



Fundamentals of Wireless LANs

Instructor Lab Manual



Modules



Take the Fundamentals of Wireless LANs Curriculum Tour



Fundamentals of Wireless LANs v1.1

This introductory course focuses on the design, installation, configuration, operation and troubleshooting of 802.11a, 802.11b, and 802.11g Wireless LANs. A comprehensive overview of wireless technologies, devices, security, design, and best practices with a particular emphasis on real world applications and skills is covered.

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the Fundamentals of Network Security course as part of an official Cisco Networking Academy Program.

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:

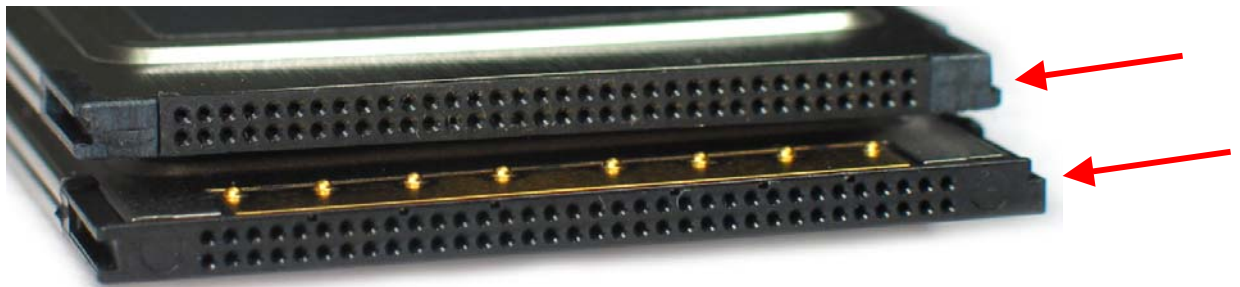
- Desktop or Laptop PC
- One Cisco Aironet PCI352, CB20A, or PCM 352 Client Adapter Network Interface Card.
- One PC installed with a Microsoft Operating System
- One Screwdriver for PCI card installation
- Instructor should preconfigure SSIDs on the APs and determine the IP addresses needed for the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

Answer: PCMCIA, PCM352, 802.11b card

- b. Which card is located on bottom?

Answer: CardBus, CB20A, 802.11a card



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.



- j. For optimal reception, position the antenna so it is straight up.
- k. 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 Install Aironet Client Utility (ACU)

Estimated Time: 30 Minutes

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

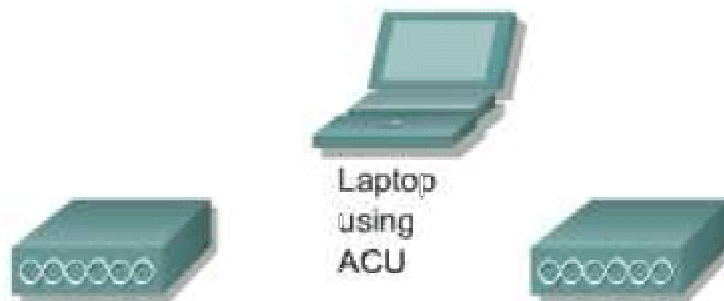
Objective

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

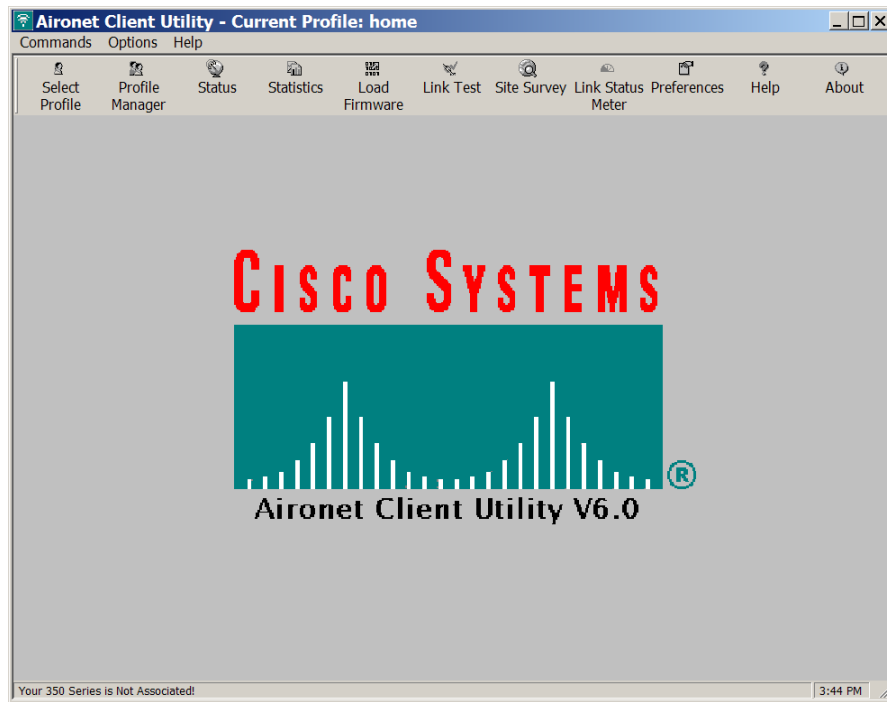
Step 1 Configure XP to use the ACU

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)

- 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.
- 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.
- 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

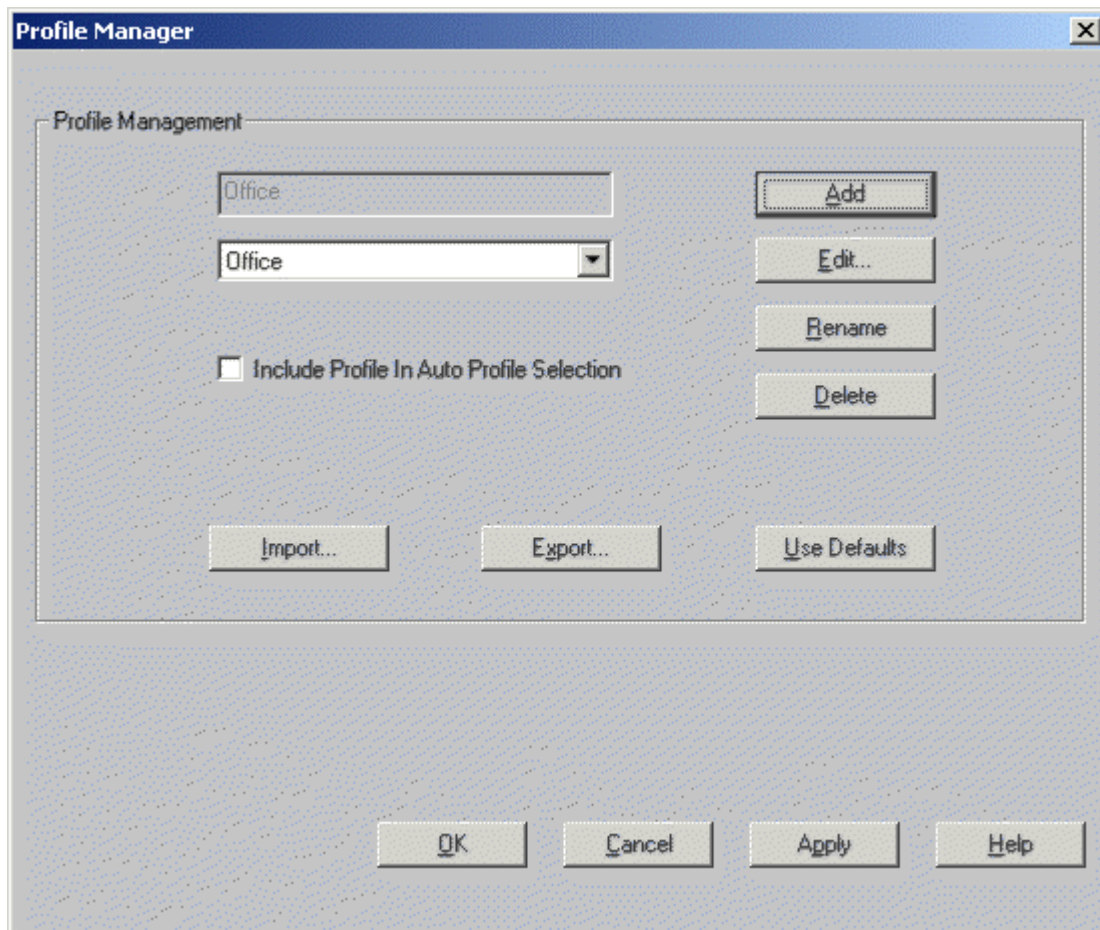
- a. Select **Start > Run** and enter the following:
- b. On Win2000 or XP, enter **cmd** to bring up the command prompt. While at the command prompt, type in **ipconfig /all** to verify the IP settings.

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



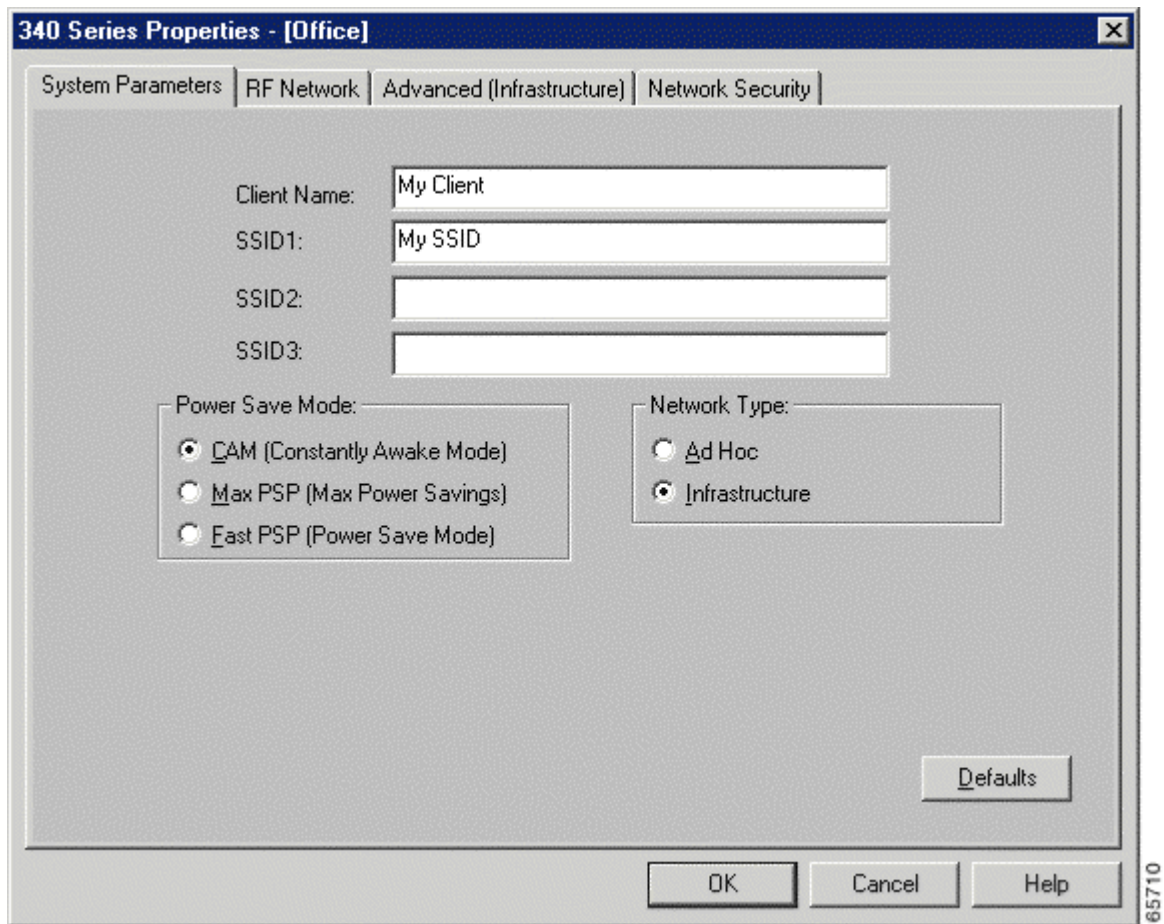
- a. Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open the ACU's profile manager.
- b. Click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears.

What tasks does the Profile manager allow?

Answer:

- Create a new profile
- Select the active profile
- Edit a profile
- Set a profile to default values
- Rename a profile
- Delete a profile
- Import a profile
- Export a profile

Step 7 Creating a new profile



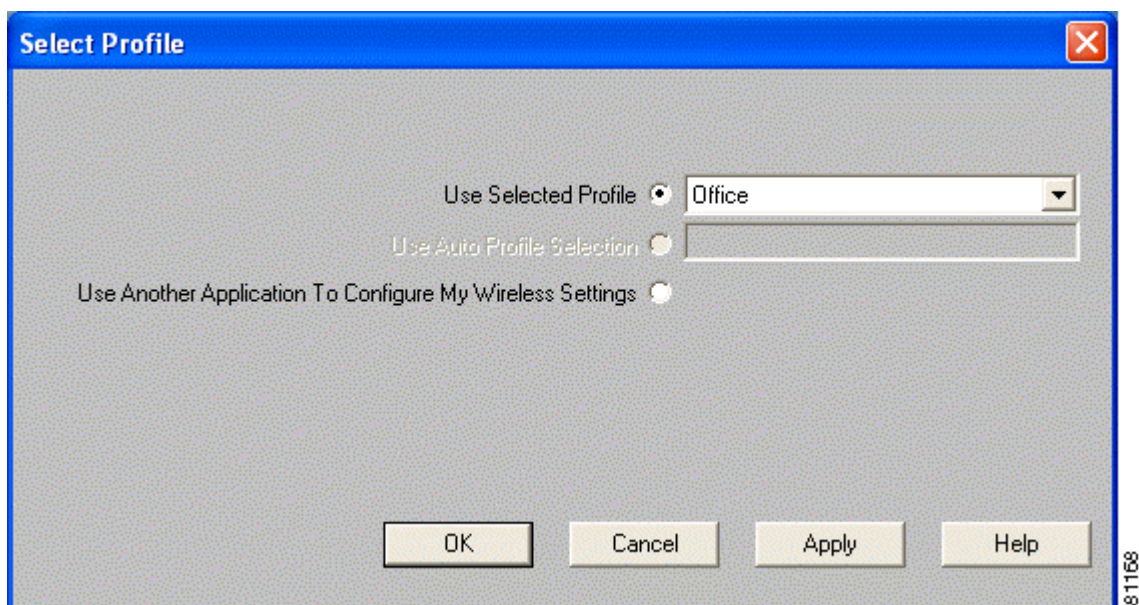
Follow the steps below to create a new profile.

- 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.

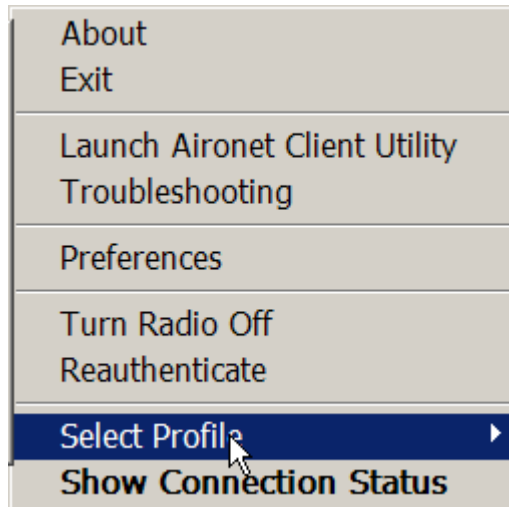
Step 9 Using the Aironet Client Monitor (ACM)

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?

Answer: Answer will vary. **Example:** The client adapter is associated to an AP, and the link quality is excellent or good.

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.

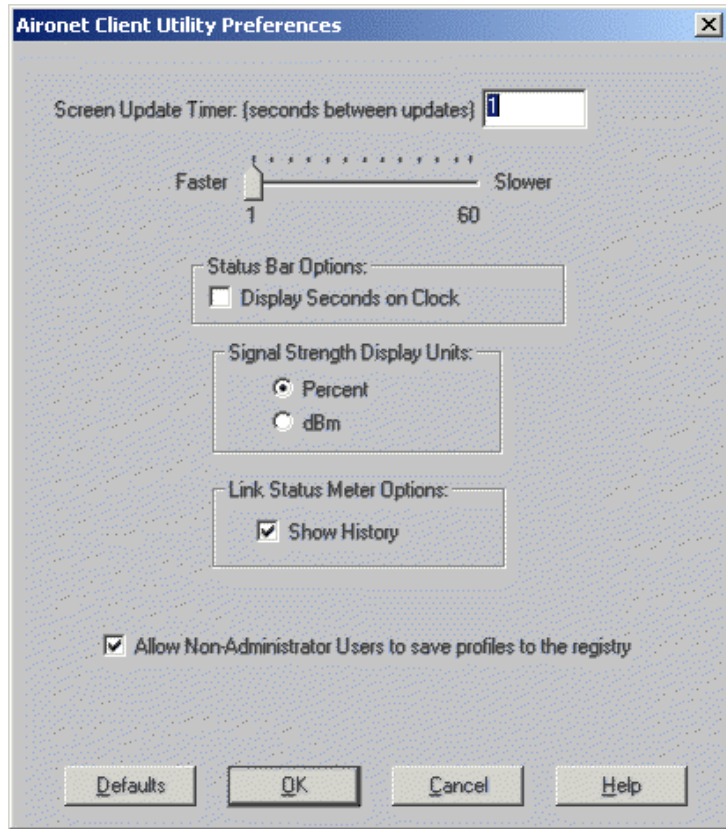
Importing a Profile

- 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 2.5.5 Configure Auto Profiles

Estimated Time: 25 Minutes

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

Objective

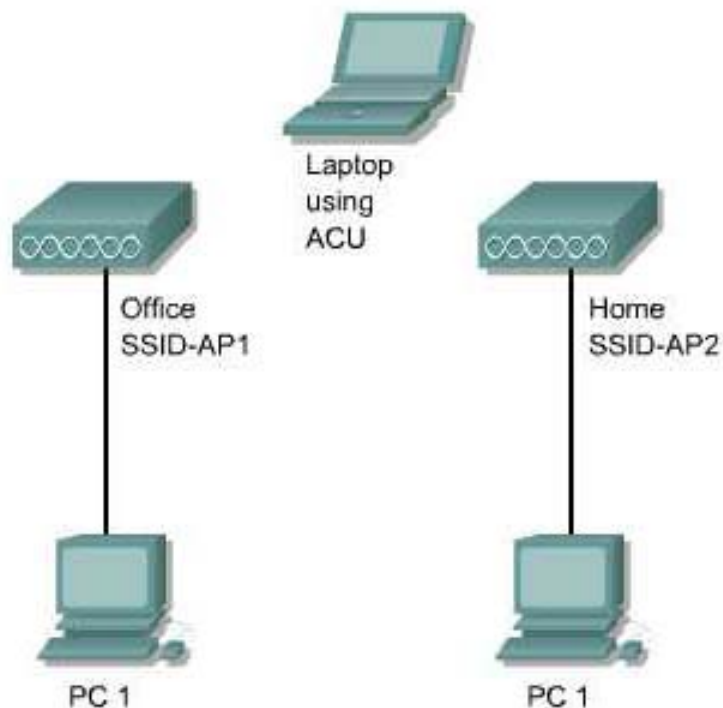
The student will learn the procedures for configuring ACU to use Auto Profiles.

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 |

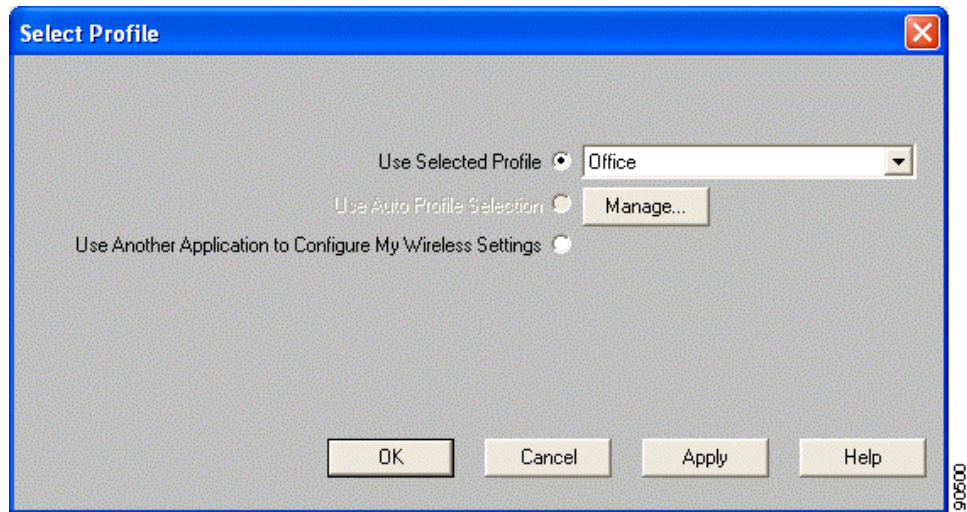
(Where StudentP is the student name)

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.

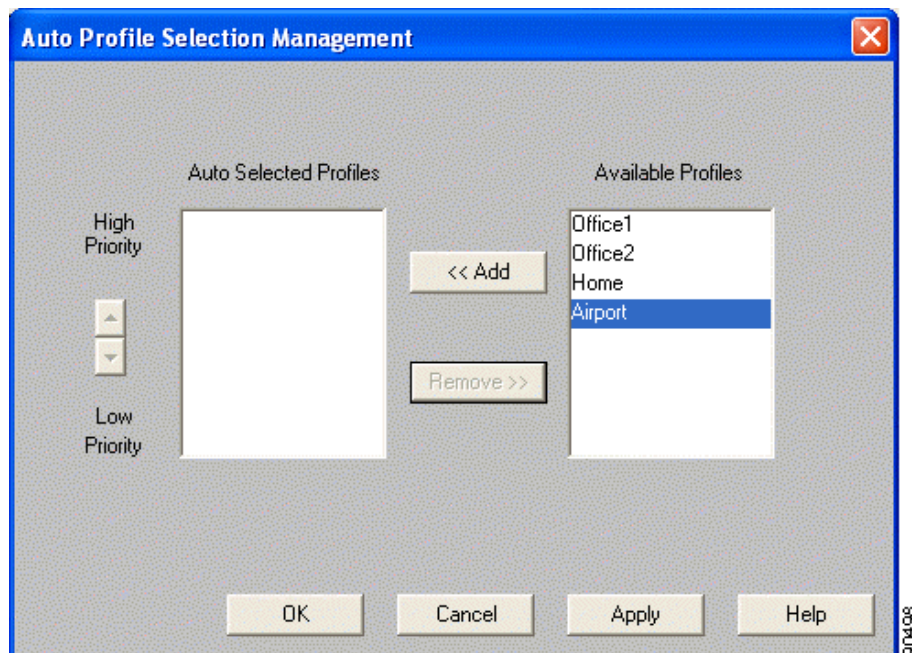
- a. Open ACU; click the **Select Profile** icon or select **Select Profile** from the Commands drop-down menu. The Select Profile screen appears



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 2.6.5.1 ACU Utilities

Estimated Time: 10 Minutes

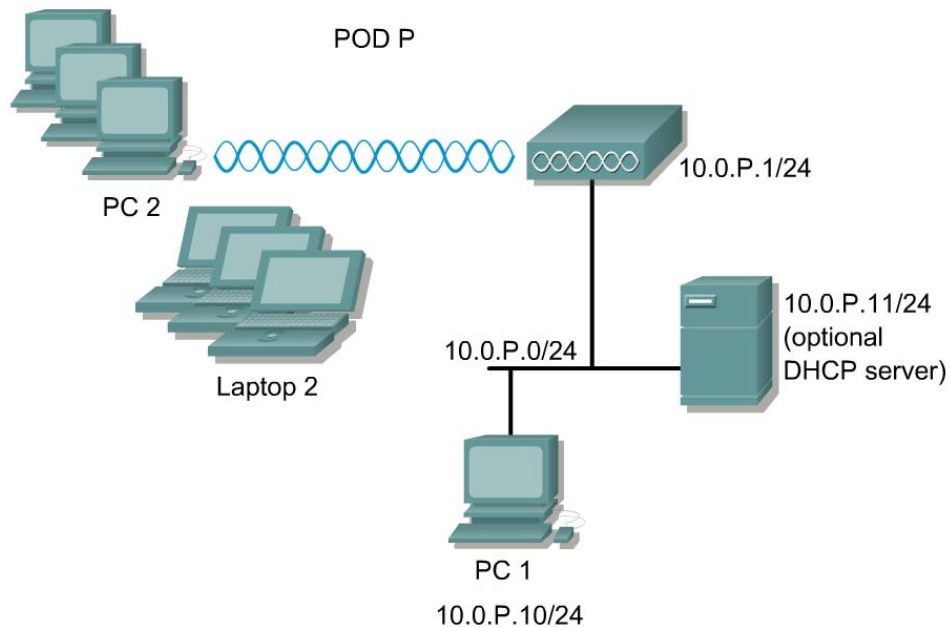
Number of Team Members: 2 students per team

Objective

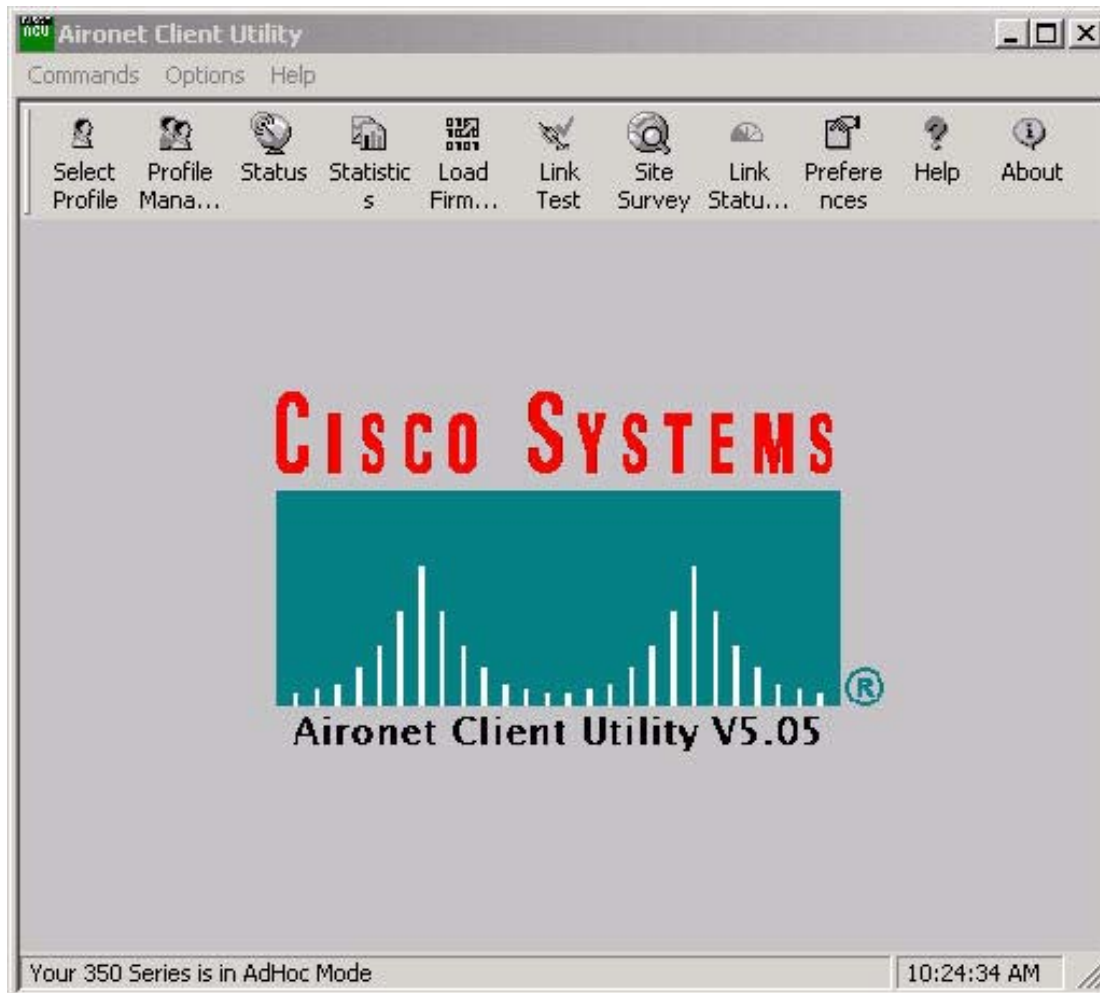
Students will use the Aironet Client Utilities (ACU) to complete the following tasks:

- 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

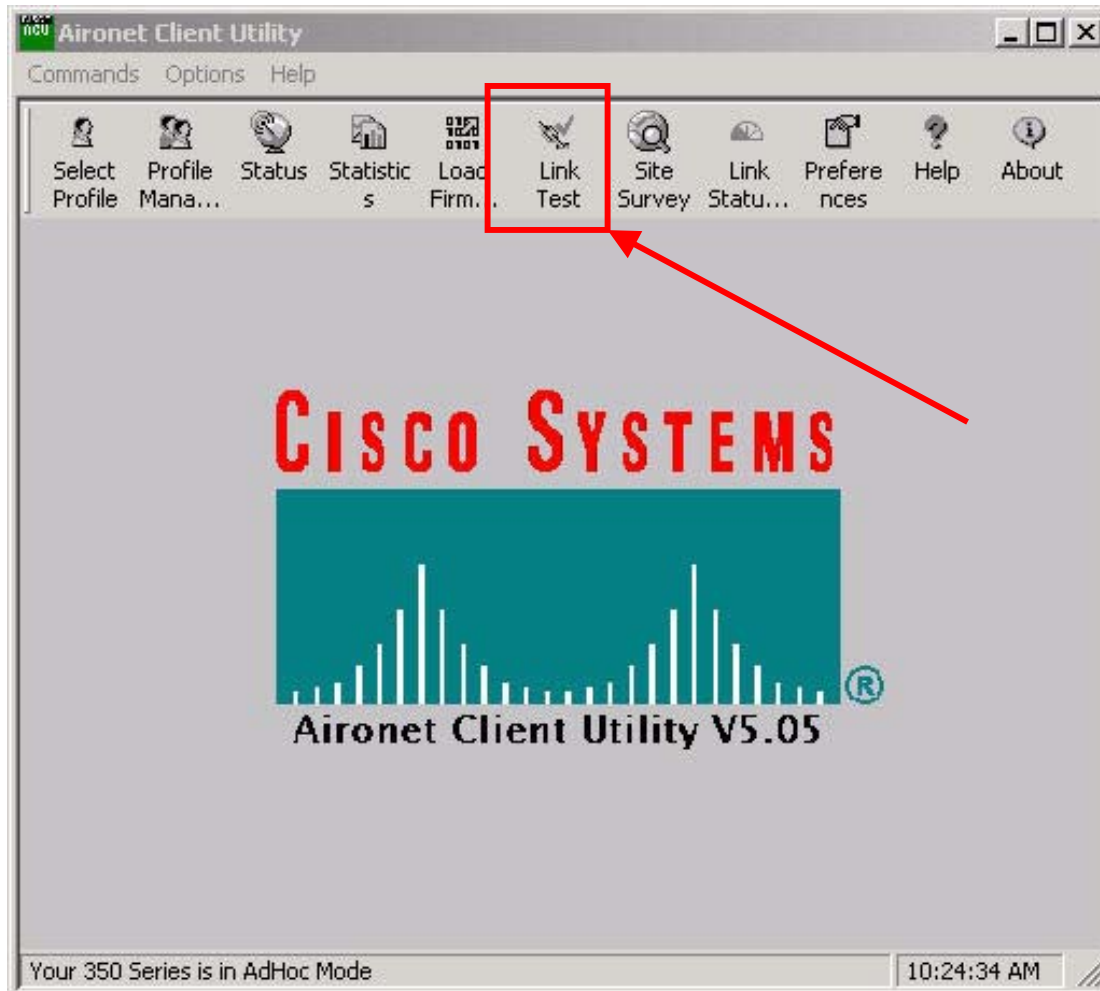
The instructor will prepare one AP that will be used by the whole class to perform this lab exercise. An IP address and SSID must be configured for the AP.

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.

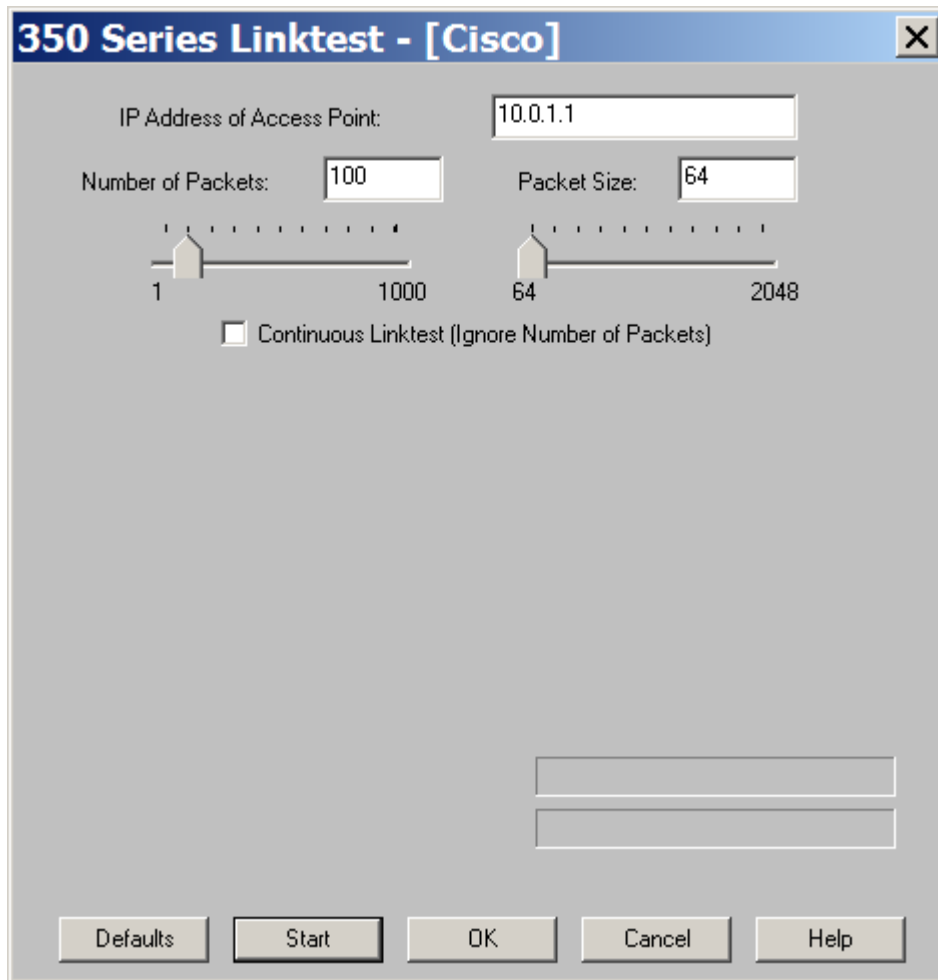
The results of the link test can be used to determine the RF network coverage and ultimately the required number and placement of APs in the network. The test also helps installers avoid areas where performance is weak. Therefore the test helps to eliminate the risk of a lost connection between the client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

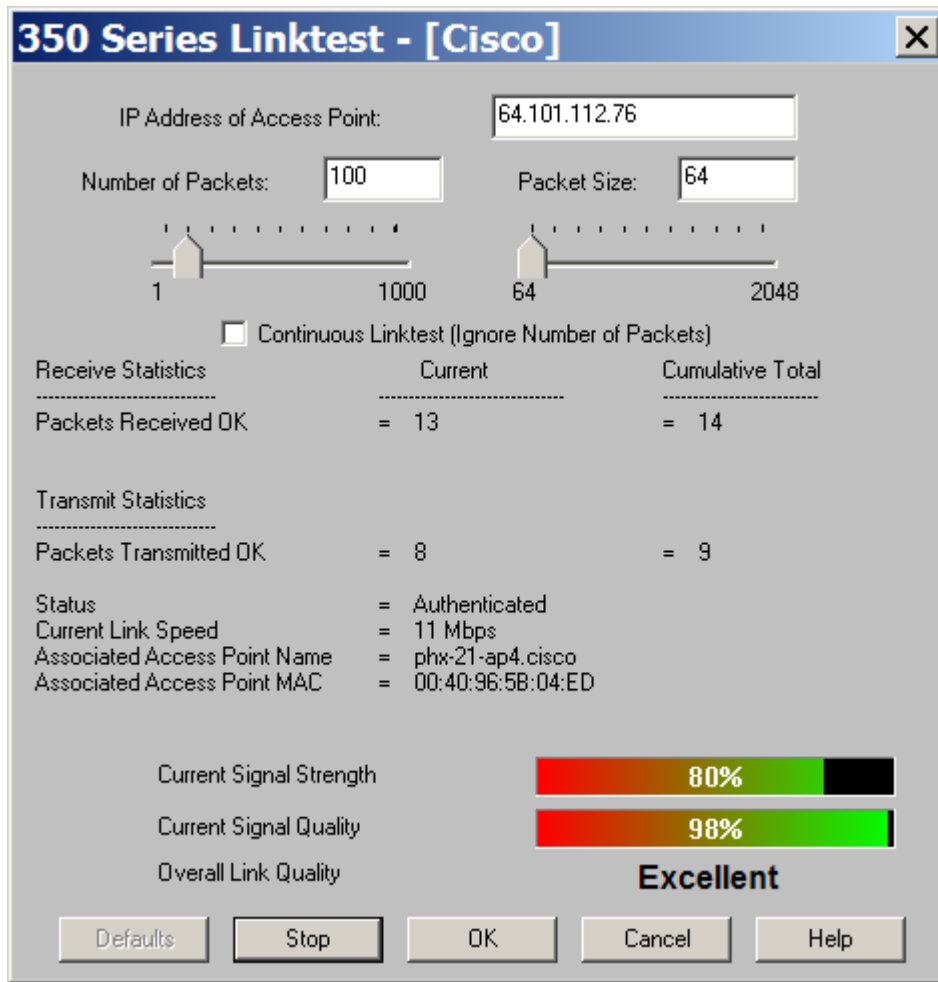


In the IP Address of AP field, notice, by default, the IP address is the AP to which the wireless NIC is associated. This IP address could be changed to another wireless device IP address.

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)?

ANSWER: Answers will vary. **Example:** 14

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

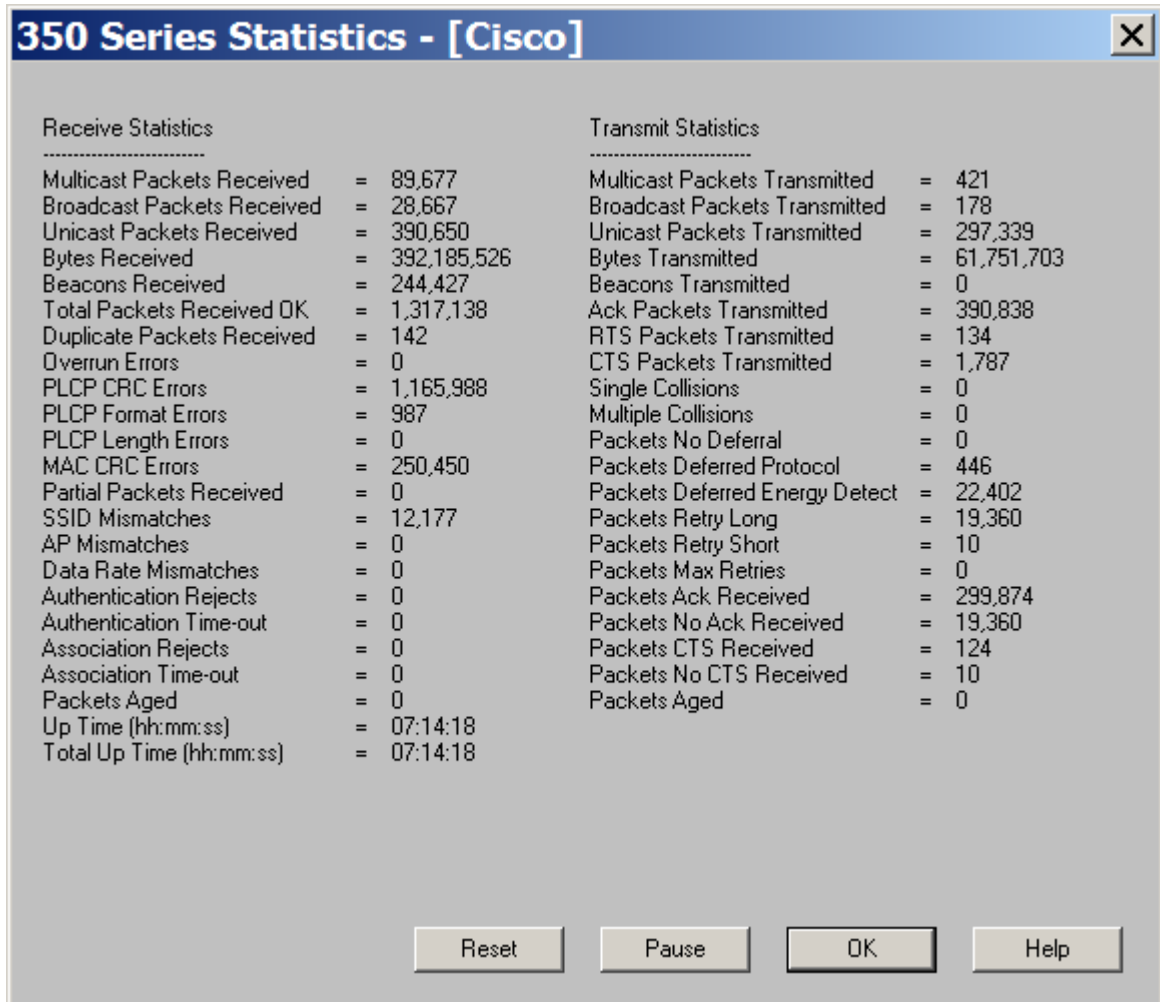
ANSWER: Answers will vary. **Example:** 9

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 _____

ANSWER: Answers will vary depending on the type and model of AP each student encounters.

Step 5 Statistics screen



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

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

ANSWER: Wireless networking is a shared media. The receive frames increment even when the transmit frames stay fairly static and no activity is being generated. This traffic is as a result of the other devices including the AP on the wireless network

- b. Define the following terms from the Statistics screen:

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

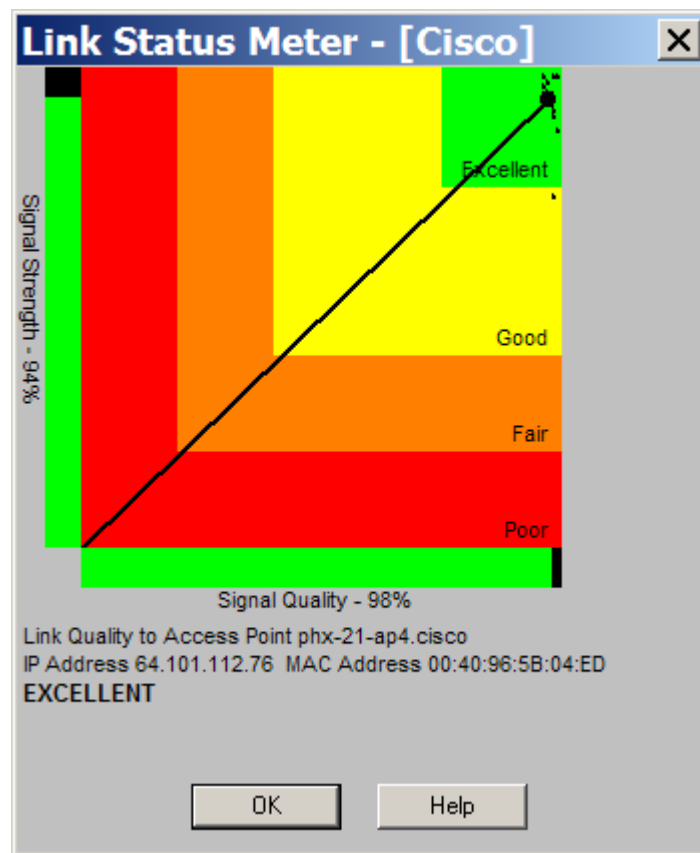
ANSWER:

RTS – Request to Send is a signal sent from the wireless NIC to the AP (or remote wireless device in an ad hoc environment) indicating that it has a frame waiting to transmit.

CTS – Clear to Send is a signal indicating that it is okay to transmit a frame.

ACK – Acknowledgement is a signal from a remote device indicating that a frame was successfully received.

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?

ANSWER: Answers will vary. **Example:** 98%

2. What is the Signal Strength of the AP?

ANSWER: Answers will vary. **Example:** 94%



Lab 2.6.5.2 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.

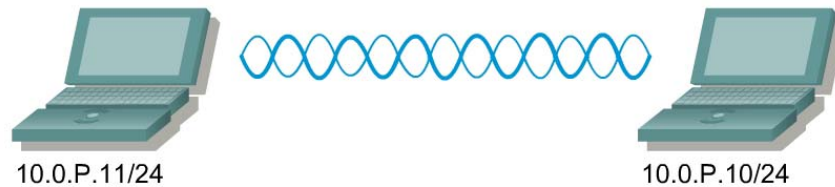
Scenario

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.

| <u>Team</u> | <u>Client Name</u> | <u>SSID</u> | <u>Client Address</u> |
|-------------|--------------------|-------------|-----------------------|
| 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)

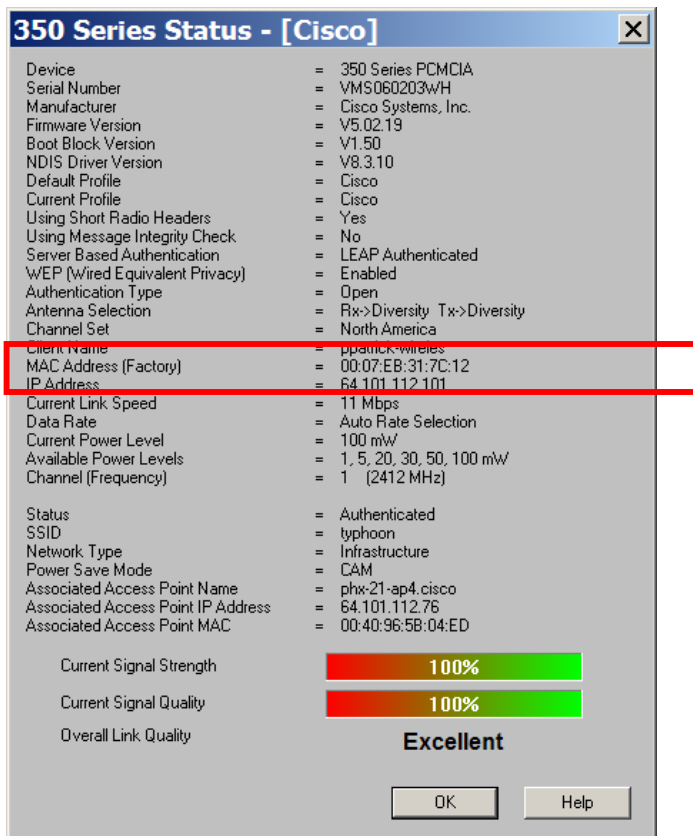
- a. Open the Cisco Aironet Client Utility.
- b. Click on the **Profile Manager** icon.
- c. Click on the **Add** button.
- d. Click on the **OK** button.
- e. From the System Parameters tab, type Adhoc# (where # is the group number assigned by the instructor) in the SSID1: box.
- f. In the Network Type 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.



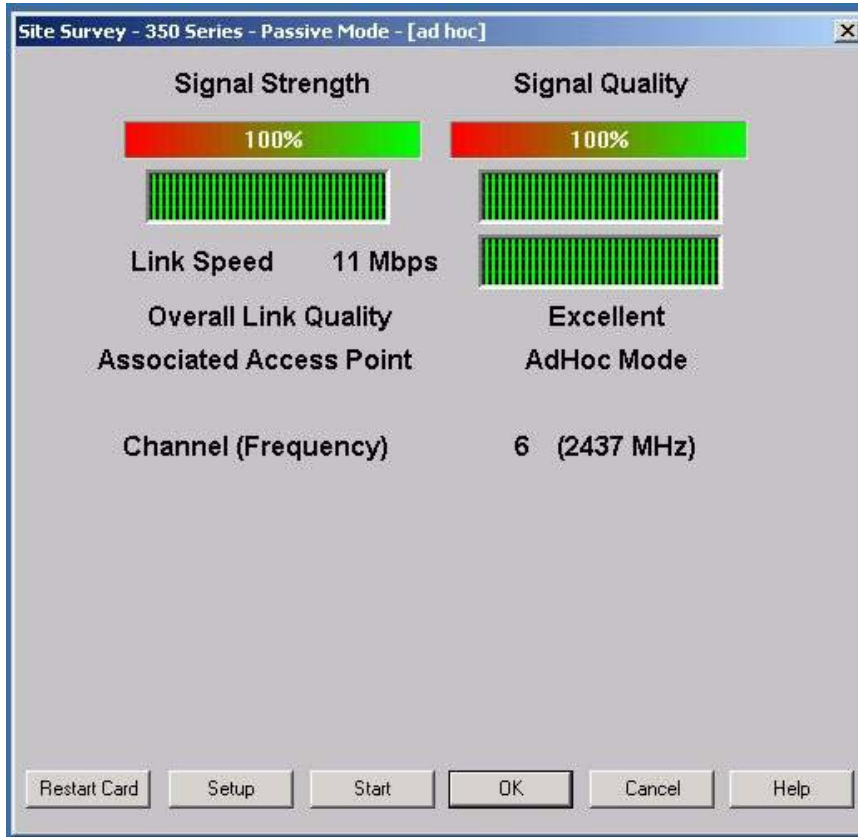
- b. What is the MAC address of the computer? Provide this information to your team partner so diagnostics can be performed.

ANSWER: Answers will vary. **Example:** 00:07:EB:31:7C:12

- c. Write your partner's MAC address.

ANSWER: Answers will vary. **Example:** 00:07:EB:45:7F:13

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?

ANSWER: The following fields appear in Ad Hoc Active Mode Screen:

1. Percent Complete
2. Percent Successful
3. Lost To Target
4. Lost to Source

Step 5 Ad Hoc Status screen



a. What is the Status of the PC?

ANSWER: Ad Hoc Mode

b. What is the SSID of the PC?

ANSWER: Adhoc# (where # is the group number assigned by the instructor)

c. What is the Network Type of the PC?

ANSWER: Ad Hoc

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

ANSWER: CAM

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

Step 6 Ad Hoc Statistics screen

The screenshot shows a window titled "350 Series Statistics - [ad hoc]" with a close button in the top right corner. The window is divided into two columns: "Receive Statistics" and "Transmit Statistics". Each column lists various metrics with their corresponding values. At the bottom of the window, there are four buttons: "Reset", "Pause", "OK", and "Help".

| Receive Statistics | | Transmit Statistics | |
|----------------------------|------------|--------------------------------|----------|
| Multicast Packets Received | = 47 | Multicast Packets Transmitted | = 0 |
| Broadcast Packets Received | = 214 | Broadcast Packets Transmitted | = 235 |
| Unicast Packets Received | = 0 | Unicast Packets Transmitted | = 0 |
| Bytes Received | = 61,385 | Bytes Transmitted | = 50,772 |
| Beacons Received | = 48,711 | Beacons Transmitted | = 48,695 |
| Total Packets Received OK | = 564,152 | Ack Packets Transmitted | = 64,271 |
| Duplicate Packets Received | = 8 | RTS Packets Transmitted | = 5,057 |
| Overrun Errors | = 0 | CTS Packets Transmitted | = 0 |
| PLCP CRC Errors | = 97,168 | Single Collisions | = 0 |
| PLCP Format Errors | = 18,568 | Multiple Collisions | = 0 |
| PLCP Length Errors | = 0 | Packets No Deferral | = 0 |
| MAC CRC Errors | = 108,419 | Packets Deferred Protocol | = 219 |
| Partial Packets Received | = 0 | Packets Deferred Energy Detect | = 1,443 |
| SSID Mismatches | = 0 | Packets Retry Long | = 8,390 |
| AP Mismatches | = 0 | Packets Retry Short | = 128 |
| Data Rate Mismatches | = 0 | Packets Max Retries | = 1,205 |
| Authentication Rejects | = 0 | Packets Ack Received | = 64,350 |
| Authentication T/O | = 0 | Packets No Ack Received | = 8,390 |
| Association Rejects | = 0 | Packets CTS Received | = 4,929 |
| Association T/O | = 0 | Packets No CTS Received | = 128 |
| Packets Aged | = 0 | Packets Aged | = 0 |
| Up Time (hh:mm:ss) | = 02:45:31 | | |
| Total Up Time (hh:mm:ss) | = 06:32:25 | | |

a. How many Broadcast packets were received?

ANSWER: Answers will vary. **Example:** 214

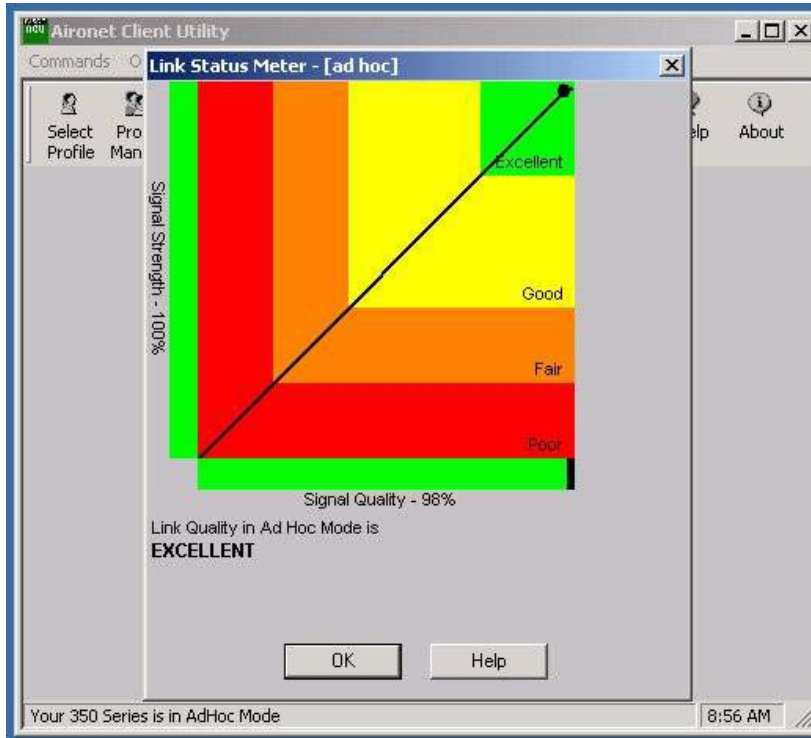
b. How many Broadcast packets were transmitted?

ANSWER: Answers will vary. **Example:** 235

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.

- 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?

ANSWER: Answers will vary. **Example:** 2000 ft

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

ANSWER: Answers will vary. **Example:** Yes

- 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?

ANSWER: Answers will vary. **Example:** wall

- 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?

ANSWER: Answers will vary, but most AP and/or clients should become disassociated to each other.

- 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?

ANSWER: Answers will vary, but generally wooden doors without any metal will have little, if any, effect on the signal quality or signal strength.

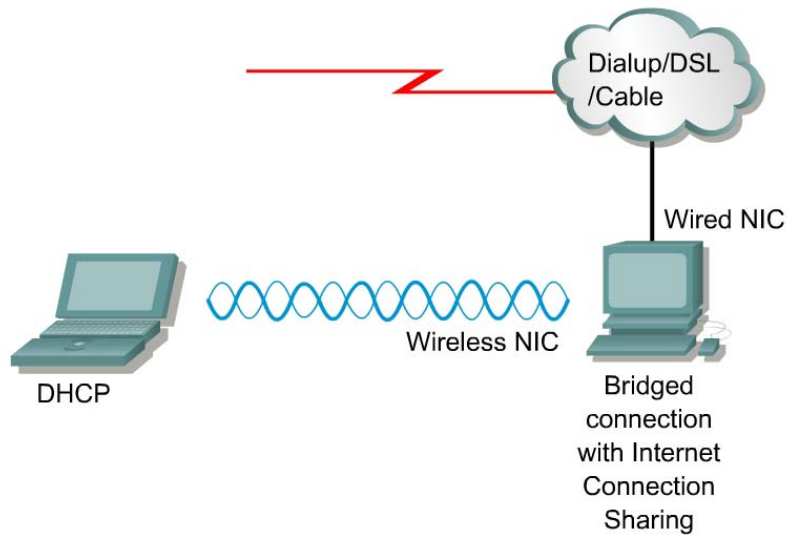
Step 8 File share in Ad Hoc Mode (OPTIONAL LAB)

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)



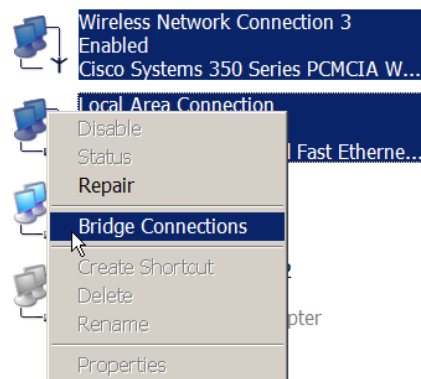
Is it necessary to purchase an AP in order to share the fast broadband connection at home? This lab is very similar to using a cross-connect cable for a small PC network, but without the use of the router or additional cables.

- a. Bridge the connection on the Desktop PC

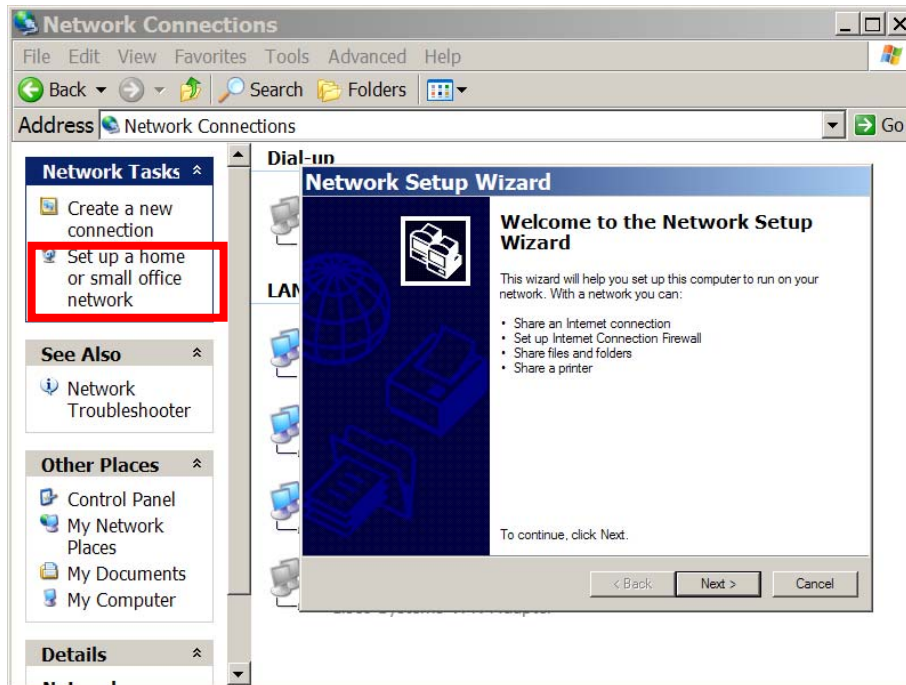
Dial-up



LAN or High-Speed Internet



b. Share an Internet connection



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

Lab 5.2.2 Configuring Basic AP Settings

Estimated Time: 30 minutes

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

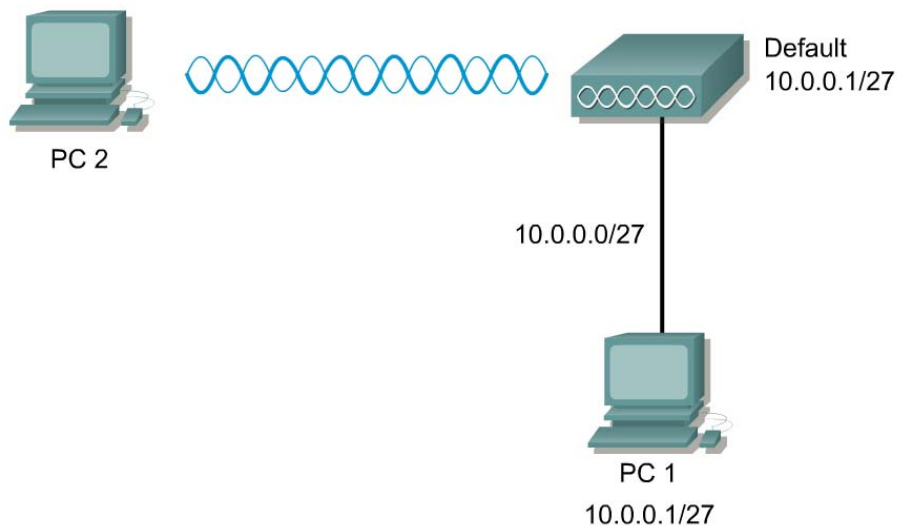
Objective

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

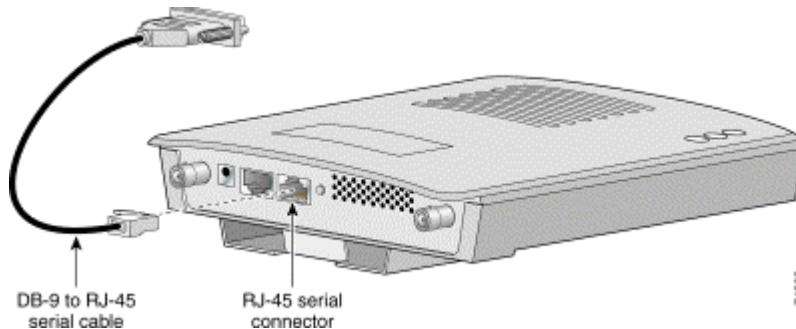
Command List

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

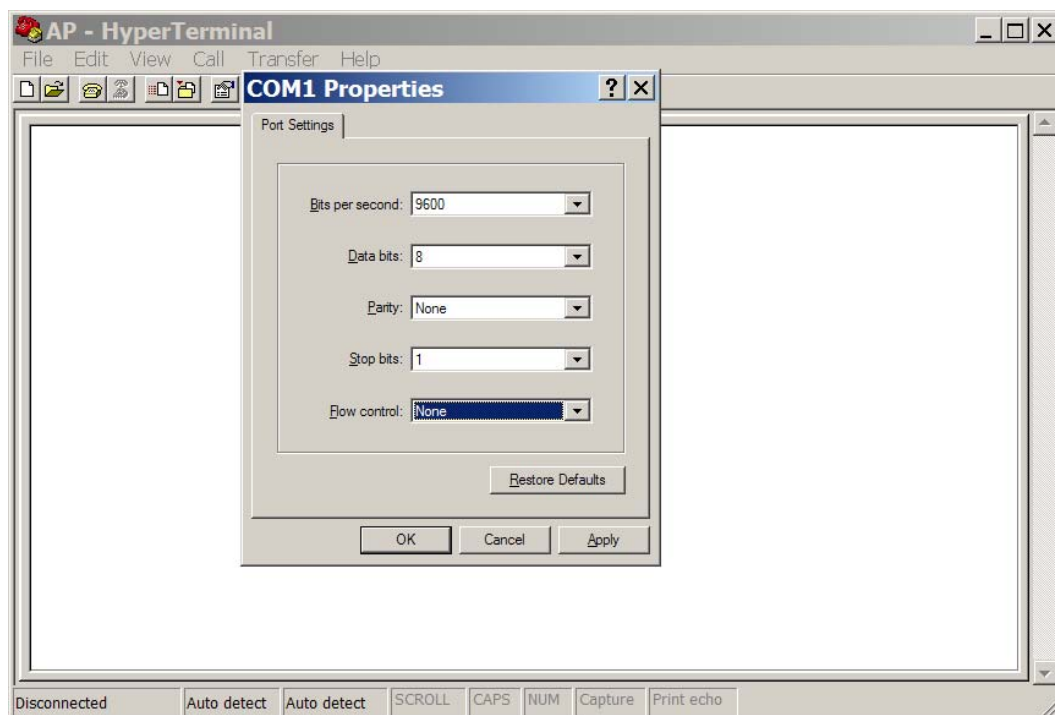
| Command | Description |
|--|--|
| <code>configure terminal</code> | Enter Global configuration mode |
| <code>hostname</code> | Set the hostname on the device |
| <code>interface bvi1</code> | Enter the virtual interface for the AP |
| <code>ip address</code> | Set the IP address and subnet mask on the device |
| <code>interface dot11radio 0</code> | Enter the device radio interface |
| <code>station role repeater root [fallback { shutdown repeater }]</code> | 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. |
| <code>ssid ssid-string</code> | 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. |
| <code>enable password password</code> | The default password is Cisco. This commands allows an administrator to change the password |
| <code>enable secret password</code> | The default enable password is <i>Cisco</i> . |
| <code>enable password level level password</code> | The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file. |

| | |
|---|---|
| <code>show dot11 associations</code> | View the connected wireless clients |
| <code>show running-config</code> | Display the current configuration of the device |
| <code>show startup-config</code> | Display the startup configuration of the device |
| <code>copy running-config startup-config</code> | Save the entries into the configuration file |
| <code>show interfaces</code> | Display interface information of the device |

Step 1 Connect to the AP using a console



- Connecting a Cisco rollover cable (console cable) between PC1 and the AP
- Open a terminal emulator.



- 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.telnet
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

- Open an Internet browser. The default IP address of an AP from the factory is 10.0.0.1.
- Type the AP IP address in the browser address location field. Press **Enter**.

.....

Cisco 1200 Access Point

| <ul style="list-style-type: none"> HOME EXPRESS SET-UP NETWORK MAP + ASSOCIATION NETWORK INTERFACES + SECURITY + SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + | <div style="text-align: right;">Hostname ap ap uptime is 12 minutes</div> <hr/> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Home: Summary Status</div> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Association</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Clients: 0</td> <td style="width: 50%;">Repeaters: 0</td> </tr> </table> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Network Identity</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">IP Address</td> <td style="width: 50%;">10.0.0.1</td> </tr> <tr> <td>MAC Address</td> <td>000b.f44a.700c</td> </tr> </table> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Network Interfaces</div> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Interface</th> <th style="width: 30%;">MAC Address</th> <th style="width: 40%;">Transmission Rate</th> </tr> </thead> <tbody> <tr> <td>↑ FastEthernet</td> <td>000b.f44a.700c</td> <td>100Mb/s</td> </tr> <tr> <td>↑ Radio0-802.11B</td> <td>0007.85b3.c270</td> <td>11.0Mb/s</td> </tr> <tr> <td>↑ Radio1-802.11A</td> <td>000b.f401.05b7</td> <td>54.0Mb/s</td> </tr> </tbody> </table> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Event Log</div> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Time</th> <th style="width: 30%;">Severity</th> <th style="width: 40%;">Description</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> | Clients: 0 | Repeaters: 0 | IP Address | 10.0.0.1 | MAC Address | 000b.f44a.700c | Interface | MAC Address | Transmission Rate | ↑ FastEthernet | 000b.f44a.700c | 100Mb/s | ↑ Radio0-802.11B | 0007.85b3.c270 | 11.0Mb/s | ↑ Radio1-802.11A | 000b.f401.05b7 | 54.0Mb/s | Time | Severity | Description | | | |
|---|---|-------------------|--------------|------------|----------|-------------|----------------|-----------|-------------|-------------------|----------------|----------------|---------|------------------|----------------|----------|------------------|----------------|----------|------|----------|-------------|--|--|--|
| Clients: 0 | Repeaters: 0 | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Address | 10.0.0.1 | | | | | | | | | | | | | | | | | | | | | | | | |
| MAC Address | 000b.f44a.700c | | | | | | | | | | | | | | | | | | | | | | | | |
| Interface | MAC Address | Transmission Rate | | | | | | | | | | | | | | | | | | | | | | | |
| ↑ FastEthernet | 000b.f44a.700c | 100Mb/s | | | | | | | | | | | | | | | | | | | | | | | |
| ↑ Radio0-802.11B | 0007.85b3.c270 | 11.0Mb/s | | | | | | | | | | | | | | | | | | | | | | | |
| ↑ Radio1-802.11A | 000b.f401.05b7 | 54.0Mb/s | | | | | | | | | | | | | | | | | | | | | | | |
| Time | Severity | Description | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | |

- A log in screen appears. Type in the password of **Cisco** (case sensitive) and click OK.
- When the AP HOME page appears, click **Express Setup** if the Express Setup does not appear.

.....

Cisco 1200 Access Point

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|--------------|----|--------------|----------------|--------------------------------|---|-------------|----------|-----------------|-----------------|------------------|---------|-----------------|------------------|--|---|-------|---------|---------------------------|---|------------------------|--|-----------------------------|--|---------------------|---|-------|---------|---------------------------|---|------------------------|--|-----------------------------|--|---------------------|---|
| <ul style="list-style-type: none"> HOME EXPRESS SET-UP NETWORK MAP + ASSOCIATION NETWORK INTERFACES + SECURITY + SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + | <div style="text-align: right;">Hostname ap ap uptime is 12 minutes</div> <hr/> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Express Set-Up</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">System Name:</td> <td style="width: 70%;">ap</td> </tr> <tr> <td>MAC Address:</td> <td>000b.f44a.700c</td> </tr> <tr> <td>Configuration Server Protocol:</td> <td><input type="radio"/> DHCP <input checked="" type="radio"/> Static IP</td> </tr> <tr> <td>IP Address:</td> <td>10.0.0.1</td> </tr> <tr> <td>IP Subnet Mask:</td> <td>255.255.255.224</td> </tr> <tr> <td>Default Gateway:</td> <td>0.0.0.0</td> </tr> <tr> <td>SNMP Community:</td> <td>defaultCommunity</td> </tr> <tr> <td></td> <td><input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write</td> </tr> </table> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Radio0-802.11B</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID:</td> <td style="width: 70%;">tsunami</td> </tr> <tr> <td>Broadcast SSID in Beacon:</td> <td><input checked="" type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td>Role in Radio Network:</td> <td><input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root</td> </tr> <tr> <td>Optimize Radio Network for:</td> <td><input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> Custom</td> </tr> <tr> <td>Aironet Extensions:</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> </table> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;">Radio1-802.11A</div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID:</td> <td style="width: 70%;">tsunami</td> </tr> <tr> <td>Broadcast SSID in Beacon:</td> <td><input checked="" type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td>Role in Radio Network:</td> <td><input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root</td> </tr> <tr> <td>Optimize Radio Network for:</td> <td><input type="radio"/> Throughput <input type="radio"/> Range <input checked="" type="radio"/> Default <input type="radio"/> Custom</td> </tr> <tr> <td>Aironet Extensions:</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> </table> | System Name: | ap | MAC Address: | 000b.f44a.700c | Configuration Server Protocol: | <input type="radio"/> DHCP <input checked="" type="radio"/> Static IP | IP Address: | 10.0.0.1 | IP Subnet Mask: | 255.255.255.224 | Default Gateway: | 0.0.0.0 | SNMP Community: | defaultCommunity | | <input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write | SSID: | tsunami | Broadcast SSID in Beacon: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Role in Radio Network: | <input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root | Optimize Radio Network for: | <input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> Custom | Aironet Extensions: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | SSID: | tsunami | Broadcast SSID in Beacon: | <input checked="" type="radio"/> Yes <input type="radio"/> No | Role in Radio Network: | <input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root | Optimize Radio Network for: | <input type="radio"/> Throughput <input type="radio"/> Range <input checked="" type="radio"/> Default <input type="radio"/> Custom | Aironet Extensions: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| System Name: | ap | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MAC Address: | 000b.f44a.700c | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Configuration Server Protocol: | <input type="radio"/> DHCP <input checked="" type="radio"/> Static IP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Address: | 10.0.0.1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Subnet Mask: | 255.255.255.224 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Default Gateway: | 0.0.0.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SNMP Community: | defaultCommunity | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SSID: | tsunami | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Broadcast SSID in Beacon: | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Role in Radio Network: | <input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Optimize Radio Network for: | <input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> Custom | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Aironet Extensions: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SSID: | tsunami | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Broadcast SSID in Beacon: | <input checked="" type="radio"/> Yes <input type="radio"/> No | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Role in Radio Network: | <input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Optimize Radio Network for: | <input type="radio"/> Throughput <input type="radio"/> Range <input checked="" type="radio"/> Default <input type="radio"/> Custom | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Aironet Extensions: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

- 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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>AP Address</u> | <u>PC1 Address</u> | <u>PC2 Address</u> |
|-------------|----------------|-------------|-------------------|--------------------|--------------------|
| 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.
 1. What IP address will be assigned to this AP?

ANSWER: 10.0.P.1. (where **P** is the assigned pod number)

- b. Enter an IP subnet mask in the **IP Subnet Mask** field.
 1. What Subnet mask will be assigned to this AP? Write the answer in dotted decimal notation.

ANSWER: 255.255.255.0.

1. What Subnet mask in binary.

ANSWER: 11111111.11111111.11111111.00000000.

- 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.

1. What SSID will be assigned to this AP?

ANSWER: APP. (where **P** is the assigned pod number)

- 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

Close Window

CISCO SYSTEMS

Cisco 1200 Access Point

Hostname AP1200 AP1200 uptime is 23 hours, 32 minutes

Association

Clients: 1 Repeaters: 0

View: Client Repeater Apply

Radio802.11B

SSID AP1200 :

| Device Type | Name | IP Address | MAC Address | State | Parent | VLAN |
|-------------|--------------|------------|--------------------------------|------------|--------|------|
| 350-client | TONORWOO-W2K | 0.0.0.0 | 0007.50ca.e208 | Associated | self | none |

Radio802.11A

Refresh

- 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 |
|-------------|
| |
| |

ANSWER: Answers will vary according to the connected devices.

- 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**.



1. Record the values below.

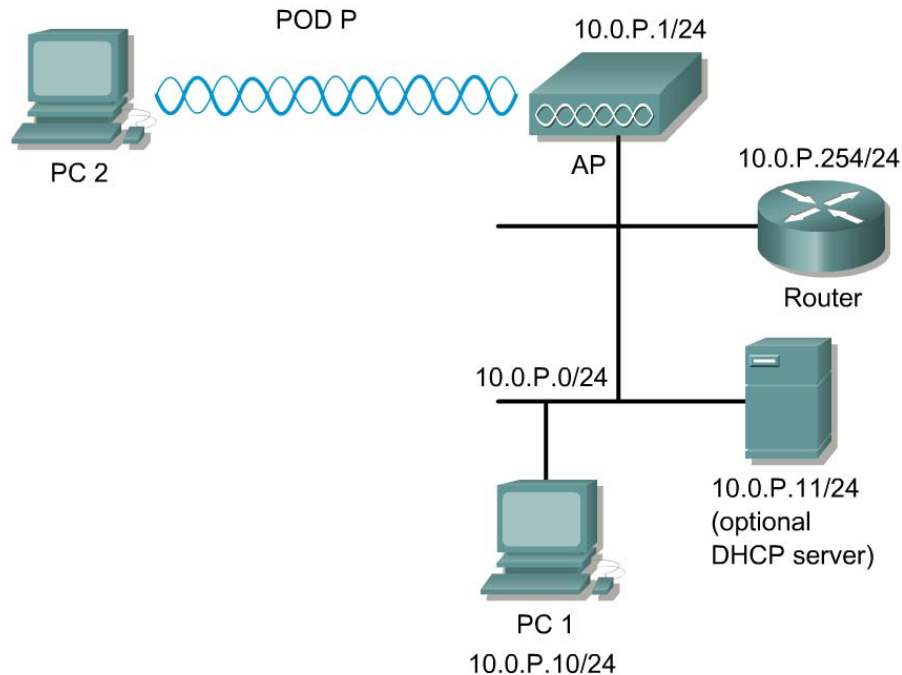
ANSWER: APP. and 10.0.P.1 (where P is the assigned pod number)

- 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.

ANSWER: Answers will vary.



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 **level1** 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 level1** 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.

- d. Configure and select a profile to connect to the AP. Make sure the SSID is configured in the profile to match the AP.
- e. Configure a unique **Client Name** in the profile, such as a first initial last name of one of the team members
- f. 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.
- g. 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**.



2. Record the values below?

ANSWER: APP. and 10.0.P.1 (where P is the assigned pod number)

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

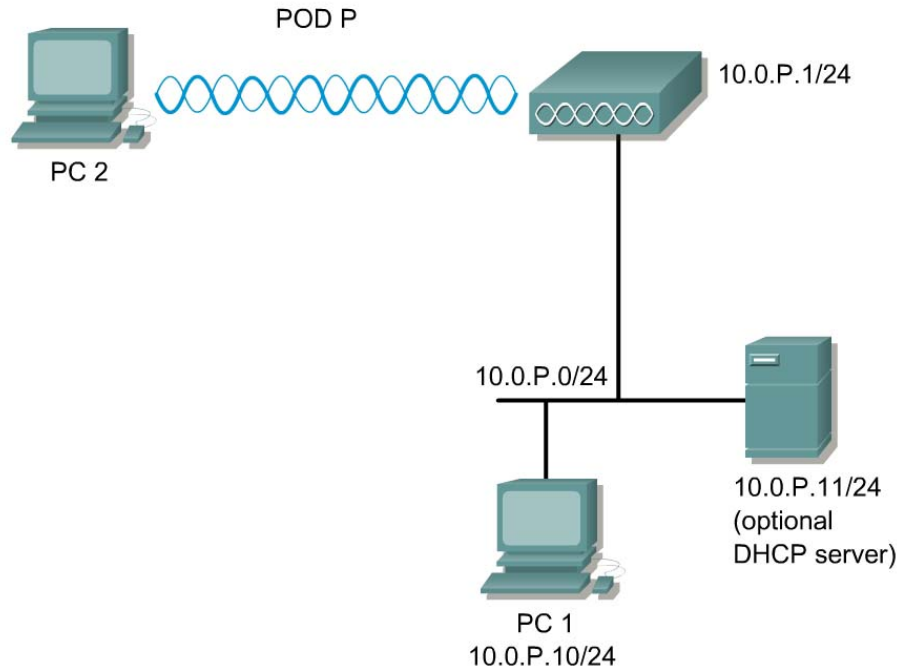
In this lab, the student will learn the following objectives:

- 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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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:

ANSWER:

```
Bits per second (baud rate): 9600
```

```
Data bits: 8
```

```
Parity: none
```

```
Stop bits: 1
```

```
Flow control: none
```

- 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?

ANSWER: **show running-config**

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

ANSWER: **show startup-config**

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

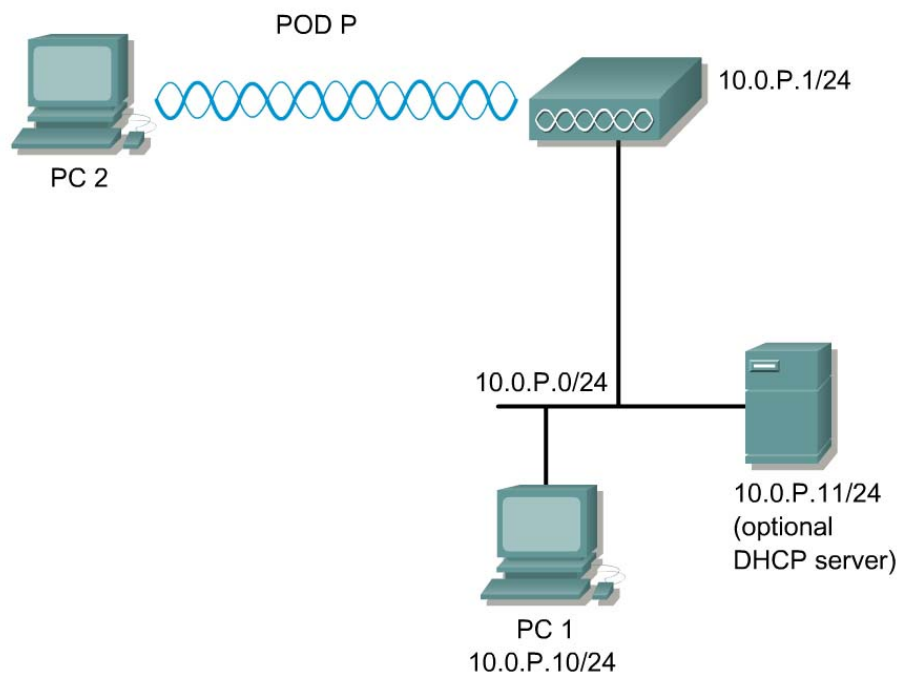
In this lab, the student will learn to manage configuration and image files.

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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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

- 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?

ANSWER: `show running-config`

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

ANSWER: `show startup-config`

- 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 | nvr | rw | nvr |
| | - | - | network | rw | tftp: |
| | - | - | opaque | rw | null: |
| | - | - | opaque | rw | system: |
| | - | - | opaque | ro | xmodem: |
| | - | - | opaque | ro | ymodem: |
| | - | - | network | rw | rcp: |
| | - | - | network | rw | ftp: |
| | - | - | network | rw | scp: |

3. What do the Flags value represent?

ANSWER: Permissions for file system

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
nvr:         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-config]?
```

- 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-config]?
```

- 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-config]?
```

- i. Verify the uploaded configuration file in NVRAM.

```
PodP#show start
```

Step 5 Manage System Image Files

.....

Cisco 1200 Access Point

HOME Hostname PodP PodP uptime is 2 hours, 5 minutes

EXPRESS SET-UP

NETWORK MAP +

ASSOCIATION

NETWORK INTERFACES +

SECURITY +

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE

Software Upgrade

System Configuration

EVENT LOG +

System Software Version: IOS (tm) C1200 Software (C1200-K9W7-M)

Product/Model Number: AIR-AP1220-IOS-UPGRD

Top Assembly Serial Number:

System Software Filename: c1200-k9w7-tar.122-11.JA

System Software Version: 12.2(11)JA

Bootloader Version: 12.2(11)JA

System Uptime: 2 hours, 5 minutes

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

4. What is the Product/Model Number?

ANSWER: AIR-AF 1220-IOS-UPGRD or similar

5. What is the System Software Filename?

ANSWER: AIR-AF 1220-IOS-UPGRD or similar

.....

Cisco 1200 Access Point

HOME HTTP UPGRADE TFTP UPGRADE

EXPRESS SET-UP Hostname PodP PodP uptime is 2 hours, 16 minutes

NETWORK MAP +

ASSOCIATION

NETWORK INTERFACES +

SECURITY +

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE

Software Upgrade

System Configuration

EVENT LOG +

System Software: Upgrade- HTTP Upgrade

System Software Filename: c1200-k9w7-tar.122-11.JA

System Software Version: 12.2(11)JA

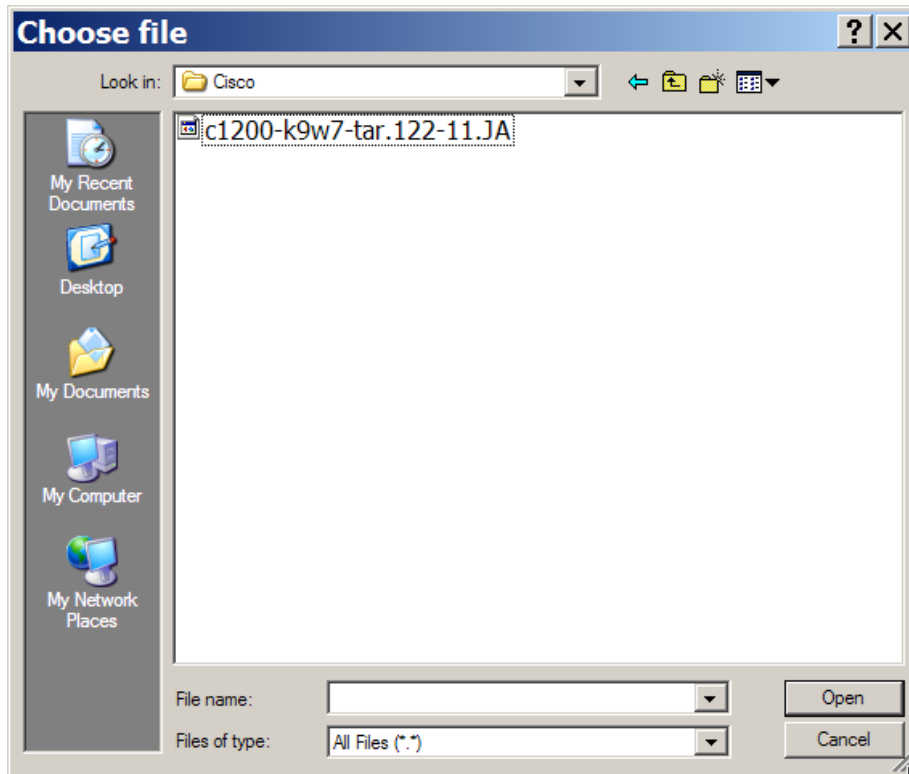
Bootloader Version: 12.2(11)JA

Upgrade System Software Tar File:

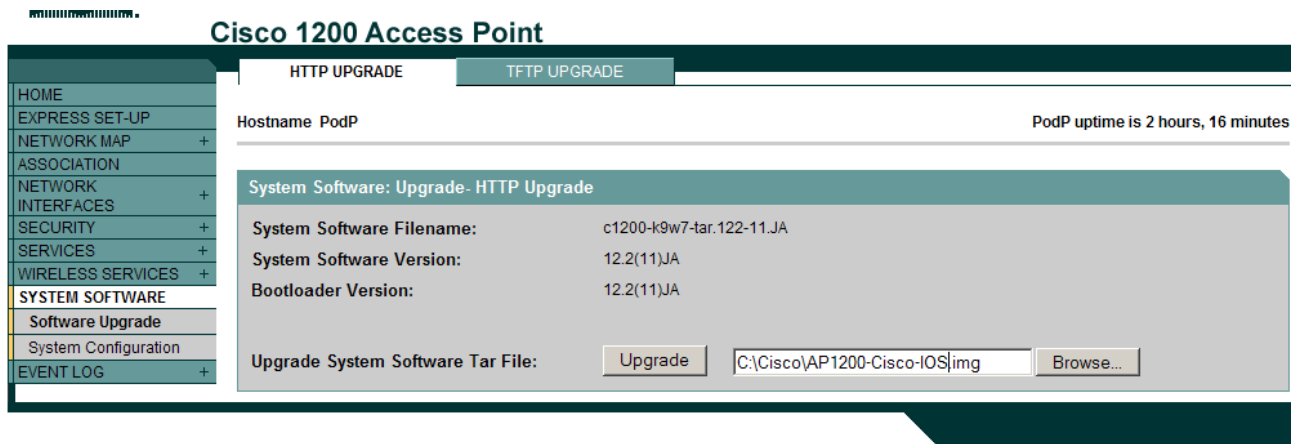
The **SYSTEM SOFTWARE>Software Upgrade** Page provides the easiest method to upgrade a system image.

- d. 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>



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



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

Note Before proceeding with Upgrade, get the instructors approval

g. Click the Upgrade button.

h. 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-config  
Write file ap1-config 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-config]?  
Write file ap1-config 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[rtrl-config]? host1-config  
Configure using host1-config from 10.0.P.10?[confirm]  
Connected to 10.0.P.10  
Loading 1112 byte file host1-config:![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.

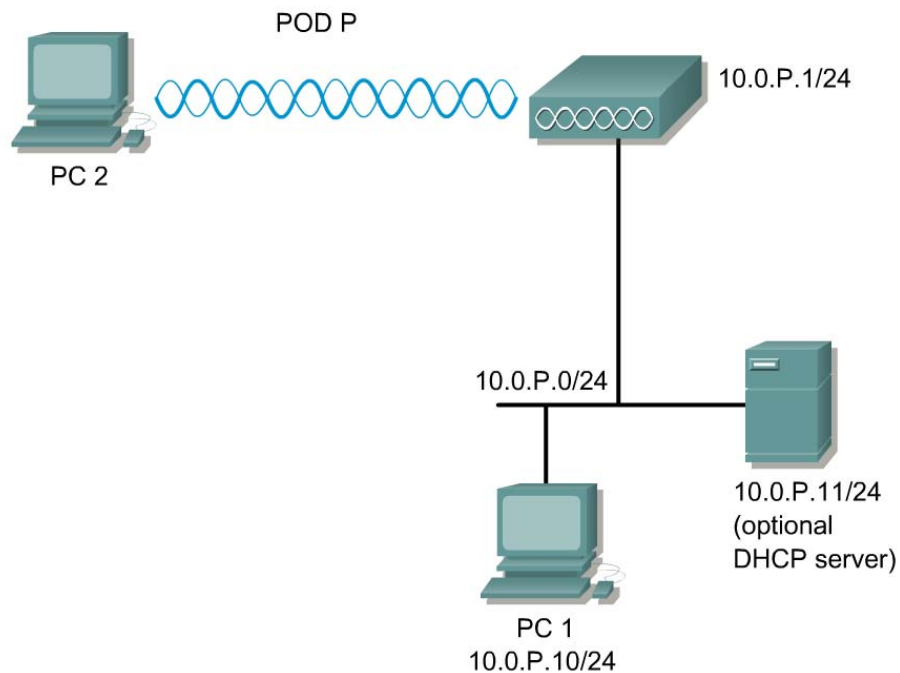
Objective

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.

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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

Cisco 1200 Access Point

| <ul style="list-style-type: none"> HOME EXPRESS SET-UP NETWORK MAP + ASSOCIATION NETWORK INTERFACES + SECURITY + SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + | <div style="display: flex; justify-content: space-between;"> Hostname ap ap uptime is 11 minutes </div> <hr/> <p>Home: Summary Status</p> <p><u>Association</u></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Clients: 0</td> <td style="width: 50%;">Repeaters: 0</td> </tr> </table> <p><u>Network Identity</u></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">IP Address</td> <td style="width: 50%;">10.0.0.1</td> </tr> <tr> <td>MAC Address</td> <td>000b.46b8.ca90</td> </tr> </table> <p><u>Network Interfaces</u></p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Interface</th> <th style="width: 30%;">MAC Address</th> <th style="width: 40%;">Transmission Rate</th> </tr> </thead> <tbody> <tr> <td>FastEthernet</td> <td>000b.46b8.ca90</td> <td>100Mb/s</td> </tr> <tr> <td>Radio0-802.11B</td> <td>0007.85b3.646f</td> <td>11.0Mb/s</td> </tr> <tr> <td>Radio1-802.11A</td> <td>000a.f4f3.4c8d</td> <td>54.0Mb/s</td> </tr> </tbody> </table> <p><u>Event Log</u></p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">Time</th> <th style="width: 25%;">Severity</th> <th style="width: 50%;">Description</th> </tr> </thead> <tbody> <tr> <td>Mar 1 00:11:22.632</td> <td>◆ Notification</td> <td>Configured from console by console</td> </tr> <tr> <td>Mar 1 00:09:56.616</td> <td>◆ Warning</td> <td>Duplicate address 10.0.0.1 on BVI1, sourced by 0006.5bb8.54f5</td> </tr> <tr> <td>Mar 1 00:07:25.197</td> <td>◆ Notification</td> <td>Line protocol on interface FastEthernet0, changed state to up</td> </tr> <tr> <td>Mar 1 00:00:20.258</td> <td>◆ Notification</td> <td>Line protocol on interface Dot11Radio1, changed state to up</td> </tr> <tr> <td>Mar 1 00:00:19.263</td> <td>◆ Error</td> <td>Interface Dot11Radio1, changed state to up</td> </tr> <tr> <td>Mar 1 00:00:19.257</td> <td>◆ Information</td> <td>Interface Dot11Radio1, frequency 5280 selected</td> </tr> <tr> <td>Mar 1 00:00:15.257</td> <td>◆ Notification</td> <td>Line protocol on interface Dot11Radio0, changed state to up</td> </tr> <tr> <td>Mar 1 00:00:15.197</td> <td>◆ Notification</td> <td>Line protocol on interface FastEthernet0, changed state to down</td> </tr> <tr> <td>Mar 1 00:00:14.276</td> <td>◆ Error</td> <td>Interface Dot11Radio0, changed state to up</td> </tr> <tr> <td>Mar 1 00:00:14.256</td> <td>◆ Information</td> <td>Interface Dot11Radio0, frequency 2452 selected</td> </tr> </tbody> </table> | Clients: 0 | Repeaters: 0 | IP Address | 10.0.0.1 | MAC Address | 000b.46b8.ca90 | Interface | MAC Address | Transmission Rate | FastEthernet | 000b.46b8.ca90 | 100Mb/s | Radio0-802.11B | 0007.85b3.646f | 11.0Mb/s | Radio1-802.11A | 000a.f4f3.4c8d | 54.0Mb/s | Time | Severity | Description | Mar 1 00:11:22.632 | ◆ Notification | Configured from console by console | Mar 1 00:09:56.616 | ◆ Warning | Duplicate address 10.0.0.1 on BVI1, sourced by 0006.5bb8.54f5 | Mar 1 00:07:25.197 | ◆ Notification | Line protocol on interface FastEthernet0, changed state to up | Mar 1 00:00:20.258 | ◆ Notification | Line protocol on interface Dot11Radio1, changed state to up | Mar 1 00:00:19.263 | ◆ Error | Interface Dot11Radio1, changed state to up | Mar 1 00:00:19.257 | ◆ Information | Interface Dot11Radio1, frequency 5280 selected | Mar 1 00:00:15.257 | ◆ Notification | Line protocol on interface Dot11Radio0, changed state to up | Mar 1 00:00:15.197 | ◆ Notification | Line protocol on interface FastEthernet0, changed state to down | Mar 1 00:00:14.276 | ◆ Error | Interface Dot11Radio0, changed state to up | Mar 1 00:00:14.256 | ◆ Information | Interface Dot11Radio0, frequency 2452 selected |
|---|--|---|--------------|------------|----------|-------------|----------------|-----------|-------------|-------------------|------------------------------|----------------|---------|--------------------------------|----------------|----------|--------------------------------|----------------|----------|------|----------|-------------|--------------------|----------------|------------------------------------|--------------------|-----------|---|--------------------|----------------|---|--------------------|----------------|---|--------------------|---------|--|--------------------|---------------|--|--------------------|----------------|---|--------------------|----------------|---|--------------------|---------|--|--------------------|---------------|--|
| Clients: 0 | Repeaters: 0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IP Address | 10.0.0.1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MAC Address | 000b.46b8.ca90 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Interface | MAC Address | Transmission Rate | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FastEthernet | 000b.46b8.ca90 | 100Mb/s | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Radio0-802.11B | 0007.85b3.646f | 11.0Mb/s | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Radio1-802.11A | 000a.f4f3.4c8d | 54.0Mb/s | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Time | Severity | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:11:22.632 | ◆ Notification | Configured from console by console | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:09:56.616 | ◆ Warning | Duplicate address 10.0.0.1 on BVI1, sourced by 0006.5bb8.54f5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:07:25.197 | ◆ Notification | Line protocol on interface FastEthernet0, changed state to up | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:20.258 | ◆ Notification | Line protocol on interface Dot11Radio1, changed state to up | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:19.263 | ◆ Error | Interface Dot11Radio1, changed state to up | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:19.257 | ◆ Information | Interface Dot11Radio1, frequency 5280 selected | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:15.257 | ◆ Notification | Line protocol on interface Dot11Radio0, changed state to up | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:15.197 | ◆ Notification | Line protocol on interface FastEthernet0, changed state to down | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:14.276 | ◆ Error | Interface Dot11Radio0, changed state to up | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mar 1 00:00:14.256 | ◆ Information | Interface Dot11Radio0, frequency 2452 selected | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

[Refresh](#)

- 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.

Answer (for Pod1):

```
ap(config)#hostname Pod1
```

```
Pod1(config)#
```

```
Pod1(config)#interface bvi1
```

```
Pod1(config-if)#ip address 10.0.1.1 255.255.255.0
```

```
Pod1(config-if)#interface dot11radio 0
```

If 802.11a is available, then:

```
Pod1(config-if)#ssid AP1
```

```
Pod1(config-if)#interface dot11radio 1
```

```
Pod1(config-if)#ssid AP1
```

```
Pod1(config-if-ssid)#
```

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

Step 2 Express Setup page

Cisco 1200 Access Point

Hostname Pod1 Pod1 uptime is 19 minutes

Express Set-Up

System Name:

MAC Address: 000b.46b8.ca90

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0-802.11B

SSID:

Broadcast SSID in Beacon: Yes No

Role in Radio Network: Access Point Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Custom

Aironet Extensions: Enable Disable

Radio1-802.11A

SSID:

Broadcast SSID in Beacon: Yes No

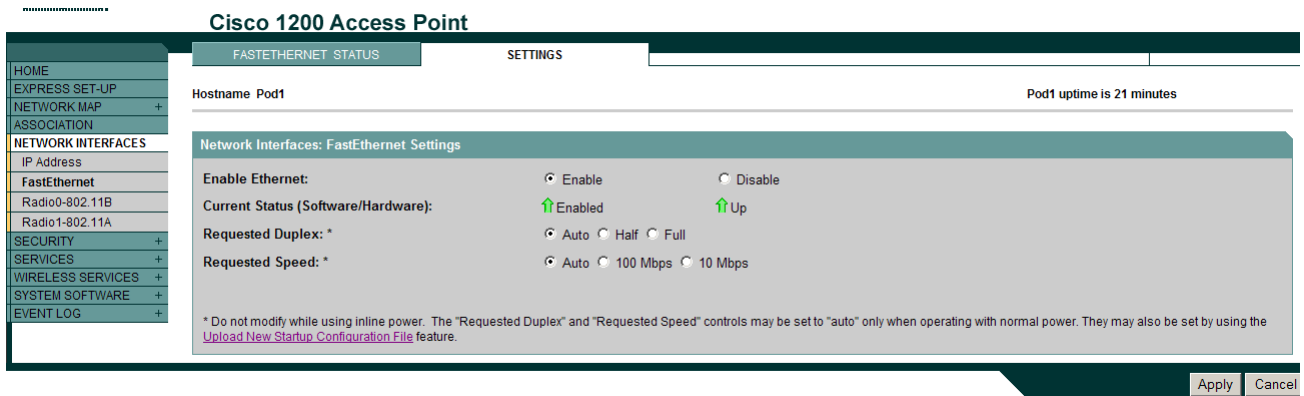
Role in Radio Network: Access Point Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

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

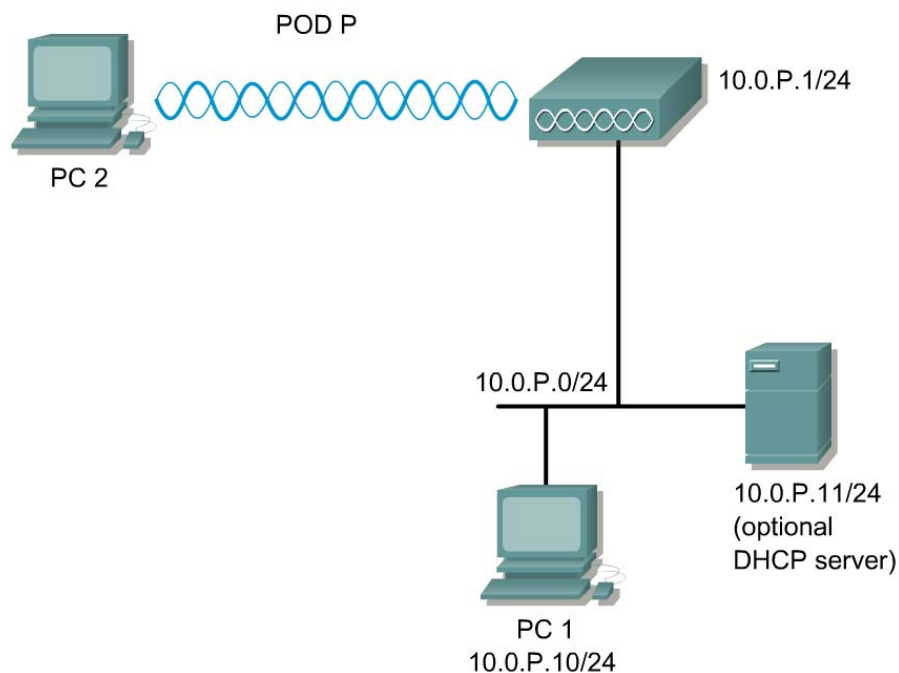
Objective

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.

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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

The screenshot shows the configuration page for a Cisco 1200 Access Point. The page title is "Cisco 1200 Access Point" and the hostname is "ap". The page shows the following information:

- Hostname: ap
- ap uptime is 17 minutes
- Home: Summary Status
- Association: Clients: 0, Repeaters: 0
- Network Identity: IP Address: 10.0.1.1, MAC Address: 000b.fd4a.700c
- Network Interfaces:

| Interface | MAC Address | Transmission Rate |
|----------------|----------------|-------------------|
| FastEthernet | 000b.fd4a.700c | 100Mb/s |
| Radio0-802.11B | 0007.85b3.c270 | 11.0Mb/s |
| Radio1-802.11A | 000b.fd01.05b7 | 54.0Mb/s |
- Event Log: (Empty table with columns: Time, Severity, Description)

- 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?

ANSWER: Answers will vary according to the devices connected to the AP.

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

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: 11.0Mb/s

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: Answers will vary according to the equipment that is issued.

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

ANSWER: 54.0Mb/s

Step 2 Network Interface settings

The screenshot shows the configuration page for a Cisco 1200 Access Point, specifically for the Radio0-802.11B interface. The page is titled "Cisco 1200 Access Point" and has a navigation menu on the left with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, FastEthernet, Radio0-802.11B, Radio1-802.11A, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Radio0-802.11B STATUS" and "DETAILED STATUS". The "SETTINGS" tab is active, showing the following configuration:

- Hostname: ap
- ap uptime is 11 minutes
- Network Interfaces: Radio0-802.11B Settings
 - Enable Radio: Enable Disable
 - Current Status (Software/Hardware): Enabled ↑ Up ↑
 - Role in Radio Network: Access Point Root (Fallback to Radio Island) Access Point Root (Fallback to Radio Shutdown) Access Point Root (Fallback to Repeater) Repeater Non-Root
 - Data Rates:

| | Best Range | Best Throughput |
|------------|---|-----------------|
| 1.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | |
| 2.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | |
| 5.5Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | |
| 11.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | |

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?

ANSWER: Answer will vary. **Example:** Enable.

- b. What is the role of this AP?

ANSWER: The role of this AP should be AP Root.

- c. What speeds are configured for the data rates?

ANSWER: All DATA RATES should be checked for **Require**.

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

ANSWER: Answer will vary. **Example:** Enable.

- e. What is the role of this AP?

ANSWER: The role of this AP should be AP Root.

f. What speeds are configured for the data rates?

ANSWER: All DATA RATES should be checked for **Require**.

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

The screenshot displays the Network Interface Settings page with the following configurations:

- Transmitter Power (mW):** 1 5 20 30 50 100 Max
- Limit Client Power (mW):** 1 5 20 30 50 100 Max
- Default Radio Channel:** Least Congested Frequency (dropdown) Channel 1 2412 Mhz
- Least Congested Channel Search:** (Use Only Selected Channels)
 - Channel 1 - 2412 MHz
 - Channel 2 - 2417 MHz
 - Channel 3 - 2422 MHz
 - Channel 4 - 2427 MHz
 - Channel 5 - 2432 MHz
 - Channel 6 - 2437 MHz
 - Channel 7 - 2442 MHz
 - Channel 8 - 2447 MHz
 - Channel 9 - 2452 MHz
 - Channel 10 - 2457 MHz
 - Channel 11 - 2462 MHz
- World Mode Multi-Domain Operation:** Enable Disable
- Radio Preamble:** Short Long
- Receive Antenna:** Diversity Left Right
- Transmit Antenna:** Diversity Left Right
- Aironet Extensions:** Enable Disable

g. What is the Transmitter Power setting?

ANSWER: Answer will vary.

h. What is the Default Radio Channel?

ANSWER: Answer will vary. **Example:** channel 1, 6 or 11.

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

| Network Interface Settings |
|----------------------------|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

ANSWER:

| Network Interface Settings |
|----------------------------------|
| Radio Preamble |
| Receive Antenna |
| Transmit Antenna |
| Aironet Extensions |
| Ethernet Encapsulation Transform |
| Reliable Multicast to RGB |
| Public Secure Packet Forwarding |
| Beacon Period |
| Max. Data Retries |
| Fragmentation Threshold |
| Repeater Parent AP Timeout |
| Beacon Period |

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

Cisco 1200 Access Point

Hostname ap ap uptime is 17 minutes

HOME
EXPRESS SET-UP
NETWORK MAP +
ASSOCIATION
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Association

Clients: 0 Repeaters: 0

View: Client Repeater Apply

Radio802.11B

| MAC | IP | Vendor | Model | Uptime | Signal | Power |
|-----|----|--------|-------|--------|--------|-------|
| | | | | | | |

Radio802.11A

| MAC | IP | Vendor | Model | Uptime | Signal | Power |
|-----|----|--------|-------|--------|--------|-------|
| | | | | | | |

Refresh

- 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.

| | | | |
|--------------------------------------|--|--|--|
| Ethernet Encapsulation Transform: | <input checked="" type="radio"/> RFC1042 | <input type="radio"/> 802.1H | |
| Reliable Multicast to WGB: | <input checked="" type="radio"/> Disable | <input type="radio"/> Enable | |
| Public Secure Packet Forwarding: | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | |
| Beacon Period: | <input type="text" value="100"/> (20-4000 Kusec) | Data Beacon Rate (DTIM): | <input type="text" value="2"/> (1-100) |
| Max. Data Retries: | <input type="text" value="32"/> (1-128) | RTS Max. Retries: | <input type="text" value="32"/> (1-128) |
| Fragmentation Threshold: | <input type="text" value="2346"/> (256-2346) | RTS Threshold: | <input type="text" value="2312"/> (0-2347) |
| Repeater Parent AP Timeout: | <input type="text" value="0"/> (0-65535 sec) | | |
| Repeater Parent AP MAC 1 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 2 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 3 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |
| Repeater Parent AP MAC 4 (optional): | <input type="text"/> (HHHH.HHHH.HHHH) | | |

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

ANSWER: Answers will vary. **Example:** Enable

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

ANSWER: Answers will vary. **Example:** Disable

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

ANSWER: Answers will vary. **Example:** 100

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

ANSWER: Answers will vary. **Example:** 2

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

ANSWER: Answers will vary. **Example:** 32

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

ANSWER: Answers will vary. **Example:** 32

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

ANSWER: Answers will vary. **Example:** 2346, Unit is bytes

- h. What is the RTS Threshold setting?

ANSWER: Answers will vary. **Example:** 2312

- i. What is Repeater Parent AP timeout?

ANSWER: Answers will vary. **Example:** Disabled

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

ANSWER: Answers will vary. **Example:** Disabled

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

ANSWER: Answers will vary. **Example:** Disabled

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

ANSWER: Answers will vary. **Example:** Disabled

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

ANSWER: Answers will vary. **Example:** Disabled

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?

ANSWER: Answers will vary.

b. Which antenna setting had the worst performance?

ANSWER: Answers will vary.

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?

ANSWER: Answers will vary.

d. Which channel setting had the worst performance?

ANSWER: Answers will vary.

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.

ANSWER: Answers will vary. **Example:** Generally as you decrease the transmitter power settings your range decreases and the data rate will shift lower to accommodate the increased range.

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

ANSWER: Answers will vary.

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

ANSWER: Answers will vary.

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.

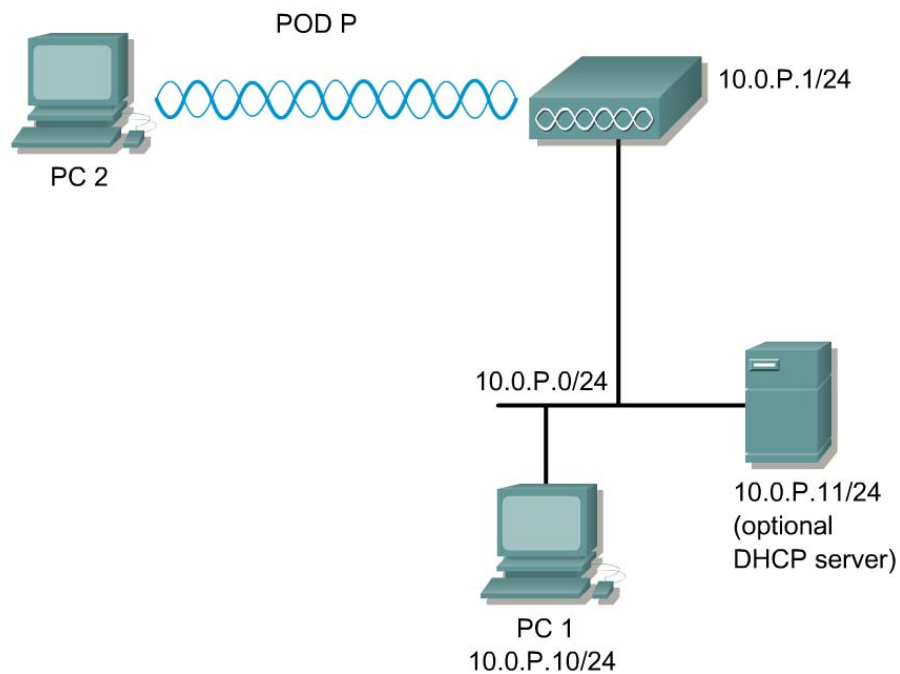
Objective

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

ANSWER: ?

Step 12 Configuring the Role in Radio Network

Configure the AP as a root AP:

- a. What command is needed?

ANSWER: PodP(config-if)#station-role root

Step 13 Configuring Radio Data Rates

View the available data rates for the 11a radio.

- a. What command is needed?

ANSWER: PodP(config-if)#speed ?

b. What speeds are available?

ANSWER:

```
12.0      Allow 12 Mb/s rate
18.0      Allow 18 Mb/s rate
24.0      Allow 24 Mb/s rate
36.0      Allow 36 Mb/s rate
48.0      Allow 48 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-12.0 Require 12 Mb/s rate
basic-18.0 Require 18 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-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>
```

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?

ANSWER:

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


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?

ANSWER:

```
PodP(config-if) #power local ?  
<5-40> One of: 5 10 20 40  
maximum Set local power to allowed maximum
```

Configure the AP radio power to 10 mW.

- c. What command is needed?

ANSWER:

```
PodP(config-if) #power local 10
```

Configure the client radio transmit power to 40 mW.

- d. What command is needed?

ANSWER:

```
PodP(config-if) #power client 40
```

Now lower the setting to 5mw.

- e. What command is needed?

ANSWER:

```
PodP(config-if) #power client 5
```

Step 15 Configuring Radio Channel Settings

See what 11a channels are available.

- a. What command is needed? What channels are available?

ANSWER:

```
PodP(config-if) #channel ?  
<36-5320> One of: 36 40 44 48 52 56 60 64 5180 5200 5220  
5240 5260 5280 5300 5320  
least-congested Scan for best frequency
```

Assign static channel 36 to the AP.

- b. What command is needed?

ANSWER:

```
PodP(config-if)#channel 36 (5180)
```

Now assign a least congested channel setting for the AP.

- c. What command is needed?

ANSWER:

```
PodP(config-if)#channel least-congested
```

Step 16 Configuring Transmit and Receive Antennas

View the available antenna settings.

- a. What command is needed? What settings are available?

ANSWER:

```
PodP(config-if)#antenna ?  
receive receive antenna setting  
transmit transmit antenna setting
```

Configure the AP to receive and transmit to right. (the interfaces will reset after each change.)

- b. What commands are needed?

ANSWER:

```
PodP(config-if)#antenna receive right  
PodP(config-if)#antenna transmit right
```

Set the AP to receive and transmit to left.

- c. What commands are needed?

ANSWER:

```
PodP(config-if)#antenna receive left  
PodP(config-if)#antenna transmit left
```

Set the AP back to receive and transmit to diversity.

- d. What commands are needed?

ANSWER:

```
PodP(config-if) #antenna receive diversity  
PodP(config-if) #antenna transmit diversity
```

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?

ANSWER:

```
PodP(config-if) #shutdown  
PodP(config-if) #no shutdown
```

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

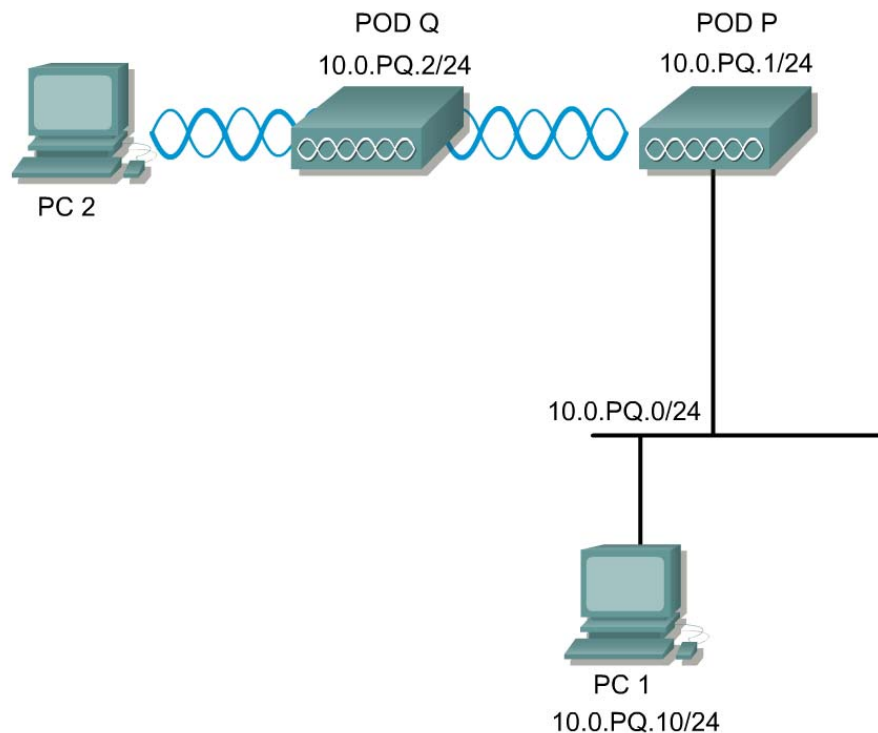
The student will extend the coverage of a basic service set topology by implementing an AP as a repeater.

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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------------|-------------|----------------|
| 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 confirm that the APs are configured and operational and clients can connect to the APs.

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 “**APPQ**”. 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 PodP, verify that PodQ 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?

ANSWER:

```
H.H.H Detailed client status
all-client Detailed status of all clients
bss-only Associations in BSS
client client information
repeater repeater information
statistics association statistics
| Output modifiers
```

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?

Answer: Yes; use the AP2#show dot11 associations command

```
Pod2#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [AP12] :
```

| MAC Address | IP address | Device | Name | Parent | State |
|----------------|------------|---------------|------|--------|-------|
| 0007.85b3.8850 | 10.0.12.2 | ap1200-Parent | AP2 | - | Assoc |
| 0007.eb30.a37d | 10.0.12.30 | 350-client | VIAO | self | Assoc |

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 6.3.6 Configure Site-to-Site Wireless Link

Estimated Time: 60 minutes

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

Objective

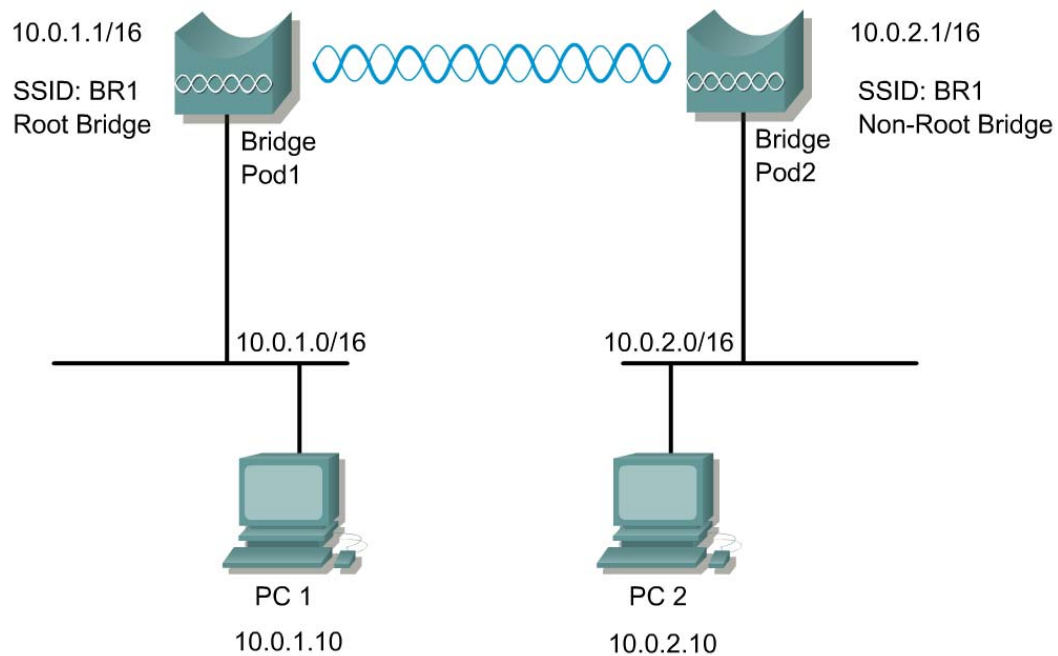
Configure a site-to-site bridged network.

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:
 - i. The **Summary Status** Page, also known as the **Home** Page
 - ii. The **Express Setup** Page

BR350-5aa7d6 Summary Status
Cisco 350 Series Bridge 12.03T

Home Map Network Associations Setup **Logs** Help

Uptime: 00:13:00

Current Associations

| | | | |
|-----------------|-------------------|-----------------|--------|
| Clients: 0 of 0 | Repeaters: 0 of 0 | Bridges: 0 of 1 | APs: 0 |
|-----------------|-------------------|-----------------|--------|

Recent Events

| Time | Severity | Description |
|------|----------|-------------|
| | | |

Network Ports *Diagnostics*

| Device | Status | Mb/s | IP Addr. | MAC Addr. |
|------------|--------|-------|----------|--------------|
| Ethernet | Up | 100.0 | 10.0.0.1 | 0040965aa7d6 |
| Root Radio | Up | 11.0 | 10.0.0.1 | 0040965aa7d6 |

BR350-5aa7d6 Express Setup
Cisco 350 Series Bridge 12.03T

Home Map Help

Uptime: 00:14:22

System Name: BR350-5aa7d6

MAC Address: 00:40:96:5a:a7:d6

Configuration Server Protocol: DHCP

Default IP Address: 10.0.0.1

Default IP Subnet Mask: 255.255.255.0

Default Gateway: 255.255.255.255

Root Radio:

Service Set ID (SSID): tsunami [more...](#)

Role in Radio Network: Root Bridge

Optimize Radio Network For: Throughput Range Custom

Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community:

Apply OK Cancel Restore Defaults

- 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.

BR350-5aa7d6 Setup CISCO SYSTEMS

Cisco 350 Series Bridge 12.03T Uptime: 00:17:25

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Express Setup

Associations

| | | | |
|----------------------------------|----------------------------------|----------------------------------|------------------------------|
| Display Defaults | Spanning Tree | Port Assignments | Advanced |
| Address Filters | Protocol Filters | VLAN | Service Sets |

Event Log

| | | |
|----------------------------------|--------------------------------|-------------------------------|
| Display Defaults | Event Handling | Notifications |
|----------------------------------|--------------------------------|-------------------------------|

Services

| | | | |
|--------------------------------|-----------------------------|----------------------------|---------------------------------|
| Console/Telnet | Boot Server | Routing | Name Server |
| Time Server | FTP | Web Server | SNMP |
| Cisco Services | Security | Accounting | Proxy Mobile IP |

Network Ports [Diagnostics](#)

| | | | | |
|----------------------------|--------------------------------|--------------------------|-------------------------|--------------------------|
| Ethernet | Identification | Hardware | Filters | Advanced |
| Root Radio | Identification | Hardware | Filters | Advanced |

- f. Now click on the **Express Setup** link. This will now bring up the Express Setup Page.

Step 4 Configure the bridge settings

BR350-5aa7d6 Express Setup CISCO SYSTEMS

Cisco 350 Series Bridge 12.03T Uptime: 00:23:24

[Home](#) [Map](#) [Help](#)

System Name:

MAC Address:

Configuration Server Protocol:

Default IP Address:

Default IP Subnet Mask:

Default Gateway:

Root Radio:

Service Set ID (SSID): [more...](#)

Role in Radio Network:

Optimize Radio Network For: Throughput Range Custom

Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community:

Configure the following settings:

| Parameter | BPod1 | BPod2 |
|--|---------------------------|---|
| a. System Name: | <i>BPod1</i> | <i>BPod2</i> |
| b. Configuration Server Protocol: | <i>None</i> | <i>None</i> |
| c. Default IP address: | <i>10.0.1.1</i> | <i>10.0.2.1</i> |
| d. Default Gateway: | <i>10.0.1.254</i> | <i>10.0.1.254</i> |
| e. Service Set ID: | <i>BR1</i> | <i>BR1</i> |
| f. Role in Radio Network: | <i>Root Bridge</i> | <i>Non-Root Bridge w/o Clients</i> |
| 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?


Root Bridge
Non-Root Bridge w/Clients
Non-Root Bridge w/o Clients
Root Access Point
Repeater Access Point
ANSWER: Site Survey Client

Step 5 Advanced radio settings for the non-root bridge

BPod1 Setup

Cisco 350 Series Bridge 12.03T

[Home](#) | [Map](#) | [Network](#) | [Associations](#) | [Setup](#) | [Logs](#) | [Help](#)



Uptime: 00:39:27

Express Setup

| Associations | | | | |
|----------------------------------|----------------------------------|----------------------------------|------------------------------|--|
| Display Defaults | Spanning Tree | Port Assignments | Advanced | |
| Address Filters | Protocol Filters | VLAN | Service Sets | |

Event Log

| | | |
|----------------------------------|--------------------------------|-------------------------------|
| Display Defaults | Event Handling | Notifications |
|----------------------------------|--------------------------------|-------------------------------|

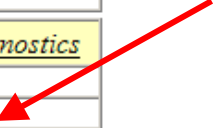
Services

| | | | |
|--------------------------------|-----------------------------|----------------------------|---------------------------------|
| Console/Telnet | Boot Server | Routing | Name Server |
| Time Server | FTP | Web Server | SNMP |
| Cisco Services | Security | Accounting | Proxy Mobile IP |

Network Ports

Diagnostics

| | | | | |
|----------------------------|--------------------------------|--------------------------|-------------------------|--------------------------|
| Ethernet | Identification | Hardware | Filters | Advanced |
| Root Radio | Identification | Hardware | Filters | Advanced |



- a. From the **Setup** Page, Click on the Root Radio>Advanced link to go to the **Radio Advanced** page of the Non-Root Bridge.

BPod1 Bridge Radio Advanced



Cisco 350 Series Bridge 12.03T

[Map](#) [Help](#)

Uptime: 00:44:08

| | |
|--|---|
| Requested Status: | Up |
| Current Status: | Up |
| Packet Forwarding: | Enabled |
| Forwarding State: | Blocking |
| Default Multicast Address Filter: | Allowed |
| Maximum Multicast Packets/Second: | 0 |
| Radio Cell Role: | Client/Non-Root |
| SSID for use by Infrastructure Stations (such as Repeaters): | 0 |
| Disallow Infrastructure Stations on any other SSID: | <input type="radio"/> yes <input checked="" type="radio"/> no |
| Use Aironet Extensions: | <input checked="" type="radio"/> yes <input type="radio"/> no |
| Classify Workgroup Bridges as Network Infrastructure: | <input checked="" type="radio"/> yes <input type="radio"/> no |
| Require use of Internal Radio Firmware: 5.20U | <input checked="" type="radio"/> yes <input type="radio"/> no |
| Ethernet Encapsulation Transform: | RFC1042 |
| Bridge Spacing (km): | 0 |

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs are enabled, the following three parameters are set independently for each enabled VLAN through [VLAN Setup](#).

| | |
|--|-----------|
| Enhanced MIC verification for WEP: | None |
| Temporal Key Integrity Protocol: | None |
| Broadcast WEP Key rotation interval (sec): | 0 (0=off) |

To configure 802.11 Authentication, EAP, Unicast Address Filters, and the Maximum Number of Associations for this radio's Primary SSID (the default SSID), please use the link below.

[Advanced Primary SSID Setup more...](#)

| | |
|---------------------------|-------------------|
| Preferred Access Point 1: | 00:00:00:00:00:00 |
| Preferred Access Point 2: | 00:00:00:00:00:00 |
| Preferred Access Point 3: | 00:00:00:00:00:00 |
| Preferred Access Point 4: | 00:00:00:00:00:00 |
| Radio Modulation: | Standard |
| Radio Preamble: | Short |
| Non-Root Mobility: | Stationary |

[Apply](#) [OK](#) [Cancel](#) [Restore Defaults](#)

- 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.

BPod1 Summary Status

Cisco 350 Series Bridge 12.03T

Uptime: 00:46:31

Home Map Network Associations Setup Logs Help

Current Associations

| | | | |
|-----------------|-------------------|-----------------|--------|
| Clients: 0 of 0 | Repeaters: 0 of 0 | Bridges: 0 of 1 | APs: 0 |
|-----------------|-------------------|-----------------|--------|

Recent Events

| Time | Severity | Description |
|------|----------|-------------|
|------|----------|-------------|

Network Ports *Diagnostics*

| Device | Status | Mb/s | IP Addr. | MAC Addr. |
|------------|--------|-------|----------|--------------|
| Ethernet | Up | 100.0 | 10.0.1.1 | 0040965aa7d6 |
| Root Radio | Up | 11.0 | 10.0.1.1 | 0040965aa7d6 |

b. Click the **Apply** button to apply the settings.

BPod1 Association Table

Network Diagnostics VLAN Service Sets

Uptime: 00:47:47

Home Map Network Associations Setup Logs Help

Client Repeater Bridge AP Infra. Host Multicast Entire Network

Press to Change Settings: Apply Save as Default Restore Current Defaults

Association Table *additional display filters?*

| Device | Name | IP Addr./Name | MAC Addr. | VLAN | State | Parent |
|-------------------|-------|---------------|--------------|------|-------|--------|
| 350 Series Bridge | BPod1 | 10.0.1.1 | 0040965aa7d6 | | | |

1. Go to the **Associations** page of the Root Bridge. Is the Non-Root Bridge in the Association table?

ANSWER: Yes

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?

ANSWER: Yes

- 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?

ANSWER: This should range from 4 to 7 Mbps

2. How was this calculated?

ANSWER: Divide the total size of the file in bits by the time in seconds

3. What is the speed limitation?

ANSWER: Can be write speed of the PC if below 6Mbps. If it is above 6Mbps, then the limitation is the wireless link.



Lab 6.4.4 Configure Bridge Services

Estimated Time: 30 minutes

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

Objective

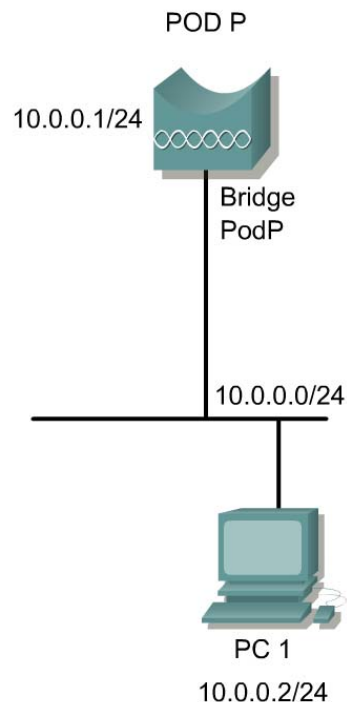
In this lab, students will configure the identity services, IP routing table, console parameters, and the time server parameters of the bridge unit.

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**.

AP1 **Boot Server Setup**

Cisco 350 Series Bridge 12.01T1

[Map](#) [Help](#)



Uptime: 24 days, 01:22:37

| | |
|---|--|
| Configuration Server Protocol: | None |
| Use previous Configuration Server settings when no server responds? | <input checked="" type="radio"/> yes <input type="radio"/> no |
| Read ".ini" file from file server? | if specified by server |
| | <input type="button" value="Load Now"/> |
| Current Boot Server: | 0.0.0.0 |
| Specified ".ini" File Server: | 0.0.0.0 |
| BOOTP Server Timeout (sec): | 120 |
| DHCP Multiple-Offer Timeout (sec): | 5 |
| DHCP Requested Lease Duration (min): | 1440 |
| DHCP Minimum Lease Duration (min): | 0 |
| DHCP Client Identifier Type: | Ethernet (10Mb) |
| DHCP Client Identifier Value: | |
| DHCP Class Identifier: | AP4800E |
| | <input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Restore Defaults"/> |

Select the Identity process, Configuration Server Protocol that the bridge will use.

There are three options:

- **None** – Disable 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?

ANSWER: The BOOTP selection is a bootstrap protocol that allows the host device to configure itself with a scaled configuration file. The configuration file is most commonly embedded in the devices firmware.

Step 2 Configuring the IP routing table parameters of the bridge unit

From the Setup page in the Services section, select the **Routing** option.

AP1 **Routing Setup**

Cisco 350 Series Bridge 12.01T1

[Map](#) [Help](#) Uptime: 24 days, 01:24:15

Default Gateway:


New Network Route:

Dest Network:

Gateway:

Subnet Mask:

Installed Network Routes:



[\[Map\]](#)[\[Login\]](#)[\[Help\]](#)

Cisco 350 Series Bridge 12.01T1

© Copyright 2002 [Cisco Systems, Inc.](#)

[credits](#)

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:
 - a. Dest. Network:

ANSWER: Answers will vary. **Example:** blank by default

- b. Gateway:

ANSWER: Answers will vary. **Example:** 255.255.255.255 by default

- c. Subnet Mask:

ANSWER: Answers will vary.

Step 3 Configuring the console/Telnet parameters of the bridge unit

From the Setup page in the Services section, select the **Console/Telnet** option.

AP1 Console/Telnet Setup

Cisco 350 Series Bridge 12.01T1

[Map](#) [Help](#)

CISCO SYSTEMS



Uptime: 24 days,
01:25:07

| | |
|--|---|
| Baud Rate: | 9600 |
| Parity: | None |
| Data Bits: | 8 |
| Stop Bits: | 1 |
| Flow Control: | SW Xon/Xoff |
| Terminal Type: | teletype |
| Columns (64-132): | 80 |
| Lines (16-50): | 24 |
| Telnet: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Apply OK Cancel Restore Defaults | |

[\[Map\]](#)[\[Login\]](#)[\[Help\]](#)

Cisco 350 Series Bridge 12.01T1

© Copyright 2002 [Cisco Systems, Inc.](#)

[credits](#)

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

ANSWER: Baud Rate is 9600.

b. Parity

ANSWER: Parity is None.

c. Data Bits

ANSWER: Data Bits is 8.

d. Stop Bits

ANSWER: Stop Bits is 1.

e. Flow Control

ANSWER: Flow Control is **Xon/Xoff** 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.

AP1 Time Server Setup

Cisco 350 Series Bridge 12.01T1



[Map](#) [Help](#)

Uptime: 24 days, 01:25:49

Simple Network Time Protocol (SNTP): Enabled Disabled

Default Time Server:

Current Time Server:

GMT Offset (hr): (GMT - 05:00) Eastern Time (US & canada)

Use Daylight Savings Time: yes no

Manually set date (YYYY/MM/DD):

Manually set time (HH:MM:SS):

[\[Map\]](#)[\[Login\]](#)[\[Help\]](#)

Cisco 350 Series Bridge 12.01T1

© Copyright 2002 Cisco Systems, Inc.

[credits](#)

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 from 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?

ANSWER: The time changing utility is necessary when the time zone in your area changes and you wish to keep the time setting accurate.

- Change the time back to the current time.



Lab 6.5.3 Manage Bridge Configuration and Image Files

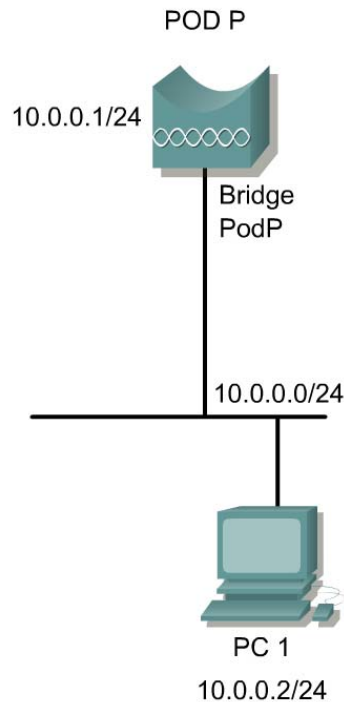
Estimated Time: 20 minutes

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.

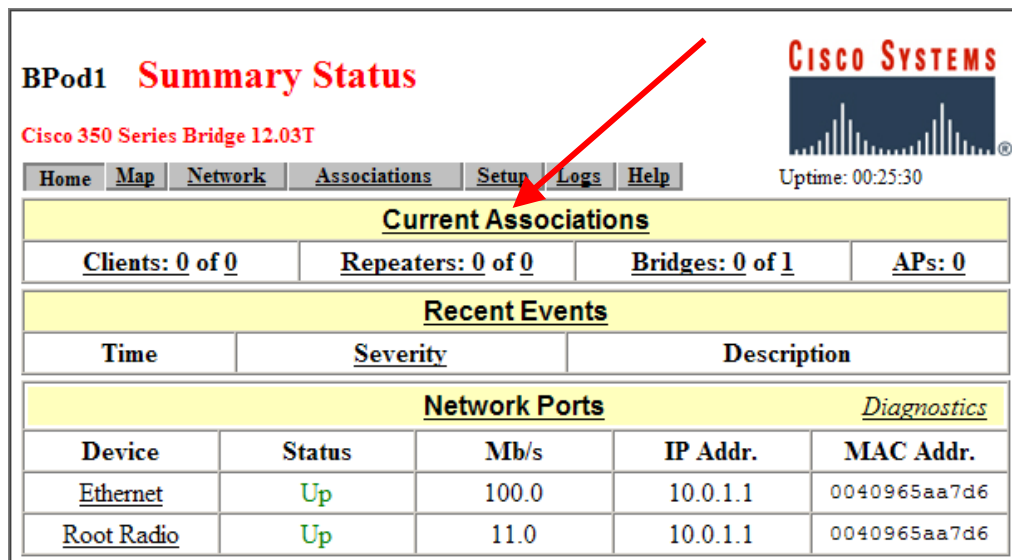
Tools and Resources

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:



BPod1 Summary Status

Cisco 350 Series Bridge 12.03T

Home Map Network Associations **Setup** Logs Help

Uptime: 00:25:30

Current Associations

| | | | |
|------------------------|--------------------------|------------------------|---------------|
| <u>Clients: 0 of 0</u> | <u>Repeaters: 0 of 0</u> | <u>Bridges: 0 of 1</u> | <u>APs: 0</u> |
|------------------------|--------------------------|------------------------|---------------|


Recent Events

| Time | Severity | Description |
|------|----------|-------------|
|------|----------|-------------|

Network Ports *Diagnostics*

| Device | Status | Mb/s | IP Addr. | MAC Addr. |
|-------------------|--------|-------|----------|--------------|
| <u>Ethernet</u> | Up | 100.0 | 10.0.1.1 | 0040965aa7d6 |
| <u>Root Radio</u> | Up | 11.0 | 10.0.1.1 | 0040965aa7d6 |

- a. On PC1, open a web browser and access the bridge. From the Home page, click on the Setup tab.

BPod1 Setup **CISCO SYSTEMS**


Cisco 350 Series Bridge 12.03T Uptime: 00:27:55

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Express Setup

Associations

| | | | |
|----------------------------------|----------------------------------|----------------------------------|------------------------------|
| Display Defaults | Spanning Tree | Port Assignments | Advanced |
| Address Filters | Protocol Filters | VLAN | Service Sets |

Event Log


| | | |
|----------------------------------|--------------------------------|-------------------------------|
| Display Defaults | Event Handling | Notifications |
|----------------------------------|--------------------------------|-------------------------------|

Services


| | | | |
|--------------------------------|-----------------------------|----------------------------|---------------------------------|
| Console/Telnet | Boot Server | Routing | Name Server |
| Time Server | FTP | Web Server | SNMP |
| Cisco Services | Security | Accounting | Proxy Mobile IP |

Network Ports *Diagnostics*

| | | | | |
|----------------------------|--------------------------------|--------------------------|-------------------------|--------------------------|
| Ethernet | Identification | Hardware | Filters | Advanced |
| Root Radio | Identification | Hardware | Filters | Advanced |



b. From the Services section, select **Cisco Services**.

BPod1 Cisco Services Setup **CISCO SYSTEMS**


Cisco 350 Series Bridge 12.03T Uptime: 00:29:23

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

[Manage Installation Keys](#)

[Manage System Configuration](#)

[Distribute Configuration to other Cisco Devices](#)

[Distribute Firmware to other Cisco Devices](#)

[Hot Standby Management](#)

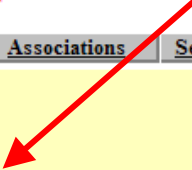
[Cisco Discovery Protocol \(CDP\)](#)

Fully Update Firmware: [Through Browser](#) [From File Server](#)

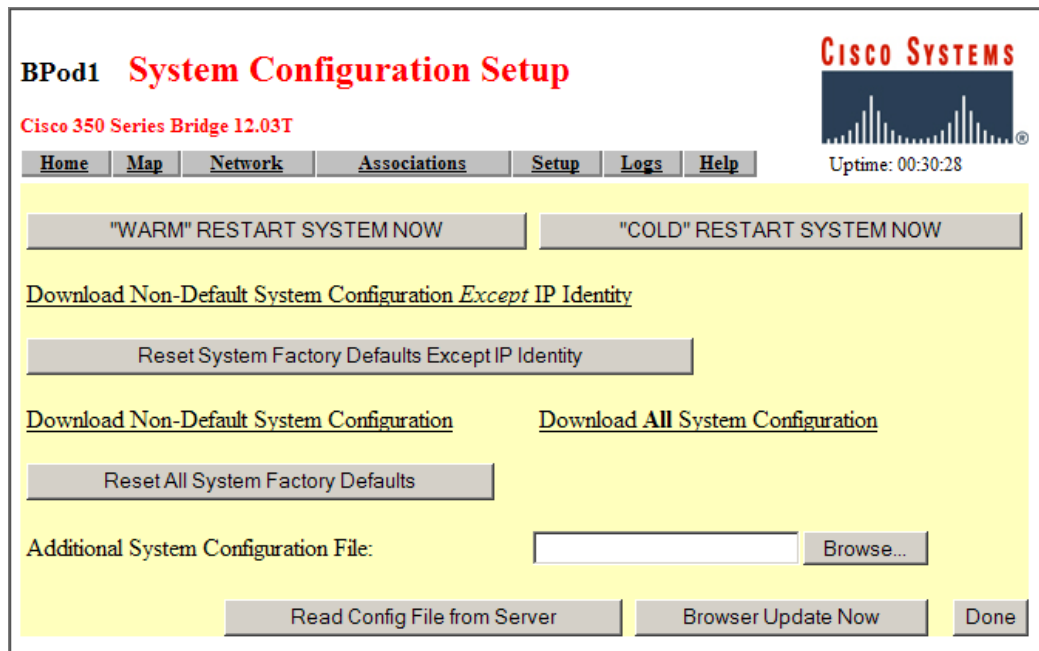
Selectively Update Firmware: [Through Browser](#) [From File Server](#)

Locate unit by flashing LEDs: Enabled Disabled

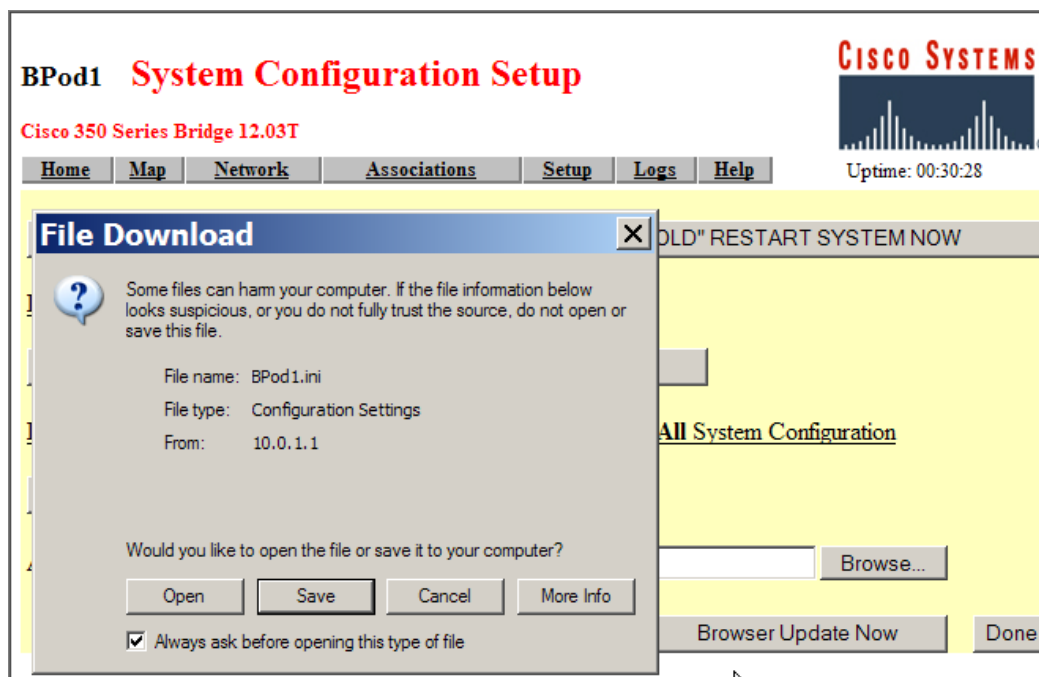
[Apply](#) [OK](#) [Cancel](#) [Restore Defaults](#)



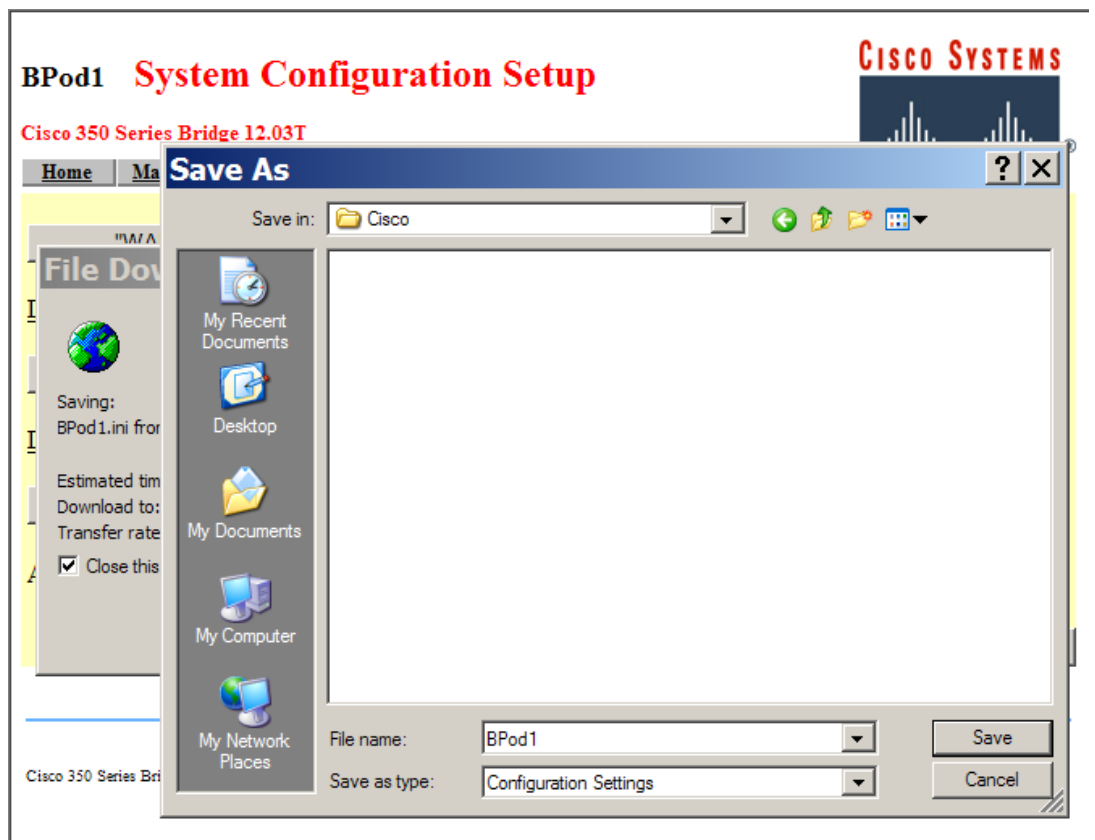
c. Click on the **Manage System Configuration** link.



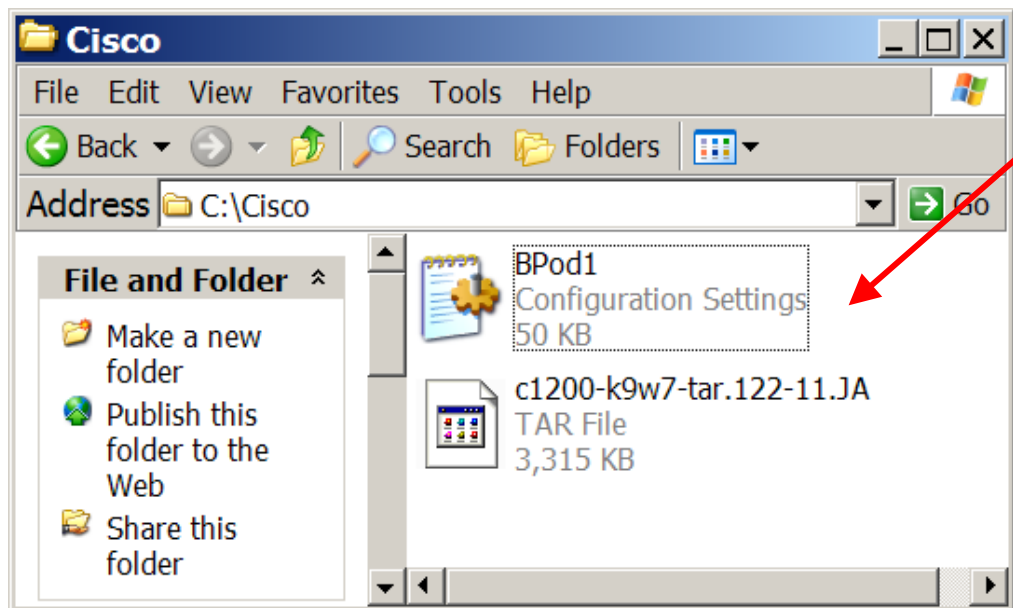
d. Click on the **Download All System Configuration** button.



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.

```
File Edit Format View Help
#===Beginning of BPod1 (Cisco 350 Series Bridge 12.03T)
Configuration File===
dot11AuthenticationResponseTimeOut.2=2000
dot11PowerManagementMode.2=active
dot11DesiredSSID.2=BR1
dot11OperationalRateSet.2=\x82\x84\x8b\x96
dot11BeaconPeriod.2=100
dot11DTIMPeriod.2=2
dot11AssociationResponseTimeOut.2=2000
dot11MultiDomainCapabilityEnabled.2=false
dot11AuthenticationAlgorithmsEnable.2.1=true
dot11AuthenticationAlgorithmsEnable.2.2=false
dot11AuthenticationAlgorithmsEnable.2.3=false
dot11PrivacyInvoked.2=false
dot11WEPDefaultKeyID.2=0
dot11WEPKeyMappingLength.2=0
dot11ExcludeUnencrypted.2=false
dot11RTSThreshold.2=2339
dot11ShortRetryLimit.2=32
dot11LongRetryLimit.2=32
dot11FragmentationThreshold.2=2338
dot11MaxTransmitMSDULifetime.2=5000
dot11MaxReceiveLifetime.2=10000
dot11ChannelAgilityEnabled.2=false
dot11CurrentTxAntenna.2=diversity
dot11CurrentRxAntenna.2=diversity
dot11CurrentTxPowerLevel.2=6
dot11CurrentDwellTime.2=19
dot11CurrentSet.2=1
dot11CurrentPattern.2=1
dot11CurrentChannel.2=6
dot11CurrentCCAMode.2=1
sysContact=Aironet Wireless Communications, Inc.
sysName=BPod1
```

- 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

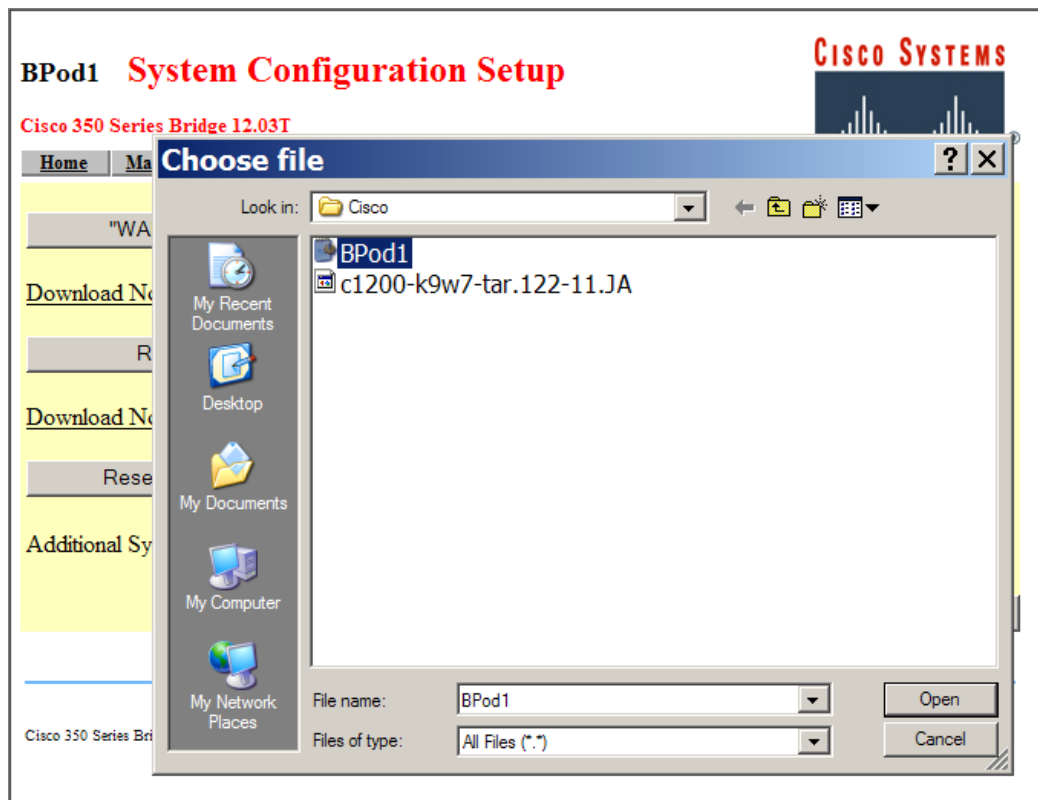
If the configuration is ever lost or corrupted, it can be restored by using the Additional System Configuration File. This is an option from the **Cisco Services Setup** menu or page to move the configuration file into the bridge. The system automatically restores the configuration based on these commands.

In order to load a configuration file, complete the following steps:

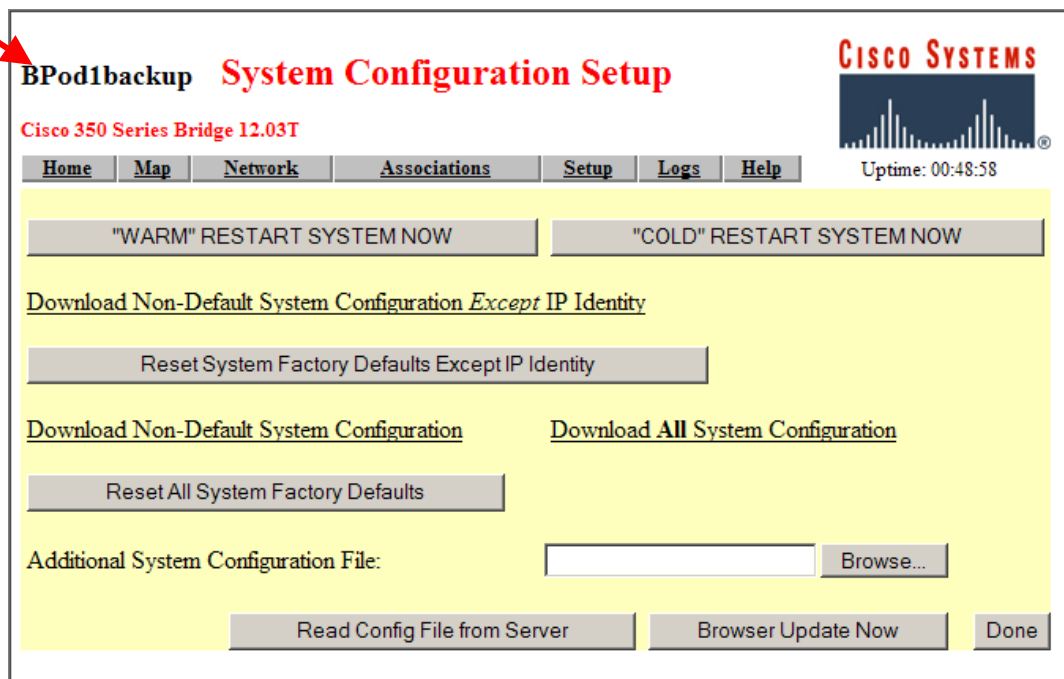
- a. On the **Cisco Services Setup** page, click on the **Manage System Configuration** button.

The screenshot shows the Cisco Services Setup interface for BPod1. The page title is "BPod1 System Configuration Setup" and it is for a "Cisco 350 Series Bridge 12.03T". The page has a navigation menu with "Home", "Map", "Network", "Associations", "Setup", "Logs", and "Help". The "Setup" menu is active. The page contains several buttons: "WARM" RESTART SYSTEM NOW, "COLD" RESTART SYSTEM NOW, "Reset System Factory Defaults Except IP Identity", "Reset All System Factory Defaults", and "Browse..." (highlighted with a red arrow). There is also an "Additional System Configuration File:" field with a text input and a "Browse..." button. At the bottom, there are buttons for "Read Config File from Server", "Browser Update Now", and "Done".

- 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.

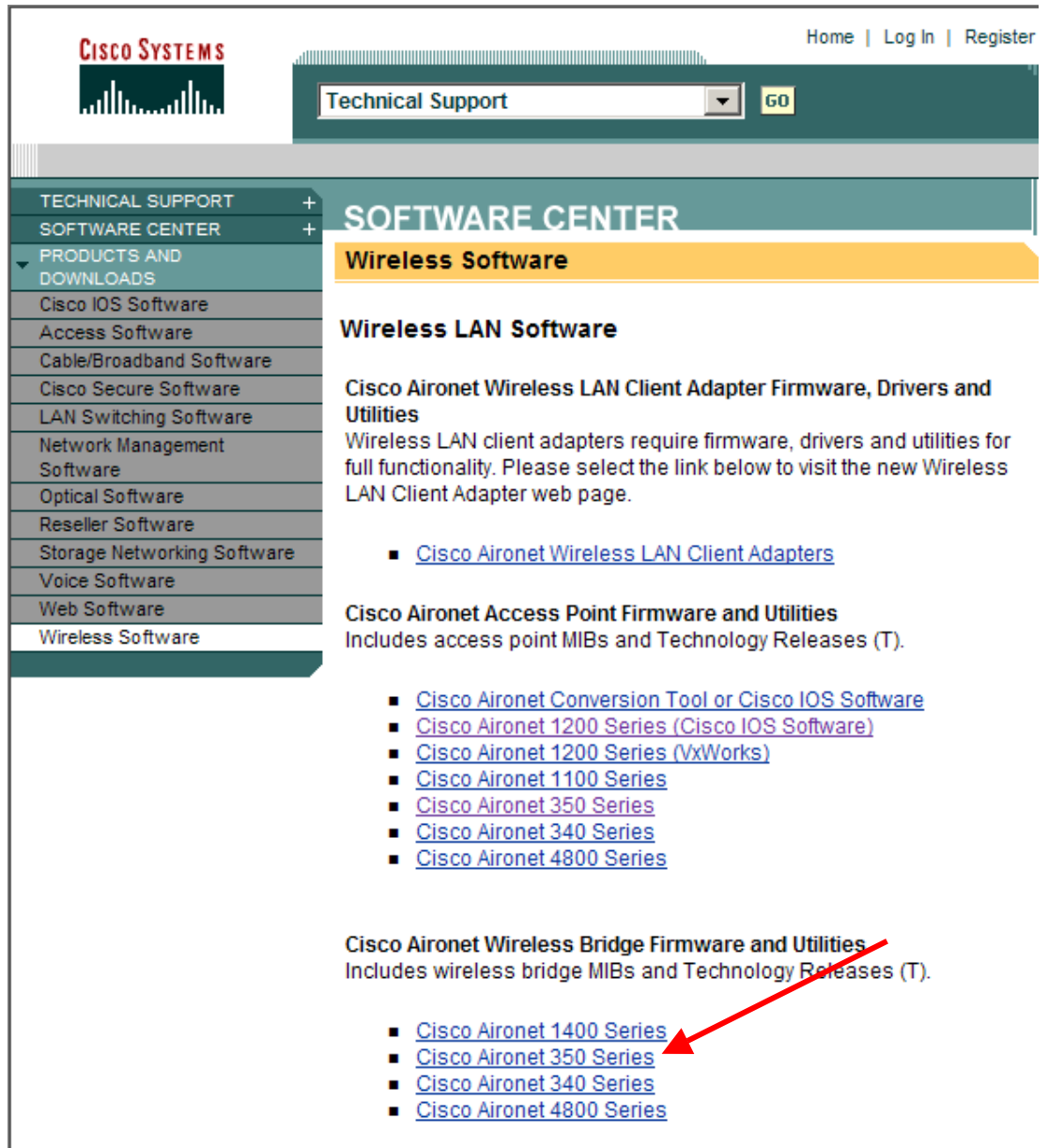
1. Was it possible to load the saved configuration file into the current configuration of the bridge? How is this confirmed?

ANSWER: Yes, the saved configuration file was successfully uploaded into the AP/bridges configuration.

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:



The screenshot shows the Cisco Systems Software Center website. The top navigation bar includes the Cisco Systems logo, a search box with 'Technical Support' entered, and links for 'Home', 'Log In', and 'Register'. A left sidebar menu lists various software categories, with 'Wireless Software' selected. The main content area is titled 'SOFTWARE CENTER' and 'Wireless Software'. It features three sections: 'Wireless LAN Software' with a link to 'Cisco Aironet Wireless LAN Client Adapters'; 'Cisco Aironet Access Point Firmware and Utilities' with a list of links including 'Cisco Aironet Conversion Tool or Cisco IOS Software', 'Cisco Aironet 1200 Series (Cisco IOS Software)', 'Cisco Aironet 1200 Series (VxWorks)', 'Cisco Aironet 1100 Series', 'Cisco Aironet 350 Series', 'Cisco Aironet 340 Series', and 'Cisco Aironet 4800 Series'; and 'Cisco Aironet Wireless Bridge Firmware and Utilities' with a list of links including 'Cisco Aironet 1400 Series', 'Cisco Aironet 350 Series', 'Cisco Aironet 340 Series', and 'Cisco Aironet 4800 Series'. A red arrow points to the 'Cisco Aironet 350 Series' link in the third section.

- a. Download the latest BR350 image from Cisco.com. Save the image file on PC1.

BPod1 Cisco Services Setup **CISCO SYSTEMS**

Uptime: 01:10:03

Cisco 350 Series Bridge 12.03T

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

[Manage Installation Keys](#)

[Manage System Configuration](#)

[Distribute Configuration to other Cisco Devices](#)

[Distribute Firmware to other Cisco Devices](#)

[Hot Standby Management](#)


[Cisco Discovery Protocol \(CDP\)](#)

Fully Update Firmware: [Through Browser](#) [From File Server](#)

Selectively Update Firmware: [Through Browser](#) [From File Server](#)

Locate unit by flashing LEDs: Enabled Disabled

- b. From the **Cisco Services Setup** Page, click on the **Fully Update Firmware: Through Browser** link.

BPod1 Update All Firmware Through Browser **CISCO SYSTEMS**

Uptime: 01:14:02

Cisco 350 Series Bridge 12.03T

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Current Version of System Firmware: 12.03

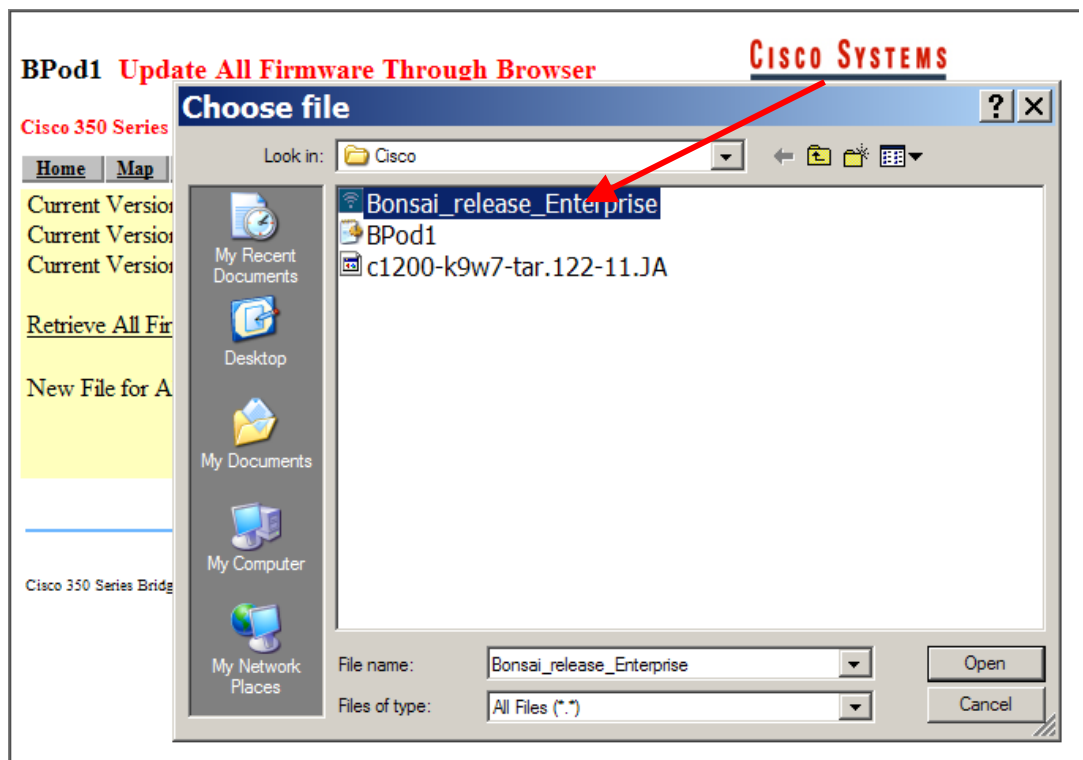
Current Version of Web Pages: 12.03

Current Version of Internal Radio Firmware: 5.20U

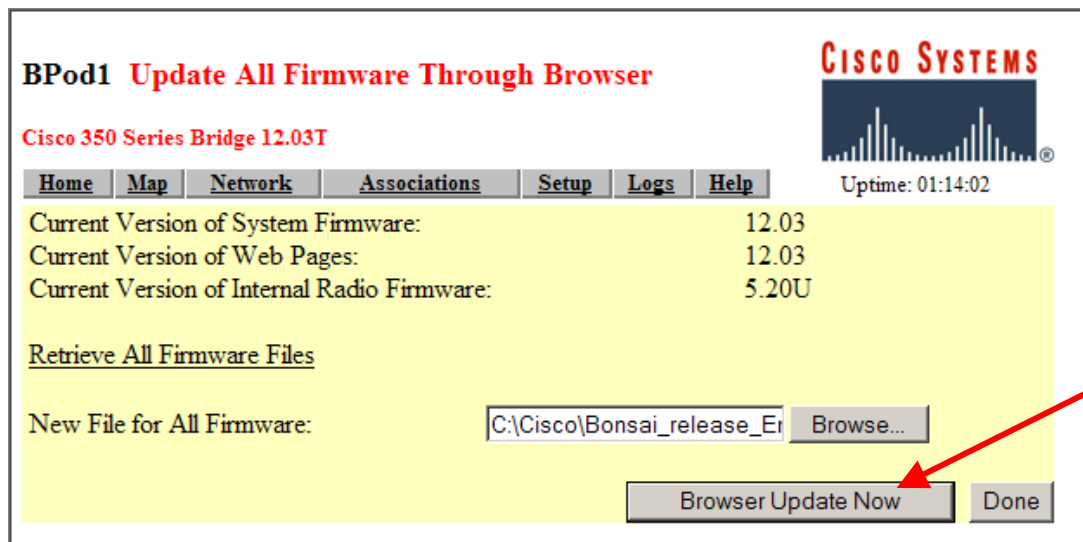
[Retrieve All Firmware Files](#)

New File for All Firmware:

- 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:

BPod1backup Cisco Services Setup

Cisco 350 Series Bridge 12.03T

Home Map Network Associations Setup Logs Help

Uptime: 00:59:08

Manage Installation Keys

Manage System Configuration

Distribute Configuration to other Cisco Devices

Distribute Firmware to other Cisco Devices

Hot Standby Management

Cisco Discovery Protocol (CDP)

Fully Update Firmware: Through Browser From File Server
Selectively Update Firmware: Through Browser From File Server

Locate unit by flashing LEDs: Enabled Disabled

Apply OK Cancel Restore Defaults

- Click on the **Distribute Firmware to other Cisco Devices** from the **Cisco Services Setup** page.

BPod1backup Distribute Firmware

Cisco 350 Series Bridge 12.03T

Home Map Network Associations Setup Logs Help

Uptime: 00:53:12

Current User: User Manager Not Enabled

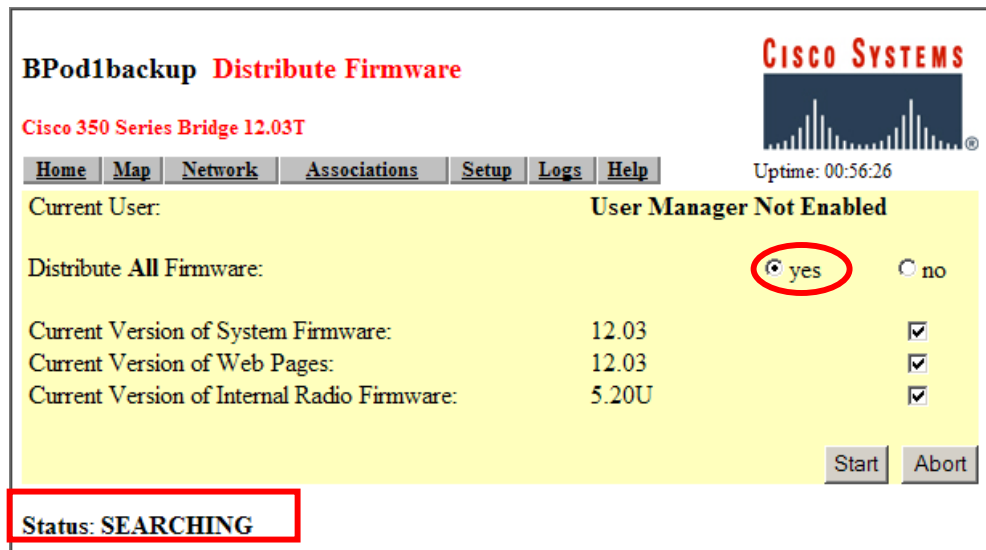
Distribute All Firmware: yes no

Current Version of System Firmware: 12.03
Current Version of Web Pages: 12.03
Current Version of Internal Radio Firmware: 5.20U

Start Abort

Status: INACTIVE

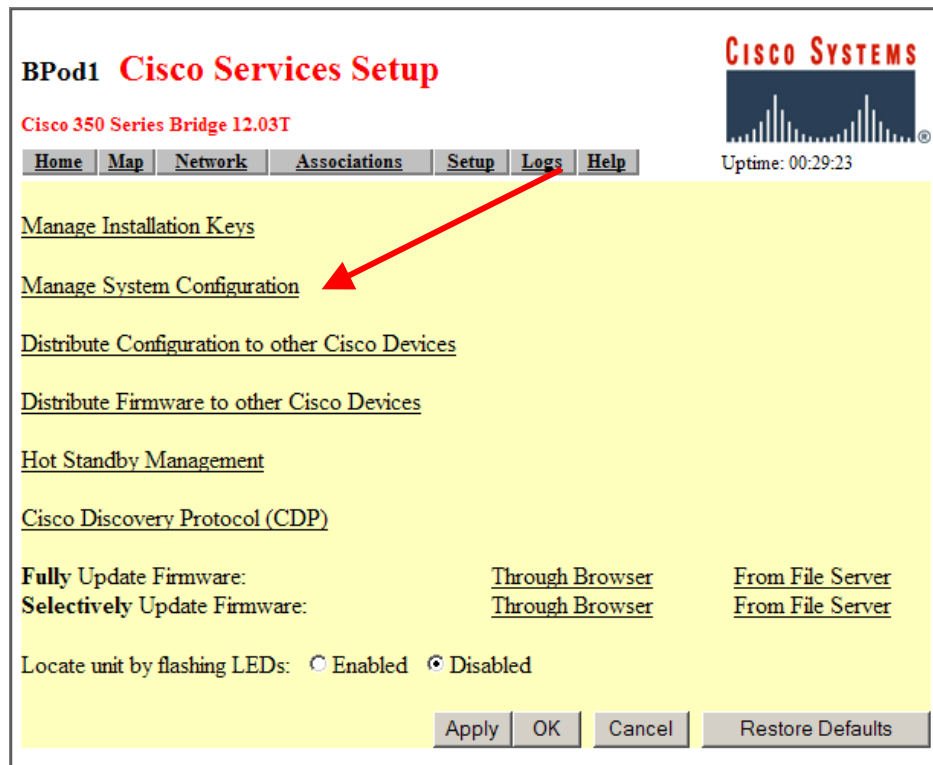
- b. From the **Distribute Firmware** Page, choose the **yes** radio button on for the Distribute all firmware option.
- c. Click the **Start** button.



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.

BPod1 System Configuration Setup

Cisco 350 Series Bridge 12.03T

Home Map Network Associations Setup Logs Help

Uptime: 01:27:57

"WARM" RESTART SYSTEM NOW "COLD" RESTART SYSTEM NOW

Download Non-Default System Configuration Except IP Identity

Reset System Factory Defaults Except IP Identity

Download Non-Default System Configuration Download All System Configuration

Reset All System Factory Defaults

Additional System Configuration File: Browse...

Read Config File from Server Browser Update Now Done

- b. From the **System Configuration Setup** Page, click on the **Reset All System Factory Defaults** button.



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.

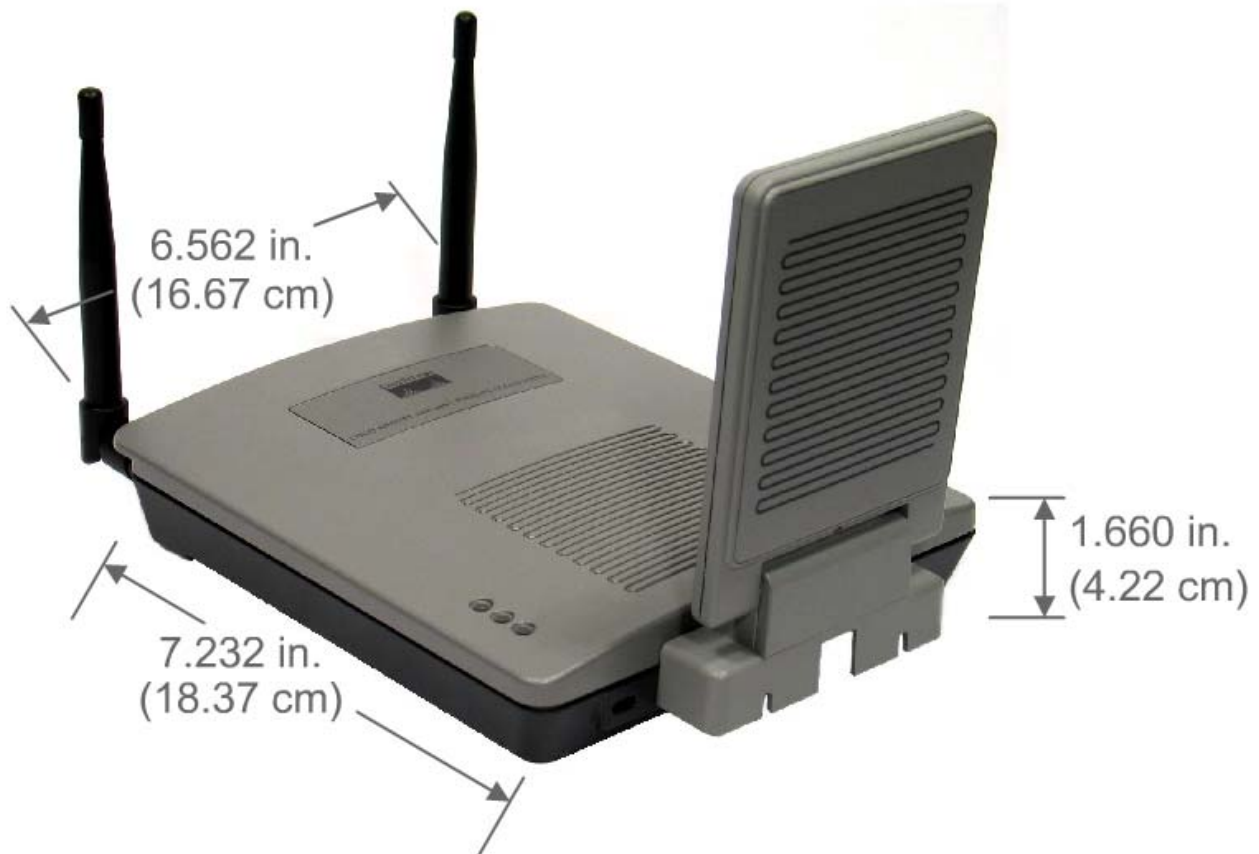
The students will perform some online Internet research and will require a computer with Internet access.

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



Total Weight = 26 oz (737g)

- 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?

ANSWER: RP-TNC stands for Reverse Polarity Threaded Naval Connector

2. What is Vertical Polarization?

ANSWER: Polarization is the physical orientation of the element on the antenna that actually emits the RF energy. The antenna is vertically polarized when the antenna is mounted with a vertical orientation.

3. Define antenna beam width.

ANSWER: Beamwidth is a measurement used to describe directional antennas. Beamwidth is sometimes called half-power beamwidth. It is the total width in degrees of the main radiation lobe, at the angle where the radiated power has fallen below that on the centerline of the lobe, by 3 dB (half-power).

4. Define antenna bandwidth.

ANSWER: The bandwidth of an antenna is the band of frequencies over which it is considered to perform acceptably.

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 antenna 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_sheet09186a0080092285.html

An additional reference can be found at the following link:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/accessory/4941.pdf>

1. Gain (in dBi)

ANSWER: 2.2 dBi

2. Frequency range

ANSWER: 2402-2495 MHz

3. What is the part number for the Cisco lightning arrester?

ANSWER: AIR-ACC3354

4. What does the Cisco lightning arrester do?

ANSWER: The Cisco Lightning arrester is supposed to protect devices on your wireless LAN network from indirect lightning strikes. (KEYWORD IS INDIRECT lightning strikes)

5. What is the gain of Cisco part number CISCO AIR-ANT1949?

ANSWER: 13.5 dBi

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

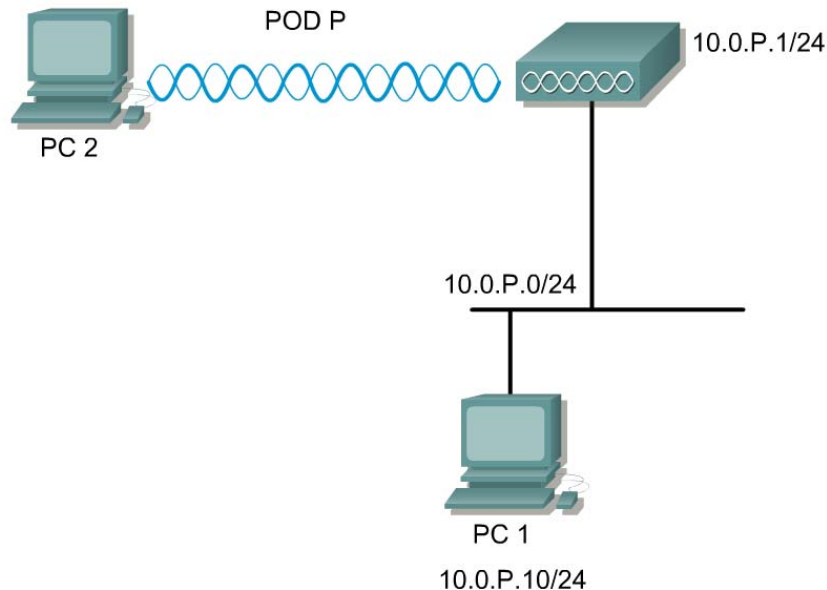
The student will test the effects of various antenna diversity settings on the Cisco Aironet AP. The student will configure the AP radio antennas through GUI and IOS command line.

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 |
|-------------------------------------|-------------------------------------|
| <code>configure terminal</code> | enter global configuration mode |
| <code>interface dot11radio 0</code> | enter the device radio interface |
| <code>antenna</code> | set the receive or transmit antenna |

Step 1 Configure the Cisco Aironet antenna settings

The screenshot shows the Cisco 1200 Access Point web interface. The main content area is titled "Network Interfaces: Radio0-802.11B Settings". It includes the following sections:

- Enable Radio:** Enable Disable
- Current Status (Software/Hardware):** Enabled Up
- Role in Radio Network:** (Fallback mode upon loss of Ethernet connection)
 - Access Point Root (Fallback to Radio Island)
 - Access Point Root (Fallback to Radio Shutdown)
 - Access Point Root (Fallback to Repeater)
 - Repeater Non-Root
- Data Rates:** A table with two tabs: "Best Range" and "Best Throughput".

| | Best Range | Best Throughput |
|------------|---|--|
| 1.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | <input type="radio"/> Enable <input type="radio"/> Disable |
| 2.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | <input type="radio"/> Enable <input type="radio"/> Disable |
| 5.5Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | <input type="radio"/> Enable <input type="radio"/> Disable |
| 11.0Mb/sec | <input checked="" type="radio"/> Require <input type="radio"/> Enable <input type="radio"/> Disable | <input type="radio"/> Enable <input type="radio"/> Disable |

- Open a web browser and type the IP address of the AP in the browser address box.
- Go to the **Radio0-802.11B** Settings page of the AP.
- Record the following information:

- Enable Radio Setting:

ANSWER: Answers will vary. **Example:** Enable

2. Role in Radio Network

ANSWER: Answers will vary. **Example:** Access Point Root

3. Default Radio Channel

ANSWER: Answers will vary. **Example:** Least congested channel – Channel 11

| | | | |
|-------------------------|--|--|-----------------------------|
| World Mode | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | |
| Multi-Domain Operation: | | | |
| Radio Preamble | <input checked="" type="radio"/> Short | <input type="radio"/> Long | |
| Receive Antenna: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left | <input type="radio"/> Right |
| Transmit Antenna: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left | <input type="radio"/> Right |

Step 2 Antenna settings

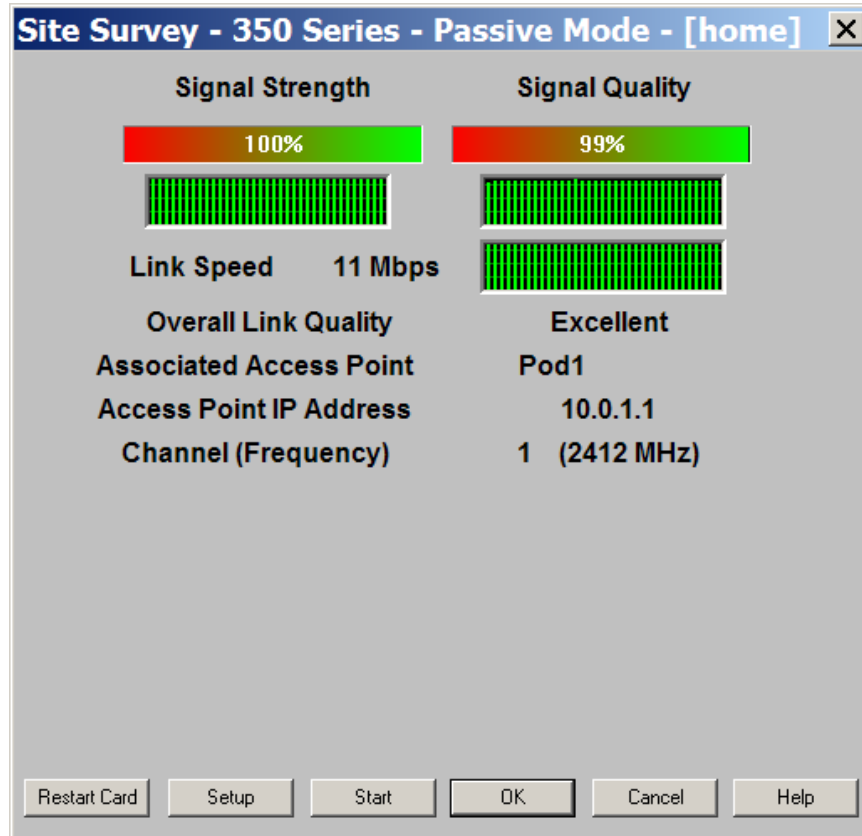
a. On the middle of the **AP Radio Hardware** page are the selections for the **Receive Antenna** and one for the **Transmit Antenna**.

b. Record the Receive Antenna Setting: _____

ANSWER: Diversity

c. Record the Transmit Antenna Setting: _____

ANSWER: Diversity



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? _____

ANSWER: Answer will vary.

c. What is the current Signal Quality? _____

ANSWER: Answer will vary.

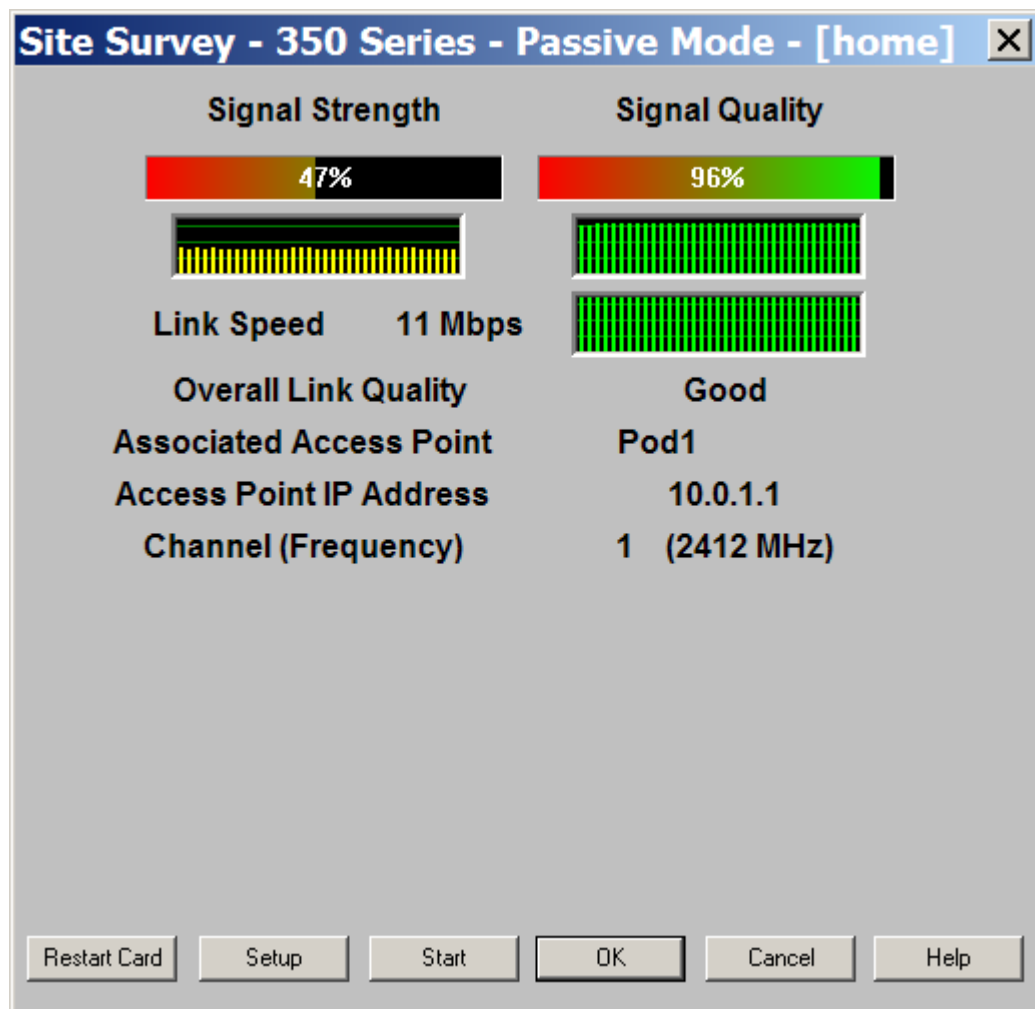
Step 4 Change antenna settings (continued)

a. Is it necessary to physically remove the antennas to change the antenna settings?

ANSWER: No

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)?

ANSWER: Answers will vary.

- e. Which antenna setting gave the strongest signal strength (Left, Right, or Diversity)?

ANSWER: Answers will vary.

- f. Which setting gave the weakest signal strength (Left, Right, or Diversity)?

ANSWER: Answers will vary.

- g. Which setting gave the weakest signal quality (Left, Right, or Diversity)?

ANSWER: Answers will vary.

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 |
|-------------------------------------|-------------------------------------|
| <code>configure terminal</code> | enter global configuration mode |
| <code>interface dot11radio 0</code> | enter the device radio interface |
| <code>antenna</code> | 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

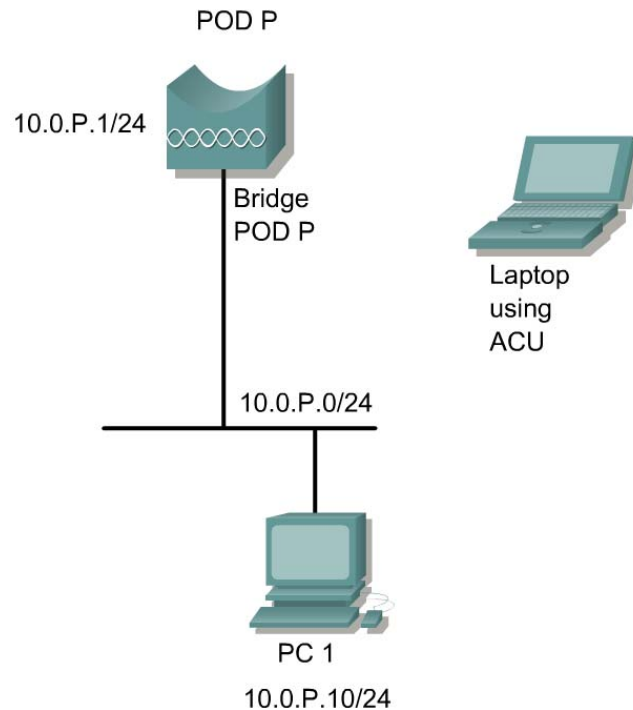
The student will test the effects of various antenna diversity settings on the Cisco BR350

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

AP1 Root Radio Hardware

Cisco 350 Series Bridge 12.01T1

[Map](#) [Help](#)

CISCO SYSTEMS



Uptime: 24 days,
04:30:46

Service Set ID (SSID): [more...](#)

Allow "Broadcast" SSID to Associate?: yes no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):

1.0 2.0 5.5 11.0

Transmit Power:

Frag. Threshold (256-2338):

RTS Threshold (0-2339):

Max. RTS Retries (1-255):

Max. Data Retries (1-255):

Beacon Period (19-5000 Kusec):

Data Beacon Rate (DTIM):

Default Radio Channel:

In Use: 1

Search for less-congested Radio Channel?: [Restrict Searched Channels](#)

Receive Antenna:

Transmit Antenna:

If VLANs are *not* enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Step 1 Configure the Cisco Aironet antenna settings

- Open a web browser and type the IP address of the bridge in the browser address box.
- Go to the Root Radio Hardware page of the bridge.
- Record the following information:
 - Service Set ID

ANSWER: Answers will vary. **Example:** AP1

- Transmit Power

ANSWER: Answers will vary. **Example:** 1mW

- Default Radio Channel

ANSWER: Answers will vary. **Example:** Channel 1

4. Search for less congested channel

ANSWER: Answers will vary. **Example:** NO

For this lab, keep this setting on NO. Both antenna settings should be set to diversity at this time.

AP1 Root Radio Hardware

Cisco 350 Series Bridge 11.23T

Map **Help** Cisco Systems
Uptime: 1 day, 01:59:01

Service Set ID (SSID):

Allow "Broadcast" SSID to Associate?: yes no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):
1.0 2.0 5.5 11.0

Transmit Power:

Frag. Threshold (256-2338): RTS Threshold (0-2339):

Max. RTS Retries (1-255): Max. Data Retries (1-255):

Beacon Period (Kusec): Data Beacon Rate (DTIM):

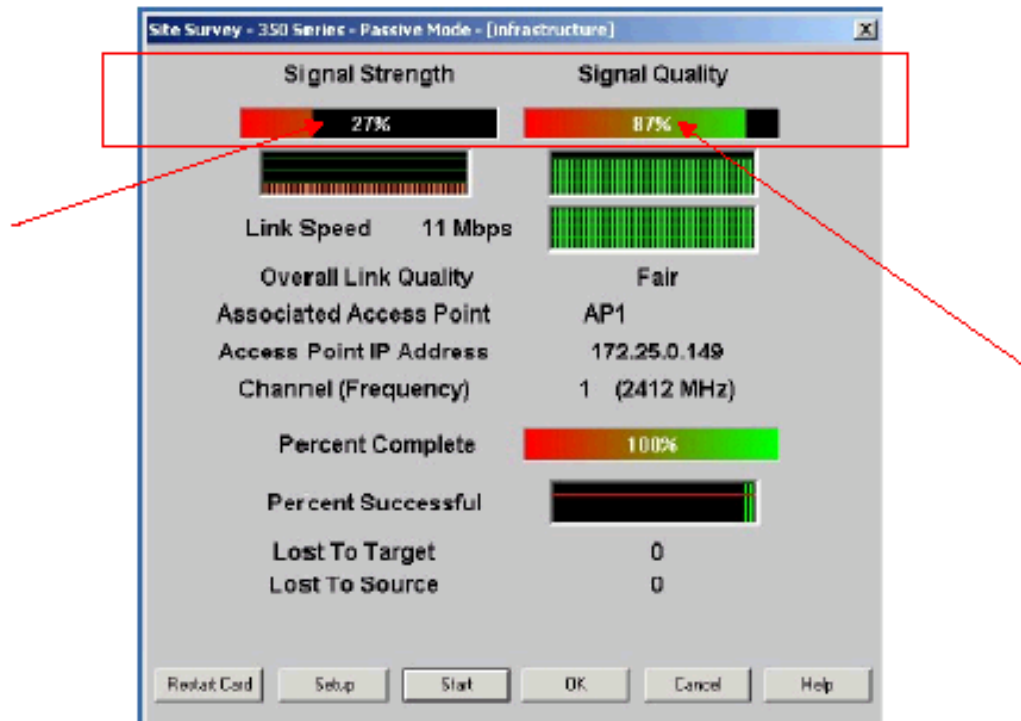
Default Radio Channel: In Use: 1

Search for less-congested Radio Channel?: [Restrict Searched Channels](#)

Receive Antenna: Transmit Antenna:

Radio Data Encry

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.

AP1 **Root Radio Hardware**

Cisco 350 Series Bridge 11.23T

CISCO SYSTEMS



Uptime: 1 day, 01:59:01

Map **Help**

Service Set ID (SSID):
 Allow "Broadcast" SSID to Associate?: yes no
 Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):
 1.0 2.0 5.5 11.0

Transmit Power:
 Frag. Threshold (256-2338): RTS Threshold (0-2339):
 Max. RTS Retries (1-255): Max. Data Retries (1-255):
 Beacon Period (Kusec): Data Beacon Rate (DTIM):
 Default Radio Channel: In Use: 1
 Search for less-congested Radio Channel?: Restrict Searched Channels

Receive Antenna: Transmit Antenna:
 Radio Data Encry: (WEP)

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?

ANSWER: NO

AP1 Root Radio Hardware

Cisco 350 Series Bridge 11.23T

Map Help Uptime: 1 day, 01:59:01

Service Set ID (SSID): AP1

Allow "Broadcast" SSID to Associate?: yes no

Enable "World Mode" multi-domain operation?: no yes

Data Rates (Mb/sec):
1.0 basic 2.0 basic 5.5 basic 11.0 basic

Transmit Power: 100 mW 200 mW 400 mW

Frag. Threshold (256-2338): RTS Threshold (0-2339):

Max. RTS Retries (1-255): Max. Data Retries (1-255):

Beacon Period (Kusec): Data Beacon Rate (DTIM):

Default Radio Channel: In Use: 1

Search for less-congested Radio Channel?: no yes [Restrict Searched Channels](#)

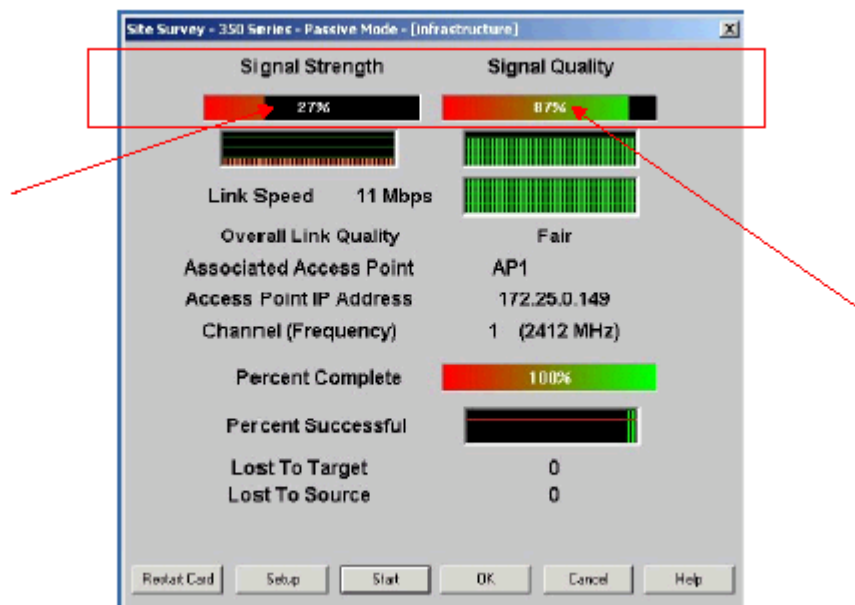
Receive Antenna: Diversity Right Left Diversity

Transmit Antenna: Diversity Right Left Diversity

Radio Data Encryption (WEP)

Apply OK Cancel Restore Defaults

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)?

ANSWER: Answers will vary. Example: Left

- f. Which antenna setting gave the strongest signal strength (Left, Right, or Diversity)?

ANSWER: Answers will vary. Example: Left

- g. Which setting gave the weakest signal strength (Left, Right, or Diversity)?

ANSWER: Answers will vary. Example: Right

- h. Which setting gave the weakest signal quality (Left, Right, or Diversity)?

ANSWER: Answers will vary. Example: Right

Lab 7.2.6 Omnidirectional Antennas

Estimated Time: 15 Minutes

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

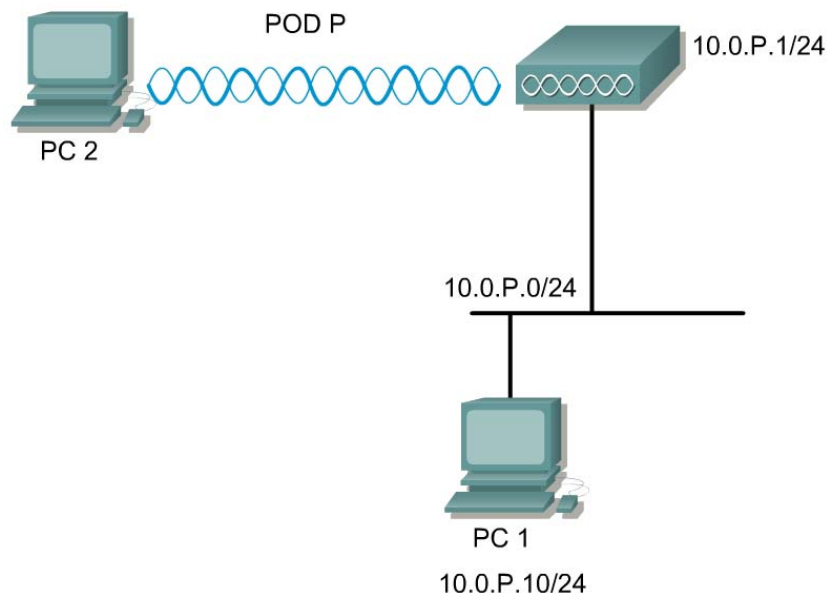
Objective

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

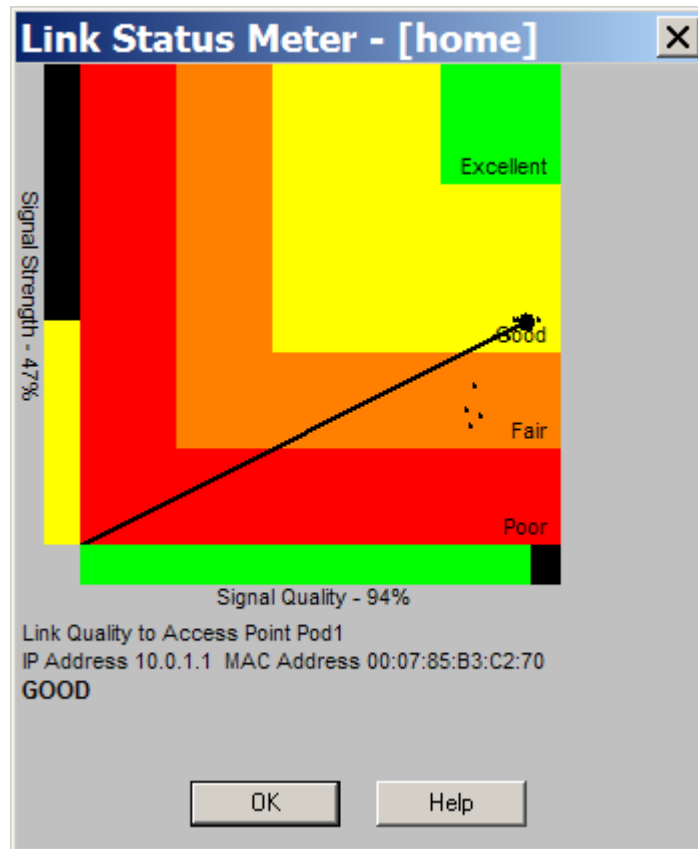
Transmit Antenna:

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.



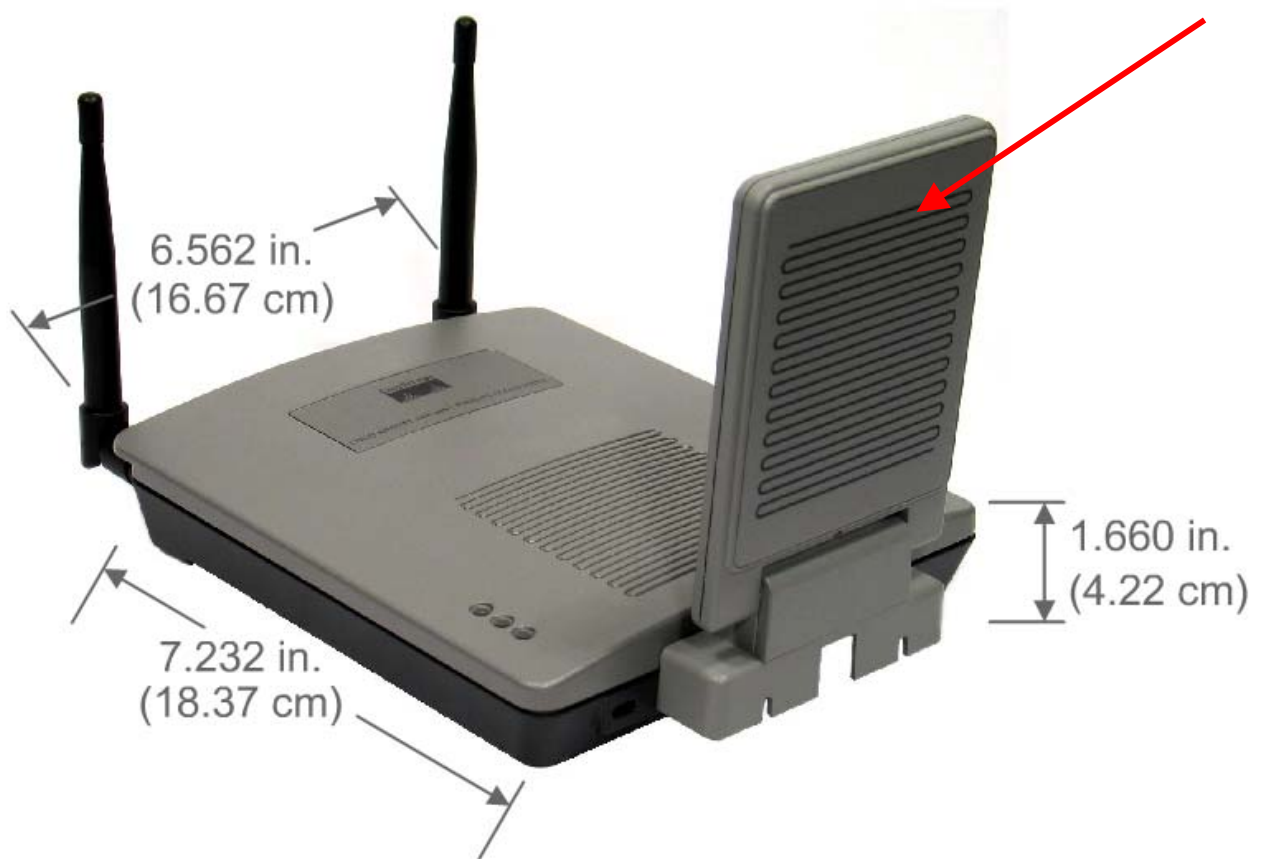
- e. Double click on the Link Status Meter (LSM) icon on the laptop and note the signal quality and signal strength meter.
- f. Move the laptop computer around the room and possibly the building to note any changes in the Link Status Meter. This will give an indication of the coverage area afforded this 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)?

ANSWER: Answers will vary depending on the data rate set. **Example:** 100 to 300 feet

- i. Experiment with changing the data rate on the AP. Were you able to extend your coverage range?

ANSWER: Answers will vary. **Example:** Yes

Step 2 Omni-directional 5GHz patch (if available)



Total Weight = 26 oz (737g)

In order to set up the Cisco Aironet 5GHz Omni directional antenna, complete the following steps:

- Flip up the patch antenna perpendicular to the Aironet AP1200.
- 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.

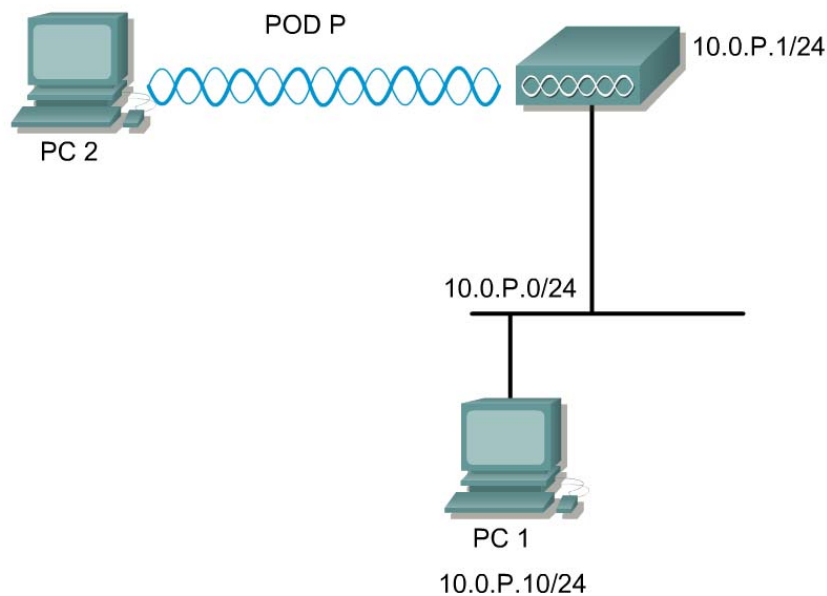
Objective

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)

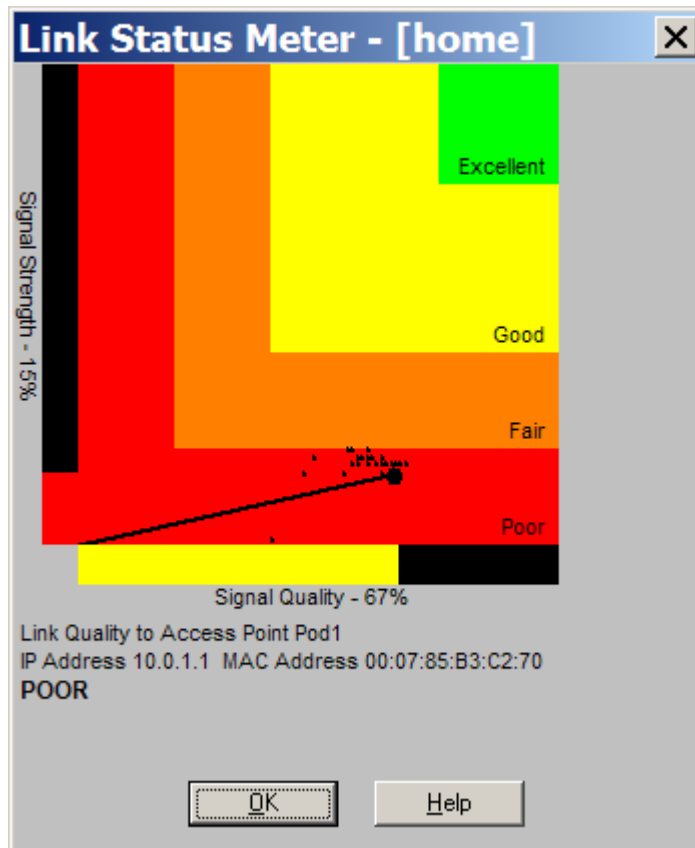
Step 1 Directional antenna (11a patch)



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?

ANSWER: Answers will vary. **Example:** 67%

j. What is the signal strength?

ANSWER: Answers will vary. **Example:** 15%

Step 2 Yagi directional antenna (optional)



In order to set up the Cisco Aironet directional antenna, complete the following steps:

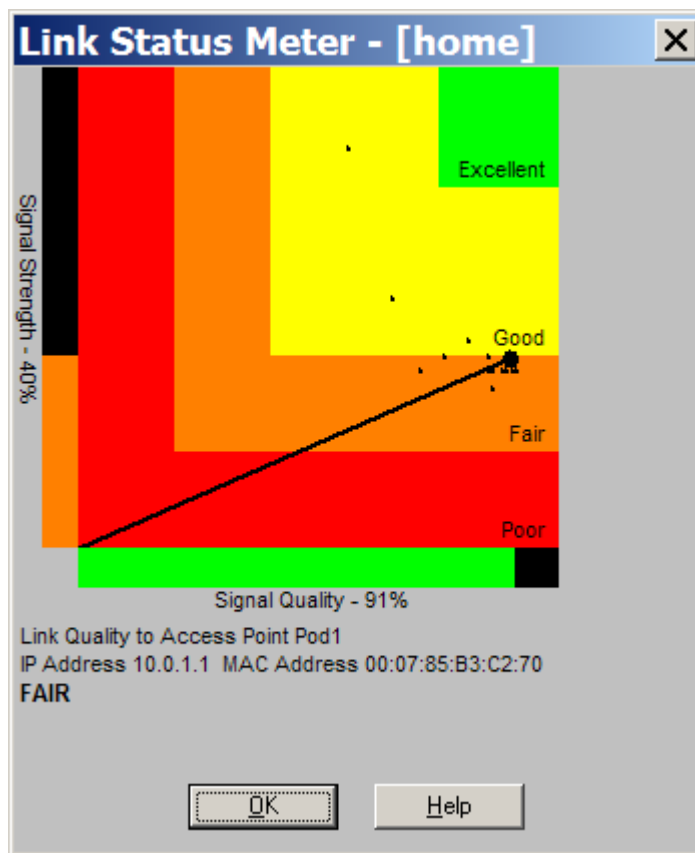
- a. Turn the power off on the AP and unscrew both standard dipole antennas from the rear of the AP. Then install the Yagi Mast Mount antenna to the AP by screwing the antenna TNC connector to the AP right TNC connector.



- 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: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left | <input type="radio"/> Right |
| Transmit Antenna: | <input checked="" type="radio"/> Diversity | <input type="radio"/> Left | <input type="radio"/> 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?

ANSWER: Answers will vary. **Example:** 91%

k. What is the signal strength?

ANSWER: Answers will vary. **Example:** 41%



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:

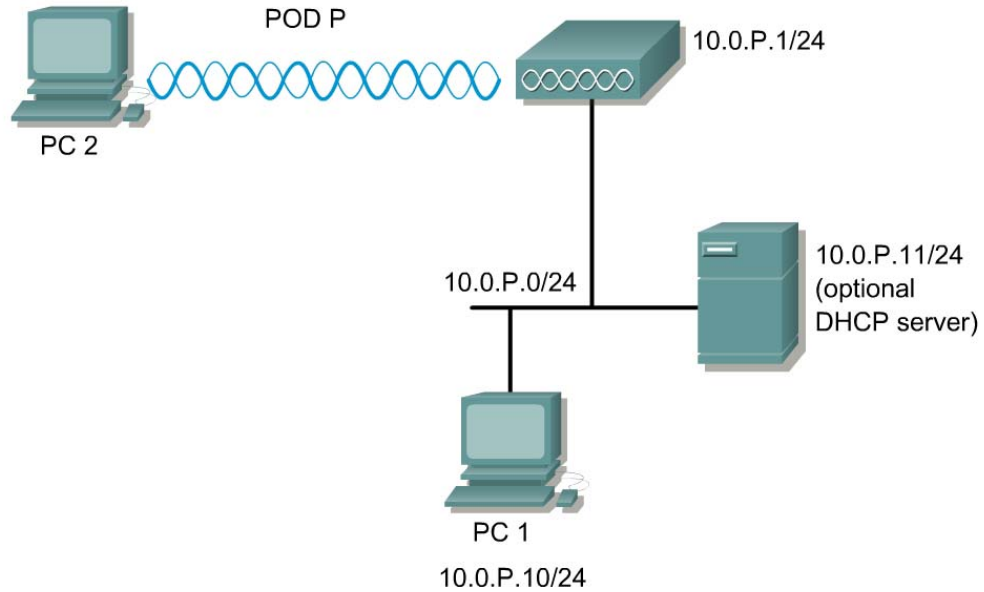
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
- Disable telnet and web (optional)

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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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

The screenshot shows the Cisco 1200 Access Point configuration interface. The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, Software Upgrade, System Configuration, and EVENT LOG. The main content area is titled "Cisco 1200 Access Point" and "System Software: System Configuration". It displays the hostname "PodP" and uptime "3 hours, 13 minutes". The configuration includes fields for "Current Startup Configuration File" (config.txt), "Load New Startup Configuration File" (with Load and Browse... buttons), "Technical Support Information" (with Show tech-support link), "Reset Startup Configuration to Factory Defaults" (with Reset to Defaults button), and "Restart Now" (with Restart button). At the bottom, there is a "Locate Access Point" section with "Blink the Access Point LEDs" set to "Disable" (radio button selected) and "Enable" (radio button unselected), with an Apply button.

- If there is an existing configuration on the AP, erase the configuration and reload either through GUI or IOS CLI.
- Configure the hostname, SSID, and BVI interface according to the Preparation table.

Step 2 Configure a new administrator account

The screenshot shows the Cisco 1200 Access Point configuration interface for "Security: Admin Access". The left sidebar is updated to show "SECURITY" expanded with sub-items: Admin Access, SSID Manager, Encryption Manager, Server Manager, Local RADIUS Server, and Advanced Security. The main content area shows "Security: Admin Access" with the hostname "PodP" and uptime "3 hours, 15 minutes". Under "Administrator Authenticated by:", there are four radio button options: "Default Authentication (Global Password)" (selected), "Local User List Only (Individual Passwords)", "Authentication Server Only", and "Authentication Server if not found in Local List". Below this are "Apply" and "Cancel" buttons. The "Default Authentication (Global Password)" section has "Default Authentication Password" and "Confirm Authentication Password" fields, both with masked input, and "Apply" and "Cancel" buttons. The "Local User List (Individual Passwords)" section has a "User List" table with a "< NEW >" button and a "Delete" button. The table contains one entry: "Cisco". To the right of the table are "Username:", "Password:", and "Confirm Password:" labels with corresponding input fields. Below the table are "Capability Settings" with "Read-Only" (radio button selected) and "Read-Write" (radio button unselected) options, and "Apply" and "Cancel" buttons.

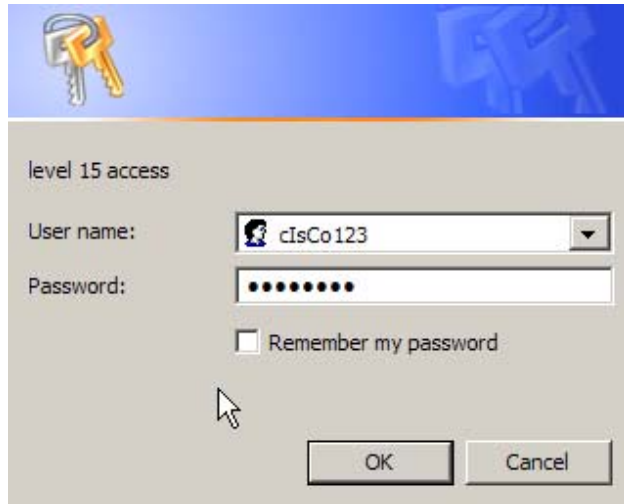
One of the easiest ways for hackers to gain access to network devices is by using default usernames and passwords.

- Configure a new administrator account from the **SECURITY>Admin Access** page. Give this user Read-Write privileges.

Username: cIsCo123

Password: cIsCo123

- 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

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 32 minutes

Services: NTP- Network Time Protocol

NTP Server

Network Time Protocol (NTP): Enabled Disabled

Time Server (optional): (Hostname or IP Address)

Time Settings

GMT Offset: (hrs)

Use Daylight Savings Time (United States only): Yes No

Manually Set Date: (yyyy/mm/dd)

Manually Set Time: (hh:mm:ss)

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?

ANSWER: Students must go to the Product Security Incident Response Team (PSIRT) web page listed above and check the list of known vulnerabilities. These will be specific to the image and platform.

1) Cisco Security Advisory: HTTP GET Vulnerability in AP1x00 (July 28, 2003)

2) Cisco Security Advisory: Aironet Telnet Vulnerability (April 9, 2002)

3) Access to the Cisco Aironet 340 Series Wireless Bridge through Web Interface (March 7, 2001)

- b. From the **SYSTEM SOFTWARE** main page, check the current image.

The screenshot shows the configuration page for a Cisco 1200 Access Point. The page title is "Cisco 1200 Access Point". On the left is a navigation menu with items like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE (highlighted), Software Upgrade, System Configuration, and EVENT LOG. The main content area shows the hostname "PodP" and uptime "PodP uptime is 3 hours, 34 minutes". Below this is a table of system software details:

| System Software Version: IOS (tm) C1200 Software (C1200-K9W7-M) | |
|---|--------------------------|
| Product/Model Number: | AIR-AP1220-IOS-UPGRD |
| Top Assembly Serial Number: | |
| System Software Filename: | c1200-k9w7-tar.122-11.JA |
| System Software Version: | 12.2(11)JA |
| Bootloader Version: | 12.2(11)JA |
| System Uptime: | 3 hours, 34 minutes |

- c. What version is running?

ANSWER: Should be c1200-k9w7-tar.122-11.JA or later

- d. Does this AP have any known vulnerabilities?

ANSWER: Possibly, but none are known or posted at this time.

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.

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 36 minutes

- HOME
- EXPRESS SET-UP
- NETWORK MAP +
- ASSOCIATION
- NETWORK INTERFACES +
- SECURITY +
- SERVICES
- Telnet/SSH
- Hot Standby
- CDP
- DNS
- Filters
- HTTP
- Proxy Mobile IP
- QoS
- SNMP
- NTP
- VLAN
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

Services: Telnet/SSH

Telnet: Enabled Disabled

Terminal Type: Teletype ANSI

Columns: (64-132)

Lines: (16-50)

Secure Shell Configuration

Secure Shell: Enabled Disabled

System Name:

Domain Name:

RSA Key Size (optional): (360-2048 bits)

Authentication Timeout (optional): (1-120 sec)

Authentication Retries (optional): (0-5)

Secure Shell Server Connections

| Connection | Version | Encryption | State | Username |
|------------|---------|------------|-------|----------|
| | | | | |

- 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?

ANSWER: 512

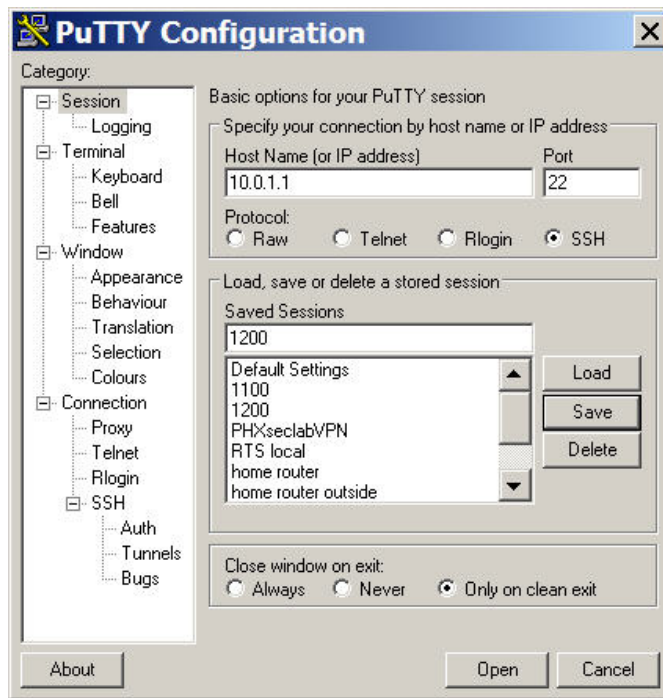
- g. Press **OK** to accept the default key size and continue.

Note In a production environment, after enabling SSH, telnet and http should be disabled.

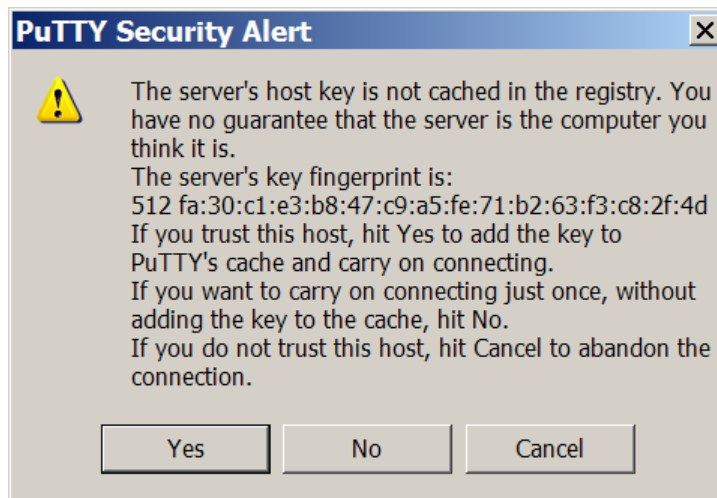
Step 6 Communicating between a SSH PC (client) to AP (server)

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.

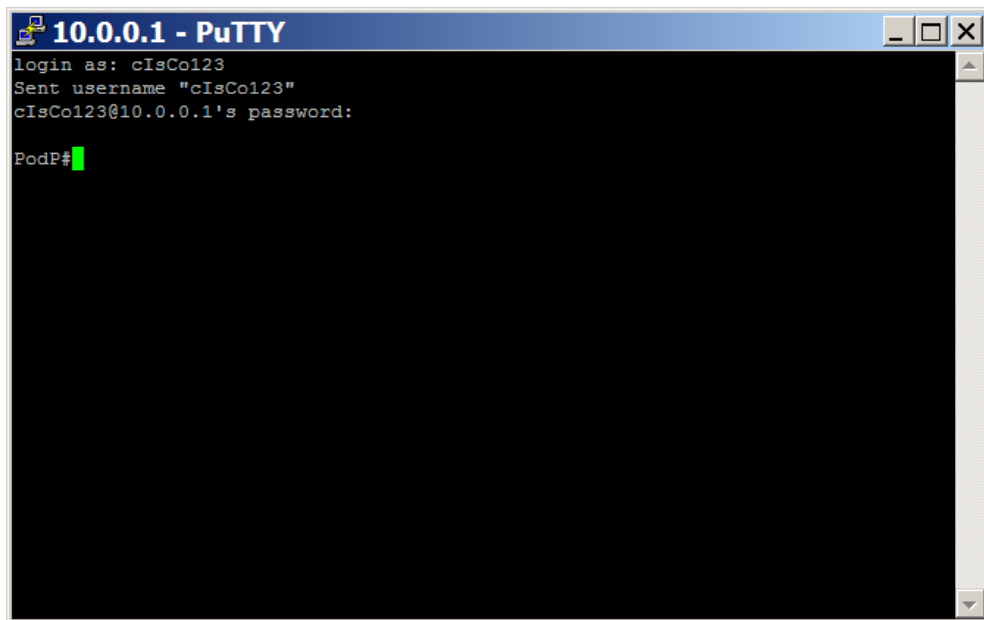
- a. The configurations will vary among different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.



- 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 “**clisCo123**” for the username and “**clisCo123**” for the password.



e. Was the SSH connection successful? If so, how is the prompt displayed?

ANSWER: Should be YES. The prompt should be PodP#, where P is the pod number.

Step 7 Verify SSH Connections

Cisco 1200 Access Point

Hostname PodP PodP uptime is 3 hours, 50 minutes

Services: Telnet/SSH

Telnet: Enabled Disabled

Terminal Type: Teletype ANSI

Columns: (64-132)

Lines: (16-50)

Secure Shell Configuration

Secure Shell: Enabled Disabled

System Name:

Domain Name:

RSA Key Size (optional): (360-2048 bits)

Authentication Timeout (optional): (1-120 sec)

Authentication Retries (optional): (0-5)

Secure Shell Server Connections

| Connection | Version | Encryption | State | Username |
|------------|---------|------------|-----------------|----------|
| 1 | 1.5 | 3DES | Session started | clsCo123 |

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 |
|------------|---------|------------|-------|----------|
| | | | | |
| | | | | |

ANSWER: Answers will vary. **Example:**

| Connection | Version | Encryption | State | Username |
|------------|---------|------------|-----------------|----------|
| 1 | 1.5 | 3DES | Session Started | cisCo123 |

- 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:

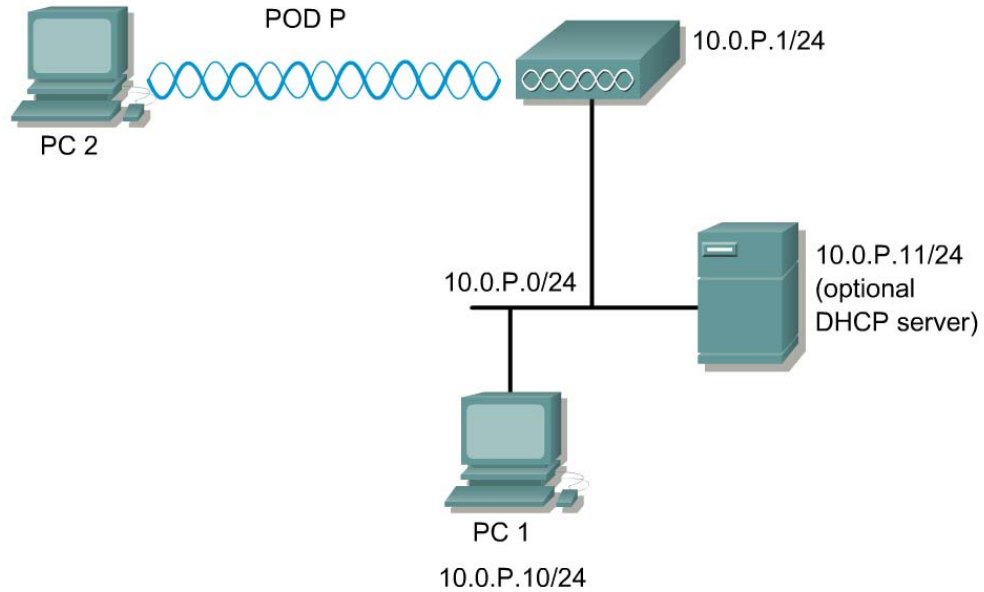
- Password protect the console
- Define administrator accounts
- Configure accurate time and check firmware
- Configure SSH
 - Limit VTY to SSH
 - Access-list to secure SSH
- Disable telnet and web

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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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 |
|--------------------------------------|--|
| <code>crypto key generate rsa</code> | Generates Rivest, Shamir, and Adleman (RSA) key pairs. |
| <code>hostname</code> | This command changes the APs hostname. |
| <code>ip domain-name</code> | Defines a default domain name that the Cisco IOS software uses to complete unqualified host names. |
| <code>ip ssh</code> | Use the <code>ip ssh</code> command to configure Secure Shell (SSH) control parameters on the AP. |
| <code>transport input</code> | Defines which protocols to use to connect to a specific line of the AP. |

Step 1 Configure basic AP settings

- Connect a Cisco rollover cable (console cable) between PC1 and the AP.
- Open a terminal emulator.
- Press return to get started.
- If there is an existing configuration on the AP, erase the configuration and reload.
- Configure the hostname, SSID, and domain name according to the Preparation table.

```
PodP(config) #  
PodP(config) #ip domain-name fw1.com
```

- Configure a wireless PC or laptop to connect to the AP. This will be used later in the lab to test the security configuration.
- Remain on PC1 to configure the following steps.
- 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.

- Configure a new administrator account.

```
PodP(config) #username cIsCo123 password cIsCo123
```

- 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?

ANSWER: Answers will vary.

- b. Check the current image.

```
PodP#show version
```

- c. What version is running?

ANSWER: Should be c1200-k9w7-mx.122-11.JA or later

- d. Does this AP have any known vulnerabilities?

ANSWER: Possibly, but none are known or posted at this time.

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?

ANSWER:

```
general-keys  Generate a general purpose RSA key pair for signing
and encryption
usage-keys    Generate separate RSA key pairs for signing and
encryption
<cr>
```

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?

ANSWER: 512

- 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?

ANSWER: 120 seconds and 5 retries

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
```

2. What are the available parameters for the `transport input` command?

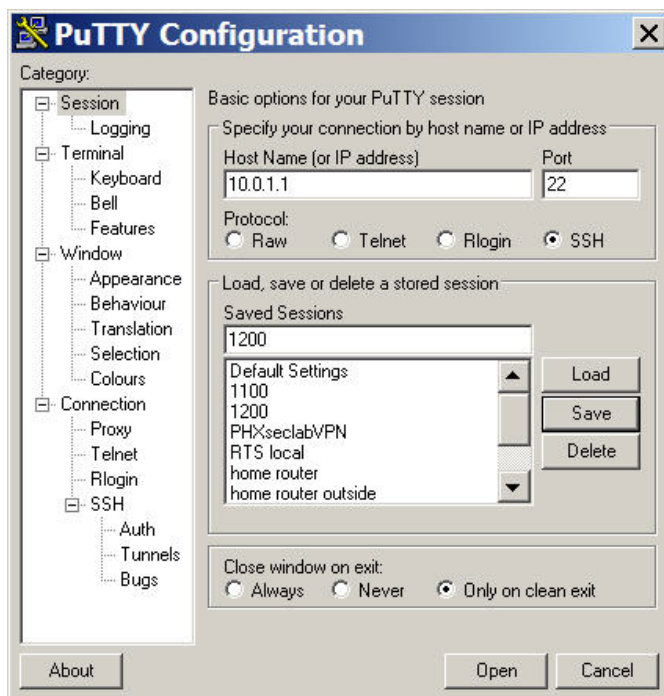
ANSWER: 512

```
all      All protocols
none     No protocols
ssh      TCP/IP SSH protocol
telnet   TCP/IP Telnet protocol
```

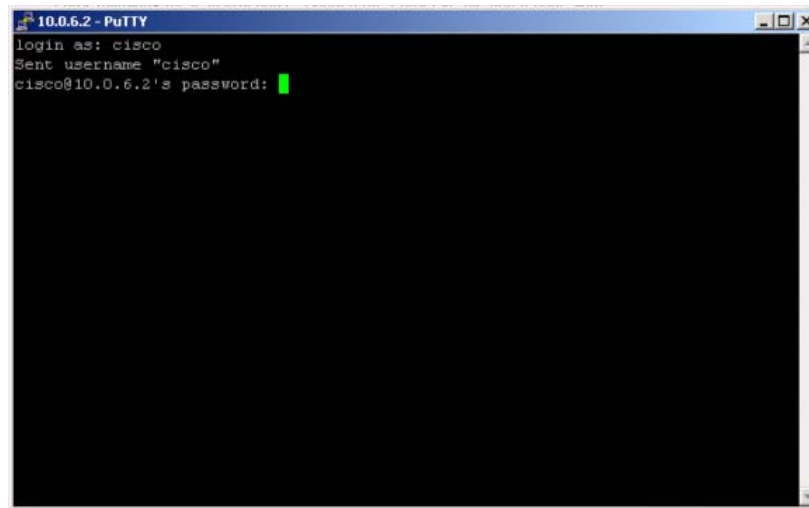
Step 9 Communicating between a SSH PC (client) to AP (server)

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?

ANSWER: Should be successful, and the prompt should look like the password of `cisco@10.0.6.2`

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_MSG_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_MSG_FAILURE message sent
```

```

03:45:44: SSH1: SSH_MSG_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_MSG_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 |
|------------|---------|------------|-------|----------|
| | | | | |

ANSWER: Answers will vary. **Example:**

| Connection | Version | Encryption | State | Username |
|------------|------------|-------------|------------------------|-----------------|
| 1 | 1.5 | 3DES | Session Started | cisCo123 |

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?

ANSWER: Answers may vary. **Example:** Yes

```

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. ii. 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?

ANSWER: Should fail. Because only the SSH session is allowed.

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?

ANSWER:

```
-c Select encryption algorithm
-l Log in using this user name
-o Specify options
-p Connect to this port
WORD IP address or hostname of a remote system
```

- g. What encryption algorithms are available?

ANSWER:

```
PodP#ssh -c ?
3des triple des
des des
```

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?

ANSWER: Should be successful. If not, ping from the PC to the AP. If the ping is successful, turn on debugging and try the connection again.

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?
-
-

ANSWER: Answers will vary Example: **debug ssh, debug ip ssh**

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?
-
-

ANSWER: Connection should fail

- 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

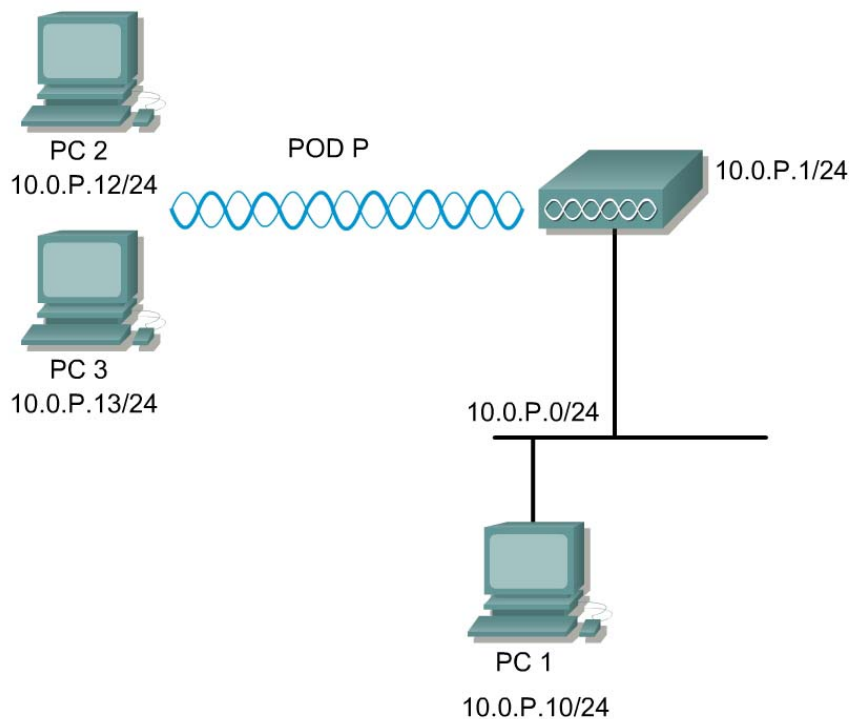
In this lab, the student will learn how to set and enable a protocol filter on the AP and how to set and enable MAC address filters on the AP.

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

| <u>Team</u> | <u>AP Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|----------------|-------------|----------------|
| 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.

Cisco 1200 Access Point

APPLY FILTERS
MAC ADDRESS FILTERS
IP FILTERS
ETHERTYPE FILTERS

Hostname Pod1 Pod1 uptime is 1 hour, 24 minutes

Services: Filters - MAC Address Filters

Create/Edit Filter Index:

Filter Index: (700-799)

Add MAC Address: Mask: Action:

(HHHH.HHHH.HHHH) (HHHH.HHHH.HHHH)

Default Action:

Filters Classes:

Mac Address: 0007.EB31.7C12 Mask: 0000.0000.0000 - Forward

Default - Block All

- a. Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu.
- b. In the Filter Index field, name the filter with a number from 701.
- c. 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).
- d. Select **Forward** from the Action menu.
- e. Click **Add**. The MAC address appears in the Filters Classes field.
- f. 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

Cisco 1200 Access Point

APPLY FILTERS
MAC ADDRESS FILTERS
IP FILTERS
ETHERTYPE FILTERS

Hostname Pod1
Pod1 uptime is 1 hour, 31 minutes

Services: Filters - Apply Filters

| | | FastEthernet | Radio0-802.11B | Radio1-802.11A |
|----------|-----------|--------------|--------------------|--------------------|
| Incoming | MAC | < NONE > | MAC 701 | MAC < NONE > |
| | EtherType | < NONE > | EtherType < NONE > | EtherType < NONE > |
| | IP | < NONE > | IP < NONE > | IP < NONE > |
| Outgoing | MAC | < NONE > | MAC 701 | MAC < NONE > |
| | EtherType | < NONE > | EtherType < NONE > | EtherType < NONE > |
| | IP | < NONE > | IP < NONE > | IP < NONE > |

Apply Cancel

- 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?

ANSWER: Yes. Should be.

- 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?

ANSWER: No. Should not be.

Step 5 Remove the MAC address filter

Before configuring any IP Filters, delete the existing MAC filter.

■■■■■■■■■■■ **Cisco 1200 Access Point**

| | | | | |
|----------------------------|--|----------------------------|-------------------------|--------------------------|
| HOME | APPLY FILTERS | MAC ADDRESS FILTERS | IP FILTERS | ETHERTYPE FILTERS |
| EXPRESS SET-UP | Hostname ap | | ap uptime is 23 minutes | |
| NETWORK MAP + | Services: Filters - Apply Filters | | | |
| ASSOCIATION | | FastEthernet | Radio0-802.11B | Radio1-802.11A |
| NETWORK INTERFACES + | Incoming | MAC < NONE > | MAC < NONE > | MAC < NONE > |
| SECURITY + | | EtherType < NONE > | EtherType < NONE > | EtherType < NONE > |
| SERVICES | | IP < NONE > | IP < NONE > | IP < NONE > |
| Telnet/SSH | Outgoing | MAC < NONE > | MAC < NONE > | MAC < NONE > |
| Hot Standby | | EtherType < NONE > | EtherType < NONE > | EtherType < NONE > |
| CDP | | IP < NONE > | IP < NONE > | IP < NONE > |
| DNS | | | | |
| Filters | | | | |
| HTTP | | | | |
| Proxy Mobile IP | | | | |
| QoS | | | | |
| SNMP | | | | |
| NTP | | | | |
| VLAN | | | | |
| WIRELESS SERVICES + | | | | |
| SYSTEM SOFTWARE + | | | | |
| EVENT LOG + | | | | |

Apply Cancel

- From the **SERVICES>Filters Page** change the 701 to <NONE> on both Incoming and Outgoing.
- Click **Apply**.
- From PC 2 and PC 3, ping the AP at 10.0.P.1.
- Was this successful? Should it be successful?

ANSWER: Should be. Yes

Step 6 Creating an IP filter

Follow this link path to reach the IP Filters page:

- Click **Services** in the page navigation bar.
- In the Services page list, click **Filters**.
- On the **Apply Filters** page, click the **IP Filters** tab at the top of the page.

Services: Filters - IP Filters

Create/Edit Filter Name: <NEW >

Filter Name: MYFILTER

Default Action: Block All

IP Address

Destination Address: 0.0.0.0 Mask: 255.255.255.255

Source Address: 10.0.1.12 Mask: 0.0.0.0

Action: Forward Add

- Make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu, and then click the **Add** button.
- Enter a descriptive name of **MYFILTER** for the new filter in the Filter Name field.
- Select **Block all** as the filter's default action from the Default Action menu.
- Configure the **Destination Address:** of 0.0.0.0 and a **Mask:** of 255.255.255.255.
- Add 10.0.P.12 as the **Source Address:** with a **Mask:** of 0.0.0.0 to permit PC2 traffic.
- Make sure Forward is selected for the **Action:**
- Click the **Add** button. The ACL will now appear in the Filters Classes Box at the bottom of the **Filters** page.
- Verify the configuration in the Filters Classes box.

Filters Classes

IP destination address: 0.0.0.0, Mask: 255.255.255.255 - source address: 10.0.1.12, Mask: 0.0.0.0 - Forward

Default - Block All

Delete Class

- If the configuration is correct, click **Apply**.

Step 7 Apply the IP filter

Cisco 1200 Access Point

| | APPLY FILTERS | MAC ADDRESS FILTERS | IP FILTERS | ETHERTYPE FILTERS |
|----------------------------|--|---------------------|------------|-------------------|
| HOME | Hostname ap ap uptime is 47 minutes | | | |
| EXPRESS SET-UP | | | | |
| NETWORK MAP + | | | | |
| ASSOCIATION | | | | |
| NETWORK INTERFACES + | | | | |
| SECURITY + | | | | |
| SERVICES | Services: Filters - Apply Filters | | | |
| Telnet/SSH | | | | |
| Hot Standby | | | | |
| CDP | | | | |
| DNS | | | | |
| Filters | | | | |
| HTTP | | | | |
| Proxy Mobile IP | | | | |
| QoS | | | | |
| SNMP | | | | |
| NTP | | | | |
| VLAN | | | | |
| WIRELESS SERVICES + | | | | |
| SYSTEM SOFTWARE + | | | | |
| EVENT LOG + | | | | |

| | | FastEthernet | Radio0-802.11B | Radio1-802.11A |
|----------|-----------|--------------|--------------------|--------------------|
| Incoming | MAC | < NONE > | MAC < NONE > | MAC < NONE > |
| | EtherType | < NONE > | EtherType < NONE > | EtherType < NONE > |
| | IP | < NONE > | MYFILTER | < NONE > |
| Outgoing | MAC | < NONE > | MAC < NONE > | MAC < NONE > |
| | EtherType | < NONE > | EtherType < NONE > | EtherType < NONE > |
| | IP | < NONE > | MYFILTER | < NONE > |

Apply Cancel

- Select **MYFILTER** from the radio ports incoming and outgoing IP fields.
- 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

- From PC 3, located at 10.0.P.13, ping the AP at 10.0.P.1.
- Was this successful? Should it be successful?

ANSWER: Should not be. NO

- From PC 2, located at 10.0.P.12, ping the AP at 10.0.P.1.
- Was this successful? Should it be successful?

ANSWER: Should be. Yes

e. List three of the EtherType filters that can be used.

ANSWER: ARP, IP, IPX, XNS, AppleTalk, NetBui, X.25, Banyan

NOTE: These are found in Appendix B1 in the Link found on 8.3.2.

f. List three of the IP filters that can be used.

ANSWER: ICMP, IGMP, TCP, IDP, TP4, UDP, SVP, Vines

NOTE: These are found in Appendix B2 in the Link found on 8.3.2.

g. List three of the port filters that can be used.

ANSWER: ECHO, PING, HTTP FTP, TELNET, DNS, KERBEROS, TIME, SMTP

NOTE: These are found in Appendix B3 in the Link found on 8.3.2.



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.

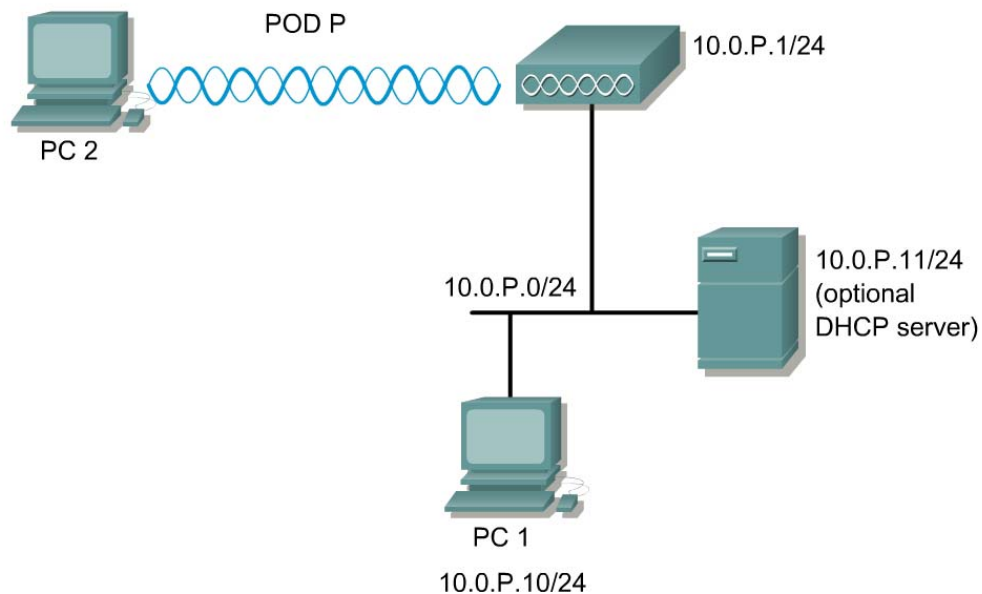
Objective

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

Cisco 1200 Access Point

Hostname ap ap uptime is 11 minutes

| Security Summary | | | | |
|--------------------------------------|-----------|------|------------|-------------|
| Administrators | | | | |
| Username | Read-Only | | Read-Write | |
| Cisco | ✓ | | | |
| Radio0-802.11B SSIDs | | | | |
| SSID | VLAN | Open | Shared | Network EAP |
| AP1 | none | ✓ | | |
| Radio1-802.11A SSIDs | | | | |
| SSID | VLAN | Open | Shared | Network EAP |
| AP1 | none | ✓ | | |

In order to configure WEP on the AP, complete the following steps:

- Verify connectivity from the wireless client (PC2) to the AP
- Open a Web browser on the PC1 and type the IP address of the AP to configure in the browser address bar.
- Go to the **Security** Setup page of the AP and click on the **Encryption Manager** option.

Step 2 Configuring WEP (continued)

.....

Cisco 1200 Access Point

RADIO0-802.11B
RADIO1-802.11A

Hostname ap ap uptime is 12 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None
 WEP Encryption Optional
Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying
 Cipher WEP 128 bit

Encryption Keys

| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|------------------------------|--|
| Encryption Key 1: | <input type="radio"/> | | 128 bit |
| Encryption Key 2: | <input checked="" type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |

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

The screenshot displays the configuration page for a Cisco 1200 Access Point, specifically for the Security: Encryption Manager - Radio0-802.11B interface. The page is divided into several sections:

- Encryption Modes:** This section contains three radio button options: None, WEP Encryption, and Cipher. The WEP Encryption option is selected, and its mode is set to 'Mandatory' via a dropdown menu. Below this, there are two checkboxes for 'Cisco Compliant TKIP Features': 'Enable MIC' and 'Enable Per Packet Keying', both of which are currently unchecked.
- Encryption Keys:** This section contains a table with four rows, each representing an encryption key. The columns are 'Transmit Key', 'Encryption Key (Hexadecimal)', and 'Key Size'.

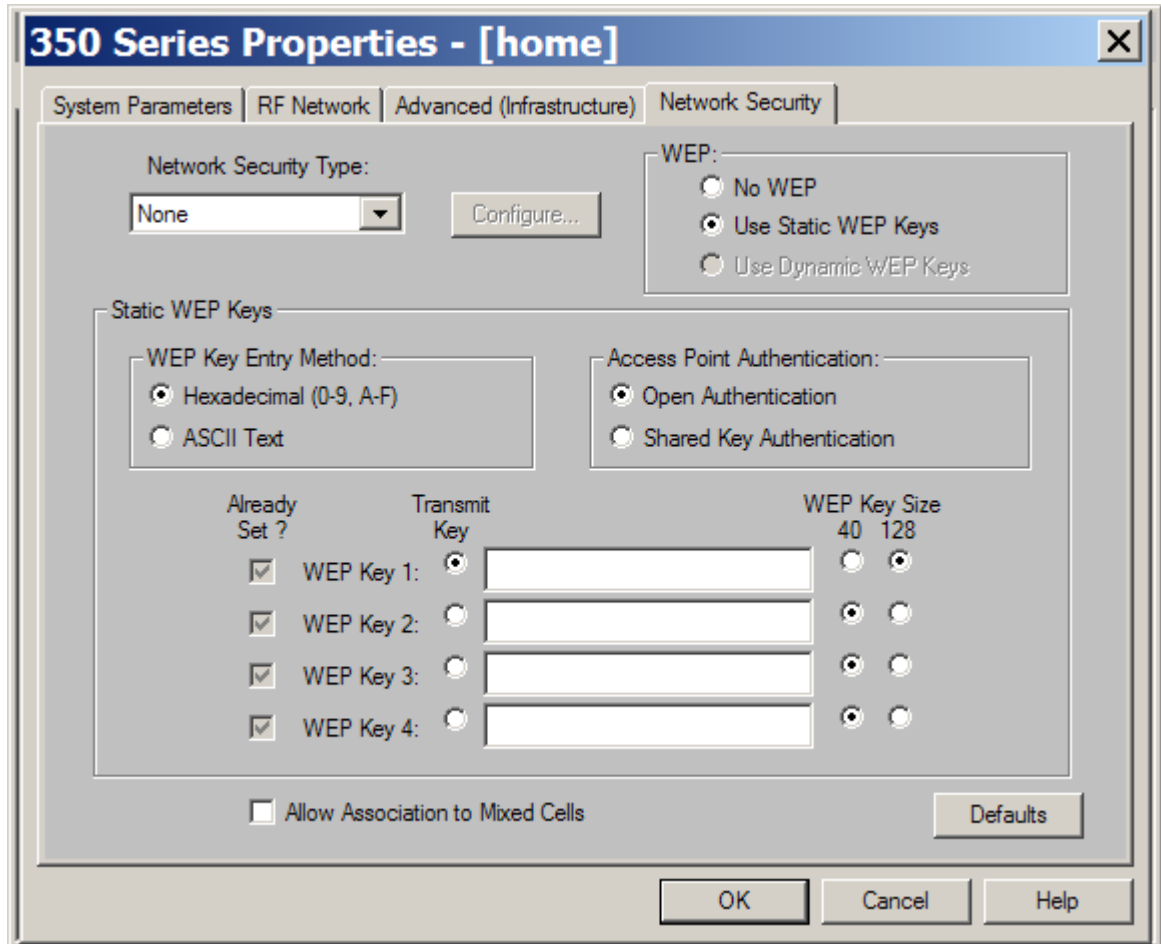
| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|------------------------------|----------|
| Encryption Key 1: | <input checked="" type="radio"/> | | 128 bit |
| Encryption Key 2: | <input type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |

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?

ANSWER: WEP Encryption Optional

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] **12345678909876543210123456**
 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?

ANSWER: Four

g. What happens if a device receives a packet that is not encrypted with the appropriate key?

ANSWER: It is dropped.

h. What is the more secure authentication method, shared key or open?

ANSWER: Open Authentication is considered the more secure method.

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

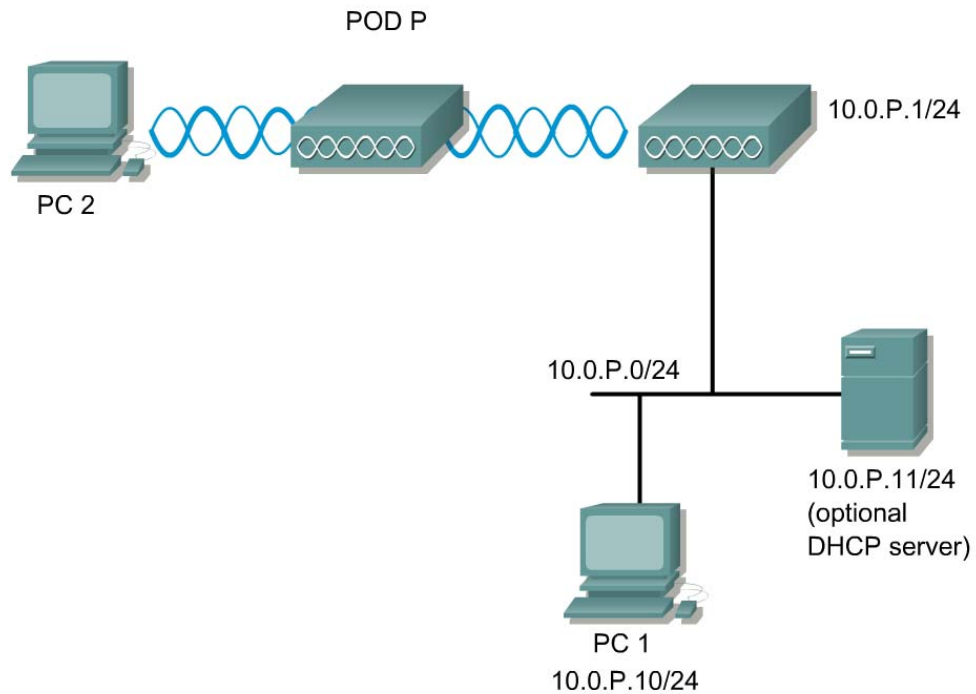
The student will extend the coverage of a basic service set topology by implementing an AP as a repeater using WEP.

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

| <u>Team</u> | <u>Access Point Name</u> | <u>SSID</u> | <u>Address</u> |
|-------------|--------------------------|-------------|----------------|
| 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.

- 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
```

- Enter interface configuration mode for the 2.4-GHz radio.

```
Pod2 (config) #interface dot11Radio 0  
Pod2 (config-if) #
```

- 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?

ANSWER: Yes. The `show dot11 associations all-clients` command displays the status of all clients associated with the access point.

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?

ANSWER: Yes. The `show dot11 associations all-clients` command displays the status of all clients associated with the access point.

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.

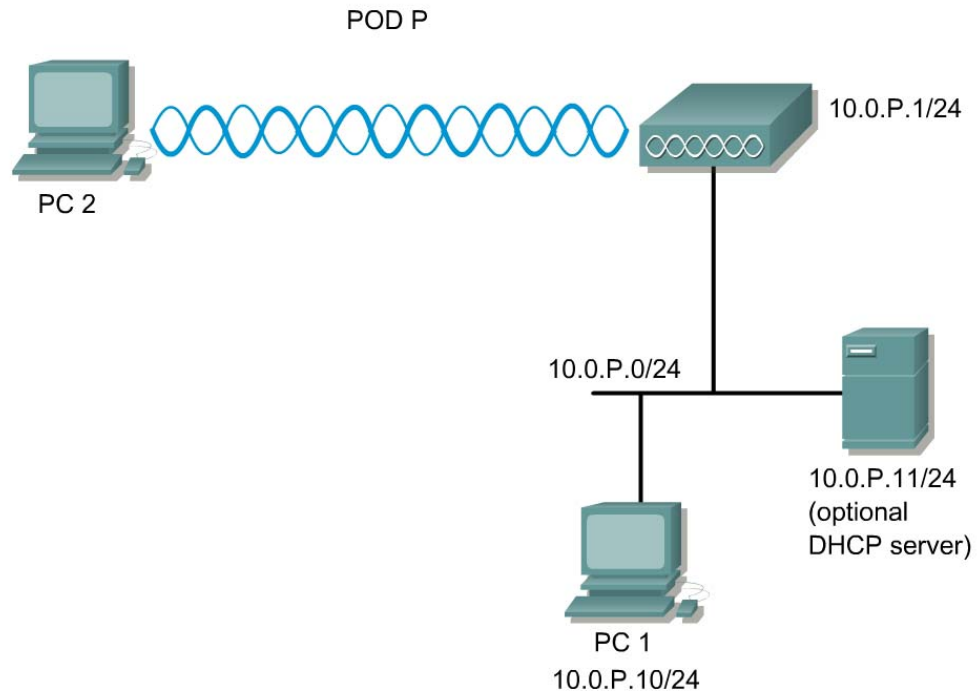
Objective

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

Cisco 1200 Access Point

RADIO0-802.11B RADIO1-802.11A

Hostname ap ap uptime is 1 hour, 46 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None
 WEP Encryption Mandatory
 Cipher WEP 128 bit

Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Encryption Keys

| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|------------------------------|----------|
| Encryption Key 1: | <input checked="" type="radio"/> | | 128 bit |
| Encryption Key 2: | <input type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |

In order to enable Cisco LEAP on the AP, WEP Encryption or a Cipher must be enabled.

- From the **SECURITY>Encryption Manager** Page of the AP, configure the Encryption Key 1.
- Click on the WEP Encryption radio button.
- Select Mandatory.
- Click **Apply-All**.
- The **Cipher** option can be used for greater security. What options are available?

WEP 128 bit
 WEP 40 bit
 TKIP
 CKIP
 CMIC
 CKIP + CMIC
 TKIP + WEP 128 bit
ANSWER: TKIP + WEP 40 bit

Step 2 Configure RADIUS server

The screenshot shows the configuration page for a Backup RADIUS Server on a Cisco 1200 Access Point. The left sidebar contains a navigation menu with categories like HOME, SECURITY, and SERVICES. The main content area has tabs for SERVER MANAGER and GLOBAL PROPERTIES. The Backup RADIUS Server section includes fields for Backup RADIUS Server (10.0.1.1) and Shared Secret (secretkey). Buttons for Apply, Delete, and Cancel are visible.

Complete the following steps to configure the Backup RADIUS Server from the **SECURITY>Server Manager** Page:

- 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
- Enter the Shared Secret key of **secretkey**
- Click **Apply**.

Step 3 Configure local RADIUS server

The screenshot shows the configuration page for a Local RADIUS Server on a Cisco 1200 Access Point. The left sidebar contains a navigation menu with categories like HOME, SECURITY, and SERVICES. The main content area has tabs for STATISTICS and GENERAL SET-UP. The Local RADIUS Server - General Set-Up section includes a list of Current Network Access Servers with a 'NEW' button and a 'Delete' button. Fields for Network Access Server (10.0.1.1) and Shared Secret (secretkey) are present. Buttons for Apply and Cancel are visible.

Complete the following steps to configure a Local RADIUS Server from the **SECURITY>Local RADIUS Server** Page:

- Click on the **GENERAL SET-UP** tab.
- 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
- Enter the Shared Secret key of **secretkey**
- Click **Apply**.

Step 4 Configure users

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

10.0.0.1

Shared Secret:

Delete

Apply Cancel

Individual User

Current User List

| | | |
|---------|--|--|
| < NEW > | | |
| aauser | Username: <input type="text"/> | |
| cisco | Password: <input type="text"/> <input checked="" type="radio"/> Text <input type="radio"/> NT Hash | |
| | Confirm Password: <input type="text"/> | |
| | Group Name: <input type="text" value="< NONE >"/> | |

Delete

Apply Cancel

Complete the following steps to configure users from the **SECURITY>Local RADIUS Server** Page:

- Continue from the **GENERAL SET-UP** tab.
- Enter the following users:

| User | Username | Password |
|------|----------|-----------|
| 1 | aauser | aaapass |
| 2 | Cisco1 | ciscopass |

- Click **Apply**.

Step 5 Configure authentication on AP

The screenshot shows the configuration page for a Cisco 1200 Access Point. The page title is "Cisco 1200 Access Point". The left sidebar contains a navigation menu with the following items: HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, Admin Access, SSID Manager, Encryption Manager, Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Security : SSID Manager - Radio0-802.11B". The page shows the configuration for the SSID "AP1". The "Authentication Methods Accepted" section has "Network EAP" checked. The "Authenticated Key Management" section has "WPA: Optional" selected. The "WPA Pre-shared Key" field is empty. The "EAP Client (optional)" section has "Username" and "Password" fields. The "Association Limit (optional)" field is set to 1. The "Enable Accounting" checkbox is checked. The "Apply-All" button is visible at the bottom right.

In order to enable Cisco LEAP on the AP, complete the following steps to configure the Authentication Method:

- On the **SECURITY>SSID** Manager page of the AP, create a new SSID of **APP**, where **P** is the Pod number.
- Check the **Network EAP** box.
- Click the **Apply-All** button.

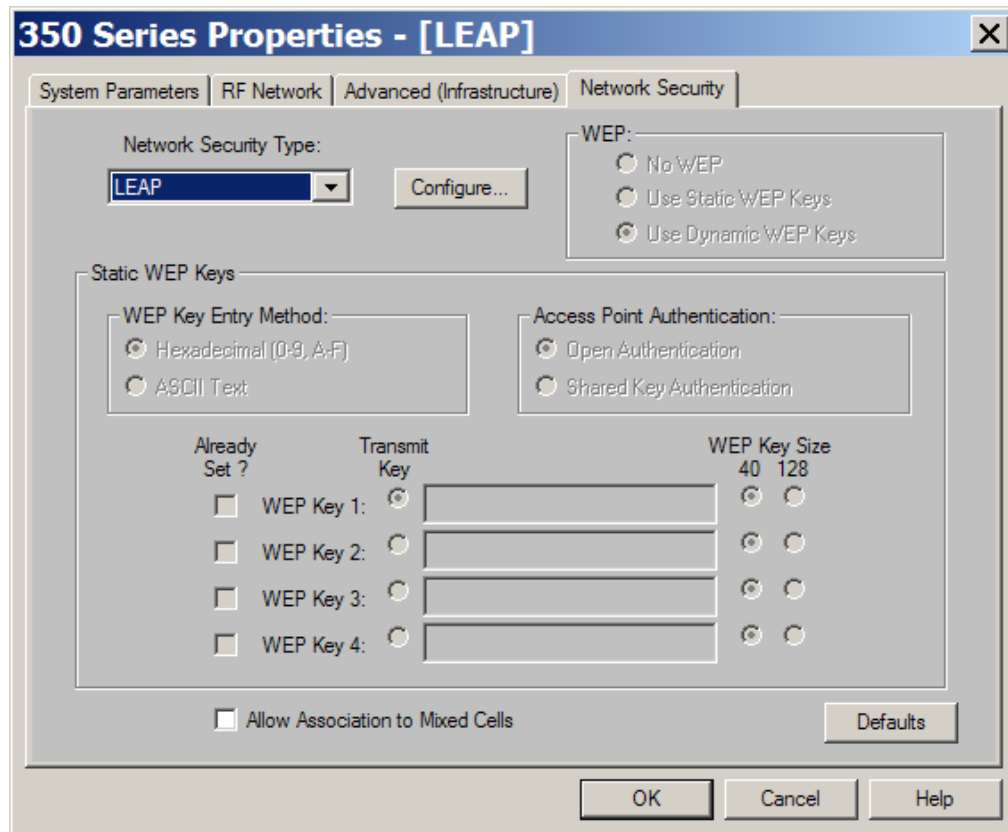
Step 6 Verify the LEAP configuration

Cisco 1200 Access Point

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|------------|-----------|-----------------|-----------|------------|------|--------------|------|------|--------|-------------|-----|------|--|--|---|------|------|------|--------|-------------|-----|------|--|--|---|-----------------|-----|-----|------|----------|-----------|------|------|--------------|--------|--|--|--|--|--|---|---|--|-----------------|-----|-----|------|----------|-----------|------|------|--------------|--------|--|--|--|--|--|---|---|--|------------------------|------|-----|-----|-----------------|-------|------------|----------|--------|---|--|--|--|--|
| <ul style="list-style-type: none"> HOME EXPRESS SET-UP NETWORK MAP + ASSOCIATION NETWORK INTERFACES + SECURITY Admin Access SSID Manager Encryption Manager Server Manager Local RADIUS Server Advanced Security SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG + | <p>Hostname ap ap uptime is 8 minutes</p> <hr/> <p>Security Summary</p> <p>Administrators</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Username</td> <td style="width: 35%;">Read-Only</td> <td style="width: 35%;">Read-Write</td> </tr> <tr> <td>Cisco</td> <td style="text-align: center;">✓</td> <td></td> </tr> </table> <p>Radio0-802.11B SSIDs</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID</td> <td style="width: 10%;">VLAN</td> <td style="width: 15%;">Open</td> <td style="width: 15%;">Shared</td> <td style="width: 30%;">Network EAP</td> </tr> <tr> <td>AP1</td> <td style="text-align: center;">none</td> <td></td> <td></td> <td style="text-align: center;">✓</td> </tr> </table> <p>Radio1-802.11A SSIDs</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID</td> <td style="width: 10%;">VLAN</td> <td style="width: 15%;">Open</td> <td style="width: 15%;">Shared</td> <td style="width: 30%;">Network EAP</td> </tr> <tr> <td>AP1</td> <td style="text-align: center;">none</td> <td></td> <td></td> <td style="text-align: center;">✓</td> </tr> </table> <p>Radio0-802.11B Encryption Settings</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Encryption Mode</td> <td style="width: 5%;">MIC</td> <td style="width: 5%;">PPK</td> <td style="width: 5%;">TKIP</td> <td style="width: 5%;">WEP40bit</td> <td style="width: 5%;">WEP128bit</td> <td style="width: 5%;">CKIP</td> <td style="width: 5%;">CMIC</td> <td style="width: 10%;">Key Rotation</td> </tr> <tr> <td>Cipher</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">✓</td> <td style="text-align: center;">✓</td> <td></td> </tr> </table> <p>Radio1-802.11A Encryption Settings</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Encryption Mode</td> <td style="width: 5%;">MIC</td> <td style="width: 5%;">PPK</td> <td style="width: 5%;">TKIP</td> <td style="width: 5%;">WEP40bit</td> <td style="width: 5%;">WEP128bit</td> <td style="width: 5%;">CKIP</td> <td style="width: 5%;">CMIC</td> <td style="width: 10%;">Key Rotation</td> </tr> <tr> <td>Cipher</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td style="text-align: center;">✓</td> <td style="text-align: center;">✓</td> <td></td> </tr> </table> <p>Server-Based Security</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Server Name/IP Address</td> <td style="width: 10%;">Type</td> <td style="width: 5%;">EAP</td> <td style="width: 5%;">MAC</td> <td style="width: 15%;">Proxy Mobile IP</td> <td style="width: 10%;">Admin</td> <td style="width: 20%;">Accounting</td> </tr> <tr> <td>10.0.1.1</td> <td style="text-align: center;">RADIUS</td> <td style="text-align: center;">✓</td> <td></td> <td></td> <td></td> <td></td> </tr> </table> | Username | Read-Only | Read-Write | Cisco | ✓ | | SSID | VLAN | Open | Shared | Network EAP | AP1 | none | | | ✓ | SSID | VLAN | Open | Shared | Network EAP | AP1 | none | | | ✓ | Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation | Cipher | | | | | | ✓ | ✓ | | Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation | Cipher | | | | | | ✓ | ✓ | | Server Name/IP Address | Type | EAP | MAC | Proxy Mobile IP | Admin | Accounting | 10.0.1.1 | RADIUS | ✓ | | | | |
| Username | Read-Only | Read-Write | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Cisco | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SSID | VLAN | Open | Shared | Network EAP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP1 | none | | | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SSID | VLAN | Open | Shared | Network EAP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AP1 | none | | | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Cipher | | | | | | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Cipher | | | | | | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Server Name/IP Address | Type | EAP | MAC | Proxy Mobile IP | Admin | Accounting | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10.0.1.1 | RADIUS | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

From the **SECURITY** Home page of the AP, verify Network EAP is checked and the only SSID is APP. The default tsunami SSID should be deleted for security. Also verify the Server Based Security is configured correctly as shown.

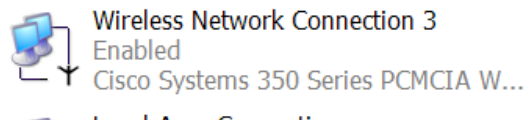
Step 7 Configuring LEAP on the ACU



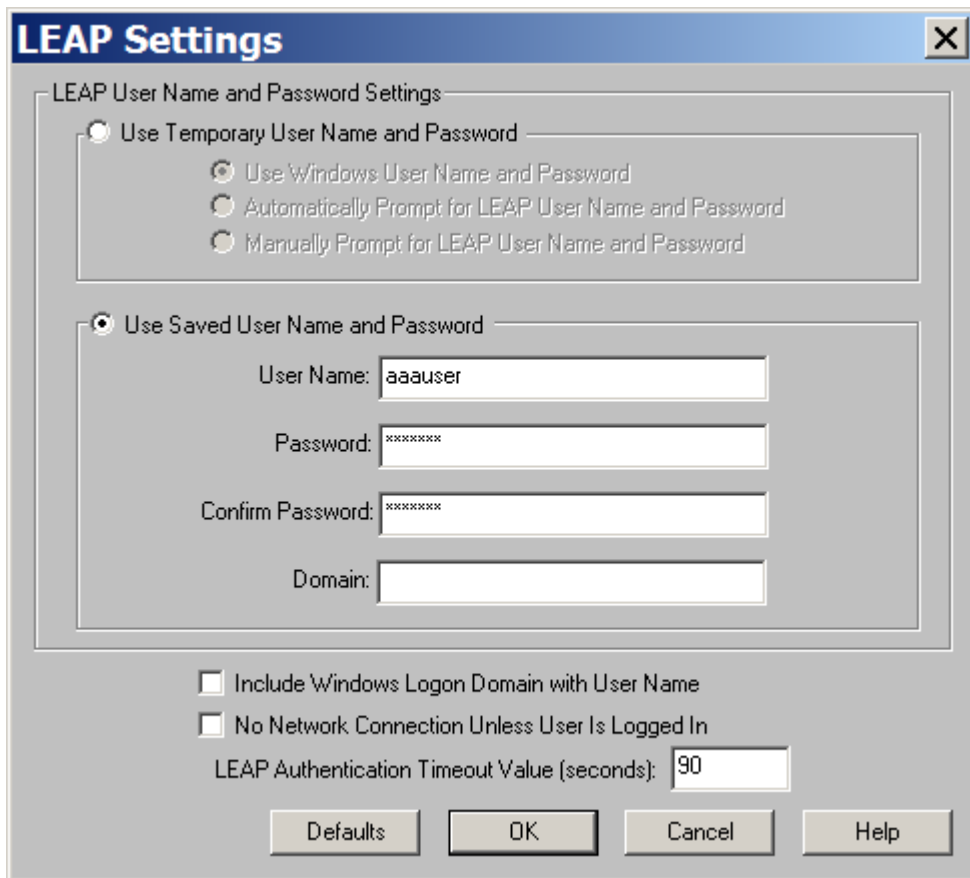
In order to enable the EAP in the Aironet client utility, complete the following steps:

- 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

LAN or High-Speed Internet



- 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?

ANSWER: Associated, Authentication Pending, Authenticated.

Step 8 Verify the wireless connection

Cisco 1200 Access Point

Hostname ap ap uptime is 1 hour, 41 minutes

Association

Clients: 1 Repeaters: 0

View: Client Repeater Apply

Radio802.11B

SSID AP :

| Device Type | Name | IP Address | MAC Address | State | Parent | VLAN |
|-------------|------|------------|----------------|----------------|--------|------|
| 350-client | - | 0.0.0.0 | 0007.eb31.7c12 | EAP-Associated | self | none |

Radio802.11A

From the **ASSOCIATION** page of the AP, verify the association state. This should display all of the connected clients.

Cisco 1200 Access Point

Hostname ap ap uptime is 2 hours, 34 minutes

Event Log

Start Display at Index: 1 Max Number of Events to Display: 20 Previous Next Refresh Clear

| Index | Time | Severity | Description |
|-------|--------------------|-------------|--|
| 1 | Mar 1 02:27:22.139 | Information | Interface Dot11Radio0, Station 0007.eb31.7c12 Associated KEY_MGMT[NONE] |
| 2 | Mar 1 02:27:20.820 | Information | Interface Dot11Radio0, Deauthenticating Station 0007.eb31.7c12 Reason: Previous authentication no longer valid |
| 3 | Mar 1 02:27:20.820 | Warning | Packet to client 0007.eb31.7c12 reached max retries, remove the client |

From the **EVENT LOG** Page of the AP, check the association logs.

Cisco 1200 Access Point

STATISTICS GENERAL SET-UP

Hostname ap ap uptime is 11 minutes

Security: Local RADIUS Server - Statistics

Local RADIUS Server Information

| | | | |
|---------------------------|---|--------------------------|---|
| Successful Authentication | 1 | Unknown Usernames | 0 |
| Client Blocks | 0 | Invalid Passwords | 0 |
| Unknown NAS | 0 | Invalid Packets From NAS | 0 |

Network Access Server Information

View Information for: < ALL servers >

Network Access Server 10.0.1.1

| | | | |
|----------------------------------|---|-------------------------|---|
| Successes | 1 | Unknown Username | 0 |
| Client Blocks | 0 | Invalid Passwords | 0 |
| Corrupted Packets | 0 | Unknown RADIUS Messages | 0 |
| No Username Attribute | 0 | Shared Key Mismatch | 0 |
| Invalid Authentication Attribute | 0 | Invalid State Attribute | 0 |
| Unknown EAP Messages | 0 | Unknown EAP Type | 0 |

User Information

| User Name | Successes | Failures | Blocks |
|-----------|-----------|----------|--------|
| aaauser | 0 | 0 | 0 |
| Cisco1 | 1 | 0 | 0 |

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 8.5.4.1 Configure Enterprise Security on AP

Estimated Time: 30 minutes

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

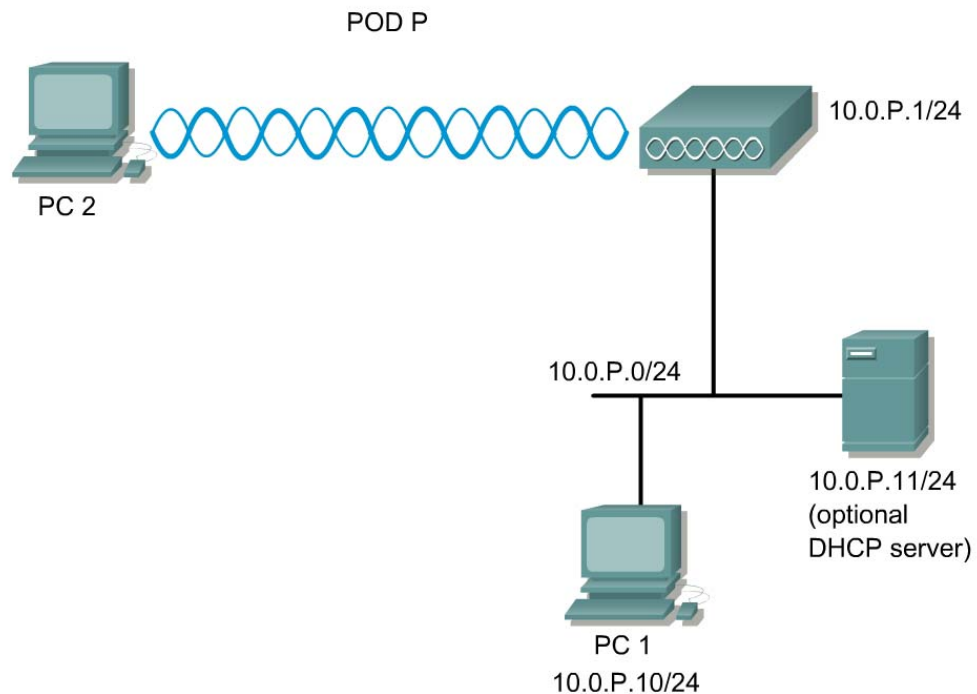
Objective

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

Cisco 1200 Access Point

RADIO0-802.11B
RADIO1-802.11A

Hostname **ap** ap uptime is 15 minutes

Security: Encryption Manager - Radio0-802.11B

Encryption Modes

None
 WEP Encryption Mandatory
Cisco Compliant TKIP Features: Enable MIC Enable Per Packet Keying

Cipher WEP 128 bit

Encryption Keys

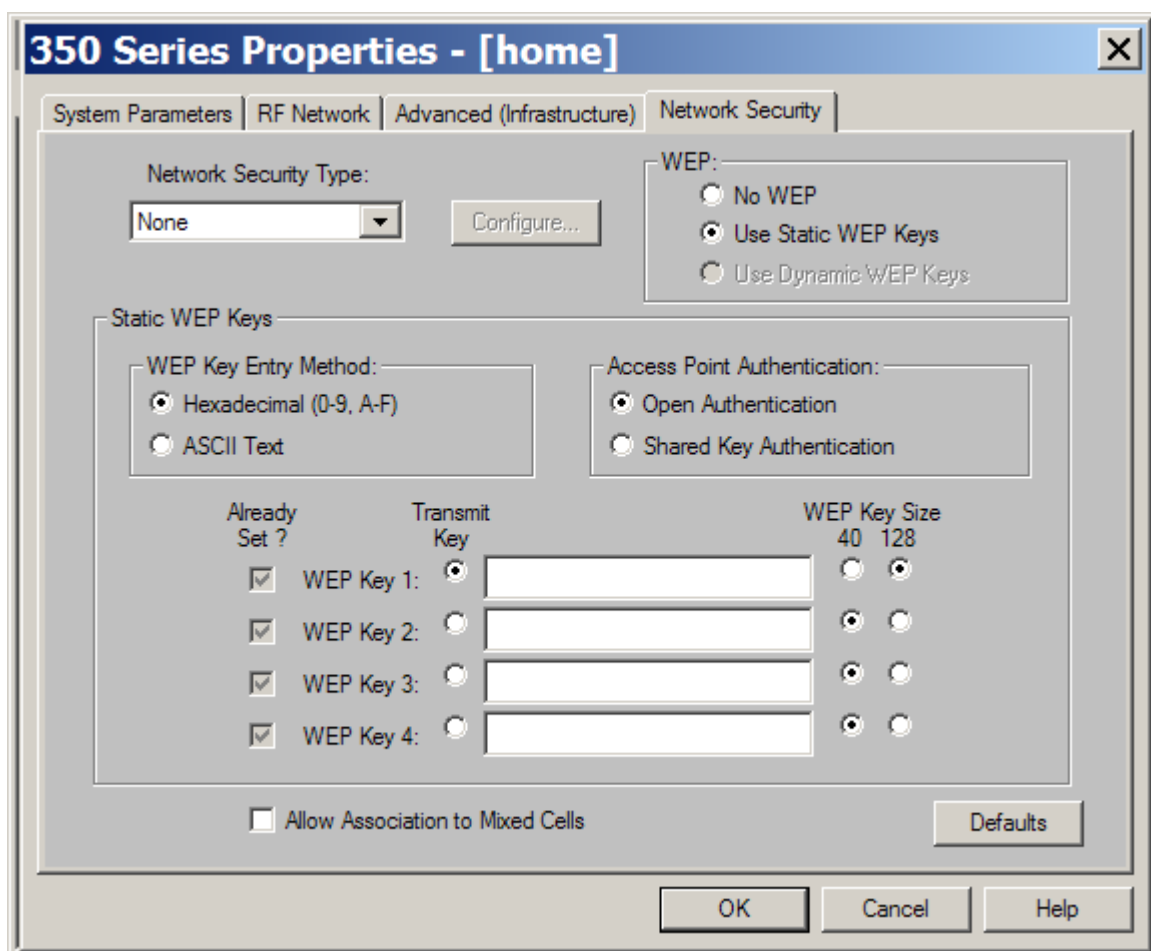
| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|---|--|
| Encryption Key 1: | <input checked="" type="radio"/> | ●●●●●●●●●●●●●●●● | 128 bit |
| Encryption Key 2: | <input type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |

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:
- Select the WEP setting – **Use Static WEP keys**
 - Select the Static WEP key entry method – **Hexadecimal**
 - Select the AP Authentication – **Open authentication**
 - Select and enter the Transmit key [for lab purposes will be] **12345678909876543210123456**
 - Select the WEP key Size – **128 bits**
 - 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.

The screenshot shows the configuration page for a Cisco 1200 Access Point. The main heading is "Cisco 1200 Access Point". Below it, there are tabs for "RADIO0-802.11B" and "RADIO1-802.11A". The page is divided into several sections:

- Security: Encryption Manager - Radio0-802.11B**: This section contains the "Encryption Modes" and "Encryption Keys" settings.
- Encryption Modes**:
 - None
 - WEP Encryption Mandatory
 - Cipher WEP 128 bit
- Cisco Compliant TKIP Features**:
 - Enable MIC
 - Enable Per Packet Keying
- Encryption Keys**:

| | Transmit Key | Encryption Key (Hexadecimal) | Key Size |
|-------------------|----------------------------------|------------------------------|----------|
| Encryption Key 1: | <input checked="" type="radio"/> | •••••••••••••••• | 128 bit |
| Encryption Key 2: | <input type="radio"/> | | 128 bit |
| Encryption Key 3: | <input type="radio"/> | | 128 bit |
| Encryption Key 4: | <input type="radio"/> | | 128 bit |

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**

The screenshot shows the "Aironet Extensions:" section. It contains two radio buttons: Enable and Disable.

- 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.

| | | | | | | | | | |
|----------------------|------------------------------------|-----------|------|--------|-------------|------------|------|------|--------------|
| NETWORK MAP + | Security Summary | | | | | | | | |
| ASSOCIATION | Administrators | | | | | | | | |
| NETWORK INTERFACES + | Username | Read-Only | | | | Read-Write | | | |
| SECURITY | Cisco | ✓ | | | | | | | |
| Admin Access | Radio0-802.11B SSIDs | | | | | | | | |
| SSID Manager | SSID | VLAN | Open | Shared | Network EAP | | | | |
| Encryption Manager | AP1 | none | ✓ | | | | | | |
| Server Manager | Radio1-802.11A SSIDs | | | | | | | | |
| Local RADIUS Server | SSID | VLAN | Open | Shared | Network EAP | | | | |
| Advanced Security | AP1 | none | ✓ | | | | | | |
| SERVICES + | Radio0-802.11B Encryption Settings | | | | | | | | |
| WIRELESS SERVICES + | Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation |
| SYSTEM SOFTWARE + | WEP-Mandatory | ✓ | ✓ | | | | | | |
| EVENT LOG + | Radio1-802.11A Encryption Settings | | | | | | | | |
| | Encryption Mode | MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC | Key Rotation |
| | WEP-Mandatory | ✓ | ✓ | | | | | | |

- g. From the **SECURITY** Page, verify MIC and PPK are enabled.

- h. What does MIC do to protect WEP?

ANSWER: MIC uses a hashing algorithm to stamp the frame. Any changes to the frame will not match the original hash value.

- i. What attack does MIC prevent?

ANSWER: bit flip attacks

- j. Why do the Aironet extensions have to be used?

ANSWER: TKIP is a Cisco proprietary implementation.

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.

Global Properties

Broadcast Key Rotation Interval:

- Disable Rotation
- Enable Rotation with Interval: (10-10000000 sec)

WPA Group Key Update:

- Enable Group Key Update On Membership Termination
- Enable Group Key Update On Member's Capability Change

- 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

The screenshot shows the configuration page for a Cisco 1200 Access Point. The left sidebar contains navigation options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, and SERVICES. The main content area is titled 'Security: Encryption Manager - Radio0-802.11B'. Under 'Encryption Modes', the 'Cipher' radio button is selected, and a dropdown menu is open showing options: WEP 128 bit, WEP 40 bit, TKIP, CKIP, CMIC, CKIP + CMIC, TKIP + WEP 128 bit, and TKIP + WEP 40 bit. Below this, the 'Encryption Keys' section has four rows for 'Encryption Key 1' through 'Encryption Key 4'. Each row has a radio button (Key 1 is selected), an 'Encryption Key (Hexadecimal)' input field, and a 'Key Size' dropdown menu set to '128 bit'.

From the **SECURITY>Encryption Manager** Page.

- Remove Key Rotation configured from the previous step.
- Check the **Cipher** radio button.
- Choose the **TKIP** option in the drop down list
- 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 | | | ✓ | | | | | |

- From the **SECURITY** Page, verify TKIP is enabled.
- Verify the wireless connection from PC2 and the AP.
- 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)

Authenticated Key Management:

None CCKM: **Mandatory** ▼ WPA: **Optional** ▼

WPA Pre-shared Key: ASCII Hexadecimal

- 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

Encryption Keys

Encryption

WEP 128 bit ▼

- WEP 128 bit
- WEP 40 bit
- TKIP
- CKIP
- CMIC
- CKIP + CMIC
- TKIP + WEP 128 bit
- TKIP + WEP 40 bit

Cipher Suites Compatible with WPA and CCKM

| Authenticated Key Management Types | Compatible Cipher Suites |
|------------------------------------|--|
| CCKM | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• 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.

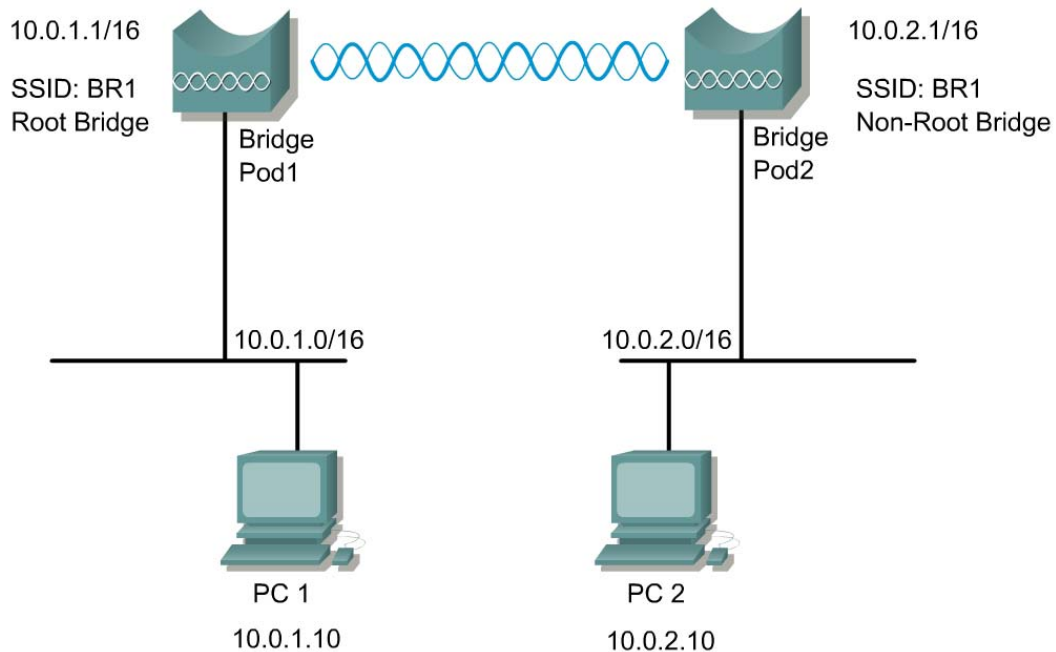
Objective

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.

| <u>Device Name</u> | <u>Label</u> | <u>SSID</u> | <u>Address</u> |
|--------------------|--------------|-------------|----------------|
| 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

- 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.
- Configure PC1 to 10.0.0.2/16.
- Open a web browser and enter the default bridge address <http://10.0.0.1> and press **Enter**.
- Either of the following pages will appear:
 - The **Summary Status** Page, also known as the **Home** Page
 - The **Express Setup** Page

BR350-5aa7d6 Summary Status
Cisco 350 Series Bridge 12.03T

Home Map Network Associations **Setup** Logs Help

Uptime: 00:13:00

Current Associations

| | | | |
|-----------------|-------------------|-----------------|--------|
| Clients: 0 of 0 | Repeaters: 0 of 0 | Bridges: 0 of 1 | APs: 0 |
|-----------------|-------------------|-----------------|--------|

Recent Events

| Time | Severity | Description |
|------|----------|-------------|
| | | |

Network Ports *Diagnostics*

| Device | Status | Mb/s | IP Addr. | MAC Addr. |
|------------|--------|-------|----------|--------------|
| Ethernet | Up | 100.0 | 10.0.0.1 | 0040965aa7d6 |
| Root Radio | Up | 11.0 | 10.0.0.1 | 0040965aa7d6 |

BR350-5aa7d6 Express Setup
Cisco 350 Series Bridge 12.03T

Home Map Help

Uptime: 00:14:22

System Name: BR350-5aa7d6
MAC Address: 00:40:96:5aa7:d6


Configuration Server Protocol: DHCP
Default IP Address: 10.0.0.1
Default IP Subnet Mask: 255.255.255.0
Default Gateway: 255.255.255.255

Root Radio:
Service Set ID (SSID): tsunami more...
Role in Radio Network: Root Bridge
Optimize Radio Network For: Throughput Range Custom
Ensure Compatibility With: 2Mb/sec Clients

Security Setup
SNMP Admin. Community:

Apply OK Cancel Restore Defaults

- 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.

BR350-5aa7d6 Setup **CISCO SYSTEMS**


Cisco 350 Series Bridge 12.03T Uptime: 00:17:25

[Home](#) [Map](#) [Network](#) [Associations](#) [Setup](#) [Logs](#) [Help](#)

Express Setup

Associations

| | | | |
|----------------------------------|----------------------------------|----------------------------------|------------------------------|
| Display Defaults | Spanning Tree | Port Assignments | Advanced |
| Address Filters | Protocol Filters | VLAN | Service Sets |

Event Log

| | | |
|----------------------------------|--------------------------------|-------------------------------|
| Display Defaults | Event Handling | Notifications |
|----------------------------------|--------------------------------|-------------------------------|

Services


| | | | |
|--------------------------------|-----------------------------|----------------------------|---------------------------------|
| Console/Telnet | Boot Server | Routing | Name Server |
| Time Server | FTP | Web Server | SNMP |
| Cisco Services | Security | Accounting | Proxy Mobile IP |

Network Ports *Diagnostics*

| | | | | |
|----------------------------|--------------------------------|--------------------------|-------------------------|--------------------------|
| Ethernet | Identification | Hardware | Filters | Advanced |
| Root Radio | Identification | Hardware | Filters | Advanced |

- f. Click on the Express Setup link. This will bring up the Express Setup Page.

Step 4 Configure the bridge settings

BR350-5aa7d6 Express Setup **CISCO SYSTEMS**


Cisco 350 Series Bridge 12.03T Uptime: 00:23:24

[Home](#) [Map](#) [Help](#)

System Name:

MAC Address:

Configuration Server Protocol:

Default IP Address:

Default IP Subnet Mask:

Default Gateway:

Root Radio:

Service Set ID (SSID): [more...](#)

Role in Radio Network:

Optimize Radio Network For: Throughput Range Custom

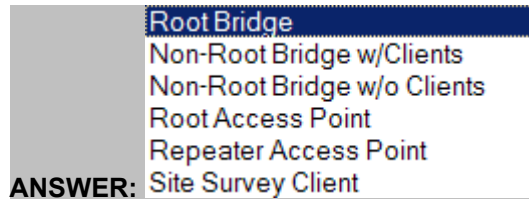
Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community:

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?

ANSWER: The BR350 is made for harsh environments such as outdoor or industrial settings where the 1200 may not be suited.

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?

ANSWER: Yes

- 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?

ANSWER: This should range from 4 to 7 Mbps

- f. What is the distance limitation between two wireless bridges?

ANSWER: up to 25 miles at 1Mbps

- g. What is the distance limitation between an AP and a Bridge?

ANSWER: 1 mile.

- h. Why are 2 bridges able to connect at longer distances?

ANSWER: The bridge modifies the wireless frame timing.

Step 6 Configure WEP on both bridges

BPod1 Root Radio Data Encryption

Cisco 350 Series Bridge 12.03T

Map Help

Uptime: 02:34:02

If VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Use of Data Encryption by Stations is: Not Available
Must set an Encryption Key or enable Broadcast Key Rotation first

| | Open | Shared | Network-EAP |
|-----------------------------|-------------------------------------|--------------------------|--------------------------|
| Accept Authentication Type: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Require EAP: | <input type="checkbox"/> | <input type="checkbox"/> | |

| Transmit With Key | Encryption Key | Key Size |
|-------------------|----------------------|-----------|
| WEP Key 1: | <input type="text"/> | not set ▼ |
| WEP Key 2: | <input type="text"/> | not set ▼ |
| WEP Key 3: | <input type="text"/> | not set ▼ |
| WEP Key 4: | <input type="text"/> | not set ▼ |

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Apply OK Cancel Restore Defaults

Follow these steps to set up WEP keys and enable WEP:

- On the Summary Status page, click **Setup**.
- On the Setup page, click **Security**.
- On the Security Setup page, click **Radio Data Encryption (WEP)**.
- From the **Root Radio Data Encryption** page.
- Before WEP can be enabled, a WEP key must be entered in at least one of the Encryption Key fields.
- Use the Key Size pull-down menu to select the **128-bit** encryption for the WEP Key 1.
- Click in the Encryption Key field and enter a WEP key.
- How many digits must be entered for 128 bit WEP?

ANSWER: 26

- i. Record the key below.


ANSWER: Answers will vary. **Example:** 12345678909876543210123456

- j. Click Apply to save the WEP Key.

BPod1 Root Radio Data Encryption

Cisco 350 Series Bridge 12.03T

[Map](#) [Help](#)



Uptime: 02:30:52

If VLANs are *not* enabled, set Radio Data Encryption on this page. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Use of Data Encryption by Stations is: No Encryption ▾

| | | | |
|-----------------------------|-------------------------------------|--------------------------|--------------------------|
| Accept Authentication Type: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Require EAP: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| | Transmit With Key | Encryption Key | Key Size |
|------------|----------------------------------|----------------|-----------|
| WEP Key 1: | <input checked="" type="radio"/> | | 128 bit ▾ |
| WEP Key 2: | - | | not set ▾ |
| WEP Key 3: | - | | not set ▾ |
| WEP Key 4: | - | | not set ▾ |

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Apply OK Cancel Restore Defaults

- 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?

ANSWER: Answers should be yes. If not, check the WEP keys.

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?

ANSWER: This should range from 4 to 7 Mbps. Should be no or minimal

- c. What other enhancements can be used to improve WEP security?

ANSWER: TKIP, MIC, BKR

- d. What technology can be used at layer 3 to improve security of the wireless link?


ANSWER: ACLs and IPSec VPN

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.

BPod1 Setup

Cisco 350 Series Bridge 12.03T



Uptime: 03:19:36

Home | Map | Network | Associations | Setup | Logs | Help

[Express Setup](#)

| Associations | | | | |
|----------------------------------|----------------------------------|----------------------------------|------------------------------|--|
| Display Defaults | Spanning Tree | Port Assignments | Advanced | |
| Address Filters | Protocol Filters | VLAN | Service Sets | |

| Event Log | | |
|----------------------------------|--------------------------------|-------------------------------|
| Display Defaults | Event Handling | Notifications |

| Services | | | |
|--------------------------------|-----------------------------|----------------------------|---------------------------------|
| Console/Telnet | Boot Server | Routing | Name Server |
| Time Server | FTP | Web Server | SNMP |
| Cisco Services | Security | Accounting | Proxy Mobile IP |

| Network Ports | | | | | <i>Diagnostics</i> |
|----------------------------|--------------------------------|--------------------------|-------------------------|--------------------------|--------------------|
| Ethernet | Identification | Hardware | Filters | Advanced | |
| Root Radio | Identification | Hardware | Filters | Advanced | |

- a. From the Setup Page, click **Root Radio** advanced link

Radio Cell Role: Access Point/Root ▾

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any *other* SSID: yes no

Use Aironet Extensions: yes no

Classify Workgroup Bridges as Network Infrastructure: yes no

Require use of Internal Radio Firmware: 5.20U yes no

Ethernet Encapsulation Transform: RFC1042 ▾

Bridge Spacing (km): 0

Quality of Service Setup

If VLANs are *not* enabled, set the following three parameters on this page. If VLANs are enabled, parameters are set independently for each enabled VLAN through [VLAN Setup](#).

Enhanced MIC verification for WEP: MMH ▾

Temporal Key Integrity Protocol: CISCO ▾

Broadcast WEP Key rotation interval (sec): 0 (0=off)

- 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.
- e. What attack does TKIP prevent?

ANSWER: Initialization Vector attacks

- f. Why do the Aironet extensions have to be used?

ANSWER TKIP is a Cisco proprietary implementation.

- 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.
- g. What attack does BKR prevent?

ANSWER: Initialization Vector attacks

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.

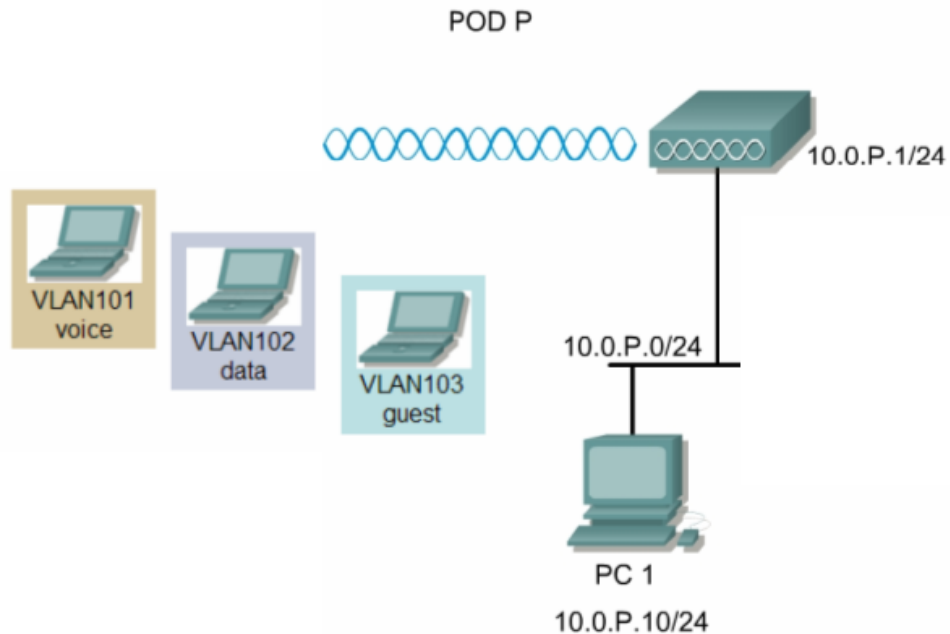
Scenario

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

| <u>Team</u> | <u>Access Point Name</u> | <u>SSID</u> | <u>VLAN</u> | <u>Authentication</u> | <u>Bridge group</u> | <u>BVI Address</u> |
|-------------|--------------------------|-------------|-------------|-----------------------|---------------------|--------------------|
| 1 | PodP | management | 10 | Network EAP | 1 | 10.0.P.1/24 |
| | | voice | 101 | Shared | 101 | |
| | | data | 102 | Network EAP | 102 | |
| | | guest | 103 | Open | 103 | |

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

The screenshot displays the 'Express Set-Up' configuration page for an AP. The page title is 'Hostname ap' and it shows 'ap uptime is 41 minutes'. The configuration fields are as follows:

- System Name: Pod1
- MAC Address: 000b.f4a.700c
- Configuration Server Protocol: DHCP Static IP
- IP Address: 10.0.1.1
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- SNMP Community: defaultCommunity
- SNMP Read-Only: Read-Only Read-Write

From the **EXPRESS SET-UP** page, configure the System Name and BVI address.

Step 2 Define the SSIDs and Authentication Type

The screenshot shows the Cisco 1200 Access Point configuration page for the SSID Manager. The page is titled "Cisco 1200 Access Point" and "Security : SSID Manager - Radio0:802.11B". The "Current SSID List" is visible, showing a dropdown menu with options: "< NEW >", "data", "guest", "management", and "voice". The "management" option is selected. Below the list, there are buttons for "Delete-Radio0" and "Delete-All". The "Authentication Methods Accepted" section includes checkboxes for "Open Authentication" (checked), "Shared Authentication", and "Network EAP". Each has a dropdown menu set to "< NO ADDITION >". The "Authenticated Key Management" section has radio buttons for "None" (selected), "CCKM: Mandatory", and "WPA: Optional". The "WPA Pre-shared Key" section has a text input field and radio buttons for "ASCII" (selected) and "Hexadecimal". The "EAP Client (optional)" section has "Username:" and "Password:" text input fields. The "Association Limit (optional)" is set to "(1-255)". There are checkboxes for "Enable Proxy Mobile IP" and "Enable Accounting". At the bottom right, there are buttons for "Apply-Radio0", "Apply-All", and "Cancel".

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

Answer: It is more secure.

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.

- 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.
- Choose the *management* SSID from the **SSID** drop down box.
- Click **Apply**.
- Repeat the steps for the voice, data, and guest VLANs.

Step 4 Verify the Configuration through GUI

| Radio0-802.11B SSIDs | | | | |
|----------------------|------|------|--------|-------------|
| SSID | VLAN | Open | Shared | Network EAP |
| data | 102 | | | ✓ |
| guest | 103 | ✓ | | |
| management | 10 | | | ✓ |
| voice | 101 | | ✓ | |

From the **SECURITY** home page

- 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)

Cisco 1200 Access Point

Hostname PodP PodP uptime is 1 hour, 15 minutes

HOME

EXPRESS SET-UP

NETWORK MAP +

ASSOCIATION

NETWORK INTERFACES +

SECURITY

Admin Access

SSID Manager

Encryption Manager

Server Manager

Local RADIUS Server

Advanced Security

SERVICES +

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

Security Summary

Administrators

| Username | Read-Only | Read-Write |
|----------|-----------|------------|
| Cisco | ✓ | |

Radio0-802.11B SSIDs

| SSID | VLAN | Open | Shared | Network EAP |
|------------|------|------|--------|-------------|
| data | 102 | | | ✓ |
| guest | 103 | ✓ | | |
| management | 10 | | | ✓ |
| voice | 101 | | ✓ | |

Radio1-802.11A SSIDs

| SSID | VLAN | Open | Shared | Network EAP |
|------------|------|------|--------|-------------|
| data | 102 | | | ✓ |
| guest | 103 | ✓ | | |
| management | 10 | | | ✓ |
| voice | 101 | | ✓ | |

- 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? _____

Answer: Yes

- b. Now change the PC2 to the Voice VLAN.

Hint: Remember this VLAN has WEP Mandatory.

Can the PCs ping each other? _____

Answer: No

- c. Finally, change the PC1 to the Voice VLAN.
Can the PCs ping each other? _____

Answer: Yes

- 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)

.....

Cisco 1200 Access Point

| | | | | |
|--------------------------------|---------------|------|-----------------------------------|-------------|
| HOME | Hostname PodP | | PodP uptime is 1 hour, 15 minutes | |
| EXPRESS SET-UP | | | | |
| NETWORK MAP + | | | | |
| ASSOCIATION | | | | |
| NETWORK INTERFACES + | | | | |
| SECURITY | | | | |
| Admin Access | | | | |
| SSID Manager | | | | |
| Encryption Manager | | | | |
| Server Manager | | | | |
| Local RADIUS Server | | | | |
| Advanced Security | | | | |
| SERVICES + | | | | |
| WIRELESS SERVICES + | | | | |
| SYSTEM SOFTWARE + | | | | |
| EVENT LOG + | | | | |
| Security Summary | | | | |
| Administrators | | | | |
| Username | Read-Only | | Read-Write | |
| Cisco | ✓ | | | |
| Radio0-802.11B SSIDs | | | | |
| SSID | VLAN | Open | Shared | Network EAP |
| data | 102 | | | ✓ |
| guest | 103 | ✓ | | |
| management | 10 | | | ✓ |
| voice | 101 | | ✓ | |
| Radio1-802.11A SSIDs | | | | |
| SSID | VLAN | Open | Shared | Network EAP |
| data | 102 | | | ✓ |
| guest | 103 | ✓ | | |
| management | 10 | | | ✓ |
| voice | 101 | | ✓ | |

- Now create the SSIDs for the 802.11a radio and apply to the existing VLANs.
- Verify the settings afterwards through the **SECURITY** home page.
- Verify the setting through IOS CLI.
- Return to Step 6 and configure 2 802.11a clients. Verify the connections.
- 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 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.

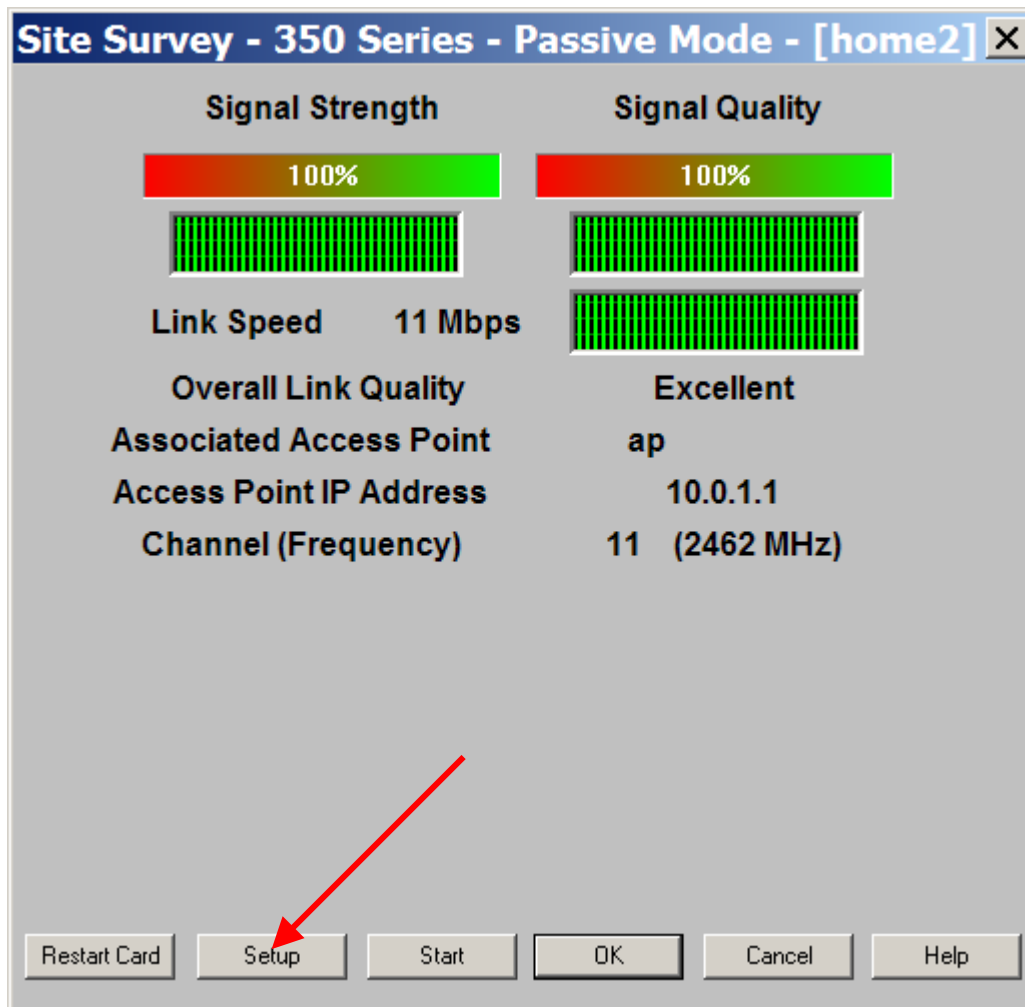
Tools and resources

The following tools and resources will be helpful with this lab:

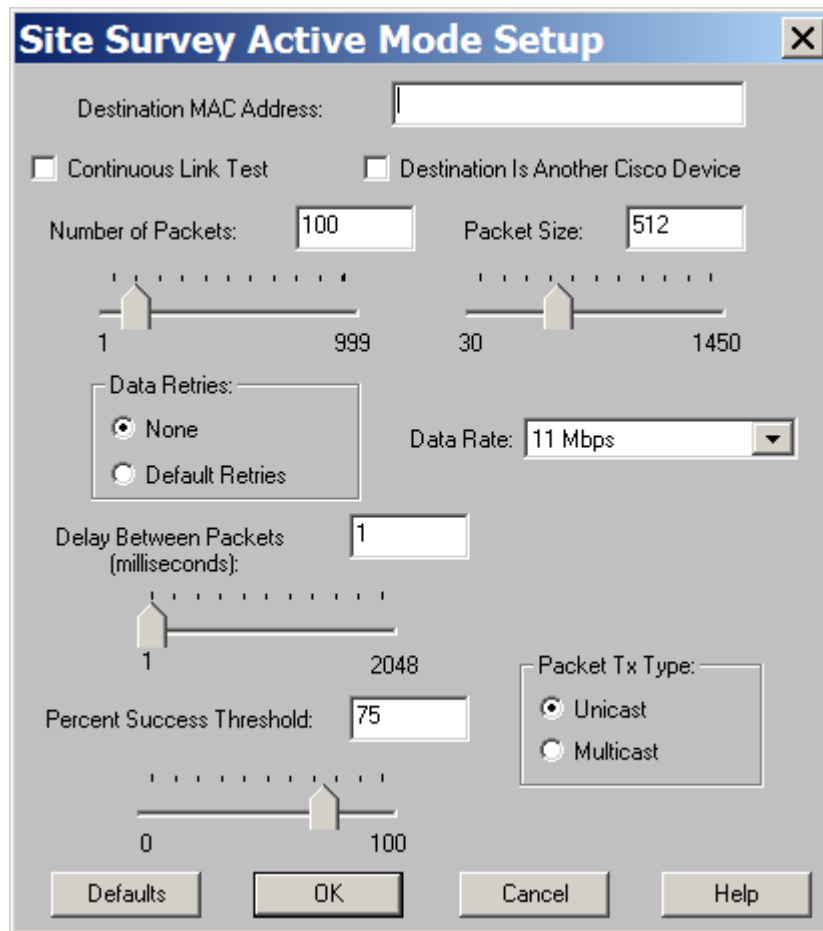
- An AP with a valid IP address
- PC or laptop with a client adapter and client utilities installed

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:

- a. What is the signal strength?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 75%

- b. What is the signal quality?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 18%

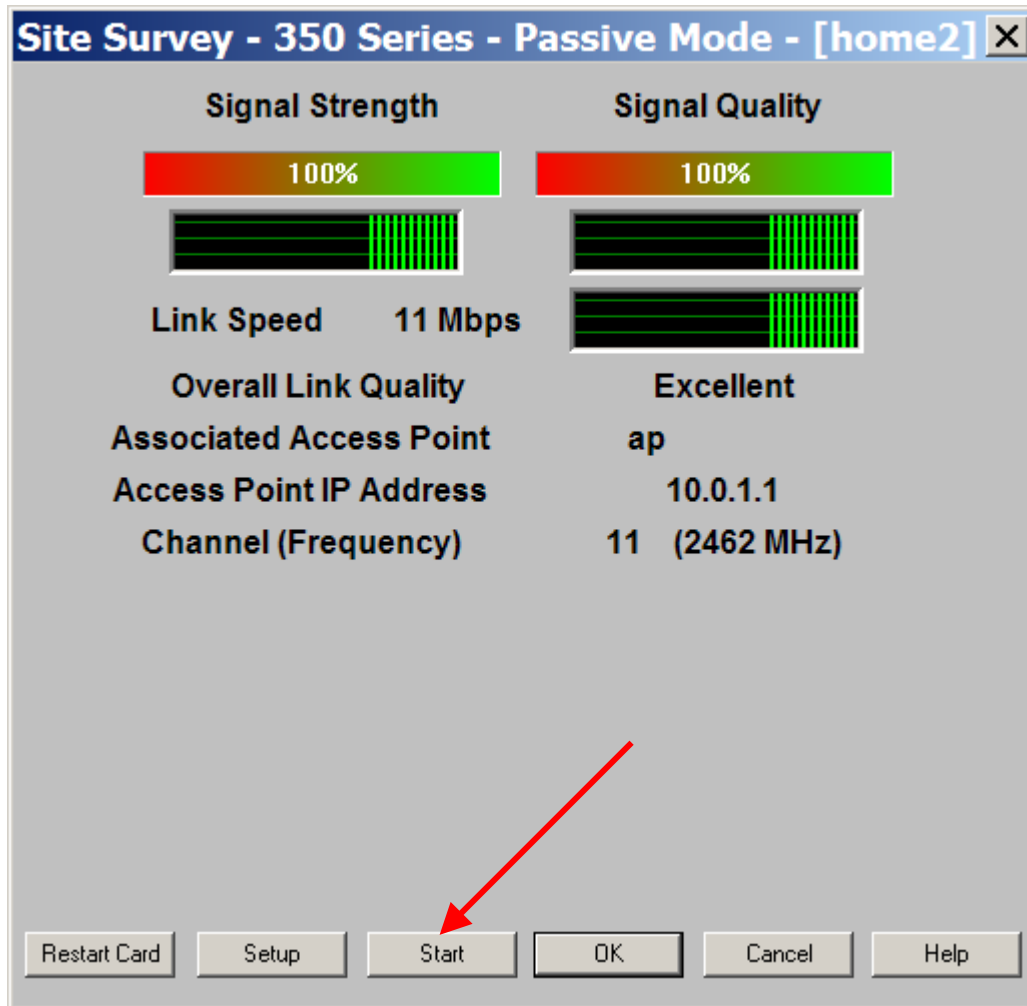
- c. What is the link speed?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 11Mbps

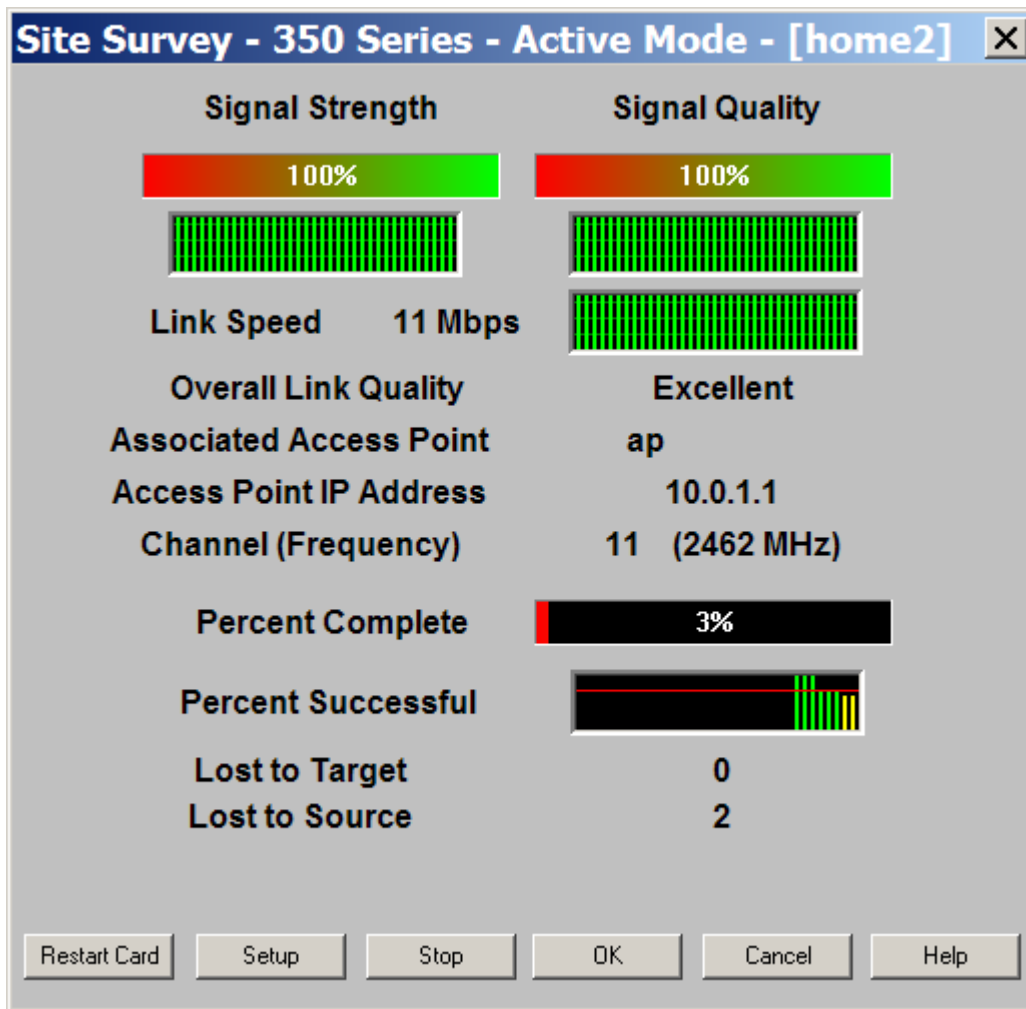
- d. What is the overall link quality?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** POOR

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?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 65%

- b. What is the signal quality?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 13%

- c. What is the link speed?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 11Mbps

- d. What is the overall link quality?

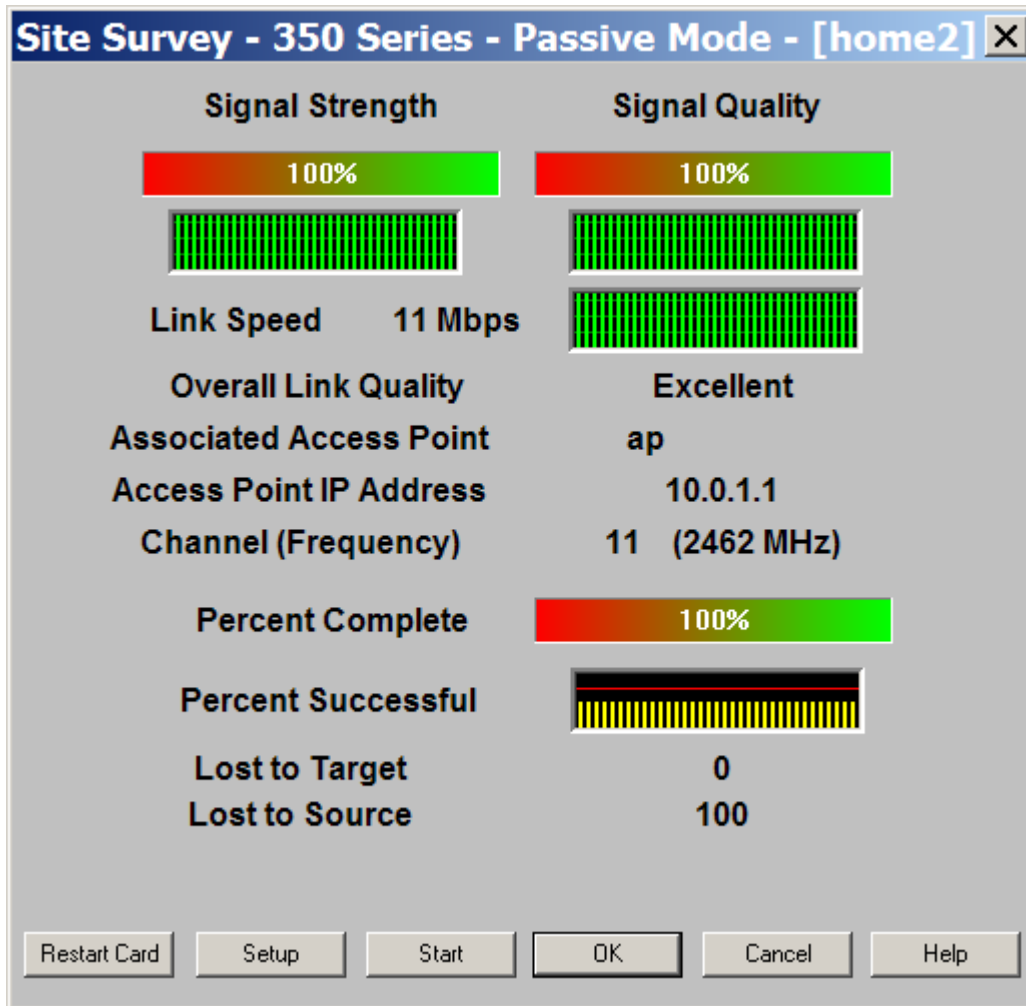
ANSWER: Answers will vary. Document the measurement on your screen. **Example:** POOR

e. How many packets were lost to target?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 0

f. How many packets were lost to source?

ANSWER: Answers will vary. Document the measurement on your screen. **Example:** 0



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:

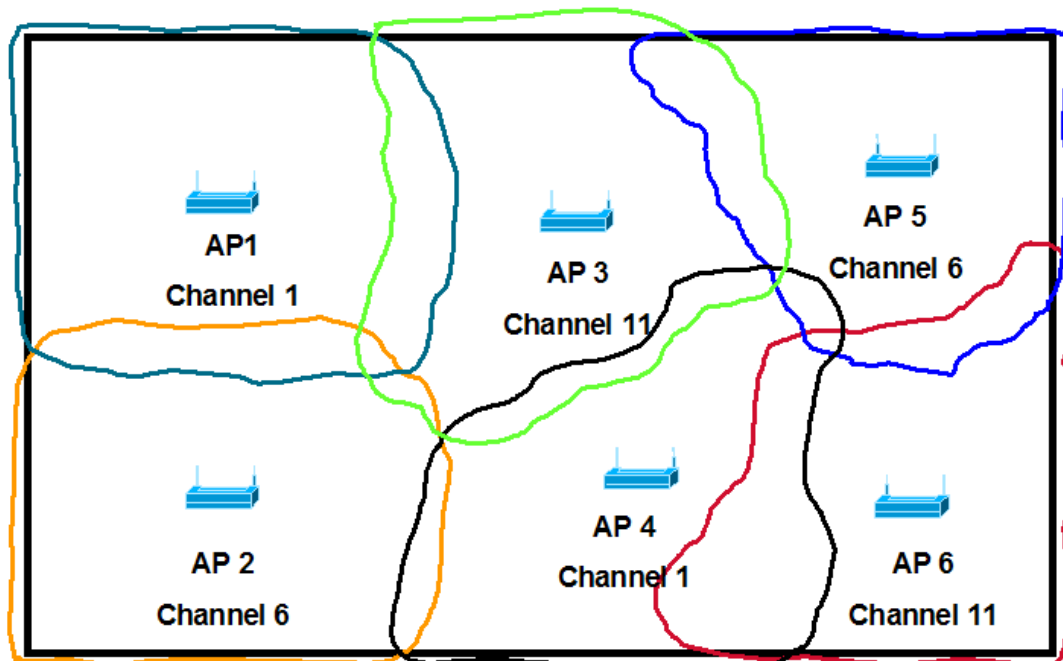
- Channel selections
- Data rates
- Antenna selection

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:

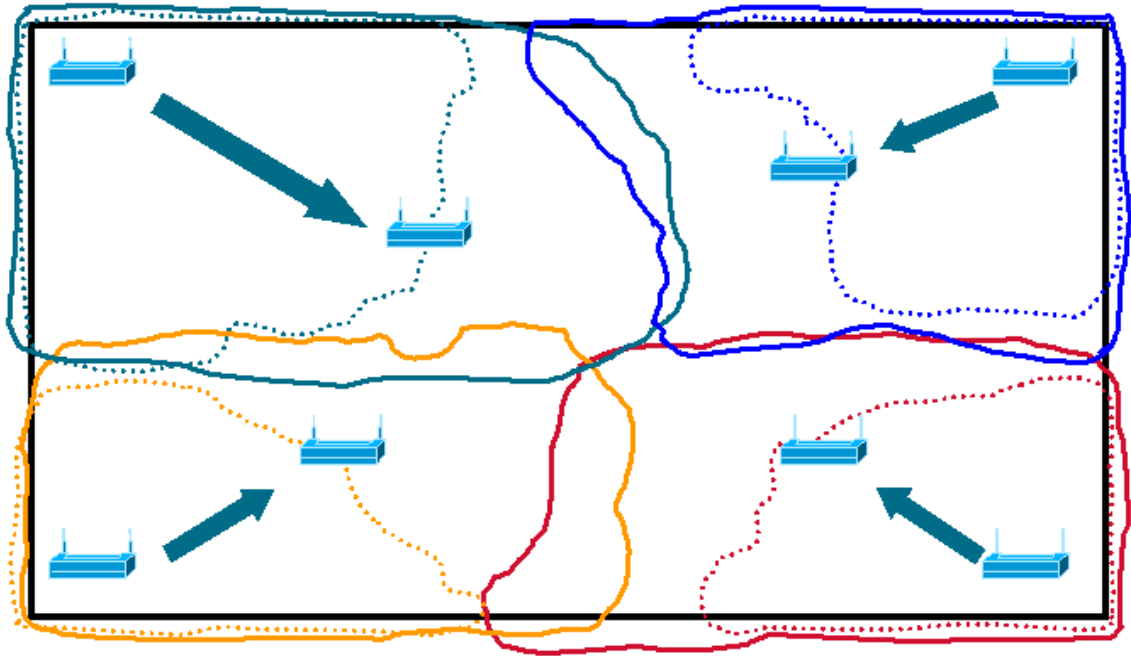
- Read through the lab prior to conducting the site survey.
- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.
- Conduct the site survey with all variables set to operational values 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

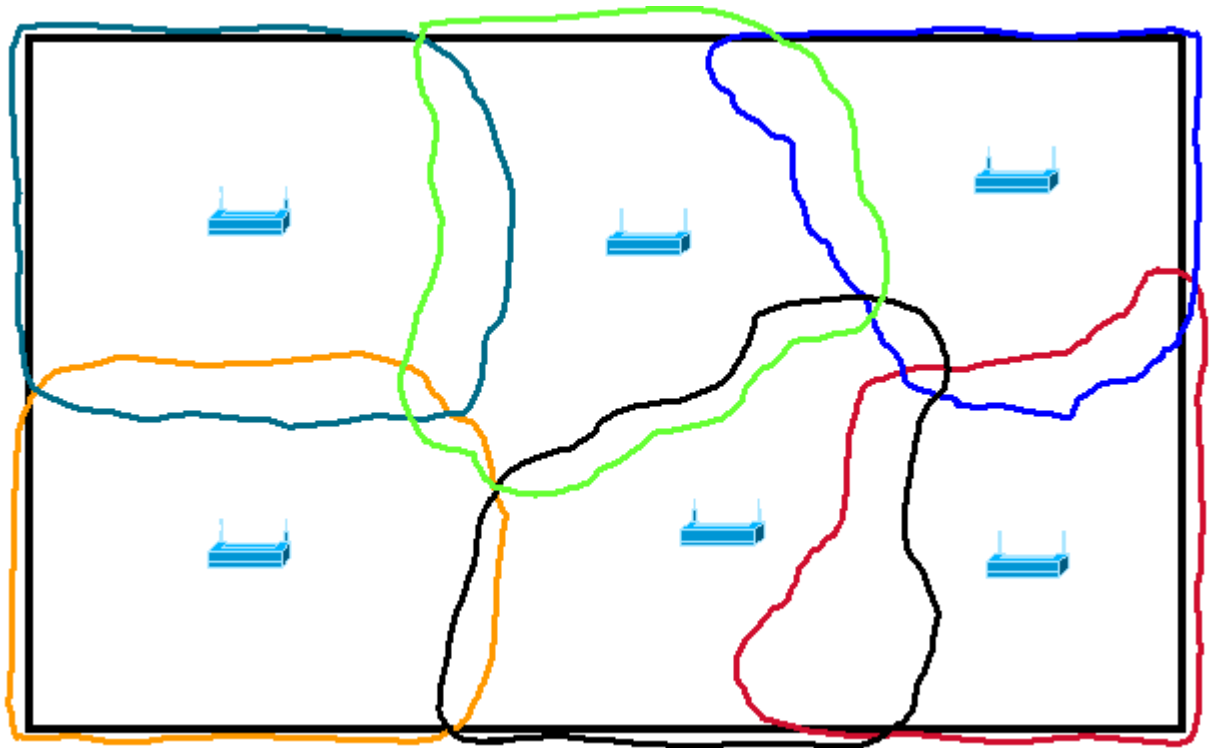


The easiest way to start a site survey is to pick one area of the facility that needs coverage. Choose a corner and place the AP in that corner. Survey the coverage of that AP and make a note of where the furthest point of coverage is from it. Then move the AP to the furthest coverage point.

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



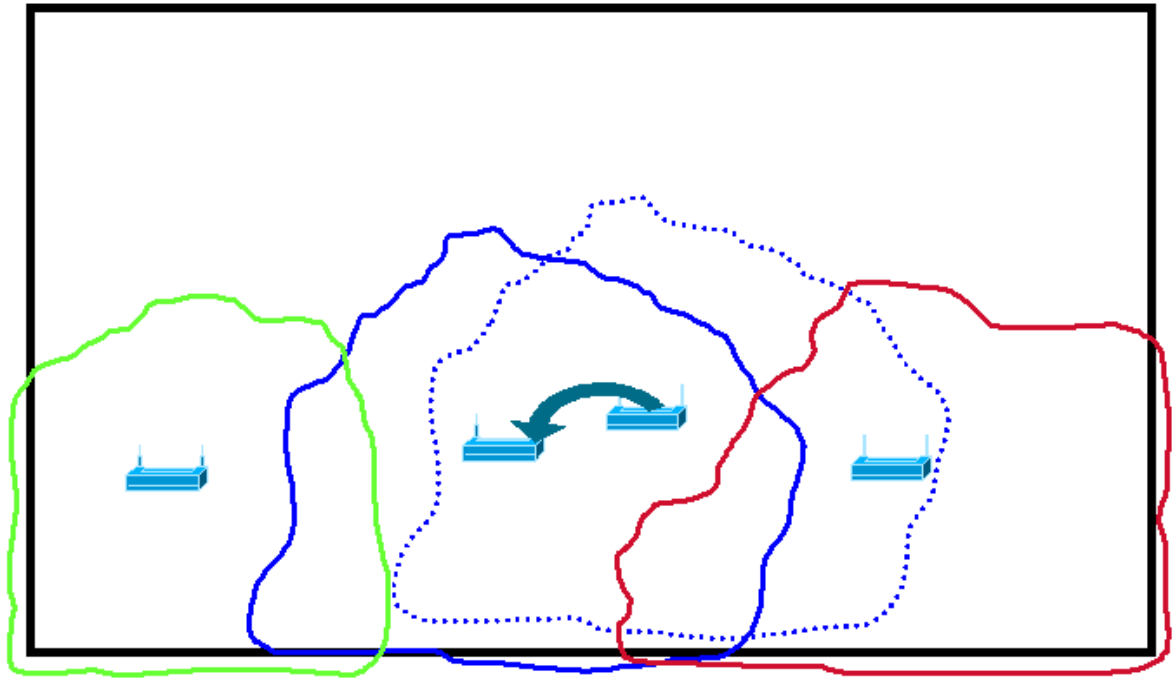
Once the AP has been moved, survey its coverage. It may be necessary to move the AP several times in order to find the best placement.

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



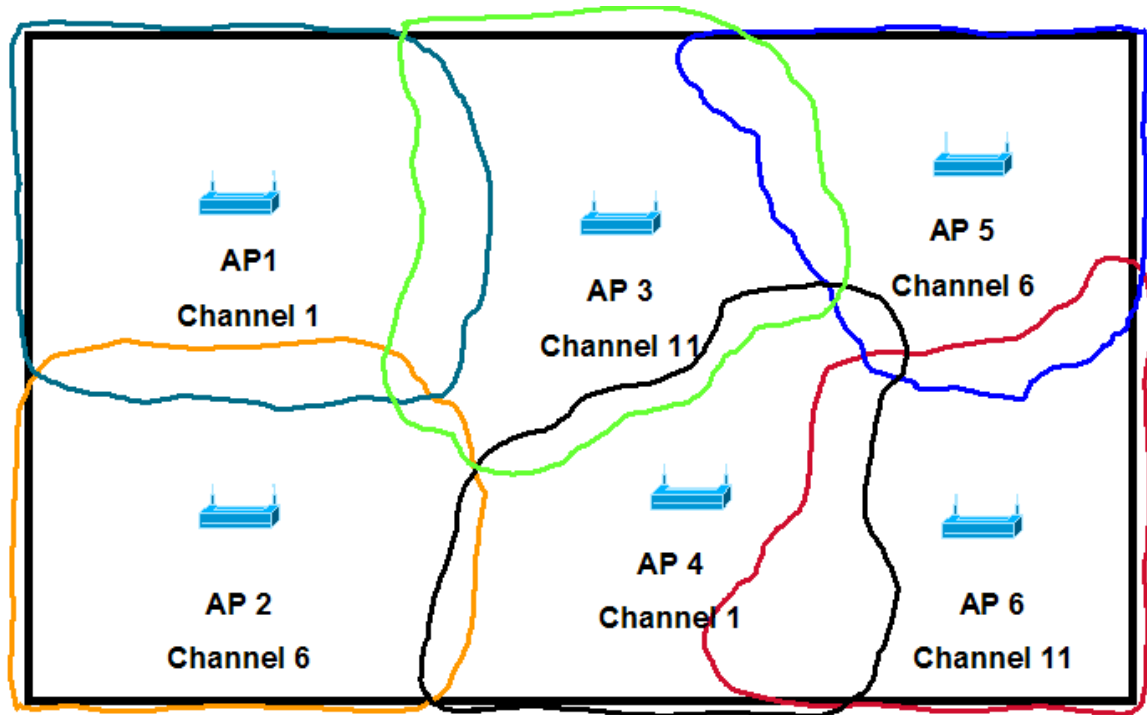
Survey the first two areas and fill in the middle

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

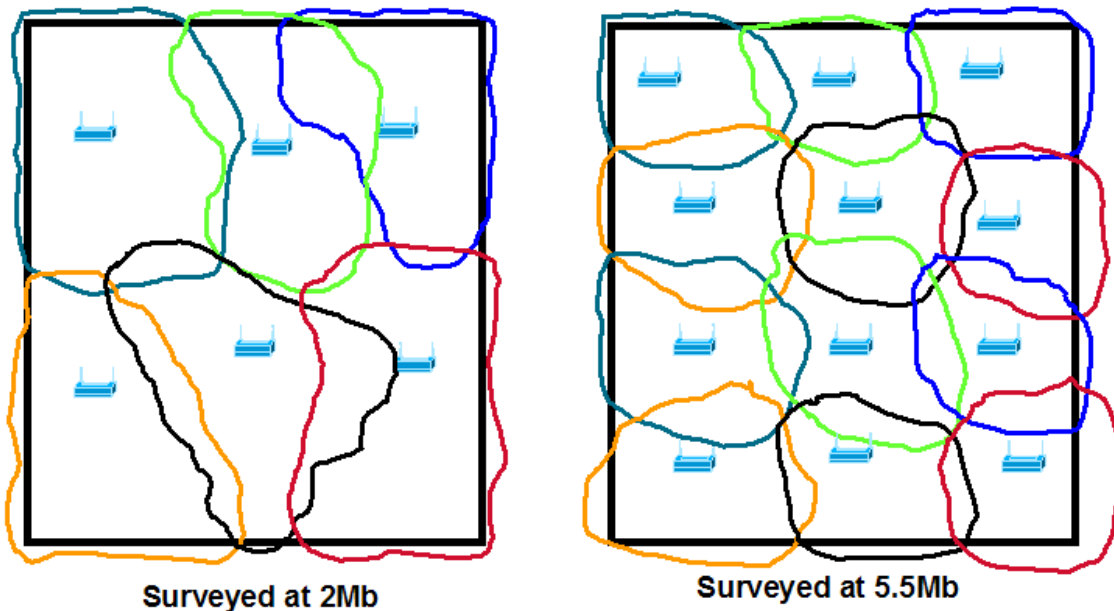


When surveying, take into account the fact that there are only three non-overlapping channels when using 802.11b and 802.11g. In order to maximize the data rate, use these channels. Using the non-overlapping channels insures that the APs will not interfere with each other.

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, and not 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.

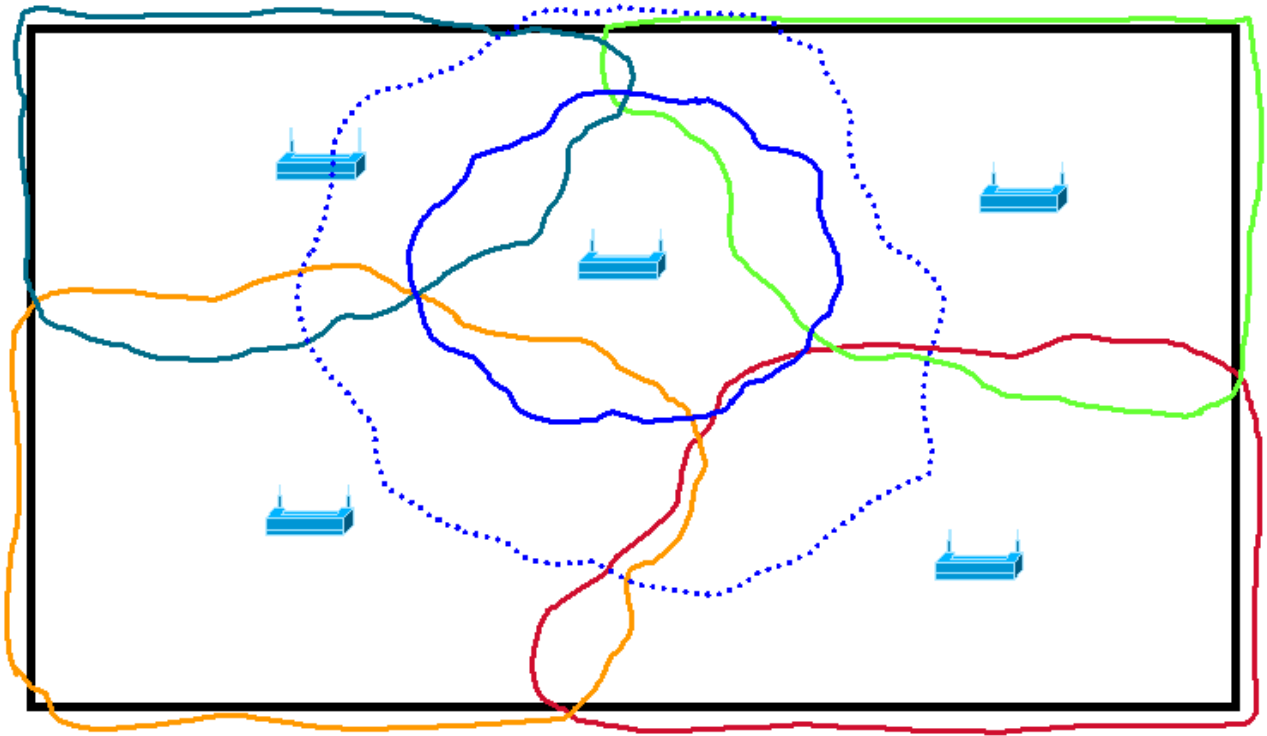
Sketch the actual site below which is surveyed. Indicate where the APs will be located and the channels to be used. Draw the patterns of coverage.

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.