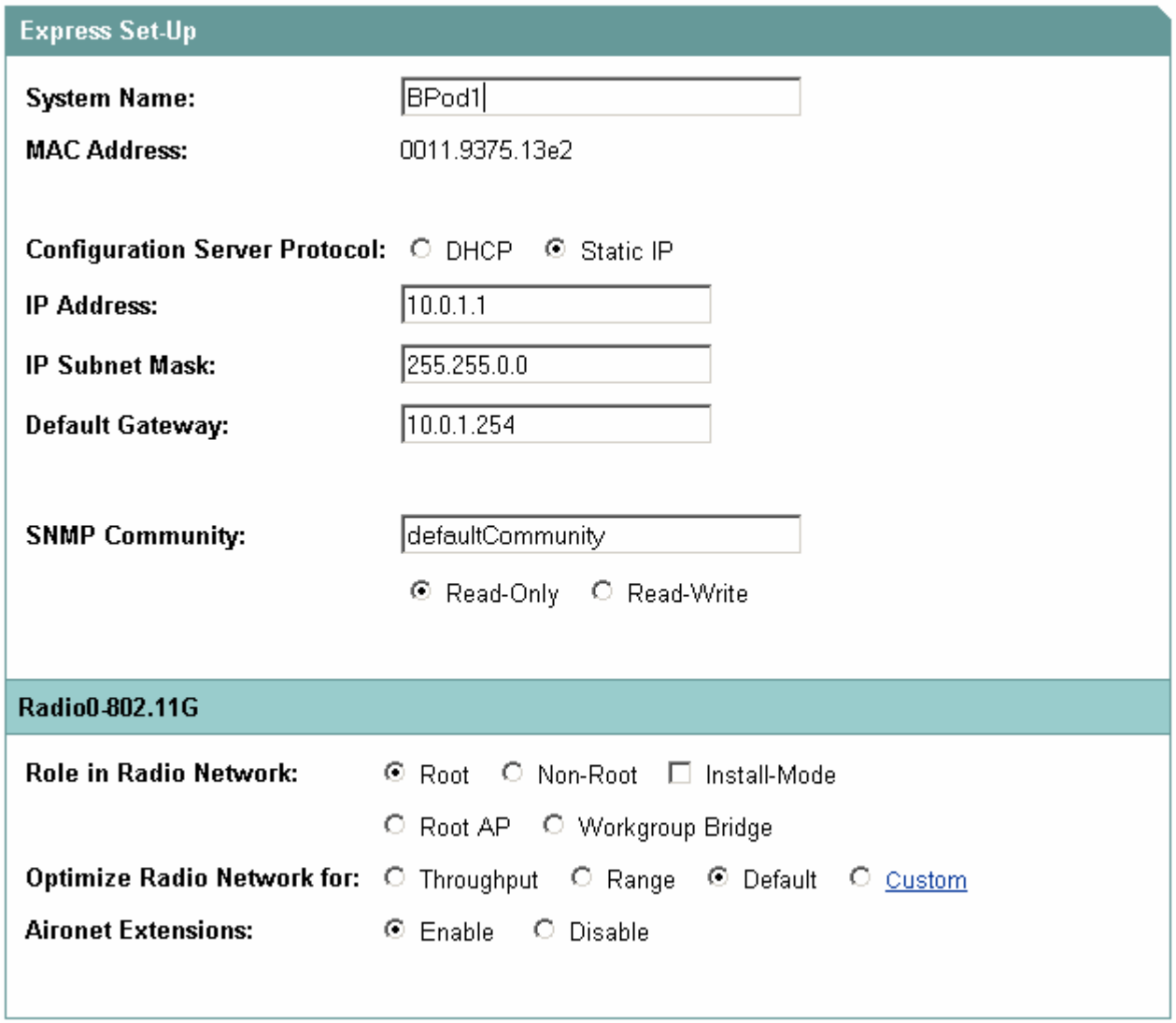
g. Browse to the configured IP address of the bridge.

1. What roles can the bridge serve in the network?

_____

_____

_____



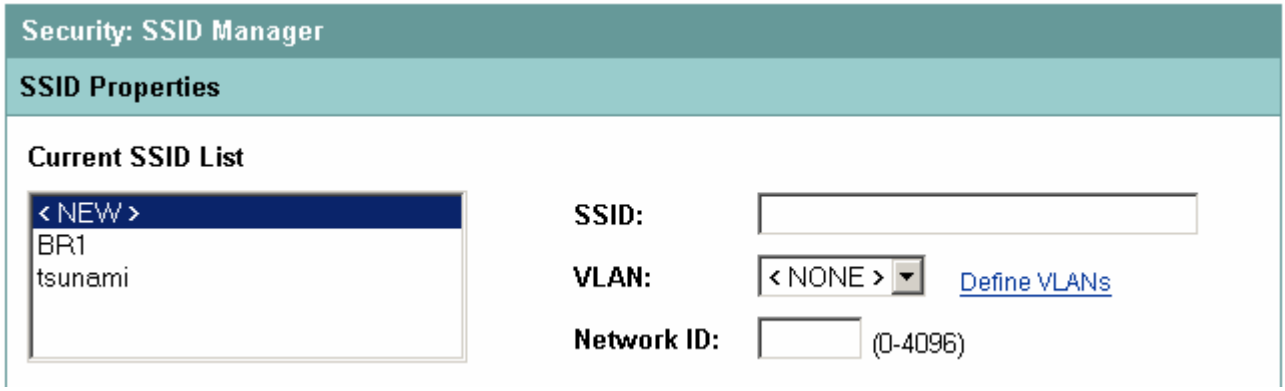
From the left navigation bar, select the Security>SSID Manager link to configure SSIDs on the bridges.

a. From the Current SSID List, make sure that <NEW> is selected. Configure a new SSID for both bridges to the value: **BR1**.

b. Leave all other fields at their default values.

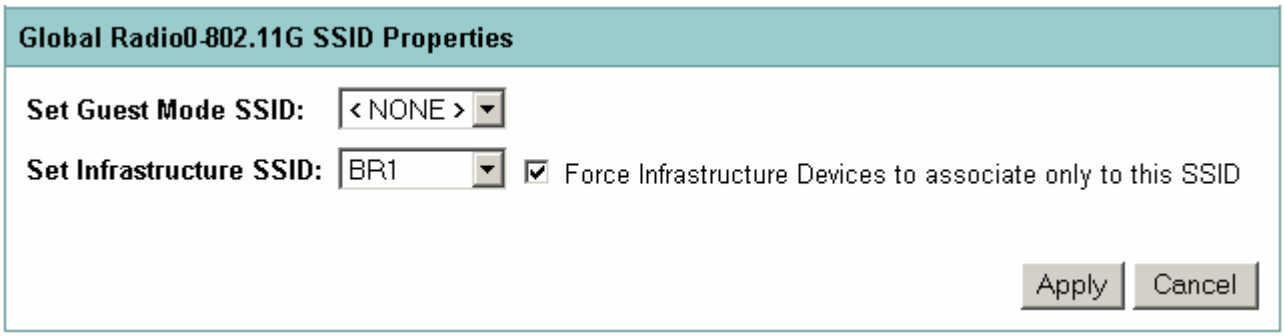
c. Click Apply to save the settings.

d. After the page refreshes, there will be 2 SSIDs in the current list.



e. Scroll to the bottom and select the *BR1* SSID for the Infrastructure SSID, and click the check box to force infrastructure devices to associate using this SSID.

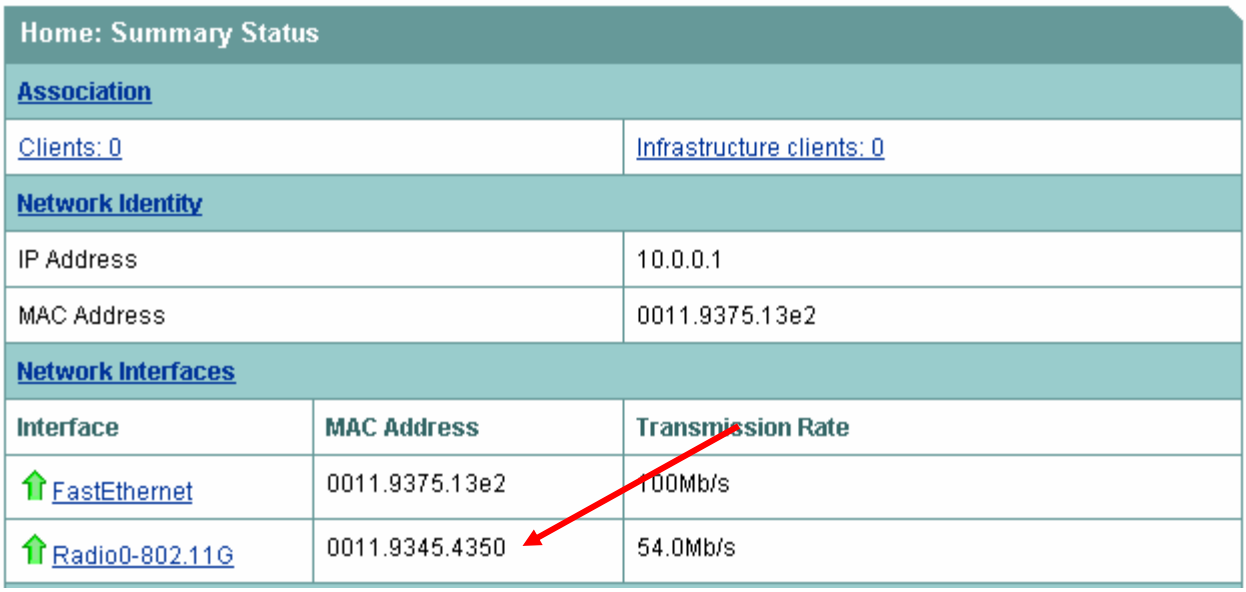
f. Click Apply to save your settings.



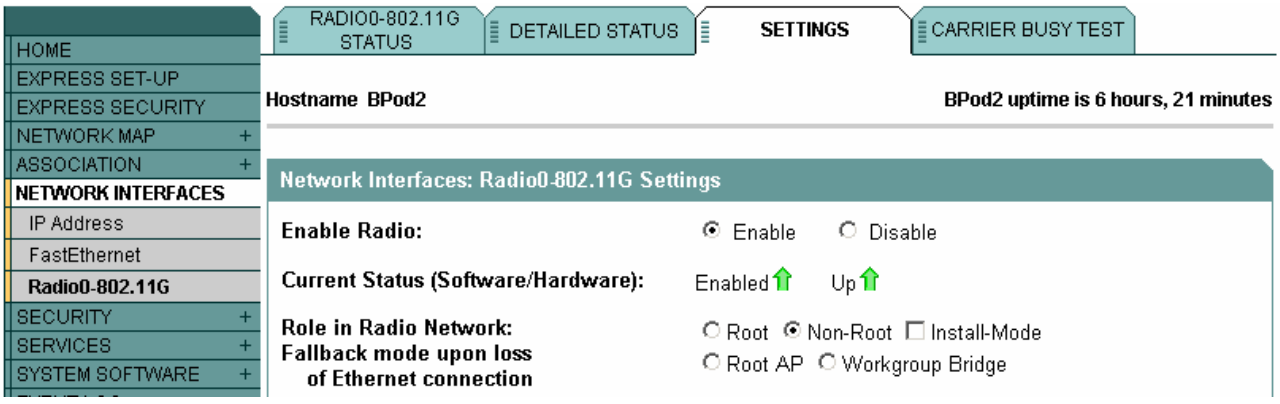
Step 5 Radio settings for the non-root bridge

To ensure that the non-root bridge associates with the correct root bridge, the root parent MAC address can be configured on the non-root bridge.

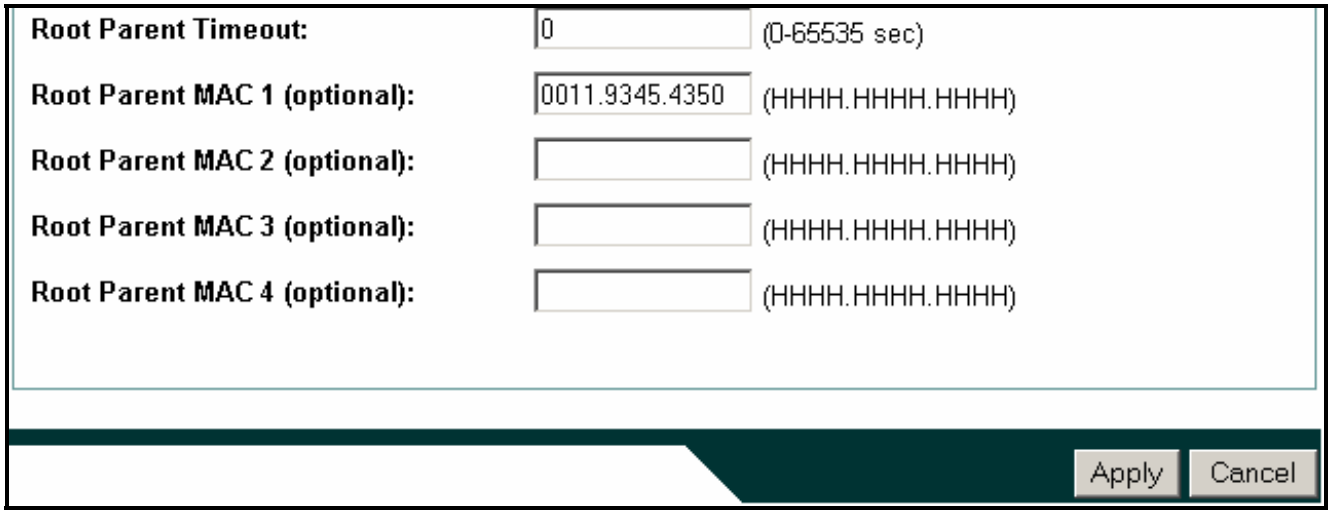
a. Record the MAC address of the root bridge radio. This address can be found on the Summary Status page of the root bridge.



b. From the non-root bridge, navigate to the Settings tab of the Radio interface.



c. Scroll to the bottom of the settings page to enter the root bridge radio MAC address in the Root Parent MAC address field. Click Apply to save the configuration.

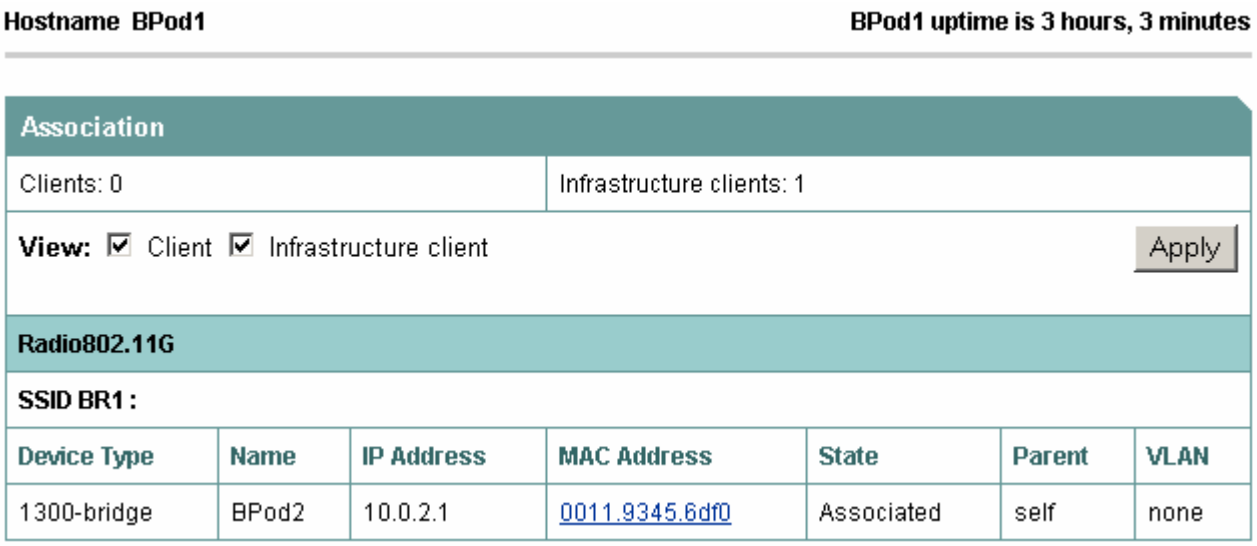


Step 7 View Associations

The non-root bridge should now be associated with the root bridge. To view the current associations on each bridge, open a web connection to the bridge from the wired PC.

a. Navigate to the bridge IP address.

b. Select the **Association** link from the left navigation bar. All associated devices should appear in the list.



1. Which devices are listed in the Association table for BR1? What device is the parent for this association?

_____

2. Which devices are listed in the Association table for BR2? What device is the parent for this association?

_____

Step 8 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices on this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, ping from PC1 to BR2. Then ping from PC1 to PC2. Were these successful?

_____

b. Test layer 7 connectivity by browsing to BR2 from PC1. Was this successful?

_____

Lab 6.4.4.1 Configure Bridge Services

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

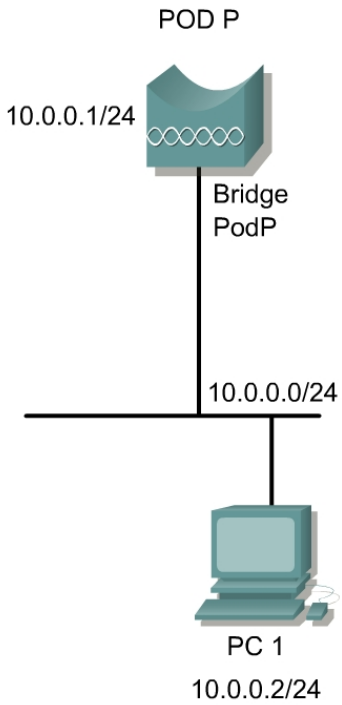
In this lab, students will configure the identity services, IP routing table, console parameters, and the time server parameters of the bridge unit.

Scenario

Configuring services includes the following:

- The Boot Server page determines how the bridge obtains its IP address and assigns required identifiers.
- Configuring the Routing Services page controls how IP packets originating from the bridge are forwarded.
- The Console/Telnet page can set up essential system parameters.
- The Time Server menu page is used to set time parameters.

Topology



Preparation

The students will read and familiarize themselves with the concepts and procedures of Chapter 6 prior to the lab.

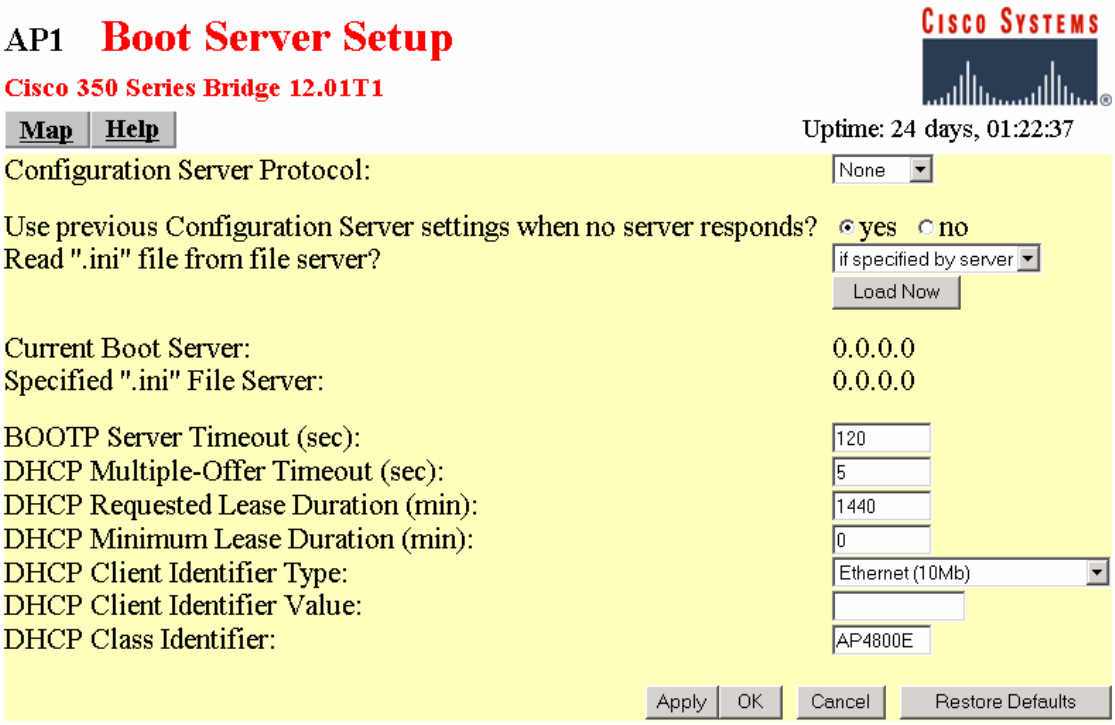
Tools and Resources

Each team will require the following:

- One multi-function wireless bridge properly set up for Web browser access
- One PC to configure each bridge

Step 1 Configuring the identity process of the bridge unit

After connecting to the bridge by way of a web browser, select the **Setup** tab to go to the Setup screen. From the Services section, select **Boot Server**.



Select the Identity process, Configuration Server Protocol that the bridge will use.

There are three options:

- **None** – Disableb BOOTP and DHCP, which is the default setting
- **BOOTP** – Configures BOOTP only
- **DHCP** – Configures DHCP

For Root Units, select **DHCP**.

For non-root units, select **None**.

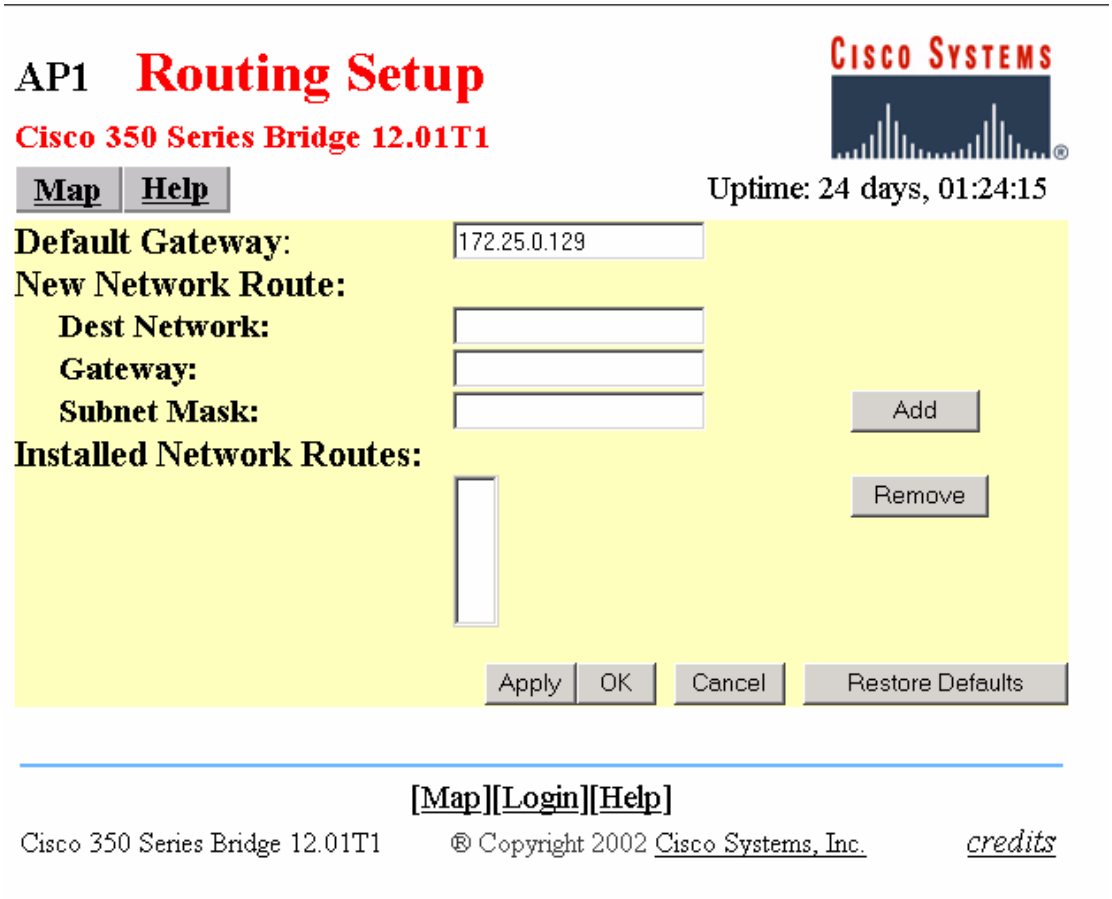
a. What is the BOOTP selection for?

_____

_____

Step 2 Configuring the IP routing table parameters of the bridge unit

From the Setup page in the Services section, select the **Routing** option.



If the destination IP address exactly matches a host entry in the routing table, the packet is forwarded to the MAC address corresponding to the next-hop IP address from the table entry.

If the destination address is on another subnet and matches the infrastructure portion of a net entry in the table (using the associated subnet mask), the packet is forwarded to the MAC address corresponding to the next-hop IP address from the table entry.

In order to configure the IP Routing Table parameters, complete the following steps:

- If DHCP has been used for the identity process, the default gateway router IP Address will be in the default gateway field.
- If a static route is to be added for handling destination addresses, fill in the following fields:

1. Dest. Network:

   _____

2. Gateway:

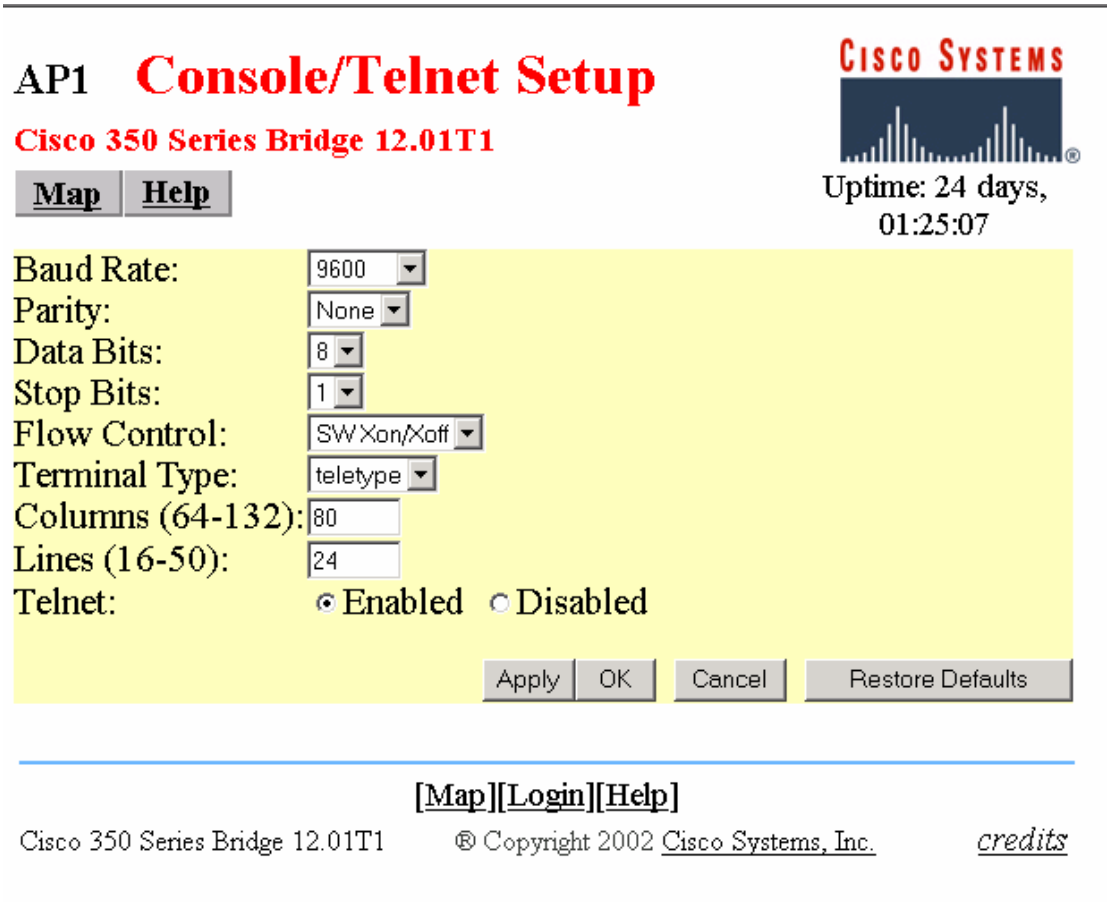
   _____

3. Subnet Mask:

   _____

Step 3 Configuring the console/Telnet parameters of the bridge unit

From the Setup page in the Services section, select the **Console/Telnet** option.



In order to configure the Console/Telnet parameters, complete the following steps:

- Use the Console/Telnet setup page to configure the parameters for HyperTerminal and/or Telnet sessions to the bridge unit.

Document the following settings:

a. Baud Rate

_____

b. Parity

_____

c. Data Bits

_____

d. Stop Bits

_____

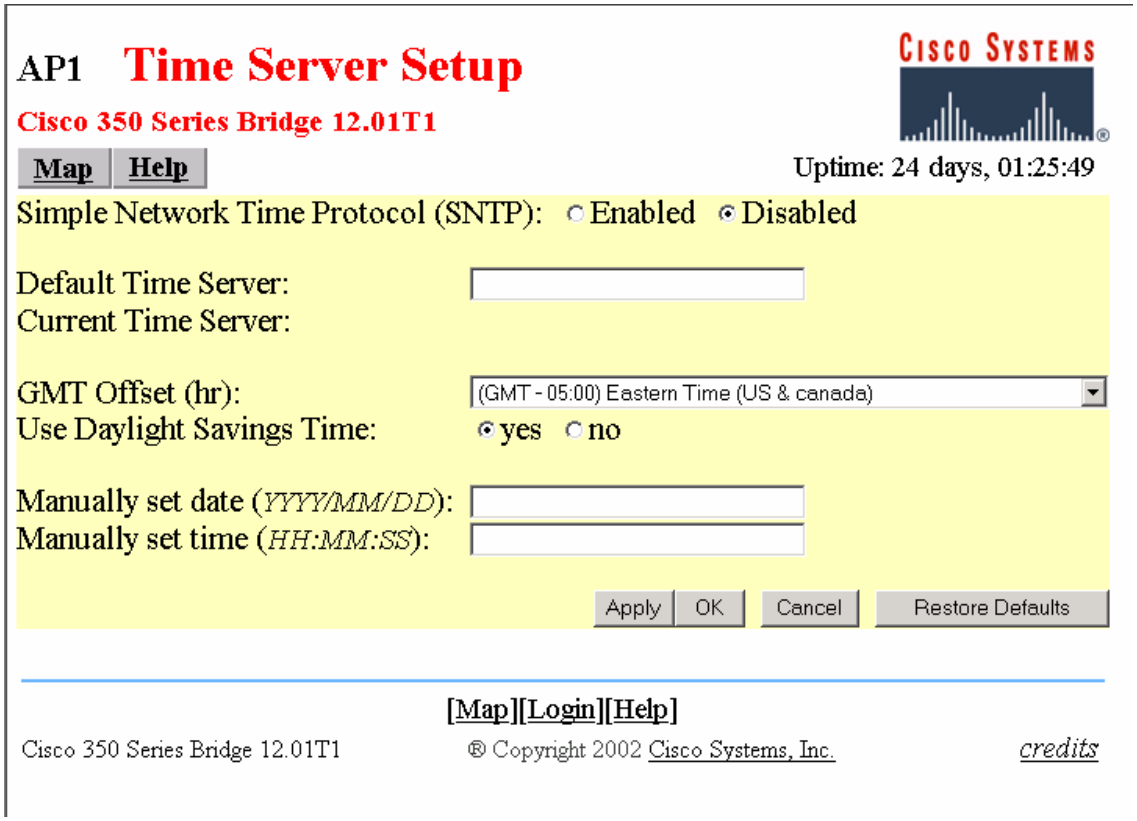
e. Flow Control

_____

- If remote access to the bridge is a concern, the Telnet feature of the bridge unit may be disabled by checking the **Disabled** button on this page.

Step 4 Configuring the time server parameters of the bridge unit to set the time

From the Setup page in the Services section, select the **Time Server** option.



Simple Network Time Protocol (SNTP) is a lightweight version of Network Time Protocol (NTP). NTP is designed for extreme accuracy, while SNTP is designed for easy synchronization. SNTP clients can obtain time form an NTP server. Even though SNTP is simple, it can easily provide accuracy within a few milliseconds.

In order to configure the Time Server parameters of the bridge unit to set the time, complete the following steps:

- Use the Time Server Setup page to change the time settings.
- Change the time to one hour ahead.
  a. When would this step be necessary?

  _____
- Change the time back to the current time.

Lab 6.4.4.2 Configure Bridge Services

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

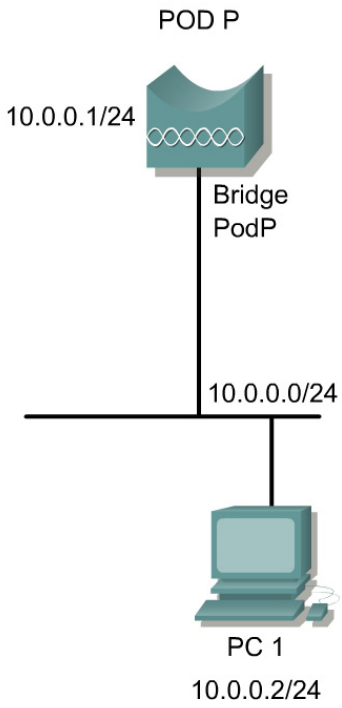
Objective

In this lab, students will configure various services on the BR1310.

Scenario

The bridge Services configuration page is used to set parameters for various services, including: Telnet/SSH, CDP, DNS, Filters, HTTP, Proxy Mobile IP, QoS, SNMP, NTP, VLAN, STP, and ARP Caching.

Topology



Preparation

The students will read and familiarize themselves with the concepts and procedures of Chapter 6 prior to the lab.

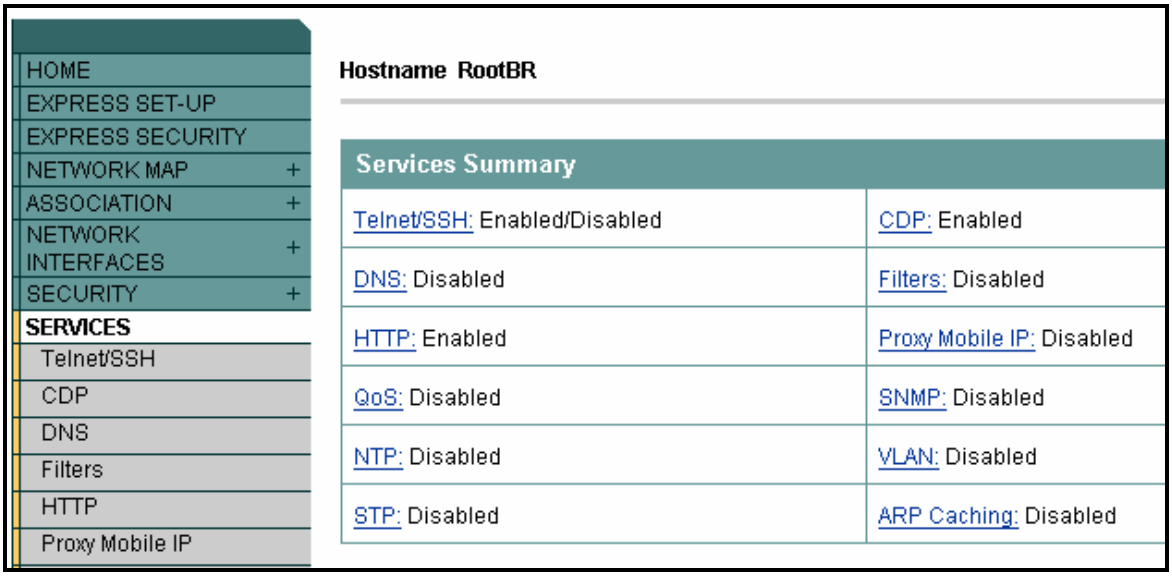
Tools and Resources

Each team will require the following:

- One multi-function wireless bridge properly set up for Web browser access
- One PC to configure each bridge

Step 1 Viewing default values

Each of the Services available on the bridge has a default value. These defaults can be viewed from the Services Summary page.



Step 2 Configuring the console/Telnet parameters of the bridge unit

From the Setup page in the Services section, select the **Telnet/SSH** link. Record the current settings.

Document the following settings:

a. Terminal Type:

_____

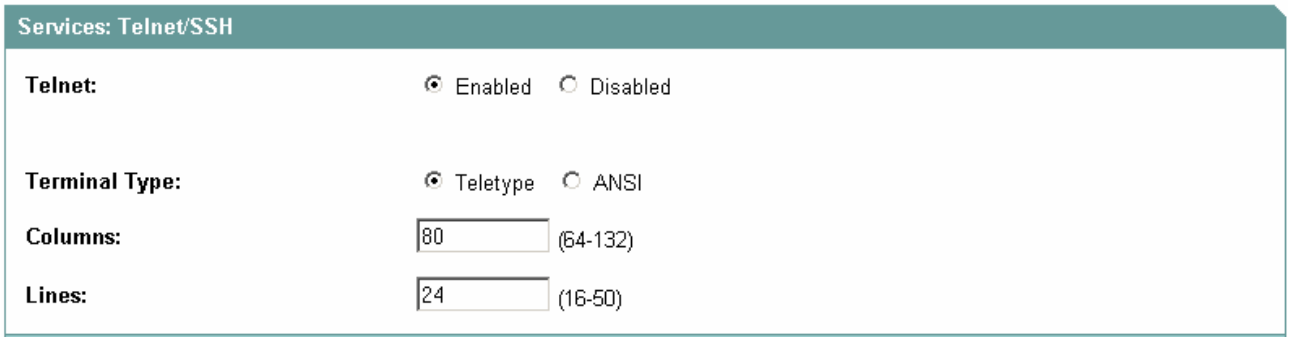
b. Columns:

_____

c. Lines:

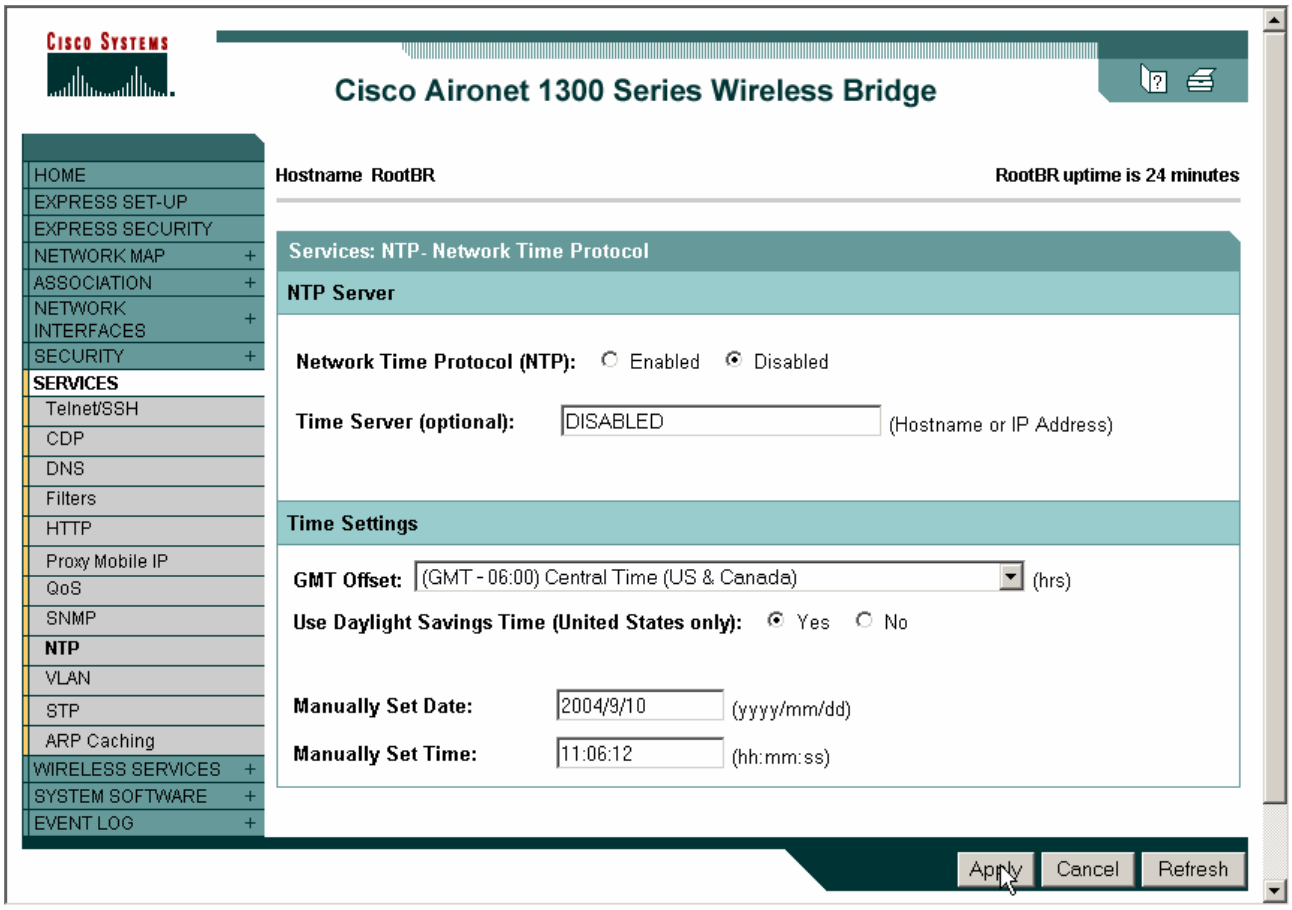
_____

If remote access to the bridge is a concern, the Telnet feature of the bridge unit may be disabled by checking the **Disabled** button on this page.



Step 3 Configuring the time server parameters of the bridge unit to set the time

From the Setup page in the Services section, select the **NTP** option.



NTP is designed for extreme accuracy and requires configuration of a Hostname or IP address of an NTP server. Time Settings can be manually entered if an NTP server is not available.

In order to configure time parameters of the bridge, complete the following steps:

a. Select the GMT Offset for your time zone from the drop down list.

b. Select the daylight savings setting appropriate for your area.

c. Manually set the date and time following the format provided in parenthesis.

d. Click **Apply** to save these settings.

e. The time settings can be confirmed by causing a log entry to be entered. From the **Express Set-up** page, change the bridge System Name and apply the new settings.

f. Navigate to the Home page after the new name is saved. The **Event Log** should have an entry with the correct GMT date and time.

Event Log

Time	Severity	Description
Sep 13 17:21:24.756	Warning	Interface Dot11Radio0, cannot associate: No matching SSID
Sep 13 17:21:16.411	Notification	Configured from console by console
Mar 1 00:40:50.536	Warning	Interface Dot11Radio0, cannot associate: No matching SSID
Mar 1 00:40:42.947	Notification	Configured from console by console

Lab 6.5.3.1 Manage Bridge Configuration and Image Files

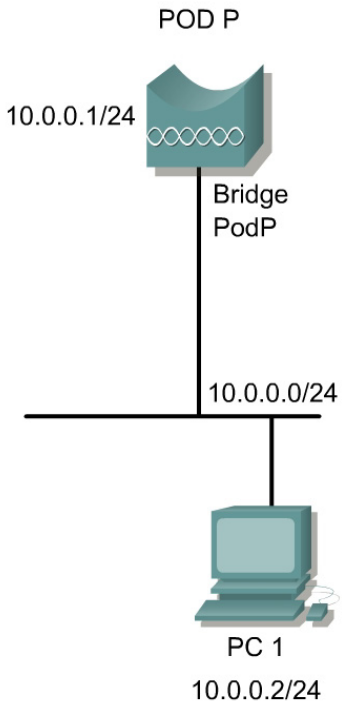
Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn the features of the wireless bridge configuration dump and the process used for wireless bridge configuration and image load processes. Additionally, in this lab, the student will learn the process for distributing firmware and configurations.

Topology



Preparation

The students will read and familiarize themselves with the concepts in Chapter 6 prior to attempting this lab.

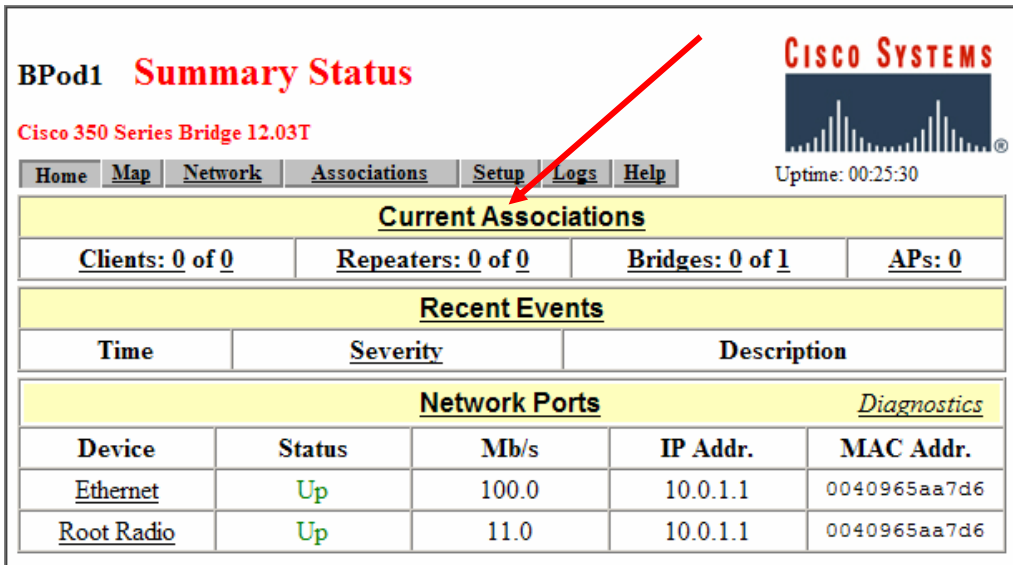
Tools and Resources

Each team will require the following:

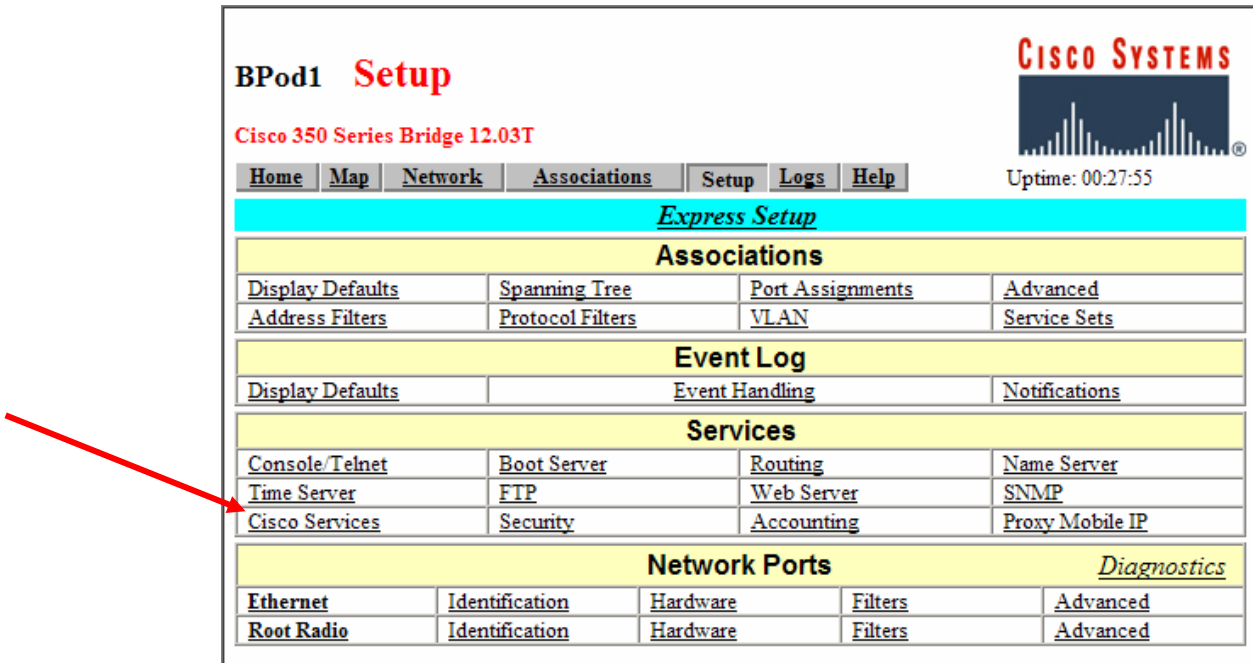
- One BR350
- One PC on the wired LAN for bridge configuration

Step 1 Backup the current configuration file

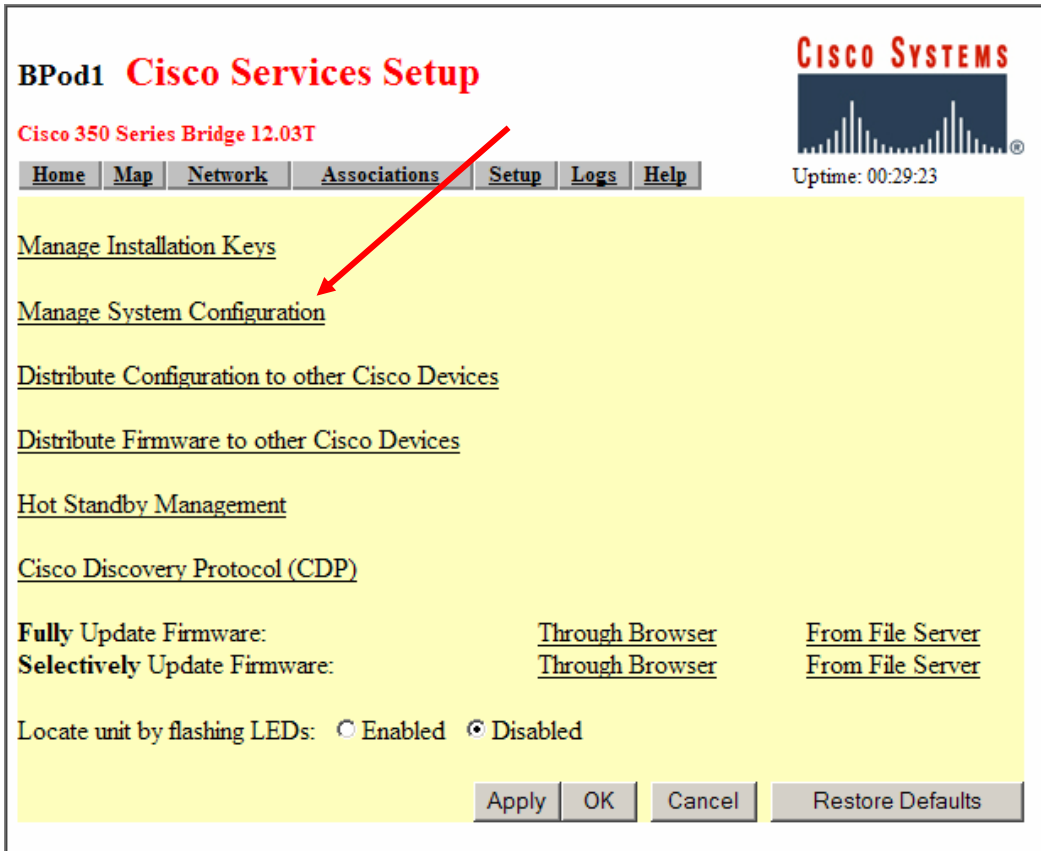
In order to backup the current configuration files, complete the following steps:



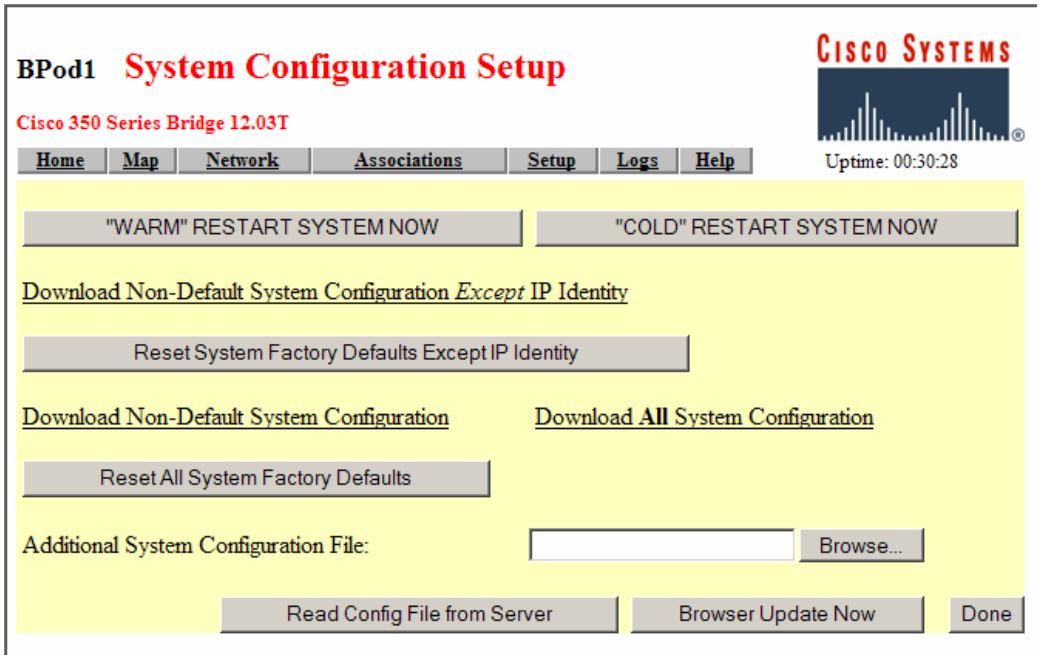
a. On PC1, open a web browser and access the bridge. From the Home page, click on the Setup tab.



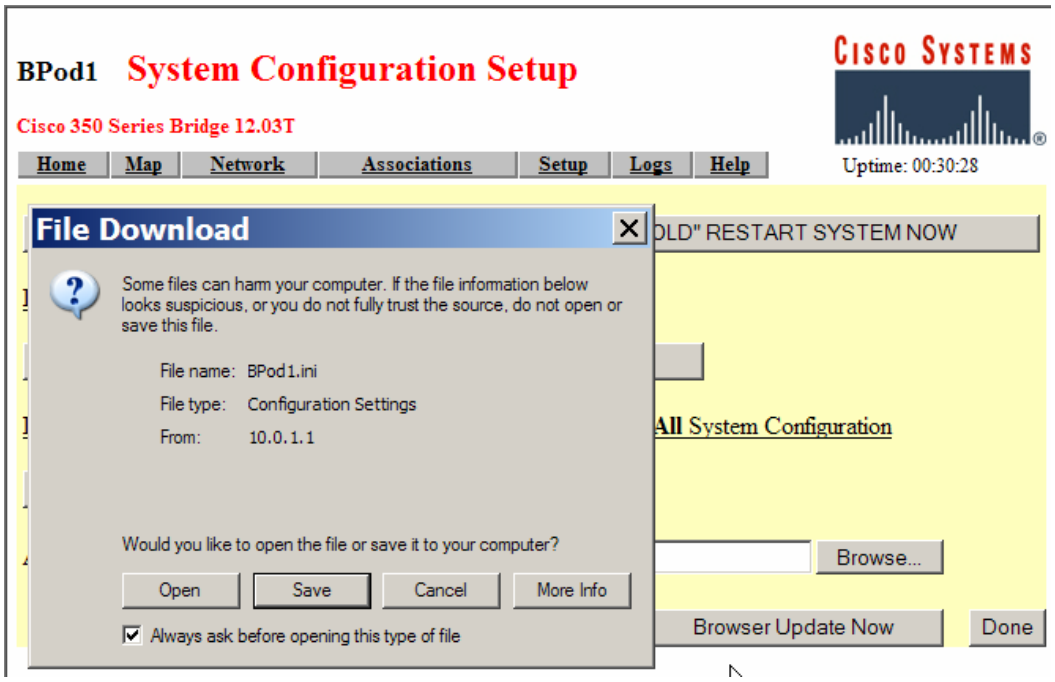
b. From the Services section, select **Cisco Services**.



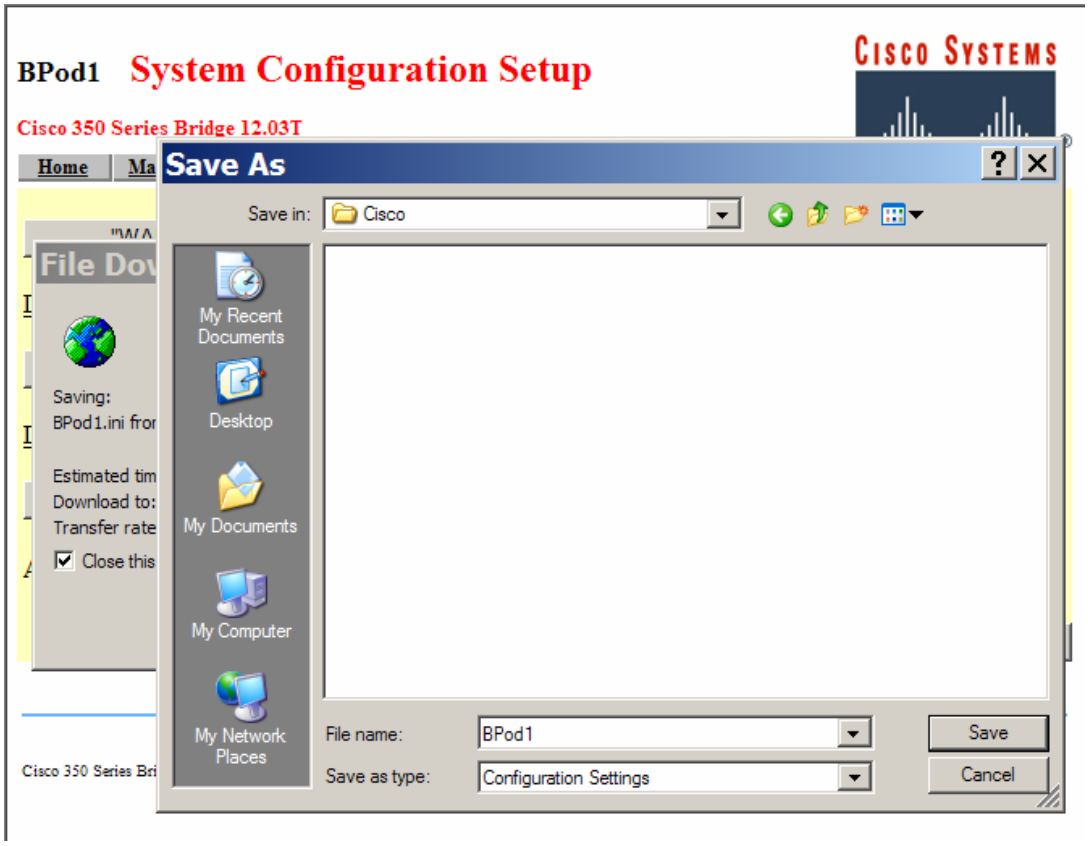
c. Click on the **Manage System Configuration** link.



d. Click on the **Download All System Configuration** button.

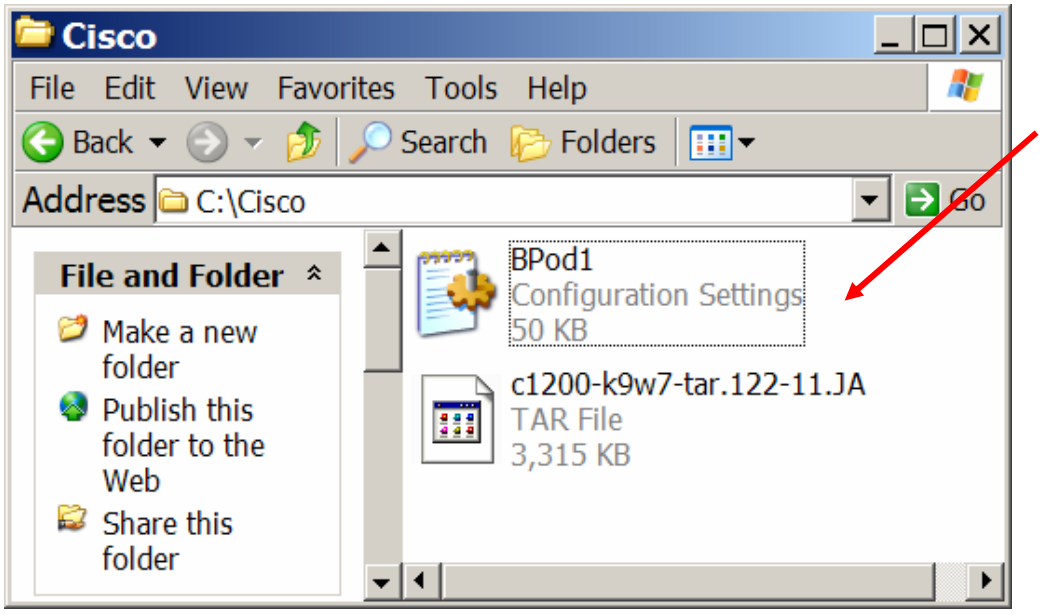


e. When the File Download screen appears, click the **Save** button.

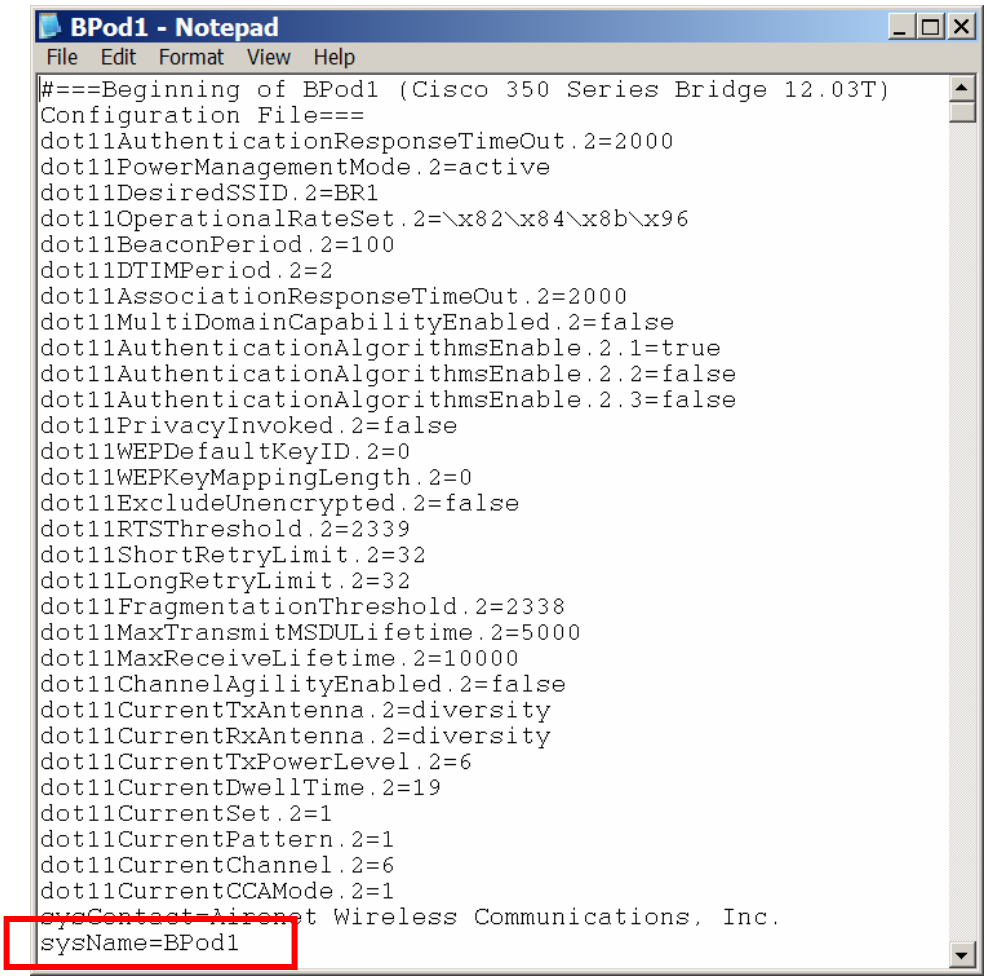


f. Choose a file name and location or click **Save** to accept the defaults.

In this example, BPod1.ini was selected as the file name, and C:\Cisco directory was selected as the location to save the configuration file.



g. Verify the configuration file is saved on PC1.



h. On PC1, open the configuration file with Notepad. Edit the “sysName=” value to BPod1backup.

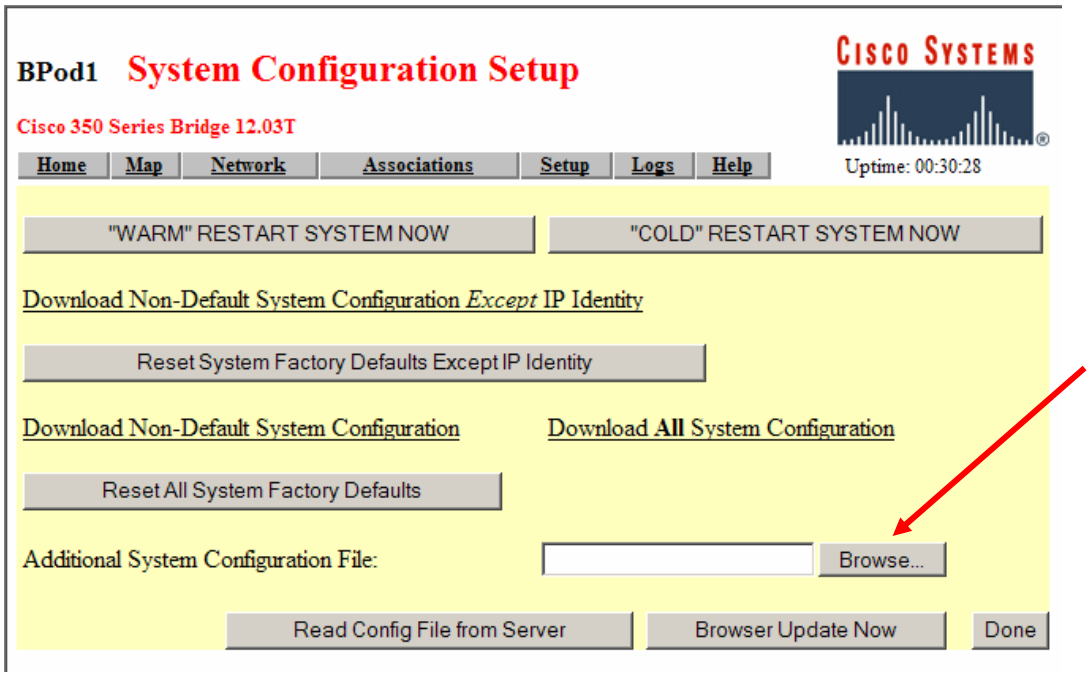
i. Save the changes and exit Notepad.

Step 2 Load a configuration file

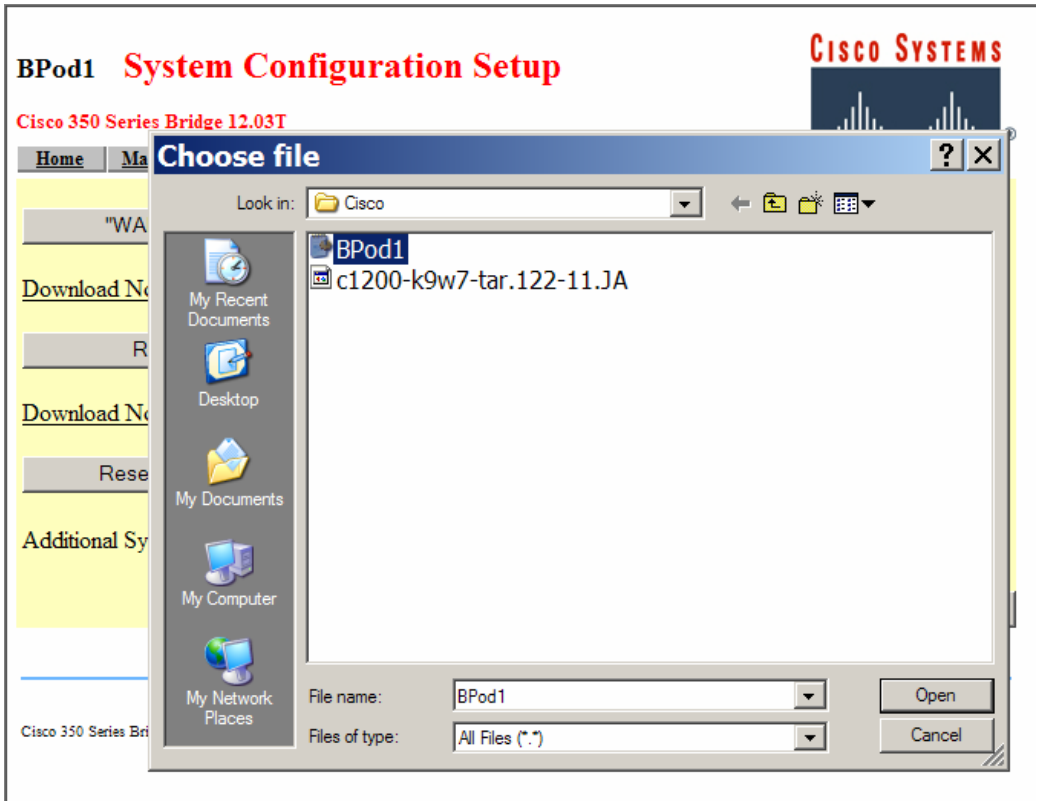
If the configuration is ever lost or corrupted, it can be restored by using the Additional System Configuration File. This is an option from the **Cisco Services** Setup menu or page to move the configuration file into the bridge. The system automatically restores the configuration based on these commands.

In order to load a configuration file, complete the following steps:

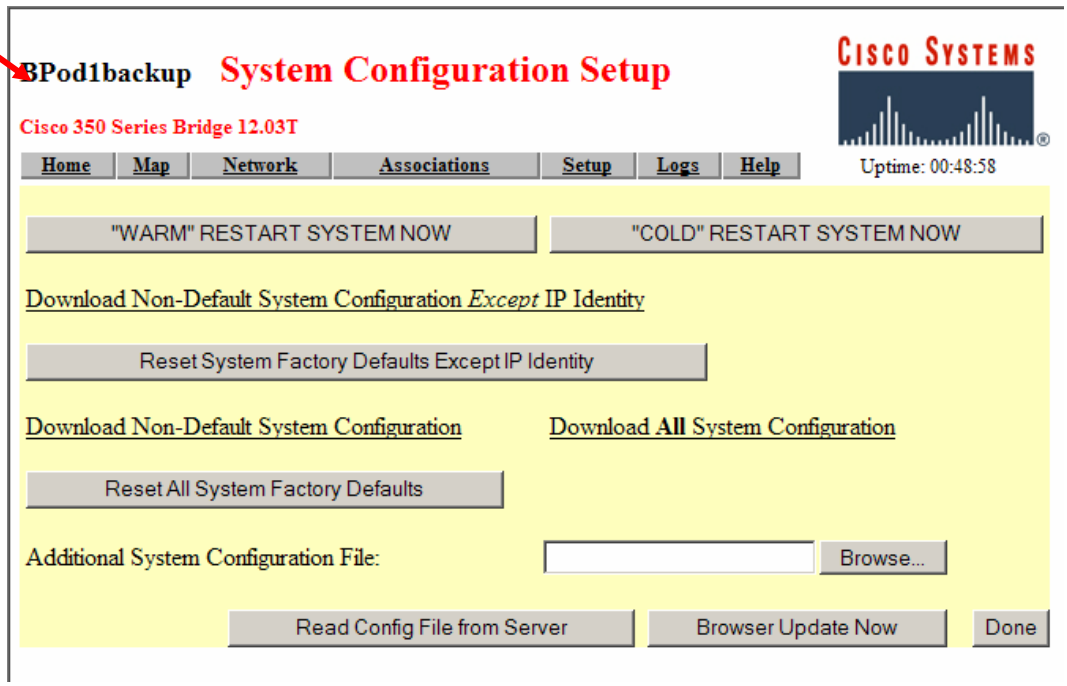
a. On the **Cisco Services Setup** page, click on the **Manage System Configuration** button.



b. From the **System Configuration Setup** Page, click on the **Browse…** button near the Additional System Configuration file: field.



c. Choose the configuration file BPod1 that is to be loaded and click the **Open** button.



d. Click the **Browser Update Now** button to load the file. After about 10 seconds, the page will update. Notice the System name will change in the upper left corner.

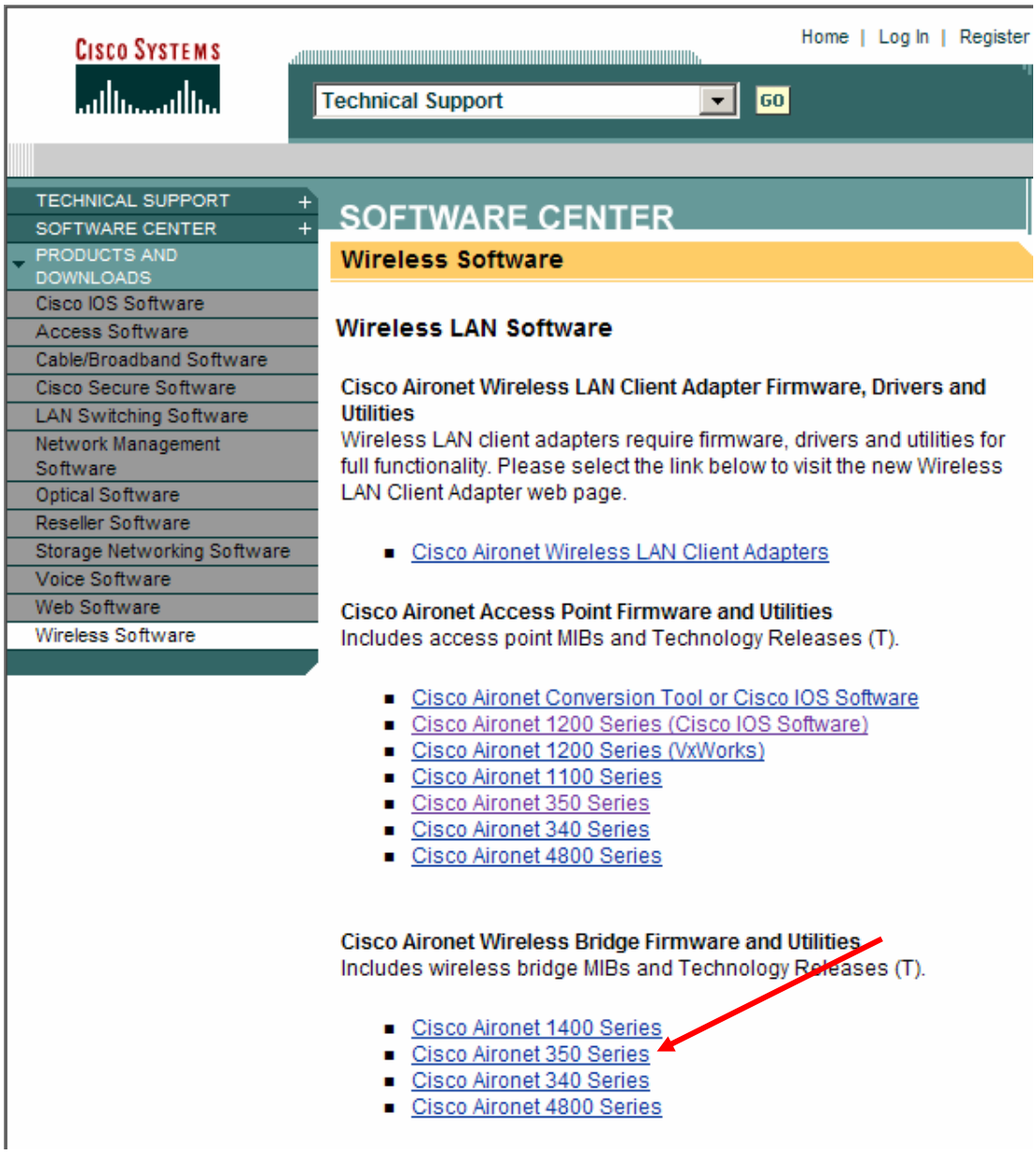
18. Was it possible to load the saved configuration file into the current configuration of the bridge? How is this confirmed?

_____

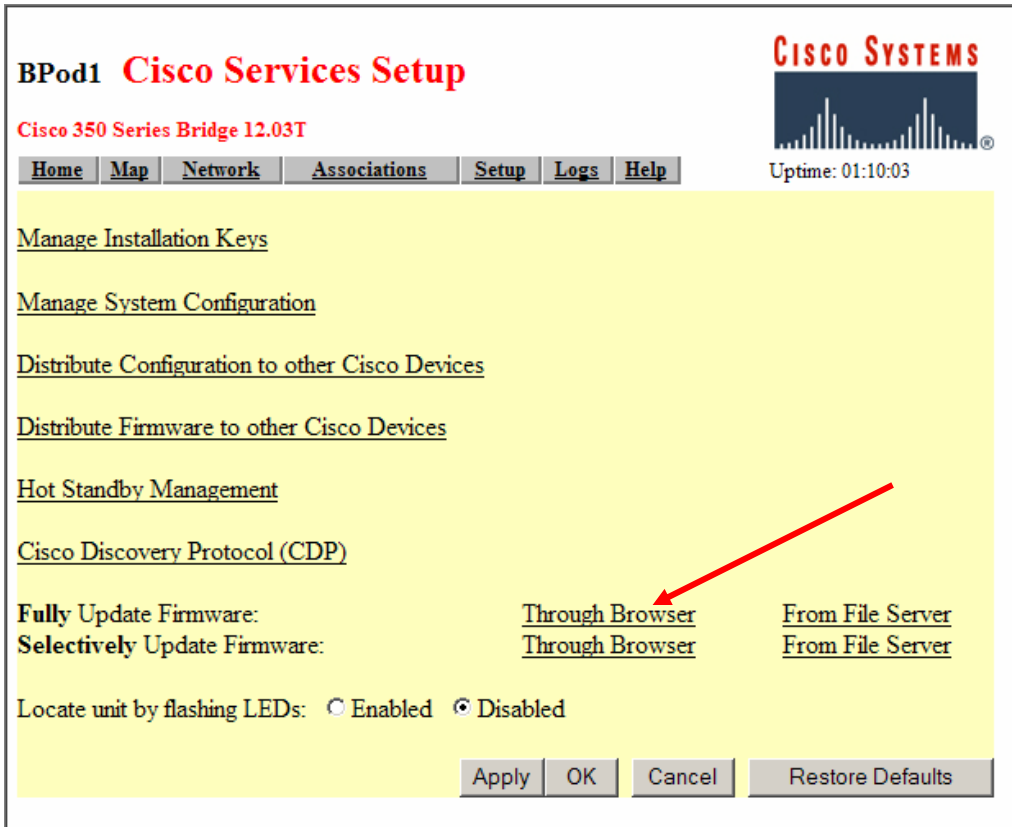
Step 3 Update bridge firmware using a browser

Bridges may need to be updated to provide new services or greater security features.

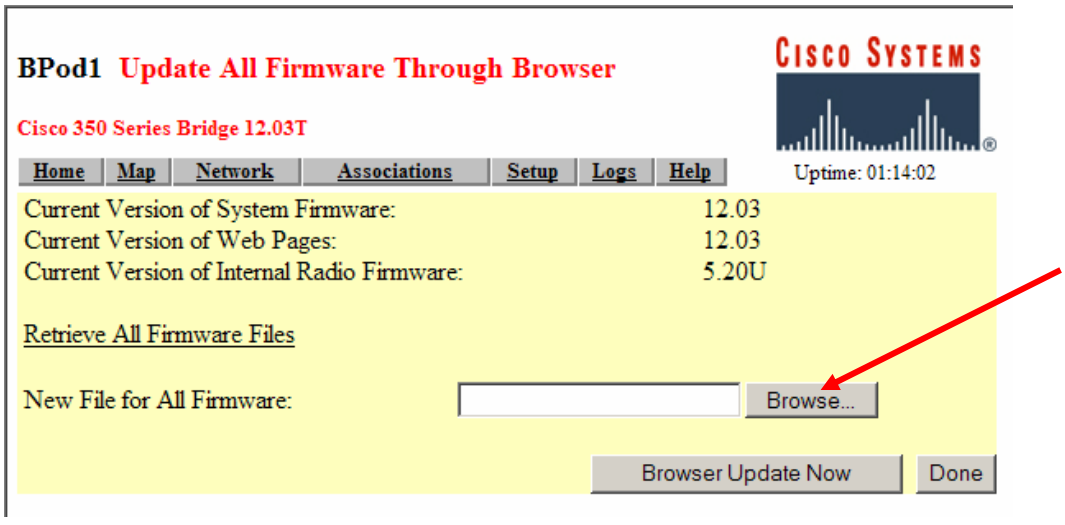
In order to update firmware using a web browser, complete the following steps:



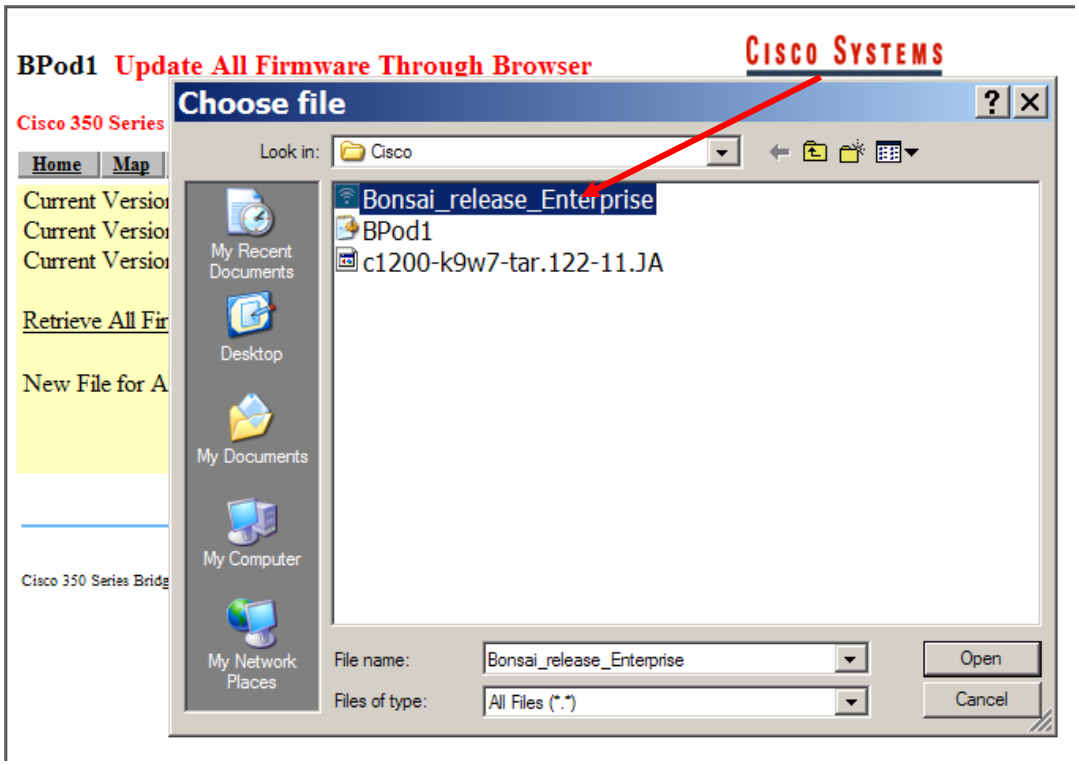
a. Download the latest BR350 image from Cisco.com. Save the image file on PC1.



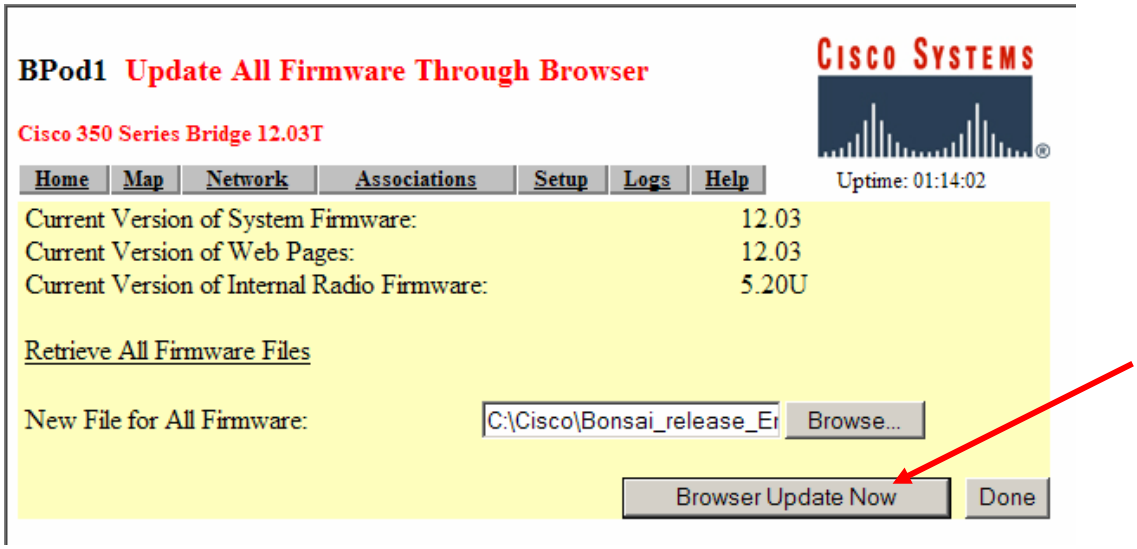
b. From the **Cisco Services Setup** Page, click on the **Fully** Update Firmware**: Through Browser** link.



c. From the **Update All Firmware Through Browser** Page, click on the **Browse…** across from the **New File for All Firmware**:



d. Select the downloaded BR350 image file and click the **Open** button.



e. The image file location will now appear in the field.

Note	If the bridge has the latest image installed, skip the next step. If the bridge requires updating, ask for instructor permission before upgrading.

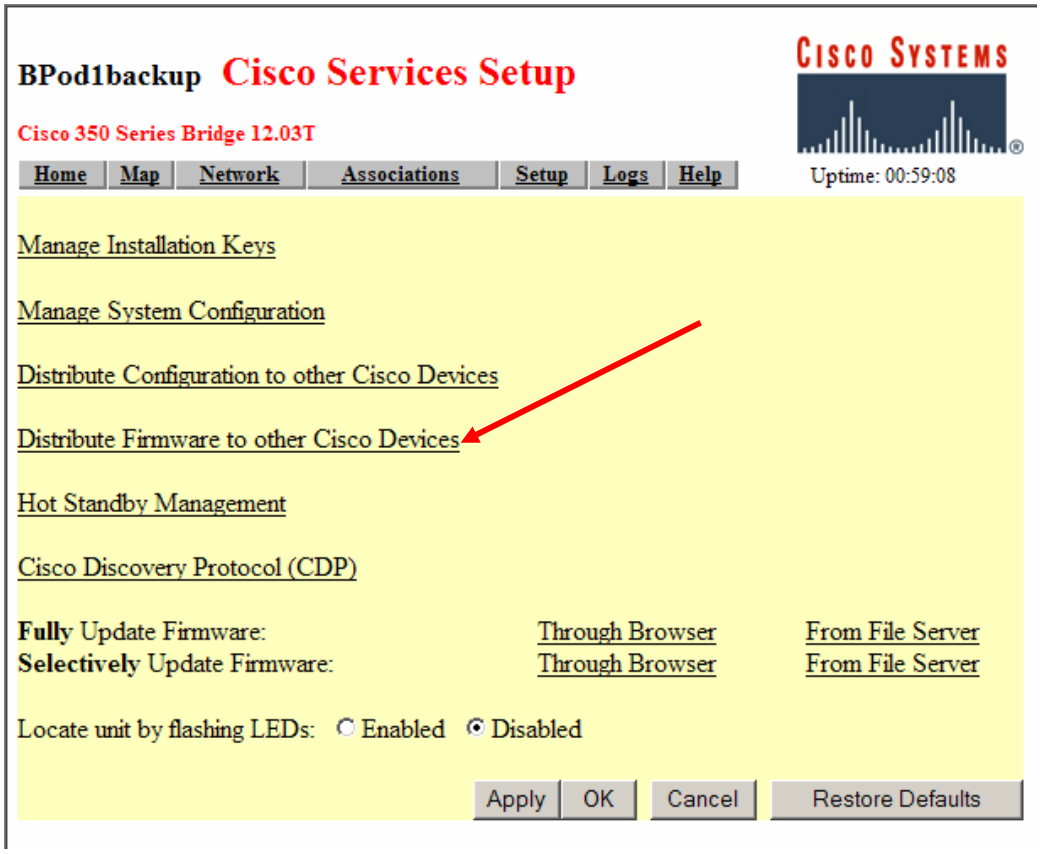
f. Click on the **Browser Update Now** button.

Note	Do not interrupt the update process one the update begins. This will corrupt the bridge operating system, rendering the bridge inoperable.

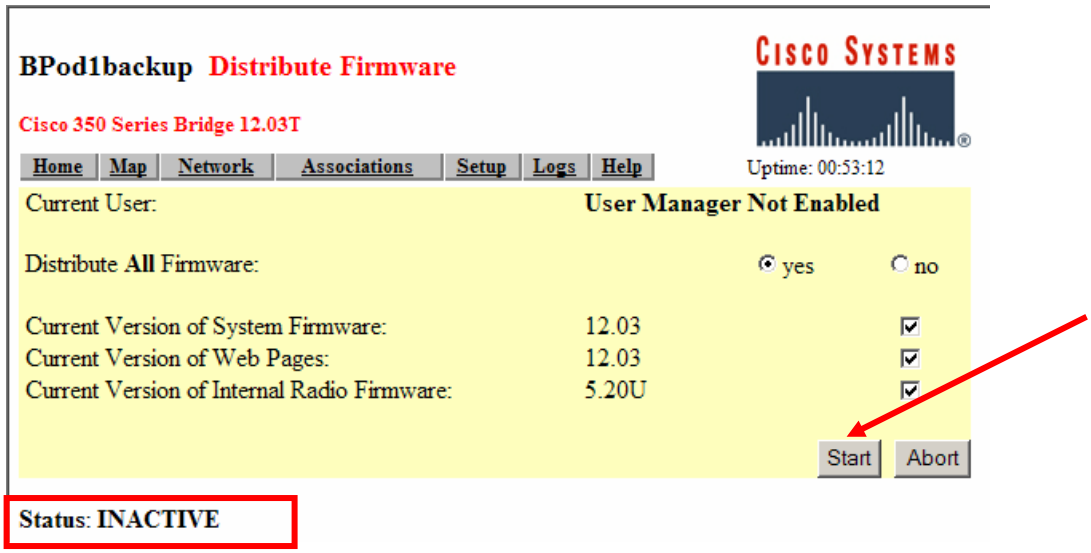
Step 4 Distribute bridge firmware

The **Cisco Services Setup** menu provides an option for distributing firmware or configuration from one bridge to all other bridges on the infrastructure. These options reduce the time needed to perform firmware upgrades or make global changes to the configuration.

In order to distribute firmware, complete the following steps:

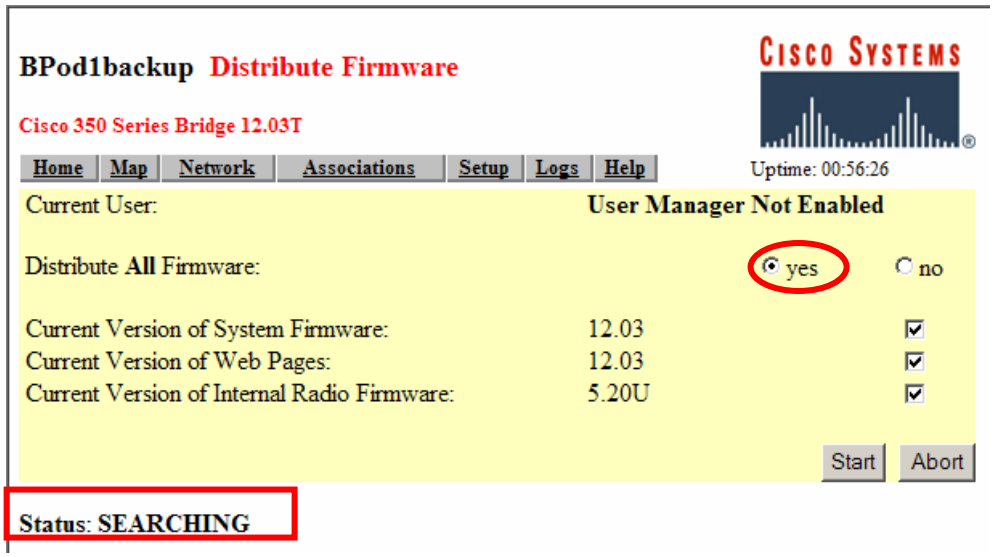


a. Click on the **Distribute Firmware to other Cisco Devices** from the **Cisco Services Setup** page.



b. From the **Distribute Firmware** Page, choose the **yes** radio button on for the Distribute all firmware option.

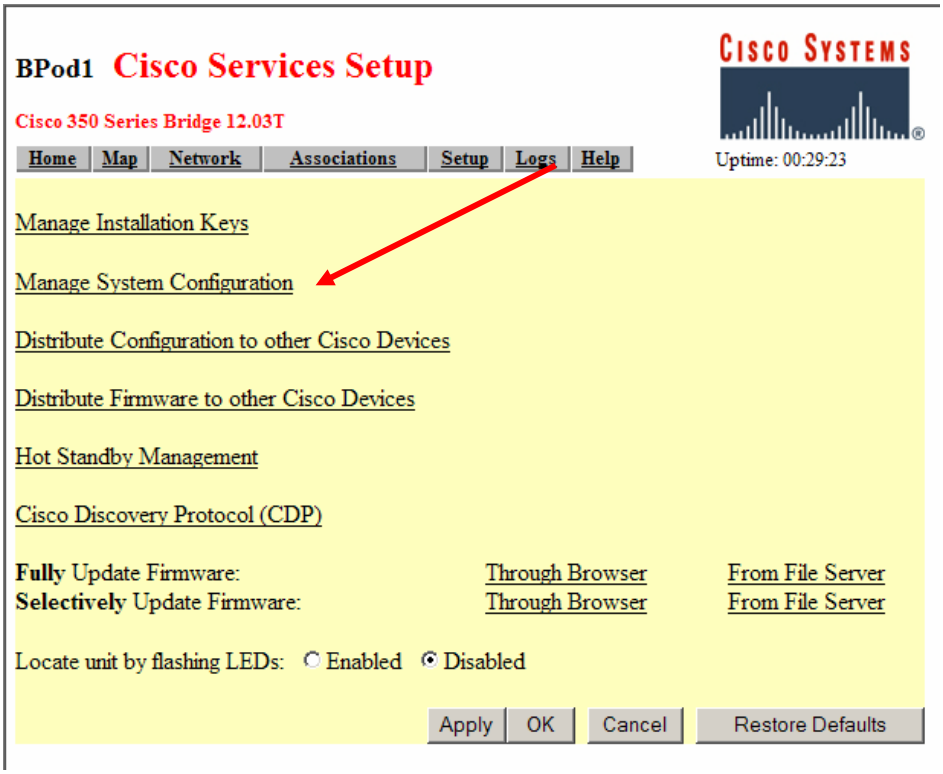
c. Click the **Start** button.



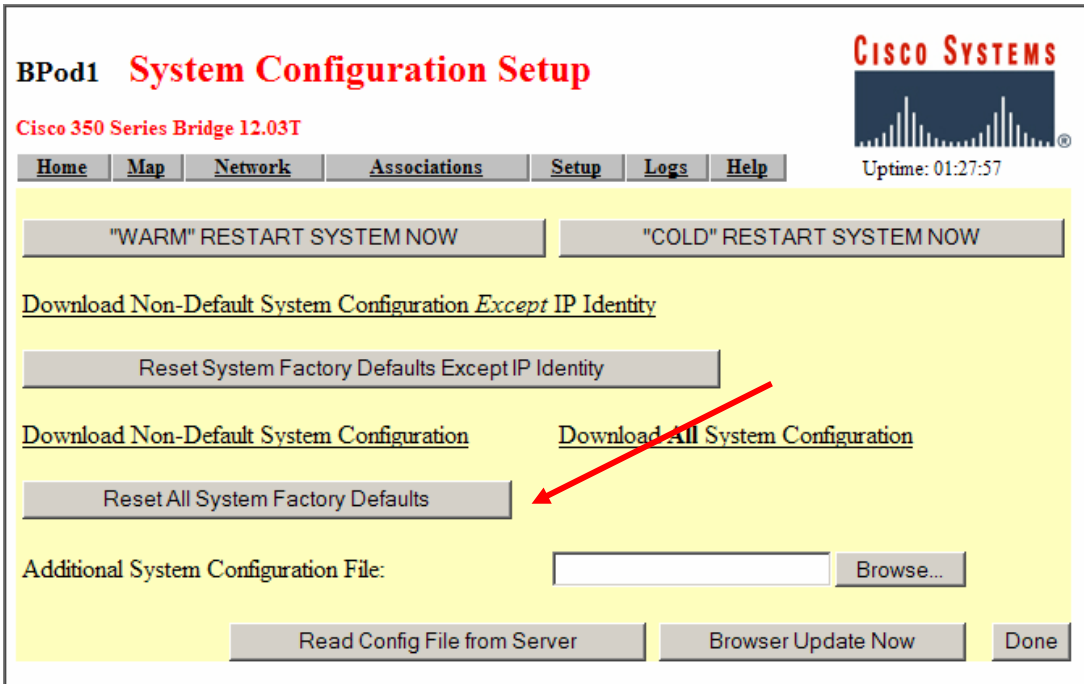
The bridge will search for other bridges to distribute its firmware to, which is indicated by the SEARCHING status in the lower left hand corner of the page. If it locates a bridge, the distribution will occur automatically. If no other bridges are available, the status will display INACTIVE.

Step 5 Reset the bridge configuration

The bridge provides an option to restore the bridge configuration back to factory defaults using a web browser. In order to reset the bridge, complete the following steps:



a. From the **Cisco Services Setup** page, click on the Manage System Configuration link.



b. From the **System Configuration Setup** Page, click on the **Reset All System Factory Defaults** button.

Lab 6.5.3.2 Manage Bridge Configuration and Image Files

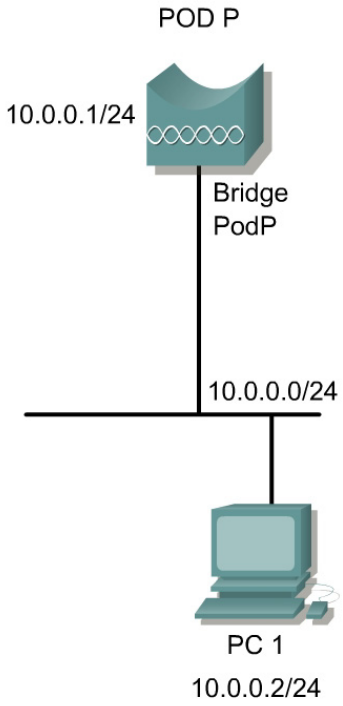
Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn the features of the wireless bridge configuration file backup and image load processes.

Topology



Preparation

The students will read and familiarize themselves with the concepts in Chapter 6 prior to attempting this lab.

Tools and Resources

Each team will require the following:

- One BR350
- One PC on the wired LAN for bridge configuration

Step 1 Backup the current configuration file

In order to backup the current configuration files, complete the following steps:

a. Test connectivity from PC1 to the bridge.

b. Launch TFTP software on PC1.

c. On PC1, open a Telnet or console connection to the bridge. If prompted for a username and password, enter the default values:

   1. Username: *Cisco*
   2. Password: *Cisco*

d. Enter enabled mode. When prompted for the password, enter *Cisco*.

```
bridge>enable
Password:*****
```

e. Test connectivity from the bridge to PC1.

```
bridge#ping 10.0.0.2
```

f. Copy the running-configuration from the bridge to the TFTP server on PC1.

```
bridge#copy running-config tftp
Address or name of remote host []? 10.0.0.2
Destination filename [bridge-confg]?
!!
1152 bytes copied in 0.081 secs (14222 bytes/sec)
```

g. On PC1 browse to the folder containing the uploaded file to ensure that it was copied correctly.

Step 2 Load a configuration file

If the configuration is ever lost or corrupted, it can be restored by using the backup configuration file. In order to load a configuration file, complete the following steps:

a. Test connectivity from PC1 to the bridge.

b. Launch TFTP software on PC1.

c. On PC1, open a Telnet or console connection to the bridge. If prompted for a username and password, enter the default values:

   1. Username: *Cisco*
   2. Password: *Cisco*

d. Enter enabled mode. When prompted for the password, enter *Cisco*.

```
bridge>enable
Password:*****
bridge#
```

e. Test connectivity from the bridge to PC1.

```
bridge#ping 10.0.0.2
```

h. Copy the saved backup configuration file from the TFTP server to the bridge. You should browse to the TFTP folder on PC1 to view the filename of the backup configuration file.

```
bridge#copy tftp running-config
Address or name of remote host []? 10.0.0.2
Source filename []? bridge-confg
Destination filename [running-config]?
Accessing tftp://10.0.0.2/bpod1-confg...
Loading bridge-confg from 10.0.0.2 (via BVI1): !
```


Step 3 Backup bridge image file

The CLI provides commands to archive a copy of the bridge image file to a TFTP server. This archived file is stored in .tar format on the TFTP server and can be downloaded to the bridge if needed.

a. Ensure that the TFTP server is running on PC1 and that the bridge can ping the IP address of PC1.

b. From CLI privileged mode, enter the following command:

```
bridge#archive upload-sw tftp://10.0.0.2/c1310-k9w7.tar
```

c. The bridge will build the image file and create the .tar file on the TFTP server. Confirm that the file was uploaded by browsing to the TFTP directory on PC1.

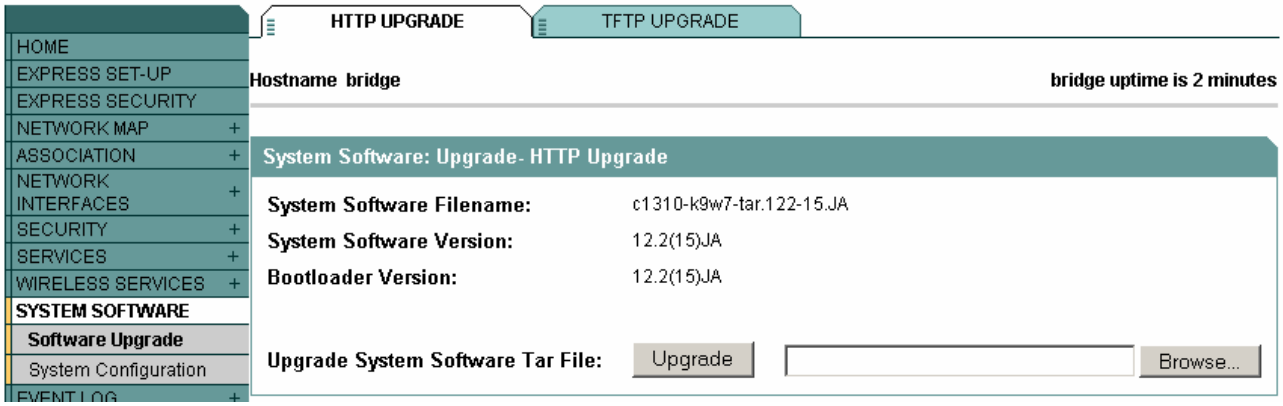
Step 4 Load a bridge image file using the web interface

If the bridge has a firmware failure, an image file must be reloaded via the Web-browser interface or by using the console serial port. The browser interface can be used if the bridge is operational.

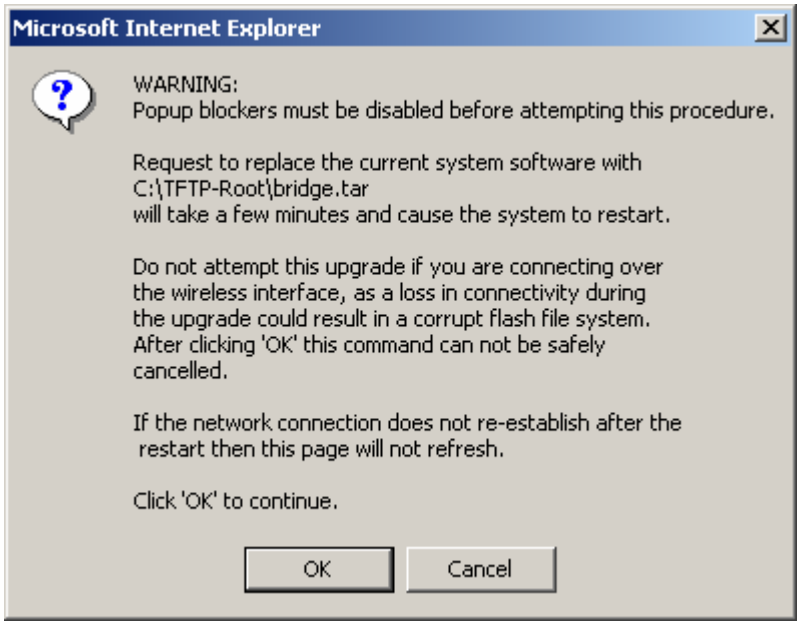
a. Prior to loading an image file from the PC to the bridge, the image file must be saved to a local directory on the PC and connectivity between the PC and the bridge must be established.

b. Access the bridge web interface from the PC. Enter a valid username and password when prompted to do so.

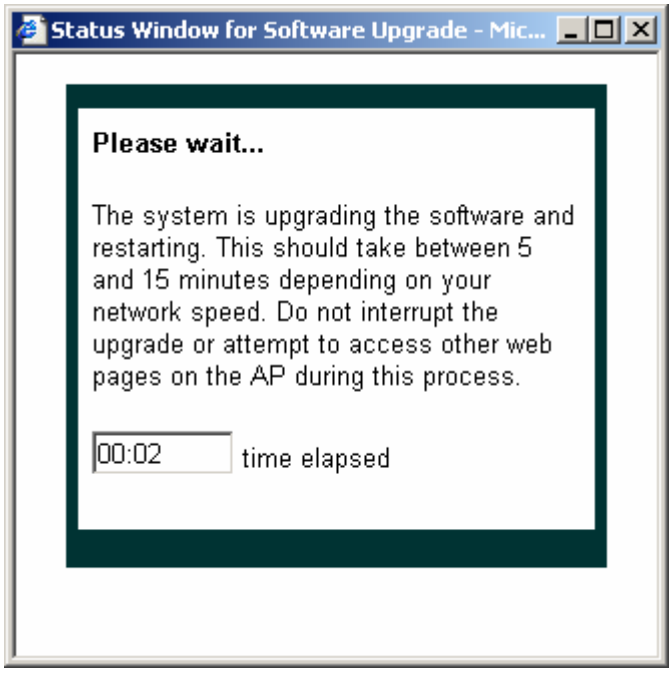
c. From the left navigation bar, click the link for **System Software** and then **Software Upgrade**. From the **HTTP Upgrade** tab, click the *Browse* button to locate the image file on the PC. Click the *Upgrade* button.



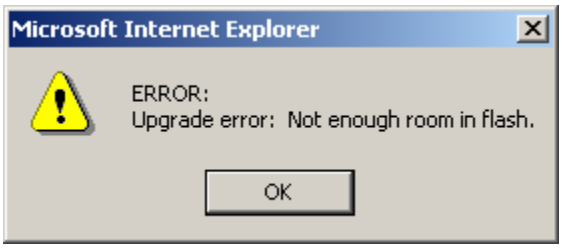
d. A warning window will display. Read the information in this window carefully before continuing with the HTTP upgrade. Click OK to continue.



e. An additional browser window will open to provide information about the upgrade process. Do not close this window or otherwise interrupt the upgrade process.



f. If the bridge does not have room in flash for the new image, an error message will display. If this error is displayed, the image must be installed using the CLI.



Step 5 Load a bridge image file using the CLI

If the bridge has a firmware failure, an image file must be reloaded via the Web-browser interface or by using the console serial port. The browser interface can be used if the bridge is operational.

a. Prior to loading an image file from the PC to the bridge, the image file must be saved to a local PC in the correct directory for the TFTP server. This PC must be running TFTP software.

b. Open the CLI using a connection to the bridge's console port.

c. Reboot the bridge by removing power and reapplying power.

d. Let the bridge boot until the command prompt appears and the bridge begins to inflate the image. When you see the # symbols on the CLI, press **Esc**:

```
Loading "flash:/c1310-k9kw-7mx.v122_15_ja.200040314-k9w7-
mx.v122_15_ja.20040314"...################################## [Esc]
```

Note: Depending on the terminal emulation software you are using, you may have to press **Esc** twice to access the boot loader.

e. At the **bridge:** prompt, enter the following commands to set an IP address on the bridge. Note: You must use upper-case characters when you enter the IP-ADDR, NETMASK, and DEFAULT_ROUTER options with the set command.

```
bridge: set IP_ADDR 10.0.0.1
bridge: set NETMASK 255.255.255.0
bridge: set DEFAULT_ROUTER 10.0.0.2
```

f. Prepare the bridge for TFTP transfer:

```
bridge: tftp_init
```

g. The `tar` command is used to load and inflate the new image from the TFTP server. The command should include each of the options listed:

   i. The `-xtract` option, which inflates the image when it is loaded.

   ii. The IP address of the TFTP server.

   iii. The directory on the TFTP server that contains the image. (Optional)

   iv. The name of the image as it appears on the TFTP server.

   v. The destination for the image (the bridge Flash)

h. To load an image file from the default TFTP directory to flash on the bridge, enter this command:

```
bridge: tar -xtract tftp://10.0.0.2/c1310-k9w7.tar flash:
```

i. The image will be downloaded and inflated. The CLI will display the progress as each file is written to the bridge flash directory. When the display becomes full the CLI pauses and displays `--MORE--`. **You must press the spacebar to continue.** If you do not press the spacebar to continue, the process eventually times out and the bridge stops inflating the image

```
extracting info (229 bytes)
c1310-k9w7-mx.122-15.JA/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA/html/ (directory) 0 (bytes)
c1310-k9w7-mx.122-15.JA/html/level1/ (directory) 0 (bytes)
extracting c1310-k9w7-mx.122-15.JA/html/level1/appsui.js (558 bytes)
extracting c1310-k9w7-mx.122-15.JA/html/level1/back.htm (205 bytes)
-- MORE --
```

j. Enter the set `BOOT` command to designate the new image as the image that the bridge uses when it reboots. The bridge creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:


```
bridge: set BOOT flash:/c1310-k9w7-mx.122-15.JA/c1310-k9w7-mx.122-
15.JA
```

k. Enter the `set` command to check the bootloader entries.

```
bridge: set
BOOT=flash:/c1310-k9w7-mx.122-15.JA/c1310-k9w7-mx.122-15.JA
DEFAULT_ROUTER=10.0.0.2
IP_ADDR=10.0.0.1
NETMASK=255.255.255.0
```

l. Enter the `boot` command to reboot the access point. When the access point reboots, it loads the new image. Any previous configurations will be retained.

```
bridge: boot
```


Lab 6.5.5.1 Configure Layer 3 Site-to-Site Wireless Link—OPTIONAL Challenge Lab

Estimated Time: 45 minutes

Number of Team Members: Students will work in teams of two.

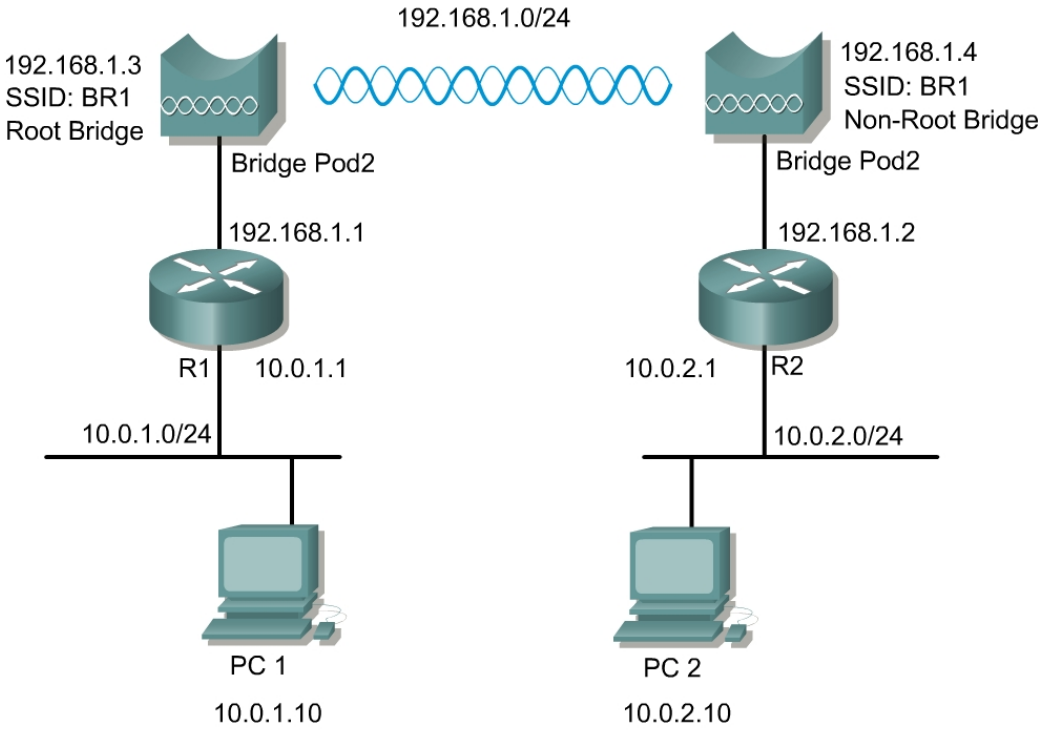
Objective

Configure a site-to-site bridge network separated by a Layer 3 device. Test the speed of the wireless bridge link.

Scenario

A remote location which is several miles away requires connectivity to the existing wired network. The connection can be bridged wirelessly with two BR350s. In large networks, it is necessary to provide Layer 2 broadcast control using routers.

Topology



Preparation

The instructor or students must cable and configure the perimeter routers in addition to the wired LAN. The routers Ethernet interfaces must be configured and enabled. Static routing should be configured on the routers. Ensure that the devices are configured according to the topology. The bridge devices should be configured as follows:

Device Name	Label	SSID	Address
BPod1	BR1	BR1	192.168.1.3/24
BPod2	BR2	BR1	192.168.1.4/24

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco BR350s with 2.4dBi dipole antenna(s)
- Two dual Ethernet routers
- Two switches or hubs(optional)

Step 1 Connect and reset both bridges

Connect a nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the bridge. (This cable ships with the bridge)

a. Open a terminal emulator.

b. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: Xon/Xoff

c. Press = to display the home page of the bridge. If the bridge has not been configured before, the Express Setup page appears as the home page. (GO TO STEP 3)

d. If the bridge is already configured, the Summary Status page appears as the home page. When Summary Status screen appears, type :**resetall**, and press **Enter**.

```
Enter "YES" to confirm Resetting All parameters to factory defaults:
YES
00:02:12 (FATAL): Rebooting System due to Resetting Factory Defaults
*** Restarting System in 5 seconds...
```

e. Type **yes**, and press **Enter** to confirm the command.

f. Power cycle the bridge by removing the power.

Step 2 Connect to the BR350s using express setup

a. Plug a second RJ-45 Ethernet cable into the power injector end labeled TO NETWORK. Plug the other end of the Ethernet cable into the Ethernet port on a switch or hub. Then connect PC1 to the switch. A crossover cable can be used to connect directly from the inline power injector to PC1/PC2.

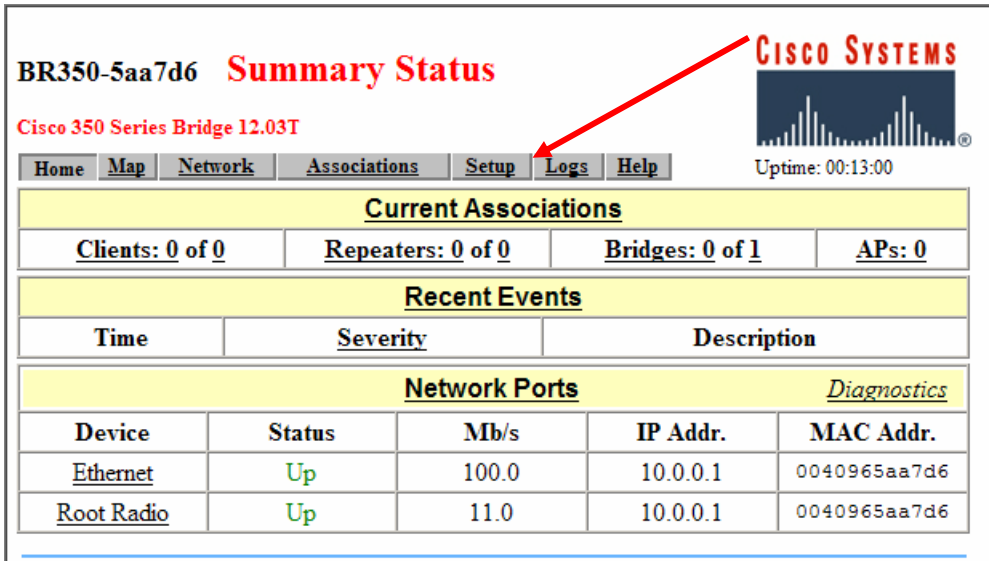
b. Configure PC1 to 10.0.0.2/24

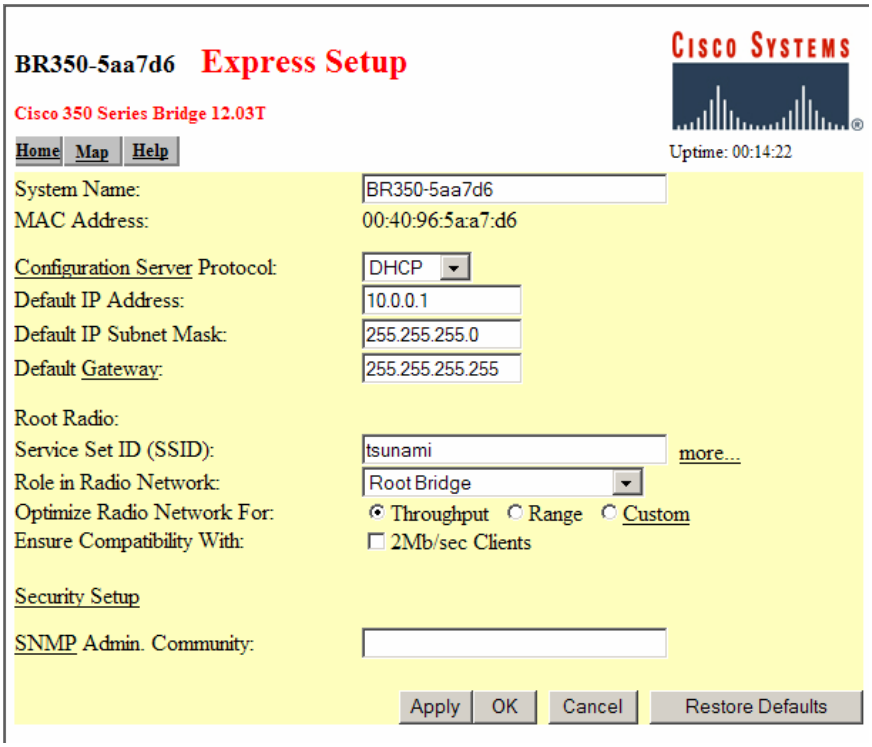
c. Open a web browser and enter the default bridge address. http://10.0.0.1 and press Enter.

d. Either of the following pages will appear:

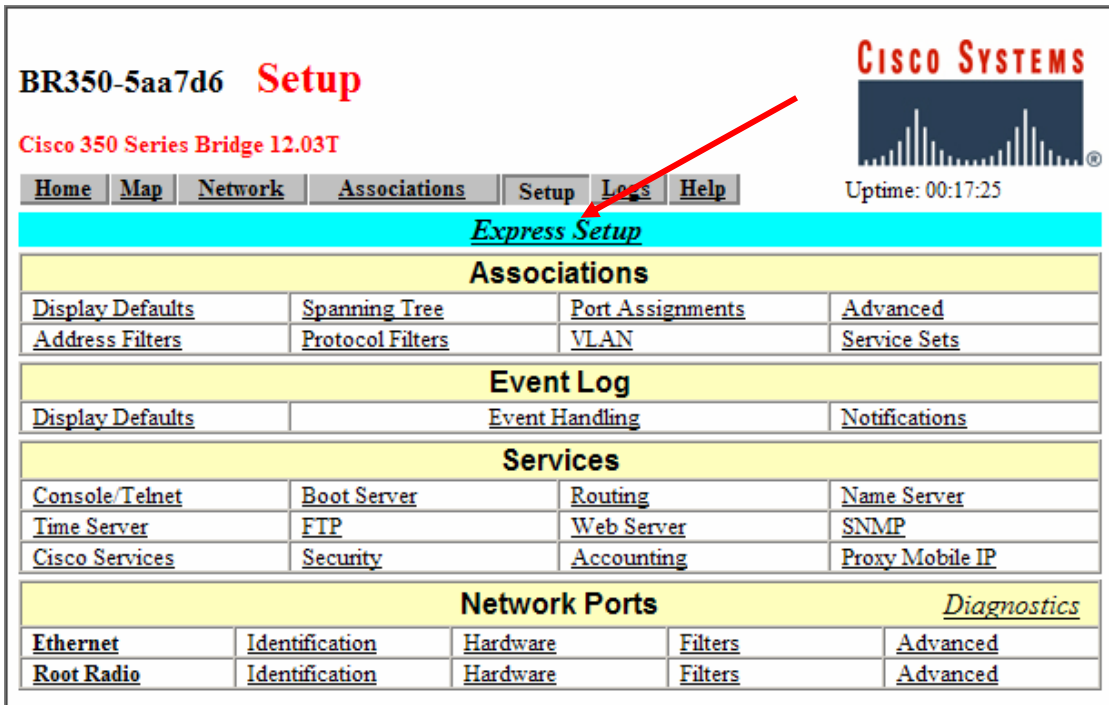
   i. The **Summary Status** Page, also known as the **Home** Page

   ii. The **Express Setup** Page



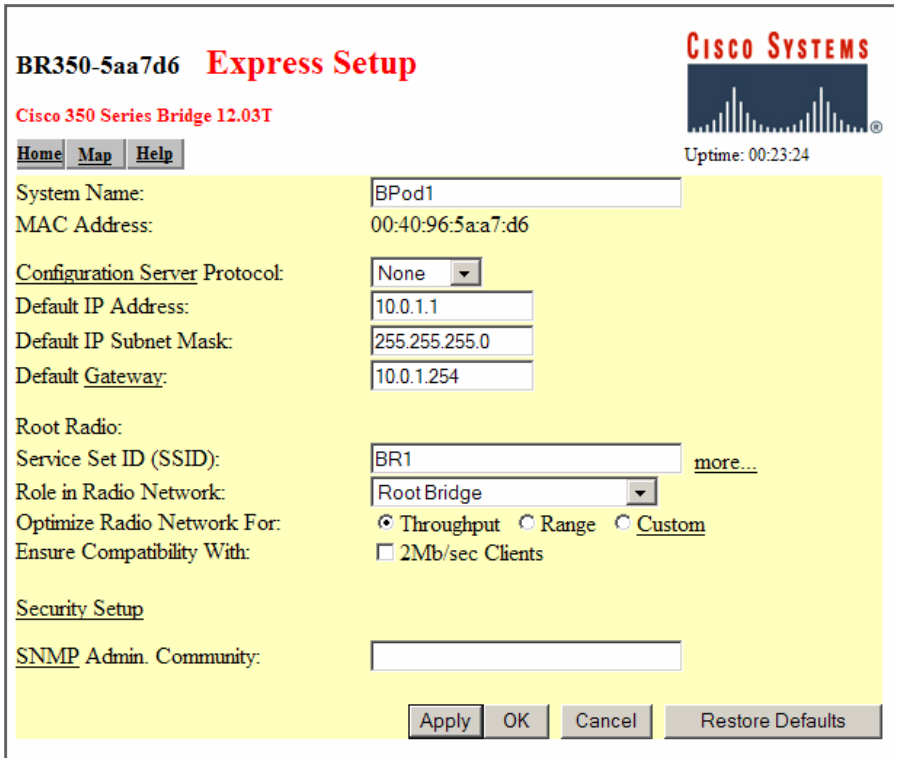


e. If the Express Setup Page does not appear, from the Summary Status Page click on the **Setup** hyperlink. This will bring up the Setup Page.



f. Now click on the ***Express Setup*** link. This will now bring up the Express Setup Page.

Step 3 Configure the bridge settings



Configure the following settings:

Parameter	BPod1	BPod2
• System Name:	***BPod1***	***BPod2***
• Configuration Server Protocol:	***None***	***None***
• Default IP address:	***192.168.1.3***	***192.168.1.4***
• Default Gateway:	***192.168.1.1***	***192.168.1.2***
• Service Set ID:	***BR1***	***BR1***
• Role in Radio Network:	***Root Bridge***	***Non-Root Bridge w/o Clients***

a. Click Apply. The connection will drop.

b. What roles can the bridge serve in the network?

_____

_____

_____

Step 4 Cable and configure the routers and PCs

Using dual Ethernet routers, such as an 806, 2514, or equivalent.

Configure both routers:

```
hostname Router1
int fa0/0
 ip address 192.168.1.1
255.255.255.0
 description outside
 no shut
!
int fa0/1
 ip address 10.0.1.1 255.255.255.0
 description inside
 no shut
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
line vty 0 4
 password cisco
 login
```

```
hostname Router2
int fa0/0
 ip address 192.168.1.2
255.255.255.0
 description outside
 no shut
!
int fa0/1
 ip address 10.0.2.1 255.255.255.0
 description inside
 no shut
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
line vty 0 4
 password cisco
 login
```

Configure the PCs:

- PC1 with an IP address of 10.0.1.10/24.
- PC2 with an IP address of 10.0.2.10/24

a. Reconnect to the using the browser. Enter 10.0.P.1 and connect.

b. Verify the settings.

1. What other routing method can be used instead of EIGRP?

_____

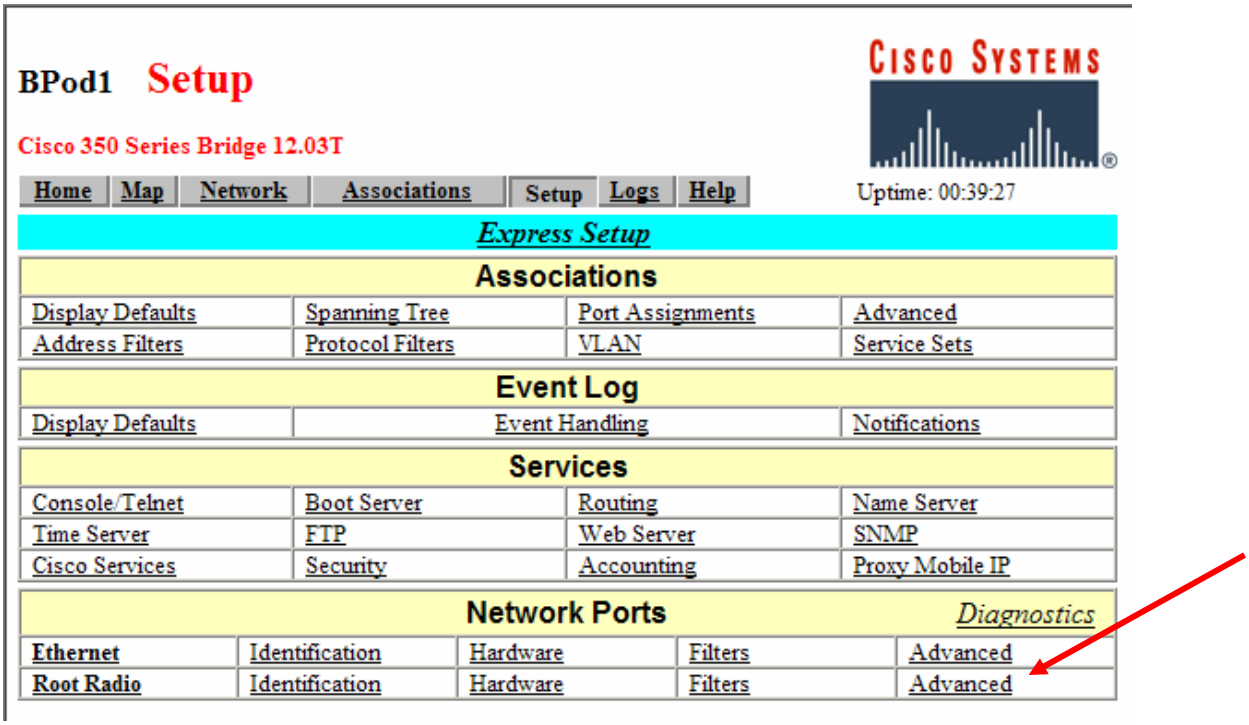
_____

2. Can static routes be used? If so, what is the advantage/disadvantage?

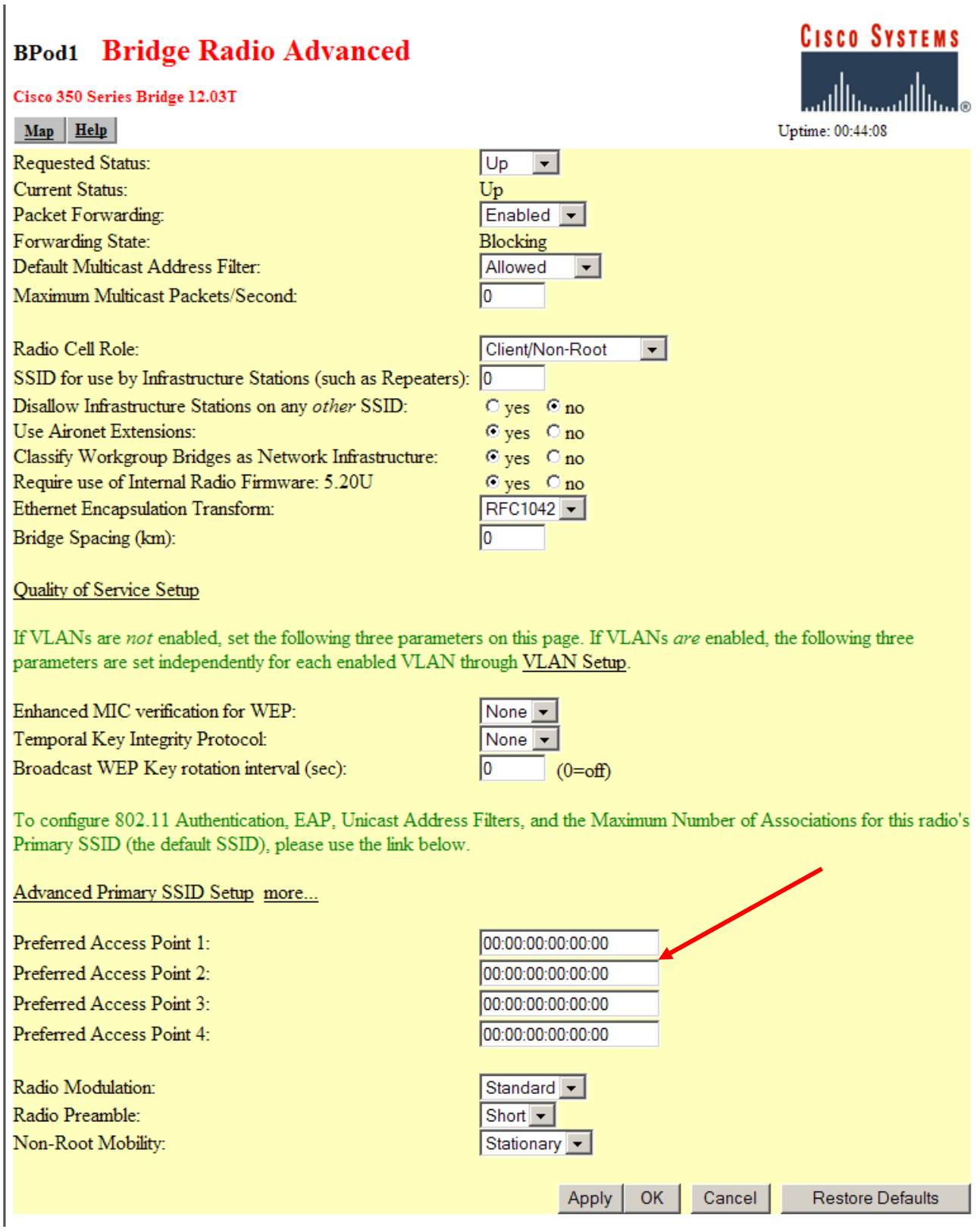
_____

_____

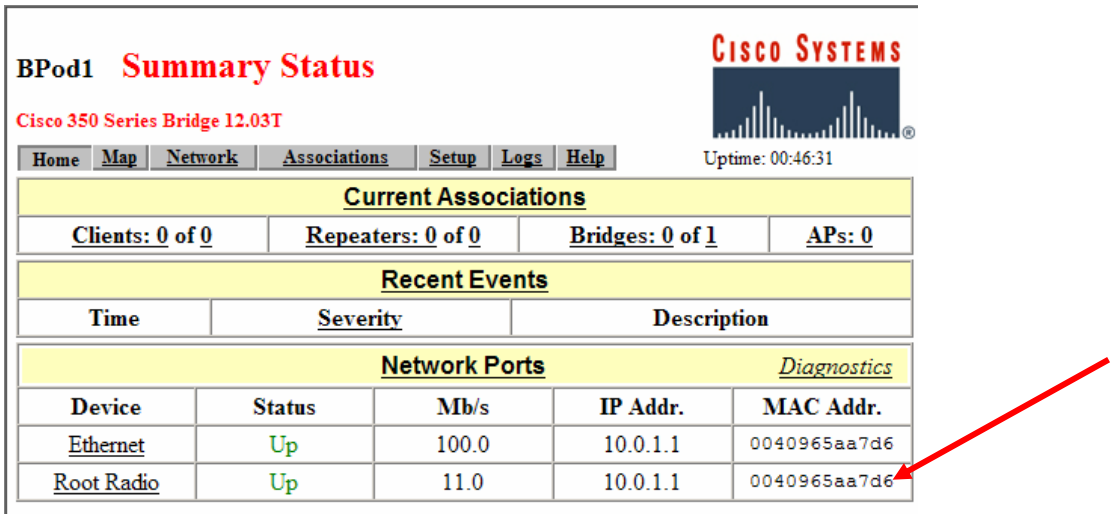
Step 5 Advanced Radio settings for the non-root bridge



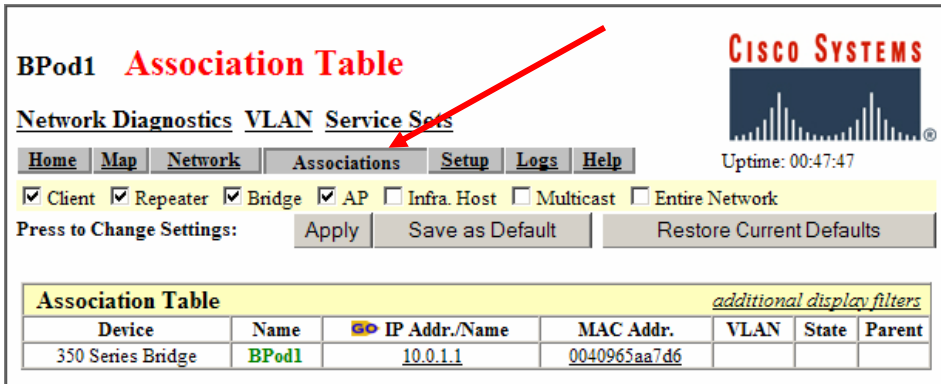
a. From the **Setup** Page, Click on the Root Radio>Advanced link to go to the **Radio Advanced** page of the Non-Root Bridge.



b. Enter the MAC address of the Root Bridge into the **Preferred AP 1:** field. This can be found on the bottom of the Root Bridge or from the Root Bridge **Home** Page.



c. Click the **Apply** button to apply the settings.



d. Go to the **Associations** page of the Root Bridge.

1. Is the Non-Root Bridge in the Association table?

_____

Step 7 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices on this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, ping from PC1 to Router 1 inside Ethernet port. Then ping to Router1 outside port. If successful, ping from PC1 to BPod2. Ping from PC1 to Router2 outside port, followed by a ping to Router2 inside port. Finally, Ping from PC1 to PC2.

b. Were these successful? _____

c. Test layer 7 connectivity by browsing to BPod2 from PC1.

d. Configure FTP or Web services on PC1 and PC2. Transfer a files from PC1 to PC2 and vice versa. Calculate the download performance across the wireless link.

e. What was the download speed in Mbps? _____

f. How was this calculated?

_____

g. What is the speed limitation?

_____

Lab 6.5.5.2 Configure Layer 3 Site-to-Site Wireless Link—OPTIONAL Challenge Lab

Estimated Time: 45 minutes

Number of Team Members: Students will work in teams of two.

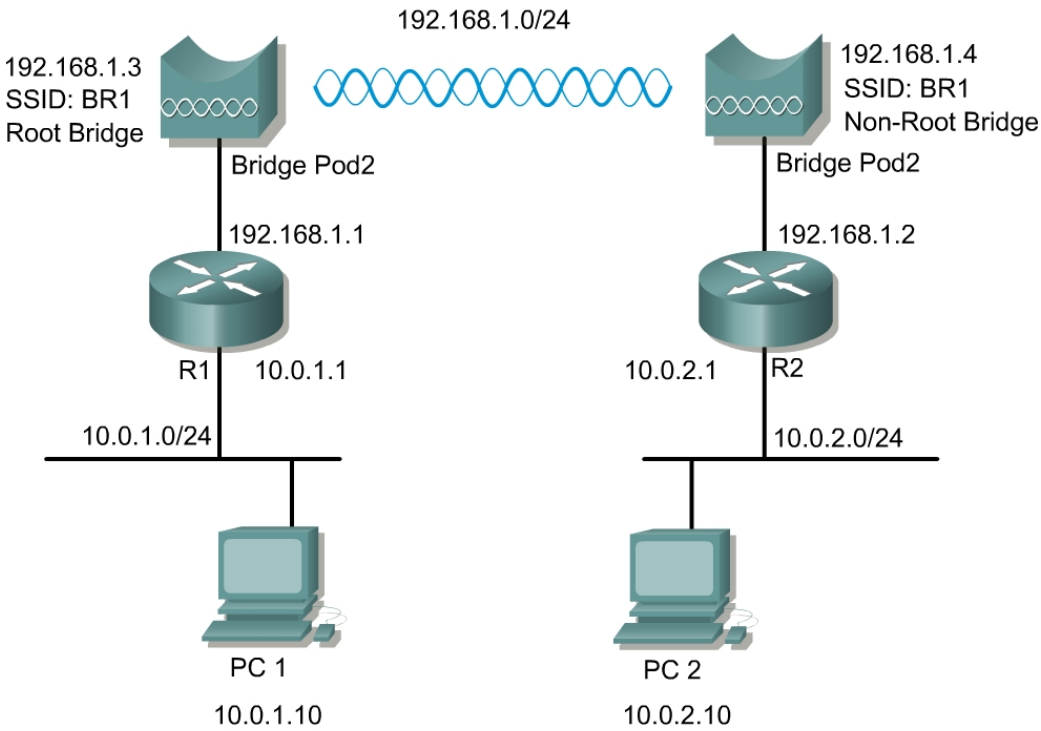
Objective

Configure a site-to-site bridge network separated by a Layer 3 device. Test the speed of the wireless bridge link.

Scenario

A remote location which is several miles away requires connectivity to the existing wired network. The connection can be bridged wirelessly with two BR350s. In large networks, it is necessary to provide Layer 2 broadcast control using routers.

Topology



Preparation

The instructor or students must cable and configure the perimeter routers in addition to the wired LAN. The routers Ethernet interfaces must be configured and enabled. Static routing should be configured on the routers. Ensure that the devices are configured according to the topology. The bridge devices should be configured as follows:

Device Name	Label	SSID	Address
BPod1	BR1	BR1	192.168.1.3/24
BPod2	BR2	BR1	192.168.1.4/24

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco 1310s with 2.4dBi dipole antenna(s)
- Two dual Ethernet routers
- Two switches or hubs(optional)

Step 1 Connect and reset both bridges

Connect to the bridge via the console connection and reset the bridge to factory default settings. Refer to a previous lab if you are unsure how to do this.

Step 2 Connect to the bridge web interface

From the wired PC, open a web browser and navigate to the default IP address of the bridge. Remember that the default factory settings are:

a. IP address: 10.0.0.1

b. Username: Cisco

c. Password: Cisco

Step 3 Configure the bridge settings

Using both the Express Set-up and Express Security pages, configure the bridge with the following settings:

Parameter	BPod1	BPod2
• System Name:	***BPod1***	***BPod2***
• Configuration Server Protocol:	***Static IP***	***Static IP***
• IP address:	***192.168.1.3***	***192.168.1.4***
• Subnet Mask:	***255.255.255.0***	***255.255.255.0***
• Default Gateway:	***192.168.1.1***	***192.168.1.2***
• Service Set ID:	***BR1***	***BR1***
• Role in Radio Network:	***Root Bridge***	***Non-Root Bridge***

Click Apply. The connection will drop.

Step 4 Cable and configure the routers and PCs

Using dual Ethernet routers, such as an 806, 2514, or equivalent. Configure both routers with the following commands:

```
hostname Router1
int fa0/0
 ip address 192.168.1.1 255.255.255.0
 description outside
 no shut
!
int fa0/1
 ip address 10.0.1.1 255.255.255.0
 description inside
 no shut
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
line vty 0 4
 password cisco
 login
```

```
hostname Router2
int fa0/0
 ip address 192.168.1.2 255.255.255.0
 description outside
 no shut
!
int fa0/1
 ip address 10.0.2.1 255.255.255.0
 description inside
 no shut
!
router eigrp 1
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
line vty 0 4
 password cisco
 login
```

a. Configure the PCs:

PC1 with an IP address of 10.0.1.10/24.
PC2 with an IP address of 10.0.2.10/24

b. Reconnect using the browser. Enter 10.0.P.1 and connect.

c. Verify the settings.

1. What other routing method can be used instead of EIGRP?

_____

_____

2. Can static routes be used? If so, what is the advantage/disadvantage?

_____

_____

Step 5 Advanced Radio settings for the non-root bridge

a. From the left navigation bar, select **Network Interfaces>Radio0 802.11G** and then the **Settings** tab.

b. Enter the MAC address of the Root Bridge radio into the **Root Parent MAC 1:** field. Remember to use the MAC address of the root bridge radio.

c. Click the **Apply** button to apply the settings.

d. Go to the **Association** page of the Root Bridge.

Ensure that the non-root bridge appears in the root bridge association table before continuing to test the connection.

Step 7 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices on this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, conduct each of the following tests:

- Ping from PC1 to Router 1 inside Ethernet port
- Ping to Router1 outside port
- Ping from PC1 to BPod2
- Ping from PC1 to Router2 outside port
- Ping from PC1 to Router2 inside port
- Ping from PC1 to PC2

b. Test layer 7 connectivity by browsing to BPod2 from PC1.

Lab 7.1.4 Antenna Setup

Estimated Time: 15 Minutes

Number of Team Members: Students will work in teams of two.

Objective

This lab will introduce the user to the Cisco Aironet AP antenna configuration.

Scenario

An antenna is used to radiate transmitted signals and/or capture received signals. Different antenna components have different ranges and capability in the area of signal they radiate. Placement of the antenna can have different effects on the range or the ability of the AP to transmit and receive the radio wave signals.

Cisco antennas use a Reverse Polarity Threaded Navy Connector (RP-TNC). This connector looks like a TNC, but the center contacts have been reversed. This prohibits a standard off-the-shelf antenna from being attached to a Cisco RF product. The U.S Federal Communication Commission (FCC) requires vendors to use non-standard connectors to prevent accidental connections to wireless equipment.

Preparation

Prior to the lab, the student should have a Cisco Aironet AP configured as a root unit and performing properly. The student will also need a laptop computer with a Cisco Aironet client adapter and the utilities installed and performing properly.

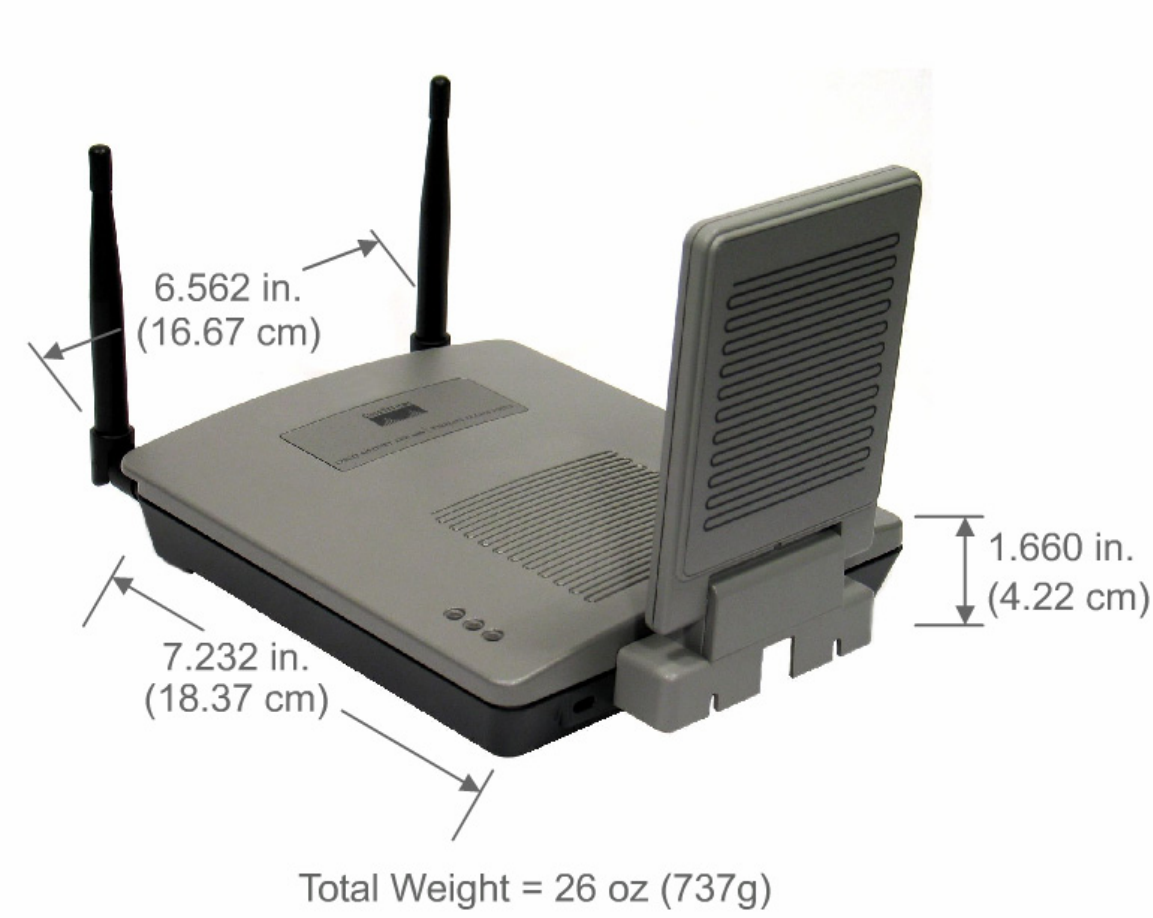
The students will perform some online Internet research and will require a computer with Internet access.

Tools and Resources

Each team will require the following:

- Cisco Aironet AP with two standard antennas
- Laptop Personal Computer with a client adapter and client utility properly installed
- Cisco Aironet Antenna components to be tested

Step 1 Antenna orientation of the AP



a. In order to set up the Cisco Aironet antenna, complete the following steps:

b. Note the image of the Aironet AP1200 series AP.

c. Note the Dual RP-TNC connectors on the AP. The right antenna coupling is the coupling on the right when looking at the AP back panel.

1. What does RP-TNC stand for?

_____

2. What is Vertical Polarization?

_____

_____

3. Define antenna beam width.

_____

_____

4. Define antenna bandwidth.

_____

_____

Step 2 Aironet AP1200 AP with dipole antennas

a. Note the image of the Aironet AP1200 Access Point with the standard dipole antennas.

b. The orientation of the antenna will be important if the standard dipole antennas are not used. When in diversity mode, the AP uses either the left or right antenna, but not both. Which antena it uses depends on the signal strength. When an optional antenna is used, the antenna receive and transmit setting will have to be changed to one side, which is either the left or right.

c. The Cisco part number for the pictured antenna is CISCO AIR-ANT4941. Do some online research and obtain the following information on this part:

   http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008009228 5.html

   An additional reference can be found at the following link:
   http://www.cisco.com/univercd/cc/td/doc/product/wireless/acessory/4941.pdf

   1. Gain (in dBi)

      _____

   2. Frequency range

      _____

   3. What is the part number for the Cisco lightning arrestor?

      _____

   4. What does the Cisco lightning arrestor do?

      _____

   5. What is the gain of Cisco part number CISCO AIR-ANT1949?

      _____

Lab 7.1.8.1 Configure AP Diversity Settings

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two.

Objective

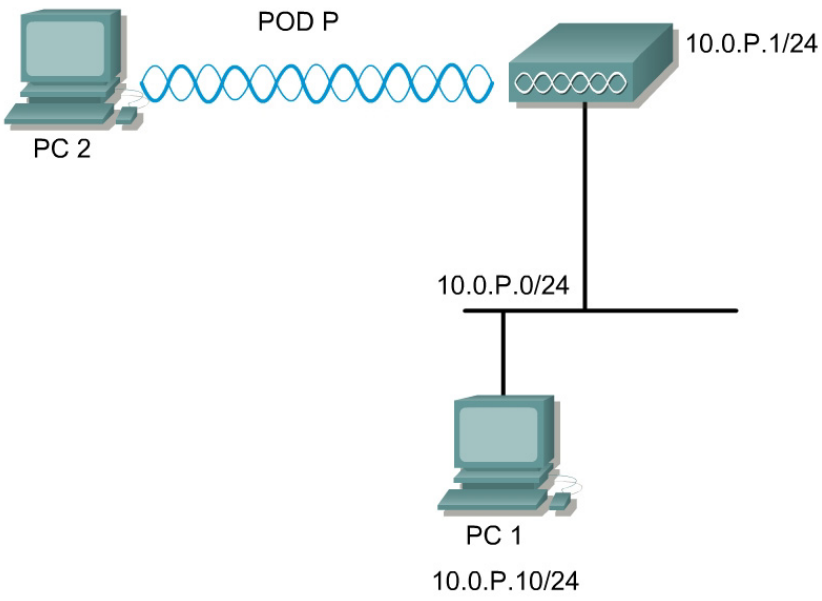
The student will test the effects of various antenna diversity settings on the Cisco Aironet AP. The student will configure the AP radio antennas through GUI and IOS command line.

Scenario

APs have two RP-TNC connectors. These two antennas connectors are for diversity in signal reception, and their purpose is not to increase coverage. They help eliminate the null path and RF being received out of phase. Only one antenna at a time is active.

Which antenna is active is selected on a per-client basis for optimal signal and only applies to that specific client. The AP can hop back and forth between antennas when talking to different clients. PCMCIA cards also have antenna diversity built into the card.

Topology



Preparation

Cisco Aironet AP configured as a root unit and performing properly.

PCs with a properly installed Cisco Aironet client adapter and ACU utility.

Tools and Resources or Equipment

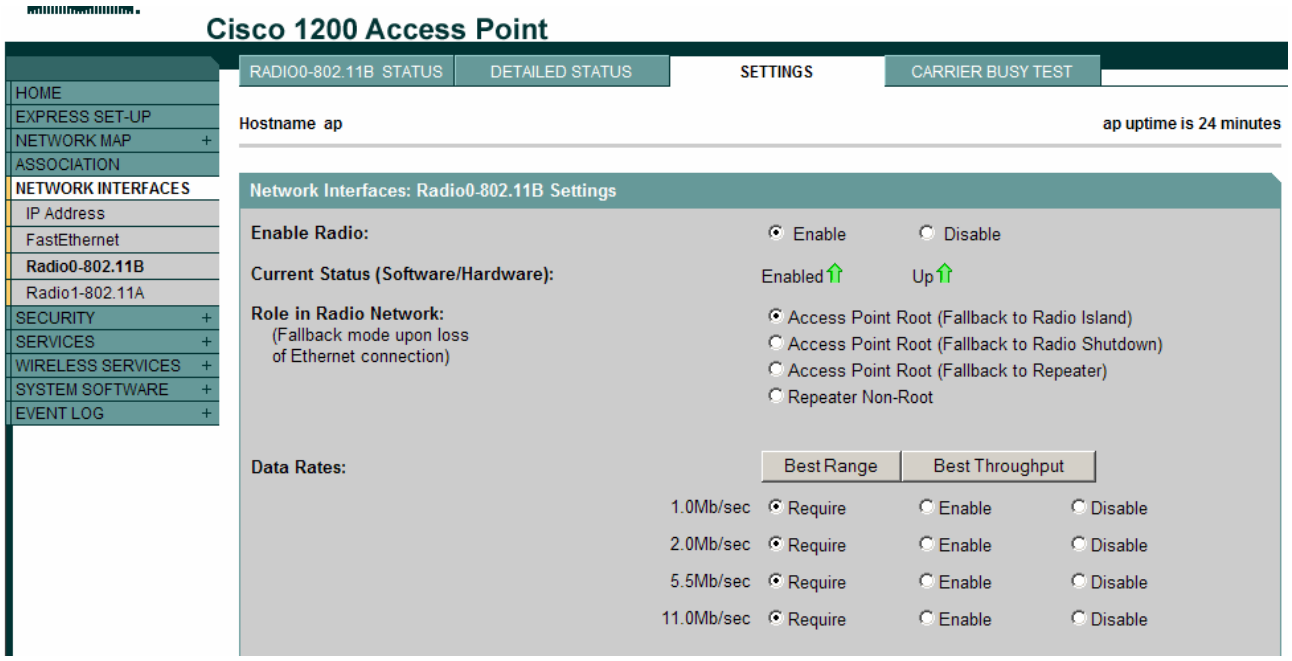
- One AP
- One wired PC or Laptop
- One wireless Laptop or PC with a client adapter properly installed

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
`configure terminal`	enter global configuration mode
`interface dot11radio 0`	enter the device radio interface
`antenna`	set the receive or transmit antenna

Step 1 Configure the Cisco Aironet antenna settings



a. Open a web browser and type the IP address of the AP in the browser address box.

b. Go to the **Radio0-802.11B** Settings page of the AP.

c. Record the following information:

1. Enable Radio Setting:

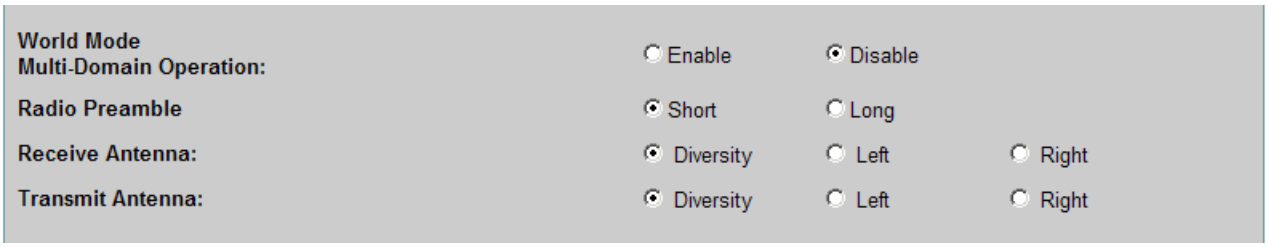
   _____

2. Role in Radio Network

   _____

3. Default Radio Channel

   _____

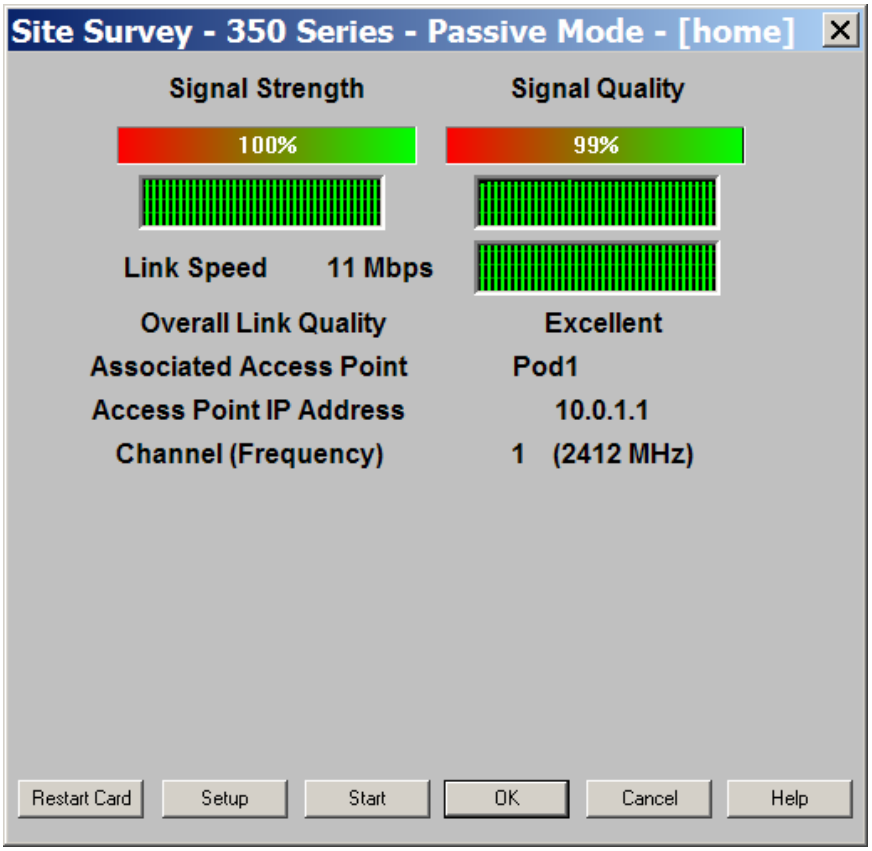


Step 2 Antenna settings

a. On the middle of the **AP Radio Hardware** page are the selections for the **Receive Antenna** and one for the **Transmit Antenna**.

b. Record the Receive Antenna Setting: _____

c. Record the Transmit Antenna Setting: _____



Step 3 Change antenna settings

a. Before making any changes to the antenna settings, open the Site Survey utility on the PC. Note the Signal Quality and Signal Strength before any changes are made.

b. What is the current Signal Strength? ____

c. What is the current Signal Strength? ____

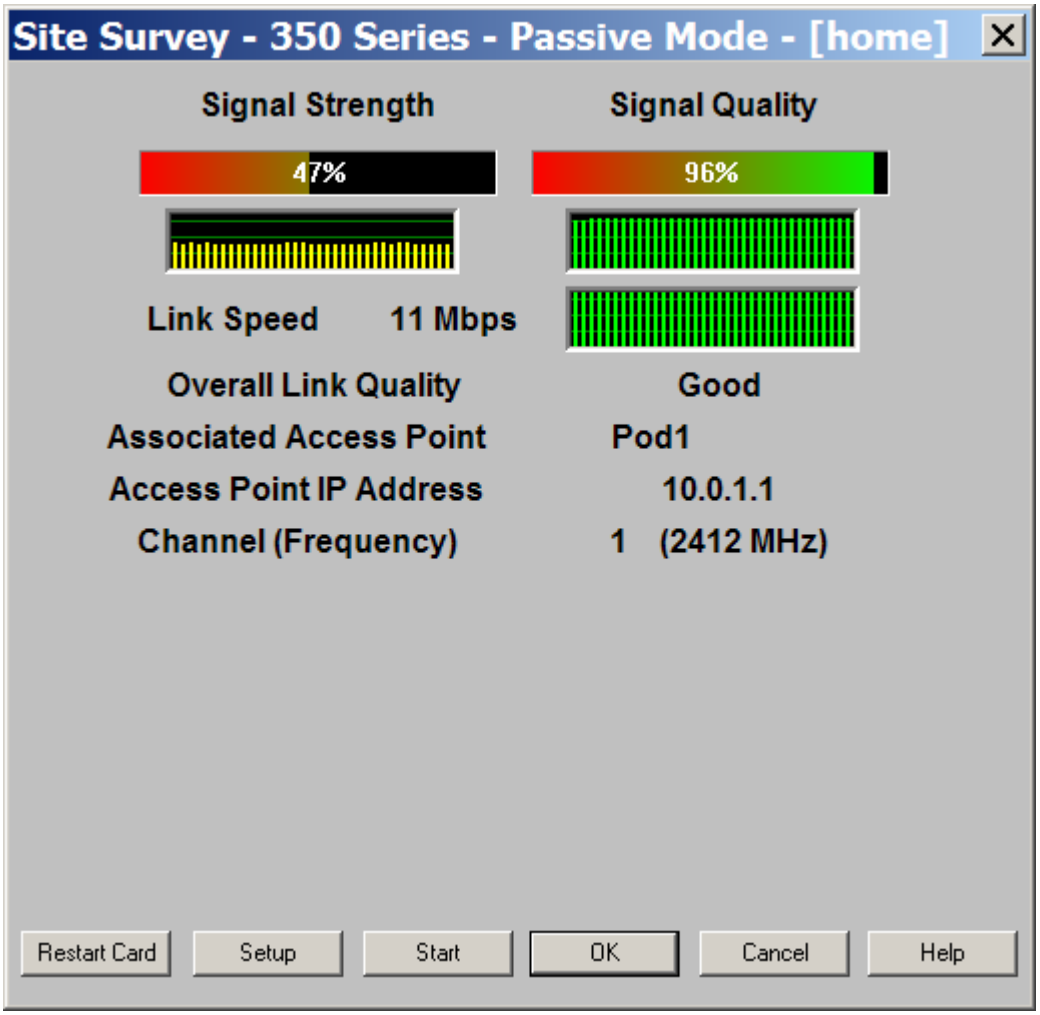
Step 4 Change antenna settings (continued)

a. Is it necessary to physically remove the antennas to change the antenna settings?

_____

b. Change the Receive and Transmit antenna settings to left, right, diversity or various combinations and note any changes on the Site Survey Meter once the changes are applied.

c. If using only one antenna, the Receive and Transmit antenna settings will have to correspond to the proper AP antenna setting for RF reception.



If you are using two standard dipole antennas, very little changes will be effected on the Site Survey Meter. If you remove one of the antennas, you will observe a more dramatic effect in the setting changes. Make numerous changes with the antenna settings and check the results with the PC Aironet Client Site Survey utility. Remember to only make one change at a time so that you have a good idea which setting change caused the effect.

d. Which antenna setting gave the strongest signal quality (Left, Right, or Diversity)?

_____

e. Which antenna setting gave the strongest signal strength (Left, Right, or Diversity)?

_____

f. Which setting gave the weakest signal strength (Left, Right, or Diversity)?

_____

g. Which setting gave the weakest signal quality (Left, Right, or Diversity)?

_____

Step 5 Configure the 802.11b antenna using the IOS CLI

This section describes how to configure the AP radio antennas using the IOS command line.

Command List:

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
configure terminal	enter global configuration mode
interface dot11radio 0	enter the device radio interface
antenna	set the receive or transmit antenna

Follow these steps to set the AP receive and transmit to right:

```
PodP(config)#interface dot11radio 0
PodP(config-if)#antenna receive right
PodP(config-if)#antenna transmit right
PodP(config-if)#
```

Follow these steps to set the AP receive and transmit to left:

```
PodP(config)#interface dot11radio 0
PodP(config-if)#antenna receive left
PodP(config-if)#antenna transmit left
PodP(config-if)#
```

Follow these steps to set the AP receive and transmit to diversity:

```
PodP(config)#interface dot11radio 0
PodP(config-if)#antenna receive diversity
PodP(config-if)#antenna transmit diversity
PodP(config-if)#
```

Step 6 Configure 802.11a antenna using the IOS CLI (optional)

Repeat Step 5 for the 802.11a radio

Lab 7.1.8.2 Configure Bridge Diversity Settings

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two.

Objective

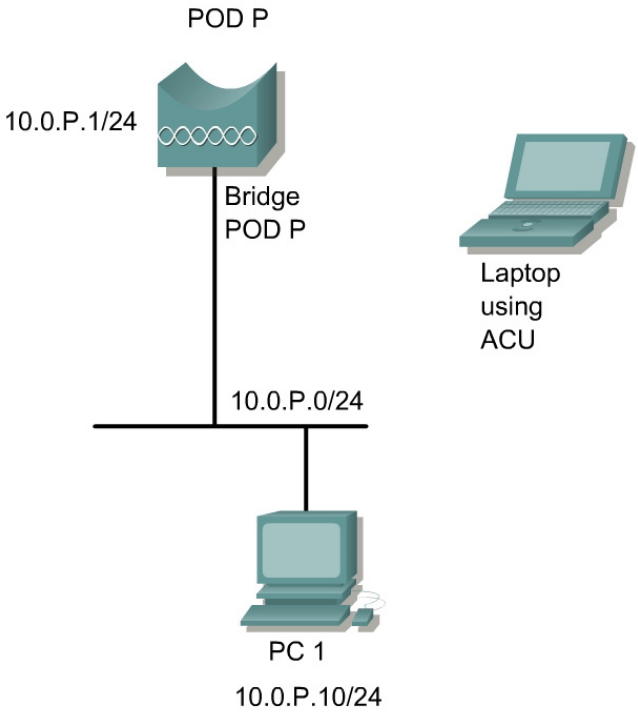
The student will test the effects of various antenna diversity settings on the Cisco BR350

Scenario

Bridges have two RP-TNC connectors attached them. These two antennas connectors are for diversity in signal reception, and their purpose is not to increase coverage or distance. They help eliminate the null path and RF being received out of phase. Only one antenna at a time is active.

Which antenna is active is selected on a per-client basis for optimal signal and only applies to that specific client. The bridge can hop back and forth between antennas when talking to different clients. This can be useful in a point to multipoint installation.

Topology



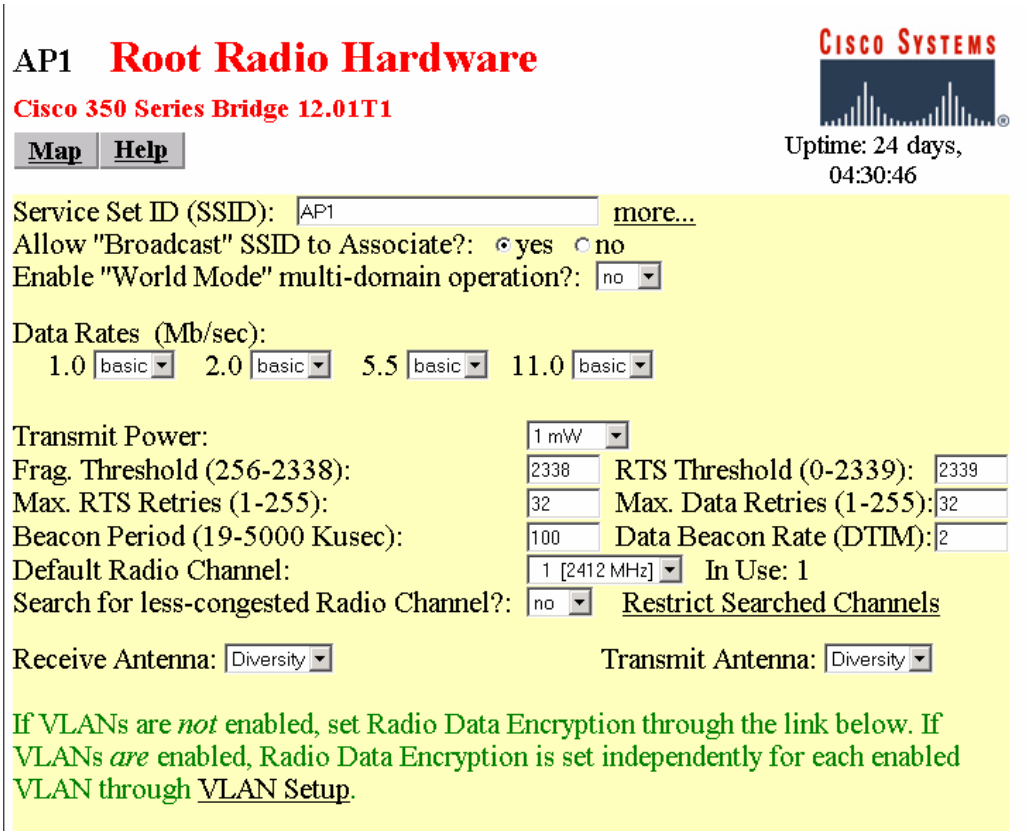
Preparation

Cisco BR350 configured as a root unit and performing properly.

Computers with a properly installed Cisco Aironet client adapter and utility.

Tools and Resources or Equipment

- Cisco BR350
- Laptop or PC with a client adapter properly installed



Step 1 Configure the Cisco Aironet antenna settings

a. Open a web browser and type the IP address of the bridge in the browser address box.

b. Go to the Root Radio Hardware page of the bridge.

c. Record the following information:

1. Service Set ID

_____

2. Transmit Power

_____

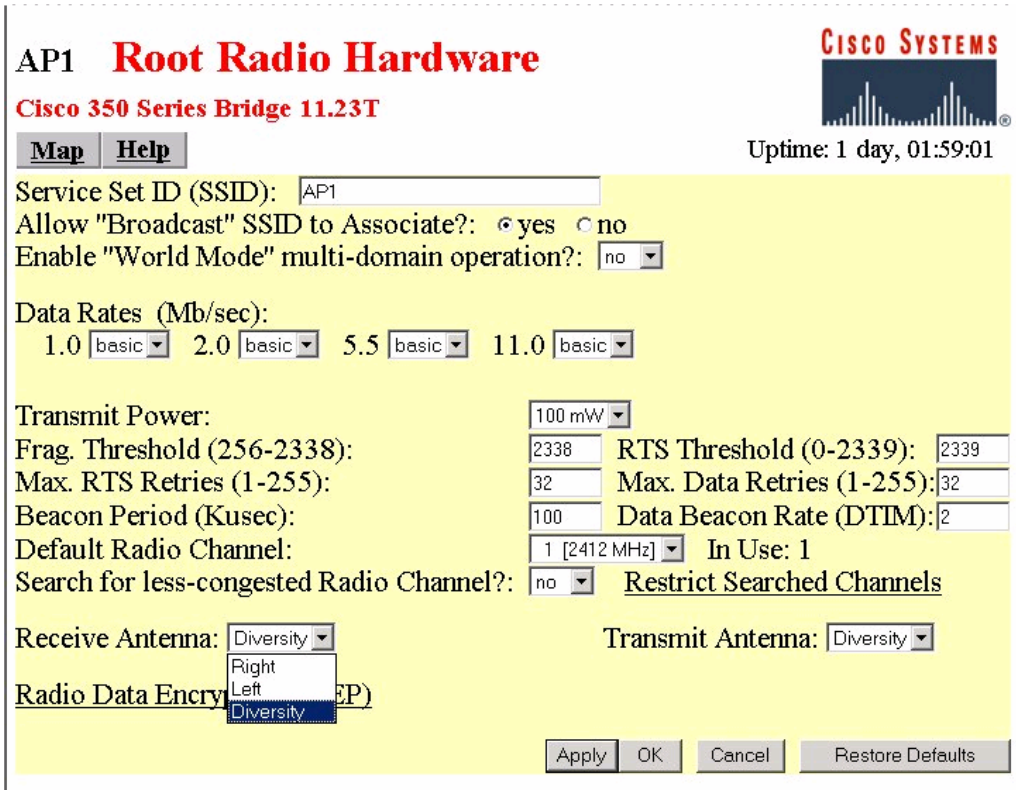
3. Default Radio Channel

_____

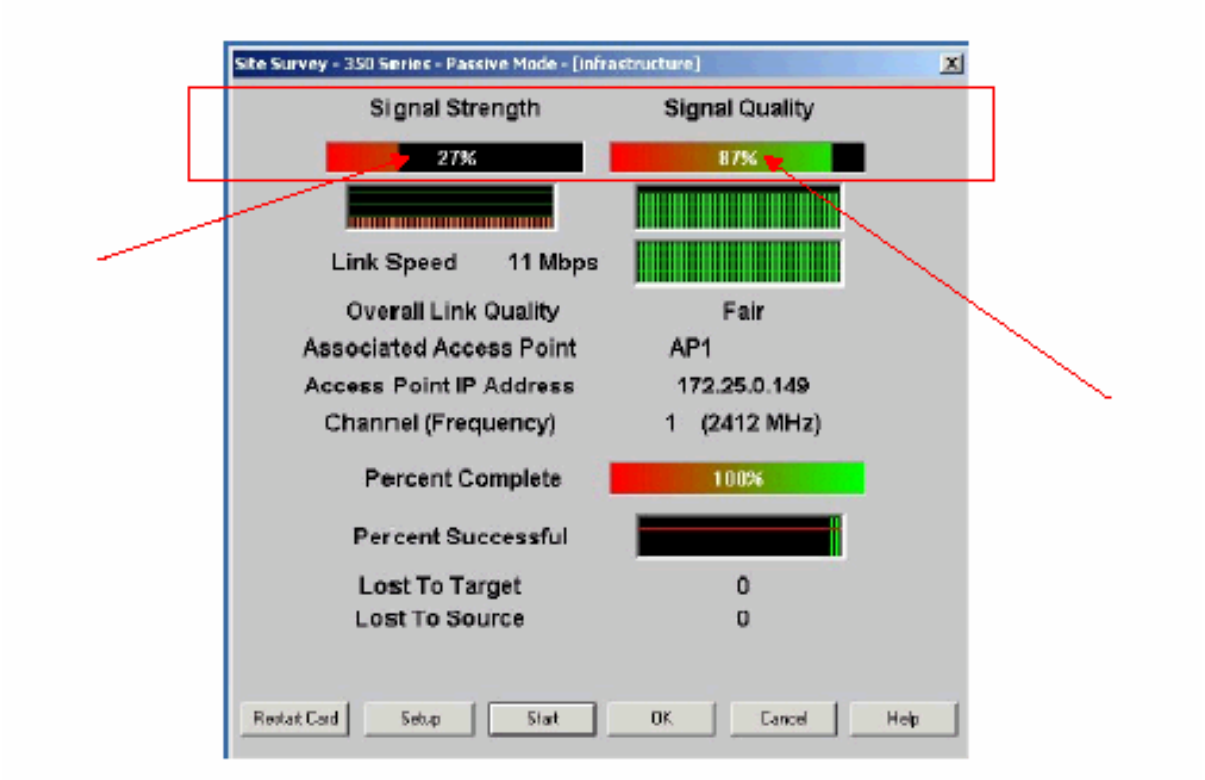
4. Search for less congested channel

_____

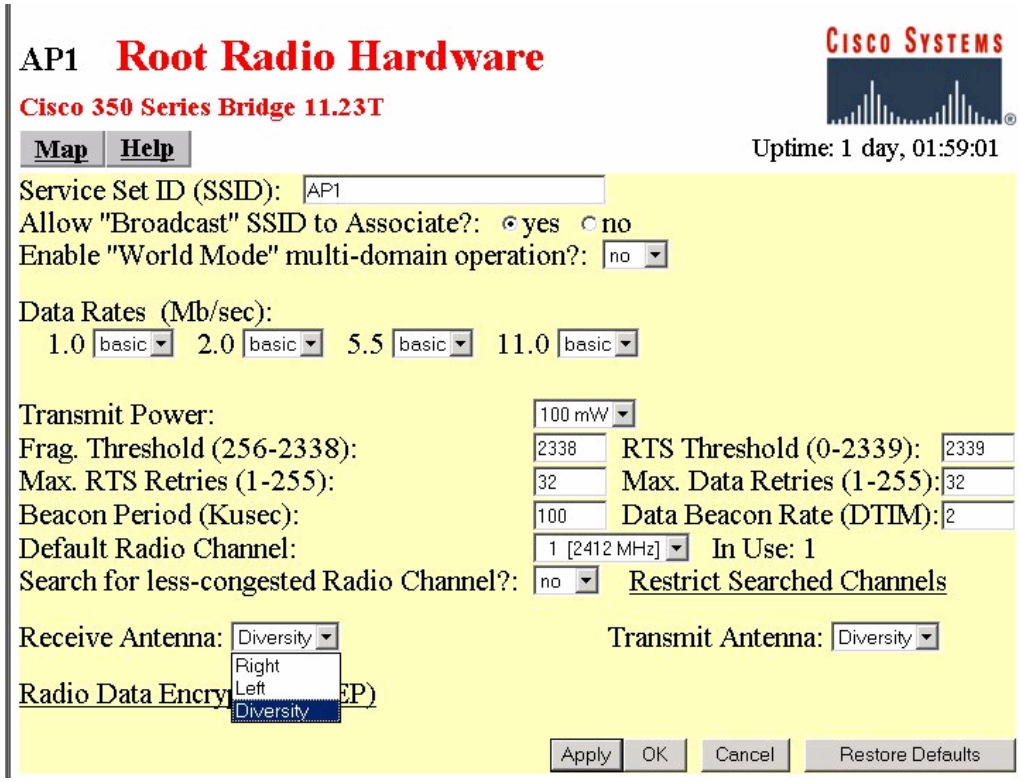
For this lab, keep this setting on NO. Both antenna settings should be set to diversity at this time.



Located near the bottom of the **Radio Hardware** page, you will see two Pull down selection menu boxes, one for the **Receive Antenna** and one for the **Transmit Antenna**.



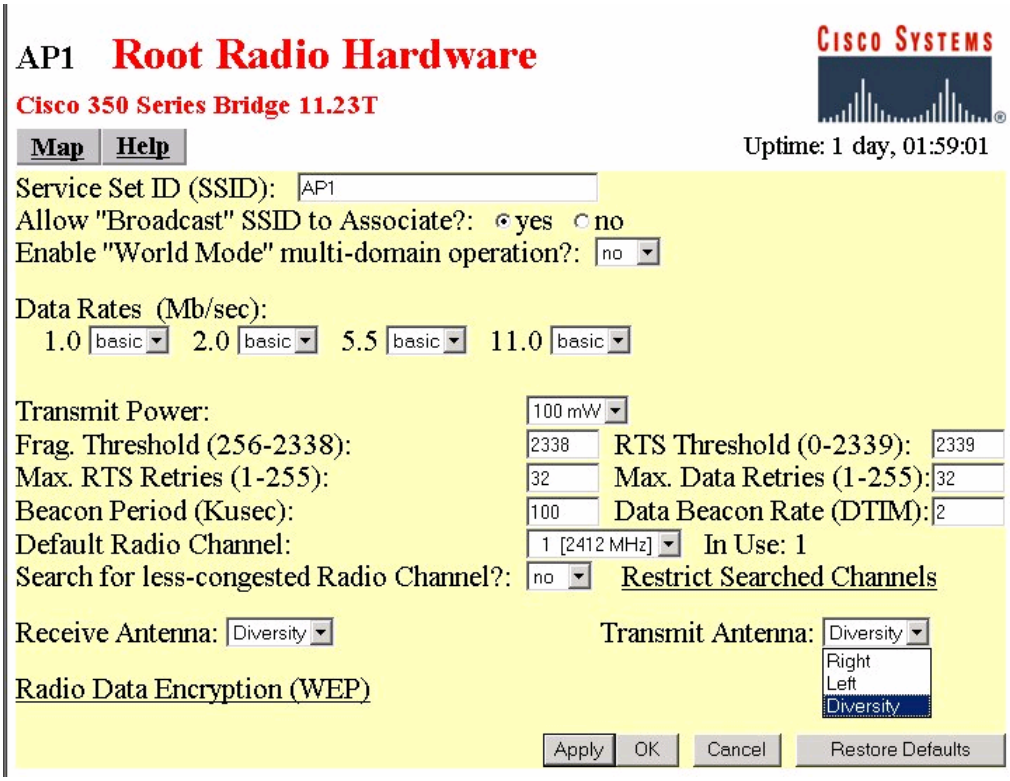
Before making any changes to the antenna settings, open the Site Survey utility on the PC. Note the Signal Quality and Signal Strength before any changes are made.



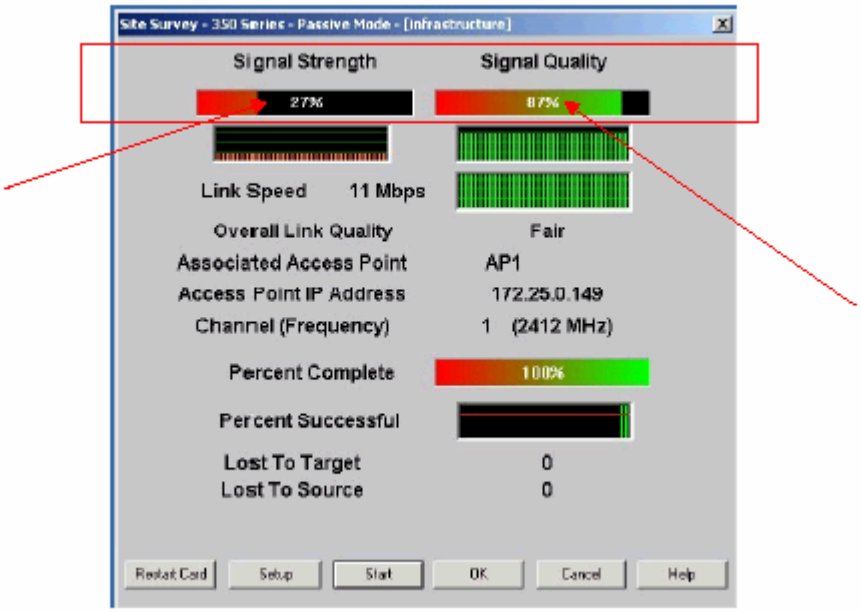
Change the Receive and Transmit antenna settings to left, right, diversity or various combinations and note any changes on the Site Survey Meter once you have applied the changes.

d. Is it actually necessary for you to physically remove the antennas?

_____



If using only one antenna, the Receive and Transmit antenna settings will have to correspond to the proper bridge antenna setting for RF reception.



If using two standard dipole antennas, very little changes will be effected on the Site Survey Meter. If you remove one of the antennas, you will observe a more dramatic effect in the setting changes. Make numerous changes with the antenna settings and check the results with the PC Aironet Client Site Survey utility. Remember to only make one change at a time so that you have a good idea which setting change caused the effect.

e. Which antenna setting gave the strongest signal quality (Left, Right, or Diversity)?

_____

f. Which antenna setting gave the strongest signal strength (Left, Right, or Diversity)?

_____

g. Which setting gave the weakest signal strength (Left, Right, or Diversity)?

_____

h. Which setting gave the weakest signal quality (Left, Right, or Diversity)?

_____

Lab 7.1.8.3 BR1310 Configure Bridge Diversity Settings

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two.

Objective

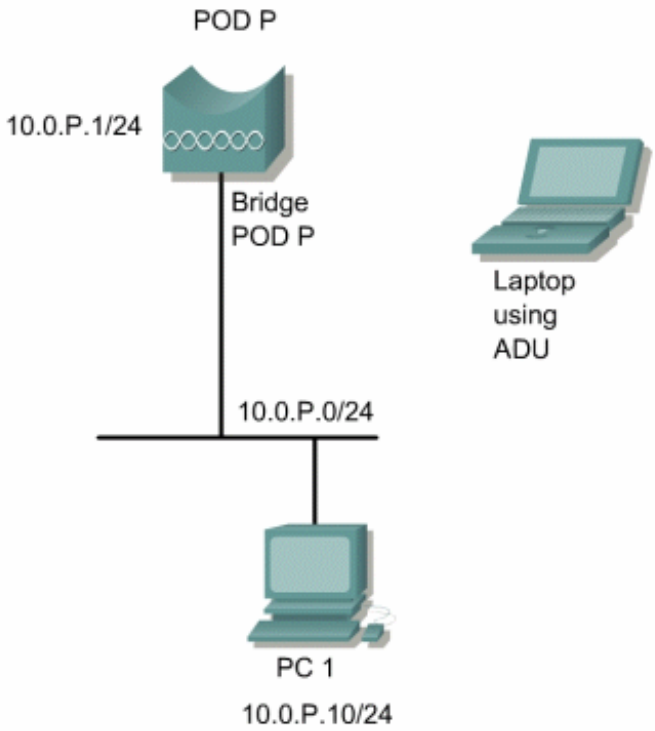
The student will test the effects of various antenna diversity settings on the Cisco BR1310

Scenario

Bridges have two RP-TNC connectors attached them. These two antennas connectors are for diversity in signal reception, and their purpose is not to increase coverage or distance. They help eliminate the null path and RF being received out of phase. Only one antenna at a time is active.

Which antenna is active is selected on a per-client basis for optimal signal and only applies to that specific client. The bridge can hop back and forth between antennas when talking to different clients. This can be useful in a point to multipoint installation.

Topology



Preparation

Cisco BR1310 configured as a root unit and performing properly.

Computers with a properly installed Cisco Aironet client adapter and utility.

Tools and Resources or Equipment

- Cisco BR1310
- Laptop or PC with a client adapter properly installed

Step 1 Configure the Cisco Aironet antenna settings

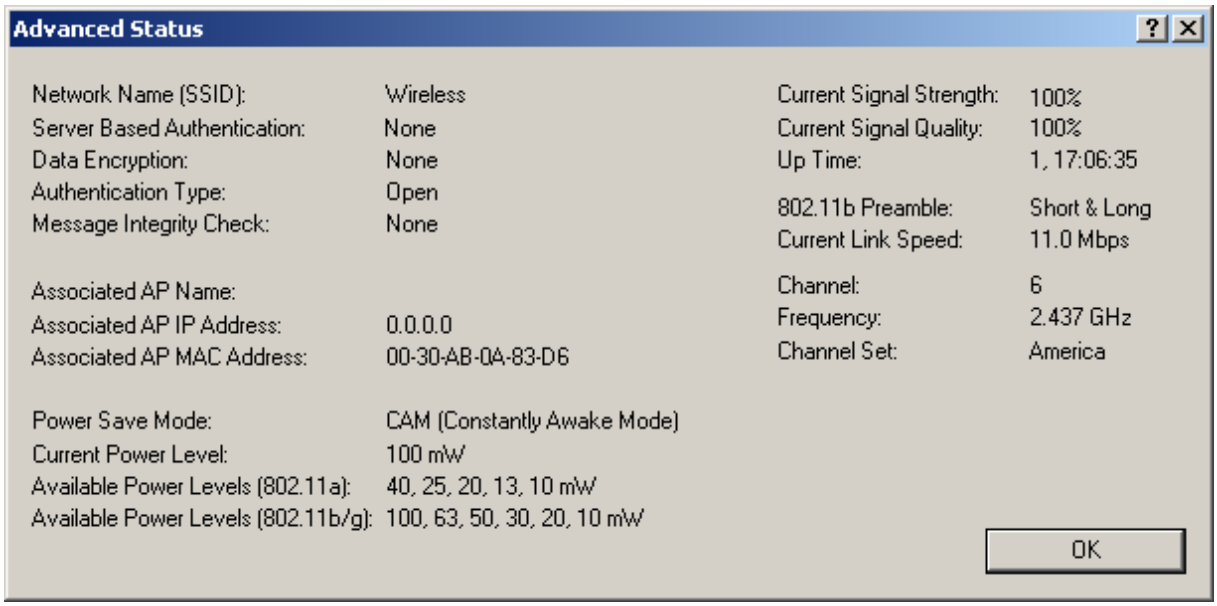
a. Open a web browser and type the IP address of the bridge in the browser address box. When prompted for the username and password enter the defaults or the username and password provided by your instructor.

b. Go to the **Network Interfaces>Radio0-802.11G>Settings** page and select the current channel as the default. The current channel will be displayed to the right of the drop down box. Click **Apply** to save the changes.

Note: if multiple bridge units are operating within the classroom it is important that they use different channels.

c. Scroll down to the Receive and Transmit Antenna section. Both the Receive and Transmit Antennas should be set to Diversity by default.

d. Before making any changes to the antenna settings, open the Aironet Desktop Utility on the PC. From the Current Status tab, click the **Advanced** button and note the Signal Quality and Signal Strength before any changes are made. The quality and strength will be updated continuously if the Advanced Status window is left open.



e. Change the Receive and Transmit antenna settings to left, right, diversity or various combinations and note any changes in the Signal Strength or Signal Quality once you have applied the changes.

1. Is it actually necessary for you to physically remove the antennas?

_____

If using only one antenna, the Receive and Transmit antenna settings will have to correspond to the proper bridge antenna setting for RF reception.

If using two standard dipole antennas, very little changes will be effected on the Site Survey Meter. If you remove one of the antennas, you will observe a more dramatic effect in the setting changes. Make numerous changes with the antenna settings and check the results with the PC Aironet Client Site Survey utility. Remember to only make one change at a time so that you have a good idea which setting change caused the effect.

1. Which antenna setting gave the strongest signal quality (Left, Right, or Diversity)?

   _____

2. Which antenna setting gave the strongest signal strength (Left, Right, or Diversity)?

   _____

3. Which setting gave the weakest signal strength (Left, Right, or Diversity)?

   _____

4. Which setting gave the weakest signal quality (Left, Right, or Diversity)?

   _____

Lab 7.2.6 Omnidirectional Antennas

Estimated Time: 15 Minutes

Number of Team Members: Students will work in teams of two.

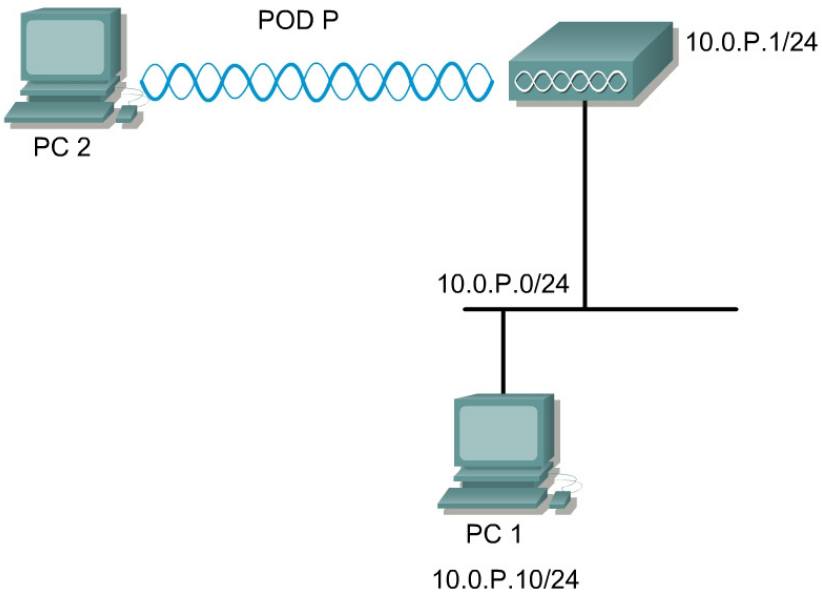
Objective

Test the range capabilities of the Cisco Aironet AP with an omni-directional antenna configuration.

Scenario

Omni-directional antennas create more coverage area away from the antenna in all directions, but the energy level directly below the antenna will become lower. Omni-directional antennas are generally used for point-to-multipoint implementations.

Topology



Preparation

Prior to the lab, configure a Cisco Aironet AP as a root unit and ensure it is performing properly. Obtain a laptop computer with a Cisco Aironet client adapter and the utilities installed.

Tools and Resources or Equipment

Each team will require the following:

- Cisco Aironet AP installed with Cisco Aironet AIR-ANT4941 2.2 dBi dipole antenna.
- Personal Computer with a client adapter properly installed

Step 1 Omni-directional antenna

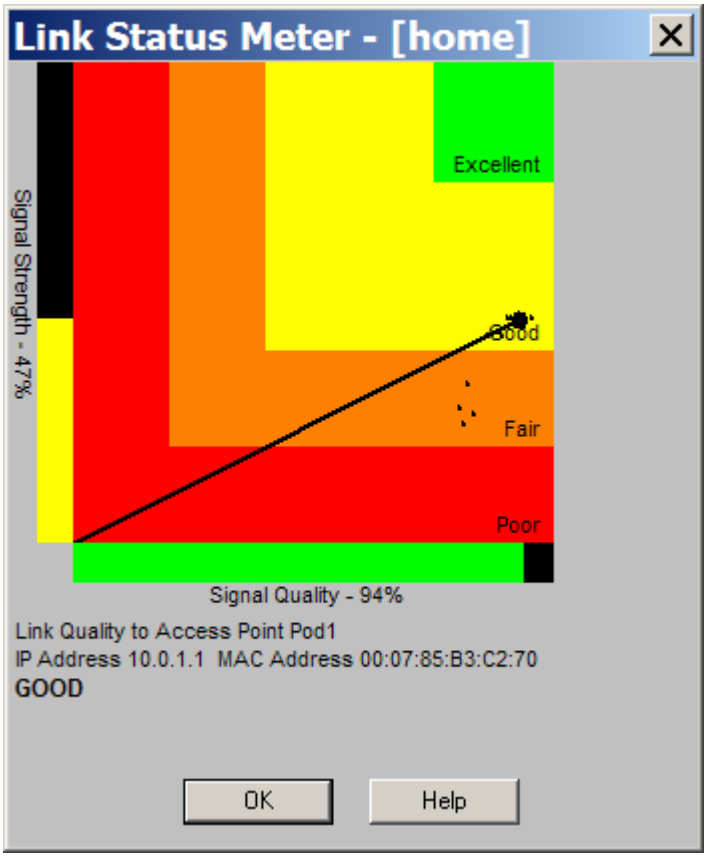
a. In order to set up the Cisco Aironet omni-directional antenna, complete the following steps:

b. The AP should be turned on and configured.

c. Open a Web browser and type in the AP IP address in the browser address box. This should bring up the AP Summary Status or home page.

Receive Antenna:	(•) Diversity	( ) Left	( ) Right
Transmit Antenna:	(•) Diversity	( ) Left	( ) Right

d. Check the Receive and Transmit mode of the antennas. Since two standard dipole antennas are being used on the AP, the Receive and Transmit antenna modes should be set to Diversity. This allows the AP to use the left or right antenna, depending on which is receiving the stronger signal.



e. Double click on the Link Status Meter (LSM) icon on the laptop and note the signal quality and signal strength meter.

f. Move the laptop computer around the room and possibly the building to note any changes in the Link Status Meter. This will give an indication of the coverage area afforded this particular antenna configuration.

g. This lab is using an omni-directional antenna and should generate a radio signal uniformly in all directions.

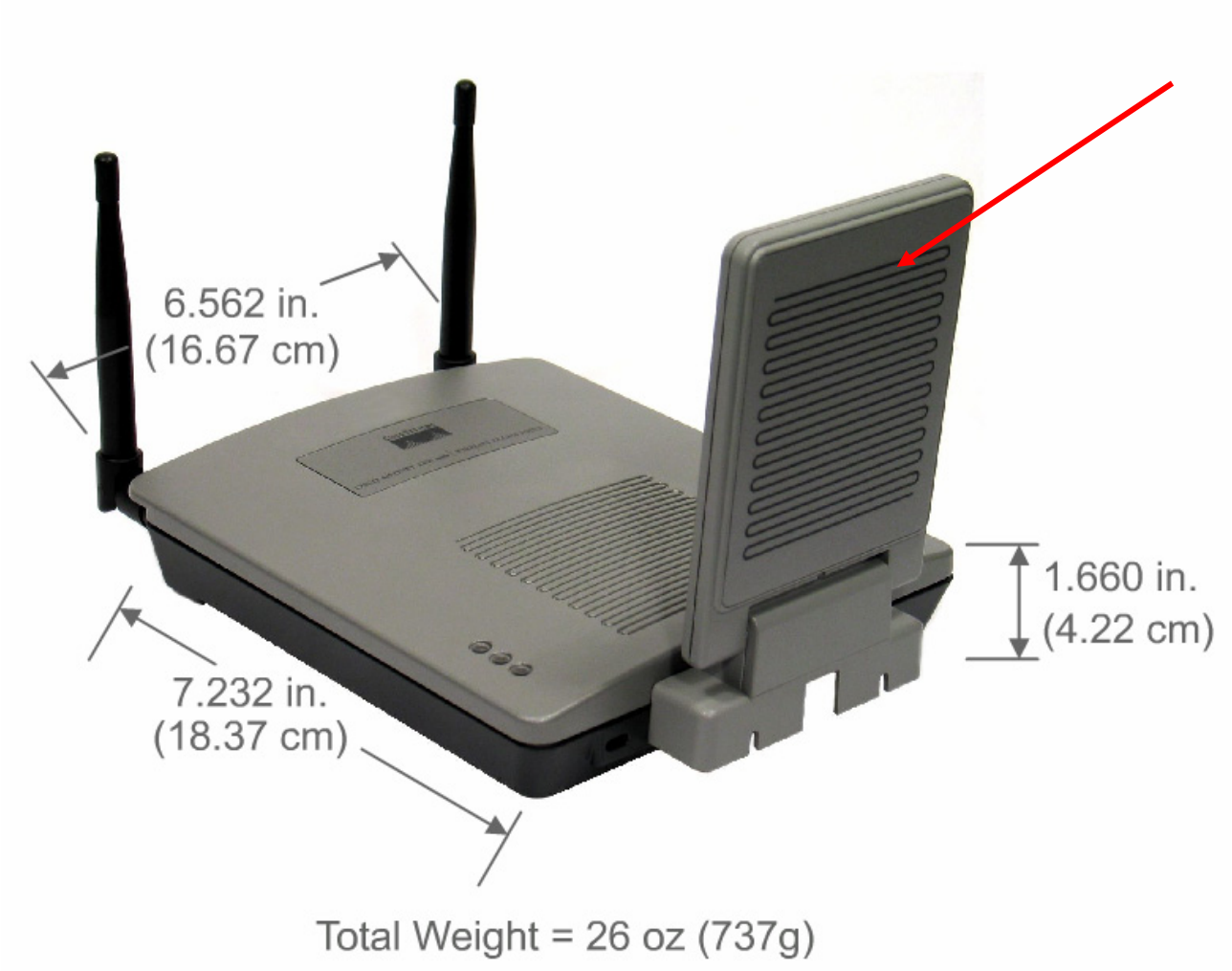
h. Approximately how far is the indoor range of the AP (Meters or Feet)?

_____

i. Experiment with changing the data rate on the AP. Were you able to extend your coverage range?

_____

Step 2 Omni-directional 5GHz patch (if available)



In order to set up the Cisco Aironet 5GHz Omni directional antenna, complete the following steps:

a. Flip up the patch antenna perpendicular to the Aironet AP1200.

b. The patch now operates in omni directional mode. The antenna is also dual diversity.

Lab 7.3.4 Directional Antennas

Estimated Time: 15 minutes

Number of Team Members: Students will work in groups of two students per team.

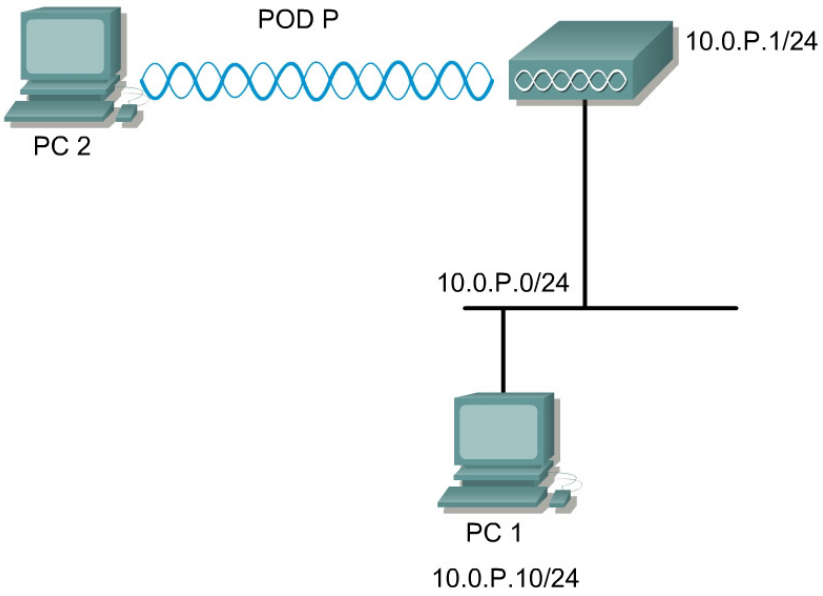
Objective

In this lab, students will test the range capabilities of the Cisco Aironet AP with a directional antenna configuration.

Scenario

Directional antennas will create a coverage area in a particular area caused by the condensed energy of the signal being pushed in a certain direction. Very little energy is in the backside of a directional antenna.

Topology



Preparation

Prior to the lab, the student should have a Cisco Aironet 1200 AP configured as a root unit and performing properly. A laptop computer is also needed with a Cisco Aironet 802.11a and a 802.11b client adapter and the utilities installed and performing properly.

Tools and Resources or Equipment

Each team will require the following:

- Cisco Aironet AP with the following:
  - Cisco Integrated 802.11a patch antenna for AP1200.
  - Laptop Personal Computer with a 802.11b client adapter properly installed
  - Cisco Aironet AIR-ANT1949 13.5 dBi Yagi Mast Mount antenna to be tested.(optional)

Step 1 Directional antenna (11a patch)

In order to set up the Cisco Aironet directional antenna, complete the following steps:

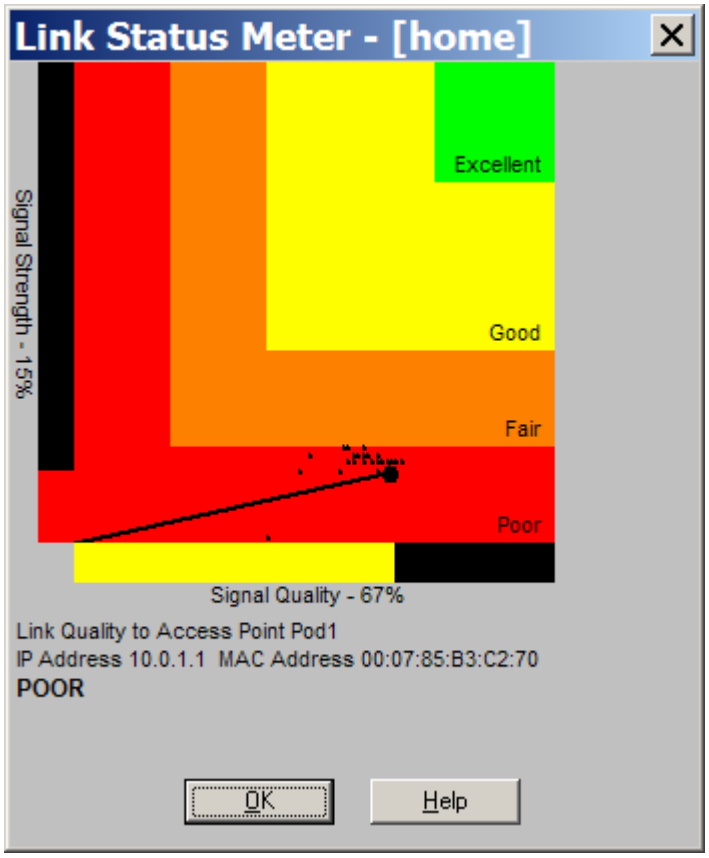
a. For Lab purposes, orient the Patch antenna by placing the antenna in the closed position, which is its directional polarization. The antenna should be pointing toward the area of coverage.

b. The AP can be turned on and configured.

c. Open a Web browser and type in the AP IP address in the browser address box.

d. Check the Receive and Transmit mode of the antenna on the AP **Radio0-802.11A** page.

e. When using the built in Patch antenna on the AP, the Receive and Transmit antenna modes should be set to **Diversity**. This allows the AP to use the both antennas for transmitting and receiving. Apply these settings.



f. On the PC, Double click on the Link Status Meter (LSM) icon on the laptop and note the Signal Quality and Signal Strength meter.

g. Move the laptop computer around the room and possibly the building to note any changes in the Link Status Meter. This will give an indication of the coverage area which is given to this particular antenna configuration.

h. Sketch the shape of the coverage of the antenna used. Show the AP and the PC client at their farthest distance.

i. What is the signal quality?

_____

j. What is the signal strength?

_____

Step 2 Yagi directional antenna (optional)

In order to set up the Cisco Aironet directional antenna, complete the following steps:

a. Turn the power off on the AP and unscrew both standard dipole antennas from the rear of the AP. Then install the Yagi Mast Mount antenna to the AP by screwing the antenna TNC connector to the AP right TNC connector.

b. For Lab purposes, orient the Yagi Mast Mount antenna by placing the antenna in a horizontal position, which is its polarization. The antenna should be pointing toward the area of coverage. Positioning of the Yagi Mast Mount is very important and affects the coverage area.

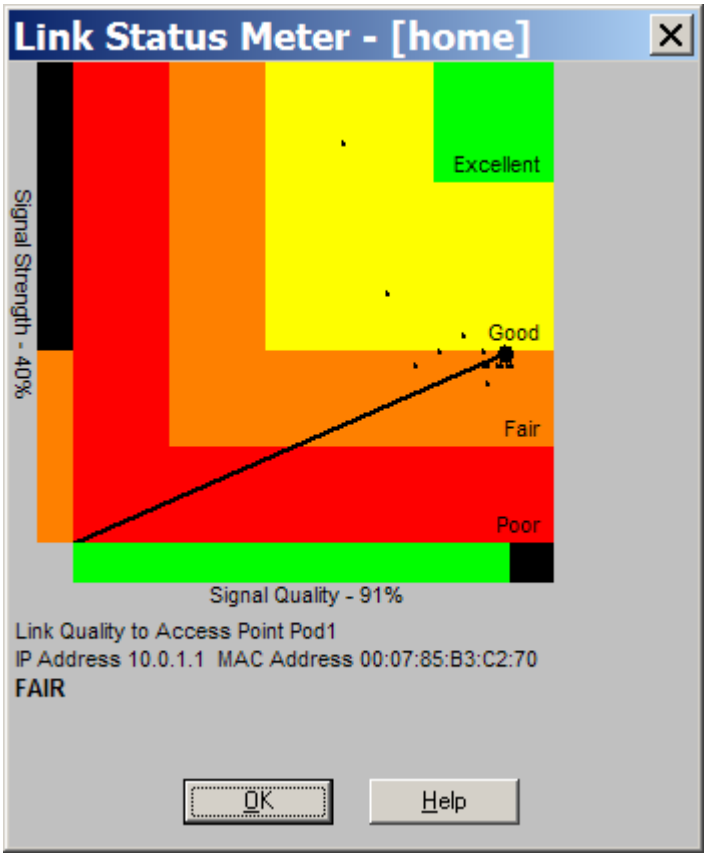
c. The AP can be turned on and configured.

d. Open a Web browser and type in the AP IP address in the browser address box.

e. Check the Receive and Transmit mode of the antenna on the AP **Radio0-802.11** page.

Receive Antenna:	(•) Diversity	( ) Left	( ) Right
Transmit Antenna:	(•) Diversity	( ) Left	( ) Right

f. When using a single Yagi Mast Mount antenna on the AP, the Receive and Transmit antenna modes should be set to **right**. This allows the AP to use the right antenna for transmitting and receiving. Apply these settings.



g. Double click on the Link Status Meter (LSM) icon on the laptop and note the Signal Quality and Signal Strength meter.

h. Move the laptop computer around the room and possibly the building to note any changes in the Link Status Meter. This will give an indication of the coverage area which is given to this particular antenna configuration.

i. Sketch the shape of the coverage of the antenna used. Show the AP and the PC client at their farthest distance.

j. What is the signal quality?

_____

k. What is the signal strength?

_____

Lab 8.2.4 Wireless Attacks and Countermeasures

Estimated Time: 25 minutes
Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will gain an understanding of the primary attack methods used to bypass conventional security measures on WLANs. Additionally, students will learn the countermeasures that can be implemented for security on a WLAN.

Scenario

Network security is the process by which digital information assets are protected. The goals of security are to maintain integrity, protect confidentiality, and assure availability.

This lab will focus on understanding wireless security concepts.

Preparation

The students will require access to the Internet for online research.

Tools and Resources

Each student team needs one PC with Internet access.

Step 1 Network security goals

Answer the following questions:

1. List the three primary goals of network security covered in FWL Module 8.

_____

_____

_____

2. Which of the goals refers to the assurance that data is not altered or destroyed?

_____

3. Which of the goals refers to the protection of data from unauthorized disclosure?

_____

4. Which of the goals refers to the continuous operation of the computing system?

_____

Step 2 Network security weaknesses

Answer the following questions:

a. List the three primary network security weaknesses covered in FWL Module 8.

_____

_____

_____

b. Which of the weaknesses refers to a lack of a written security policy?

_____

c. Which of the weaknesses refers to unsecured default settings?

_____

d. Which of the weaknesses refers to weak initialization vector, poor encryption and authentication schemes, and firewall holes?

_____

Step 3 Network security threats

Answer the following questions:

a. List the four basic network security threats covered in FWL Module 8.

_____

_____

_____

_____

Step 4 Attack methods

Answer the following questions:

a. List the three primary attack methods covered in FWL Module 8.

_____

_____

_____

b. Which of the attacks is occurring when the attacker now controls one system and can either deface the public Web presence or continue hacking for more interesting information?

_____

c. How is this attack performed? What tools are available?

_____

_____

_____

d. Which of the attacks is occurring when the attack results in obtaining address ranges, hosts, and services? In this case, the known servers and the firewall may or may not be detected.

_____

e. How is this attack performed? What tools are available?

_____

_____

_____

f. Which of the attacks is occurring when the attacker has disabled valid users from accessing the target network causing lost revenue, lost communications, and damaged software and hardware?

_____

g. How is this attack performed? What tools are available?

_____

_____

_____

Step 5 The security wheel

Answer the following questions:

a. List the four processes involved in building a secure network.

_____

_____

_____

_____

b. Which of the processes involve collecting and analyzing information from the monitoring and testing phases to make security improvements?

_____

c. Which of the processes involve monitoring the network for violations and attacks against the corporate security policy?

_____

d. Which of the processes involve testing the effectiveness of the security safeguards in place?

_____

e. Which of the processes involve implementing security devices, which include firewalls, identification authentication systems, and virtual private networks?

_____

f. What is at the center of the Wireless Security Wheel?

_____

Step 6 WLAN security technologies

Answer the following questions:

a. List the two first-generation security technologies covered in FWL Module 8.

_____

_____

b. Name the one that serves to logically segment the users and APs that form part of a wireless subsystem.

_____

c. Name the other that replaces the original data payload with the output of the encryption algorithm.

_____

d. What are the two types of authentication methods defined in IEEE 802.11?

_____

_____

e. What are the three elements of the association process?

_____

_____

_____

Lab 8.3.1.1 Configure Basic AP security through GUI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn the following objectives:

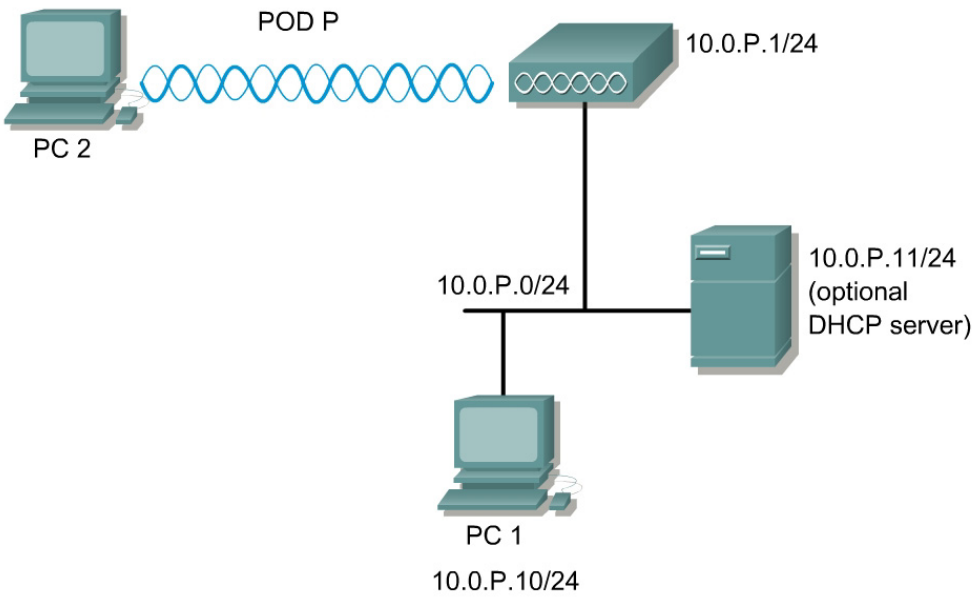
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
- Disable telnet and web (optional)

Scenario

Students will learn to secure the AP through GUI. The security policy of the company mandates all devices should be locked down according to minimum standards. Also, SSH must be used for remote management.

SSH is a program, similar to Telnet, which allows a network administrator to log into another computer over a network. SSH allows an administrator to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure networks. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

The instructor should have a working wired network. PC1 should be connected to the wired network. Prior to starting the lab, ensure that each host PC is loaded with a SSH client. There are numerous SSH clients available for free on the Internet. The lab was developed using the PuTTY SSH client.

Tools and Resources

Each team will need:

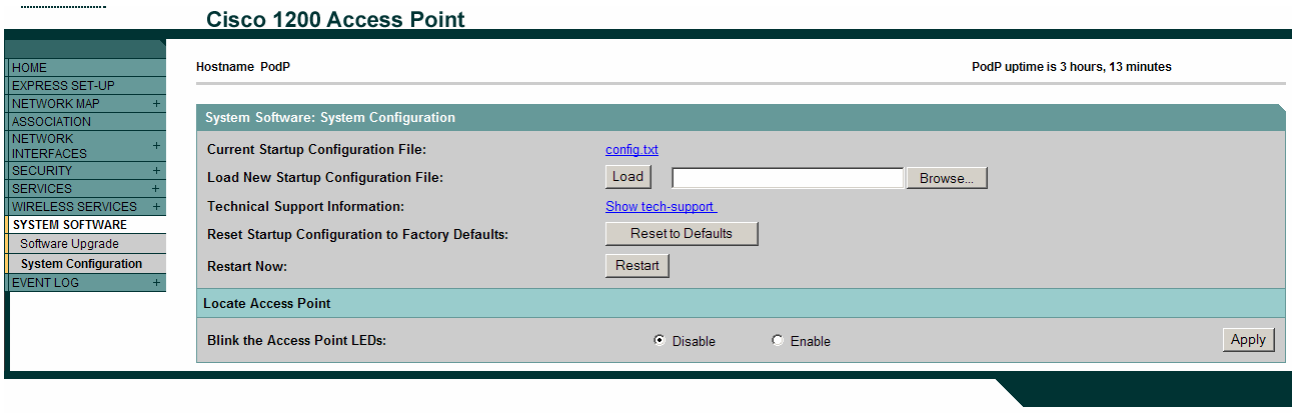
- AP
- PC or laptop
- Console cable
- SSH client software

Additional Materials:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

http://www.chiark.greenend.org.uk/~sgtatham/putty/

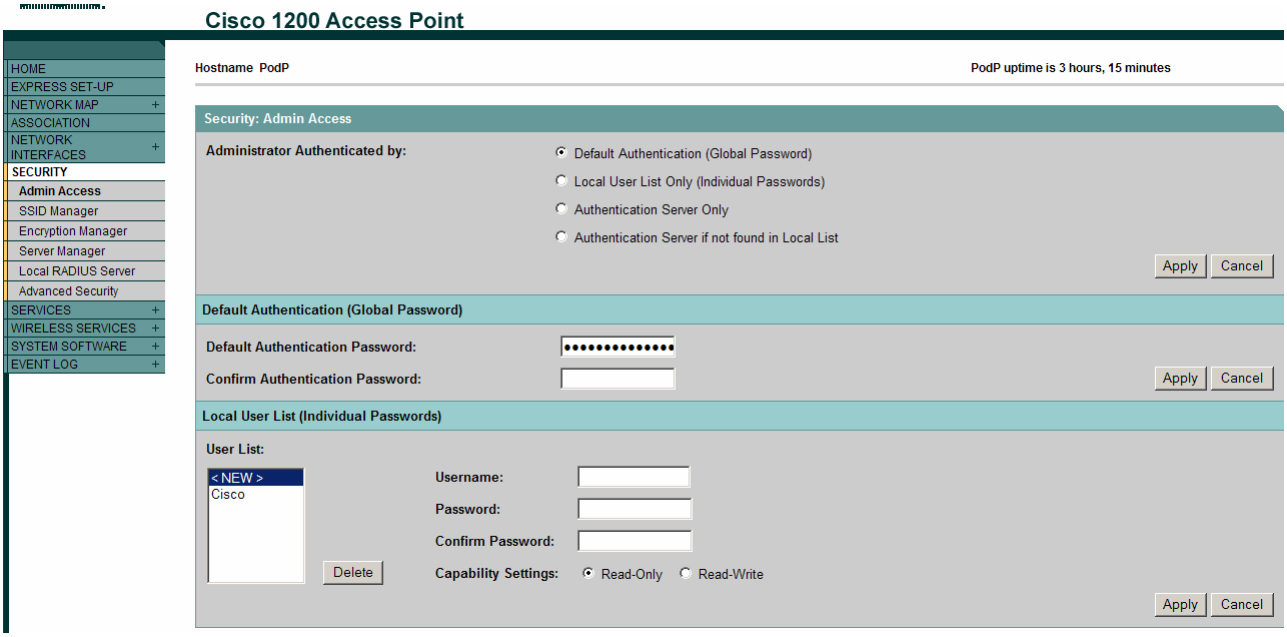
Step 1 Configure basic AP settings



a. If there is an existing configuration on the AP, erase the configuration and reload either through GUI or IOS CLI.

b. Configure the hostname, SSID, and BVI interface according to the Preparation table.

Step 2 Configure a new administrator account



One of the easiest ways for hackers to gain access to network devices is by using default usernames and passwords.

a. Configure a new administrator account from the **SECURITY>Admin Access** page. Give this user Read-Write privileges.

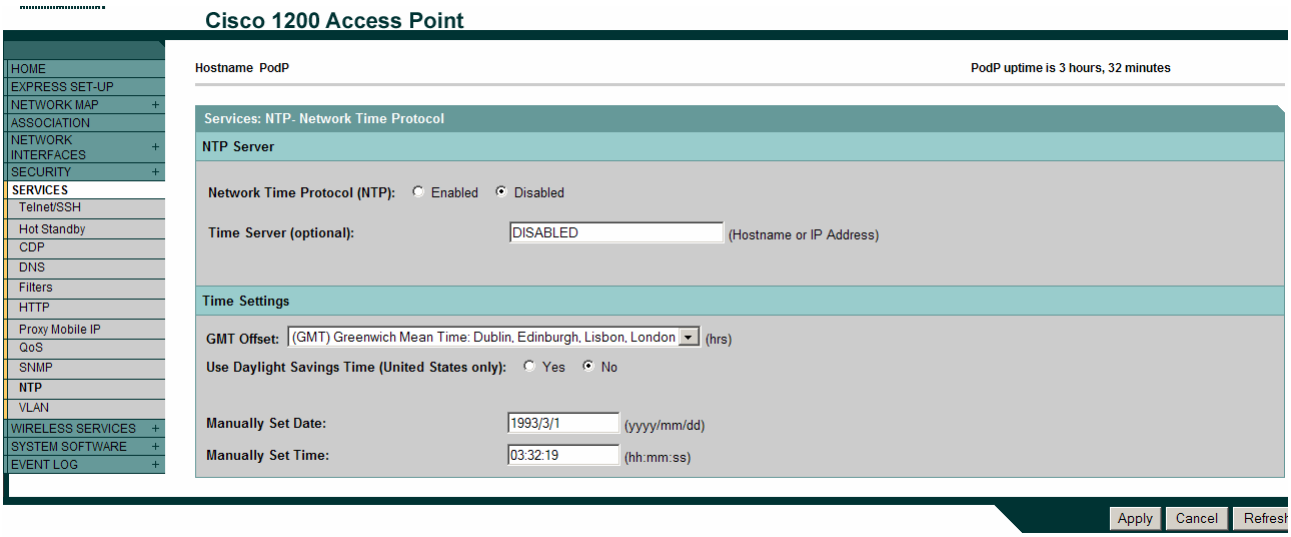
   Username: clsCo123

   Password: clsCo123

b. In a production environment, it is necessary to delete the old account. However, in the lab, do not remove the existing account. Also, it is important to encrypt the passwords in the configurations if there are multiple administrator accounts with various privilege levels. By default, this is enabled on the AP 1200. Notice the password is bulleted out.

c. Enable only Local User List Only and click **Apply**. At this point, the AP will require authentication with the new Username.

Step 3 Configure accurate time



In order to keep track on any potential attacks, it is important to maintain proper time.

a. From the **SERVICES>NTP** page manually set the correct time and date. Click **Apply** to save the changes.

Step 4 Verify the AP image file

Many attacks can be prevented by maintaining the most up to date image. In order to keep up with any vulnerabilities in Cisco products go to:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_tech_note09186a0080132a8a.shtml

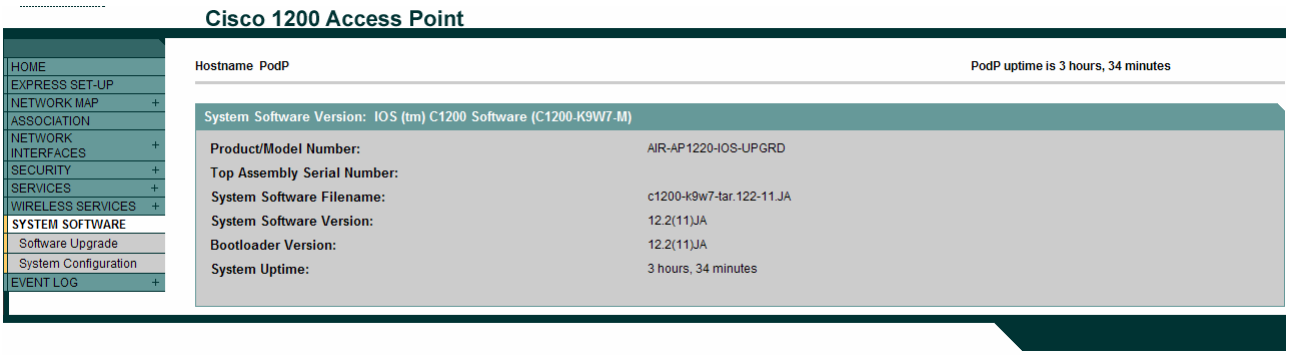
a. Are there any wireless vulnerabilities listed? If so, what are they?

_____

_____

_____

b. From the **SYSTEM SOFTWARE** main page, check the current image.



c. What version is running?

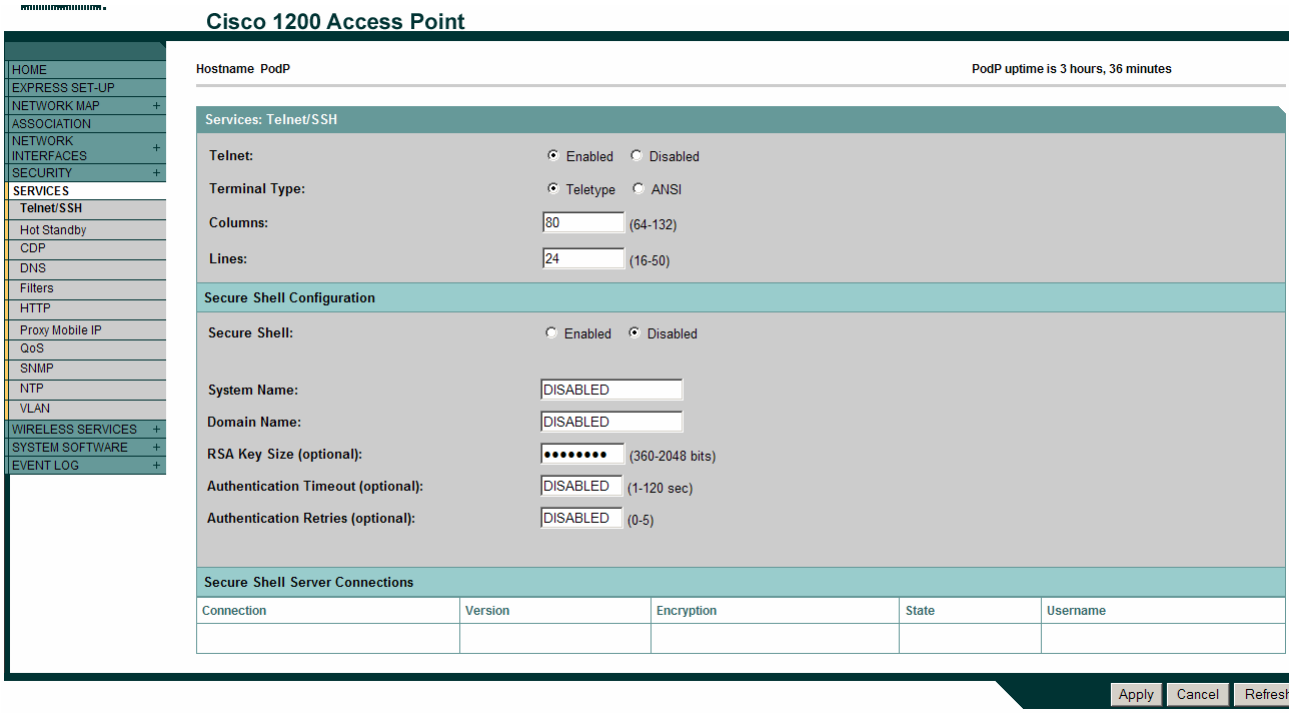
_____

d. Does this AP have any known vulnerabilities?

_____

Step 5 Configure SSH

In some circumstances, attackers may be able to use a packet analyzer to intercept telnet passwords, which may enable them to gain access to the AP or other networking devices. The SSH protocol is a secure form of telnet, providing both authentication and encryption.



a. From the **SERVICES>Telnet/SSH** page enable Secure Shell.

b. Enter the System name of PodP (where P is the pod number).

c. Enter a domain name of fwl.com.

d. Enter a key size (optional).

e. Keep the default Timeout and Retries values.

f. Click Apply.

g. What is the default size, in bits, of the key modulus?

_____

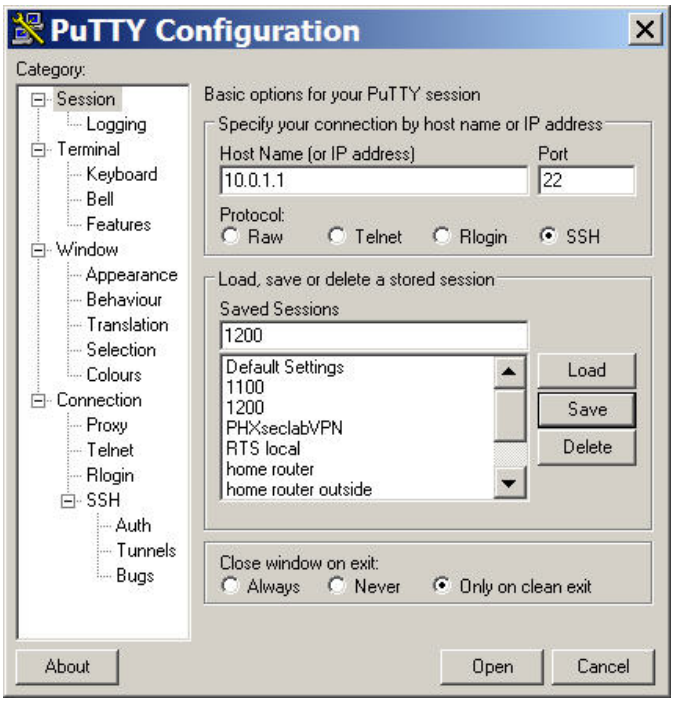
h. Press **OK** to accept the default key size and continue.

Note In a production environment, after enabling SSH, telnet and http should be disabled.

Step 6 Communicating between a SSH PC (client) to AP (server)

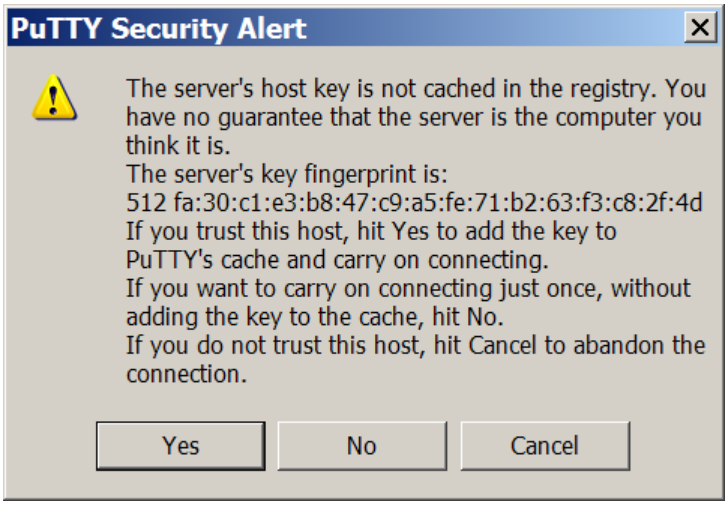
The basic settings to allow a PC and an AP to establish a SSH session are now configured. In order to establish a SSH session, launch the SSH client from the student PC.

a. The configurations will vary among different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.

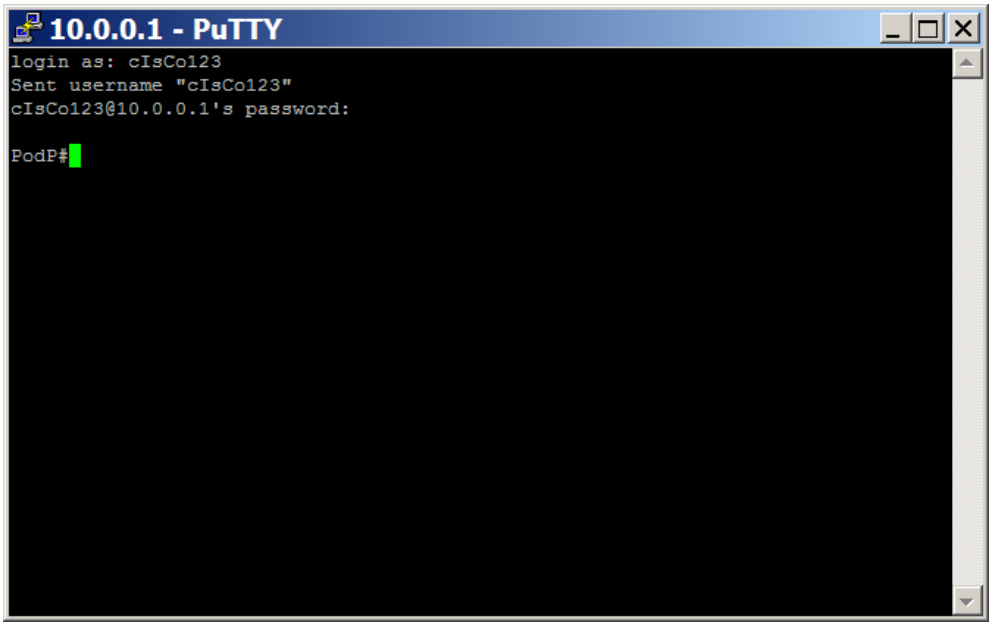


b. In the “Host Name (or IP address)” input box, enter the IP address of the pod AP. Next, change the protocol to “SSH”. These two values must be sent to establish the SSH. To test the connection, press the **Open** command button at the bottom of the window.

c. The SSH Client will popup a Security Alert window. Click **Yes** to trust the host.



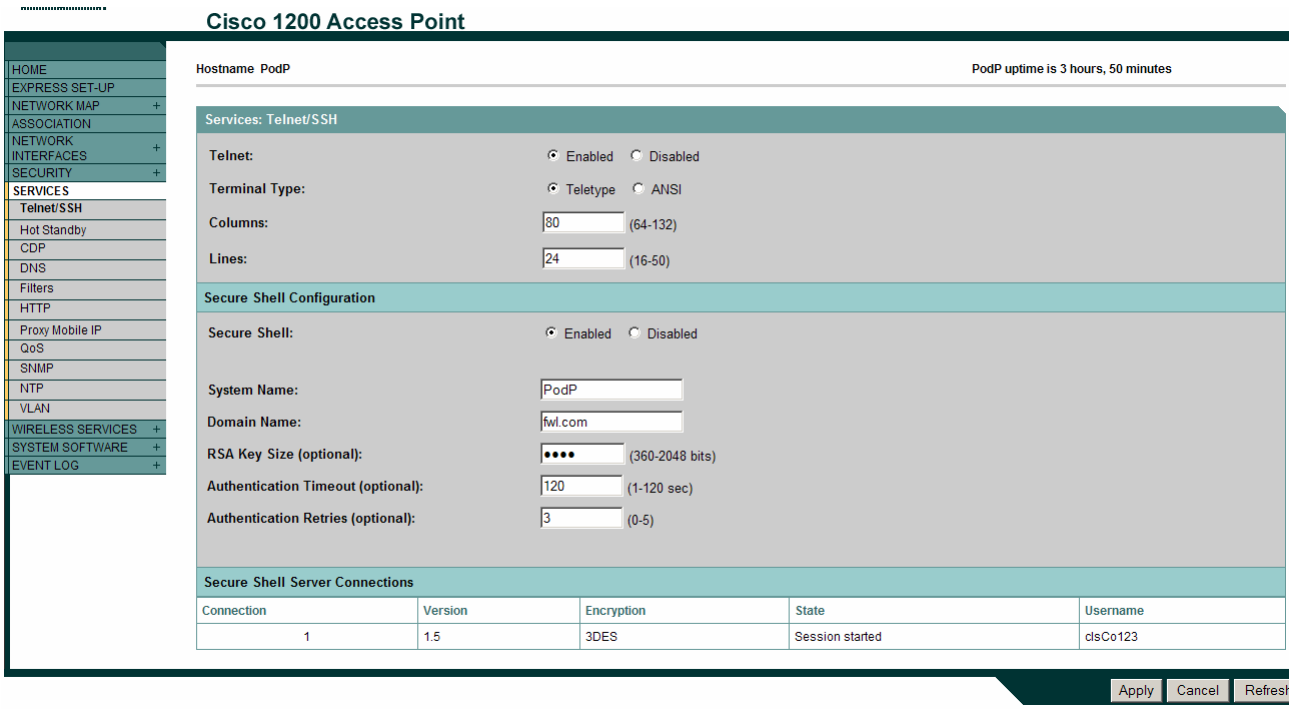
d. The SSH client will prompt for the local username and password that was previously set on the Pod AP. Enter the “**clsCo123**” for the username and “**clsCo123**” for the password.



e. Was the SSH connection successful? If so, how is the prompt displayed?

_____

Step 7 Verify SSH Connections



a. From the **SERVICES>Telnet/SSH** Page, view the active SSH sessions.

b. Fill in the appropriate values in the table below based on the active Secure Shell Server Connections.

Connection	Version	Encryption	State	Username

c. Reset the AP back to the factory default configuration.

Lab 8.3.1.2 Configure Basic AP Security through IOS CLI

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn the following objectives:

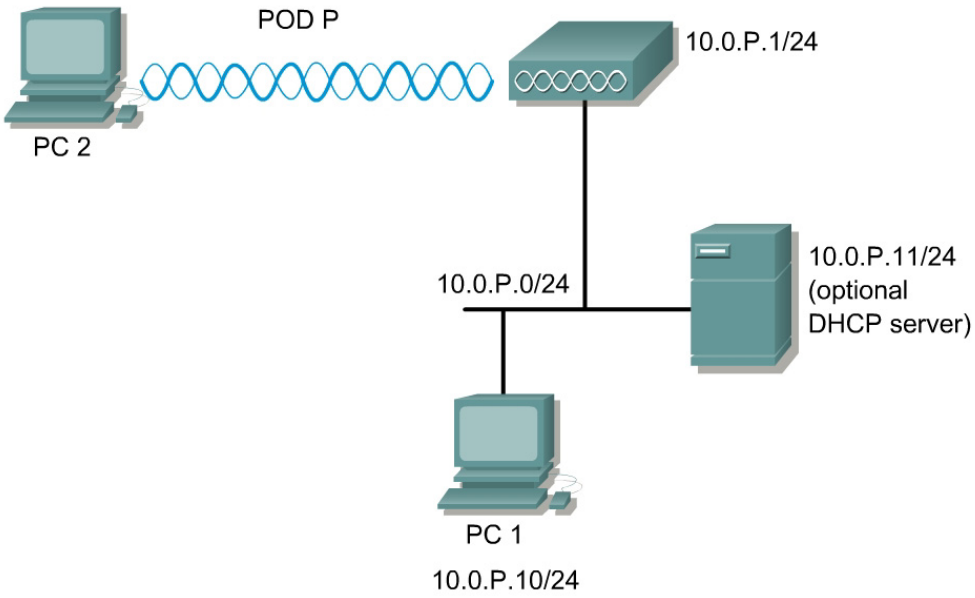
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
  - Limit VTY to SSH
  - Access-list to secure SSH
- Disable telnet and web

Scenario

Students will learn to secure the AP through Cisco Internetworking Operating System (IOS). The security policy of the company mandates all devices should be locked down according to minimum standards. Also, SSH must be used for remote management.

SSH is a program, similar to Telnet, which allows a network administrator to log into another computer over a network. SSH allows an administrator to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure networks. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

The instructor should have a working wired network. PC1 should be connected to the wired network. Prior to starting the lab, ensure that each host PC is loaded with a SSH client. There are numerous SSH clients available for free on the Internet. The lab was developed using the PuTTY SSH client.

Tools and Resources

Each team will need:

- AP
- PC or laptop
- Console cable
- SSH client software

Additional Materials

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

http://www.chiark.greenend.org.uk/~sgtatham/putty/

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
crypto key generate rsa	Generates Rivest, Shamir, and Adleman (RSA) key pairs.
hostname	This command changes the APs hostname.
ip domain-name	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names.
ip ssh	Use the **ip ssh** command to configure Secure Shell (SSH) control parameters on the AP.
transport input	Defines which protocols to use to connect to a specific line of the AP.

Step 1 Configure basic AP settings

a. Connect a Cisco rollover cable (console cable) between PC1 and the AP.

b. Open a terminal emulator.

c. Press return to get started.

d. If there is an existing configuration on the AP, erase the configuration and reload.

e. Configure the hostname, SSID, and domain name according to the Preparation table.

```
PodP(config)#
PodP(config)#ip domain-name fwl.com
```

f. Configure a wireless PC or laptop to connect to the AP. This will be used later in the lab to test the security configuration.

g. Remain on PC1 to configure the following steps.

h. While in configuration mode, check the configuration

```
PodP(config)#do show run
```

Step 2 Configure a new administrator account

One of the easiest ways for hackers to gain access to network devices is by using default usernames and passwords.

a. Configure a new administrator account.

```
PodP(config)#username cIsCo123 password cIsCo123
```

b. In a production environment, it is necessary to delete the old account.

```
PodP(config)#no username Cisco password Cisco
```


c. Also, it is important to encrypt the passwords in the configurations if there are multiple administrator accounts with various privilege levels. By default, this is enabled on the AP 1200.

```
PodP(config)#service password-encryption
```

d. While in configuration mode, verify the user accounts and password encryption.

```
PodP(config)#do show run
```

e. Secure the console connection by requiring a password.

```
PodP(config)#line con 0
PodP(config-line)#login
PodP(config-line)#password cIsCo123
```

f. Exit out of the AP and log back in.

```
User Access Verification

Password:
```

g. A more secure method is to require a username and password combination. Return to configuration mode and configure local authentication on the console.

```
PodP(config)#line con 0
PodP(config-line)#login local
```

h. Exit out of the AP and log back in using the username password combination configured in step 2a.

```
User Access Verification

Username:
Password:
PodP>
```

Step 3 Configure accurate time

In order to keep track on any potential attacks, it is important to maintain proper time.

a. Configure the correct time. Use the help feature if needed.

```
PodP#clock set
```

b. Set the correct timezone

```
PodP(config)#clock timezone [name of time zone] [offset in hours]

Example:
PodP(config)#clock timezone PhoenixAZ -7
```


c. (Optional) Configure daylight savings time. Use the help feature or command reference if needed.

```
PodP(config)#clock summer-time
```

d. Check the clock settings while in configuration mode.

```
PodP(config)#do show clock
```

Step 4 Configure MOTD and login banner

a. Configure a message-of-the-day (MOTD). The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

```
PodP(config)#banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
PodP(config)#
```

b. Exit out of the console or telnet session to check the MOTD.

```
con0 is now available

Press RETURN to get started.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.
```

c. Configure a login banner. This banner appears after the MOTD banner and before the login prompt.

```
PodP(config)#banner login $
Access for authorized users only. Please enter your username and
password.
$
PodP(config)#
```

d. Exit out of the console to check the banner.

```
con0 is now available

Press RETURN to get started.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

Access for authorized users only. Please enter your username and
password.

User Access Verification

Username:
```


Step 5 Verify the image file

Many attacks can be prevented by maintaining the most up to date image. In order to keep up with any vulnerabilities in Cisco products go to:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_tech_note09186a0080132a8a.shtml

a. Are there any wireless vulnerabilities listed? If so, what are they?

_____
_____
_____

b. Check the current image.

```
PodP#show version
```

c. What version is running?

_____

d. Does this AP have any known vulnerabilities?

_____

Step 6 Configure SSH

In some circumstances, attackers may be able to use a packet analyzer to intercept telnet passwords, which may enable them to gain access to the AP or other networking devices. The SSH protocol is a secure form of telnet, providing both authentication and encryption.

First, begin by generating the asymmetric keys used in the SSH authentication process.

Generate RSA keys

a. Enter the following command in the configuration mode:

```
PodP(config)#crypto key generate rsa ?
```

b. What are the available help options for this command?

_____

Generate RSA keys (continued)

- To enable SSH for local and remote authentication on the AP, enter the command **crypto key generate rsa** and press **Enter**. The AP will respond with a message showing the naming convention for the keys.

c. What is the default size, in bits, of the key modulus?

_____

d. Press **Enter** to accept the default key size and continue.

Step 7 Configure SSH timeouts

a. Configuring SSH timeouts and authentication retries is a way of providing additional security for the connection. Use the command **ip ssh {[time-out seconds]} {authentication-retries integer}** to enable timeouts and authentication retries. Set the SSH timeout to 15 seconds and the amount of retries to 3 by entering the following commands:

```
PodP(config)#ip ssh time-out 15
PodP(config)#ip ssh authentication-retries 3
```

1. What is the maximum timeout value allowed? What is the maximum amount of authentication retries allowed?

_____

Step 8 Configure local authentication and VTY

a. Use the following commands to define a local user and assign SSH communication to the vty lines:

```
PodP(config)# username cisco password student
PodP(config)# line vty 0 4
PodP(config-line)# transport input ssh
PodP(config-line)# login local
```

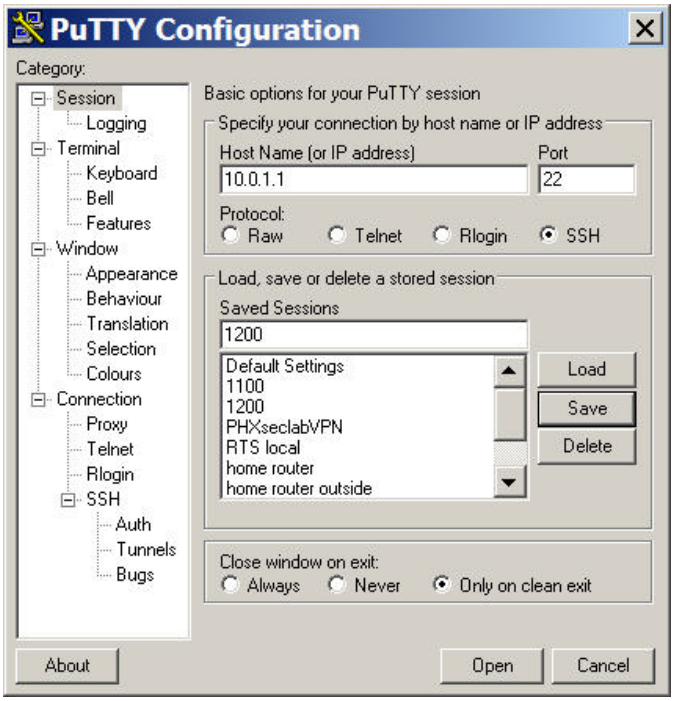
1. What are the available parameters for the **transport input** command?

_____

Step 9 Communicating between a SSH PC (client) to AP (server)

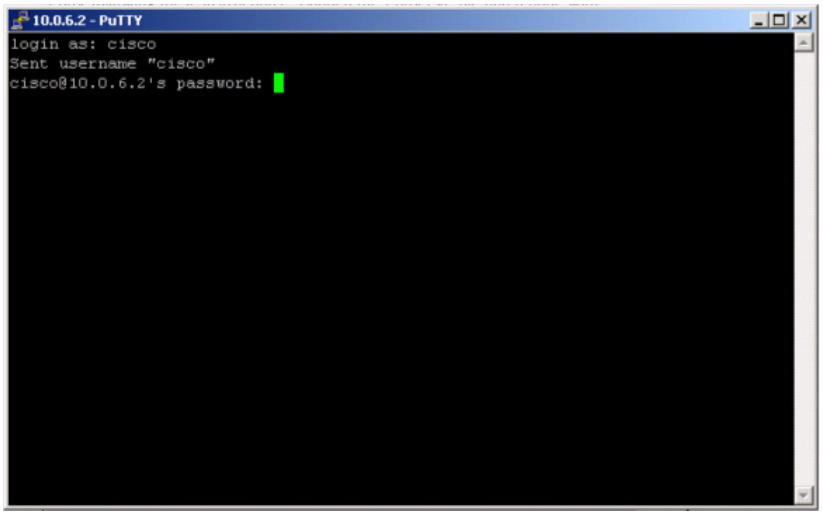
The basic settings to allow a PC and an AP to establish a SSH session are now configured. In order to establish a SSH session, launch the SSH client from the student PC.

a. The configurations will vary among different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.



b. In the “Host Name (or IP address)” input box enter the IP address of the pod AP. Next, change the protocol to “SSH”. These two values must be sent to establish the SSH. To test the connection, press the **Open** command button at the bottom of the window.

c. The SSH client will prompt for the local username and password that was previously set on the Pod AP. Enter the “**clsCo123**” for the username and “**clsCo123**” for the password.



d. Was the SSH connection successful? If so, how is the prompt displayed?

_____

Step 10 debug and verify SSH

Enable debugging

a. Enable debugging of SSH by entering the following commands:

```
PodP(config)#logging on
PodP(config)#exit
PodP#terminal monitor
PodP#debug ip ssh
```

b. SSH debug output

c. Next, open another instance of the SSH client and connect to the AP. Use the correct username and password to log in to the AP. The debug output should be similar to the output below.

```
03:45:37: SSH1: starting SSH control process
03:45:37: SSH1: sent protocol version id SSH-1.5-Cisco-1.25
03:45:37: SSH1: protocol version id is - SSH-1.5-PuTTY-Release-0.53b
03:45:37: SSH1: SSH_SMSG_PUBLIC_KEY msg
03:45:38: SSH1: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
03:45:38: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH: RSA decrypt started
03:45:39: SSH: RSA decrypt finished
03:45:39: SSH1: sending encryption confirmation
03:45:39: SSH1: keys exchanged and encryption on
03:45:41: SSH1: SSH_CMSG_USER message received
03:45:41: SSH1: authentication request for userid cisco
03:45:41: SSH1: SSH_SMSG_FAILURE message sent
03:45:44: SSH1: SSH_CMSG_AUTH_PASSWORD message received
03:45:44: SSH1: authentication successful for cisco
03:45:44: SSH1: requesting TTY
```



```
   03:45:44: SSH1: setting TTY - requested: length 24, width 80; set:
length 24, width 80
   03:45:44: SSH1: SSH_CMSG_EXEC_SHELL message received
   03:45:44: SSH1: starting shell for vty03:45:37: SSH1: starting SSH
control process
```

d. To get an idea of the debugging process and the debugging message, open another instance of the SSH client and intentionally enter the wrong username or password. View the debugging output for failed authentication.

   Disable debugging

```
PodP#undebug all
All possible debugging has been turned off
```

e. Viewing SSH sessions

f. Use the **show ssh** command to view the active SSH sessions.

g. Fill in the appropriate values of the table below, based on the output of the **show ssh** command.

Connection	Version	Encryption	State	Username

   Viewing SSH parameters

h. To display the version information and SSH parameters, use the **show ip ssh** command.

i. Is the output displayed exactly as the output below? If not, what are the differences?

_____

_____

_____

```
PodP>sh ip ssh
SSH Enabled - version 1.5
Authentication timeout: 15 secs; Authentication retries: 3
```

Step 11 AP to AP SSH Connection (Optional)

Confirm peer SSH configurations.

a. Verbally communicate with the peer team to ensure the peer AP has been configured to accept a SSH connection. Instead of using a SSH client running on a host computer, the AP will be the SSH client and will establish a connection to the peer AP. By default, the Cisco IOS will act as both a SSH server and SSH client.

b. In order to communicate between the two APs across the wired LAN, the BVI interfaces will have to be on the same subnet. This can be accomplished by changing the masks to 255.255.0.0 on both AP BVI interfaces. One other option is to use a router between the two APs, which will route between the two subnets.

   Test Telnet.

c. When the peer group is ready, enter the **telnet** command and establish connectivity with the peer AP.

```
PodP#telnet 10.0.Q.1  (where Q is the peer team AP)
```


d. Was the Telnet connection successful? Why or why not?

_____

Enter SSH parameters.

e. Enter the following commands to establish a SSH connection to the peer AP:

```
PodP#ssh ?
```

f. What are the additional arguments of the **ssh** command?

_____

g. What encryption algorithms are available?

_____

Establish AP to AP SSH connection.

h. Enter the following command to establish a SSH connection to the peer AP:

```
PodP>ssh -c des -l cisco 10.0.Q.1   (where Q is the peer team AP)
```

This command makes a SSH connection to a peer AP with an address of 10.0.Q.2, DES as the encryption, and cisco as the login username.

i. Was the SSH connection successful?

_____

Verify SSH.

j. Enter the following command to verify the SSH connection:

```
PodP#show ip ssh
PodP#show ssh
```

k. What other commands could be useful to verify and troubleshoot SSH connections?

_____

_____

Step 12 Disable web (optional)

Many security policies may mandate http access to devices be disabled. If https is not available, then SSH is the second best option for secure communication to remote LAN devices.

a. Now that SSH is configured, disable web access to the AP.

```
PodP(config)#
PodP(config)#no ip http server
```

b. Open a web browser and try to connect to the AP?

_____

_____

c. If the configuration was saved to flash, erase the startup configuration and reload the AP.

```
PodP#erase startup-config
PodP#reload
```


Lab 8.3.2 Configure Filters on AP

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two.

Objective

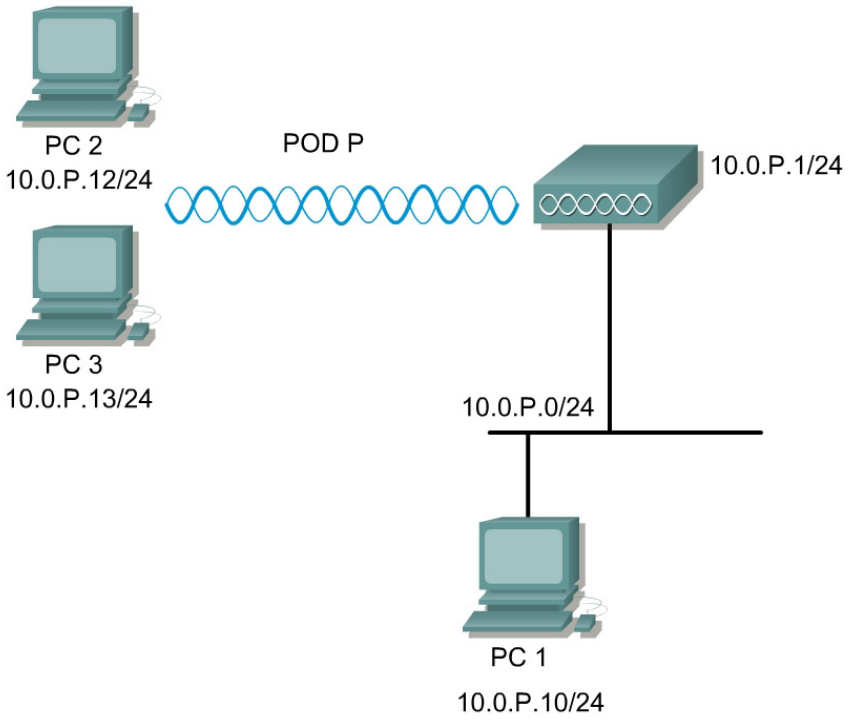
In this lab, the student will learn how to set and enable a protocol filter on the AP and how to set and enable MAC address filters on the AP.

Scenario

Protocol filters prevent or allow the use of specific protocols through the AP. Individual protocol filters or sets of filters can be set up for either the Radio or Ethernet ports. Protocols can be filtered for wireless client devices, users on the wired LAN, or both.

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. A filter can be created that passes traffic to all MAC addresses except those that are specified. A filter can also be created that blocks traffic to all MAC addresses except those that are specified.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

The APs and PC client adapter and utility should be installed and properly configured prior to the lab. The students will also familiarize themselves with the various EtherType, IP, and port filters available on the AP.

Tools and Resources

Each team of students will require the following:

- Cisco Aironet AP
- 1 wired PC or laptop
- 2 wireless PCs with ACU

Step 1 Creating a MAC address filter

Make sure the Topology is cabled and configured according to the Topology.

a. Verify the SSID is configured

b. Verify both PC2 and PC3 are associated and TCP/IP is configured

c. Verify both PC2 and PC3 can ping the AP at 10.0.P.1

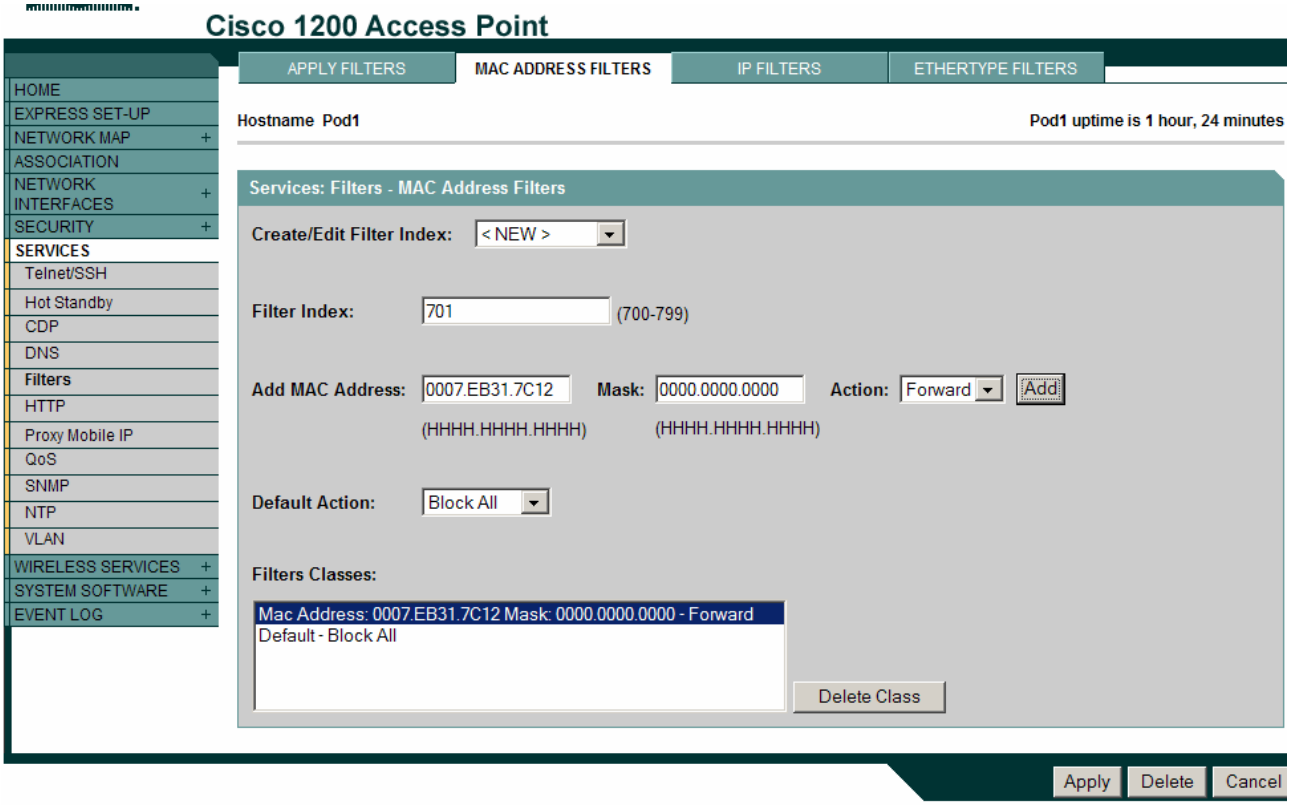
Step 2 Creating a MAC address filter

Follow the path below to reach the Address Filters page:

a. Click **SERVICES** in the page navigation bar.

b. In the Services page list, click **Filters**.

c. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.



d. Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu.

e. In the Filter Index field, name the filter with a number from 701.

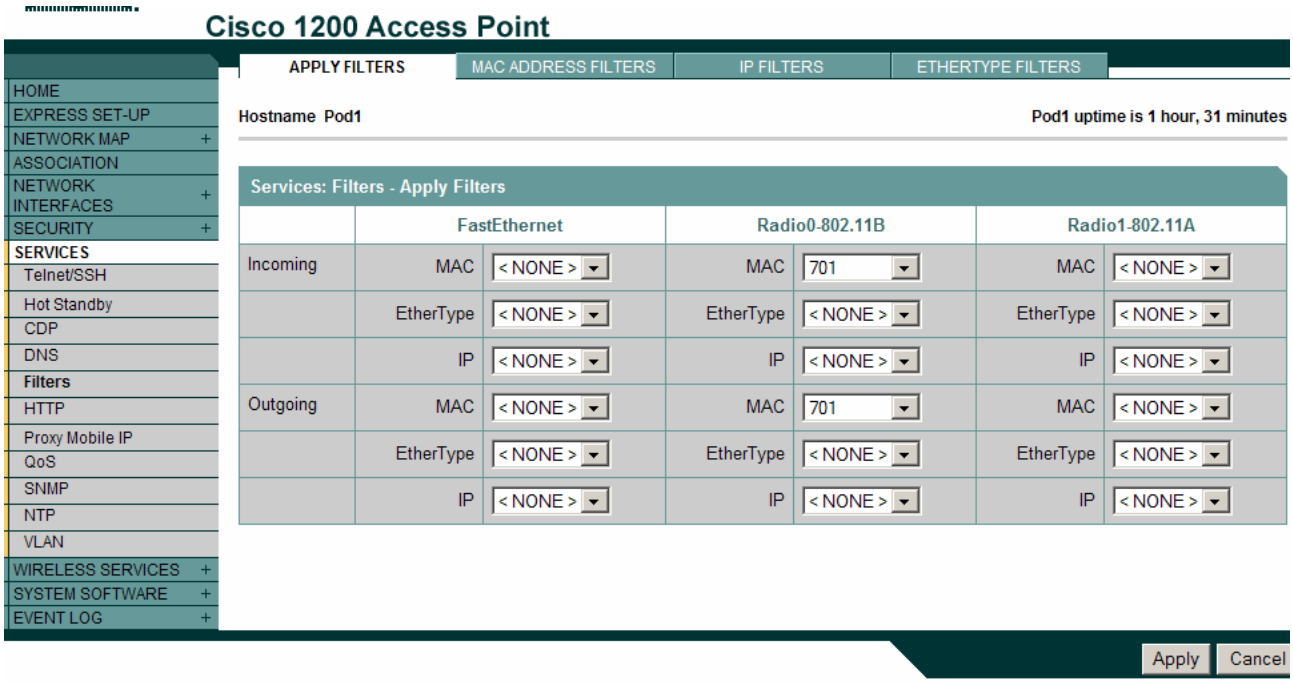
f. Enter a MAC address wireless PC2 in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0007.50CA.E208, for example).

g. Select **Forward** from the Action menu.

h. Click **Add**. The MAC address appears in the Filters Classes field.

i. Click **Apply**. The filter is saved on the AP, but it is not enabled until it is applied on the Apply Filters page.

Step 3 Apply the MAC address filter



a. From the **SERVICES>Filters** Page, go to the APPLY FILTERS tab.

b. Select the filter number 701 from the Radio0-802.11B MAC drop-down menus. Apply the filter to incoming and outgoing packets.

c. Click **Apply**. The filter is enabled on the selected ports.

Note Client devices with blocked MAC addresses cannot send or receive data through the AP, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the AP stops monitoring them, when the AP reboots, or when the clients associate with another AP.

Step 4 Test the MAC address filter

When applying any security, it is important to test the configuration

a. From PC 3, located at 10.0.P.13, ping the AP at 10.0.P.1.

b. Was this successful? Should it be successful?

_____

_____

c. From PC 2, located at 10.0.P.12, ping the AP at 10.0.P.1

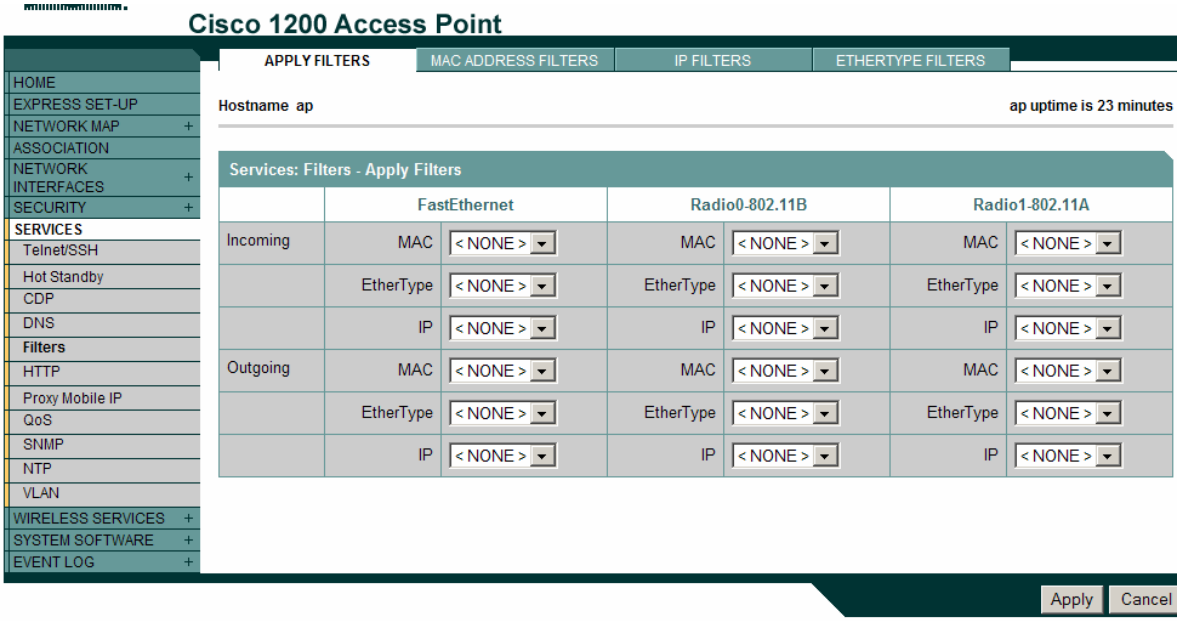
d. Was this successful? Should it be successful?

_____

_____

Step 5 Remove the MAC address filter

Before configuring any IP Filters, delete the existing MAC filter.



a. From the **SERVICES>Filters Page** change the 701 to <NONE> on both Incoming and Outgoing.

b. Click **Apply**.

c. From PC 2 and PC 3, ping the AP at 10.0.P.1.

d. Was this successful? Should it be successful?

_____

_____

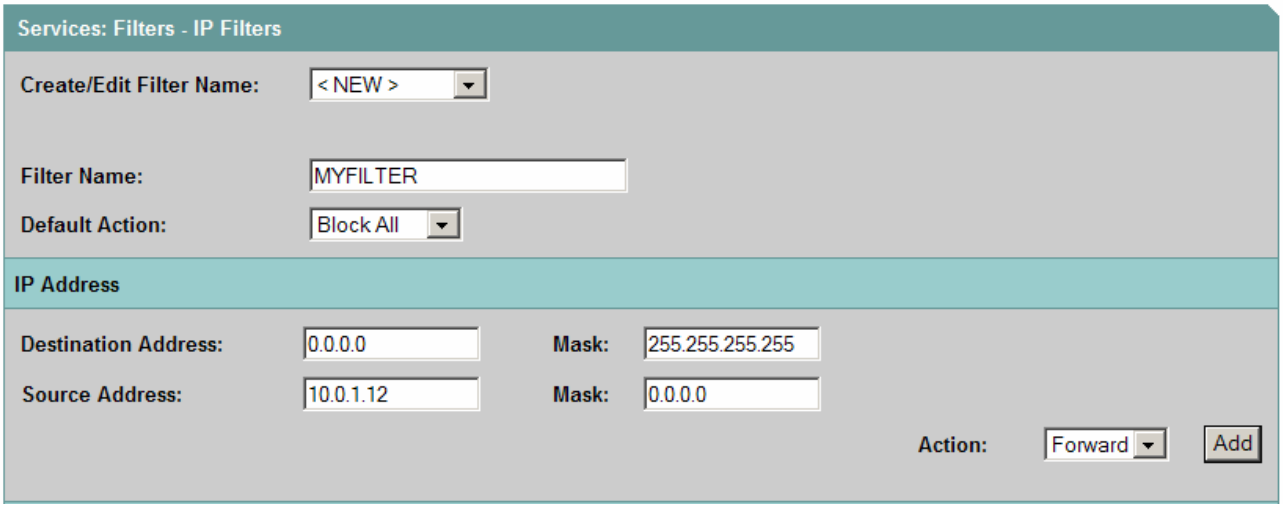
Step 6 Creating an IP filter

Follow this link path to reach the IP Filters page:

a. Click **Services** in the page navigation bar.

b. In the Services page list, click **Filters**.

c. On the **Apply Filters** page, click the **IP Filters** tab at the top of the page.



d. Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu, and then click the **Add** button.

e. Enter a descriptive name of **MYFILTER** for the new filter in the Filter Name field.

f. Select **Block all** as the filter's default action from the Default Action menu.

g. Configure the **Destination Address:** of 0.0.0.0 and a **Mask:** of 255.255.255.255.

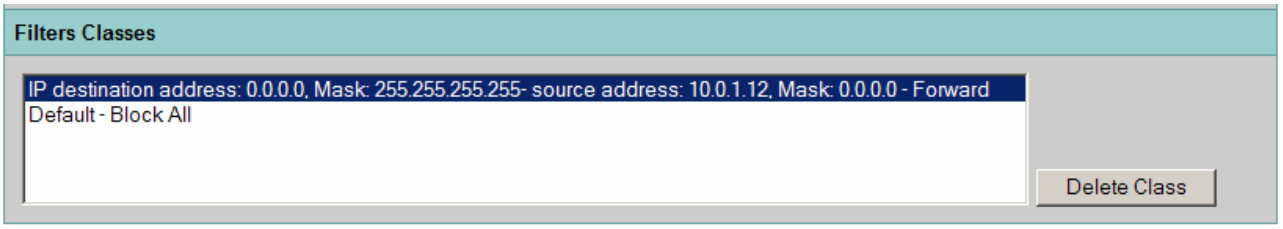
h. Add 10.0.P.12 as the **Source Address:** with a **Mask:** of 0.0.0.0 to permit PC2 traffic.

i. Make sure Forward is selected for the **Action:**

j. Click the **Add** button. The ACL will now appear in the Filters Classes Box at the bottom of the **Filters** page.

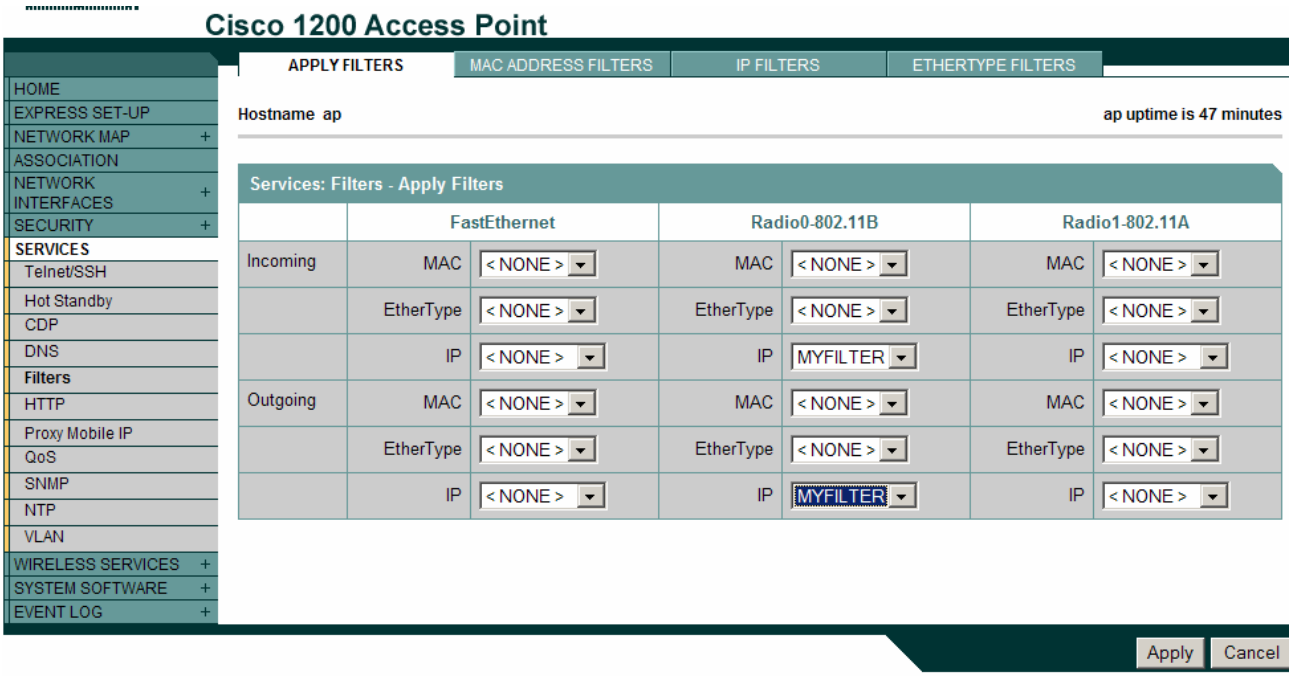
k. Verify the configuration in the Filters Classes box.

.



l. If the configuration is correct, click **Apply**.

Step 7 Apply the IP filter



a. Select **MYFILTER** from the radio ports incoming and outgoing IP fields.

b. Click **Apply**. The filter is now enabled on the selected interface(s).

Step 8 Test the IP filter

When applying any security, it is important to test the configuration

a. From PC 3, located at 10.0.P.13, ping the AP at 10.0.P.1.

b. Was this successful? Should it be successful?

_____

c. From PC 2, located at 10.0.P.12, ping the AP at 10.0.P.1.

d. Was this successful? Should it be successful?

_____

e. List three of the EtherType filters that can be used.

_____

_____

_____

f. List three of the IP filters that can be used.

_____

_____

_____

g. List three of the port filters that can be used.

_____

_____

_____

Lab 8.3.3.1 Configure WEP on AP and Client

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

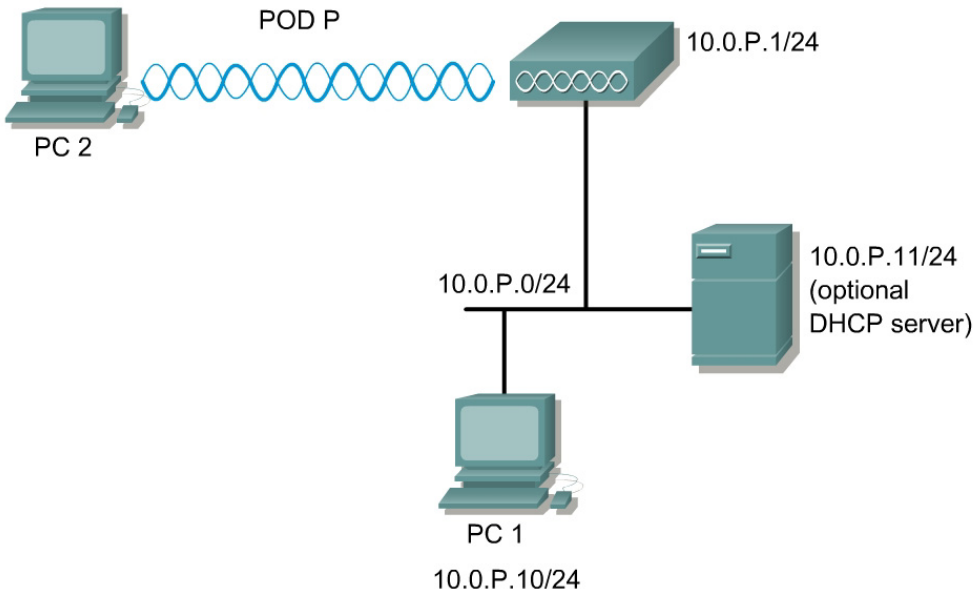
Objective

In this lab, students will demonstrate an understanding of the role of a Wired Equivalent Privacy (WEP) key in network security. Additionally, students will learn how to enable WEP on an AP and on the client PC.

Scenario

The purpose of WEP is to protect the privacy of transmitted data. WEP keys are used to encrypt the data signals the AP transmits and to decrypt the data signals the AP receives (and includes data transmitted and received by the client).

Topology



Preparation

The students will read and understand FWL Chapter 8 prior to the lab.

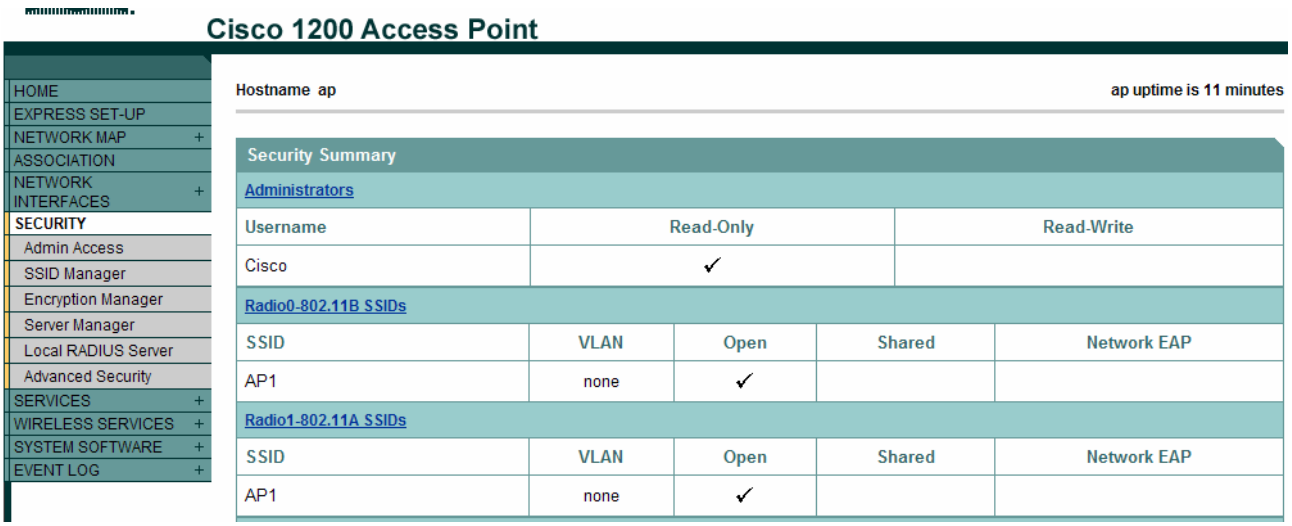
All APs and PCs will be properly setup according to the topology prior to the lab. Ensure an existing wireless connection is present from PC2 to the AP.

Tools and Resources

Each team of students will require the following:

- Cisco Aironet APs
- PCs with the Cisco Aironet client adapter and utility properly installed

Step 1 Configuring WEP on the access point



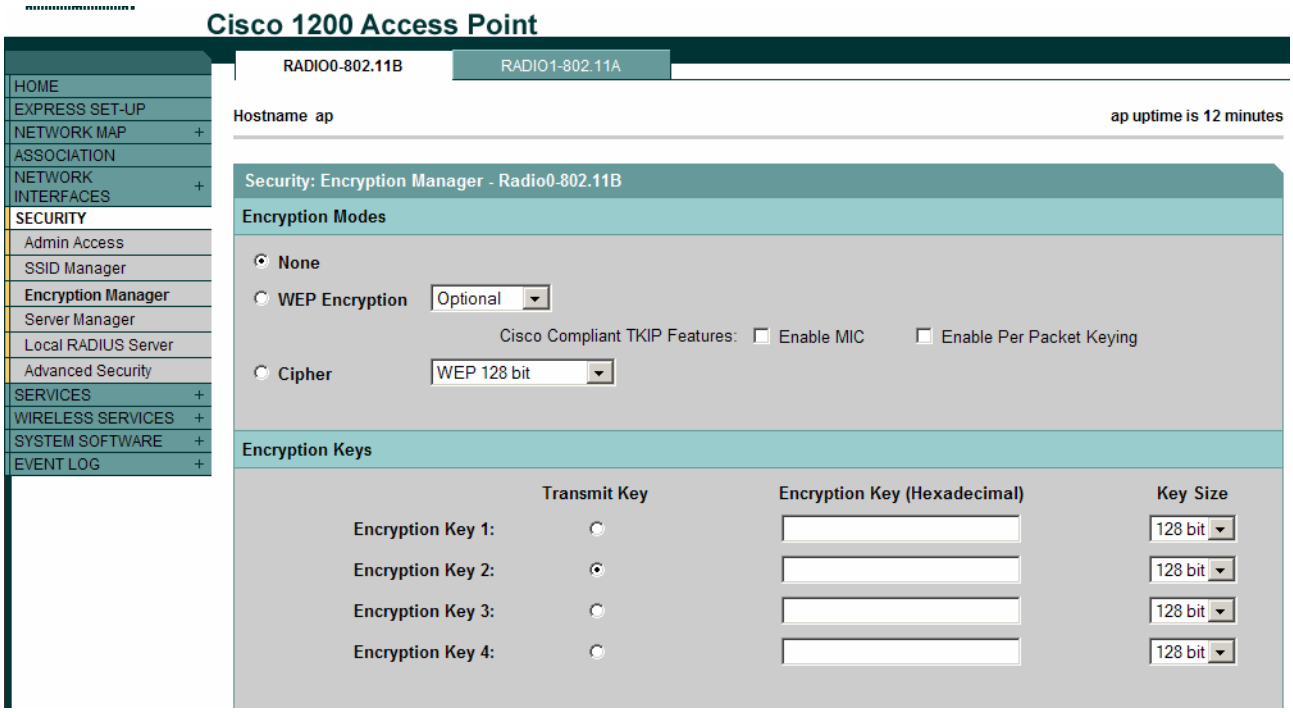
In order to configure WEP on the AP, complete the following steps:

a. Verify connectivity from the wireless client (PC2) to the AP

b. Open a Web browser on the PC1 and type the IP address of the AP to configure in the browser address bar.

c. Go to the **Security** Setup page of the AP and click on the **Encryption Manager** option.

Step 2 Configuring WEP (continued)



WEP keys can be entered in ASCII or hexadecimal on most equipment. Cisco Aironet equipment requires WEP keys to be entered in hexadecimal. 40-bit WEP keys are 10 hexadecimal characters long. 128-bit WEP keys are 26 hexadecimal characters long. To configure WEP, follow the steps below:

a. Check the radio button WEP Encryption Mode for **WEP Encryption**

b. Use the Pull Down Menu to select **Mandatory**

c. Select the **Transmit Key**

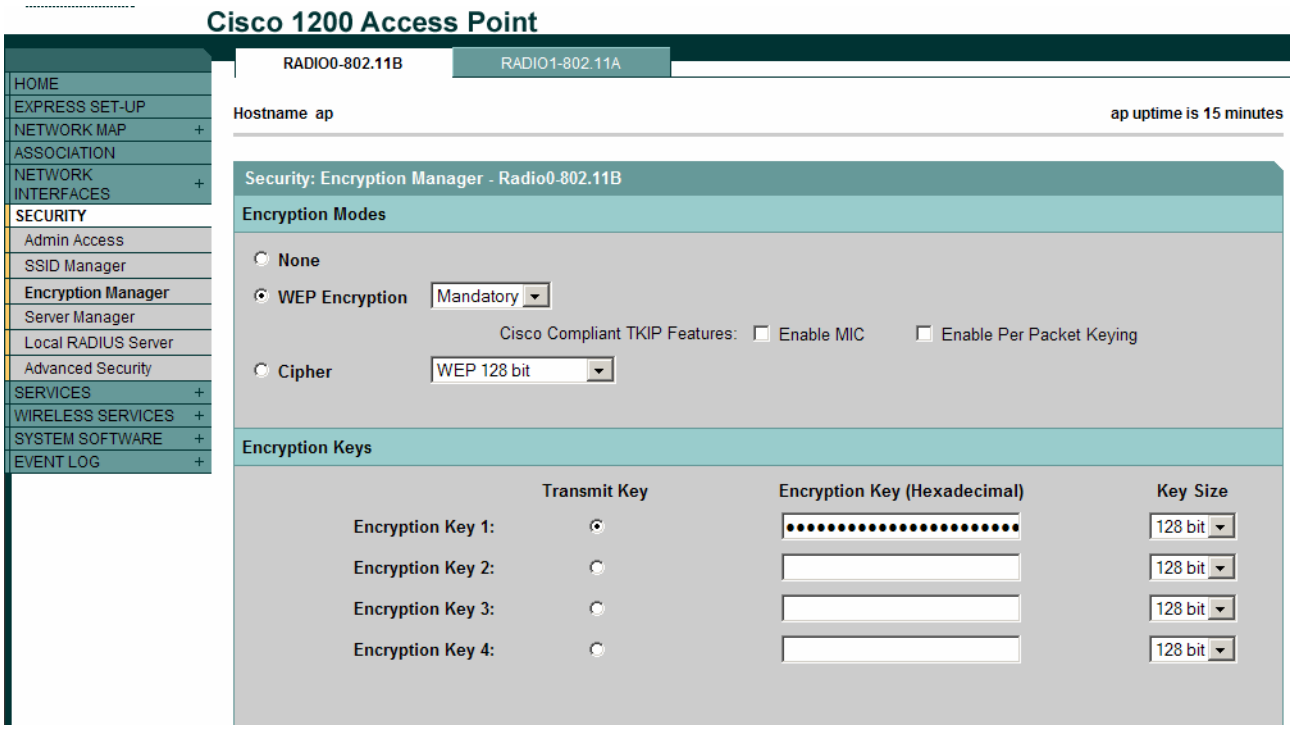
d. Enter the Encryption key (for lab purposes will be) **12345678909876543210123456**

e. Select the Key size **128 bits**

f. Click the **Apply-All** button to apply these options.

g. Once WEP is configured on the AP with a **Mandatory** option, all the clients will become disassociated to this AP.

Step 3 Verify the WEP configuration

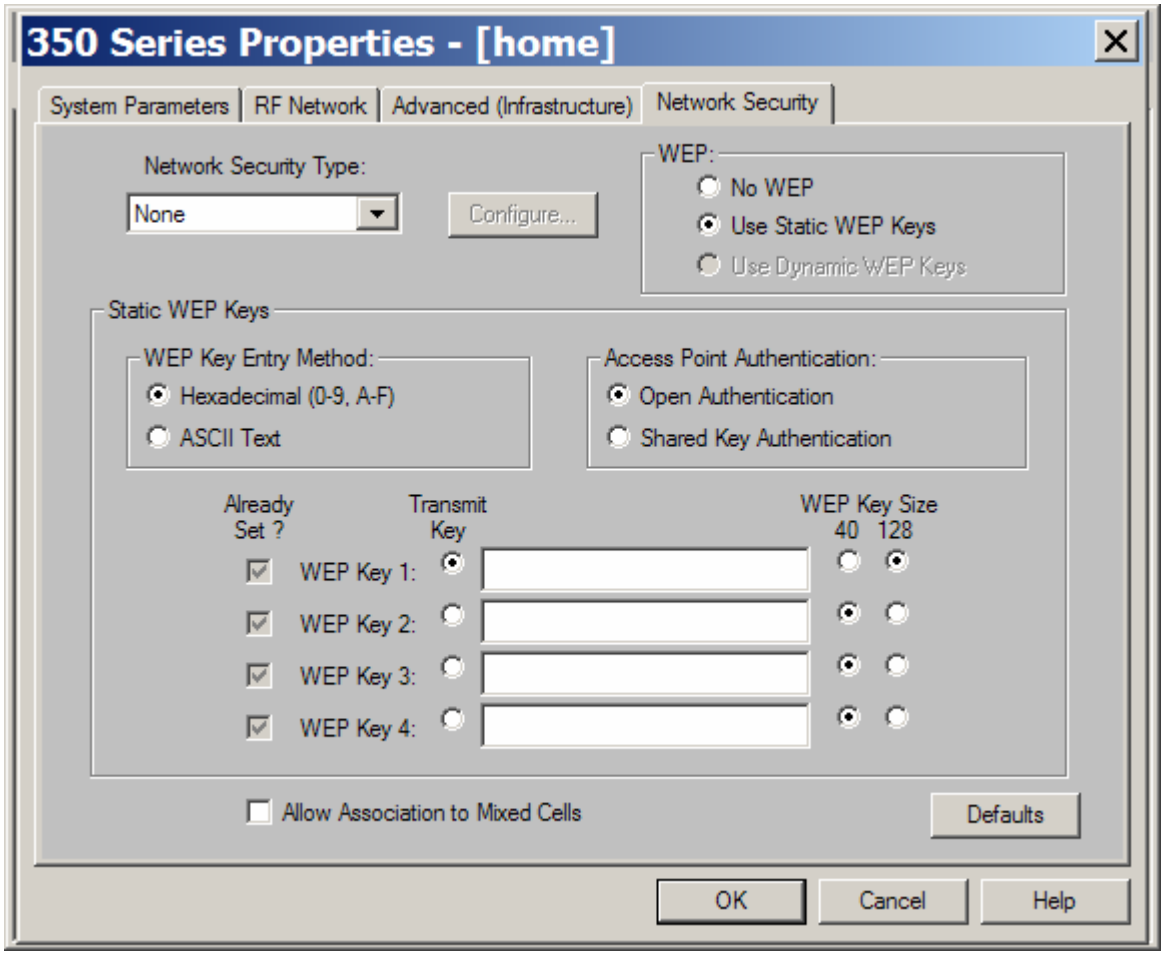


View the **SECURITY>Encryption Manager** page. The WEP settings should be configured and the Encryption Key field should be stored in the AP. However, the Key field should be encrypted with asterisk symbols to prevent unauthorized users from viewing the Encryption Key.

1. What Encryption option allows client devices that can communicate with the AP either with or without WEP?

   _____

Step 4 Configure WEP on PC2 using the client adapter utility



In order to configure the WEP settings on the wireless client adapter, complete the following steps:

a. Open the Aironet client utility by clicking on the ACU icon.

b. Click Profile Manager to edit the WEP settings.

c. Under the Profile Management section, choose the profile being used for this lab, and click Edit.

d. Go to the **Network Security** tab of the profile that is being used for the lab.

e. Configure the following settings for WEP:

1. Select the WEP setting – **Use Static WEP keys**
2. Select the Static WEP key entry method – **Hexadecimal**
3. Select the AP Authentication – **Open authentication**
4. Select and enter the Transmit key [for lab purposes will be] **1234567890987654321012345 6**
5. Select the WEP key Size – **128 bits**
6. Click the **OK** button to apply the WEP settings to the client
7. The client should re-associate to the AP once WEP is enabled properly on the AP and the client adapter utility.

f. How many WEP keys can be stored on the Cisco client adapter?

_____

g. What happens if a device receives a packet that is not encrypted with the appropriate key?

_____

h. What is the more secure authentication method, shared key or open?

_____

Lab 8.3.3.2 Configure an AP as a repeater using WEP

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

Objective

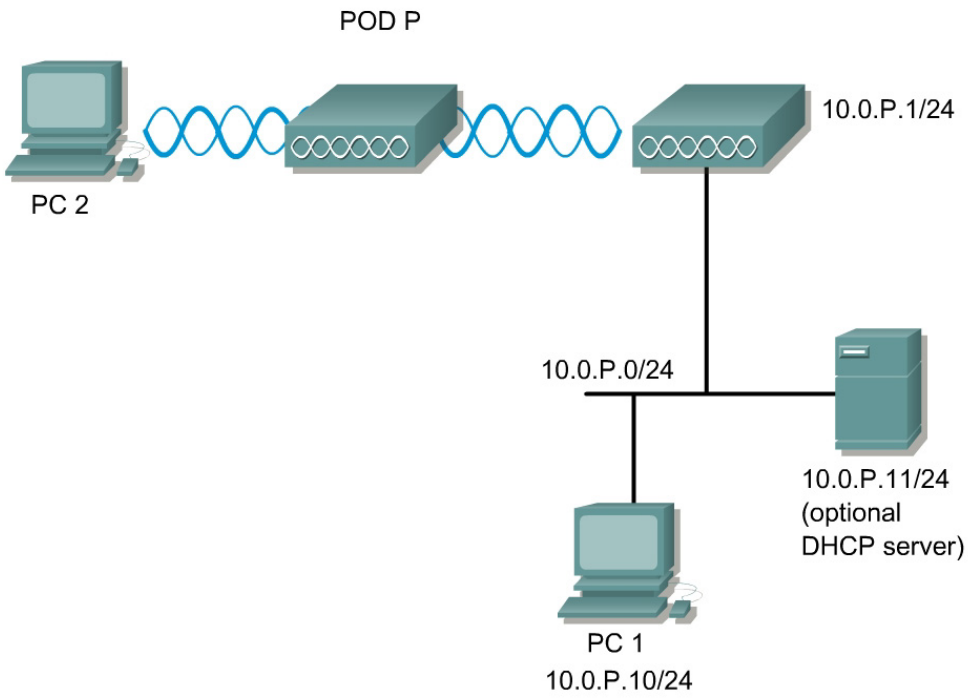
The student will extend the coverage of a basic service set topology by implementing an AP as a repeater using WEP.

Scenario

An AP can be configured as a repeater to extend the wireless infrastructure range or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to another repeater or to an AP connected to the wired LAN. The data is sent through the route that provides the best performance for the client. In this lab, the Root AP will be Pod1. The repeater AP will be Pod2.

WEP must now be enabled per the security policy.

Topology



Preparation

Team	Access Point Name	SSID	Address
1	Pod1 (root)	AP1	10.0.1.1/24
2	Pod2 (repeater)	AP1	10.0.1.2/24

The instructor should have a working wired network. PC1 should be connected to the wired network.

Tools and Resources

Each team will need:

- 2 APs
- A PC or laptop
- Console cable

Additional Materials

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Step 1 Configure the repeater AP

Make sure the first AP is configured and operational and clients can connect to the AP1. Pod1 will be the root AP and should have a SSID of AP1. Pod2 will become the repeater AP. The repeater AP will not require any Ethernet cables when configured in repeater mode.

a. Enter global configuration mode. Enter interface configuration mode for the 5-GHz radio 1. Turn the interface off.

```
Pod2(config)#interface dot11Radio 1
Pod2(config-if)#shutdown
```

b. Enter interface configuration mode for the 2.4-GHz radio.

```
Pod2(config)#interface dot11Radio 0
Pod2(config-if)#
```

c. Create the SSID that the repeater uses to associate to a root AP. The next step will designate this SSID as an infrastructure SSID. If an infrastructure SSID was created on the root AP, create the same SSID on the repeater.

```
Pod2(config-if)#ssid AP1
Pod2(config-if-ssid)#
```

d. Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root AP. Infrastructure devices must associate to the repeater AP using this SSID unless the optional keyword is also entered.

```
Pod2(config-if-ssid)#infrastructure-ssid
Pod2(config-if-ssid)#
*Mar  1 01:12:54.406: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset
*Mar  1 01:12:54.424: %LINK-3-UPDOWN: Interface Dot11Radio0, changed
state to up
```



```
Pod2(config-if-ssid)#
```

e. Exit SSID configuration mode and return to radio interface configuration mode.

```
Pod2(config-if-ssid)#exit
Pod2(config-if)#
```

f. Set the role of the AP in the wireless LAN to repeater.

```
Pod2(config-if)#station-role repeater
```

g. If Aironet extensions are disabled, enable Aironet extensions.

```
Pod2(config-if)#dot11 extension aironet
```

h. MAC addresses can be entered for up to four parent APs. The repeater attempts to associate to MAC address 1 first; if that AP does not respond, the repeater tries the next AP in its parent list. (Optional) Enter the MAC address for the AP to which the repeater should associate.

```
Pod2(config-if)#parent 1 0987.1234.e345
```

(This should be the MAC address of Pod1 11.b radio.)

i. Verify the configuration

```
Pod2#show run
   interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid AP1
       authentication open
       infrastructure-ssid
   !
    parent 1 0987.1234.e345
    speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
    rts threshold 2312
    station-role repeater
```

Step 2 Verify connections on Pod1

After the repeater is setup, check the LEDs on top of the repeater AP. If the repeater is functioning correctly, the LEDs on the repeater and the root AP to which it is associated will behave as follows:

- The status LED on the root AP is steady green, indicating that at least one client device is associated with it (in this case, the repeater).
- The status LED on the repeater AP is steady green when it is associated with the root AP and the repeater has client devices associated to it. The status LED of the repeater flashes steady green for 7/8 of a second and off for 1/8 of a second when it is associated with the root AP, but the repeater has no client devices associated to it.

The repeater AP should also appear as associated with the root AP in the Association Table of the root AP. On Pod1, verify that Pod2 is connected. There may also be other wireless clients associated.

a. Check the detailed status of all clients

```
Pod1#show dot11 associations all-clients
```


Step 3 Verify connections on Pod2

Move the wireless laptop out of the range of Pod1 into the range of Pod2.

On Pod2, verify that the laptop is associated. There may also be other wireless clients associated.

a. Check the detailed status of all clients

```
Pod2#show dot11 associations all-clients
```

b. Is the laptop associated? What information can be used to verify the connection?

_____

_____

Step 4 Configure WEP on the root and repeater AP

a. In interface mode, check the available encryption types that can be set. Then view the available key sizes.

```
Pod2(config-if)#encryption ?
  key   Set one encryption key
  mode  encryption mode
  vlan  vlan
PodP(config-if)#encryption key 1 size ?
  128bit  128-bit key
  40bit   40-bit keyCreate a WEP key and set the key properties
```

b. Create a WEP key and set up its properties.

```
PodP(config-if)#encryption key 1 size 128 12345678901234567890123456
transmit-key
```

Step 5 Verify connections on Pod1

a. After the WEP is setup, check the LEDs on top of the repeater AP for correct operation.

b. The repeater AP should also appear as associated with the root AP in the root AP Association Table. On Pod1, verify that Pod2 is connected. There may also be other wireless clients associated.

c. Check the detailed status of all clients.

```
Pod1#show dot11 associations all-clients
```

Step 6 Verify connections on Pod2

a. Now move the wireless laptop out of range of Pod1 into the range of Pod2.

b. On Pod2, verify that the laptop is associated. There may also be other wireless clients associated.

c. Check the detailed status of all clients.

```
Pod2#show dot11 associations all-clients
```

d. Are any laptops associated? Why?

_____

_____

Step 7 Configure the 802.11a radio as a repeater (optional)

Erase the configuration on Pod2. Return to Step 1 and configure the repeater topology using the 801.11a radio instead. In this case, disable the 11b radio. Make sure Pod1 is configured to accept the 5 GHz clients.

Lab 8.4.5.1 Configuring LEAP/EAP using Local RADIUS Authentication

Estimated Time: 40 minutes

Number of Team Members: Students can work in teams of two.

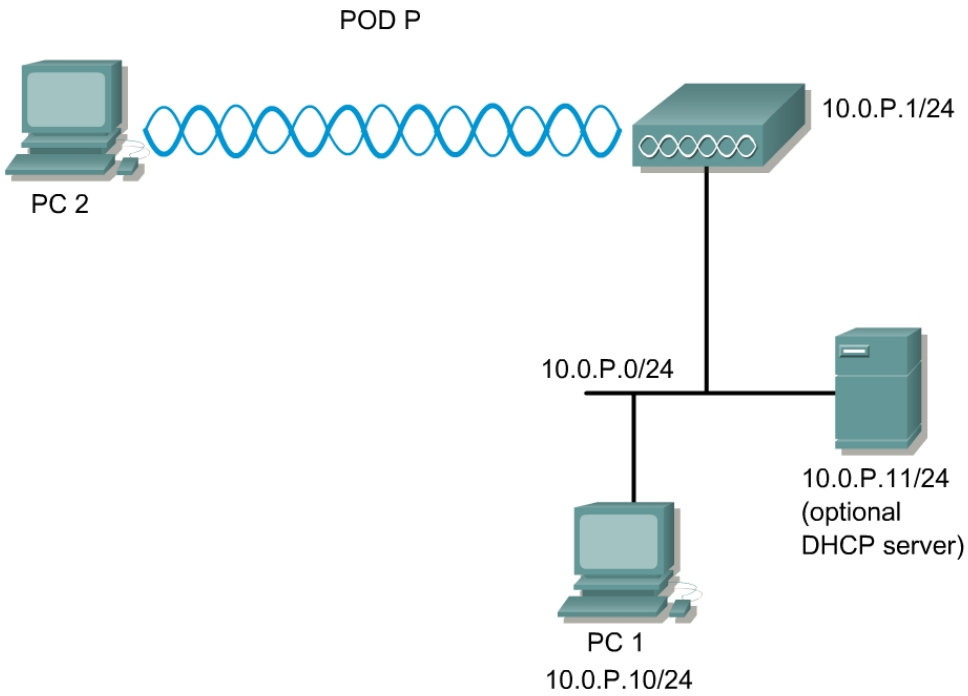
Objective

In this lab, the student will learn about the second generation of Wireless LAN security and how to implement LEAP on a Wireless LAN for secure client authentication.

The main steps to this lab are:

1. Configure AP WEP Key or Cipher
2. Configure RADIUS Server
3. Configure Local RADIUS Server
4. Configure Users
5. Configure and verify LEAP/EAP Authentication on the AP
6. Configure LEAP/EAP on the client (PC2) through ACU
7. Monitor the connection, login, and authentication statistics

Topology



Scenario

One way to secure wireless LANs and improve network security is to use authentication for accessing the AP. Wireless clients can use Extensible Authentication Protocol (EAP) to authenticate to a wireless LAN. 802.1x local RADIUS authentication is available on the 1100 and 1200 APs. This allows LEAP/EAP to be used without requiring a Cisco Secure ACS Server. Furthermore, this feature provides a backup for ACS Servers in an Enterprise network.

Preparation

Prior to this lab, the Cisco Aironet AP should be configured to allow clients to associate. The IP address, hostname and SSID should be configured on the AP. A PC should be installed with a Cisco Aironet Client Card, and it should already be associated to the AP.

Cable the equipment according to the Topology.

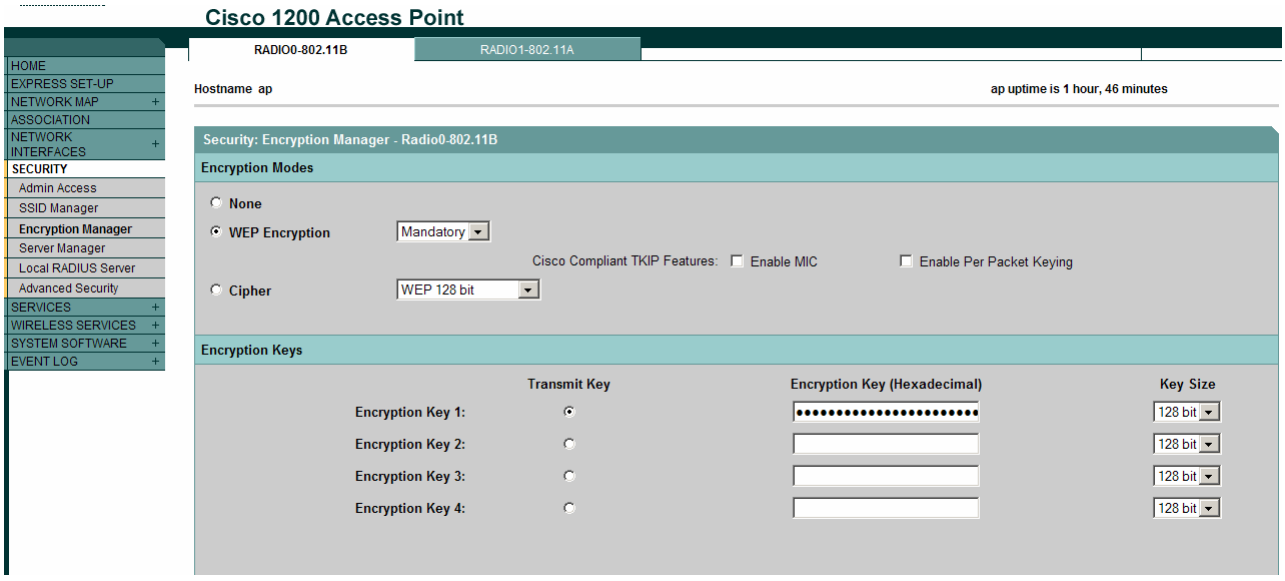
Update the Aironet Client Utility version 6.0 or later.

Tools and Resources

Each team of students will require the following:

- Cisco Aironet AP
- Hub or switch
- A wireless PC, laptop, or handheld (PC2) with a Cisco Aironet Client Adapter Card and utility properly installed and configured.
- One wired PC (PC1)

Step 1 Configure the AP WEP keys or cipher



In order to enable Cisco LEAP on the AP, WEP Encryption or a Cipher must be enabled.

a. From the **SECURITY>Encryption Manager** Page of the AP, configure the Encryption Key 1.

b. Click on the WEP Encryption radio button.

c. Select Mandatory.

d. Click **Apply-All**.

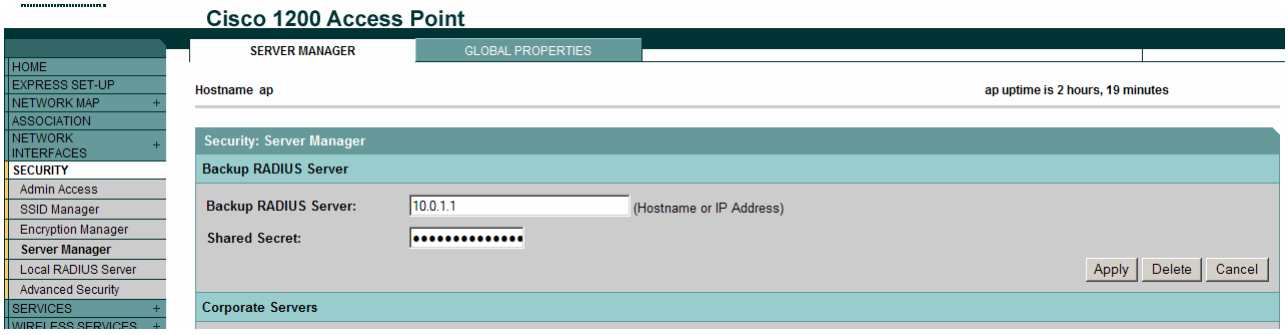
e. The **Cipher** option can be used for greater security. What options are available?

_____

_____

_____

Step 2 Configure RADIUS server



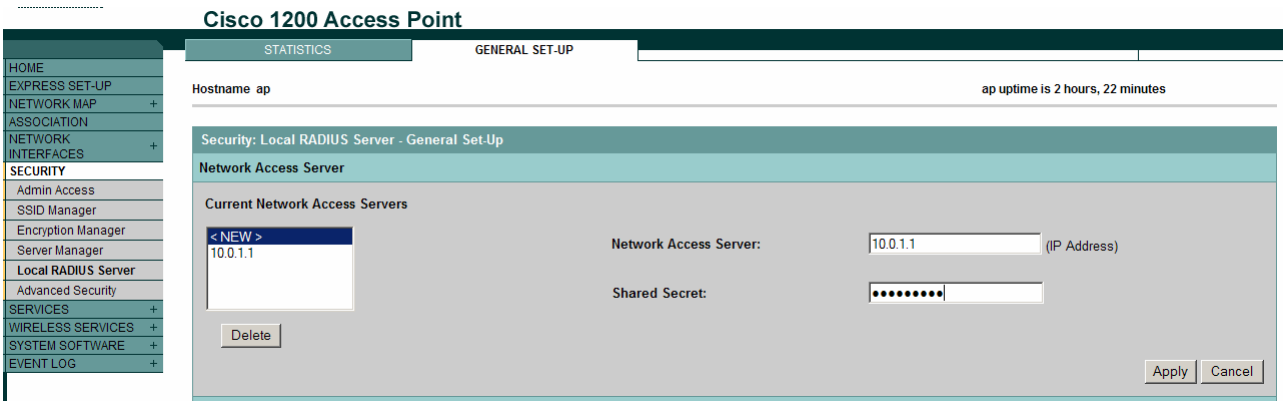
Complete the following steps to configure the Backup RADIUS Server from the **SECURITY>Server Manager** Page:

a. Enter the IP address of the Local RADIUS server in the Server Name/IP entry field. This will be the IP address of the AP where the local RADIUS database is running. Should be 10.0.P.1

b. Enter the Shared Secret key of ***secretkey***

c. Click **Apply.**

Step 3 Configure local RADIUS server



Complete the following steps to configure a Local RADIUS Server from the **SECURITY>Local RADIUS Server** Page:

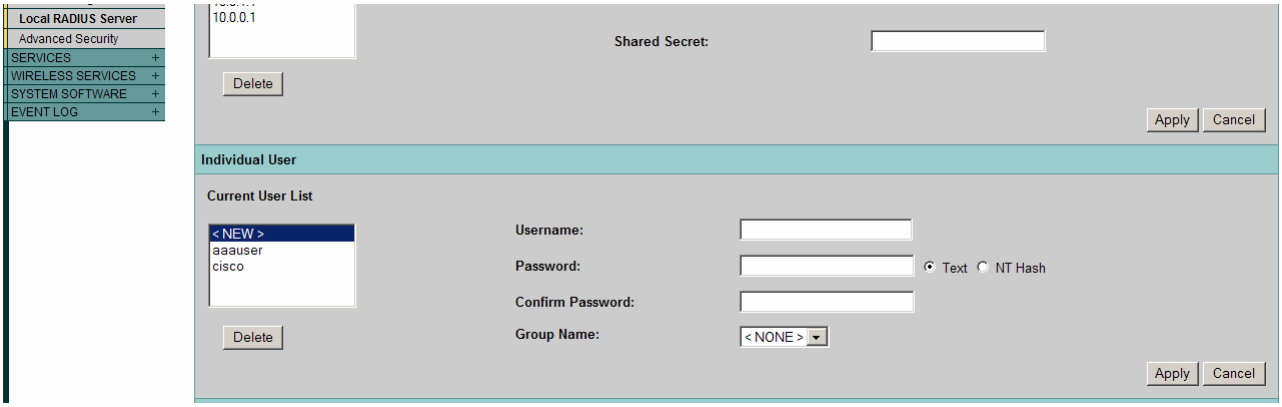
a. Click on the **GENERAL SET-UP** tab.

b. Enter the IP address of the Local RADIUS server in the Server Name/IP entry field. This will be the IP address of the AP where the local RADIUS database is running, 10.0.P.1

c. Enter the Shared Secret key of ***secretkey***

d. Click **Apply.**

Step 4 Configure users



Complete the following steps to configure users from the **SECURITY** > **Local RADIUS Server** Page:

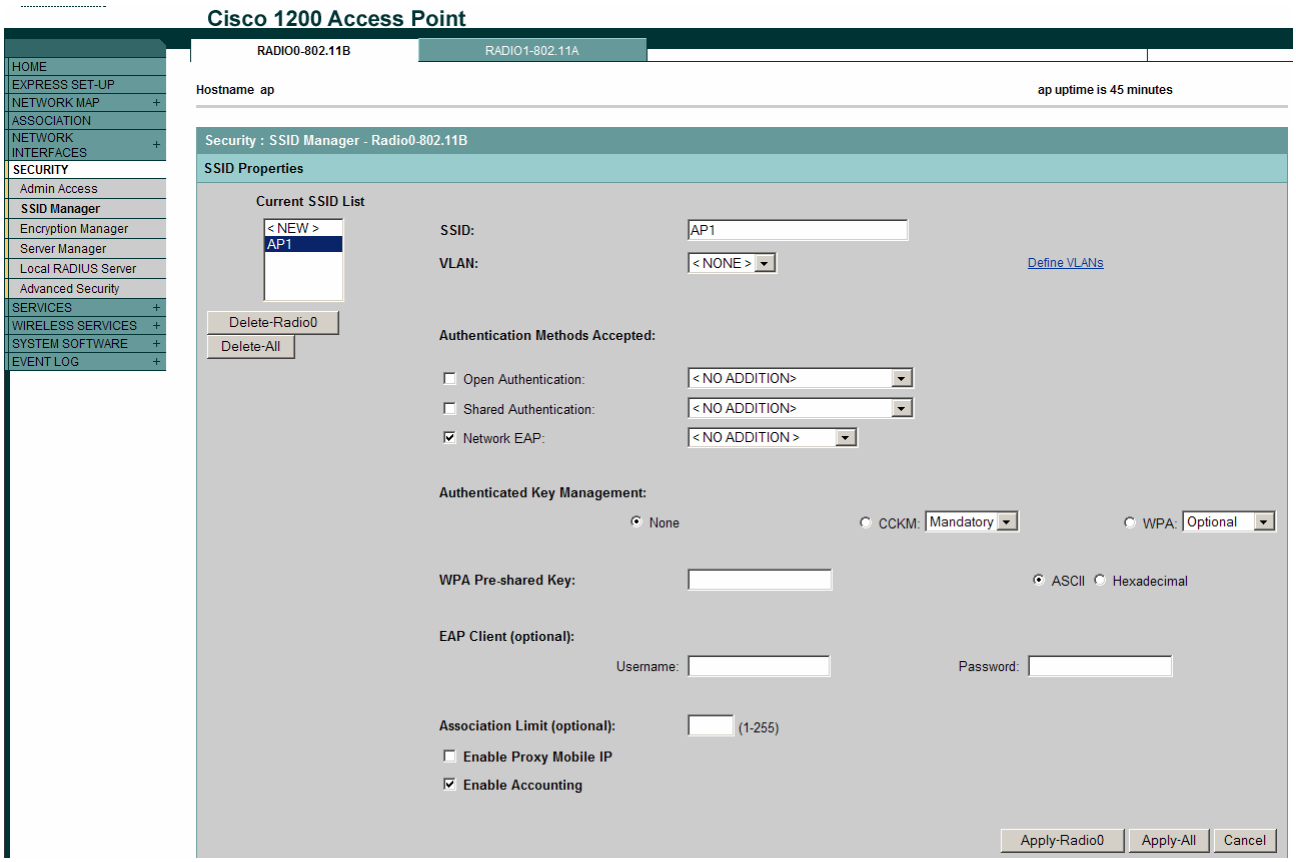
a. Continue from the **GENERAL SET-UP** tab.

b. Enter the following users:

User	Username	Password
1	aaauser	aaapass
2	Cisco1	ciscopass

c. Click **Apply**.

Step 5 Configure authentication on AP



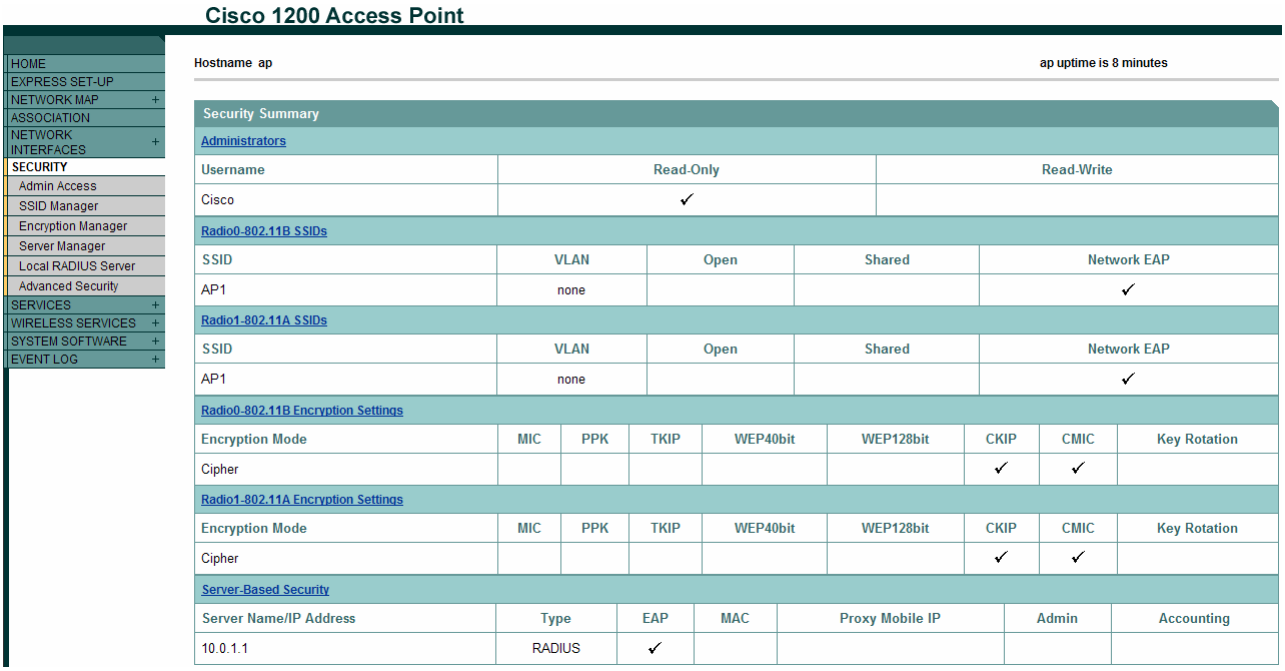
In order to enable Cisco LEAP on the AP, complete the following steps to configure the Authentication Method:

a. On the **SECURITY>SSID** Manager page of the AP, create a new SSID of AP**P**, where **P** is the Pod number.

b. Check the **Network EAP** box.

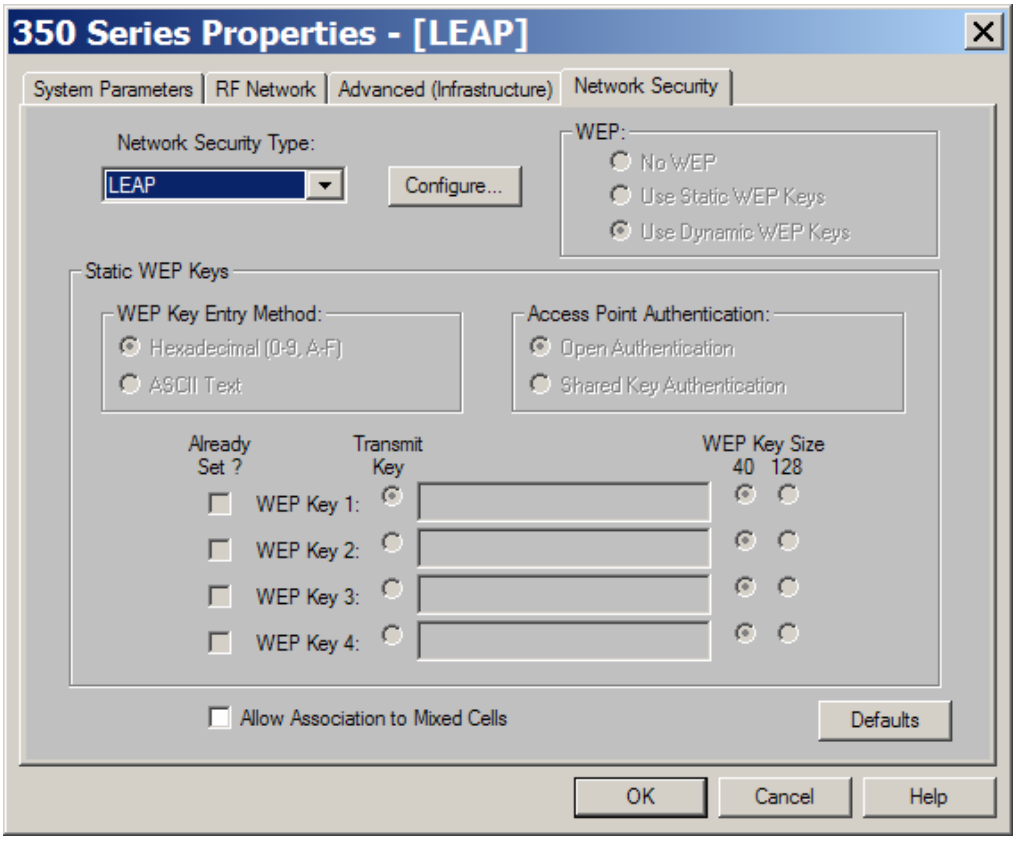
c. Click the **Apply-All** button.

Step 6 Verify the LEAP configuration



From the **SECURITY** Home page of the AP, verify Network EAP is checked and the only SSID is AP**P**. The default tsunami SSID should be deleted for security. Also verify the Server Based Security is configured correctly as shown.

Step 7 Configuring LEAP on the ACU



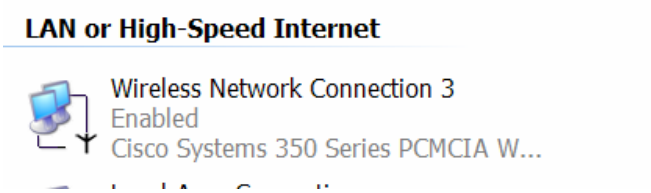
In order to enable the EAP in the Aironet client utility, complete the following steps:

a. On PC2, configure the TCP/IP settings for the **Wireless Network Connection** if a DHCP server is not available. Otherwise, when the client authenticates, the wireless PC will not be able to communicate through IP.

   i. IP address of 10.0.P.12

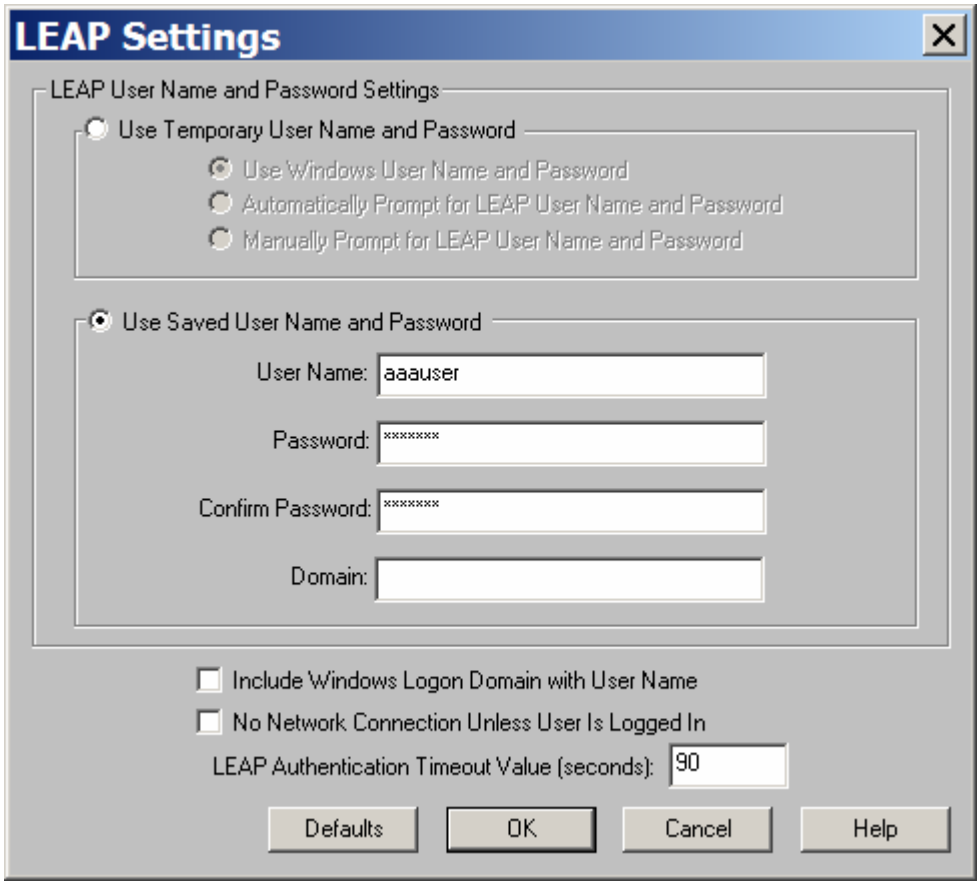
   ii. Subnet mask of 255.255.255.0

   iii. Gateway of 10.0.P.254



b. Go to the **Network Security** tab in the Aironet Client Utility on PC2 and each of the wireless client computers.

c. Select the **LEAP** from the **Network Security Type:** drop down list and click **Configure**.



d. Click on **Use Saved User Name and Password.**

   i. Enter ***aaauser*** for the **User Name.**

   ii. Enter ***aaapass*** for the **Password.**

   iii. Enter ***aaapass*** for the **Confirm Password.**

   iv. Uncheck the two checkboxes at the bottom of the LEAP Settings window.

   v. Click **OK**.

e. In the profile manager, select the profile which LEAP is configured on and click OK. If a save username and password was not configured, an authentication screen should come up asking for a user ID and password. Type in the following.

   i. The username for authentication is ***aaauser***.

   ii. The password for authentication is ***aaapass***.

f. The ACM icon should change to green once the authentication is complete.

g. From PC1, PC2 or the ACS Server, browse to the AP **ASSOCIATION** page to verify the connection.

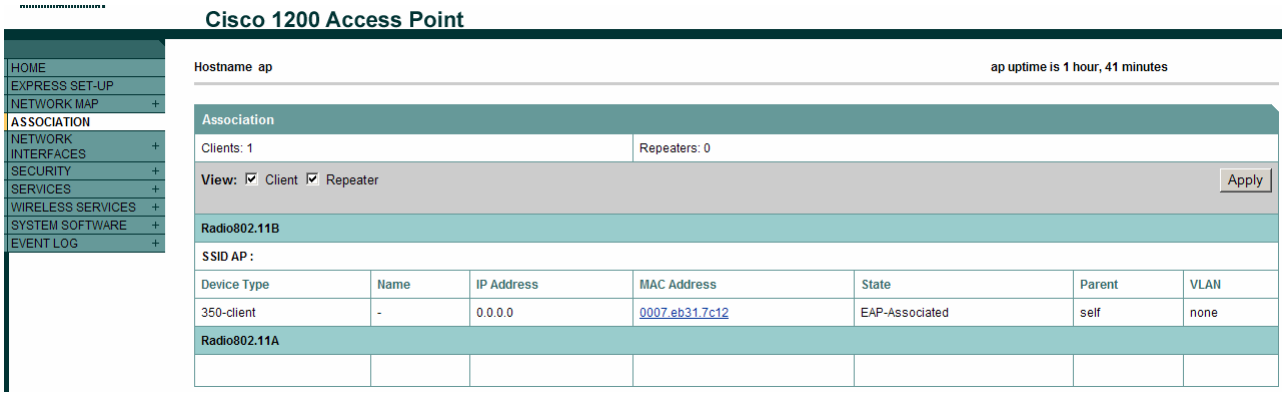
h. What are the three authentication states?

_____

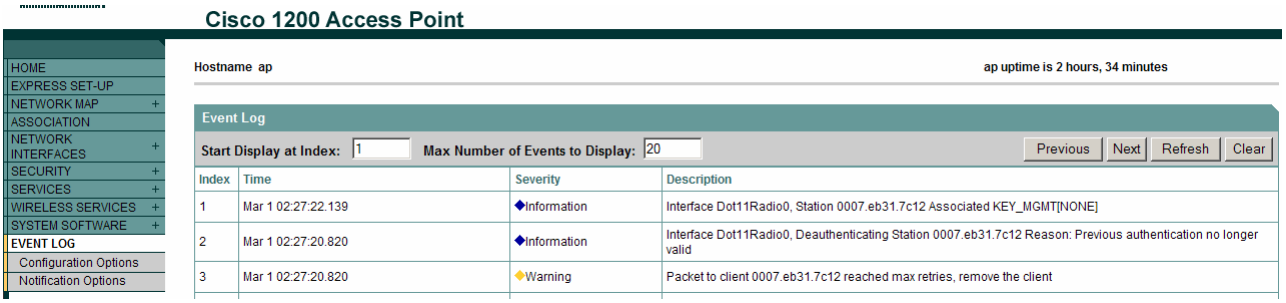
_____

_____

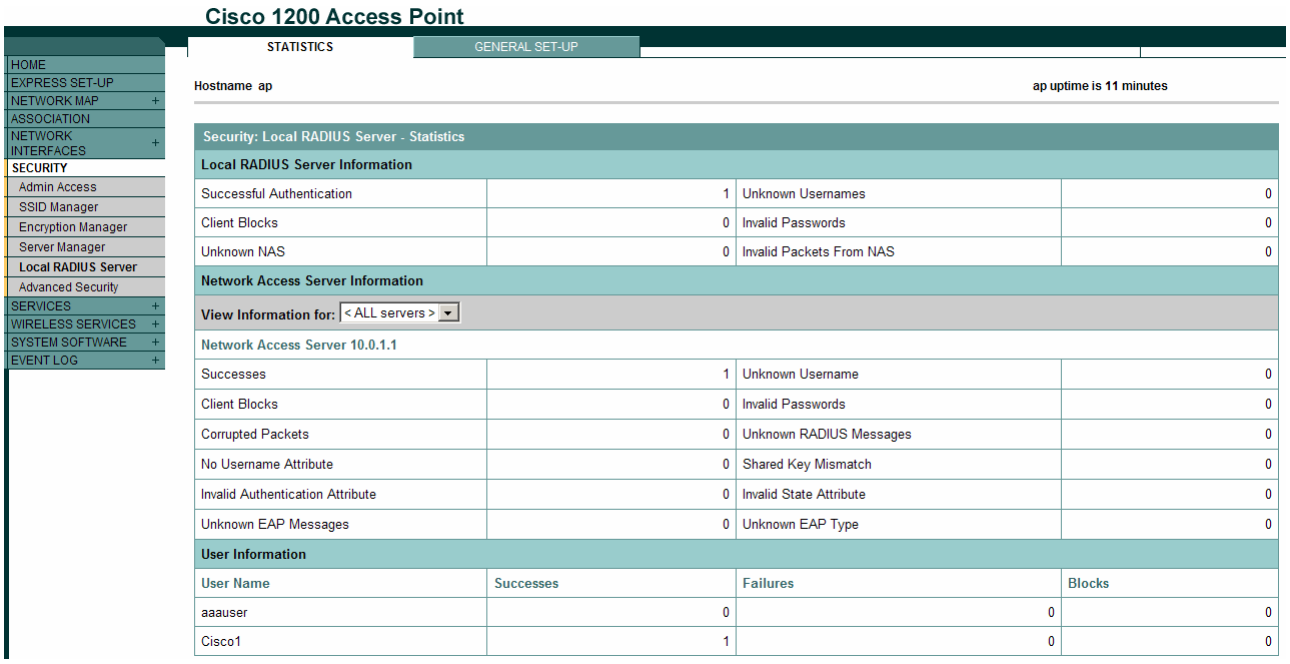
Step 8 Verify the wireless connection



From the **ASSOCIATION** page of the AP, verify the association state. This should display all of the connected clients.



From the **EVENT LOG** Page of the AP, check the association logs.



From the **SECURITY>Local RADIUS Server** Page of the AP, click on the **STATISTICS** tab. Verify the User Information for authentication successes, failures, and blocks.

Lab 8.4.5.2 Configuring LEAP/EAP using Cisco Secure ACS (OPTIONAL)

Estimated Time: 60 minutes

Number of Team Members: Students can work in teams of two.

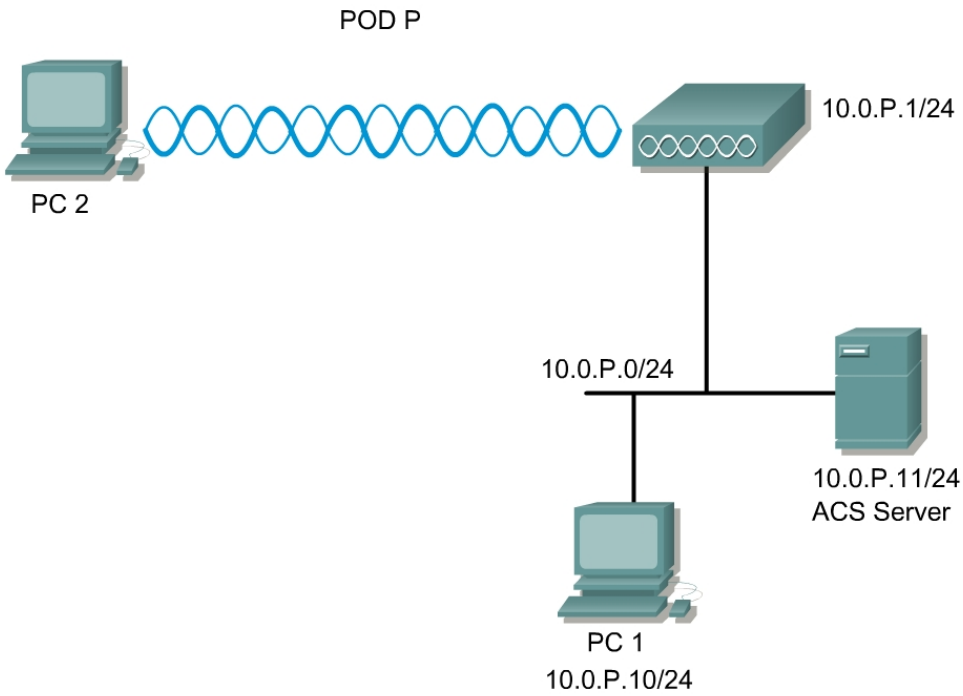
Objective

In this lab, the student will learn about the second generation of Wireless LAN security and how to implement LEAP on a Wireless LAN for secure client authentication.

The main steps to this lab are:

8. Install Cisco Secure ACS software (Instructor)
9. Configure the Cisco Secure ACS software
10. Create user accounts in the Access Control Server (ACS)
11. Configure AP WEP Key or Cipher
12. Configure LEAP/EAP on the AP
13. Configure LEAP/EAP on the client (PC2) through ACU
14. Monitor the connection and login

Topology



Scenario

One way to secure wireless LANs and improve network security is to use authentication for accessing the AP. Wireless clients can use Extensible Authentication Protocol (EAP) to authenticate though a wireless LAN. EAP can authenticate through digital certificates such as public key infrastructure (PKI) or passwords and usernames. EAP can pass authentication information onto an Authentication, Authorization, Accounting (AAA) RADIUS server, such as a Cisco Access Control Server (ACS).

The Network Authentication Process can be summarized in four main stages:

- The client adapter uses the username and password to start the authentication process.
- The AP communicates with the EAP-compliant RADIUS server to authenticate the username and password.
- If the username and password are valid, the RADIUS server and the client adapter negotiate a dynamic, session-based Wired Equivalent Privacy (WEP) key. The key, which is unique for the authenticated client, provides the client with secure network access.
- The client and AP use the WEP key for all data transmissions during the session.

Preparation

Prior to this lab, the Cisco Aironet AP should be configured to allow clients to associate. The IP address, hostname and SSID should be configured on the AP. A PC should be installed with a Cisco Aironet Client Card, and it should already be associated to the AP.

Cable the equipment according to the Topology.

A Windows 2000 Server running ACS 2.6 or above must be available.

Update the Aironet Client Utility version 6.0 or later.

Tools and Resources

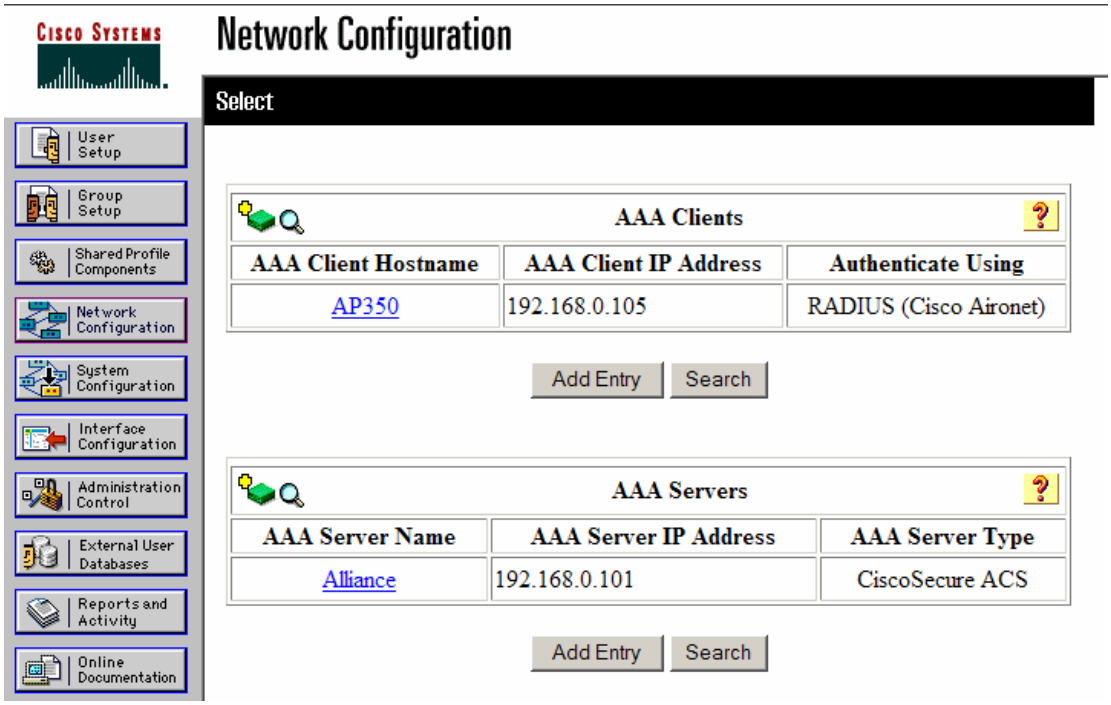
Each team of students will require the following:

- Cisco Aironet AP
- Hub or switch
- A wireless PC, laptop, or handheld (PC2) with a Cisco Aironet Client Adapter Card and utility properly installed and configured.
- Windows 2000 Server running Cisco Secure ACS 2.6 or above.
- One wired PC (PC1)

An evaluation copy of Cisco Secure ACS can be downloaded from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des

Step 1 Add a AAA client

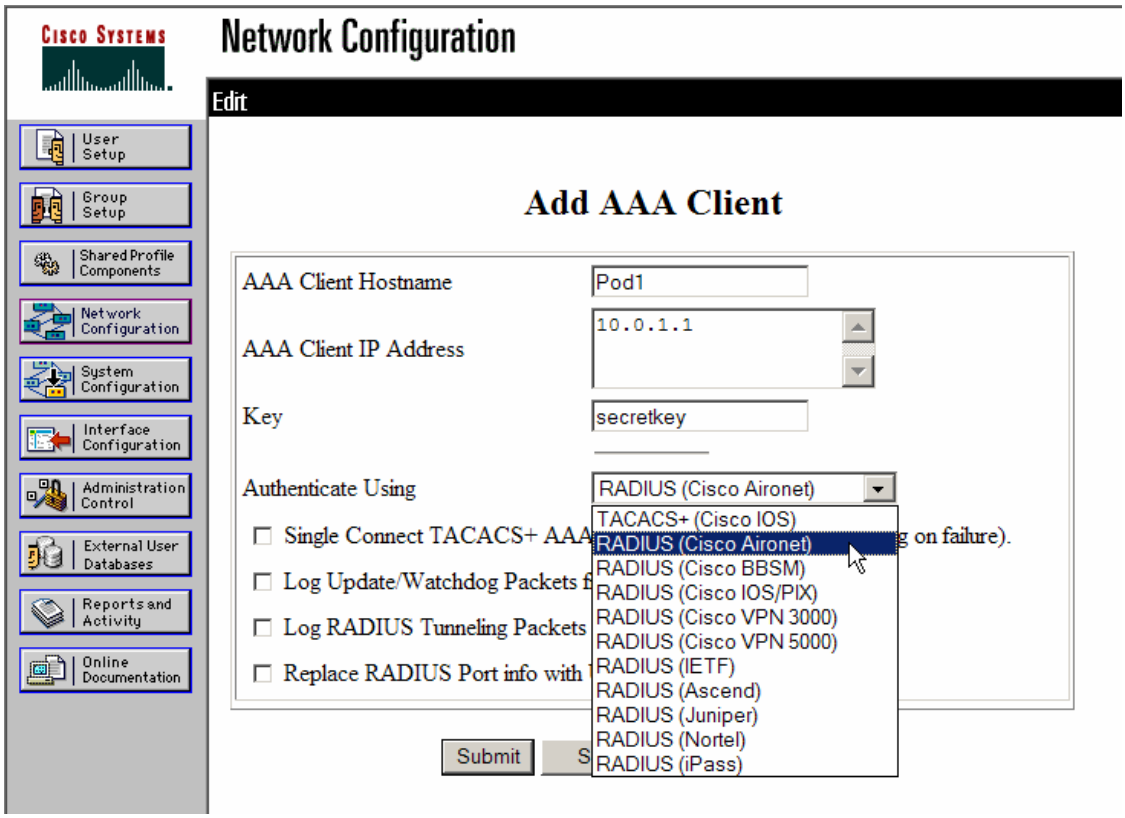


Follow these steps to include the AP as a **AAA Client** in Cisco Secure ACS:

a. After properly loading the TACACS software on the Windows Server computer, on the ACS main menu, click **Network Configuration**.

b. Click **Add New Access Server**, or it may display **Add Entry**.

Step 2 Configure AAA Client



a. In the **Network Access Server Hostname** box, type the system name of the AP. Enter ***PodP*** (where **P** is the Pod number)

b. In the **Network Access Server IP address** box, type the AP IP address. Enter **10.0.P.1** (where P is the Pod number)

c. In the **Key** box, type the shared secret that the AP and Cisco Secure ACS use to encrypt the data. For correct operation, the identical key, which is case sensitive, must be configured on the AP. For simplicity of the lab, use the word ***secretkey***.

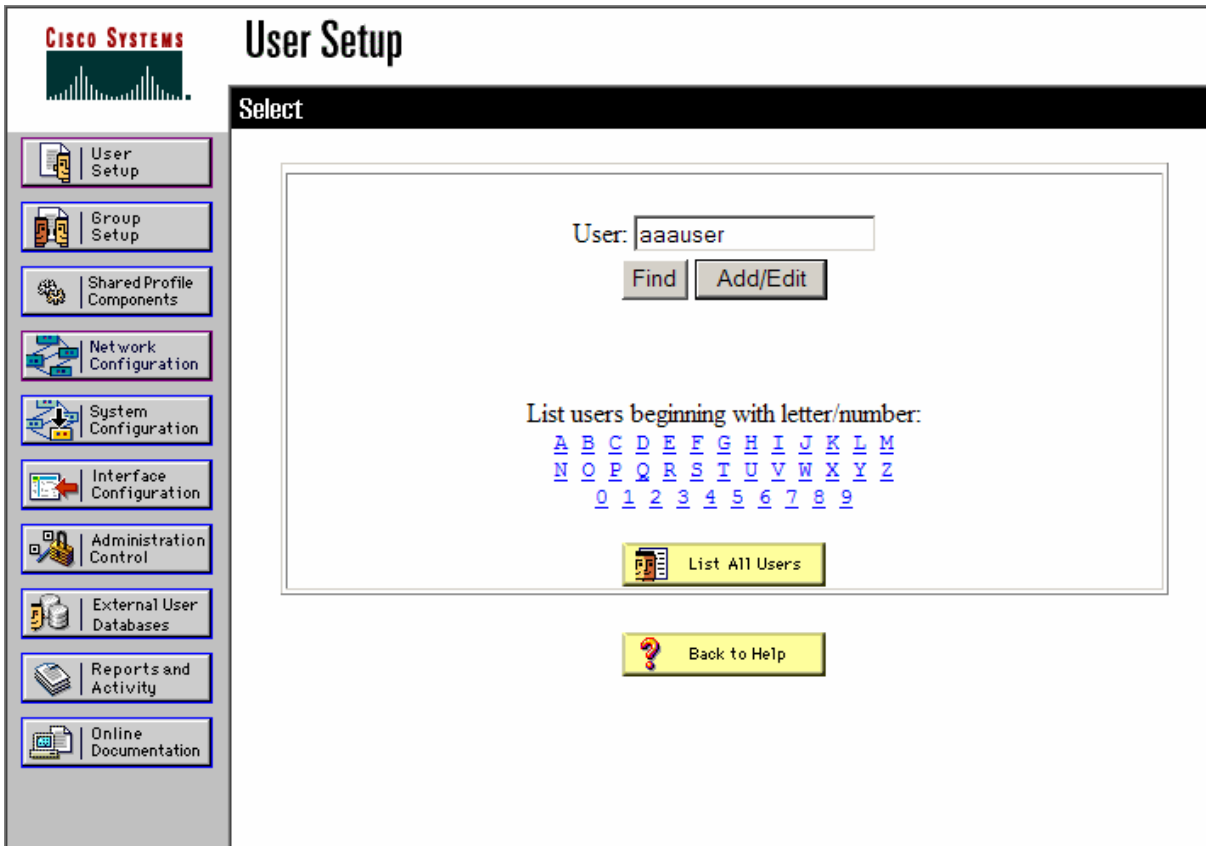
d. From the **Authenticate Using** list box, click the network security protocol. Select **RADIUS (Cisco Aironet**).

e. Each AP in the class will have to be added to this list if it will be using LEAP.

f. Remote Access Services must be started on the RADIUS Server for LEAP to work properly. To save the changes and apply them immediately, click the **Submit + Restart** button.

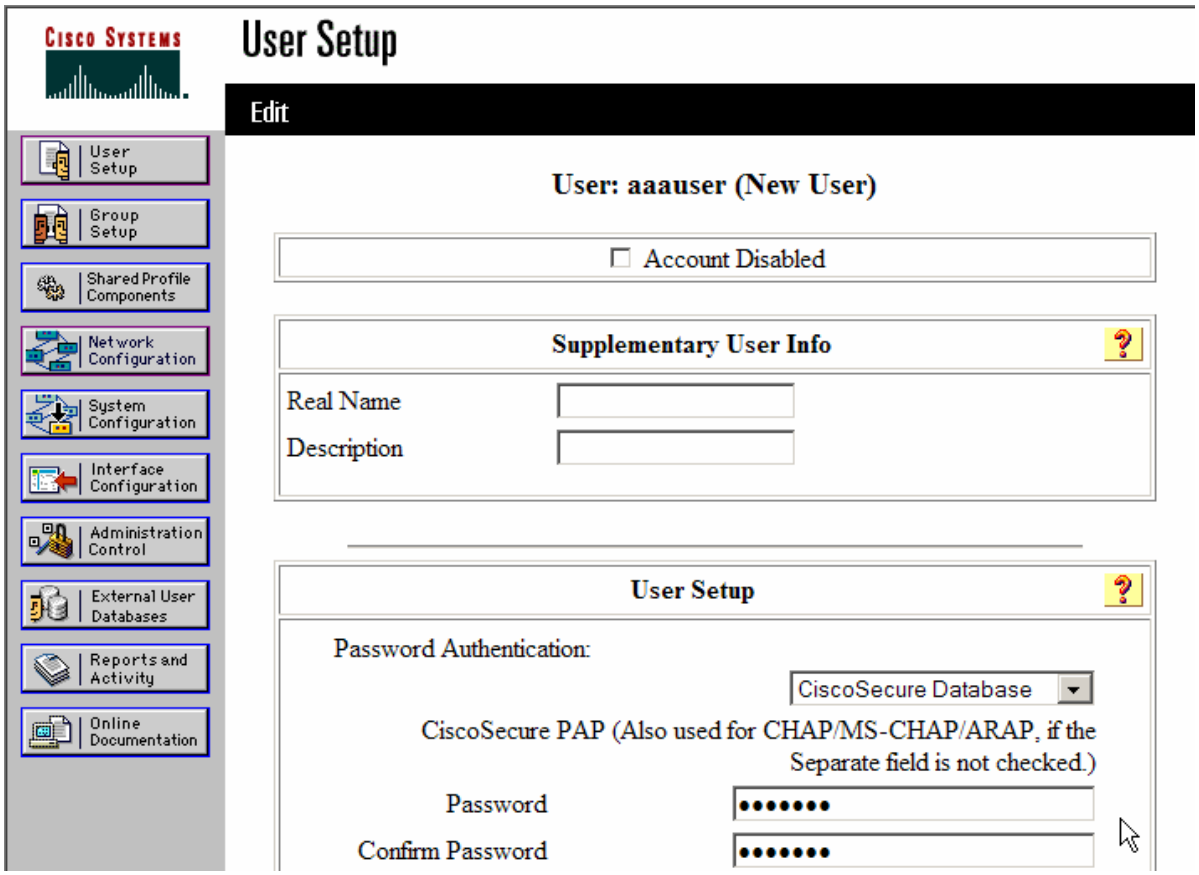
Note	It is very important to click **Submit + Restart**

Step 3 Create a user account in the Access Control Server (ACS)



a. Click on the **User Setup** button located on the left side of the ACS Home page.

b. Type the user name ***aaauser*** in the **User**: field box, and then click on the **Add/Edit** button beneath this box.

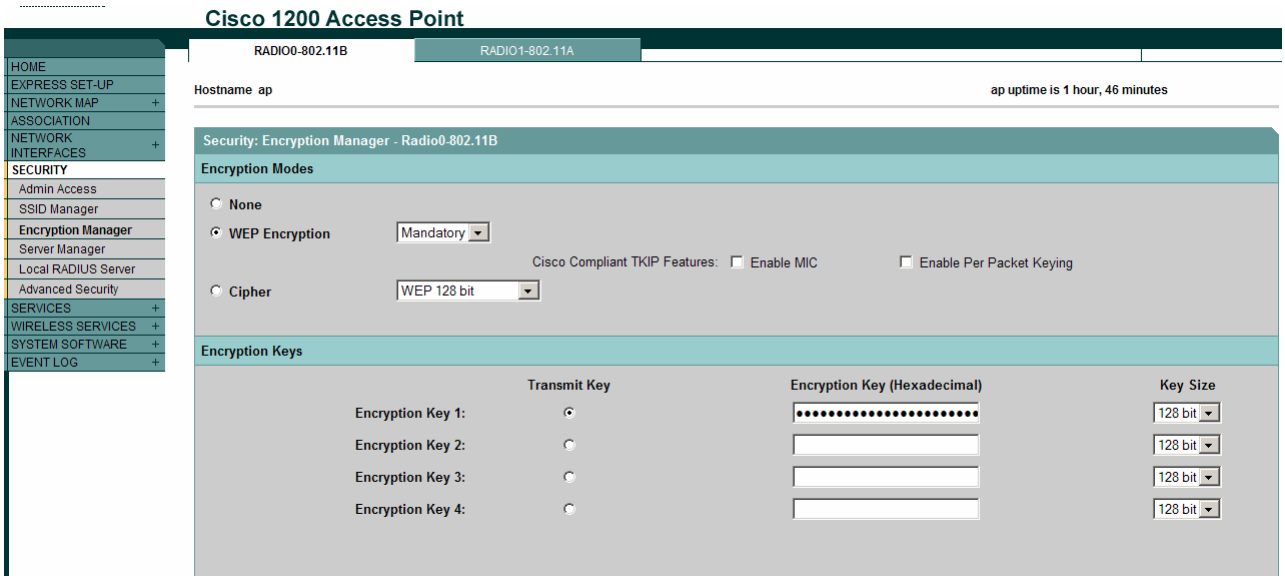


c. Type the user password ***aaapass*** in the Password: box and then type ***aaapass*** in the Confirm Password: box.

d. Click on the **Submit** button to add this entry to the user list.

e. Additional users can be added to this database list for each wireless PC client.

Step 4 Configure the AP WEP Keys or Cipher



In order to enable Cisco LEAP on the AP, WEP Encryption or a Cipher must be enabled.

a. From the **SECURITY>Encryption Manager** page of the AP, configure the Encryption Key 1.

b. Click on the WEP Encryption radio button.

c. Select Mandatory.

d. Click **Apply-All**.

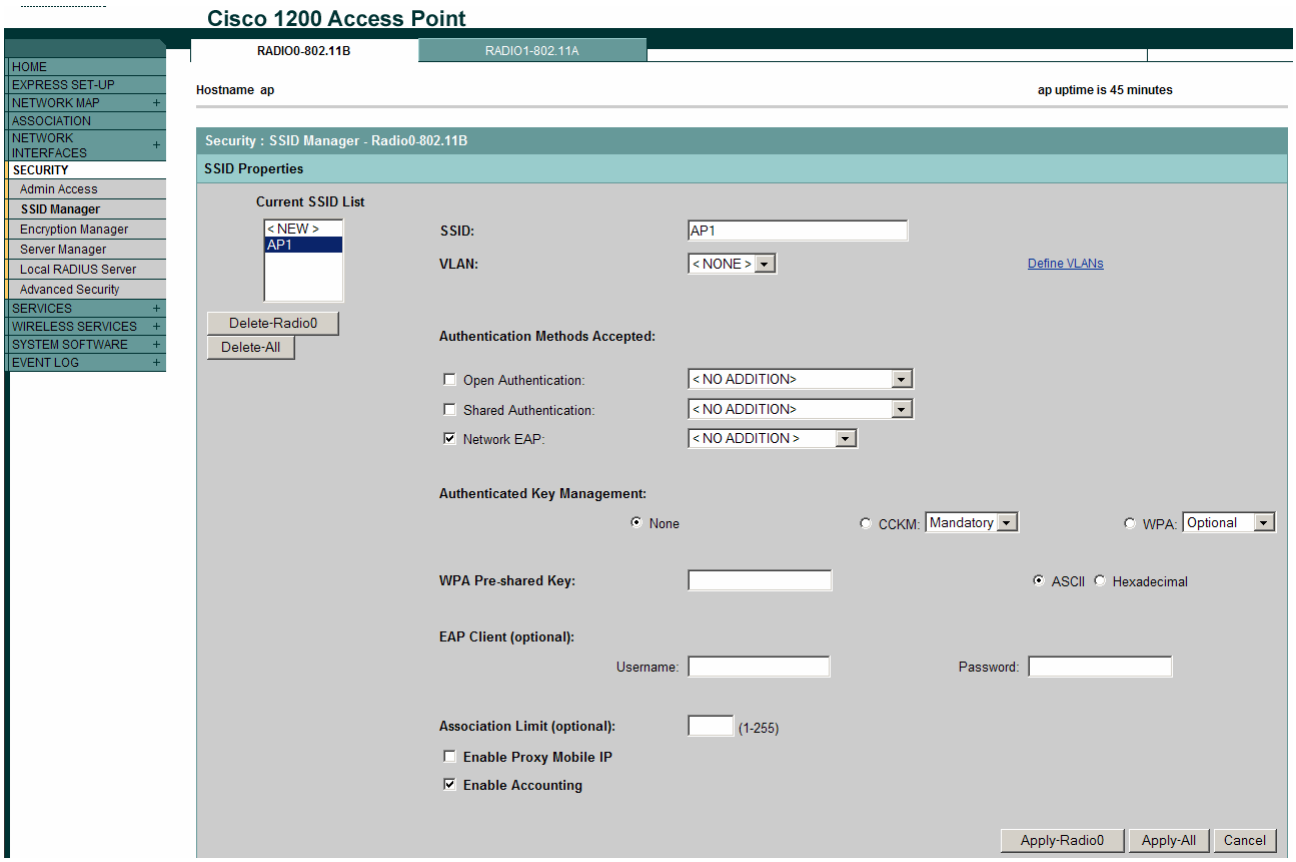
e. **The Cipher** option can be used for greater security. What options are available?

_____

_____

_____

Step 5 Configure authentication on AP



In order to enable Cisco LEAP on the AP, complete the following steps to configure the Authentication Method:

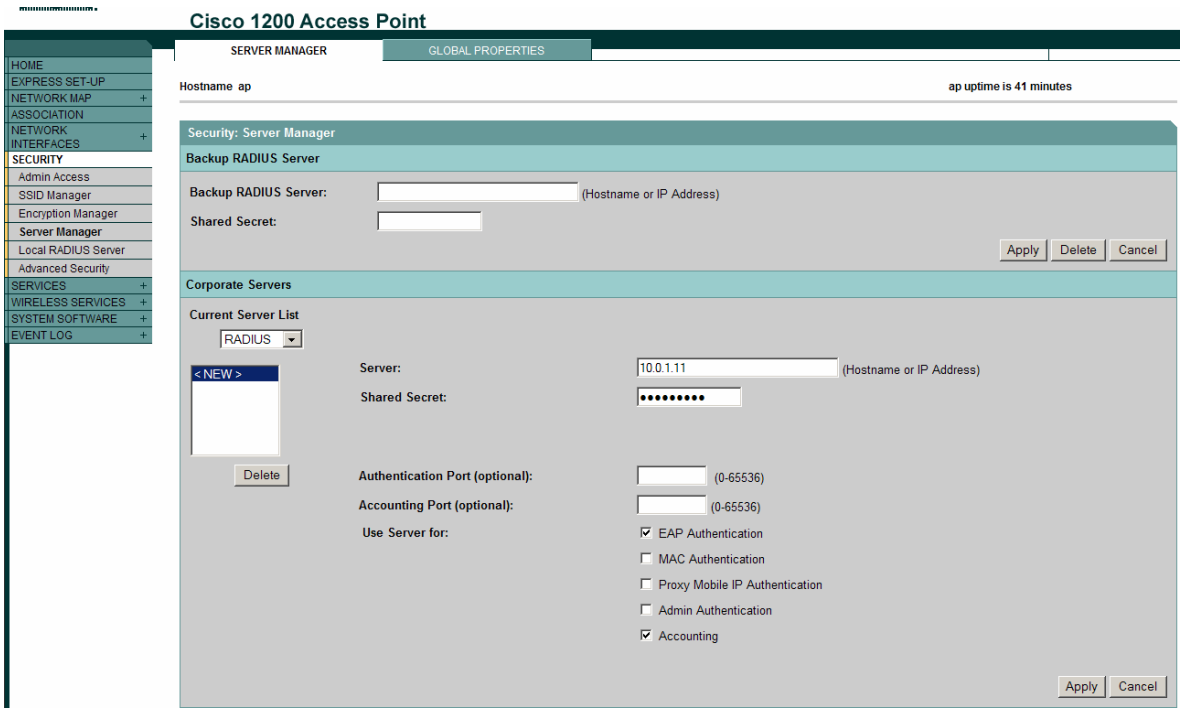
a. On the **SECURITY>SSID Manager** page of the AP, create a new SSID of AP**P** (where **P** is the Pod number)

b. Check the **Network EAP** box.

c. Check the **Enable Accounting** box.

d. Click the **Apply-All** button.

Step 6 AP RADIUS configuration



In order to enable Cisco LEAP on the AP, complete the following steps to configure a RADIUS Server from the SECURITY>**Server Manager** Page:

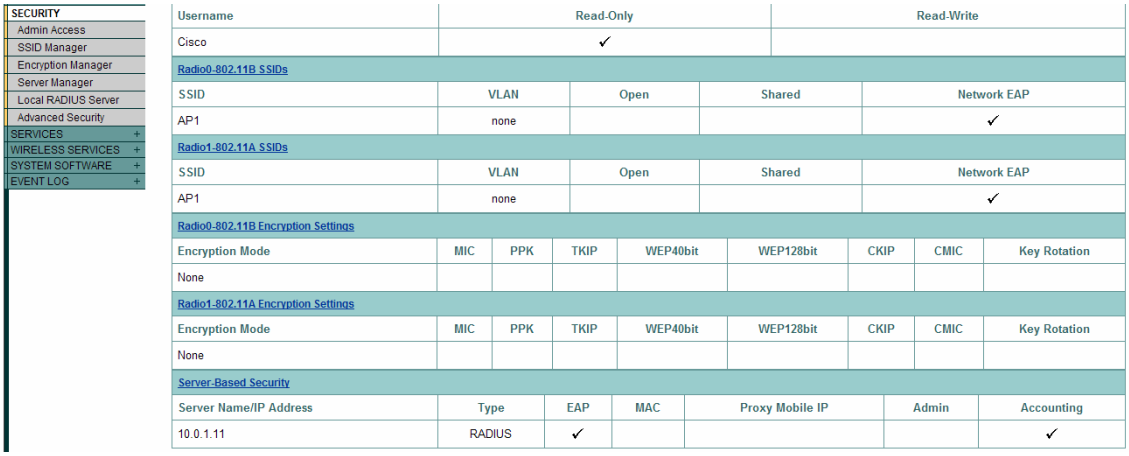
a. Enter the IP address of the RADIUS server in the Server Name/IP entry field. This will be the IP address of the Windows Server where the ACS software is running. Should be 10.0.P.11.

b. Enter the port number the RADIUS server uses for authentication. This will default to port **1645** if the field is left empty.

c. Enter the shared secret used by the RADIUS server in the Shared Secret entry field. This was configured as ***secretkey*** on ACS. The shared secret on the AP must match the shared secret on the RADIUS server.

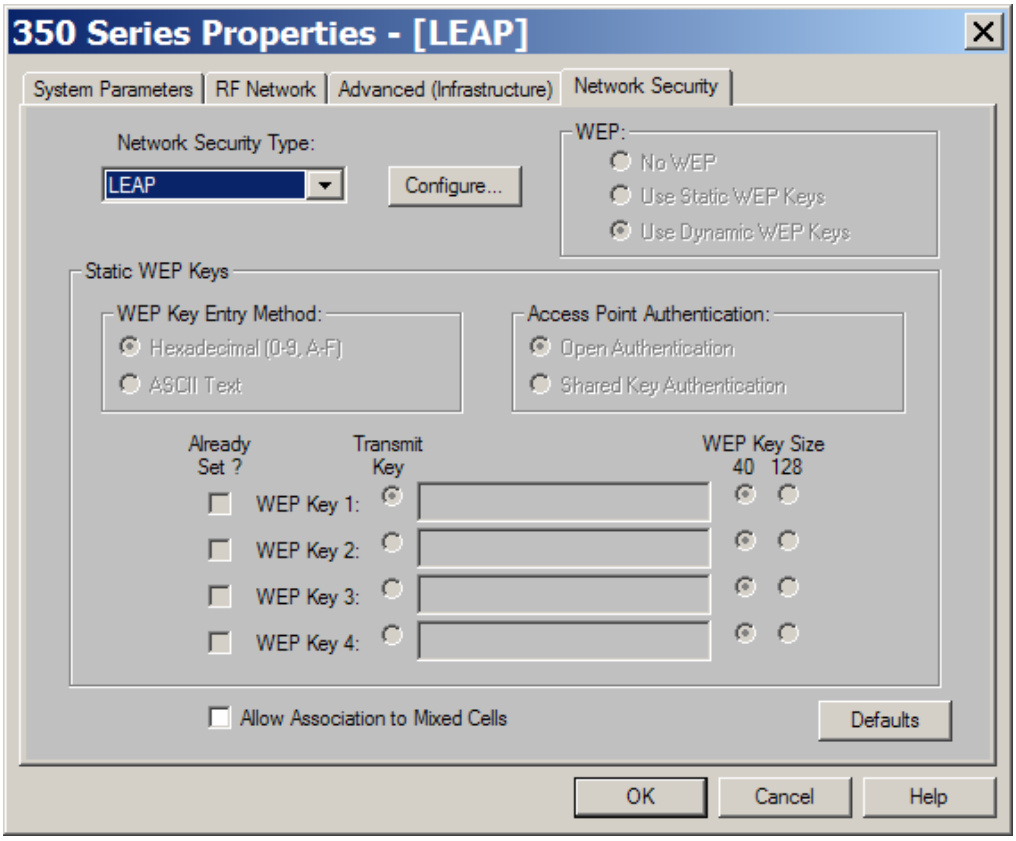
d. Check the **EAP Authentication** and **Accounting** box.

e. Click the APPLY button.



f. From the **SECURITY** Home page of the AP, verify Network EAP is checked and the only SSID. The default tsunami SSID should be deleted for security. Also verify the Server Based Security is configured correctly as shown.

Step 7 Configuring LEAP on the ACU



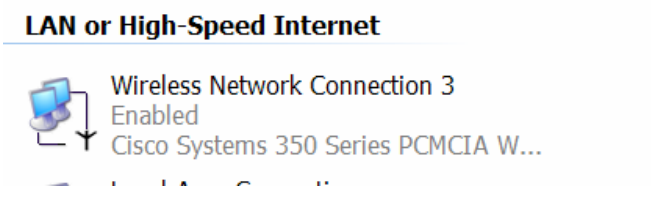
In order to enable the EAP in the Aironet client utility, complete the following steps:

a. On PC2, configure the TCP/IP settings for the **Wireless Network Connection** if a DHCP server is not available. Otherwise, when the client authenticates, the wireless PC will not be able to communicate through IP.

   i. IP address of 10.0.P.12

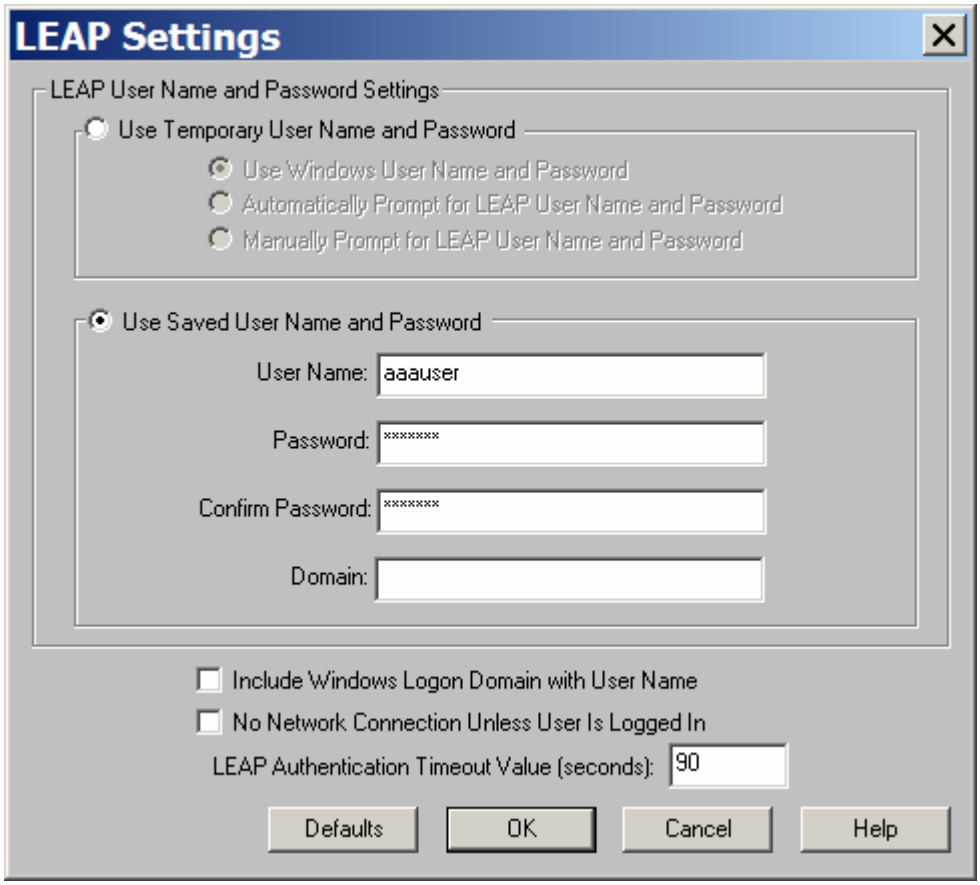
   ii. Subnet mask of 255.255.255.0

   iii. Gateway of 10.0.P.254



b. Go to the **Network Security** tab in the Aironet Client Utility on PC2 and each of the wireless client computers.

c. Select the **LEAP** from the **Network Security Type:** drop down list and click **Configure**.



d. Click on **Use Saved User Name and Password**

   i. Enter ***aaauser*** for the **User Name**

   ii. Enter ***aaapass*** for the **Password**

   iii. Enter ***aaapass*** for the **Confirm Password**

   iv. Uncheck the two checkboxes at the bottom of the LEAP Settings window

   v. Click **OK**.

e. In the profile manager, select the profile which LEAP is configured on and click OK. If a save username and password was not configured, an authentication screen should come up asking for a user ID and password. Type in the following.

   i. The username for authentication is ***aaauser***.

   ii. The password for authentication is ***aaapass***.

f. From PC1, PC2 or the ACS Server, browse to the AP **ASSOCIATION** page to verify the connection.

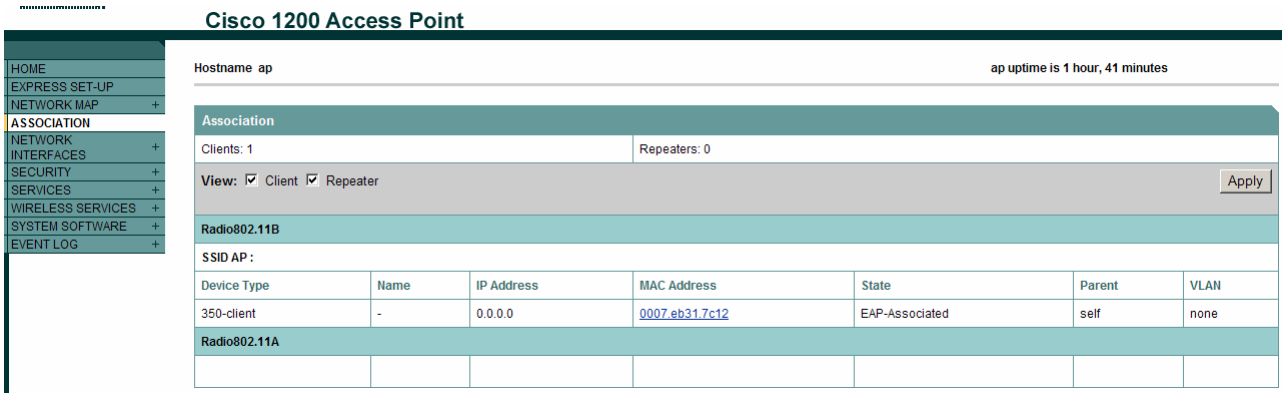
g. What are the three authentication states?

_____

_____

_____

Step 8 Verify connection

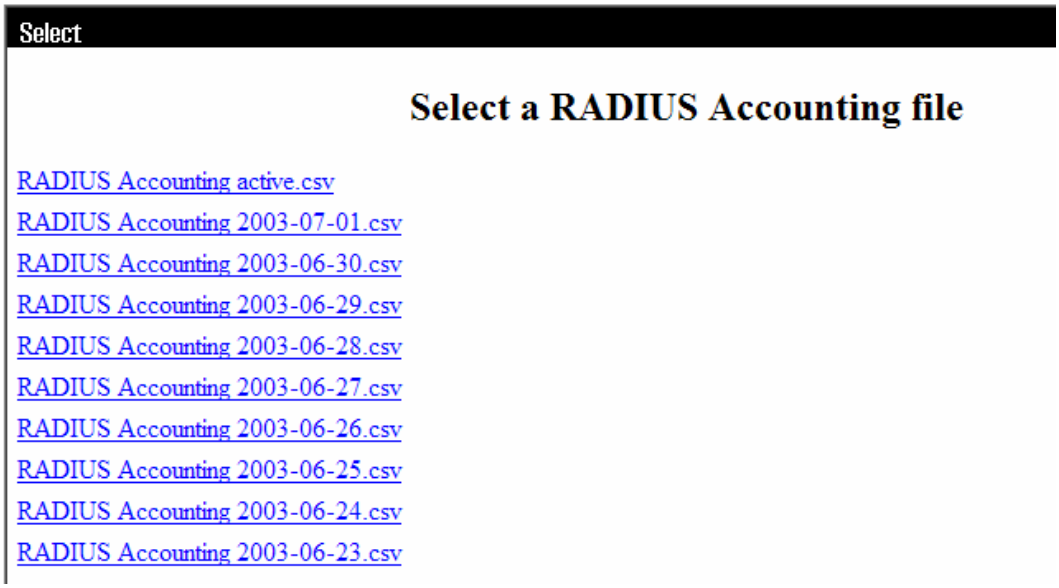


From the ASSOCIATION page of the AP, verify the association state. This should display all of the connected clients.

Step 9 Monitoring LEAP login on ACS (Optional)

a. Click on the **Reports and Activity** button located on the left side of the ACS Home page.

b. Next, click on the RADIUS Accounting link.



c. On the right hand side, select the **RADIUS Accounting active.csv** link.

d. Fill in the information found in the accounting file below.

Lab 8.5.4.1 Configure Enterprise Security on AP

Estimated Time: 30 minutes

Number of Team Members: Students will work in teams of two.

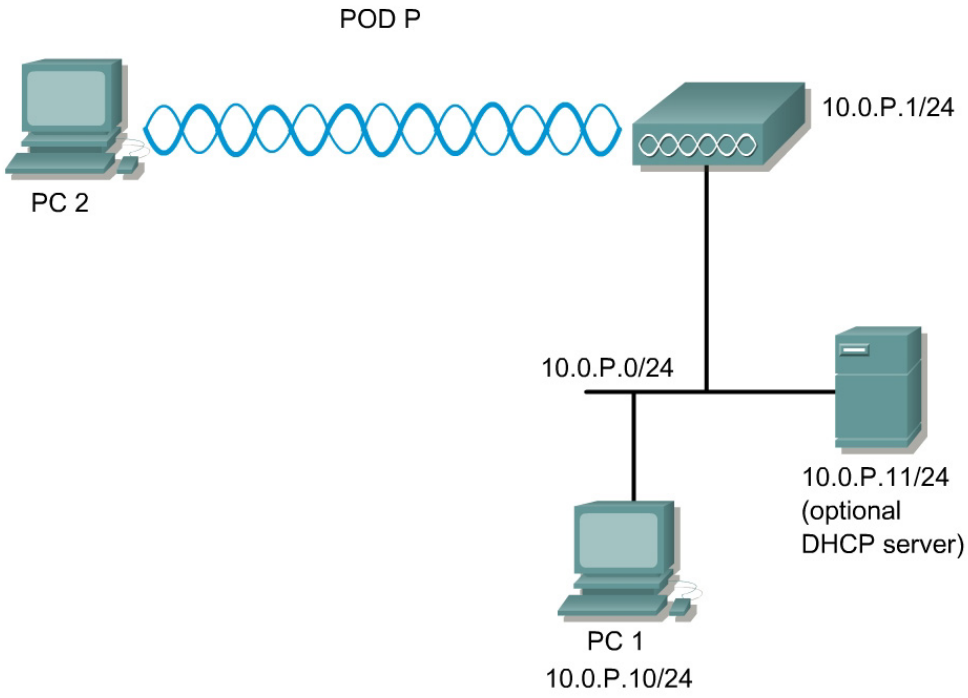
Objective

In this lab, students will demonstrate an understanding of the role of enterprise wireless network security. Additionally, students will configure MIC, TKIP and BKR on an AP.

Scenario

The purpose of WEP is to protect the privacy of transmitted data. However, WEP has inherent security weaknesses. There are many mechanisms available to provide additional security for WEP.

Topology



Preparation

The AP and PCs should be properly setup according to the topology prior to the lab. Ensure an existing wireless connection is present from PC2 to the AP.

Tools and Resources

Each team of students will require the following:

- One AP
- Wireless PC with the ACU
- Wired PC

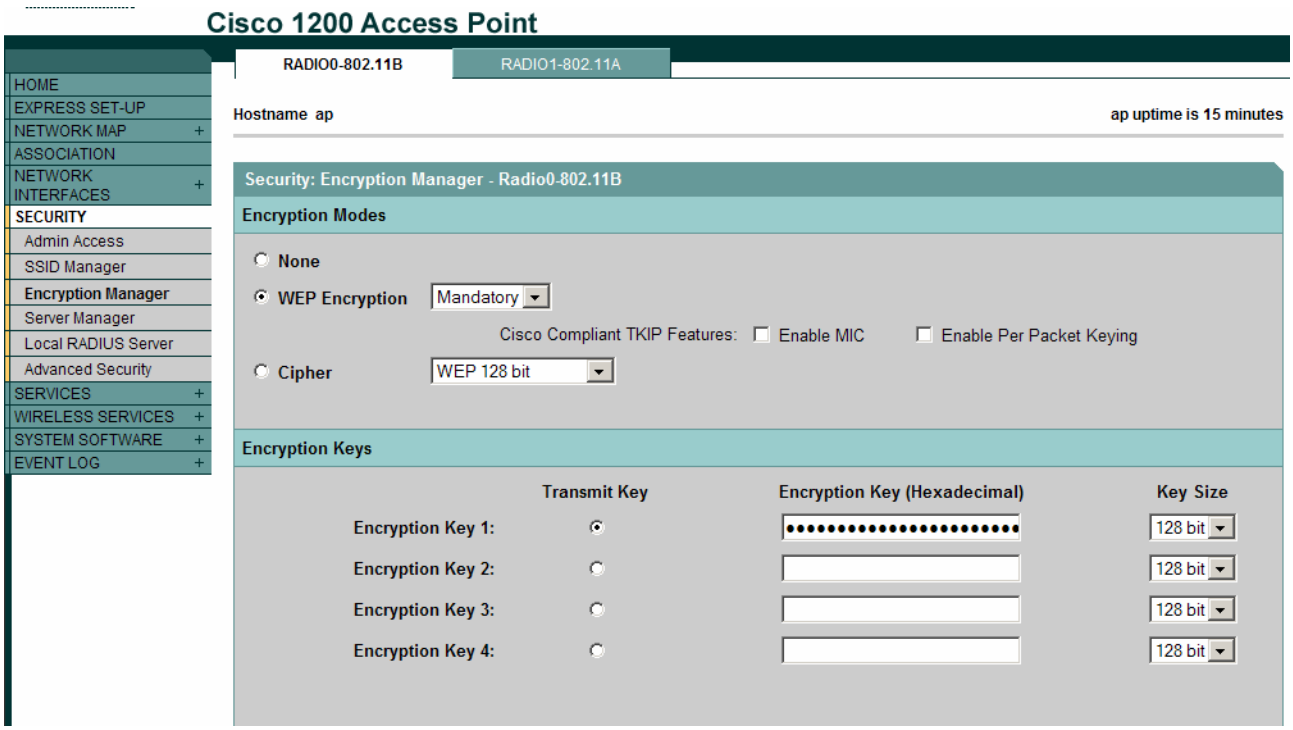
Understanding wireless security terminology:

- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
  - A per-packet key mixing function to defeat weak-key attacks
  - A new IV sequencing discipline to detect replay attacks
  - A cryptographic message integrity Check (MIC), called Michael, to detect forgeries such as bit flipping and altering packet source and destination
  - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's Michael, Cisco's message integrity check mechanism is designed to detect forgery attacks.
- Broadcast key rotation—Broadcast Key Rotation allows the AP to generate the best possible random key and update all key-management capable clients periodically.

Understanding WEP Key Restrictions

Security Configuration	WEP Key Restriction on AP
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	AP and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both AP and clients
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys

Step 1 Configure and verify WEP on the AP



In order to configure WEP on the AP, complete the following steps:

a. Verify connectivity from the wireless client (PC2) to the AP.

b. Open a Web browser on PC1 and type the IP address of the AP to configure in the browser address bar.

c. Go to the **Security** Setup page of the AP and click on the **Encryption Manager** option.

d. Check the radio button WEP Encryption Mode for **WEP Encryption.**

e. Use the Pull Down Menu to select **Mandatory.**

f. Select the **Transmit Key.**

g. Enter the Encryption key (for lab purposes will be) **12345678909876543210123456**.

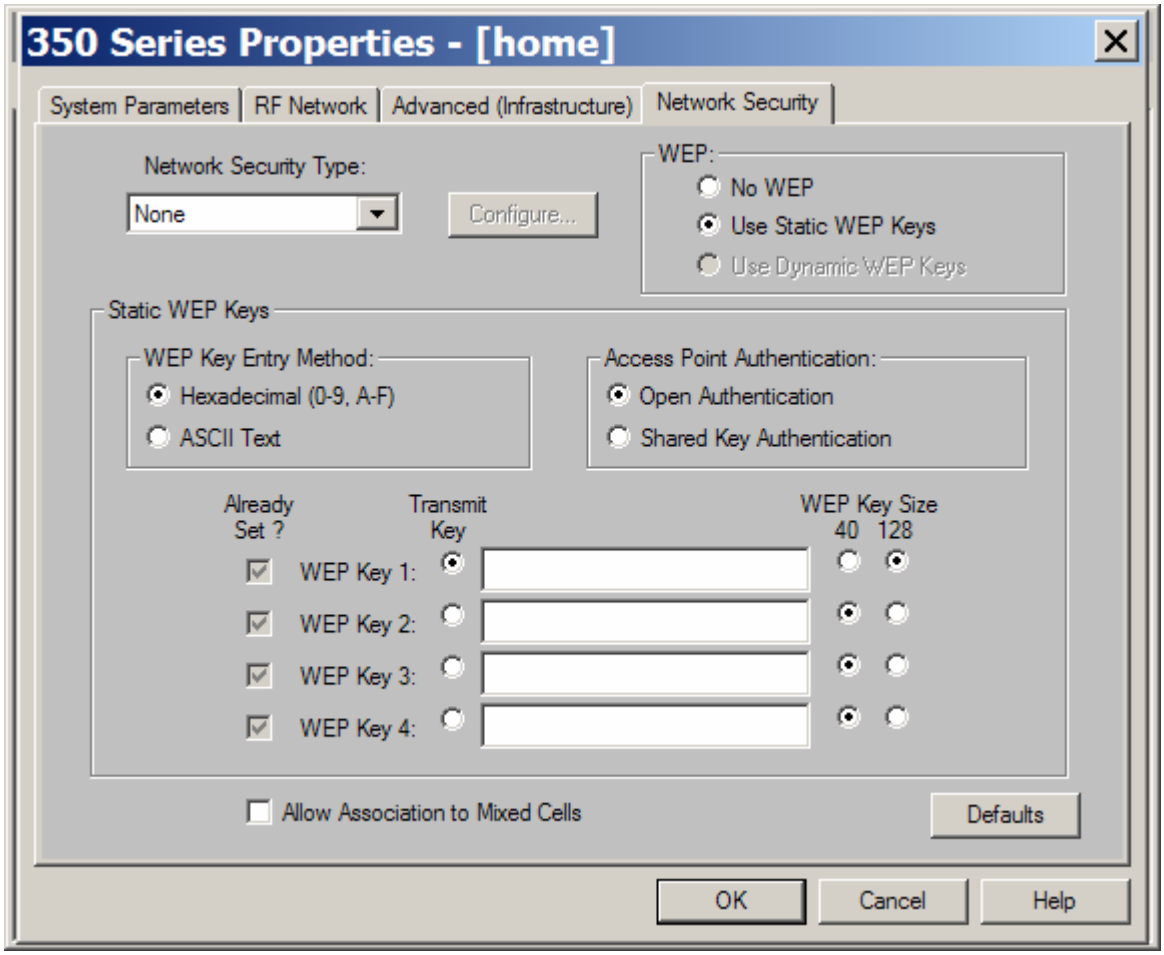
h. Select the Key size **128 bits**.

i. Click the **Apply-All** button to apply these options.

j. Once WEP is configured on the AP with a **Mandatory** option, all the clients will become disassociated to this AP.

k. View the **SECURITY>Encryption Manager** page. The WEP settings should be configured and the Encryption Key field should be stored in the AP. However, the Key field should be encrypted with asterisk symbols to prevent unauthorized users from viewing the Encryption Key.

Step 2 Configure and verify WEP on the client



a. Open the Aironet client utility by clicking on the ACU icon.

b. Click Profile Manager to edit the WEP settings.

c. Under the Profile Management section, choose the profile being used for this lab, and click Edit.

d. Go to the **Network Security** tab of the profile that is being used for the lab.

e. Configure the following settings for WEP:

   i. Select the WEP setting – **Use Static WEP keys**

   ii. Select the Static WEP key entry method – **Hexadecimal**

   iii. Select the AP Authentication – **Open authentication**

   iv. Select and enter the Transmit key [for lab purposes will be] **12345678909876543210123456**

   v. Select the WEP key Size – **128 bits**

   vi. Click the **OK** button to apply the WEP settings to the client

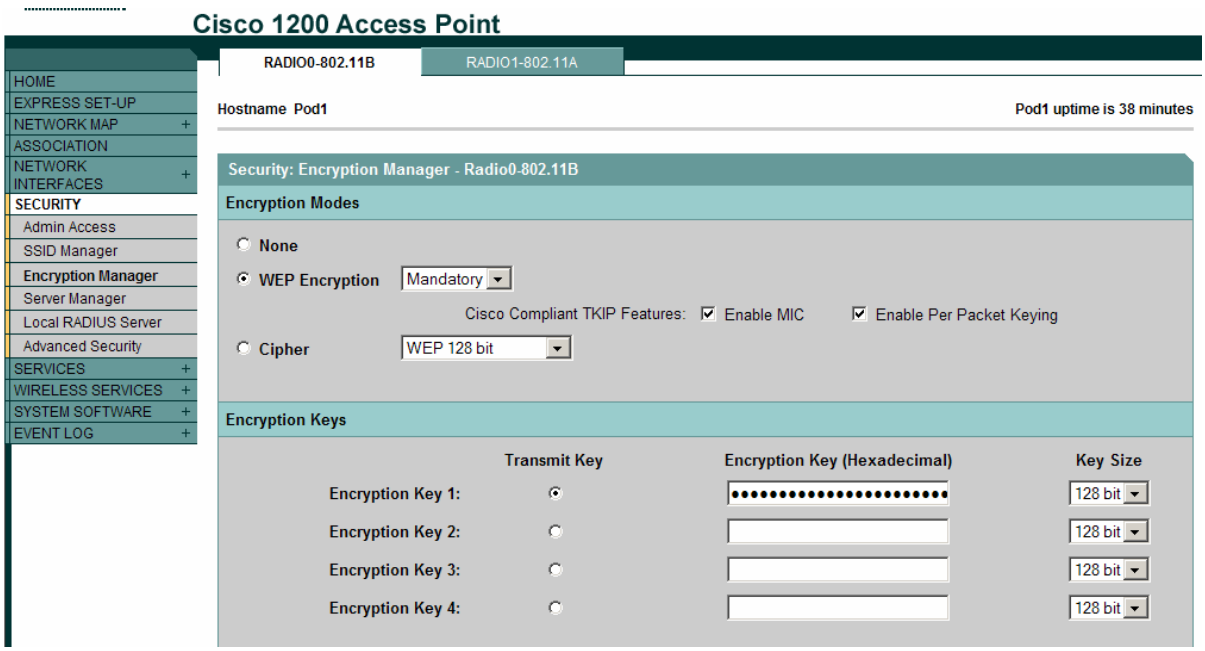
   vii. The connection should be reestablished between PC2 and the AP.

   viii. From the ACU Statistics Page, notice the “Packets Aged” and “Up-Time” values on the lower left hand corner.

Step 3 Enable MIC and TKIP

Once WEP is configured correctly, additional measures should be configured to secure the wireless link.

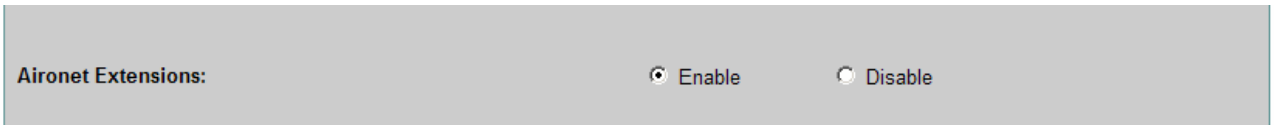
- **Message Integrity Check (MIC)**—MIC prevents attacks on encrypted packets called bit-flip attacks. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC, implemented on both the AP and all associated client devices, adds a few bytes to each packet to make the packets tamper proof.
- **TKIP (Temporal Key Integrity Protocol, also known as WEP key hashing)**—This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. On the AP, this feature is the Enable Per Packet Keying (PPK) option.



From the **SECURITY>Encryption Manager** Page, enable Cisco Compliant TKIP features.

a. Check the **Enable MIC** and **Enable Per Packet Keying (PPK).** These mechanisms can be used separately or together.

b. Click **Apply-All**

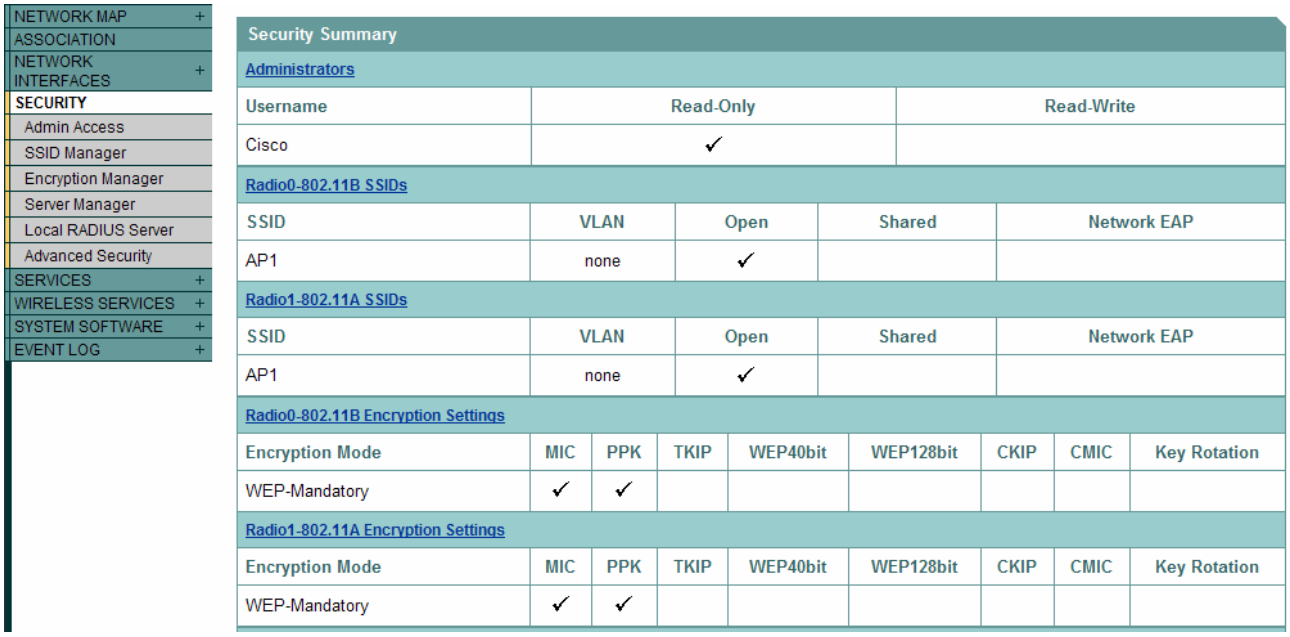


c. From the **NETWORK INTERFACES>Radio0-802.11b** Settings tab, verify the Aironet Extensions are enabled.

d. Also, check the 802.11a interface if applicable.

e. Verify the connection between PC2 and the AP

f. From the ACU Statistics Page, verify the “Packets MIC OK” statistics. The MIC statistics should now appear between the “Packets Aged” and “Up-Time” values. These values appear when MIC is enabled on the AP.



g. From the **SECURITY** Page, verify MIC and PPK are enabled.

h. What does MIC do to protect WEP?

_____

i. What attack does MIC prevent?

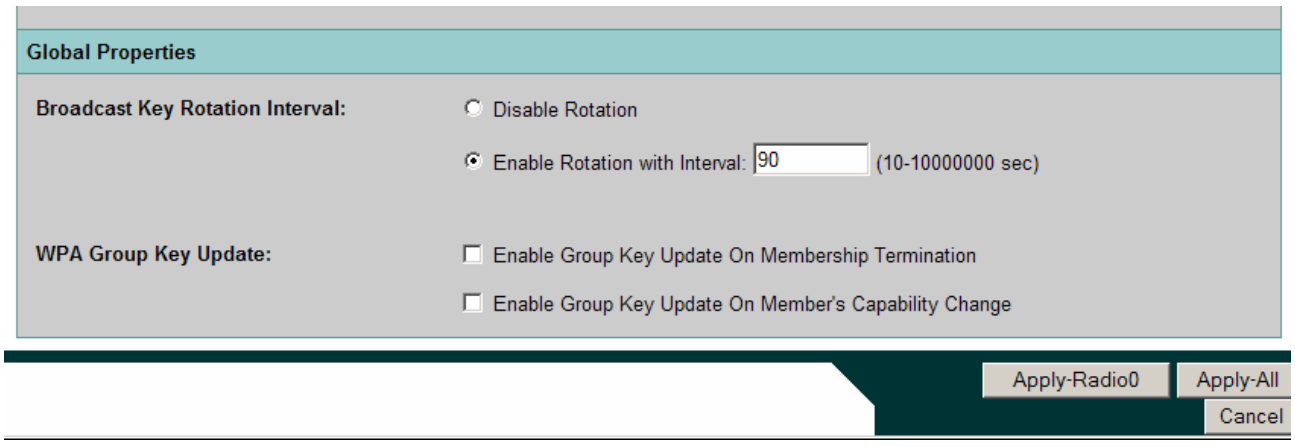
_____

j. Why do the Aironet extensions have to be used?

_____

Step 4 Enable Broadcast Key Rotation (BKR)

Broadcast key rotation (BKR)—When enabled, the AP provides a dynamic broadcast WEP key and changes it at the selected interval. Broadcast key rotation is an excellent alternative to TKIP if the wireless LAN supports wireless client devices that are not Cisco devices or that cannot be upgraded to the latest firmware for Cisco client devices.



a. Remove MIC and PPK configured from the previous step.

b. Check the **Enable Rotation with Interval** radio button.

c. Enter a value of 90 seconds.

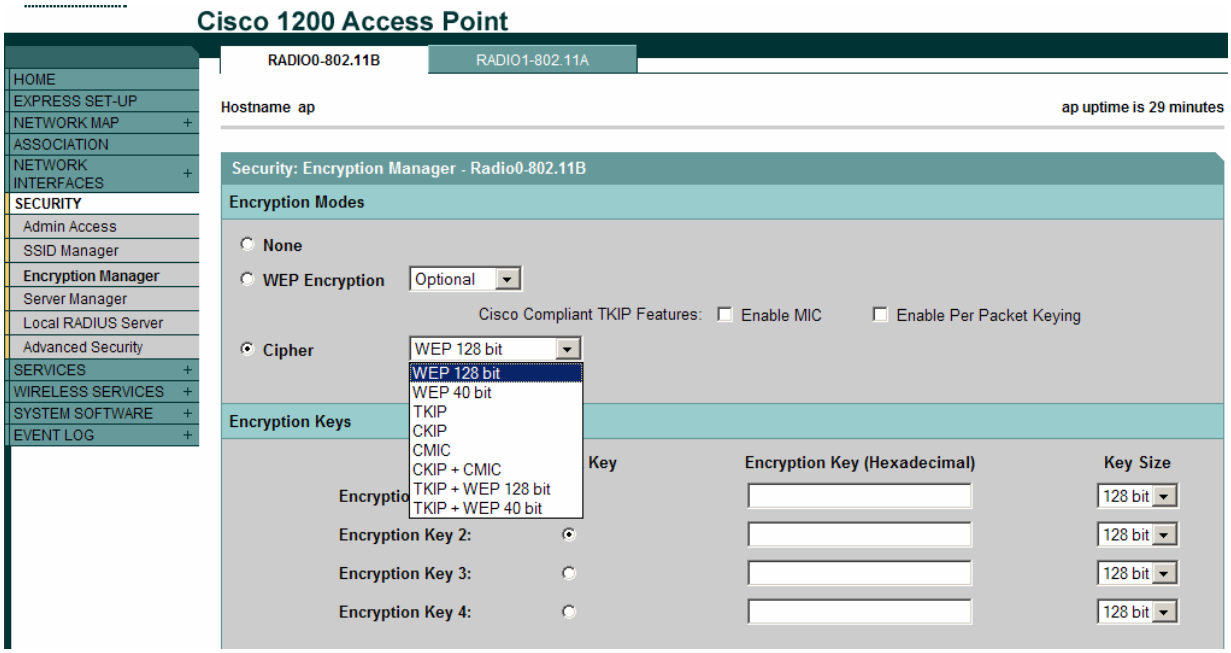
d. Click **Apply-All**

Radio0-802.11B Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
WEP-Mandatory								✓
Radio1-802.11A Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
WEP-Mandatory								✓

e. From the **SECURITY** Page, verify Key Rotation is enabled.

f. Verify connectivity from PC2 to the AP.

Step 5 Enable a cipher



From the **SECURITY>Encryption Manager** Page.

a. Remove Key Rotation configured from the previous step.

b. Check the **Cipher** radio button.

c. Choose the **TKIP** option in the drop down list

d. Click **Apply-All**

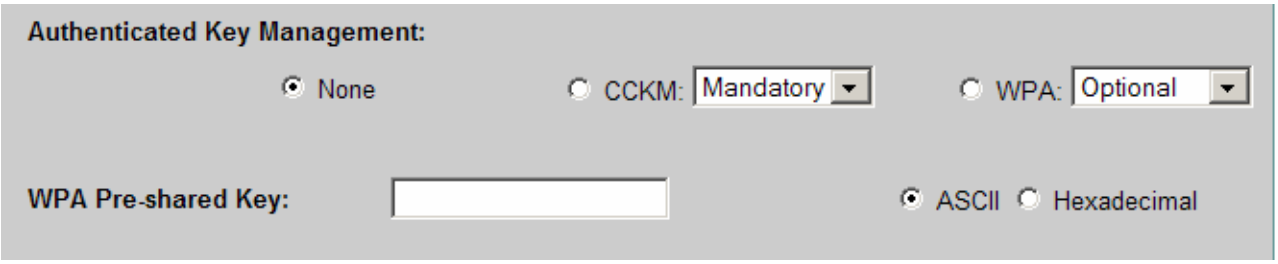
Radio0-802.11B Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher			✓					
Radio1-802.11A Encryption Settings								
Encryption Mode	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	Key Rotation
Cipher			✓					

e. From the **SECURITY** Page, verify TKIP is enabled.

f. Verify the wireless connection from PC2 and the AP.

g. Return to step 5c and try some of the various Cipher settings. Verify the changes from the SECURITY Page.

Step 6 Understanding ciphers and Key Management (optional challenge)

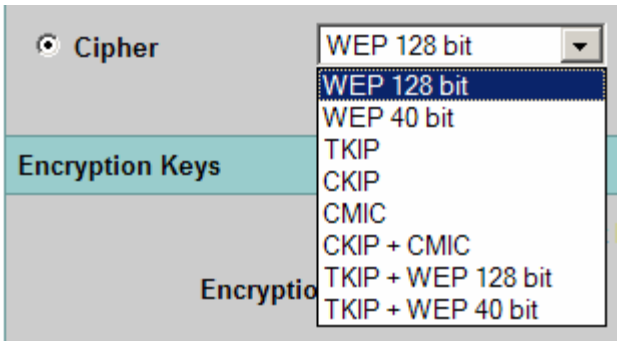


a. From the **SECURITY>SSID Manager** Page, check the **Authenticated Key Management** options.

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one AP to another without any perceptible delay during reassociation. An AP on the network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS AP cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new AP. When a client device roams, the WDS AP forwards the client's security credentials to the new AP, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new AP. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications.

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the AP. Using WPA-PSK, a pre-shared key must be configured on both the client and the AP, and that pre-shared key is used as the PMK.



Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode cipher wep128 • encryption mode cipher wep40 • encryption mode cipher ckip • encryption mode cipher cmic • encryption mode cipher ckip-cmic • encryption mode cipher tkip • encryption mode cipher tkip wep128 • encryption mode cipher tkip wep40
WPA	• encryption mode cipher tkip • encryption mode cipher tkip wep128 • encryption mode cipher tkip wep40

b. Explore the different Cipher settings.

Lab 8.5.4.2 Configuring Site-to-Site Wireless Link using Enterprise Security

Estimated Time: 45 minutes

Number of Team Members: Students will work in teams of 2.

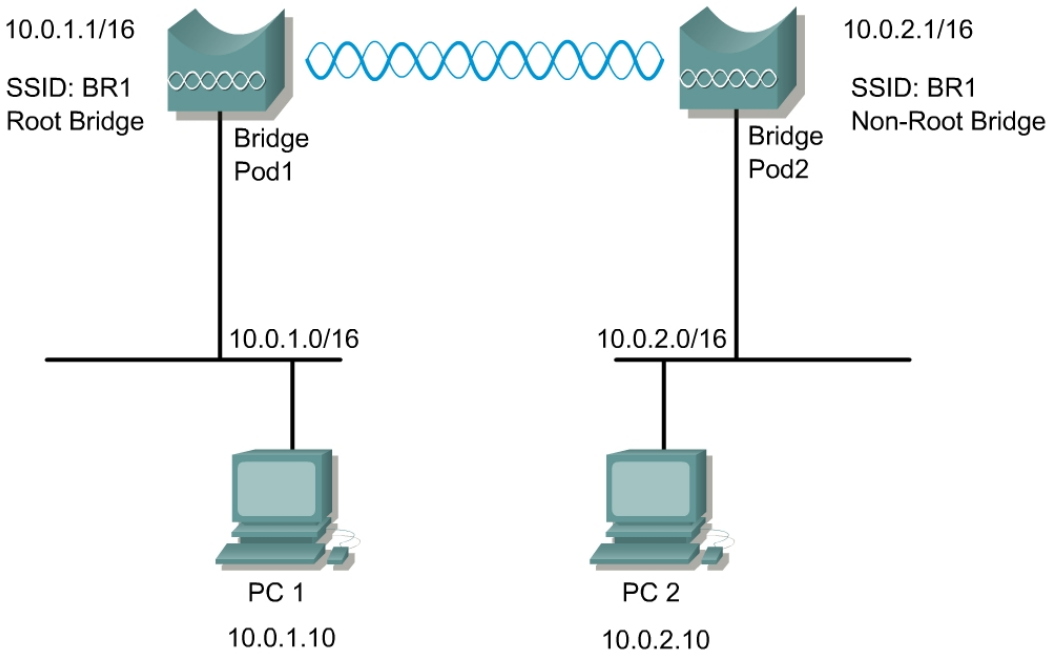
Objective

Configure a site-to-site bridged network using enterprise security features.

Scenario

A remote location located several miles away requires connectivity to the existing wired network. The connection can be bridged wirelessly with the use of two BR350s. The company's security policy mandated a minimum of 128 bit WEP security for all wireless connections.

Topology



Preparation

In this lab, the following will be configured.

Device Name	Label	SSID	Address
BPod1	BR1	BR1	10.0.1.1/16
BPod2	BR2	BR1	10.0.2.1/16

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco BR350
- PC with FTP server loaded and a file to transfer in the root directory of the FTP server

Step 1 Cable and power the bridge

a. First, attach 2 rubber duck antennas to the RP-TNC connectors.

b. Plug the RJ-45 Ethernet cable into the Ethernet port on the back of the bridge. Plug the other end of the Ethernet cable into the Cisco Aironet power injector TO AP/BRIDGE end.

c. Connect the power cable into the inline power injector and to the receptacle.

Step 2 Connect to the bridge

Connect a nine-pin, male-to-female, straight-through serial cable to the COM port on a computer and to the RS-232 serial port on the bridge. (This cable ships with the bridge)

a. Open a terminal emulator.

b. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: Xon/Xoff

c. Press **=** to display the home page of the bridge. If the bridge has not been configured before, the Express Setup page appears as the home page. If this is the case, go to Step 3.

d. If the bridge is already configured, the Summary Status page appears as the home page. When Summary Status screen appears, type :**resetall**, and press **Enter**.

```
Enter "YES" to confirm Resetting All parameters to factory defaults:
YES
00:02:12 (FATAL): Rebooting System due to Resetting Factory Defaults
*** Restarting System in 5 seconds...
```

e. Type **yes**, and press **Enter** to confirm the command.

f. Power cycle the bridge by removing the power.

Step 3 Connect to the BR350 through Express Setup

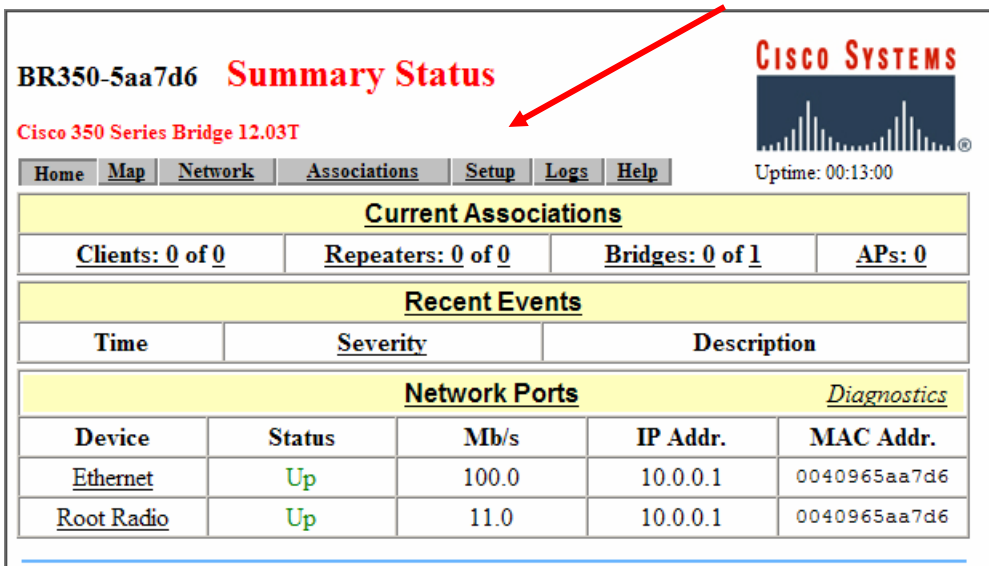
a. Plug a second RJ-45 Ethernet cable into the power injector end labeled TO NETWORK. Plug the other end of the Ethernet cable into the Ethernet port on a switch or hub. Then connect PC1 to the switch. A crossover cable can be used to connect directly from the inline power injector to PC1/PC2.

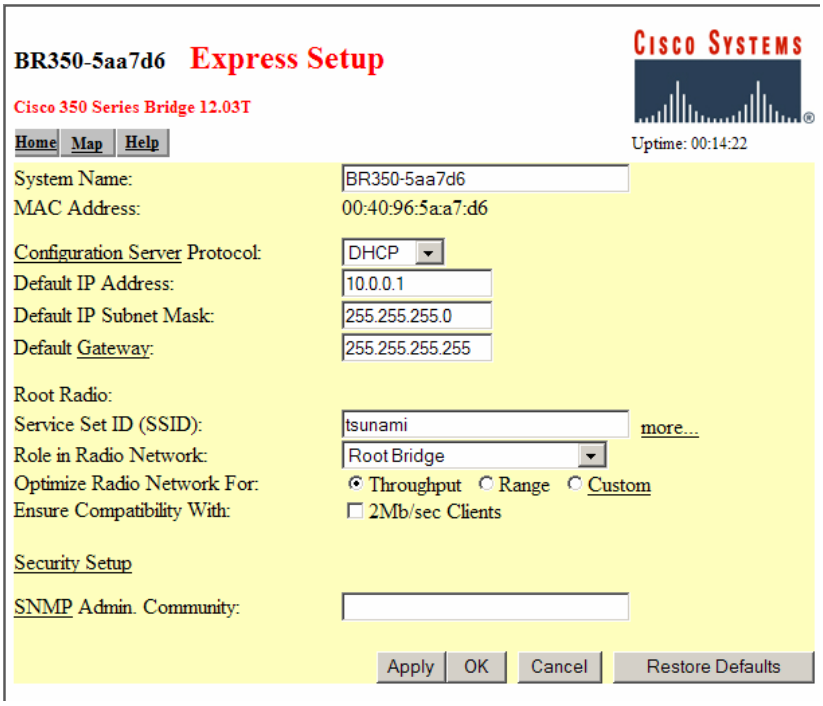
b. Configure PC1 to 10.0.0.2/16.

c. Open a web browser and enter the default bridge address http://10.0.0.1 and press **Enter**.

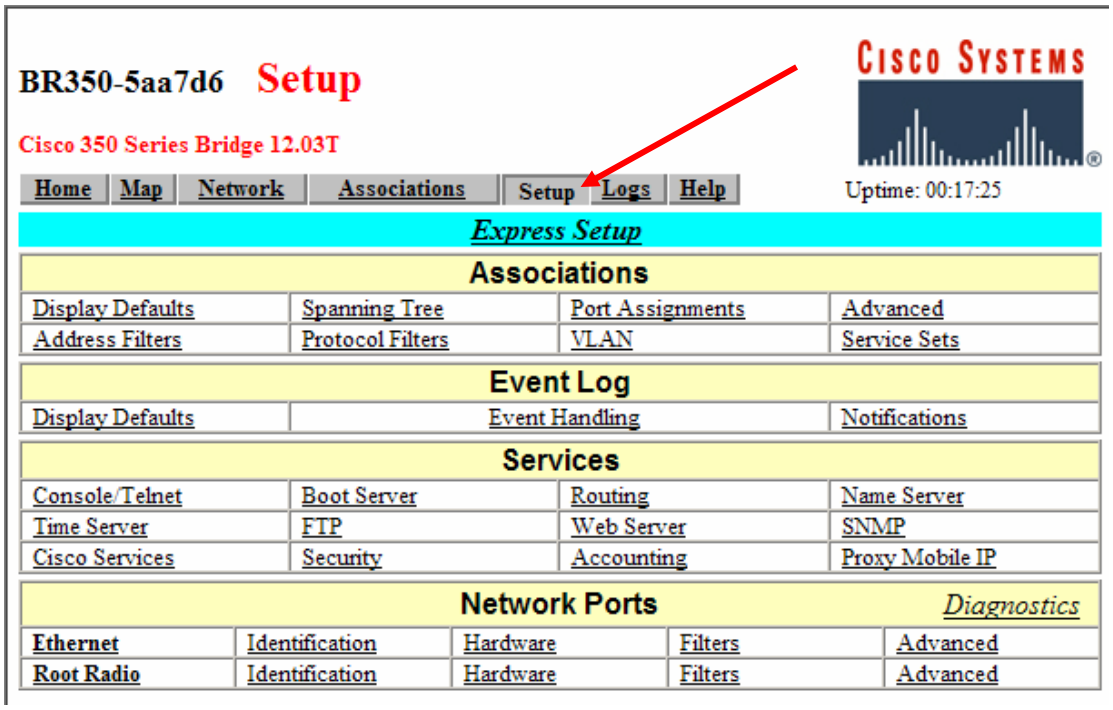
d. Either of the following pages will appear:

- The **Summary Status** Page, also known as the **Home** Page
- The **Express Setup** Page



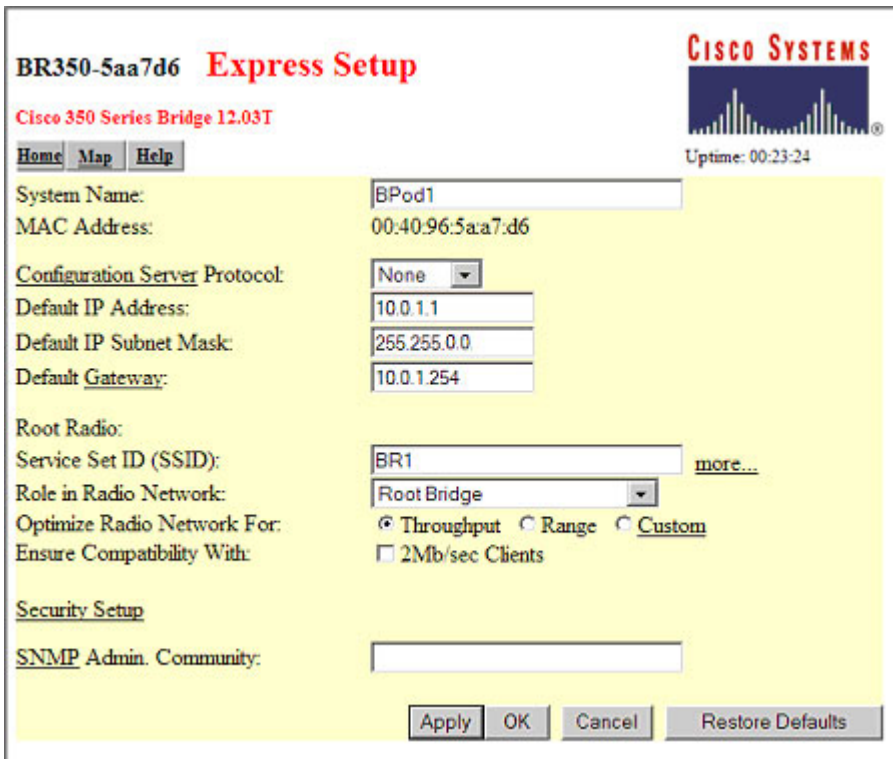


e. If the **Express Setup** Page does not appear, from the **Summary Status** Page click on the **Setup** hyperlink. This will bring up the Setup Page.



f. Click on the Express Setup link. This will bring up the Express Setup Page.

Step 4 Configure the bridge settings



Configure the following settings:

	Parameter	BPod1	BPod2
a.	System Name:	***BPod1***	***BPod2***
b.	Configuration Server Protocol:	***None***	***None***
c.	Default IP address:	***10.0.1.1***	***10.0.2.1***
d.	Default Gateway:	***10.0.1.254***	***10.0.1.254***
e.	Service Set ID:	***BR1***	***BR1***
f.	Role in Radio Network:	***Root Bridge***	***Non-Root Bridge w/o Clients***

g. Click Apply. The connection will drop.

h. Configure the PCs.

- PC1 with an IP address of 10.0.1.10/16
- PC2 with an IP address of 10.0.2.10/16

i. Reconnect to the using the browser. Enter 10.0.P.1 and connect.

j. Verify the settings.

k. What roles can the bridge serve in the network?

_____
_____
_____

l. Why would the BR350 be used in Root AP mode, compared to using a 1200 or 1100 AP?

_____
_____
_____

Step 5 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices on this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, ping from PC1 to BPod2. Then ping from PC1 to PC2.

b. Were these successful?

_____

c. Test layer 7 connectivity by browsing to BPod2 from PC1.

d. Configure FTP or Web services on PC1 and PC2. Transfer a files from PC1 to PC2 and vice versa. Calculate the download performance across the wireless link.

e. What was the download speed in Mbps?

_____

f. What is the distance limitation between two wireless bridges?

_____

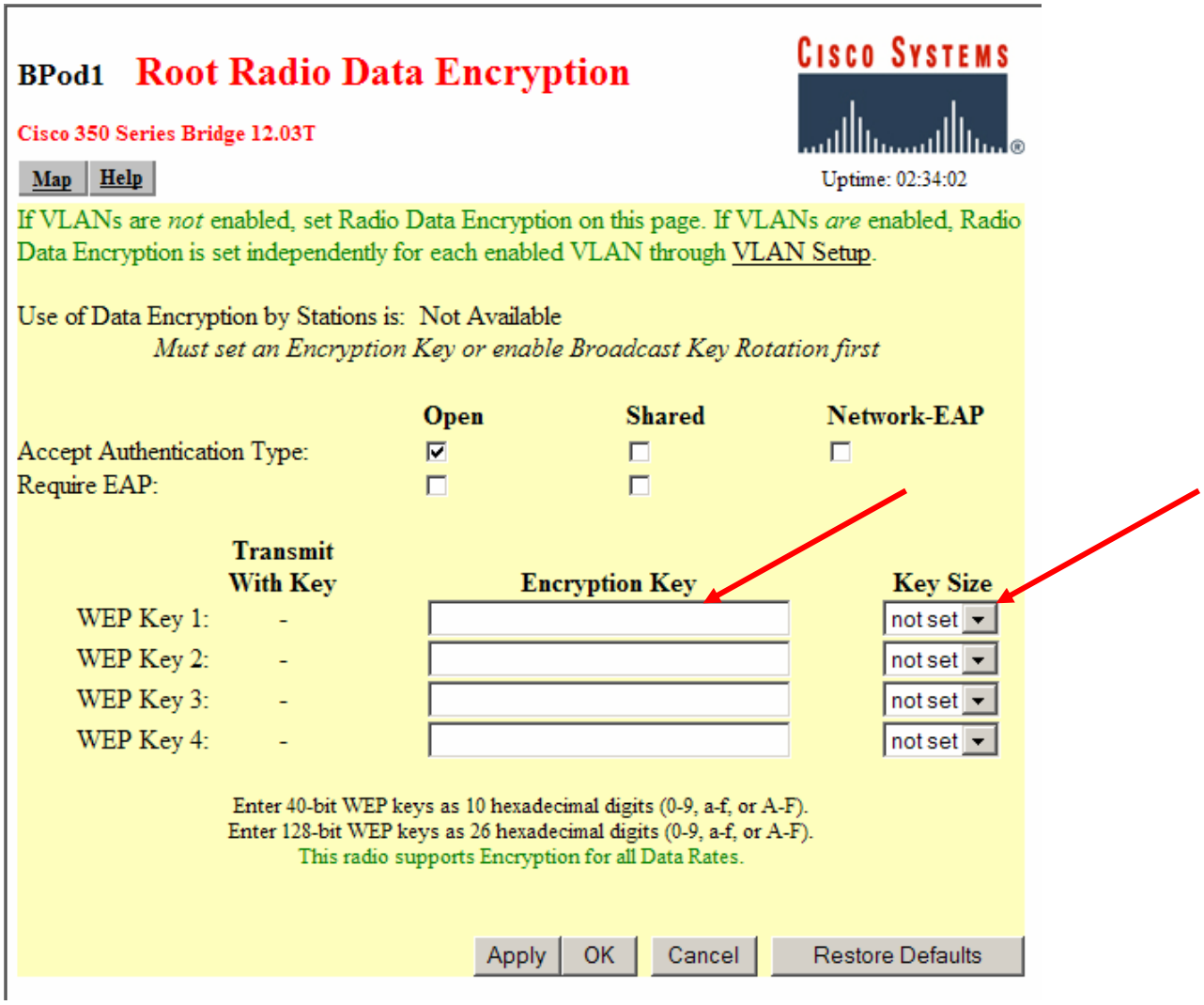
g. What is the distance limitation between an AP and a Bridge?

_____

h. Why are 2 bridges able to connect at longer distances?

_____

Step 6 Configure WEP on both bridges



Follow these steps to set up WEP keys and enable WEP:

a. On the Summary Status page, click **Setup.**

b. On the Setup page, click **Security**.

c. On the Security Setup page, click **Radio Data Encryption (WEP)**.

d. From the **Root Radio Data Encryption** page.

e. Before WEP can be enabled, a WEP key must be entered in at least one of the Encryption Key fields.

f. Use the Key Size pull-down menu to select the **128-bit** encryption for the WEP Key 1.

g. Click in the Encryption Key field and enter a WEP key.

h. How many digits must be entered for 128 bit WEP?

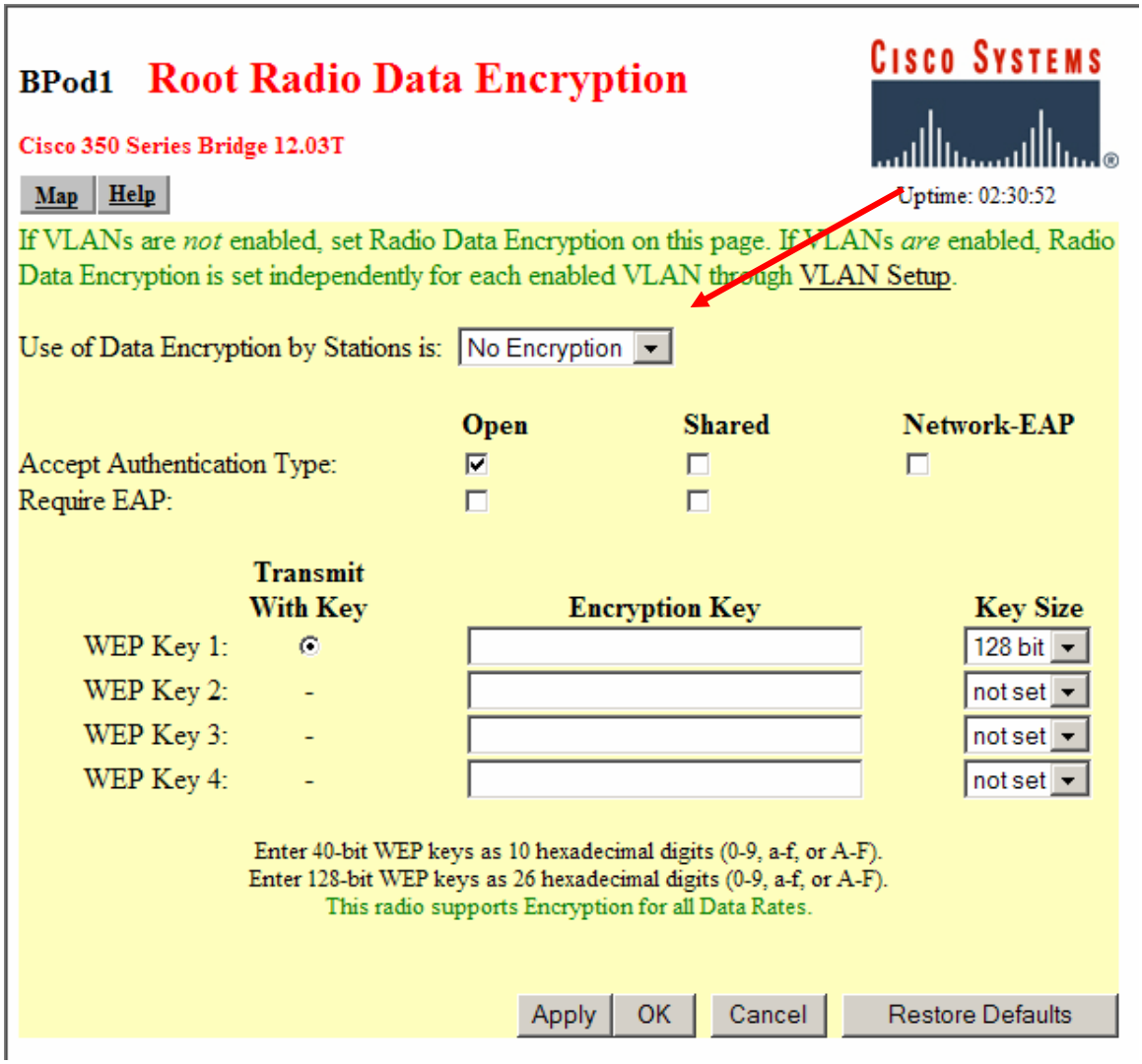
_____

i. Record the key below.

_____

_____

j. Click Apply to save the WEP Key.



k. Notice that the Drop down box appears next to the **Use of Data Encryption by Stations is**. Select Full Encryption from the pull-down menu labeled **Use of Data Encryption by Stations is**.

l. Click OK, which returns the bridge to the **Security Setup** Page.

m. Repeat the same steps on the other bridge.

Note The characters typed for the key contents appear only when typing. After the click **Apply** or **OK**, the key contents cannot be viewed. Select **Not set** from the Key Size pull-down menu to clear a key.

WEP Key Setup Example

Key Slot	Bridge (Root)		Non-Root Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	-	12345678901234567890abcdef
2	-	09876543210987654321fedcba	x	09876543210987654321fedcba
3	-	not set	-	not set
4	-	not set	-	not set

Because the bridge WEP key 1 is selected as the transmit key, WEP key 1 on the other device must contain the same contents.

Step 7 Retest the connection

Once the wireless bridge link is configured with WEP, ping each PC to test end-to-end connectivity between the two PCs.

a. Was this successful? If not, what should be checked?

_____

Configure ftp services on PC1 and PC2. Calculate the download performance across the wireless link.

b. What was the download speed in Mbps? Did WEP have a impact on performance?

_____

c. What other enhancements can be used to improve WEP security?

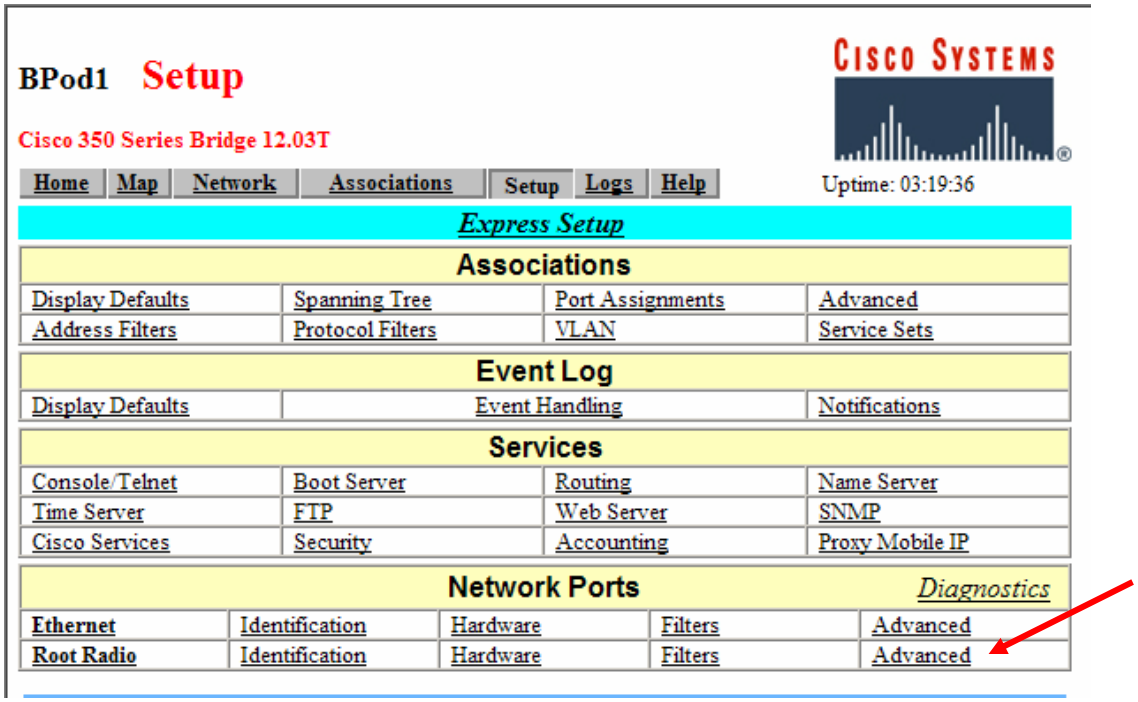
_____

d. What technology can be used at layer 3 to improve security of the wireless link?

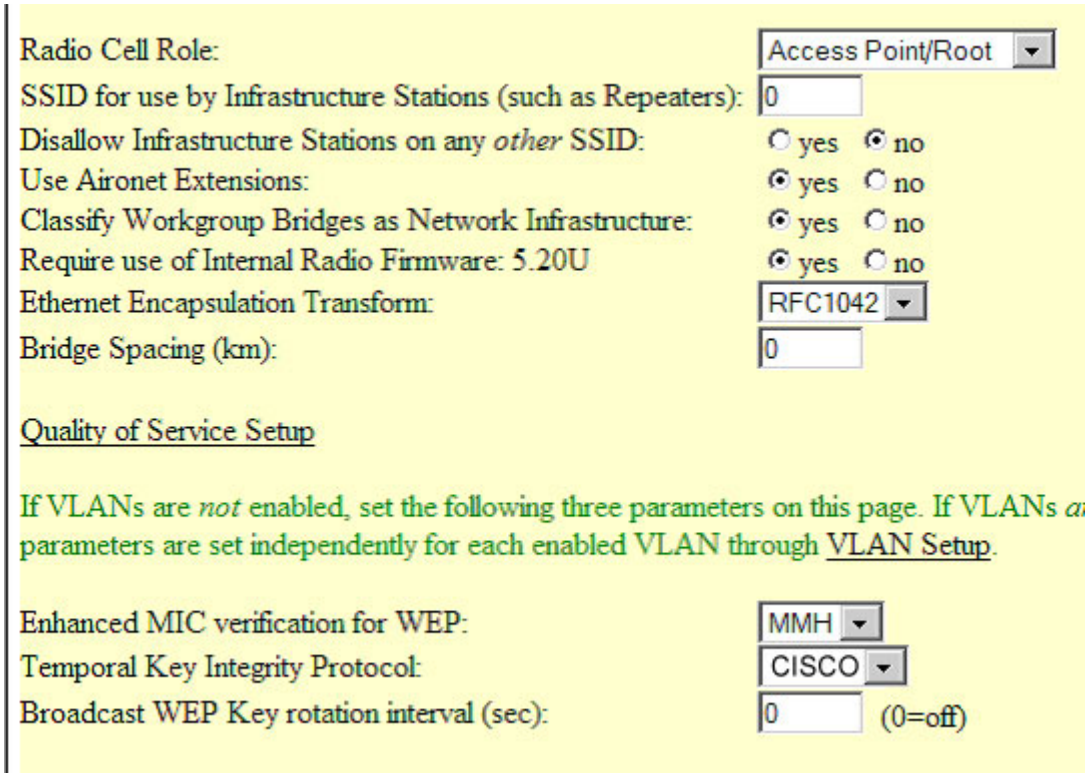
_____

Step 8 Enable enterprise security

Once WEP is configured correctly, additional measures should be configured to secure the wireless link. Follow these steps to set up TKIP, MIC and BKR.



a. From the Setup Page, click **Root Radio** advanced link



b. From the **Root Radio Advance** page, select **MMH** from the drop down list for the Enhanced MIC verification for WEP:.

c. Verify the Use Aironet Extensions is selected as yes.

d. Click the **Apply** button. The wireless link will be lost with the other bridge.

e. Configure the other bridge with the same security setting.

f. The link should be re-established.

g. From the **Root Radio Advance** page, select **Cisco** from the drop down list for the Temporal Key Integrity Protocol:.

h. Verify the Use Aironet Extensions is selected as yes.

i. Click the **Apply** button. The wireless link will be lost with the other bridge.

j. Configure the other bridge with the same security setting.

k. The link should be re-established.

- What attack does TKIP prevent?

  _____

- Why do the Aironet extensions have to be used?

  _____

l. From the **Root Radio Advance** page, select enter a value of 90 seconds as the **Broadcast WEP Key rotation interval**.

m. Click the **Apply** button. The wireless link will be lost with the other bridge.

n. Configure the other bridge with the same security setting.

o. The link should be re-established.

- What attack does BKR prevent?

  _____

Lab 8.5.4.3 BR1310 Configuring Site-to-Site Wireless Link using Enterprise Security

Estimated Time: 45 minutes

Number of Team Members: Students will work in teams of 2.

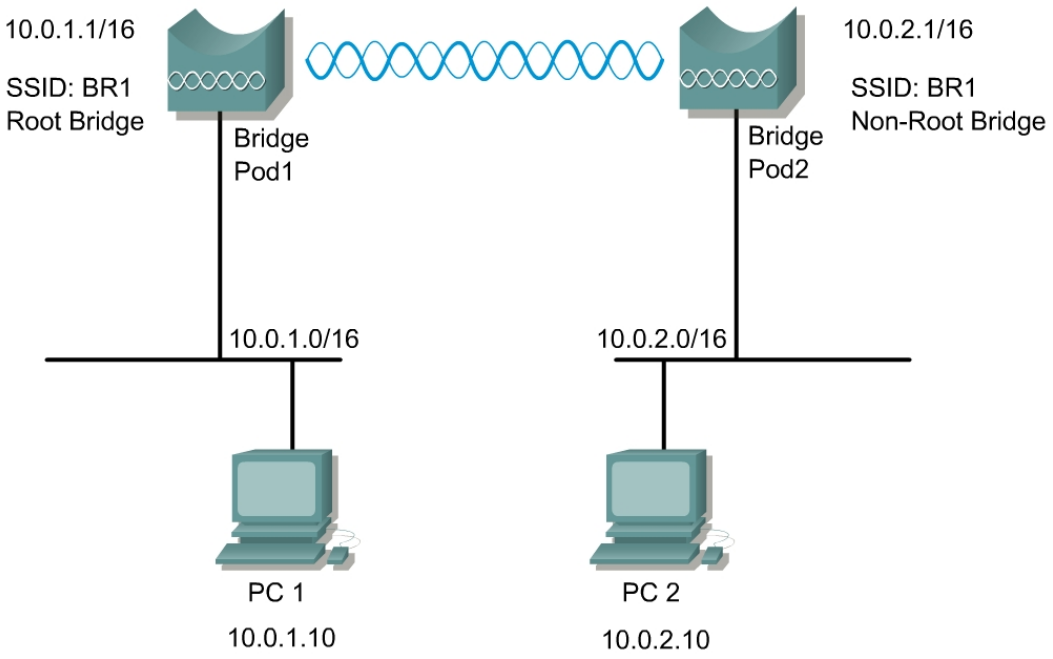
Objective

Configure a site-to-site bridged network using enterprise security features.

Scenario

A remote location located several miles away requires connectivity to the existing wired network. The connection can be bridged wirelessly with the use of two BR1310s. The company's security policy mandated a minimum of 128 bit WEP security for all wireless connections.

Topology



Preparation

In this lab, the following will be configured.

Device Name	SSID	BVI Address
BPod1	BR1	10.0.1.1/16
BPod2	BR1	10.0.2.1/16

Tools and Resources

Each team will require the following:

- Two wired LAN segments that will be bridged together
- Two Cisco BR1310
- PC with FTP server loaded and a file to transfer in the root directory of the FTP server

Step 1 Cable and power the bridge

a. For each bridge, attach 2 rubber duck antennas to the RP-TNC connectors.

b. Connect the power cable to the Power Injector and to a wall receptacle.

Step 2 Connect to the bridge and clear existing configurations

Connect a PC to the bridge power injector's serial port using a DB-9 to RJ-45 serial cable.

a. Open a terminal emulator.

b. Enter these settings for the connection:

- Bits per second (baud rate): 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

c. Press **Return** to get started

d. Enter privileged mode. ***Cisco*** is the default password.

```
PodP>enable
Password:
PodP#
```

e. Turn off notification logging to avoid interruptions as you enter commands.

```
PodP#configure terminal
PodP(config)#logging console 4
```

f. Erase the configuration with the following commands:

```
PodP#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]      (press Enter)
[OK]
Erase of nvram: complete
PodP# reload
```

```
System configuration has been modified. Save? [yes/no]:  N
Proceed with reload? [confirm]    (press Enter)
```

g. After the system reboots, repeat the step to turn off notification logging.

h. Assign an IP address and address mask to the BVI.

```
PodP(config)#interface bvi1
PodP(config-if)#ip address 10.0.P.1 255.255.0.0
```

i. Configure the PCs.

- PC1 with an IP address of 10.0.1.10/16
- PC2 with an IP address of 10.0.2.10/16

Step 3 Connect to the BR1310 through a web browser

a. Connect an RJ-45 Ethernet cable to the Ethernet port on the bridge Power Injector. Connect the other end of the Ethernet cable to the wired network.

b. Open a web browser, enter the bridge BVI address http://10.0.P.1, and press **Enter**.

Step 4 Configure the bridge settings

Configure the following settings from the **Express Set-Up** page:

	Parameter	BPod1	BPod2
a.	System Name:	***BPod1***	***BPod2***
b.	Configuration Server Protocol:	***Static IP***	***Static IP***
c.	IP address:	***10.0.1.1***	***10.0.2.1***
d.	Subnet Mask:	***255.255.0.0***	***255.255.0.0***
e.	Default Gateway:	***10.0.1.254***	***10.0.1.254***
f.	Role in Radio Network:	***Root***	***Non-Root***

g. Click **Apply** to save these changes.

h. Navigate to the **Express Security** page and configure the SSID: ***BR1***

i. Verify the settings on both bridges. Navigate to the **Association** page to confirm that the bridges have associated.

Step 5 Test the connection

Verify client PCs are configured with the appropriate IP address. The only wireless devices in this topology will be the two wireless multi-function bridges used for the point-to-point connection.

a. Once the wireless bridge link is configured properly, ping from PC1 to BPod2. Then ping from PC1 to PC2.

b. If these pings are not successful, troubleshoot as necessary.

c. Test layer 7 connectivity by browsing from PC1 to BPod2.

d. Configure FTP or Web services on PC1 and PC2. Transfer a file from PC1 to PC2 and vice versa. Observe the download performance across the wireless link.

e. What was the download speed in Mbps?

_____

Step 6 Configure static WEP on both bridges

Follow these steps to set up WEP keys and enable WEP:

a. From the **Security: Encryption Manager** page, click the radio button next to **WEP Encryption** and select **Mandatory** from the drop down list.

b. Select the radio button for **Encryption Key 1** in the Transmit Key column. Make sure that drop down list has **128-bit** selected for Key Size.

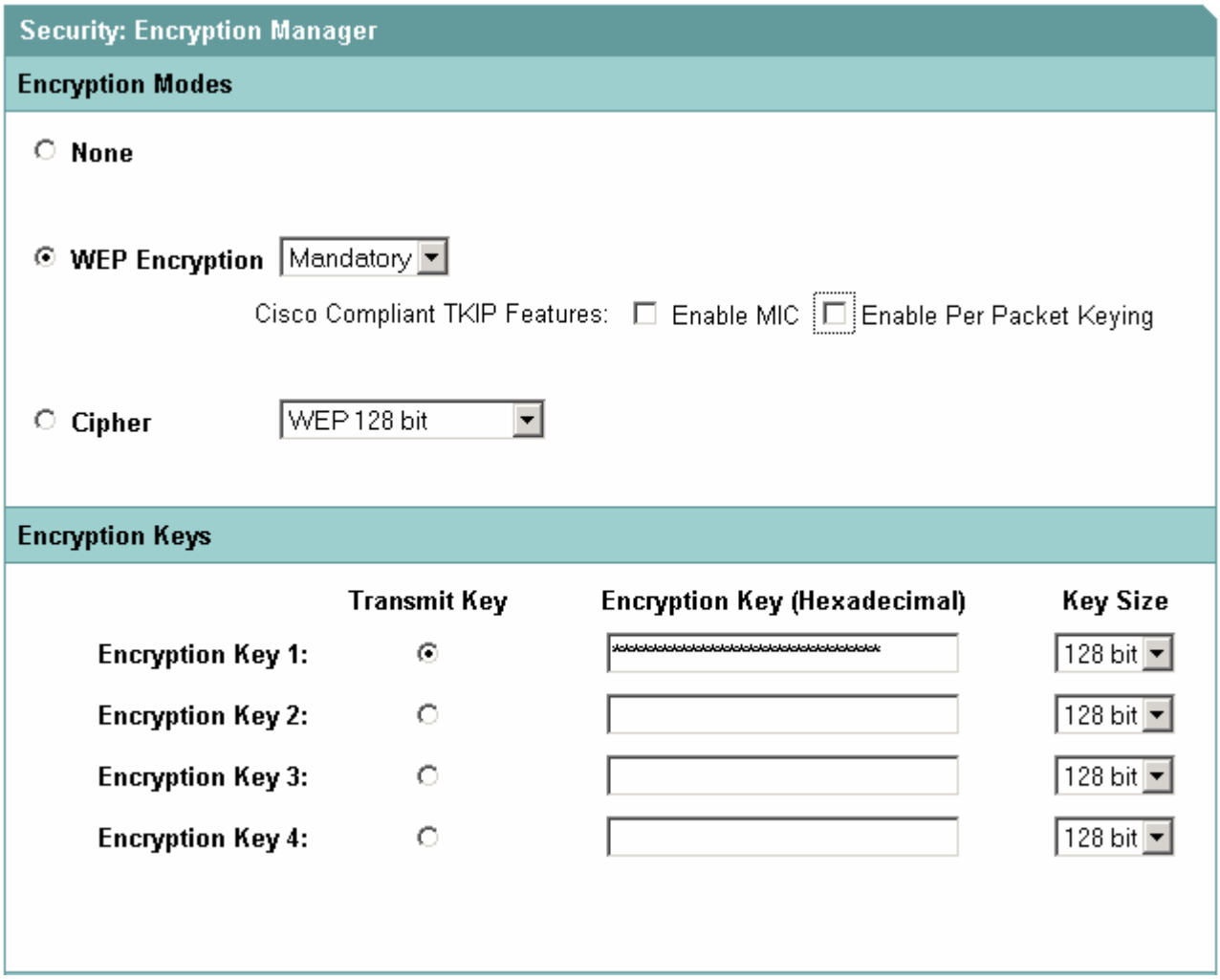
c. Click in the Encryption Key field and enter a WEP key. For a 128-bit encryption, the key will need to be 26 hexadecimal characters in length. Only the numbers 0-9 and the letters A-F can be used.

d. Record the key below.

_____

e. Click **Apply** to save the WEP Key.

f. Repeat the same steps on the other bridge.



Step 7 Retest the connection

From either bridge, navigate to the **Association** page to view the status of the wireless link. If the bridges do not associate, troubleshoot the static WEP configuration.

a. Once the wireless bridge link is functional, ping from PC1 to PC2 to test end-to-end connectivity.

b. Repeat the FTP download process from PC1 to PC2. Observe the download performance across the wireless link.

c. What was the download speed in Mbps? Did WEP have an impact on performance?

_____

Step 8 Enable enterprise security

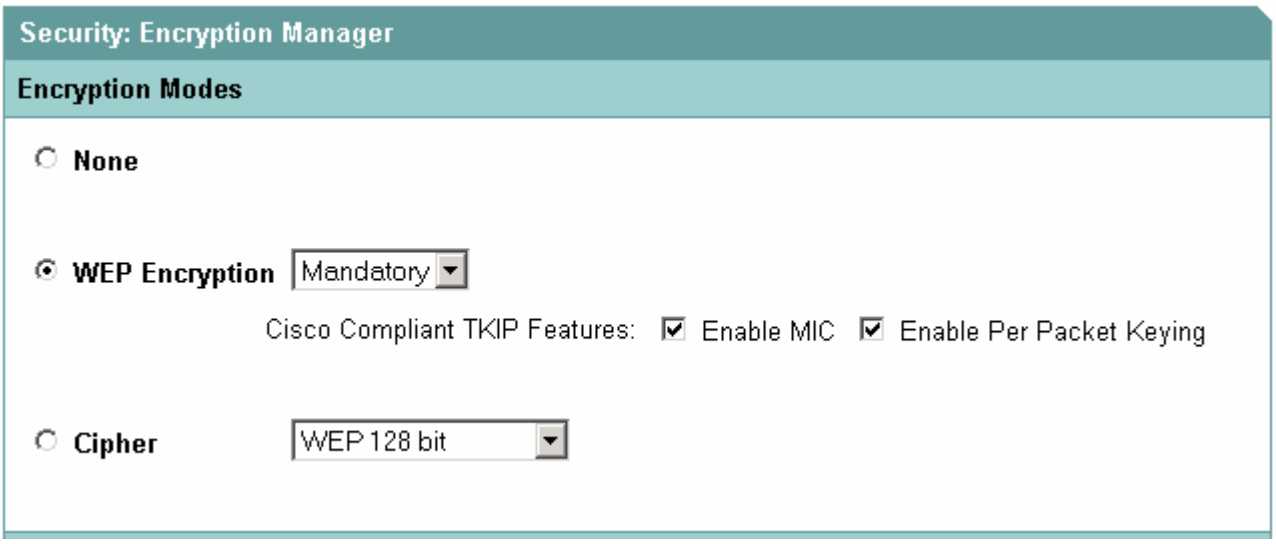
Once WEP is configured correctly, additional measures should be configured to secure the wireless link. Follow these steps to set up Per Packet Keying and MIC.

a. From the **Encryption Manager** page, select the check boxes for the Cisco Compliant TKIP features.

b. Click the **Apply** button. The wireless link will be lost with the other bridge.

c. Configure the other bridge with the same security setting.

d. The link should be re-established.



e. What attack does TKIP prevent?

_____

f. View the Security Summary via the web browser for an overview of the security settings.

Security Summary								
Administrators								
Username	**Read-Only**		**Read-Write**					
Cisco	✓							
Radio0-802.11G SSIDs								
SSID	**VLAN**	**Open**	**Shared**	**Network EAP**				
BR1	none	no addition						
Radio0-802.11G Encryption Settings								
Encryption Mode	**WEP**		**Cipher**					**Key Rotation**
	MIC	**PPK**	**TKIP**	**WEP40bit**	**WEP128bit**	**CKIP**	**CMIC**	
WEP-Mandatory	✓	✓						

Lab 8.6.2 Configure VLANs on the AP

Estimated Time: 40 minutes

Number of Team Members: Students will work in teams of two.

Objective

The student will extend VLANs into a WLAN.

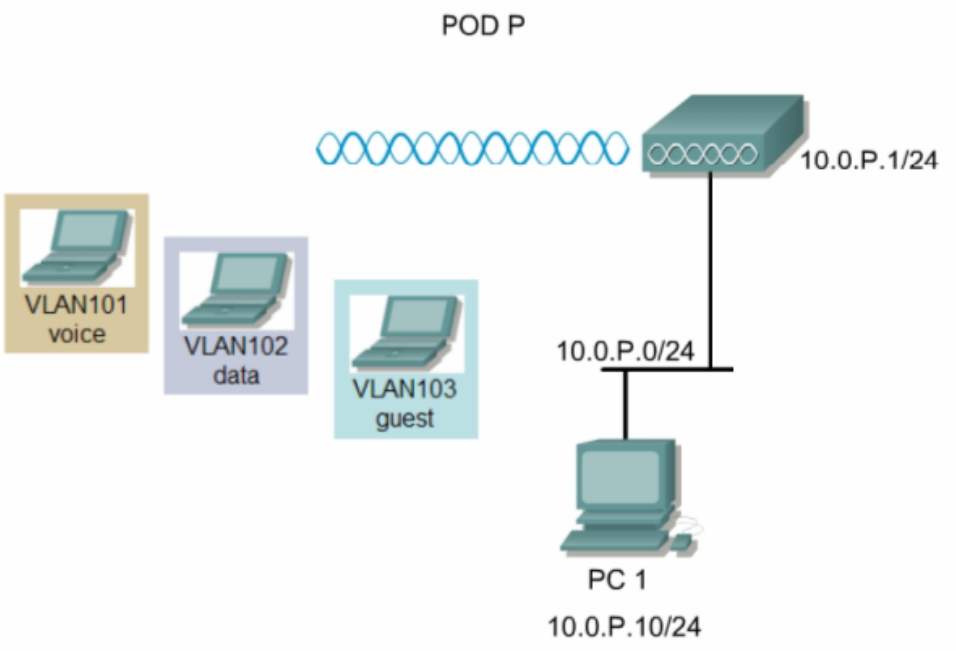
Scenario

VLANs can be extended into a WLAN by adding IEEE 802.11Q tag awareness to the AP. Frames destined for different VLANs are transmitted by the AP wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

The basic wireless components of a VLAN consist of an AP and a client associated to it using wireless technology. The AP is physically connected through a trunk port to the network VLAN switch on which the VLAN is configured. The physical connection to the VLAN switch is through the AP Ethernet port. A router is also necessary to route between the different VLANs. Up to 16 SSIDs can be configured on the AP, hence 16 VLANs are supported. Configuring the AP to support VLANs is a three-step process:

1. Create SSIDs and assign authentication settings to SSIDs.
2. Assign SSIDs to VLANs and enable the VLAN on the radio and Ethernet ports.

Topology



Preparation

Team	Access Point Name	SSID	VLAN	Authentication	Bridge group	BVI Address
1	PodP	management voice data guest	10 101 102 103	Network EAP Shared Network EAP Open	1 101 102 103	10.0.P.1/24

Reset the AP to the default configuration.

Tools and Resources

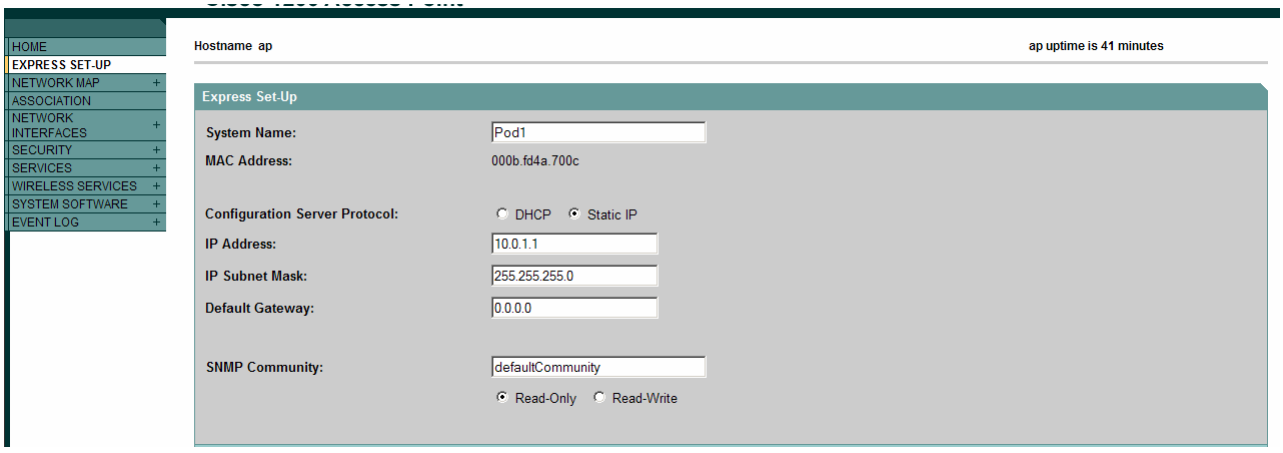
Each team will need:

- 1 AP
- 2 PCs or laptop
- Console cable

Additional Materials

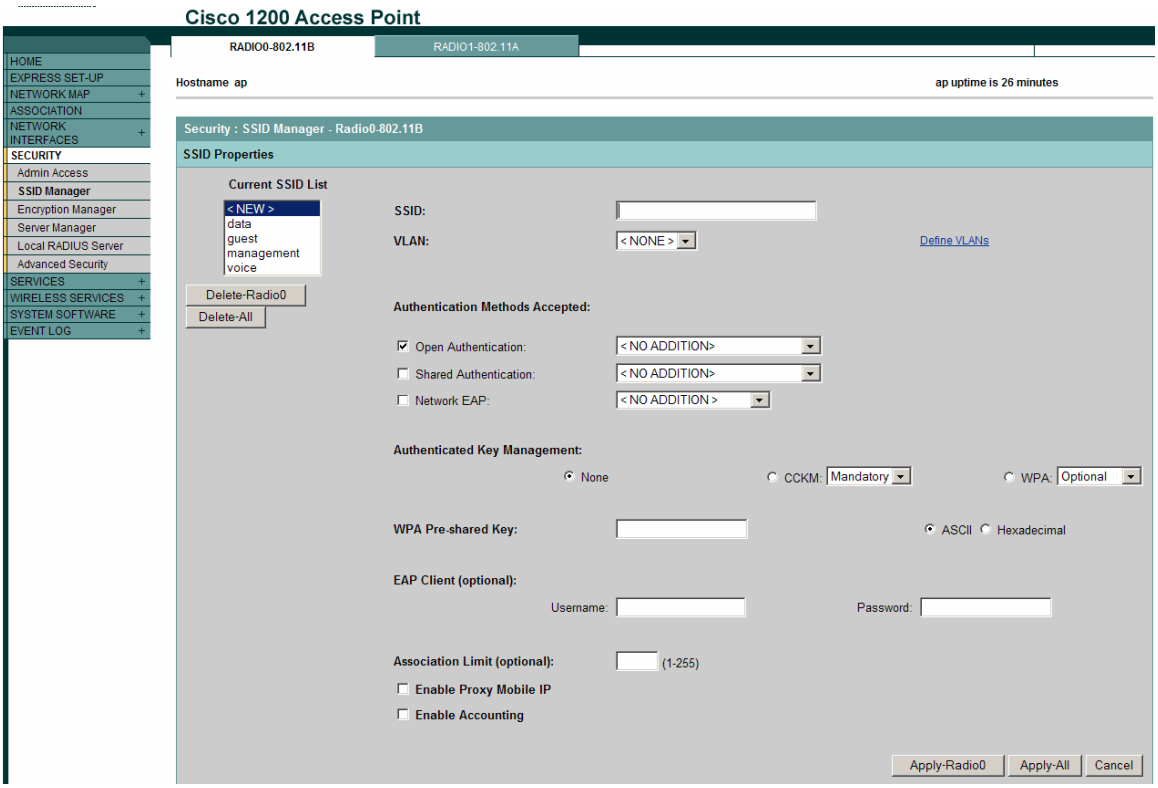
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_book09186a0080147d69.html

Step 1 Configure the System Name and BVI address



From the **EXPRESS SET-UP** page, configure the System Name and BVI address.

Step 2 Define the SSIDs and Authentication Type



From the **SECURITY>SSID Manager** page, configure the 802.11b radio management, voice, data, and guest SSIDs, and authentication type according to the Preparation table.

a. Enter the *management* SSID in the SSID: box.

b. Select the authentication method.

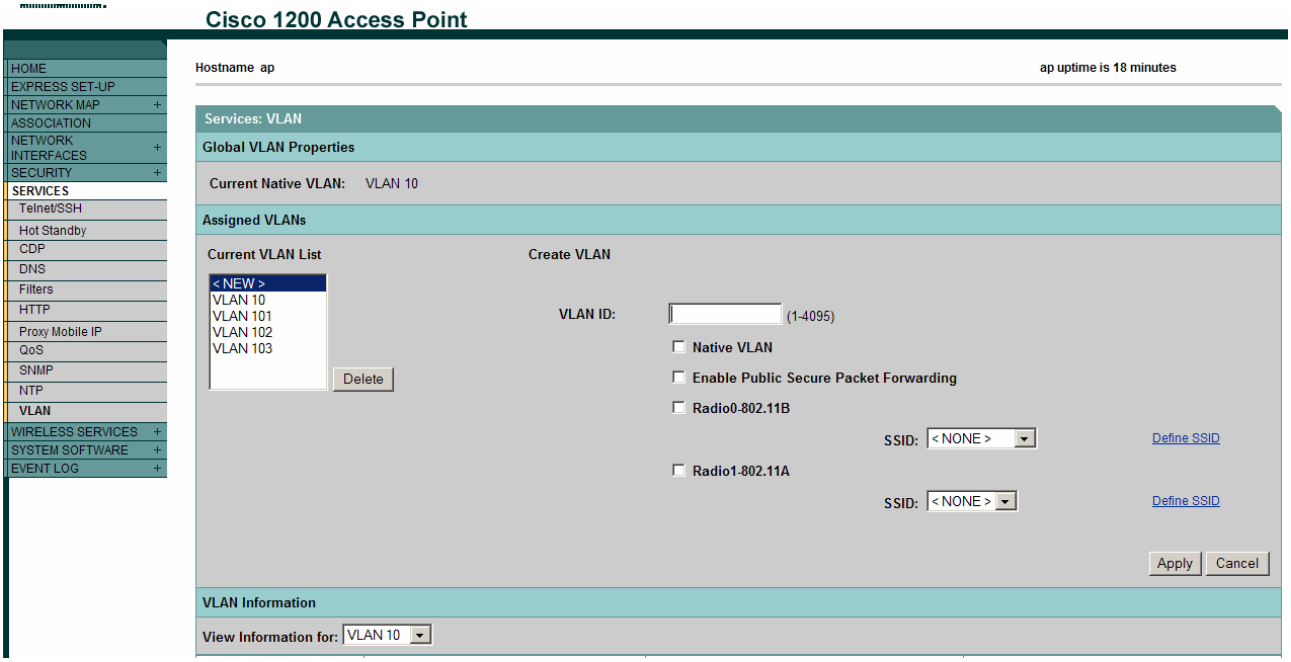
c. Click **Apply**.

d. Repeat the steps for the voice, data, and guest SSIDs.

1. Why is VLAN ID 10 used for the management VLAN instead of VLAN ID 1?

_____

Step 3 Define the VLANs



From the **SERVICES>VLAN** page, configure the 802.11b radio for management, voice, data, and guest VLANs according to the Preparation table.

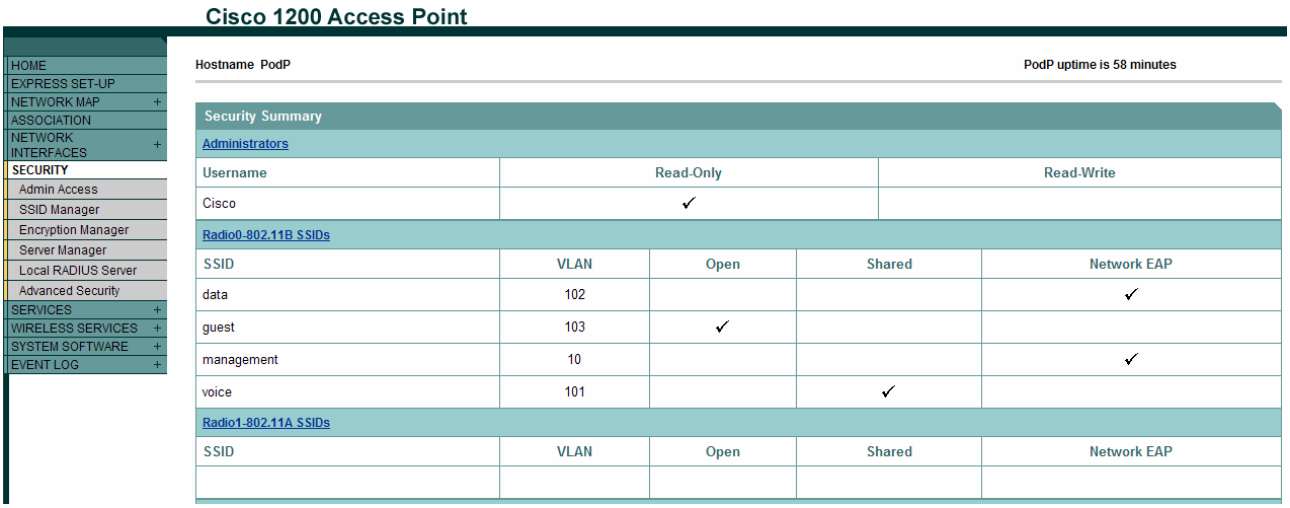
a. Enter VLAN ID *10* in the **VLAN ID**: box. Since this is the management VLAN, check the Native VLAN box. Also, check the Radio0-802.11B.

b. Choose the *management* SSID from the **SSID** drop down box.

c. Click **Apply.**

d. Repeat the steps for the voice, data, and guest VLANs.

Step 4 Verify the Configuration through GUI



From the **SECURITY** home page

a. Verify the VLAN configuration through the GUI

Step 5 Verify the Configuration through the IOS CLI

Telnet or Console into the AP.

a. Verify the configuration through IOS CLI.

```
PodP#show run
Building configuration...

Current configuration : 3167 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PodP
!
enable secret 5 $1$N46P$W9Eb.bK3xvfZ1XgDmRXDZ1
!
username Cisco password 7 01300F175804
ip subnet-zero
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid data
    vlan 102
    authentication network-eap eap_methods
 !
 ssid guest
    vlan 103
    authentication open
 !
 ssid management
    vlan 10
    authentication network-eap eap_methods
 !
 ssid voice
    vlan 101
    authentication shared
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
```

```
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.101
 encapsulation dot1Q 101
 no ip route-cache
 bridge-group 101
 bridge-group 101 subscriber-loop-control
 bridge-group 101 block-unknown-source
 no bridge-group 101 source-learning
 no bridge-group 101 unicast-flooding
 bridge-group 101 spanning-disabled
!
interface Dot11Radio0.102
 encapsulation dot1Q 102
 no ip route-cache
 bridge-group 102
 bridge-group 102 subscriber-loop-control
 bridge-group 102 block-unknown-source
 no bridge-group 102 source-learning
 no bridge-group 102 unicast-flooding
 bridge-group 102 spanning-disabled
!
interface Dot11Radio0.103
 encapsulation dot1Q 103
 no ip route-cache
 bridge-group 103
 bridge-group 103 subscriber-loop-control
 bridge-group 103 block-unknown-source
 no bridge-group 103 source-learning
 no bridge-group 103 unicast-flooding
 bridge-group 103 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.101
 encapsulation dot1Q 101
```

```
 no ip route-cache
 bridge-group 101
 no bridge-group 101 source-learning
 bridge-group 101 spanning-disabled
!
interface FastEthernet0.102
 encapsulation dot1Q 102
 no ip route-cache
 bridge-group 102
 no bridge-group 102 source-learning
 bridge-group 102 spanning-disabled
!
interface FastEthernet0.103
 encapsulation dot1Q 103
 no ip route-cache
 bridge-group 103
 no bridge-group 103 source-learning
 bridge-group 103 spanning-disabled
!
interface BVI1
 ip address 10.0.P.1 255.255.255.0
 no ip route-cache
!
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/
prodconfig/help/eag/ivory/1100
bridge 1 route ip
!
!
line con 0
line vty 0 4
 login local
line vty 5 15
 login
!
end

PodP#
```

Step 6 Configure PCs and connect to the AP

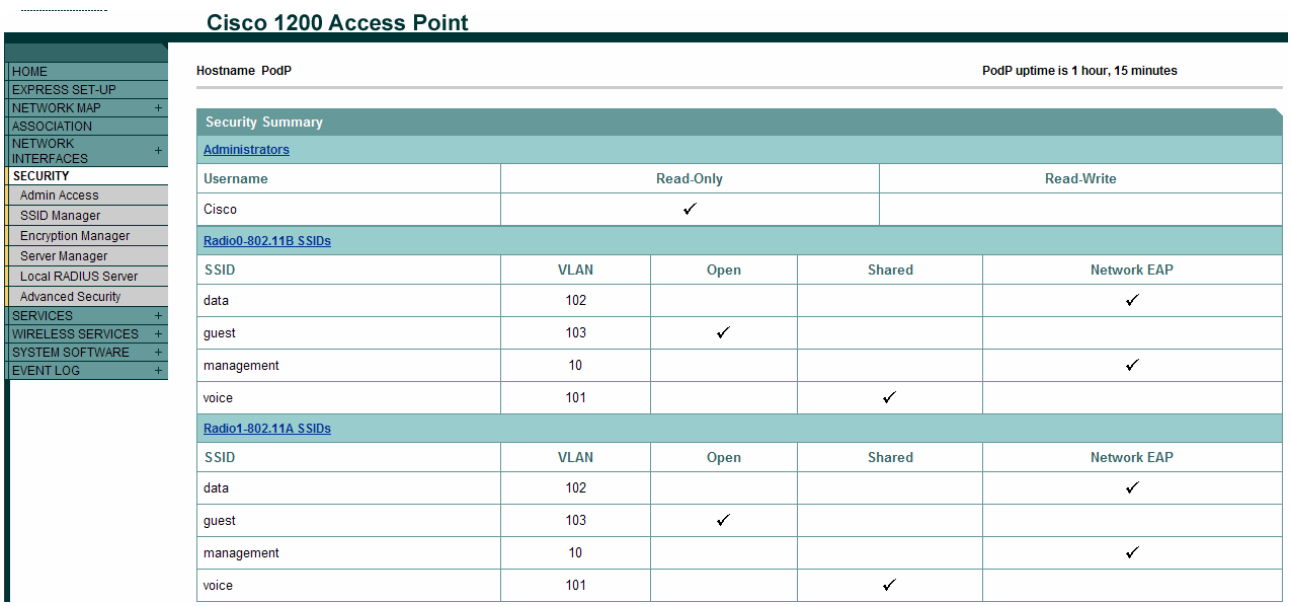
a. Now configure 2 wireless PCs.

- PC 1 with Open Authentication with a SSID of guest
- PC2 with Shared Authentication with a SSID of voice

b. Verify the connection through the **ASSOCIATION** page.

Note	Cisco recommends not using shared keys due to inherent security flaws with the technology

Step 7 Configure 802.11a VLANs (optional)



a. Now create the SSIDs for the 802.11a radio and apply to the existing VLANs .

b. Verify the settings afterwards through the **SECURITY** home page.

c. Verify the setting through IOS CLI.

d. Return to Step 6 and configure 2 802.11a clients. Verify the connections.

e. Save the configuration to a text file.

Step 7 Configure 802.11a VLANs through IOS CLI (Optional Challenge)

From the IOS CLI:

a. Erase the existing startup configuration and reload the AP.

b. Configure the SSIDs and VLANs for the 802.11b radio.

c. Verify the configuration by comparing to Step 5.

d. Configure the SSIDs and VLANs for the 802.11a radio.

e. Compare to the text file saved from Step 6d.

Step 7 Configure PCs and connect to the AP

a. Now configure 2 wireless PCs for the guest VLAN (Client and TCP/IP setting).

Can the PCs ping each other? _____

b. Now change the PC2 to the Voice VLAN.

Hint: Remember this VLAN has WEP Mandatory.

Can the PCs ping each other? _____

c. Finally, change the PC1 to the Voice VLAN.

Can the PCs ping each other? _____

d.

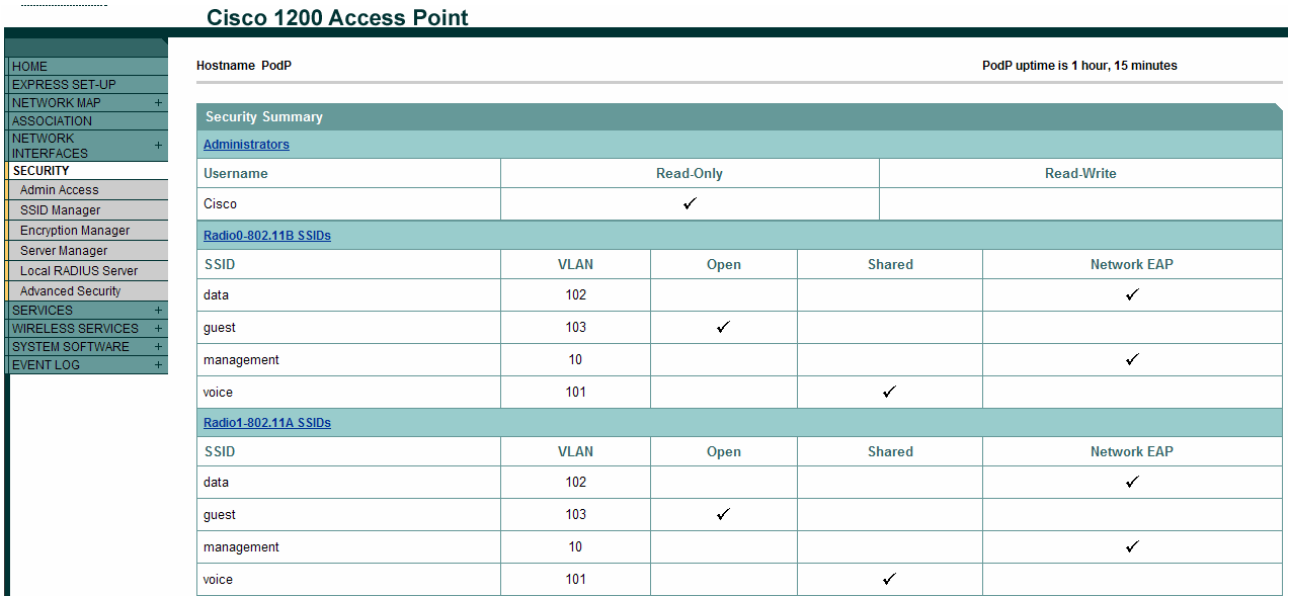
- PC 1 with Open Authentication with a SSID of guest

- PC2 with Shared Authentication with a SSID of voice

e. Verify the connection through the **ASSOCIATION** page.

Note	Cisco recommends not using shared keys due to inherent security flaws with the technology

Step 8 Configure 802.11a VLANs (Optional)



a. Now create the SSIDs for the 802.11a radio and apply to the existing VLANs.

b. Verify the settings afterwards through the **SECURITY** home page.

c. Verify the setting through IOS CLI.

d. Return to Step 6 and configure 2 802.11a clients. Verify the connections.

e. Save the configuration to a text file.

Step 9 Trunk AP to AP (Optional Challenge)

In this optional step, create a trunk between Pod APs through one of the following methods:

- On a 802.1q enabled switch, connect each APs to a switch with 802.1q trunking enabled on the port connecting each AP.
- Use a crossover cable between both APs

a. Change the BVI address to a 16 bit mask.

b. Configure the IP addresses on the wireless PCs with a 16 bit mask

c. Test connectivity between the PCs in VLAN 103.

d. Attempt to connect to the BVI address from the wireless PCs located in VLAN 103. Notice there is no connectivity between VLANs, only within VLANs.

e. Configure LEAP authentication for the data VLAN and test connectivity between pods PCs which are connecting through Data profiles.

f. Notice that there in no connectivity between VLANs. If time permits, configure a “router on a stick” to route between the VLANs. If using an enterprise 3550 or routing capable switch, inter VLAN routing can be configured without using a router.

Step 10 Configure 802.11a VLANs through IOS CLI (Optional Challenge)

From the IOS CLI:

a. Erase the existing startup configuration and reload the AP.

b. Configure the SSIDs and VLANs for the 802.11b radio

c. Verify the configuration by comparing to Step 5

d. Configure the SSIDs and VLANs for the 802.11a radio.

e. Compare to the text file saved from Step 6d.

f. Return to Step 6.

Lab 9.3.9 WLAN Design

Estimated Time: The time needed for this lab may vary

Number of Team Members: Students will work individually or in small groups.

Objective

In this lab, students will identify various applications of wireless local area networks (WLANs). The student will then choose one application and detail a WLAN design for it. The detailed design should utilize all of the following to present their findings:

- Drawings
- Configurations
- Topologies
- Issues
- Advantages
- Disadvantages
- Challenges
- Any other useful information

Scenario

The four main design requirements for a WLAN solution are as follows:

- It must have high availability
- It must be scalable
- It must be manageable
- It must be an open architecture allowing integration with third-party equipment

Along with the design requirements there are a few WLAN design basics:

- Same principles apply to all WLAN designs
- Get to know the customer and the customer's needs
- Design the WLAN to meet those needs

Preparation

The student will read and understand the material presented in FWL Module 9 prior to the lab.

Tools and resources

The following tools and resources will be helpful with this lab:

- Online Internet Research
- Industry Site Visits or contacts
- Trade Journals

Step 1 Customer industry

Identify the customer's industry that the team will design the Wireless LAN application for. Some common industries are listed below:

- Retailing
- Warehousing
- Healthcare
- Hotel/Hospitality
- Education
- Wireless Office
- Transportation
- Government and Military
- Internet Service Provider

Provide a brief summary of the business.

_____

_____

_____

_____

Step 2 Data collection

When dealing with data collection, consider the following questions:

What are the needs of the customer?

What applications will be used over the WLAN?

What bandwidth do these applications require?

Notes:

_____

_____

_____

_____

_____

_____

Step 3 Load and coverage

The following questions should be answered when dealing with load and coverage:

What is the total number of potential wireless clients on the network?

How big of an area has to be covered by the wireless LAN?

A diagram or sketch of the coverage area is required with this section.

Notes:

_____

_____

_____

_____

_____

_____

Step 4 Bandwidth and throughput

The following should be dealt with in regards to bandwidth and throughput:

What actual bandwidth speed is required by the wireless networking application used?

How will this bandwidth requirement be achieved with the chosen AP configuration?

Cell size

Channels

Data rate settings

High speed technologies like 802.11a or 802.11g

Note this information on the diagram.

Notes:

_____

_____

_____

_____

_____

_____

Step 5 Mobile users

When dealing with WLANs the demands of mobile users must be considered:

Will the users need to roam about the coverage area?

Will they require seamless roaming?

What kind of design can be used in the topology to accomplish these objectives?

Notes:

Step 6 Power consumption

What kind of power settings will be used on the wireless clients to conserve power when and if they need to be mobile and roam about the facility?

Notes:

Step 7 Interference

The following steps must be taken when dealing with potential interference to the WLAN:

Identify the typical sources of RF interference for the type of industry that the WLAN application is being designed for.

Locate each type of RF interference and note a possible option or solution for this type of interference.

Note the sources of RF interference on the diagram.

Step 8 Encryption

Encryption must also be considered depending on the client and the industry the WLAN is being designed for:

What are the data security and privacy requirements of the customer?

What methods will be used to ensure their privacy and security requirements for the wireless LAN?

No encryption

40 bit encryption

128 bit encryption

Note the advantages and disadvantages of each.

_____

_____

_____

_____

_____

_____

Step 9 Fire code and safety

What are the fire and safety risks usually associated with the industry coverage area that has been chosen? List each risk and identify the available options and solutions for each of them.

Notes:

_____

_____

_____

_____

_____

_____

Lab 9.5.5 Link Status Meter and Preferences

Estimated Time: 5 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will operate the Link Status Meter (LSM) utility for the wireless client adapter. Students will then learn how to set the Preferences options for the Aironet Client Utilities (ACU).

Scenario

This section explains how to use the LSM utility to determine the performance of the radio frequency (RF) link between the client adapter and its associated AP.

The second section explains how to set optional Preferences for the Aironet Client Utility.

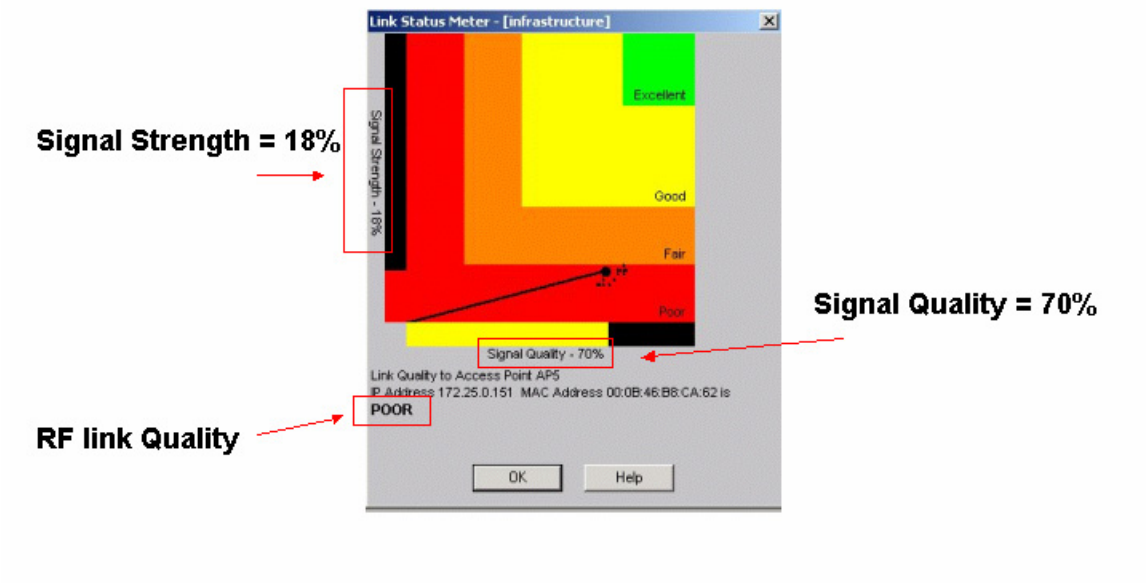
Preparation

The student will read and understand the material presented in FWL Module 9 prior to the lab.

Tools and Resources

The following tools and resources will help with this lab:

- Cisco Aironet AP properly operating and configured
- PC or laptop with a Cisco Aironet Wireless client adapter and utility properly installed



Step 1 Link Status Meter

Use the Link Status Meter to determine the signal strength.

Open the Aironet Client Utility screen.

Click on the **Link Status Meter** button. The Link Status Meter screen appears.

Data pertaining to the performance of the RF link can be accessed from ACU and LSM. However, they are displayed differently by each utility. This data is represented by histograms in ACU and is depicted graphically in LSM.

The Link Status Meter screen provides a graphical display of the following:

- **Signal strength**— The strength of the radio signal from the client adapter at the time packets are being received. It is displayed as a percentage along the vertical axis.
- **Signal quality**— The quality of the radio signal from the client adapter at the time packets are being received. It is displayed as a percentage along the horizontal axis.

1. What is the signal strength of the PC to the AP (%)?

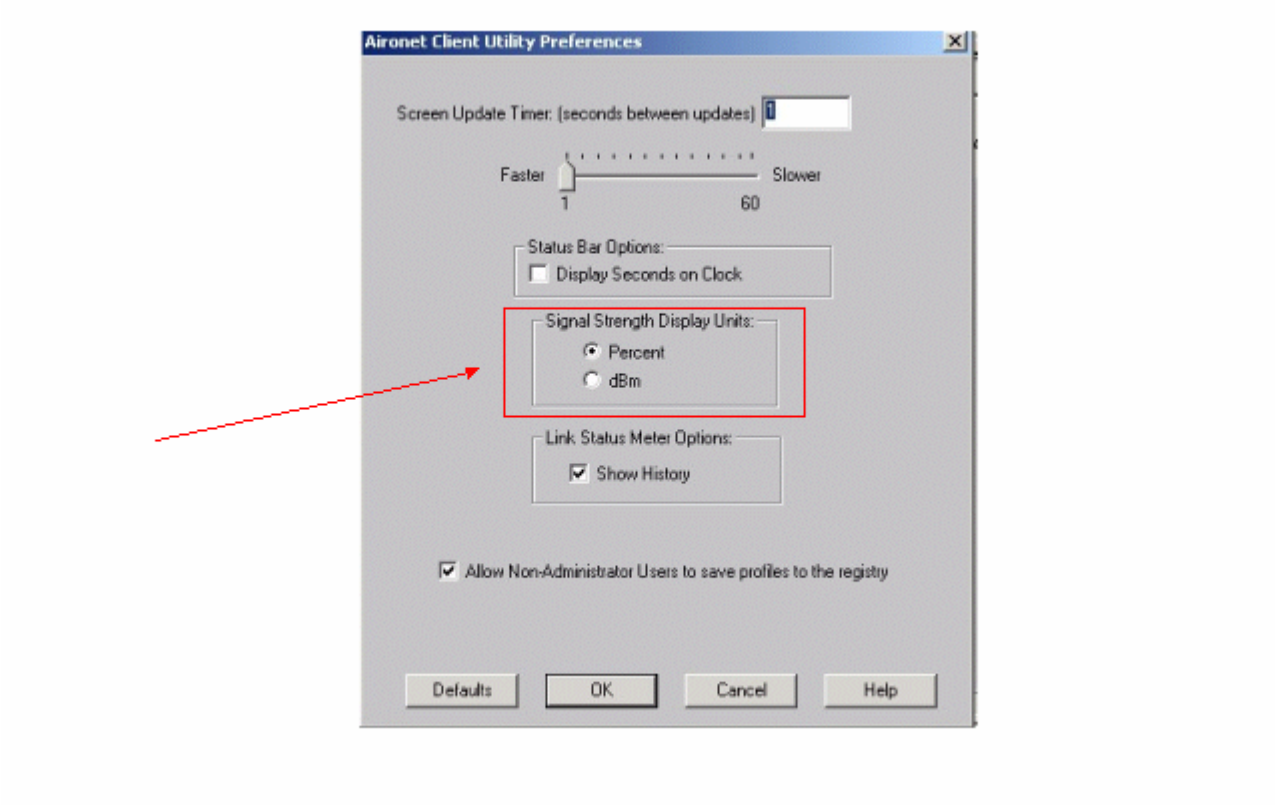
_____

2. What is the signal quality of the PC to the AP (%)?

_____

3. What is the quality of the overall RF link?

_____



Step 2 ACU preferences

Open the ACU Screen.

Click on the **Preference** button on the ACU screen.

a. What units are the signal strength and signal quality expressed in?

_____

_____

Click on the Percent or the dBm option to change the Signal Strength Display Units. Choose the opposite of whatever the current setting is.

Click the **OK** button to save the changes.

Click on the **Site Survey** button on the ACU screen.

b. What units are the signal strength and signal quality expressed in now?

_____

_____

Click on the **Preference** button and change the Preferences to the settings preferred.

Click the **OK** button to save the changes.

Lab 9.6.2 Using the Bridge Range Calculation Utility

Estimated Time: 15 minutes

Number of Team Members: Students will work in teams of two or individually

Objective

The student will learn how to use the Cisco Bridge Range Calculation Utility to determine bridge distances based on the following:

- Type of bridge
- Antenna
- Cables
- Splitter
- Other applicable wireless connectors

Scenario

Cisco makes it easy to calculate bridge distances by using the Cisco distance calculations spreadsheet that is available from the Cisco Web site.

These values are for line-of-sight and provide a 10dB fade margin, which helps assure that the calculations will work.

Preparation

The student should download the Cisco Bridge Range Calculation Utility at the following link:

http://www.cisco.com/application/vnd.ms-excel/en/us/guest/products/ps458/c1225/ccmigration_09186a00800a912a.xls

Tools and resources

Outdoor Bridge Range Calculation Utility

for

FCC, ISTC and other similar approvals areas

and

ETSI and similar (max +20dBm EIRP) areas.

Directions for use.

1. Select the proper page based upon your approvals for installation locations.
2. Select Product Being used for both sides of the link.
3. Select Datarate being used
4. Select power setting (if applicable) for both sides of the link (ETSI Calculation only)
5. Select antenna used oin each side . If using something other than Cisco/Aironet antennas, enter the gain factor in dBi.
6. Select cables being used on each side. If using something other than Aironet cable, enter the loss/100 ft
7. REMEMBER These are THEORETICAL calculations.
8. LINE OF SITE IS REQUIRED!

Cisco Systems
Empowering the Internet Generation℠

Cisco Wireless training © 2000, Cisco Systems, Inc. www.cisco.com 2

Address http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/obrc_in.xls

Links My Yahoo! Yahoo! Mail Yahoo! News Yahoo! Customize Links Free Hotmail RealOne Player Windows Media Windows

A2 = For Cisco Aironet 2.4GHz Outdoor Links ONLY

	A	B	C	D	E	F	G	H
1	Cisco Systems				Cisco Systems			
2					For Cisco Aironet 2.4GHz Outdoor Links ONLY			
3	Models Supported- Cisco Aironet BR350, BR340, BR500, WGB350, WGB340, PCI350 and PCI340							
4								
5	Regulatory Domain------>	North America/FCC		Select this from Power Regulatory Domain page				
6								
7		Site 1				Site 2		
8								
9	Select Product #1 ------->	AIR-BR350			Select Product #2 ------->	AIR-BR350		
10								
11	Select Power level------->	100			Select Power level------->	100		
12								
13	Select Datarate---------->	11Mbps						
14								
15	Select Antenna 1 here----->	13.5dBi Yagi			Select Antenna 2 Here----->	13.5dBi Yagi		
16								
17	For other Antenna- Enter Gain Here-->		6		For other Antenna- Enter Gain Here---->		6	
18								
19	Select Cable 1------->	100ft ULTRA LOW loss			Select Cable 2------->	100ft ULTRA LOW loss		
20								
21	For 'OTHER' Cable				For 'OTHER' Cable			
22	Enter Cable Loss/100 ft here---------->		4.4		Enter Cable Loss/100 ft here---------->		4.4	
23	Enter in Length Here---------->		100		Enter in Length Here---------->		100	
24								
25	Effective Isotrpoic Radiated Power-->		29.1		Effective Isotrpoic Radiated Power--->		29.1	
26								
27								
28								
29	Max Distance (w/ 10dB Fade Margin)---------->				2.8 Miles		4.6 Kilometers	
30								
31	Earth Bulge at above distance---------->				5 feet		1.5 Meters	

Step 1 Use the Cisco bridge range calculation worksheet

a. Download, Install and Open the bridge range calculation utility.

b. Select the product line being used. If using APs outdoors, the same procedures can be followed.

c. Next select the proper antenna for both sites:

d. For other non-Cisco antennas, enter the gain in dBi. If the gain is provided in dBd, simply add 2.14 to the number to convert to dBi.

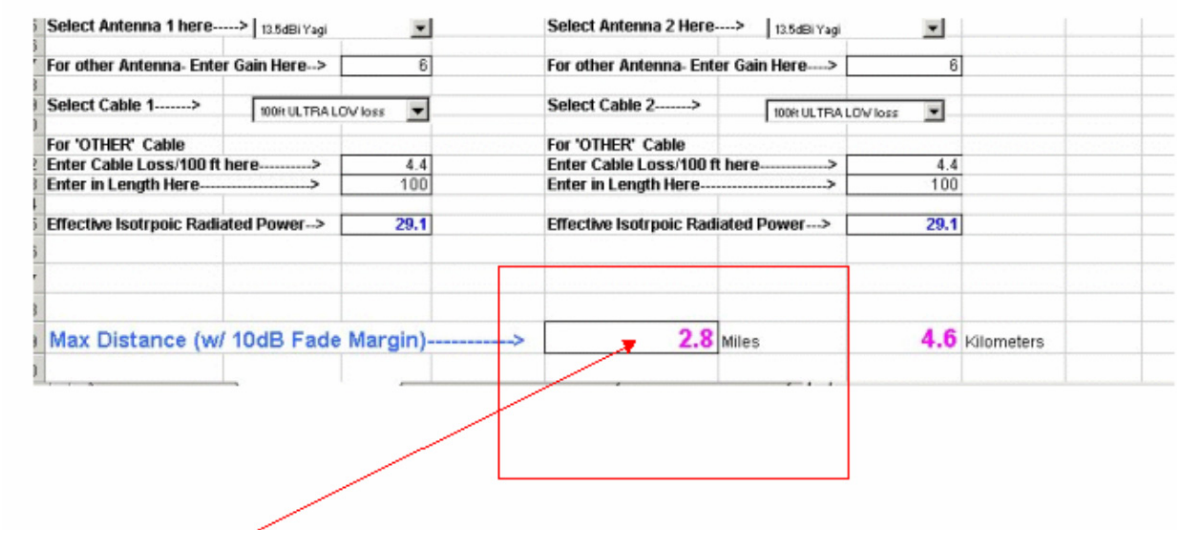
e. Then select the cable used on both sites.

- If using something other than standard Cisco antennas, enter in the length and cable loss per 100 ft. in the appropriate place. For Cisco cables this is 6.7dB /100 feet at 2.4Ghz.
- If a different cable is being used, contact the cable vendor for this information.

f. Add any other losses due to splitters, connectors and so forth into the misc. column.

g. The figure example uses the following:

- 20dBm, or 2.4 GHz, for the transmitter power
- - 13.5 dBi yagis antennas
- 2 cables of 20 feet each



The Bridge range calculation tool gives a maximum distance of approximately 2.8 miles.

a. What is the maximum distance when changing the data rate to 5.5Mbps?

_____

b. What is the maximum distance when changing the data rate to 2Mbps?

_____

c. What is the maximum distance when changing the data rate to 1Mbps?

_____

d. What is an easy way to extend the maximum distance while using the same power settings and antenna?

_____

Lab 10.2.7.1 Site Survey Active Mode

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will determine the best placement and coverage, or overlap, for the wireless APs. This will be done through the use of the wireless client adapter site survey utility.

Scenario

A site survey provides detailed information about all of the following:

- Where the APs are to be located
- How they will be mounted
- How they will be connected to the network
- Where any cabling or power may need to be installed

The Aironet Client Utility (ACU) site survey tool operates at the radio frequency (RF) level and is used to determine the best placement and coverage, or overlap, for APs.

During the site survey, the current status of the network is read from the client adapter and displayed four times per second so network performance can be accurately gauged.

The feedback received can help to eliminate areas with low RF signal levels that can result in a loss of connection between the client adapter and its associated AP.

The site survey tool can be operated in two modes:

- **Passive Mode** – This is the default site survey mode. It does not initiate any RF network traffic. It simply listens to the traffic that the client adapter hears and displays the results.
- **Active Mode** – This mode causes the client adapter to actively send or receive low-level RF packets to or from its associated AP. It then provides information on the success rate. It also allows parameters to be set governing how the site survey is performed.

Preparation

The student will read and understand the material presented in FWL Chapter 10 prior to the lab.

- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.
- When using the active mode, conduct the site survey with all variables set to operational values.

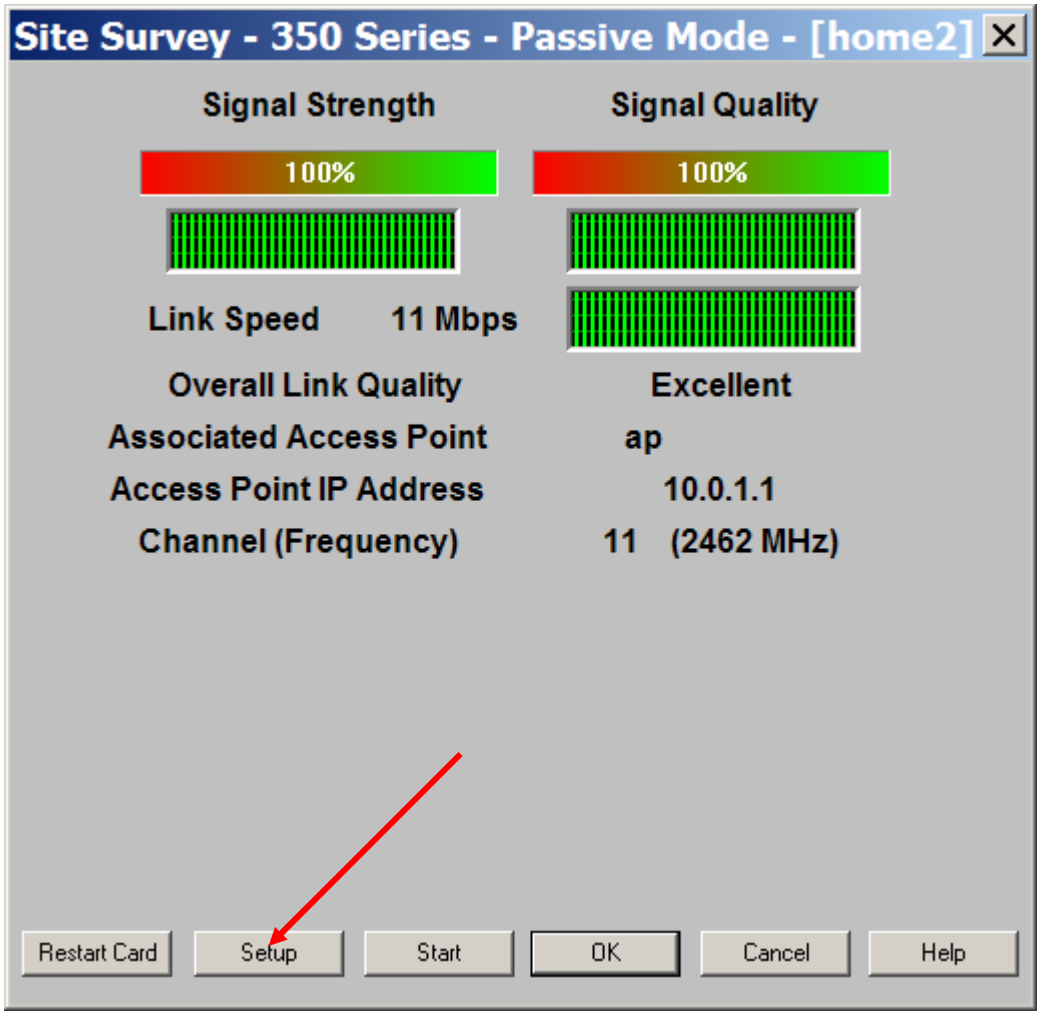
Tools and resources

The following tools and resources will be helpful with this lab:

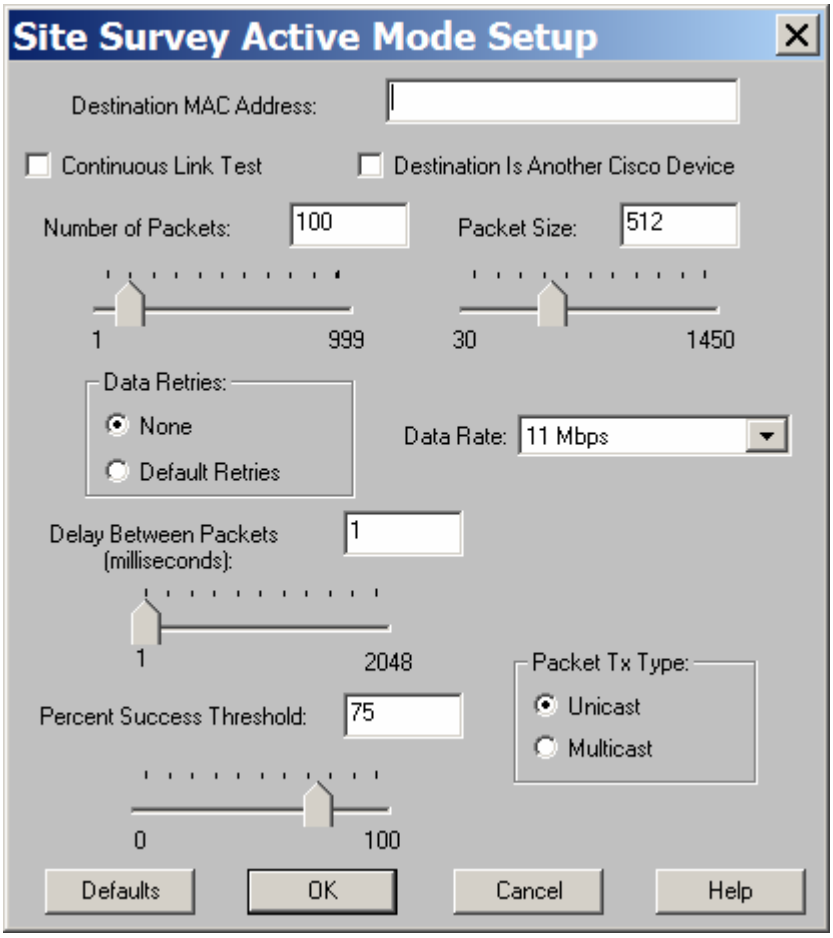
- An AP with a valid IP address
- PC or laptop with a client adapter and client utilities installed

Step 1 Using Active Mode

Follow the steps below to activate the site survey active mode and obtain current information about the ability of the client adapter to transmit and receive RF packets.



From the Client Utility Site Survey Passive Mode screen click the Setup button. The Site Survey Active Mode Setup screen looks like the example below.



Step 2 Using Passive Mode

After setting any parameters, click OK to save the settings. The Site Survey Passive Mode screen appears.

Note the information on the Passive Mode screen:

1. What is the signal strength?

   _____

2. What is the signal quality?

   _____

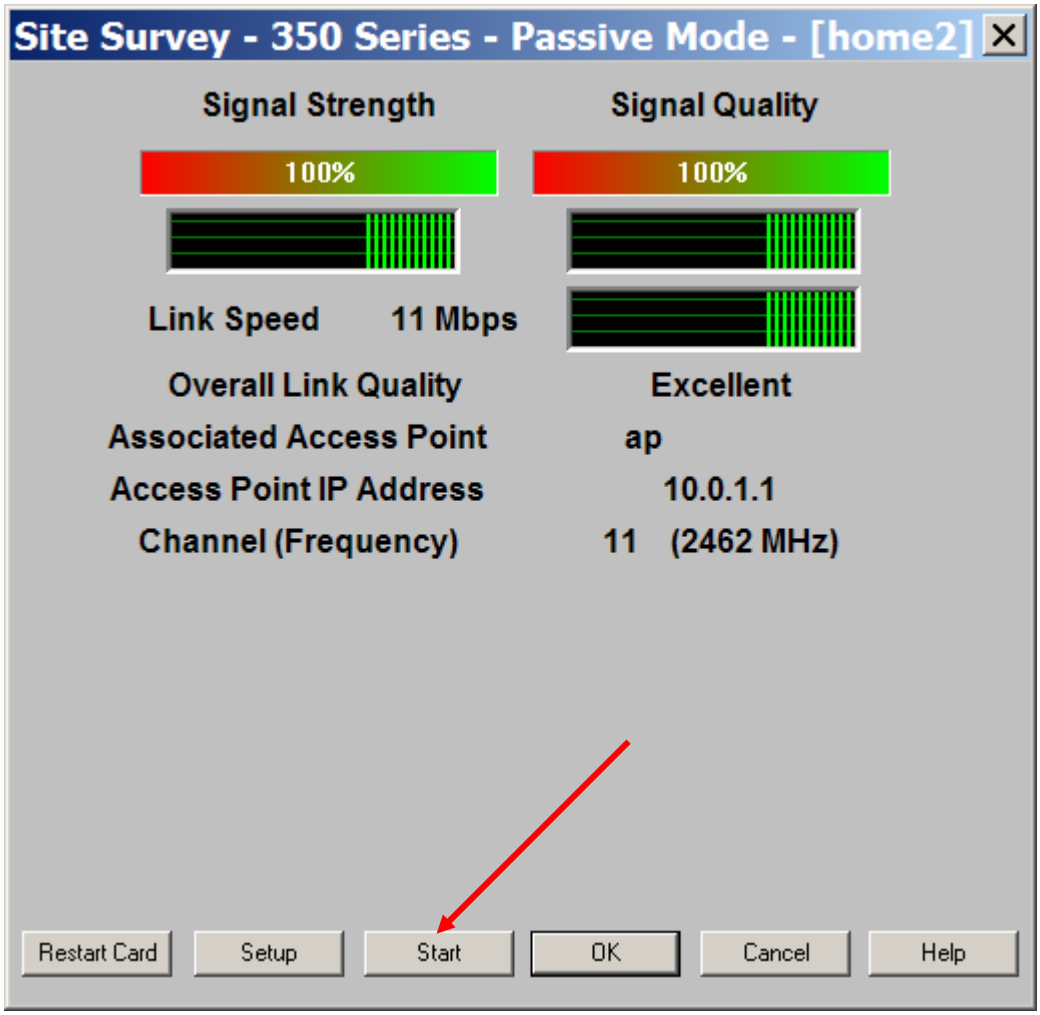
3. What is the link speed?

   _____

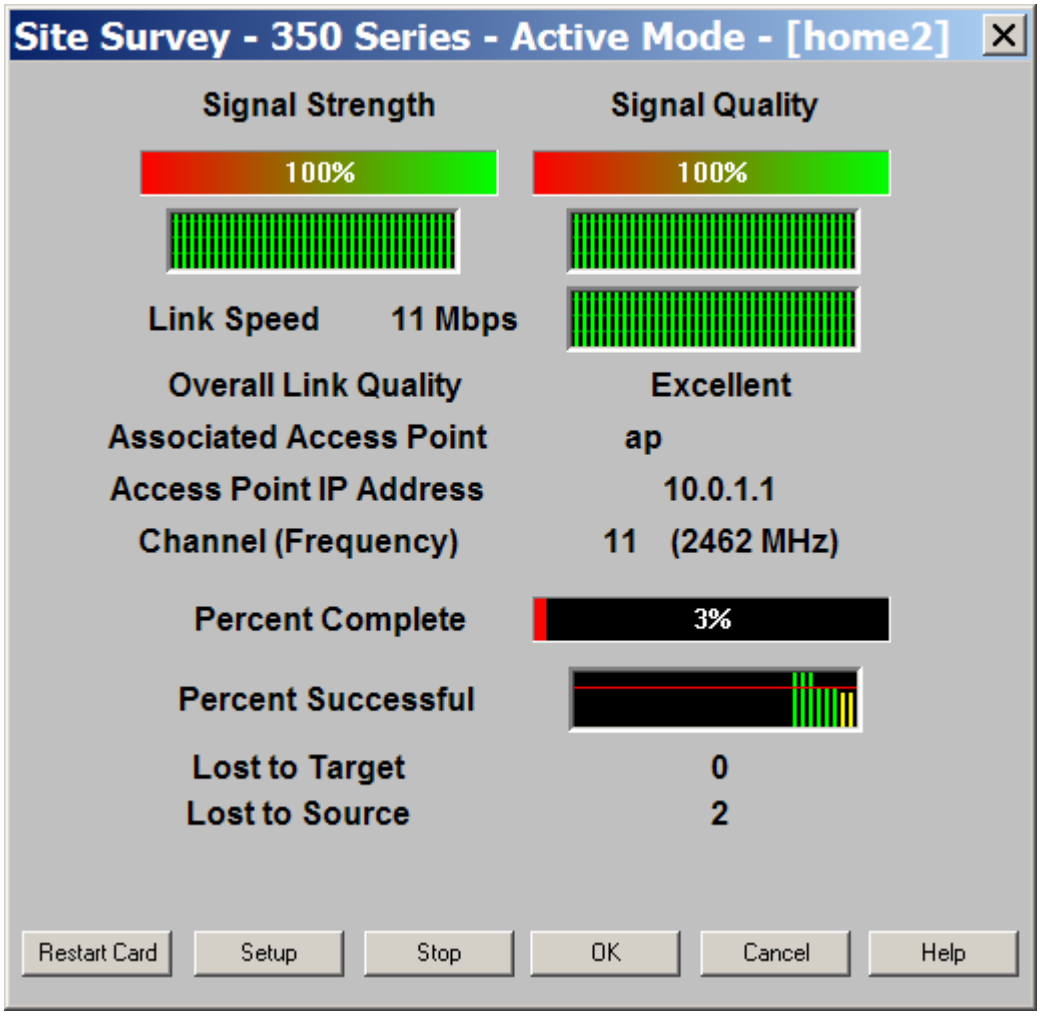
4. What is the overall link quality?

   _____

Step 3 Run Site Survey test



Click the Start button to run the site survey test.



The Site Survey Active Mode screen appears.

Position the Laptop PC in various locations relative to the AP.

Note the changes in the indicator field values listed below:

a. What is the signal strength?

_____

b. What is the signal quality?

_____

c. What is the link speed?

_____

d. What is the overall link quality?

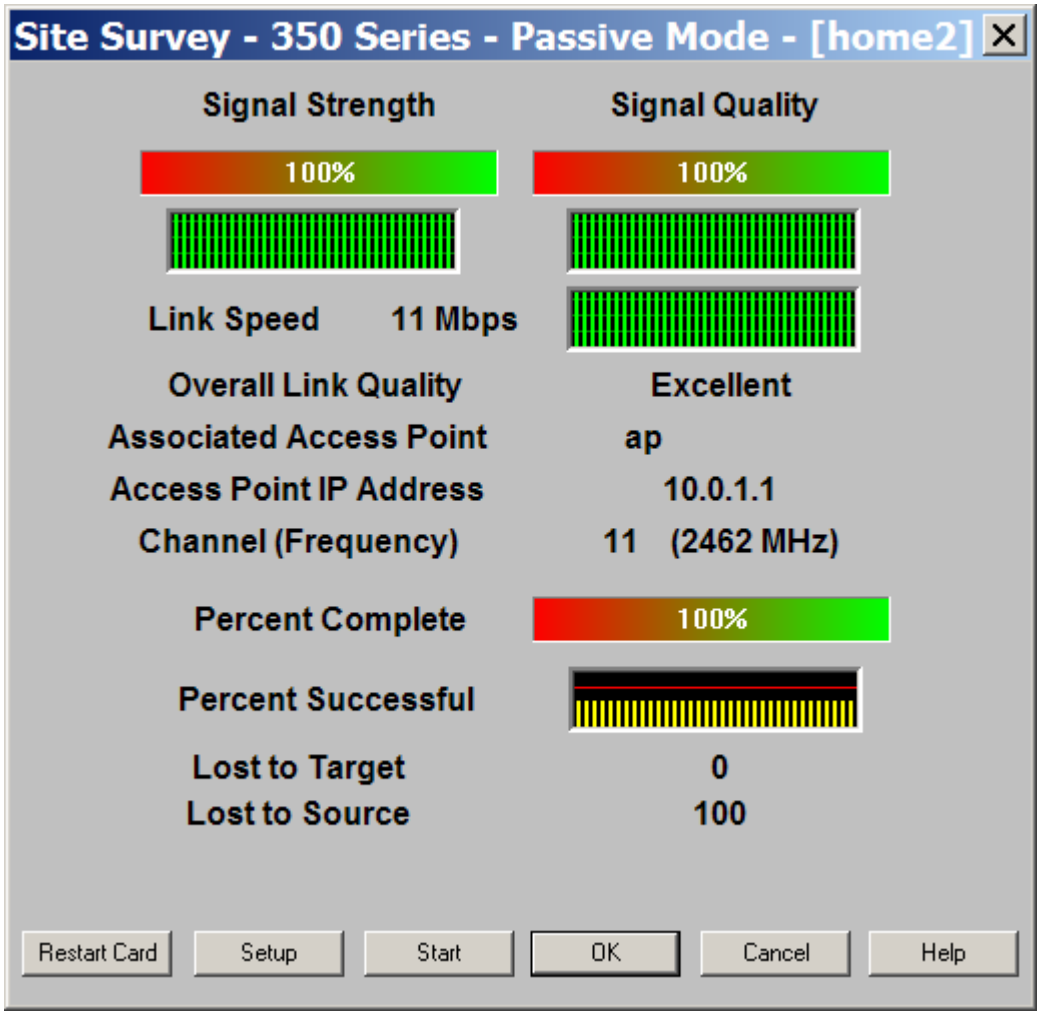
_____

e. How many packets were lost to target?

_____

f. How many packets were lost to source?

_____



When the Stop button is clicked or the Percent Complete reaches 100%, the active mode changes back to the passive mode.

Click **OK** or Cancel to exit the site survey application.

Lab 10.2.7.2 Survey the Facility

Estimated Time: Actual time will vary depending on the size of the site.

Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will perform a site survey of an assigned location. Students should include all of the following in site survey results:

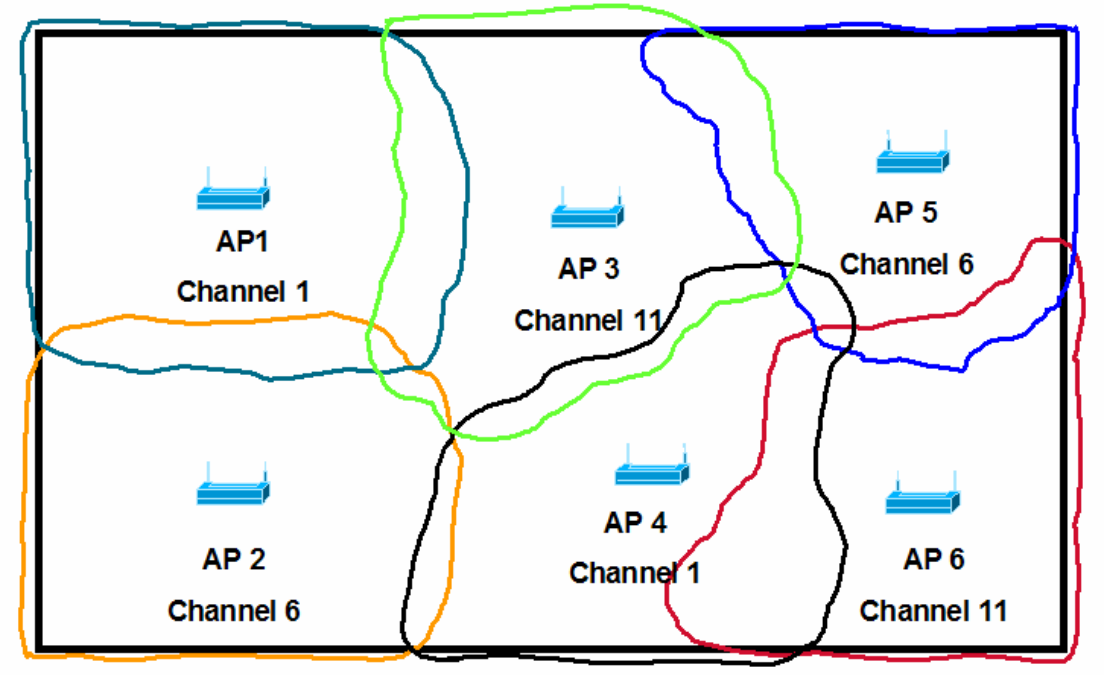
- Channel selections
- Data rates
- Antenna selection

Scenario

A site survey provides detailed information about the following:

- Where the APs are to be located
- How they will be mounted
- How they will be connected to the network
- Where any cabling or power may need to be installed

By providing the customer with a detailed site survey report, the IT manager can turn the necessary portions over to a local contractor. The contractor can then install the network cabling and power cabling that may be needed to provide the wireless local-area network (WLAN) connectivity to the network.



Preparation

The student should perform all of the following in preparation for this lab:

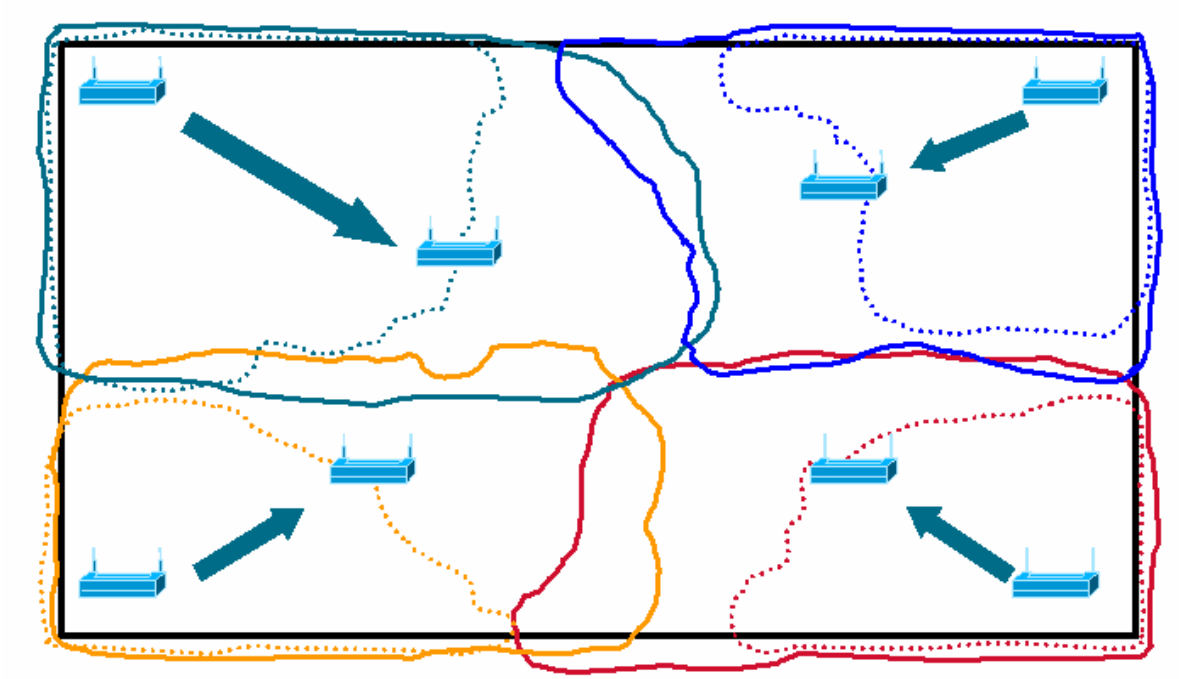
- Read through the lab prior to conducting the site survey.
- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.
- Conduct the site survey with all variables set to operational values for use in the active mode.
- Obtain a site map and permission to use the areas that are to be surveyed in advance.

Tools and resources

The following tools and resources will be helpful with this lab:

- An AP with a valid IP address.
- A PC with a client adapter and client utilities installed.
- A site map of the area you are surveying.
- An optional site survey kit for performing the site survey at an extended site other than the classroom.

Step 1 Begin the site survey in a corner of the facility

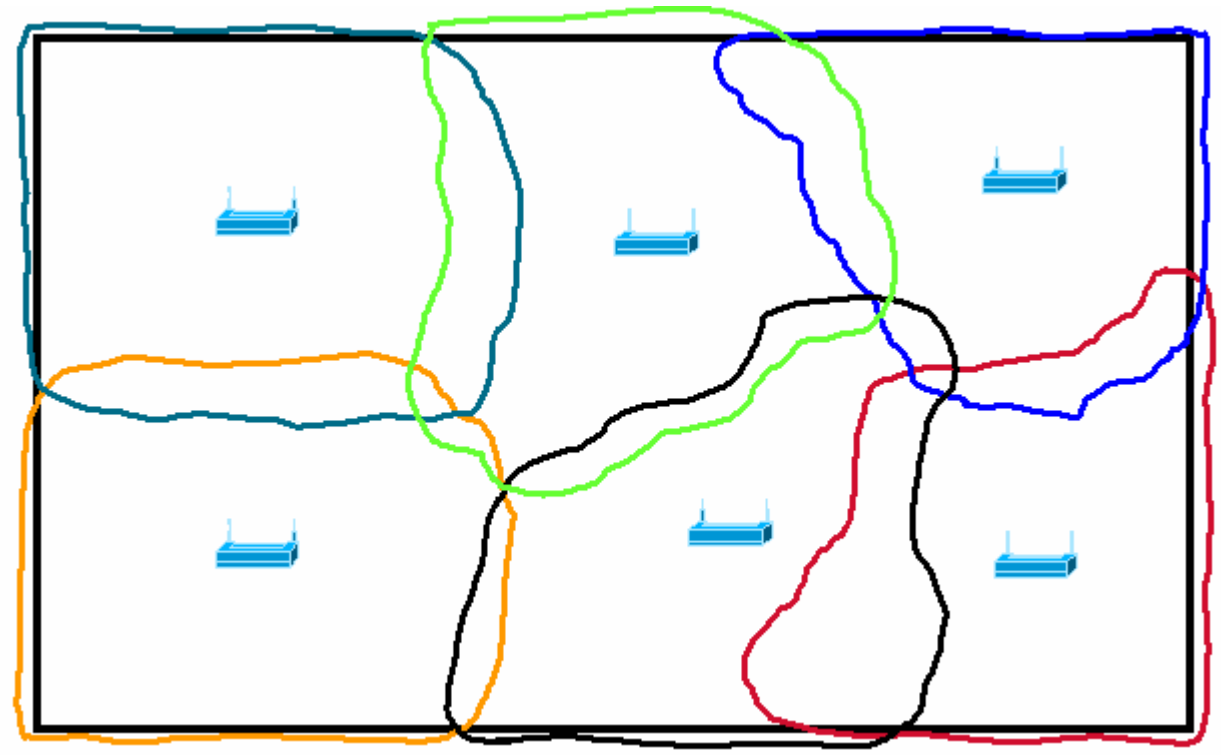


The easiest way to start a site survey is to pick one area of the facility that needs coverage. Choose a corner and place the AP in that corner. Survey the coverage of that AP and make a note of where the furthest point of coverage is from it. Then move the AP to the furthest coverage point.

Note If the AP is placed in the corner, as much as 75 percent of your coverage cell might be wasted covering an area outside the building that does not need coverage.

Sketch the actual site below which is surveyed. Indicate where the AP is located. Draw the pattern of coverage.

Step 2 Plan for overlap



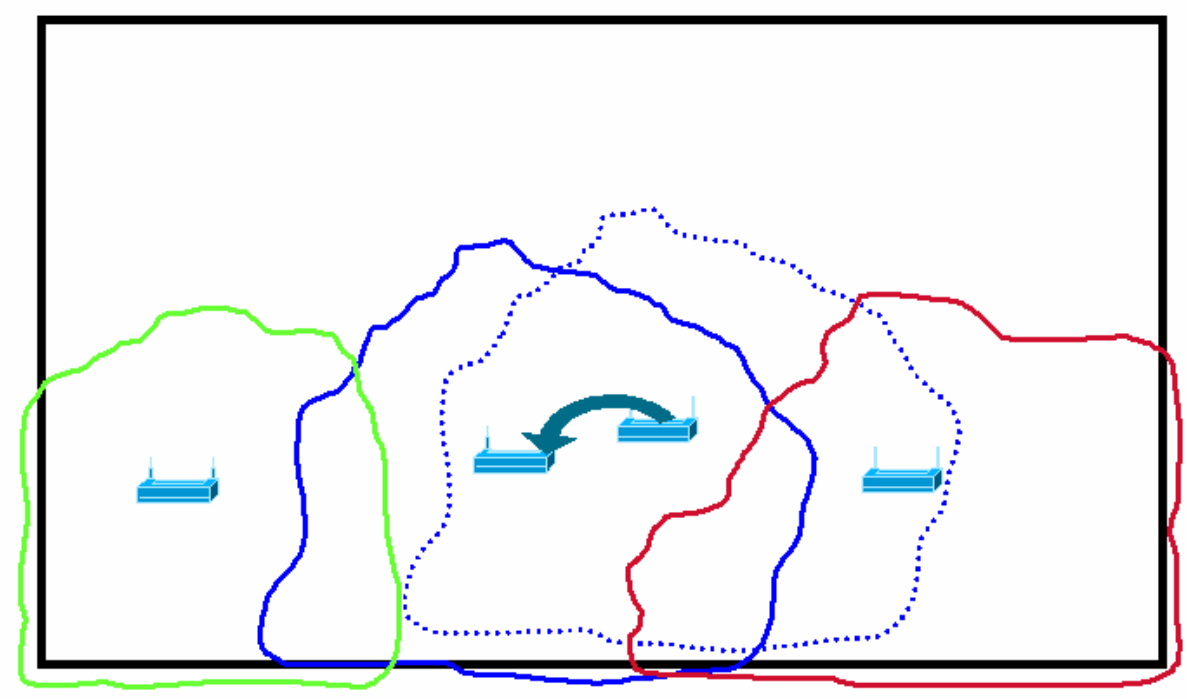
Once the AP has been moved, survey its coverage. It may be necessary to move the AP several times in order to find the best placement.

Once the best location for that AP has been decided on, move to a different corner of the facility and repeat the process. In a more advanced survey, repeating the process four times might only provide coverage around the perimeter of the facility.

Now fill in the holes in coverage. This is where experience and judgment will come into play. Some engineers might elect to survey the perimeter and then fill in the center. Remember, if seamless coverage is needed, the coverage cells must overlap. For a standard survey, 15 percent overlap is usually sufficient to provide for smooth, transparent handoffs.

Sketch the actual site below which is surveyed. Indicate where the APs will be located. Draw the patterns of coverage.

Step 3 Survey from the middle



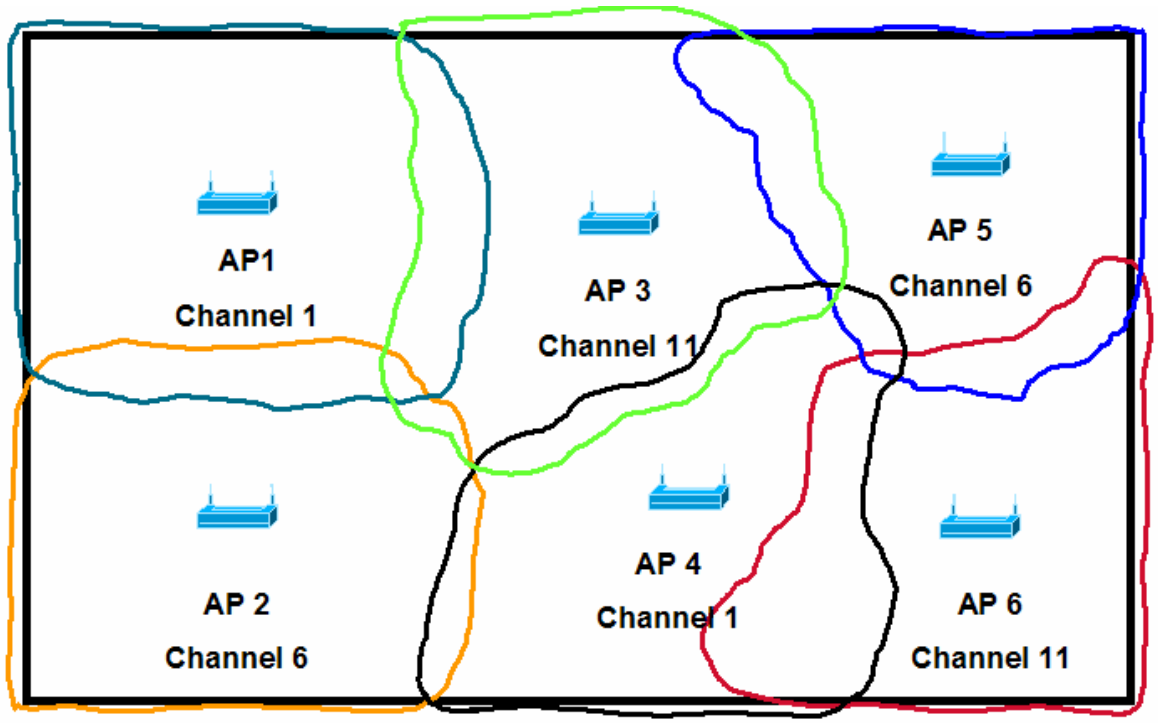
Survey the first two areas and fill in the middle

Another approach is to survey the first two APs and find the coverage areas.

Place an AP at the edge of the first AP cell, survey the coverage, and then move the AP out further to utilize its entire cell. This allows the size of the cell to be roughly judged. Then survey the new location to determine feasibility and adjust as necessary.

Once the AP location has been decided, continue this process until the entire facility is covered.

Step 4 Channel selection

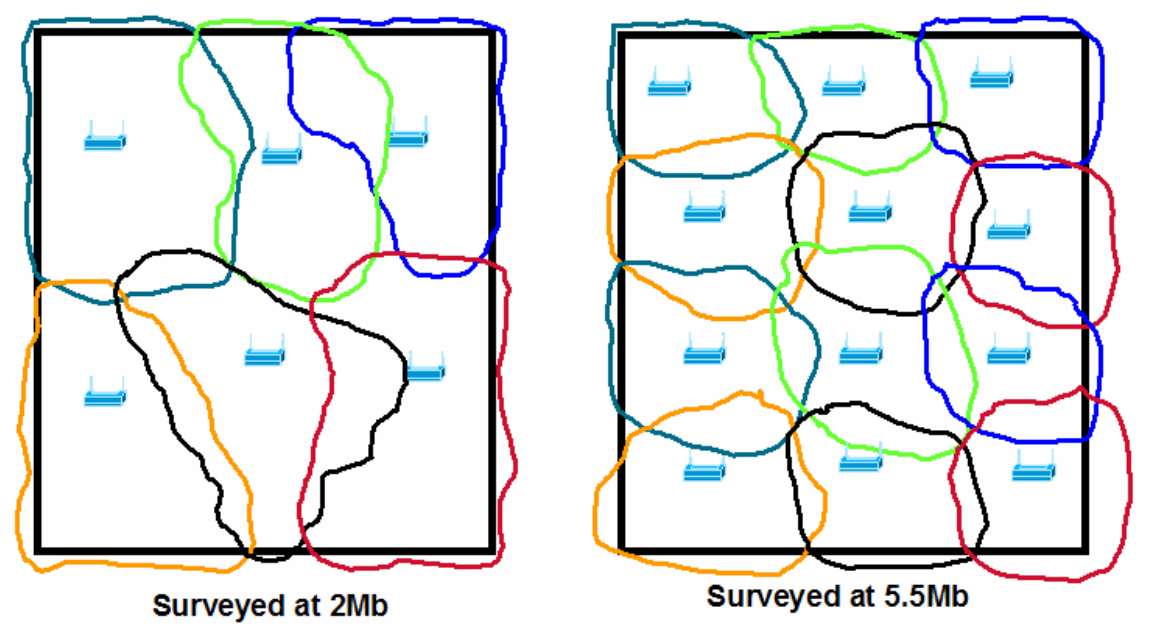


When surveying, take into account the fact that there are only three non-overlapping channels when using 802.11b and 802.11g. In order to maximize the data rate, use these channels. Using the non-overlapping channels insures that the APs will not interfere with each other.

As the WLAN is being designed, survey using the channel that the AP is intended to operate on. Part of the surveying duties is to test for interference. If every AP is surveyed using the same channel, andnot the actual channel the AP will be using, it will be difficult to verify that no interference exists on the channel that the AP will actually be using.

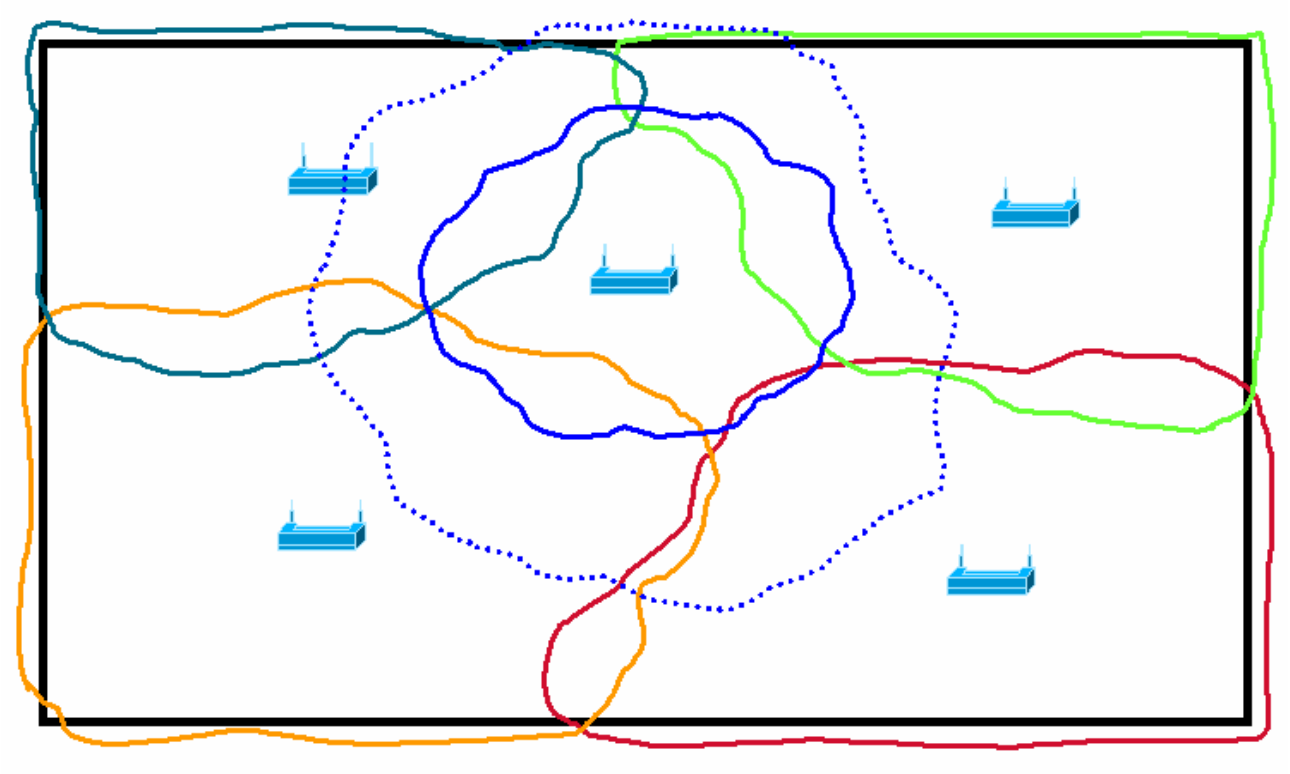
Sketch the actual site below which is surveyed. Indicate where the APs will be located and the channels to be used. Draw the patterns of coverage.

Step 5 Survey the data rates



Once the minimum data rate that the customer will be using has been determined, survey at that data rate. The data rate that is chosen will drastically affect the results of the site survey. In the example in the figure, the same area is surveyed at two different data rates. If the survey is done at 2Mb it takes six APs to cover the facility. If the survey is done at 5.5Mb it might take twelve APs to cover the facility.

Step 6 Antenna choice, power level and cell size



The student may elect to use a different antenna to obtain more coverage from the APs, use smaller antennas and add more APs. Another possibility is changing the power levels on one or more of the APs to change the size of the coverage cell or cells. Finally, the student may elect to use a combination of these options to get the coverage they need.

Lab 10.3.6 Mounting and Installation

Estimated Time: Actual times will vary depending on the amount of supplies and tools.

Number of Team Members: Students will work in teams of two.

Objective

The objective of this lab is to explore wireless installation options and methods for:

- BR350
- AP1200

Scenario

Proper installation techniques are required to complete a safe and professional installation. Students should demonstrate proficiency using drywall or concrete anchors and wood screws. Proper routing and anchoring of Ethernet cables can be covered as well.

Tools and resources

The following are required

- Cordless Drill and screwdriver
- 1200 AP
- 1200 AP mounting Brackets
- BR350 Mounting Kit
- Tie Wraps
- Wood Blocks
- Available flat surface and drop ceiling for practice mounting
- Ceiling enclosure (optional)

Additional resources

http://www.chatsworth.com/zone/wireless.htm

http://www.nema-enclosures.cc/

http://www.nema.org/index_nema.cfm/606/

http://ulstandardsinfonet.ul.com/scopes/2043.html

CAUTION	*Always consult the instructor before drilling in any surface.*
CAUTION	*Never drill additional holes in antennas, APs, or bridges as this will void the warranty*
CAUTION	*Make sure any electrical power is turned off*
CAUTION	*Always have a person hold the ladder when in use.*
CAUTION	*Always create a buffer zone with bright markers or cones*

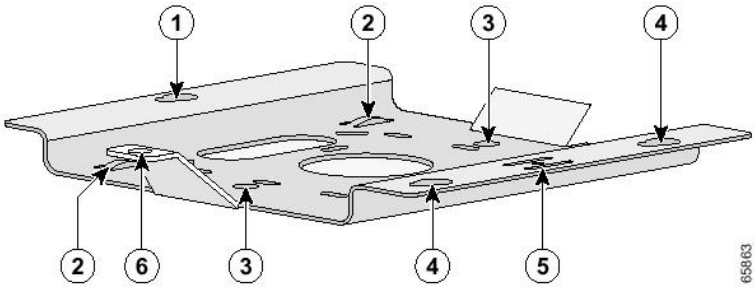
Step 1 AP Installation mounting on surface

The 1200 AP can be mounted on the following surfaces:

- Horizontal or vertical flat surfaces, such as walls or ceilings
- Suspended ceilings

The 1200 AP meets Underwriters Laboratories (UL) 2043 certification, and has an extended operating temperature of (-20 to 55ºC or -4 to 131ºF). Keep this in mind when deciding where to mount the AP.

The AP ships with a detachable mounting bracket and the necessary mounting hardware. Because it is detachable, the mounting bracket can be used as a template to mark the positions of the mounting holes for the installation. Then install the mounting bracket and attach the AP when ready. The mounting bracket provides a professional look to the installation.



1	Access point mount	**4**	Access point mounts
2	Cable tie points	**5**	Locking detent
3	Ceiling mount holes	**6**	Security hasp

Mounting on a horizontal or vertical surface

Follow these steps to mount the AP on a horizontal or vertical surface.

a. Use the mounting bracket as a template to mark the locations of the four mounting holes.

b. Drill one of the following sized holes at the locations marked:

- 3/16 in. (4.7 mm) if using wall anchors
- 1/8 in. (6.3 mm) if not using wall anchors

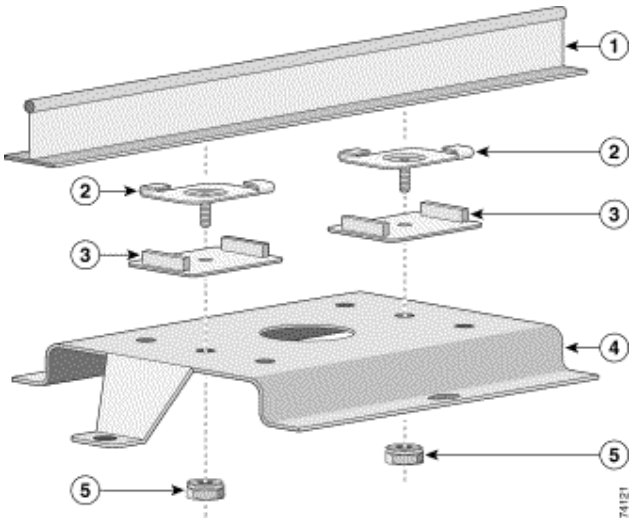
c. Install the anchors into the wall if using them. Otherwise, go to Step 4.

d. Secure the mounting bracket to the surface using the #8 fasteners.

e. Attach the AP to the mounting bracket.

Note The installation can be made more secure by mounting it to a stud or major structural member and using the appropriate fasteners. On a vertical surface, mount the bracket with its security hasp facing down.

1	Suspended ceiling T-rail
2	Caddy fastener
3	Plastic spacer
4	Mounting bracket
5	Keps nut



Single Band

Dual Band

Mounting on a suspended ceiling

Note	To comply with NEC code, a #10-24 grounding lug is provided on the mounting bracket

Follow these steps to mount the AP on a suspended ceiling or as directed by the instructor.

a. Determine where to mount the AP.

b. Attach two caddy fasteners to the suspended ceiling T-rail.

c. Use the mounting bracket to adjust the distance between the caddy fasteners so that they align with the holes in the mounting bracket.

d. Use a standard screwdriver to tighten the caddy fastener studs in place on the suspended ceiling T-rail. Do not overtighten.

e. Install a plastic spacer on each caddy fastener stud. The legs of the spacer should contact the suspended ceiling T-rail.

f. Attach the mounting bracket to the caddy fastener studs and start a Keps nut on each stud.

g. Use a wrench or pliers to tighten the Keps nuts. Do not overtighten.

h. Attach the AP to the mounting bracket.

Attaching the AP to the mounting bracket

Follow these steps to attach the AP to the mounting bracket:

a. Line up the three mounting pins on the AP with the large ends of the keyhole-shaped holes on the mounting bracket.

b. Insert the AP into the keyhole shaped holes and maintain a slight pressure to hold it in place.

c. Slide the mounting pins for the AP into the small ends of the keyhole-shaped holes on the mounting bracket and push the connector end of the AP. You will hear a click when the locking detent contacts the AP and locks it into place.

d. Attach and adjust the antenna(s) or antenna cables.

e. Connect the Ethernet cable to the Ethernet port of the AP.

f. Insert the 1200 series power module cable connector into 48 VDC power port of the AP, if using a local power source.

Securing the AP to the mounting bracket

The security hasp on the mounting bracket allows the AP to lock to the bracket to make it more secure. When the AP is properly installed on the mounting bracket, the holes in the security hasps line up so a padlock can be installed.

Known compatible padlocks are Master Lock models 120T or 121T.

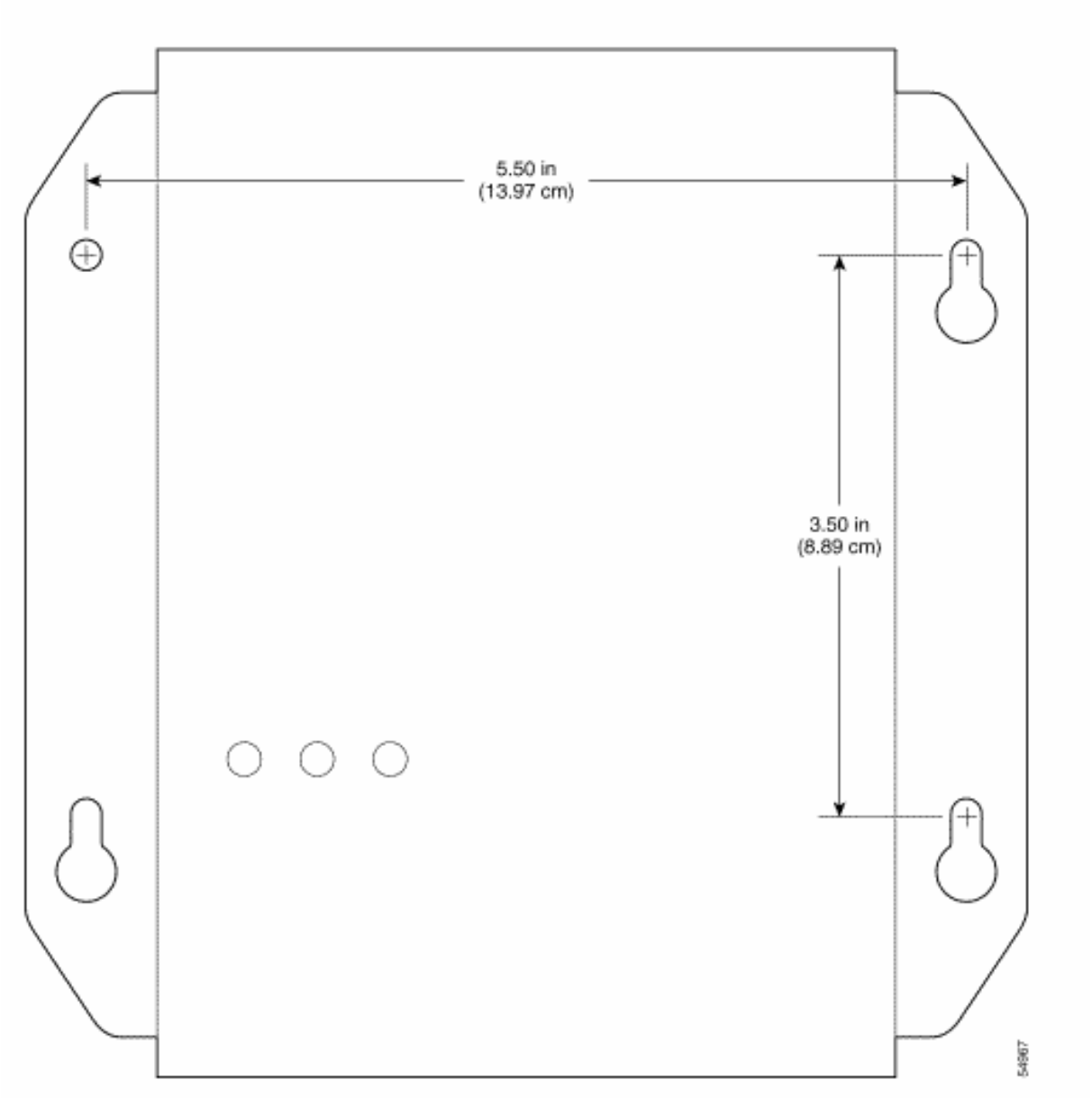
Other options

The AP can be mounted using nylon or metal tie wraps. Also, wood blocks can be attached to steel beams. ¾" Plywood can be attached to concrete walls to provide a buffer against moisture. Attaching a mounting bracket to wood is much easier than mounting directly to steel or concrete.

Step 3 Bridge installation indoors

Mount the bridge or AP to a wall using the mounting kit and the mounting template. The kit contains the following parts:

- Four #6 - #10 plastic wall anchors
- Four #8 x 0.88" sheet-metal screws



a. If the original mounting template cannot be found, create a mounting template to drill four holes in the wall. Take the BR350 and trace the outline of the bridge and the holes on a separate piece of cardstock or paper. Or, check it with the one shown above.

b. Mark the holes on the wall.

c. Drill the holes. The holes should be 3/16 in. (0.48 cm) in diameter and 1 in. (2.54 cm) deep.

d. Tap the wall anchors into the holes.

e. Drive three screws into the wall anchors corresponding to the key-holes in the mounting template, leaving a small gap between the screw head and the anchor.

f. Position the keyholes of the case over the screws and pull down to lock it in place.

g. Drive the remaining screw into the fourth wall anchor and tighten all mounting screws.

h. Connect the Ethernet cable to the AP or bridge.

i. If the AP or bridge has removable antennas, connect the antennas or antenna cables to the AP or bridge.

Step 4 Using enclosures to mount APs and bridges

Enclosures can be used to mount APs and bridges indoors and outdoors. There are many types and styles of enclosures

Below is a sample wall enclosure:

Alternative AP installation in drop ceiling (optional)

Using a Ceiling Mounted enclosure, the Cisco 350, 1100, or 1200 with the standard dipole (rubber duck) can be safely installed in a drop ceiling grid. This saves time and cost of installing other antennas.

Ceiling Mounted Enclosures from Chatsworth include:

- AAT-CAP-35 - Faceplate for Cisco® 350
- AAT-CAP-11 -Faceplate for Cisco® 1100
- AAT-CAP-12 – Faceplate for Cisco® 1200

Consult with the local, state, and federal guidelines for the proper enclosure. Below are NEMA Rating levels.

NEMA	Use	Protection Against
1	indoor	hand contact with enclosed equipment. low cost enclosure but suitable for clean and dry environments.
2	indoor	limited amounts of falling dirt and water
3	outdoor	Wind-blown dust, rain, and sleet; ice which forms on the enclosure.
3R	outdoor	falling rain and sleet; ice which forms on the enclosure
4	indoor	windblown dust and rain, splashing water, and hose directed water; ice which forms on the enclosure
4X	indoor / outdoor	corrosion, windblown dust and rain, splashing water, and hose directed water; ice which forms on the enclosure
6	Indoor / outdoors	occasional temporary submersion
6P	Indoor / outdoors	occasional prolonged submersion. Corrosion protection
12	Indoor / outdoors	dust, falling dirt, and dripping non-corrosive liquids
13	indoor	dust, spraying of water, oil, and non-corrosive coolant

Lab 10.4.2.1 Request for Proposal

Estimated Time: The time will vary depending on the scope of the project.

Number of Team Members: Students will work in teams of two.

Objective

The objective of this lab is to prepare a request for proposal (RFP) for a fictitious business for adding a wireless local-area network (WLAN) to their business network.

Scenario

An RFP lists a customer's design requirements and the types of solutions a network design must include. Organizations send a RFP to vendors and design consultants. They use the responses they receive to help select a suitable vendor or supplier.

Preparation

The instructor will compile a list of approved fictitious businesses used for the RFP.

Tools and resources

The following tools and resources will be helpful with this lab:

- Online Internet research
- Vendor literature and site contacts
- Trade journals and publications
- Additional materials

A variety of technology RFPs are available at http://networkcomputing.telezoo.com/asp/vrfp/showvendorrfp.asp?idcats=722&history=^709^722&techname=Wireless

Step 1

Prepare a RFP that lists the design requirements of the business selected and the types of solutions for the network design. The RFP must include all of the following:

- Business goals for the project
- Scope of the project
- Information on the existing network and applications
- Information on new applications
- Technical requirements including the following:
  - Scalability
  - Availability
  - Performance
  - Security

    - Manageability
    - Usability
    - Adaptability
    - Affordability
- Warranty requirements for products
- Environmental or architectural constraints that could affect implementation
- Training and support requirements
- Preliminary schedule with milestones and deliverables
- Legal contractual terms and conditions

Lab 10.4.2.2 RFP Response

Estimated Time: The time will vary depending on the scope of the project.

Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will prepare a response to a request for proposal (RFP) for the addition of a wireless local-area network addition to an existing wired LAN. Compete against other student teams by responding to the same RFP.

Scenario

In the previous lab, a RFP was prepared for a fictitious business seeking to add a wireless local area network to their existing network.

The instructor has reviewed those RFPs and has decided that each team will respond to the RFP.

Organizations send a RFP to vendors and design consultants. They then use the responses they receive to weed out suppliers that cannot meet requirements.

RFP responses help organizations compare all of the following presented by competing suppliers:

- Designs
- Product capabilities
- Pricing
- Service
- Support alternatives

Despite the fact that a response to an RFP must stay within the guidelines specified by the customer, use ingenuity to ensure that the response highlights the benefits of the design.

Base the response on an analysis of the customer's business and technical goals, and the flow and characteristics of network traffic. Write the response so the reader can easily recognize that the design satisfies critical selection criteria.

When writing the response, be sure to consider the competition. Try to predict what other vendors or design consultants might propose and then call attention to the aspects of this solution that are likely to be superior to competing designs.

In addition, pay attention to the customer's business style. Remember the importance of understanding the customer's biases and any office politics or project history that could affect the perception of the proposed design.

Preparation

The instructor will choose one RFP prepared from lab 10.5.2. All the student groups will use this RFP. All student teams will be responding to the same RFP chosen by the instructor.

Tools and resources

The following tools and resources will be helpful with this lab:

- Online Internet research sites
- Vendor literature, trade journals, and publications
- Response requirements

Step 1

The RFP states that the response must include some or all of the following topics:

- A network topology for the new design
- Information on the protocols, technologies, and products that form the design
- An implementation plan
- A training plan
- Support and service information
- Prices and payment options
- Qualifications of the responding vendor or supplier
- Recommendations from other customers for whom the supplier has provided a solution
- Legal contractual terms and conditions

Lab 10.4.2.3 Review of RFP Response

Estimated Time: Actual times will vary depending on the scope of the project

Number of Team Members: The instructor will review the responses with the class

Objective

In this lab, students will review the response written to the request for proposal (RFP) and determine whether the response meets the requirements of the RFP. Students shall rank the responses according to how well they addressed the RFP.

Scenario

Organizations use the responses they receive to eliminate suppliers that cannot meet requirements. RFP responses help organizations compare all of the following presented by competing suppliers:

- Design
- Product capabilities
- Pricing
- Service and support alternatives
- Security

Use the comparison chart for the responses to rank them prior to this lab.

Tools and resources

Comparison chart for ranking the responses.

TEAM	DESIGN	PRODUCT CAPABILITIES	PRICING	SERVICE and SUPPORT	TRAINING	SECURITY
TEAM 1						
TEAM 2						
TEAM 3						
TEAM 4						
TEAM 5						
TEAM 6						
TEAM 7						
TEAM 8						
TEAM 9						
TEAM 10						

Step 1 Ranking the RFP responses

Review the responses to the RFP and determine if it meets the guidelines that were set in the RFP.

Rank each response

Use the following criteria to help rank the RFPs:

- Business goals for the project
- Scope of the project
- Information on the existing network and applications
- Information on new applications
- Technical requirements including scalability, availability, performance, security, manageability, usability, adaptability, and affordability
- Warranty requirements for products
- Environmental or architectural constraints that could affect implementation
- Training and support requirements
- Preliminary schedule with milestones and deliverables
- Legal contractual terms and conditions

Step 2 Weighting systems

A weight will be assigned to each criterion as shown below. Assigning a weight to each criterion makes allowances to a team's total score based upon the importance of an individual criterion's impact on the project.

For example, a team may score very high on its design and low on support. But which of the criterion is more important to the success of the project? Should each of these criteria be given the same weighted score? If training is more important to the organization, then assign a higher weight to it, if the pricing is of higher importance to the organization, then assign a higher weight to the pricing category.

Have the class rank the criterion in an order of importance to the project. As an example: a multiplier based upon criterion importance is placed next to each criterion.

TEAM	DESIGNS (3X)	PRODUCT CAPABILITIES (5X)	PRICING (4X)	SERVICE and SUPPORT (3X)	TRAINING (2X)	SECURITY (5X)
TEAM 1						
TEAM 2						
TEAM 3						
TEAM 4						
TEAM 5						
TEAM 6						
TEAM 7						
TEAM 8						
TEAM 9						
TEAM 10						

The ranking system can be based upon how well each of the teams addressed the projects criterion, for example the following can be used:

1 – Poor

2 – Satisfactory

3 – Above Average

4 – Excellent

The score will take the ranking number and multiplier to assign a weighted score to the team. For example: TEAM 1 scored:

Designs – 2, the weighted score becomes 2 times 3 equaling 6.

Product Capabilities – 3, the weighted score becomes 3 times 5 equaling 15

Pricing – 4, the weighted score becomes 4 times 4 equaling 16

Service – 3, the weighted score becomes 3 times 3, equaling 9

Training – 3, the weighted score becomes 3 times 2 equaling 6

Security – 2, the weighted score becomes 2 times 5 equaling 4

TEAM	DESIGNS (3X)	PRODUCT CAPABILITIES (5X)	PRICING (4X)	SERVICE and SUPPORT (3X)	TRAINING (2X)	SECURITY (5X)
TEAM 1	6	15	16	9	6	10
TEAM 2						
TEAM 3						
TEAM 4						
TEAM 5						
TEAM 6						
TEAM 7						
TEAM 8						
TEAM 9						
TEAM 10						

TEAM 1's total score becomes 6 + 15 + 16 + 9 + 9 + 4 = 59

Score each team. The team with the largest numerical score wins the contract.

Lab 11.1.4 Basic Troubleshooting on AP

Estimated Time: 10 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will utilize basic troubleshooting procedures for problems with an AP.

Scenario

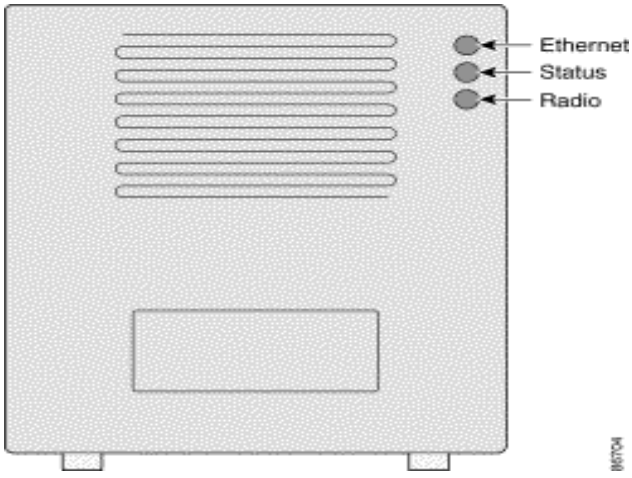
Troubleshooting networks, including WLANs, is more important than ever. Networks continue to add services as time goes on and with each added service comes more variables involved in implementing networks. This adds to the complexity of troubleshooting the networks as well. So, organizations increasingly depend on network administrators and network engineers having strong troubleshooting skills.

Tools and resources

The following tools and resources will be helpful with this lab:

- AP properly installed and configured on a wired LAN
- PC with a properly installed wireless NIC and client utility

Step 1 Check the top panel indicators



a. If the AP is not communicating, check the three indicators on the top panel. These indicators can be used to quickly assess the status of the unit.

b. The indicator lights have the following meanings:

c. The Ethernet indicator signals traffic on the wired LAN, or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.

d. Is the Ethernet Indicator light blinking on your AP? Yes or No

_____

e. The Status indicator signals operational status. Blinking green indicates that the AP is operating normally but is not associated with any wireless devices. Steady green indicates that the AP is associated with a wireless client.

f. Is the status of the AP associated or not associated?

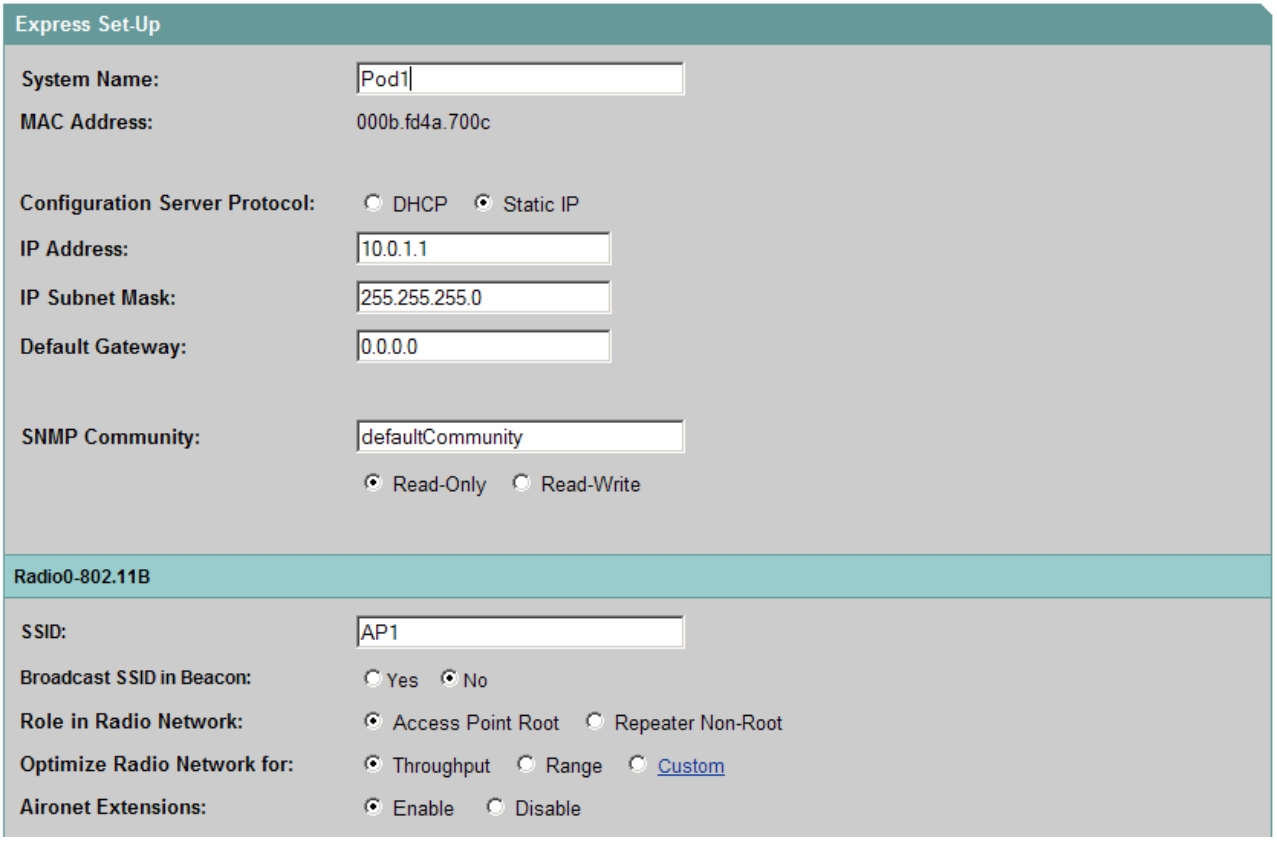
_____

g. The Radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the radio of the AP.

h. Is there radio traffic on your AP? Yes or No

_____

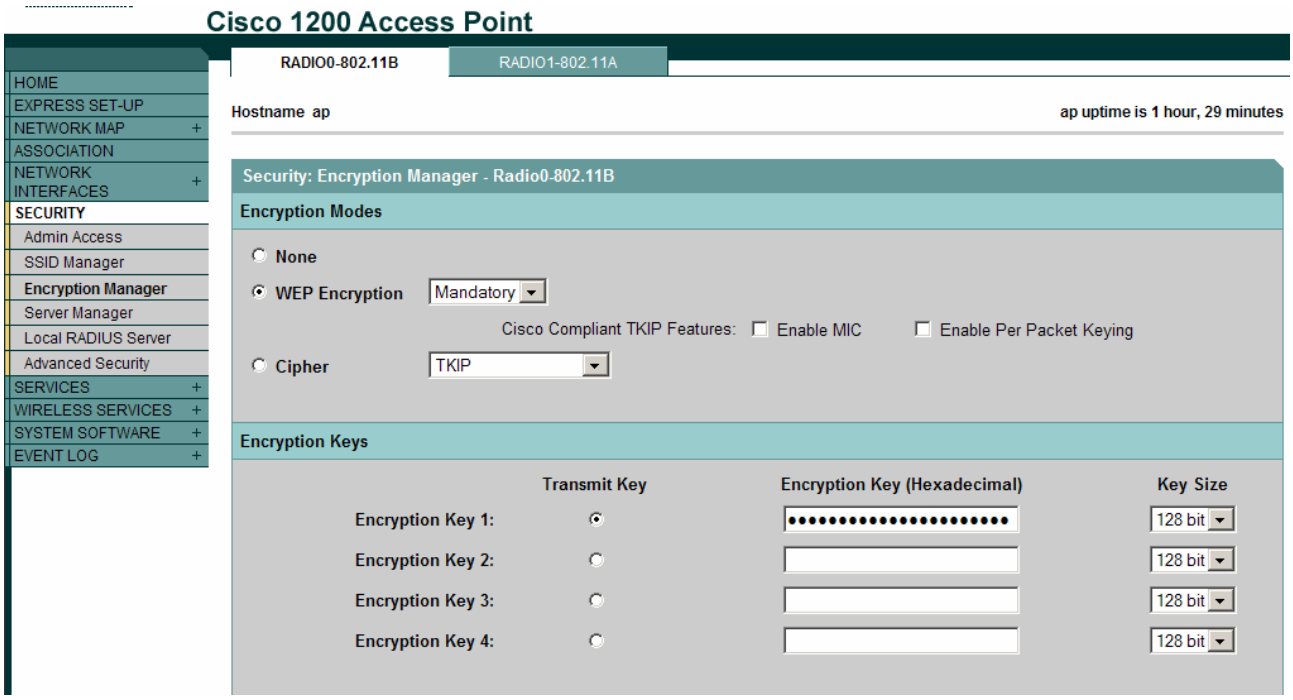
Step 2 Check the basic settings



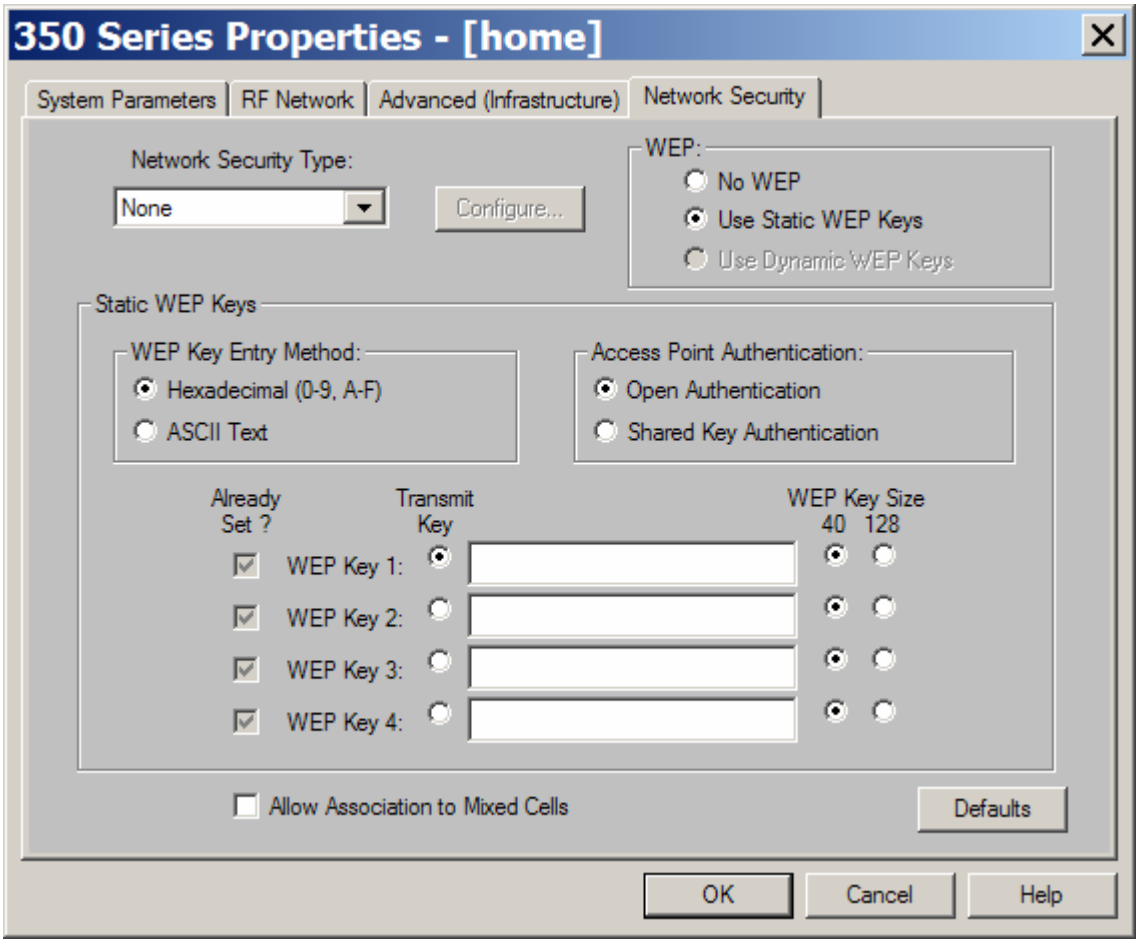
a. Check the Service Set Identifier (SSID) of the AP and client. Mismatched basic settings are the most common causes of lost connectivity with wireless clients. Wireless clients attempting to associate with the AP must use the same SSID as the AP.

b. Verify authentication is set to **Open** on the AP and client. Shared Key exposes the Wired Equivalent Protocol (WEP) key unnecessarily due to weaknesses in design.

Step 3 Check the WEP key



a. The WEP key used to transmit data must be set up exactly the same on the AP and any wireless devices with which it associates. Make sure to enter the key in hexadecimal on the client and AP.



b. If there is a possibility that the AP WEP Key and the Client Adapter WEP Key are not congruent to each other, reset the WEP setting to the default configuration or overwrite the current WEP Key.

c. If the password that allows the AP to be configured is unknown, or if major changes to the configuration need to be made, the configuration may need to be completely reset.

Lab 11.2.6 Troubleshooting TCP/IP Issues

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, standard TCP/IP commands are utilized to troubleshoot connectivity problems between the wireless client and the AP.

Scenario

Basic troubleshooting for TCP/IP on Windows machines combines facts gathered from the perspective of all of the following:

- The router
- The switch
- The bridge
- The AP
- The Windows client or server

Check to see if it is possible to connect using IP addresses. Use an IP address as a target for the standard TCP/IP commands such as **`ping`**, **`tracert`**, and **`telnet`**. Basic IP setup can be verified with the **`winipcfg`** utility for Windows 95 and 98 and the **`ipconfig`** utility for Windows NT, 2000, and XP.

Preparation

The student should read and understand the material presented in FWL Chapter 11 prior to the lab.

Tools and resources

The following tools and resources will help with this lab:

- AP configured on a wired network
- PC with wireless client adapter and utility properly installed
- A NeoTrace Express freeware program can be downloaded at the following URL:

  http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm

Additional materials

Microsoft

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/tcpip_utils.asp

Step 1 Ping

The ping command can be used to confirm basic network connectivity on IP networks. For IP, the ping command sends Internet Control Message Protocol (ICMP) Echo messages. ICMP is the Internet protocol that reports errors and provides information relevant to IP packet addressing. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source.

It is a good idea to use the ping command when the network is functioning properly to see how the command works under normal conditions and to have something to compare against when troubleshooting.

a. From the PC, ping the AP and examine the results.

```
C:\>ping 172.25.0.149

Pinging 172.25.0.149 with 32 bytes of data:

Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249
Reply from 172.25.0.149: bytes=32 time<10ms TTL=249

Ping statistics for 172.25.0.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
C:\>
```

Step 2 Tracert

The **tracert** tool on a Windows host reports each router a TCP/IP packet crosses on its way to a destination. It does essentially the same thing as the **trace** command in the Cisco IOS Software. The syntax for the **tracert** command is as follows:

- **tracert [-d [-h maximum_hops] [-j host-list] [-w timeout] target_name.**
- The following is an explanation of the parameters of the command:
- **d** – specifies to not resolve addresses to host names (use recommended in test networks to avoid DNS delays)
- **h maximum_hops** - specifies the maximum number of hops to search for target
- **j host-list** – specifies loose source route along the host list
- **w timeout** – waits the number of milliseconds specified by timeout for each reply
- **target_name** – name or IP address of the target host
- Errors that may occur include the asterisk (*) and the 'request timed out' message. These messages indicate a problem with the router or a problem elsewhere on the network. The error may relate to a forwarded packet or one that timed out.
- Another common error is a report of 'destination network unreachable'. This error usually indicates that network filtering is happening, likely from a firewall. It may also indicate a routing problem, such as a failed network link.

  a. From the PC, perform a `tracert` to http://www.cisco.com

  ```
  C:\>tracert www.cisco.com
  ```



```
Tracing route to www.cisco.com [198.133.219.25] over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  sjc8-00-gw1.cisco.com [171.71.88.2]
  2   <10 ms   <10 ms   <10 ms  sjc2-dtb-gw1.cisco.com [171.71.240.105]
  3   <10 ms   <10 ms   <10 ms  sjc5-sbb4-gw1.cisco.com [171.71.241.153]
  4   <10 ms   <10 ms   <10 ms  sjc12-rbb-gw4.cisco.com [171.71.241.254]
  5   <10 ms   <10 ms   <10 ms  sjck-rbb-gw2.cisco.com [171.69.7.229]
  6   <10 ms   <10 ms   <10 ms  sj-wall-1.cisco.com [171.69.7.182]
  7   <10 ms   <10 ms   <10 ms  sjce-dirty-gw1.cisco.com [128.107.240.197]
  8   <10 ms   <10 ms   <10 ms  sjck-sdf-ciod-gw2.cisco.com [128.107.239.102]
  9   <10 ms   <10 ms   <10 ms  www.cisco.com [198.133.219.25]
Trace complete.
```

Step 3 Ipconfig

The command syntax for **ipconfig** and **winipcfg** is as follows:

- **ipconfig** [**/all** | **/renew** [*adapter*] | **/release** [*adapter*]]
- The following are the parameters of the command:
- **All-** Produces a full display. Without this switch, **ipconfig** displays only the IP address, subnet mask, and default gateway values for each network card.
- **/renew** [*adapter*]– Renews DHCP configuration parameters. This option is available only on systems running the DHCP Client service. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
- **/release** [*adapter*]- Releases the current dynamic host configuration protocol (DHCP) configuration. This option disables TCP/IP on the local system and is available only on DHCP clients.
- With no parameters, the **ipconfig** utility presents all of the current TCP/IP configuration values to the user, including IP address and subnet mask.
- To check the local host configuration, enter a DOS window on the host and enter the **ipconfig /all** command. This command shows your TCP/IP address configuration, including the address of the Domain Name System (DNS) server. If any of the IP addresses are incorrect or if no IP address is displayed, determine the correct IP address and edit it or enter it for the local host.

  a. Complete the information table below:

IPCONFIG COMMAND	INFORMATION
Host Name	
Primary DNS Suffix	
Node Type	
IP Routing Enabled	
WINS Proxy Enabled	
DNS Suffix Search List	
Connection-specific DNS Suffix	
Description	
Physical Address	
DHCP Enabled	
Autoconfiguration Enabled	
IP Address	
Subnet Mask	

Default Gateway	
DHCP Server	
DNS Servers	
Primary WINS Server	
Secondary WINS Server	
Lease Obtained	
Lease Expires	

Step 4 Telnet

a. Telnet from the host PC to the AP to test layer 7 connectivity:

```
C:\>telnet 10.0.P.1
User Access Verification
Username:
Password:
AP1200#
```

b. Was the Telnet successful?

_____

c. Which command will be used for testing in the following situations?

Situation	Command
Host cannot access other hosts through AP or bridge.	
Host cannot access certain networks by the way of AP or bridge.	
Users can access some hosts, but not others.	
Some services are available and others are not.	
Users cannot make any connections when one parallel path is down.	
Certain protocols are blocked and others are not.	

Step 5 Freeware Software utilities for telnet, trace and ping

There are freeware utilities available for download over the Internet that allow telnet, trace and ping in a Graphical User Interface (GUI) environment. One such program is NeoTrace Express. It can be downloaded at the following URL site:

http://www.networkingfiles.com/PingFinger/Neotraceexpress.htm

Other programs are:

A great free utility for the PocketPC is vxUtil. The utilities include:

- DNS Audit
- DNS Lookup
- Finger
- Get HTML
- Info
- IP Subnet Calculator
- Password Generator
- Ping
- Ping Sweep
- Port Scanner
- Quote
- Time Service
- Trace Route
- Whois

http://www.cam.com/vxutil.html

a. Perform an Internet search to find two other TCP/IP utlities? Record them below. Share with the class.

_____

Lab 11.5.6.1 Configure Syslog on AP

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will configure and use syslog logging to monitor network events.

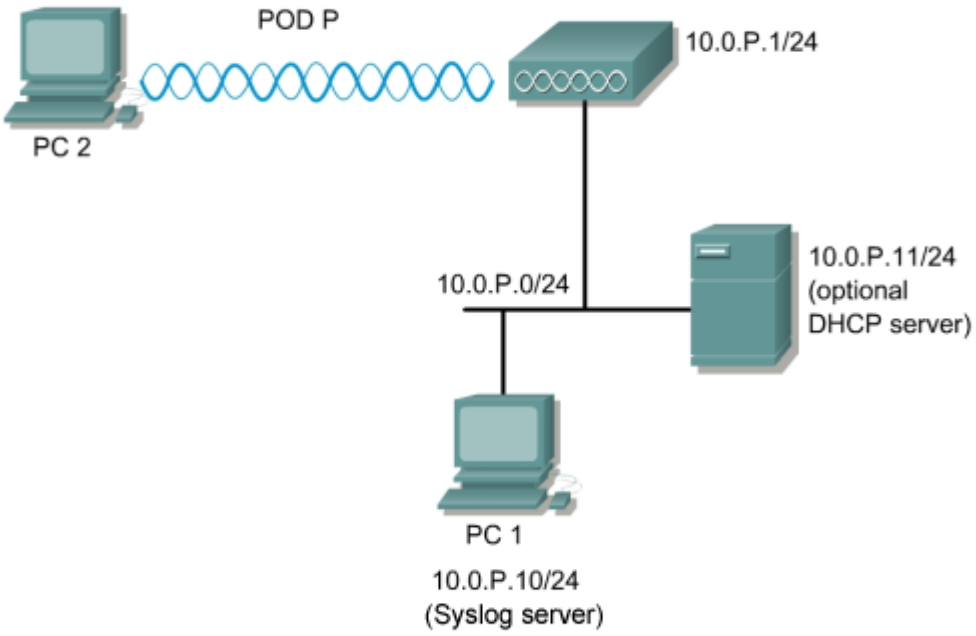
Scenario

A network security administrator should always log significant events on the AP to the syslog server. A syslog server should be located on a secure internal network to ensure log integrity. The syslog server can be a dedicated server or another server running syslog services.

A Syslog Server is a basic application that allows Aironet AP and bridge event information to be viewed from a Windows system. It includes all the following features:

- Receiving syslog messages through either TCP or UDP
- Full reliability because messages can be sent through TCP
- Ability to receive syslog messages from devices

Topology



Preparation

The student will read and understand material presented in FWL Chapter 11 prior to this lab.

There are numerous syslog servers available on the Internet. This lab assumes that Kiwi Syslog Daemon is used. This is a freeware utility that can be downloaded at http://www.kiwisyslog.com. Download the syslog server and install the executable file.

Tools and resources

The following tools and resources will be helpful with this lab:

- A properly setup wired LAN
- A properly setup and installed AP
- A PC acting as the syslog server with a static IP address
- A PC with a properly installed wireless client adapter and utility

Additional materials

Further information about the objectives covered in this lab can be found at the following website: http://www.kiwisyslog.com

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

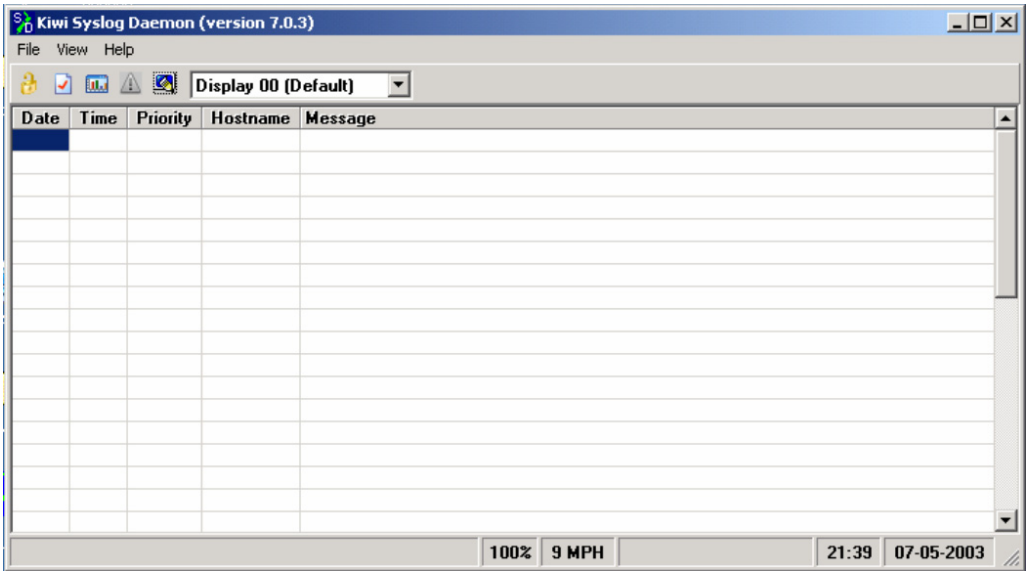
Command	Description
configure terminal	Enter global configuration mode
logging on	Enables Message Logging
logging host	Log Messages to a syslog server host
show logging	Verify the log settings and entries entries.
show running-config	Verify the active configuration in DRAM.
copy running-config startup-config	Save the active configuration into Flash
service timestamps log uptime	Enable log timestamps.
service sequence-numbers	Enable sequence numbers.

Step 1 Download and install the Kiwi Syslog software

a. Go to the http://www.kiwisyslog.com/software_downloads.htm site and download the free edition of the kiwi syslog software.

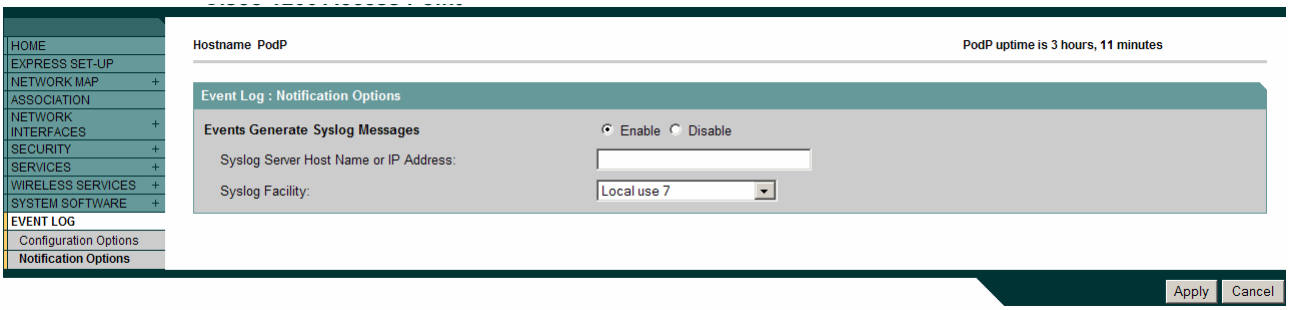
b. Install the executable file.

Step 2 Setup the Kiwi Syslog Daemon



a. Click on the **Kiwi Syslog Daemon** Icon on the desktop to bring up the syslog screen.

Step 3 Enable logging on the AP



a. Open up the AP browser menu and go to the **EVENT LOG>Notification Options** Page.

b. Enable the **Event Generate Syslog Messages** utility on the AP

c. Type in the Syslog Server Host IP address. This should be 10.0.P.10

d. Set the Syslog Facility logging level. The default, Local7, can be used.

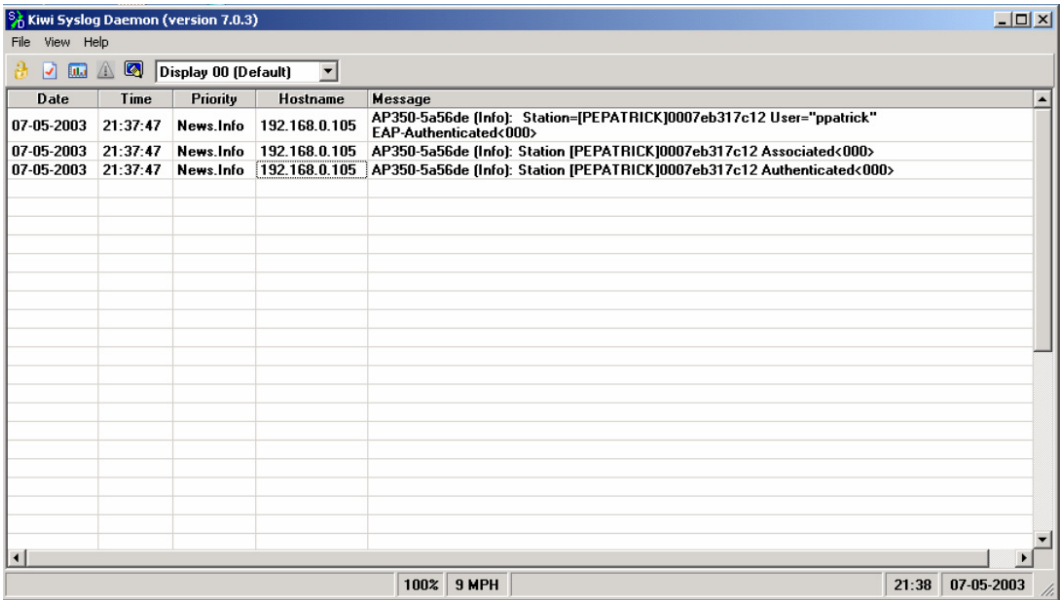
e. What other selections are available?

_____

_____

f. Click the apply button to begin logging events to the Kiwi Syslog.

Step 4 View the Kiwi Syslog event log



a. Generate events to the syslog by logging into the AP that is being monitored.

b. Have the wireless users log onto the AP.

c. Have the wireless users log off the AP.

d. These changes will trigger a logged event on the syslog. What is the message that was displayed on the syslog?

_____

_____

Step 5 Enabling logging on the AP

a. Erase the configuration and reload the AP.

b. Configure the AP according to the Topology.

c. Enabled on an AP using the Cisco IOS with the following commands:

```
PodP(config)#logging on
```

d. To send the logging messages to a syslog server which is located on PC1, use the following command:

```
PodP(config)#logging host 10.0.P.10 (where P is the Pod number)
```

e. View the available messaging levels for syslog :

```
PodP(config)#logging trap ?

  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
```



```
debugging      Debugging messages                (severity=7)
emergencies    System is unusable                (severity=0)
errors         Error conditions                  (severity=3)
informational  Informational messages            (severity=6)
notifications  Normal but significant conditions (severity=5)
warnings       Warning conditions                (severity=4)
<cr>
```

f. Configure the syslog message level to debugging.

```
PodP(config)#logging trap debugging  (or 7)
```

g. Enable the service timestamps on the AP using the following command:

```
PodP(config)#service timestamps log uptime
```

h. Enable the service sequence numbers on the AP logging using the following command:

```
PodP(config)#service sequence-numbers
```

Step 6 Verify the configuration

a. Verify the configuration on the AP.

```
PodP#show running-config
Building configuration...

Current configuration : 2552 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
service sequence-numbers
!
hostname PodP
!
logging trap debugging
logging 10.0.1.10
!
[output omitted]
```


b. Use the show logging command to view the entries.

```
PodP#show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns)
    Console logging: level debugging, 312 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 314 messages logged
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 316 message lines logged
Log Buffer (4096 bytes):
*Mar  4 04:44:28.924: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticatin
 Station 0007.8592.e4ea Reason: Previous authentication no longer valid
*Mar  4 04:47:55.076: %DOT11-6-ASSOC: Interface Dot11Radio0, Station csawyer 00
9.b74c.b479 Associated KEY_MGMT[NONE]
*Mar  4 04:51:36.967: %DOT11-4-MAXRETRIES: Packet to client 0009.b74c.b479 reac
ed max retries, remove the client
*Mar  4 04:51:36.968: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticatin
 Station 0009.b74c.b479 Reason: Previous authentication no longer valid
*Mar  4 05:36:44.416: %DOT11-6-ASSOC: Interface Dot11Radio0, Station KDEVIAEN-W
K02 00d0.59c8.ca3f Reassociated KEY_MGMT[NONE]
 --More--
[output omitted]
```

c. To clear the log, use the following command:

```
PodP#clear logging
Clear logging buffer [confirm]
PodP#
```

d. Issue the show log command again to view the clear log:

```
PodP#show log
    Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
     0 overruns)
        Console logging: level debugging, 312 messages logged
        Monitor logging: level debugging, 0 messages logged
        Buffer logging: level debugging, 314 messages logged
        Logging Exception size (4096 bytes)
        Count and timestamp logging messages: disabled
        Trap logging: level informational, 316 message lines logged

    Log Buffer (4096 bytes):
    PodP#
```


Step 7 View the Kiwi Syslog event log

a. Generate events to the syslog by establishing a wireless connection to the AP. Next, use Telnet or SSH to log into the AP.

b. The login will trigger logged events on the syslog server located on PC1.

c. What is the message that was displayed on the syslog?

_____

_____

Lab 11.5.6.2 Configure SNMP on AP

Estimated Time: 20 minutes

Number of Team Members: Students will work in teams of two.

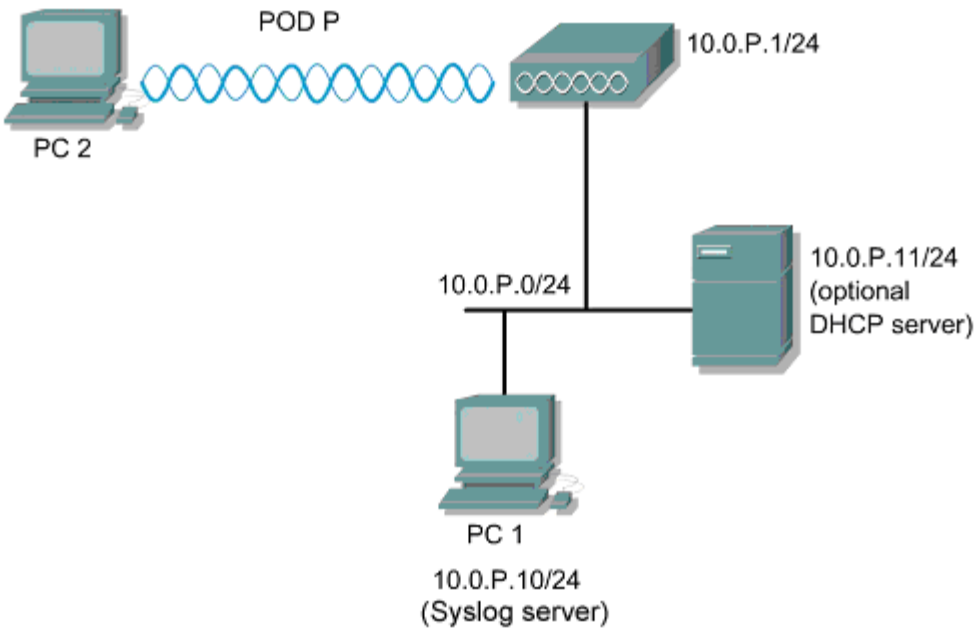
Objective

In this lab, the student will install and configure the Kiwi Syslog Daemon to listen for SNMP logs. The student will configure the contact and location of the SNMP agent and test the configuration.

Scenario

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP uses User Datagram Protocol (UDP) port 161 for most requests and responses. SNMP traps use UDP port 162.

Topology



Preparation

Team	AP Name	SSID	Address
1	Pod1	AP1	10.0.1.1/24
2	Pod2	AP2	10.0.2.1/24

Tools and resources

The following tools and resources are required:

- One AP 1200
- A wired PC (PC1) acting as the SNMP server.
- A wireless PC or laptop with ACU

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise:

Command	Description
no snmp-server	Disable SNMP.
show snmp	Monitors SNMP status.
snmp-server community	Defines the community access string.
snmp-server contact	Sets the system contact string.
snmp-server enable traps snmp	Enables the sending of traps, and specifies the type of notification to be sent.
snmp-server host	Configures the recipient of an SNMP trap operation.
snmp-server location	Sets the system location string.

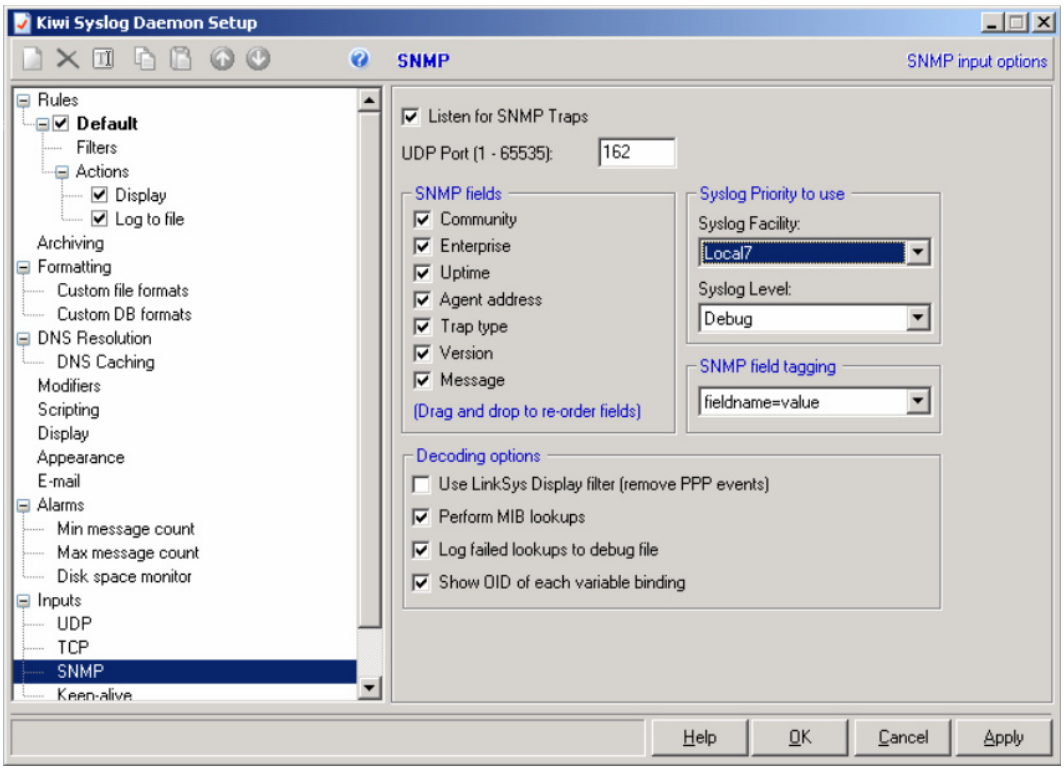
Step 1 Download and install the software

Go to the following web sites and download Kiwi Syslog Daemon Standard version software

http://www.kiwisyslog.com/software_downloads.htm

Install the program on PC1.

Step 2 Setup and execute the Kiwi Syslog Daemon



a. Click on the **Setup** icon located in the upper left corner of the syslog program window.

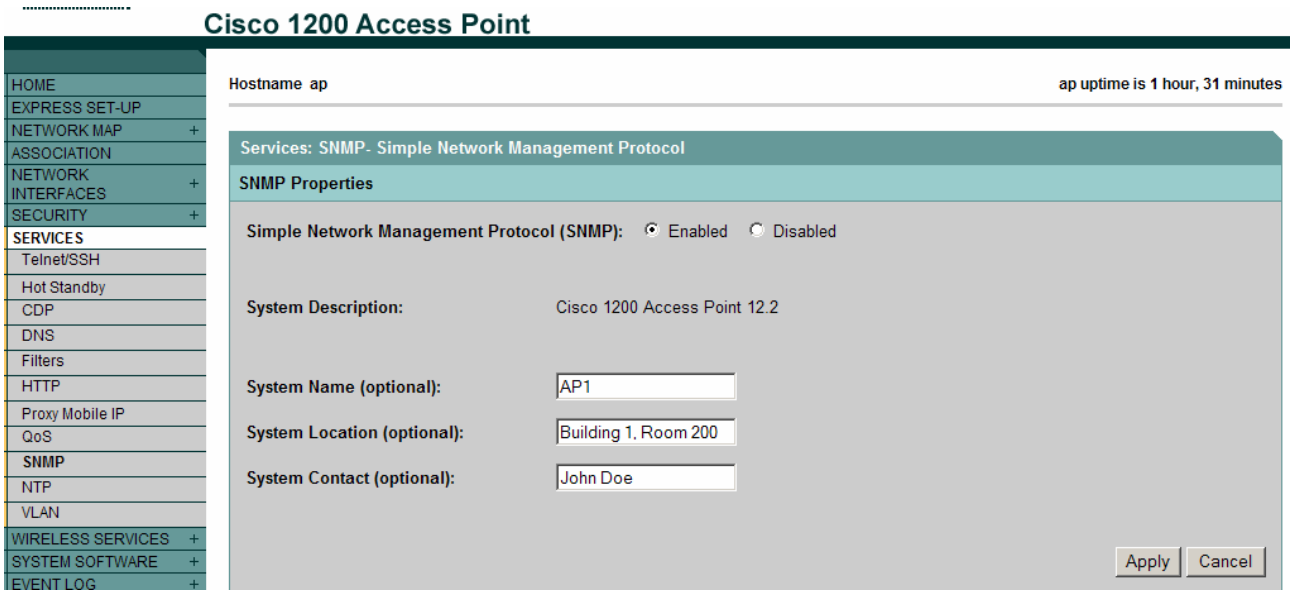
b. Configure SNMP on Kiwi Syslog Daemon by checking the **Listen for SNMP Traps** box.

c. Click the **OK** button to save the changes.

d. What UDP port does SNMP Trap Watcher listen on?

_____

Step 3 Use the web browser to setup SNMP



a. Ensure the AP is configured according to the Topology and Preparation table. Ping from PC1, located at 10.0.P.10 to the AP to ensure connectivity.

b. Browse to the **SERVICES>SNMP** Page of the AP.

c. Click the Enabled radio button to Enable SNMP on the AP.

d. Set a System Name (this is optional, but useful)

e. Set a System Location (this is optional, but useful)

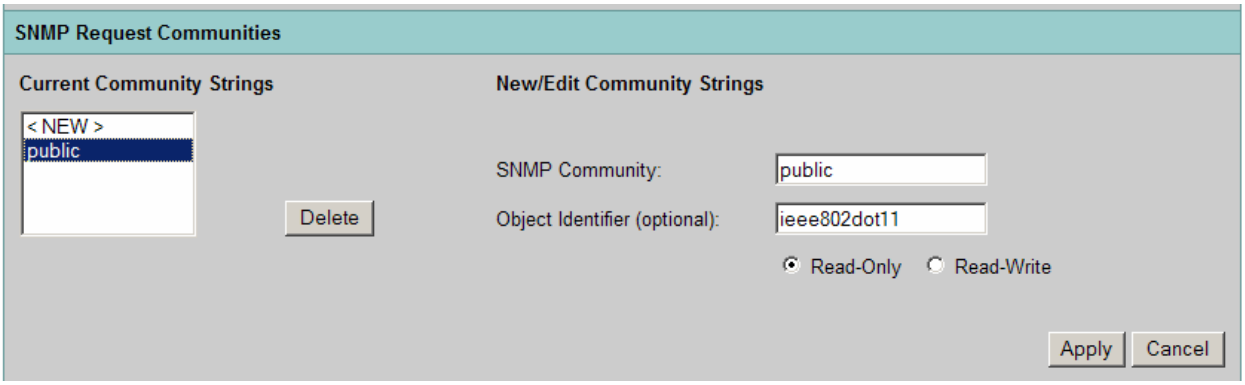
f. Set a System Contact (this is optional, but useful)

g. Complete the following information for your AP in the table below:

System Name	
System Location	
System Contact	

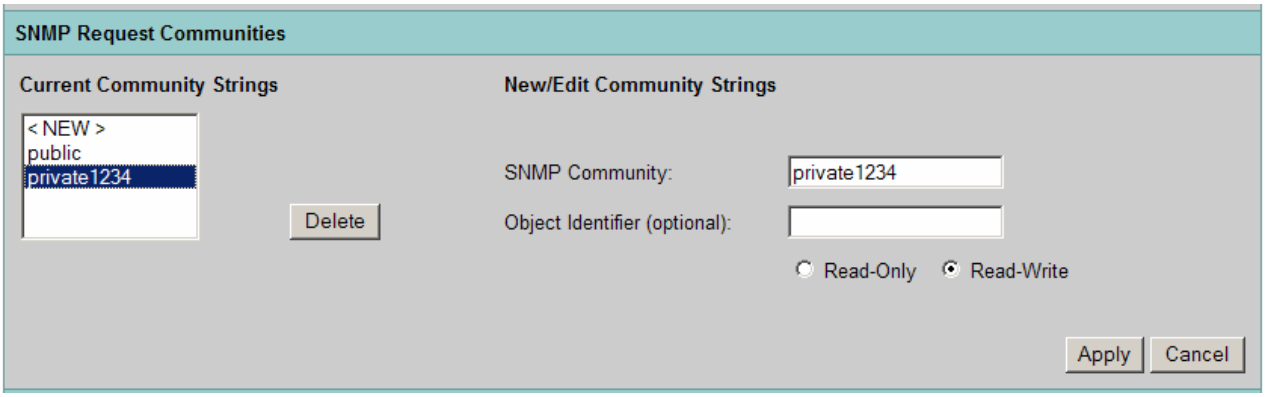
h. Click on the **Apply** buttion.

Step 4 Public community string



Create a public community string with Read Only. In a production environment, it is important to configure a unique string for increase security. SNMP read only provides monitoring through an SNMP management application.

Step 5 Private community string



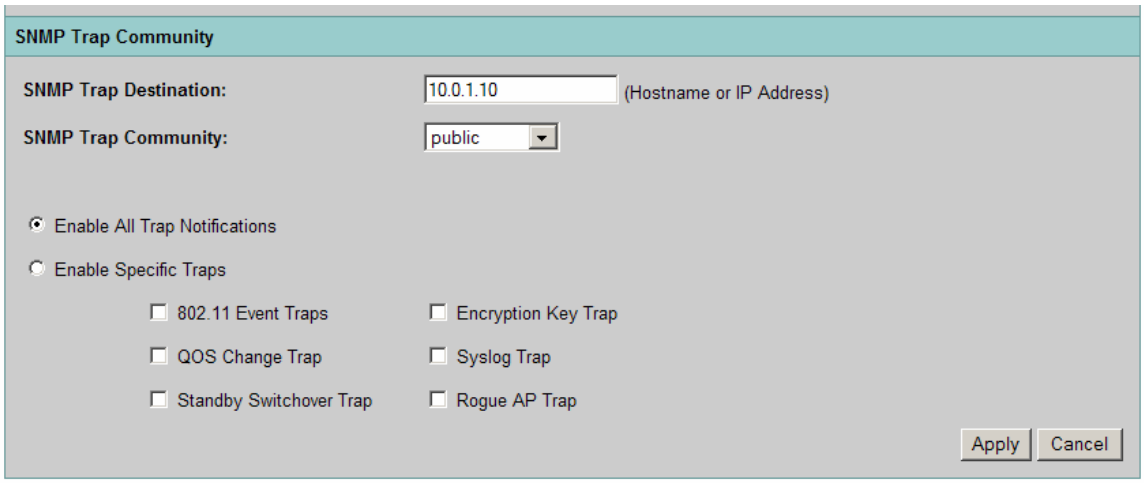
SNMP read-write access monitoring and management using SNMP management applications.

a. Click on the <NEW> in the Current Community String

b. Create a private1234 community string with Read_Write

c. Click the **Apply** button to create the string.

Step 6 SNMP trap destinations



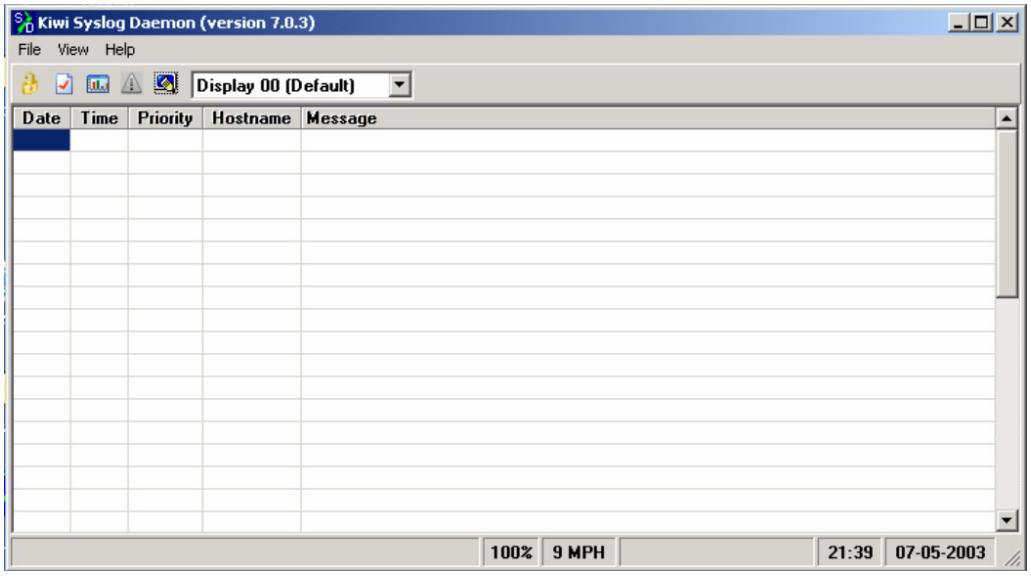
a. Set a SNMP Trap Destination by entering the IP address of PC1 located at 10.0.P.10.

b. Set the SNMP Trap Community to public.

c. Enable All Trap Notifications.

d. Click the **Apply** button.

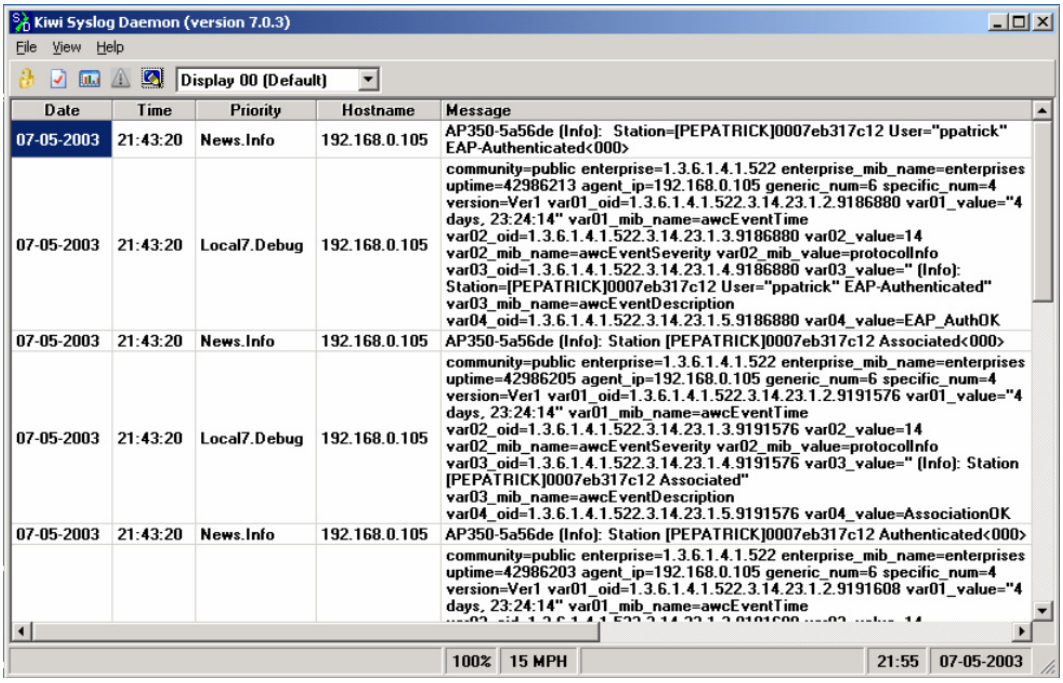
Step 7 Test the configuration



a. Click on the **Kiwi Syslog Daemon** Icon on the desktop to bring up the syslog application. The Kiwi Syslog Daemon can be customized or the defaults can be used.

b. Have a wireless user connect to the bridge.

c. Have the wireless user disconnect from the bridge.



d. View the main logging screen on Kiwi.

Step 8 Set the system contact, and location of the SNMP agent through IOS CLI

Before beginning this step, reset the AP back to factory configuration. Configure the AP according to the Topology and Preparation table.

a. Now configure the system contact and location:

```
PodP(config)#snmp-server contact [name] [phone]
PodP(config)#snmp-server location [location]
```

b. What command would be used to verify this information on an AP?

_____

Step 9 Enable SNMP traps

a. Enable all the SNMP trap types at once,

```
PodP(config)#snmp-server enable traps snmp
```

b. Specify to the SNMP destination host the trap notifications will be sent to.

```
PodP(config)#snmp-server host 10.0.P.10 private udp-port 162
```

c. If the default for an SNMP response is on port 162, what port is the request sent on?

_____

Step 10 Test the configuration

a. Exit out of the AP and log back in using the wrong password. After the failed attempts log back into the AP. There will now be entries of traps sent from the AP to the SNMP server. Check the SNMP application on PC1.

Besides **`startup-config`** and **`running-config`**, where would information on the contact, location, and SNMP logging information for SNMP on the router be?

_____

Step 11 Disable the SNMP traps on the AP by using the following commands

```
PodP(config)#no snmp-server enable traps
PodP(config)#no snmp-server system-shutdown
PodP(config)#no snmp-server trap-auth
```

Note	By disabling SNMP trap notifications, which are not needed, the amount of free bandwidth can be increased and unnecessary SNMP processing tasks can be eliminated.

Lab 11.5.6.3 Configure Syslog and SNMP on the Bridge

Estimated Time: 25 minutes

Number of Team Members: Students will work in teams of two.

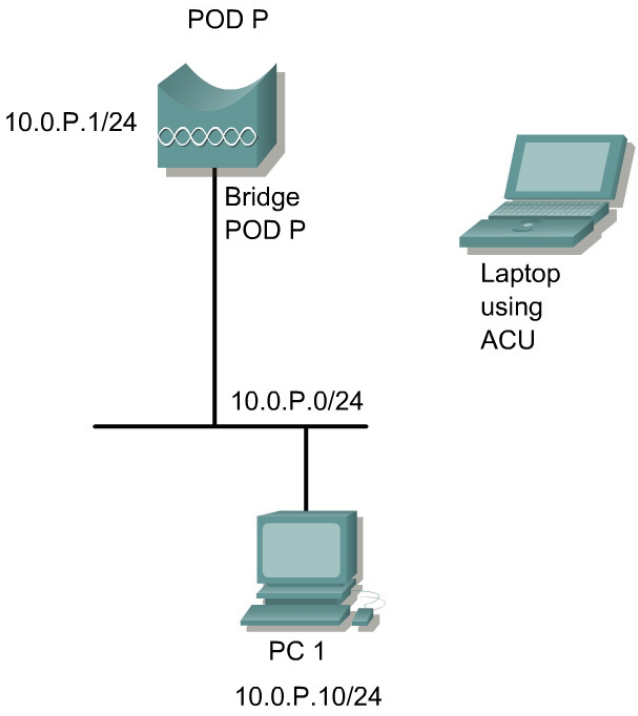
Objective

In this lab, students will configure and use syslog logging to monitor network events. Also, the student will configure the contact and location of the SNMP agent and test the configuration.

Scenario

A network security administrator should always log significant events on the bridge to the syslog or SNMP server. A server should be located on a secure internal network to ensure log integrity. The server can be a dedicated server or another server running syslog services or SNMP

Topology



Preparation

The student will read and understand material presented in FWL Chapter 11 prior to this lab.

Tools and resources

The following tools and resources are required:

- One BR350
- A wired PC (PC1) acting as the syslog and syslog server with a static IP address
- A PC or laptop with a properly installed wireless client adapter and utility

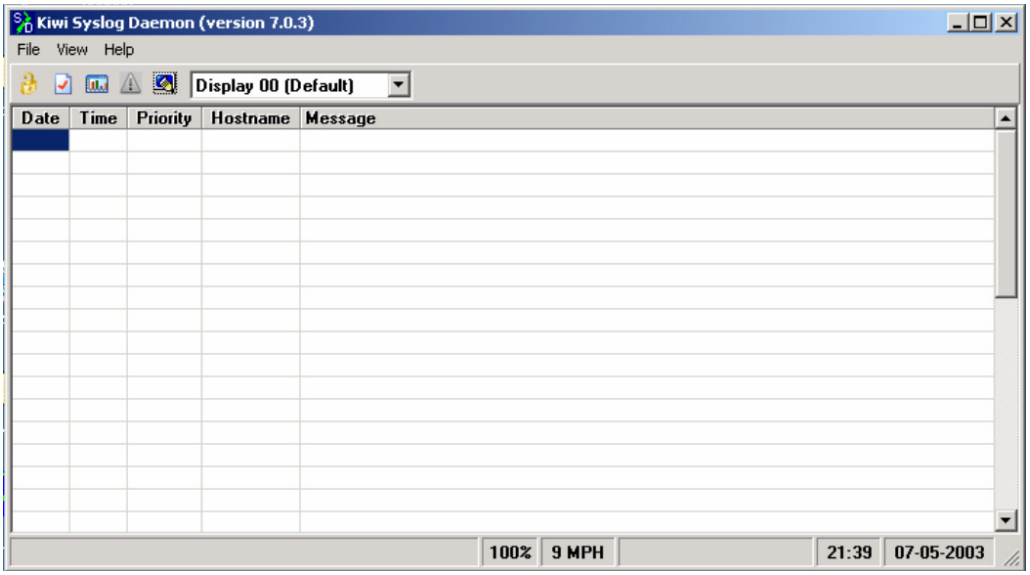
Step 1 Download and install the software

Go to the following web sites and download Kiwi Syslog Daemon Standard version software

http://www.kiwisyslog.com/software_downloads.htm

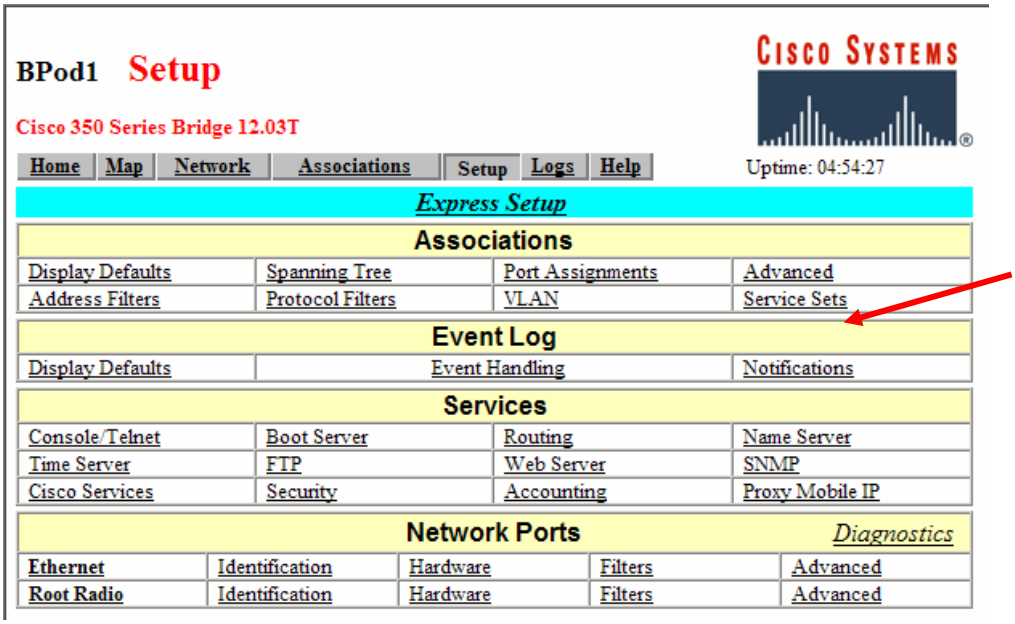
Install the program on PC1.

Step 2 Setup and execute the Kiwi Syslog Daemon

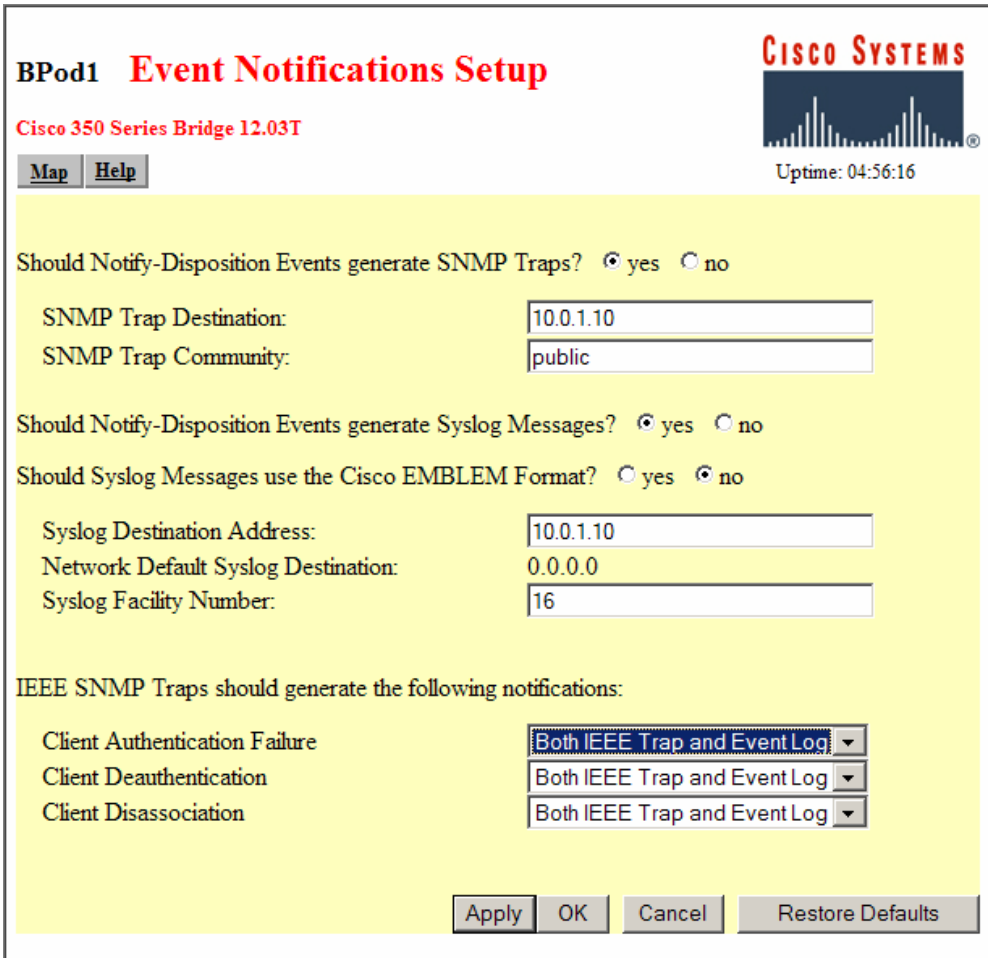


a. Click on the **Kiwi Syslog Daemon** Icon on the desktop to bring up the syslog application. The Kiwi Syslog Daemon can be customized or the defaults can be used.

Step 3 Enable logging on the bridge

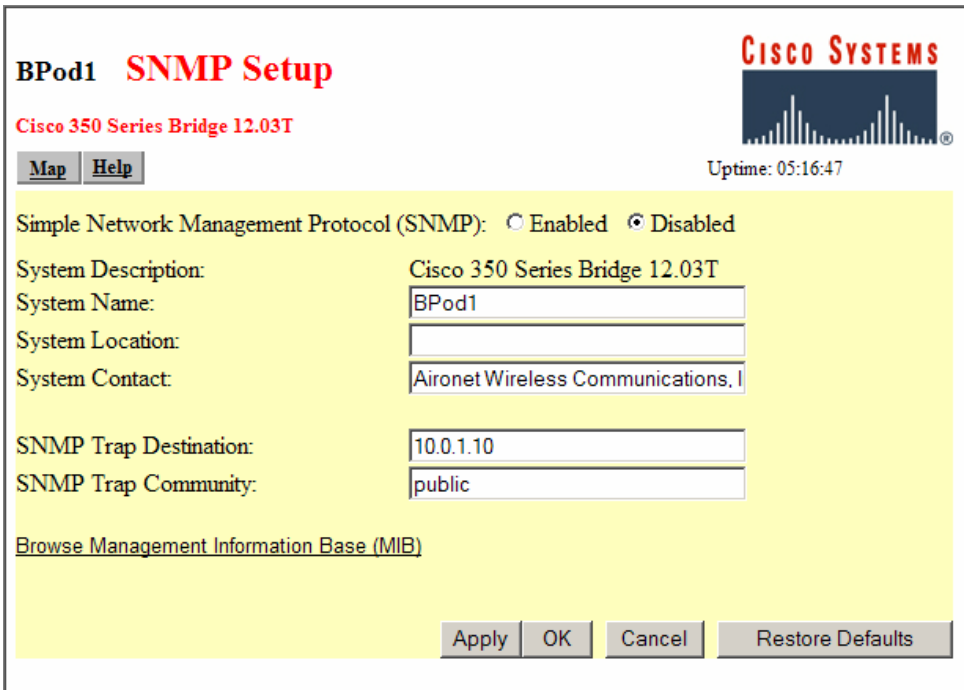


a. From the Setup Page, click on the **Event Log** Notifications link.



b. Type in the Syslog and SNMP Destination Host IP address. This should be 10.0.P.10

c. Click the **Apply** button to begin logging events to the Kiwi Syslog.



d. From the Setup Page, click on the **Services** SNMP link.

e. Click on the **Enabled** radio button to enable SNMP.

f. Configure a System location and contact.

g. Click the **Apply** button to begin logging events to the SNMP Trap Watcher.

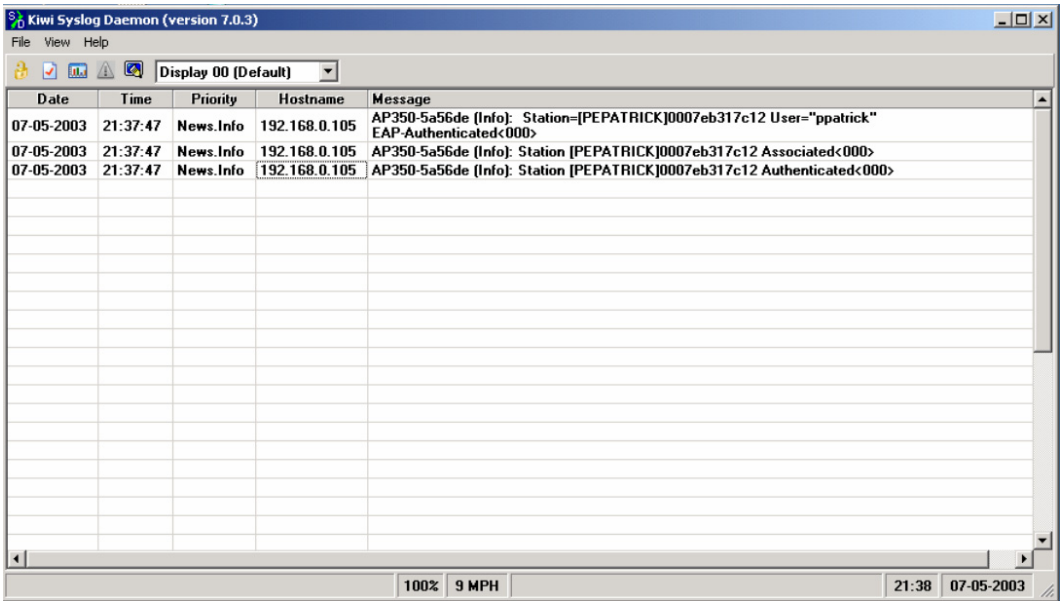
Step 4 View event logs

Configuring logging is only half of the logging scenario. A security administrator must monitor the logs on a daily basis.

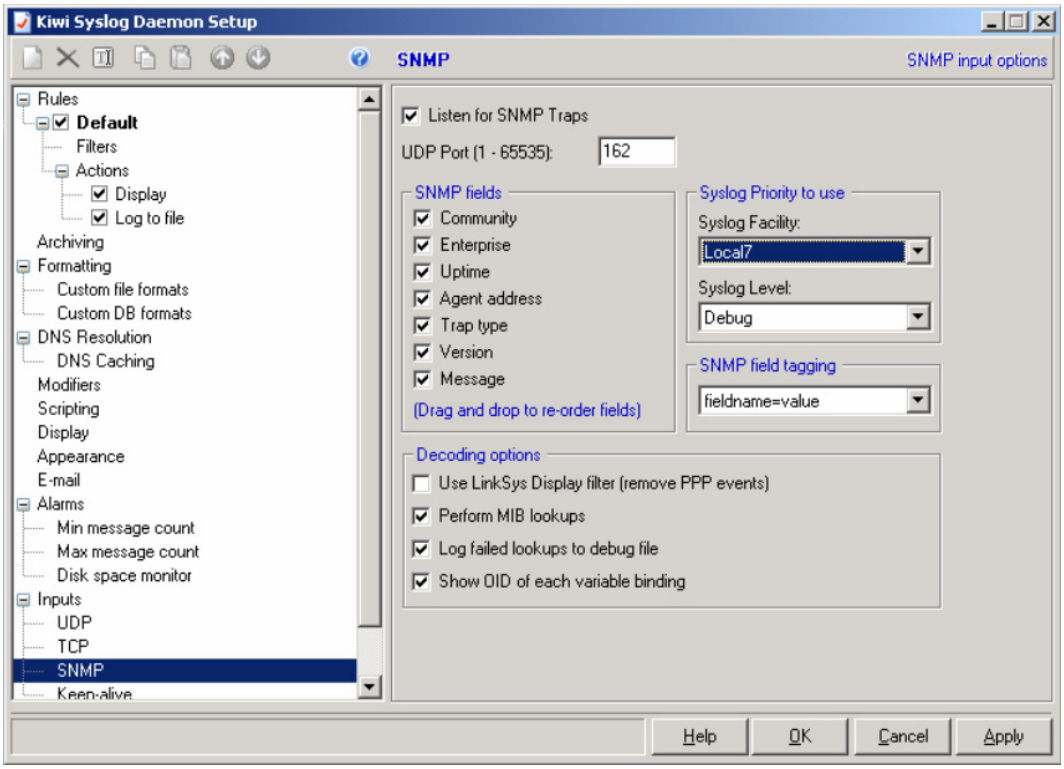
Generate events to the syslog by logging into the bridge that is being monitored.

a. Have a wireless user connect to the bridge.

b. Have the wireless user disconnect from the bridge.



c. View the messages in the Kiwi syslog window. The Hostname should match the IP address of the bridge.



d. Click on the **Setup** icon located in the upper left corner of the syslog program window.

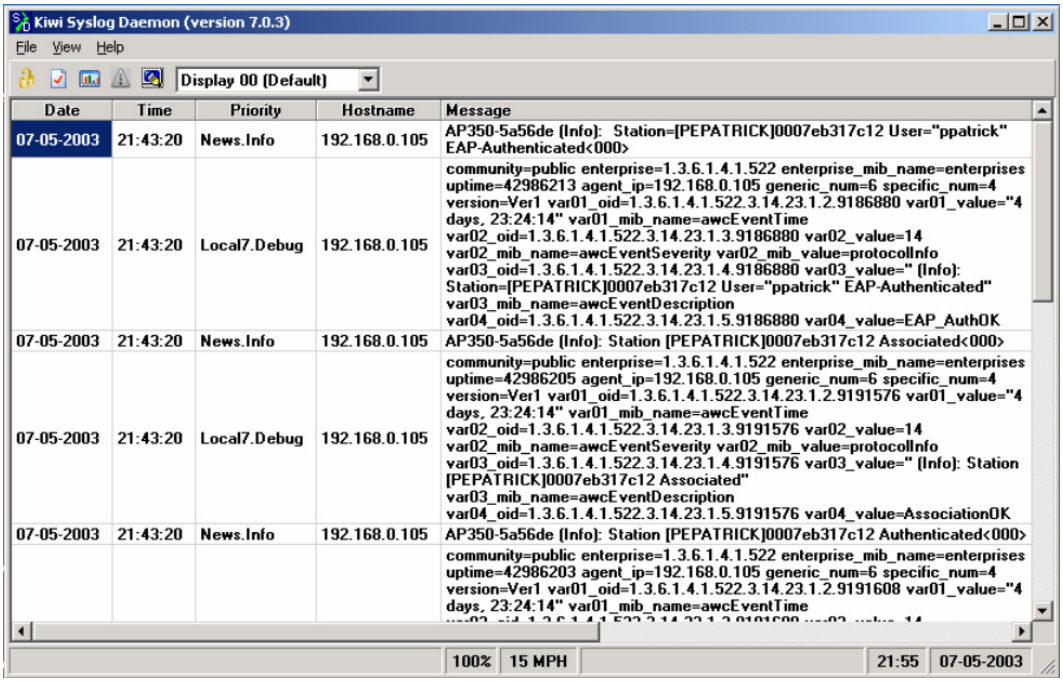
e. Configure SNMP on Kiwi Syslog Daemon by checking the **Listen for SNMP Traps** box.

f. Click the OK button to save the changes.

g. Have a wireless user connect to the bridge.

h. Have the wireless user disconnect from the bridge.

i. View the main logging screen on Kiwi.



j. Notice the SNMP messages contain much more information than the syslog messages. The Hostname should match the IP address of the bridge.

k. When using the Cisco WLAN Solutions engine or other enterprise level SNMP applications, SNMP can be used for monitoring and management.

Lab 12.4.8.1 Wireless Case Study of a School

Estimated Time: Actual time of completion will vary.

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will determine the feasibility of deploying a WLAN at a local school in their area.

Scenario

Connectivity to IT tools is often restricted to IT classrooms or computer labs. However, with the emergence of on-line curriculum and multimedia learning materials, the demand for student access from any part of the campus is growing. Productivity for professors, lecturers, and teachers is no different. A wireless network can enable teachers and students to gain access to information, productivity tools, and applications regardless of their environment or smart devices like laptops, PDA's, BlackBerries, and phones.

Step 1 Arrange the visit

Locate a school in the area and make arrangements for a site visit. Then schedule an interview with the person responsible for the school or district computer network.

1. Name of the school:

   _____

2. Person Contacted:

   _____

Step 2 Document the existing network

a. Summarize the existing computer network available for student access at this school. A good place to start may be the access available in the library.

_____

_____

_____

_____

_____

_____

_____

Step 3 List the educational initiatives relating to WLANs

a. List any planned future enhancements to this network:

_____

_____

_____

_____

_____

b. How much of the future enhancements involve additional cabling? Are classrooms cabled for network access? Is there an outdoor study area that student's use that could benefit from a wireless hotspot?

_____

_____

_____

_____

_____

Step 4 Determine the user needs

a. Determine how many additional users are expected to utilize the wired network.

This will help determine the amount of APs that will be needed to service the users. For example, using the 2.4 GHz range, estimate one AP per 10-15 users and three APs per cell area for normal bandwidth users. This allows approximately 30 to 45 students per cell coverage. In the 5 GHz range, four APs can be colocated in one area and possibly up to 12, but heavy bandwidth users should stay with a wired network.

_____

_____

_____

_____

_____

_____

Step 5 Prepare and estimate

a. Prepare a rough estimate of the project cost. Include labor, equipment, and supplies. Create a separate spreadsheet of WLAN devices and accessories to be ordered.

_____

_____

_____

_____

Step 6 Develop a proposed WLAN solution for this school

The following information should be included in the WLAN solution for the school:

- Frequency range spectrum chosen and the reason
- Total number of APs
- Type of antenna
- How to secure access to the WLAN
- Budget
- Installation Schedule
- Total cost for the WLAN deployment
- Pros and cons of the WLAN solution
- Conclusion

Step 7 Present the proposal

Present the proposal to the classroom in a PowerPoint presentation.

Lab 12.4.8.2 Wireless Case Study of an Organization

Estimated Time: Actual time of completion will vary.

Number of Team Members: Students will work in teams of two.

Objective

In this lab, the student will learn about the process of implementing a WLAN in an existing organization.

Scenario

A recent study of WLANs, conducted by NOP World-Technology, studied the perceived benefits of WLANs after implementation. The study found that WLANs increase productivity. End-users stay connected to the network an average of 1.75 hours longer each day, and report average daily time savings of 70 minutes. Overall, WLANs create a productivity increase of 22 percent.

Preparation

The instructor can do some of the preliminary research involved in locating organizations in the area that have implemented or have plans to implement a WLAN.

Step 1

Locate an organization that has implemented a WLAN

1. List the organization name and describe its core service or business:

_____

_____

_____

_____

_____

Step 2

Coordinate an on site interview with the IT manager

a. Who was contacted?

_____

b. What is this person's primary responsibility?

_____

_____

c. Was a site survey performed?

_____

d. What prompted the necessity of the WLAN?

e. Describe the organizations wired network prior to adding a WLAN. For example, what routers, switches, workstations, servers, and applications were used?

f. List the equipment that was added for the WLAN deployment.

g. What methods are used to secure access onto the WLAN?

h. What quantifiable results were achieved?

