# Make Mine Wireless (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Objective

Explain how wireless LAN components are deployed in a small- to medium-sized business.

Instructor Notes: This activity can be completed individually, in small groups, or as a class.

## Scenario

As the network administrator for your small- to medium-sized business, you realize that your wireless network needs updating, both inside and outside of your building. Therefore, you decide to research how other businesses and educational and community groups set up their WLANs for better access to their employees and clients.

To research this topic, you visit the Customer Case Studies and Research website to see how other businesses use wireless technology. After viewing a few of the videos, or reading some of the case study PDFs, you decide to select two to show to your CEO to support upgrading to a more robust wireless solution for your company.

To complete this class modeling activity, open the accompanying PDF for further instructions on how to proceed.

## Resources

Internet access to the WWW

### Step 1: Open your browser and the URL specified for this activity.

a. Choose two case studies about wireless LAN upgrades from the list to read, located on the Customer Case Studies and Research website.

b. As you view the media or read the PDFs, write notes for the following categories:

   1) The WLAN ***challenge*** that the company sought to mitigate

   2) The ***solution*** that was found to the challenge

   3) The ***results*** that were gained by WLAN updates

### Step 2: Share your findings.

a. Share your findings with the class or a classmate.

b. Play the media or show the PDF for one of the case studies you chose from the URL page.

c. In your own words, explain the challenge, solution, and results learned from the media or PDF.

d. Explain how the results you found could be applied to improve your company's network.

## Instructor Suggested Example

### Barrick Gold Corporation

#### Challenge

Provide continuous access and updates to the Caterpillar Minestar software for fleet management, drilling and blasting, loading, hauling, dozing, and truck management.

#### Solutions

Created an outdoor mesh wireless network, deployed on solar-powered trailers across the mine and inside the mining pit.

### Results

- Closely monitored dispatch process and managed operational efficiency.
- Improved productivity and safety.
- Cut costs by implementing single network for communications and data sharing of new applications.

## Identify elements of the model that map to IT-related content:

- Wireless topologies
- Inside-building wireless solutions
- Outside-building wireless solutions
- Wireless LAN devices
- Wireless LAN communication

# Lab – Investigating Wireless Implementations (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Objectives

**Part 1: Explore Integrated Wireless Routers**

**Part 2: Explore Wireless Access Points**

## Background / Scenario

The number of mobile devices, such as smart phones, tablets, and laptops, continues to increase. These mobile devices can connect via integrated wireless routers or wireless access points (WAPs) to access the Internet and other network resources. Wireless routers are typically employed in home and small business networks. WAPs are more common in larger, more complex networks.

In this lab, you will explore some integrated wireless routers and Cisco WAPs. You will access online emulators for some of Linksys routers and Cisco WAPs. The emulators imitate the configuration screens for the Linksys routers and Cisco WAPs.

## Required Resources

Device with Internet access

# Part 1: Explore Integrated Wireless Routers

Integrated wireless routers usually perform the functions of the following devices:

- a switch by connecting wired devices
- an access point by connecting wireless devices
- a router/gateway by providing access to the Internet through a modem to the ISP

Currently there are many different broadcast standards for wireless routers:

- 802.11b
- 802.11g
- 802.11n
- 802.11ac

The differences between these standards are speed and signal strength. In addition to the standards, each integrated wireless router may have features that meet your network requirement, such as content filtering, QoS, IPv6 support, and wireless security.

In Part 1, you will search the Internet for three different wireless routers and create a list of the important router feature by recording them in the following table. During your search, you can also record additional features that are important to you in the **Other Features** column in the table.

To explore emulators for some of the Linksys routers, go to http://ui.linksys.com/files/.

**Note**: The Linksys emulators may not provide the most current version of the firmware.

| Brand/Model | Price | IPv6-Enabled | Wireless Security | Band | Other Features |
|---|---|---|---|---|---|
| Linksys/EA4500 | $129.99 USD | Yes | WPA2 | Dual-band N (2.4 GHz and 5 GHz) | Separate Guest Network, 4 Gigabit Ethernet Ports, QoS, remote administration from mobile devices, such as smart phones |
| | | | | | |
| | | | | | |
| | | | | | |

After you have completed the table above, determine which integrated wireless router you would choose for your home. Explain your choice.

_____

_____

_____

Answer will vary. Some of the reasons can include ease of configuration, parental control, and QoS.

## Part 2: Explore Wireless Access Points

Unlike integrated wireless routers, a WAP does not have integrated switch and router functions. A WAP only allows users to access the network wirelessly using mobile devices and provides a connection to the main wired network infrastructure. With the correct user credentials, wireless users can access resources on the network.

In this part, you will explore two Cisco WAPs, WAP321 and AP541N. Cisco's website (http://www.cisco.com) can provide you with technical specifications regarding these WAPs. Furthermore, online emulators are also available at the following links:

To access an online WAP321 emulator, go to https://www.cisco.com/assets/sol/sb/WAP321_Emulators/WAP321_Emulator_v1.0.2.3/main.html.

To access an online AP541N emulator, go to http://www.cisco.com/assets/sol/sb/AP541N_Emulators/AP541N_Emulator_v1.9.2/Getting_Started.htm.

| Model | Security | Band | Other Features / Comments |
|---|---|---|---|
| WAP321 | | | |
| AP541N | | | |

## Reflection

What features on the wireless routers or WAPs are important for your network? Why?

_____

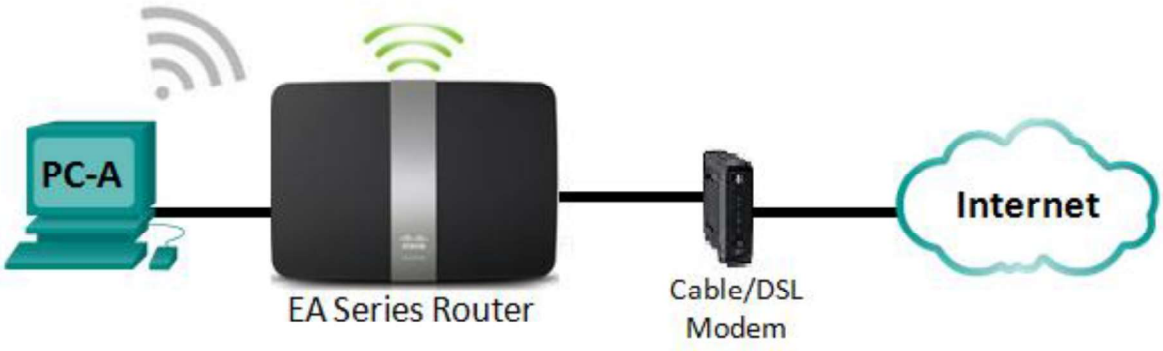
_____

Answer will vary. For example, wireless security is important because unauthorized wireless access to the network can have devastating consequences, such as loss of confidential company information.

# Lab – Configuring a Wireless Router and Client (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Topology




## Linksys Router Settings

| | |
|---|---|
| **Network Name (SSID)** | CCNA-Net |
| **Network Password** | cisconet |
| **Router Password** | cisco123 |

## Objectives

**Part 1: Configure Basic Settings on a Linksys EA Series Router**

**Part 2: Secure the Wireless Network**

**Part 3: Review Additional Features on a Linksys EA Series Router**

**Part 4: Connect a Wireless Client**

## Background / Scenario

Surfing the web from anywhere in the home or office has become common. Without wireless connectivity, users would be limited to connect only where there is a wired connection. Users have embraced the flexibility that wireless routers provide for accessing the network and the Internet.

In this lab, you will configure a Linksys Smart Wi-Fi router, which includes applying WPA2 security settings and activating DHCP services. You will review some added features available on these routers, such as USB storage, parental controls, and time restrictions. You will also configure a wireless PC client.

## Required Resources

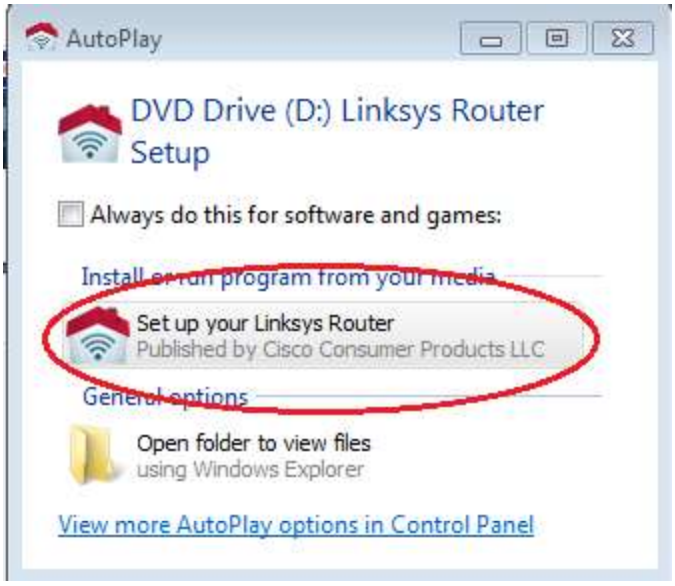
- 1 Linksys EA Series Router (EA4500 with firmware version 2.1.39.145204 or comparable)
- 1 Cable or DSL modem (Optional - needed for Internet service and normally supplied by ISP)
- 1 PC with a Wireless NIC (Windows 7, Vista, or XP)
- Ethernet cables as shown in the topology

# Part 1: Configure Basic Settings on a Linksys EA Series Router

The most efficient way to configure basic settings on an EA Series router is to run the Linksys EA Series Setup CD that came with the router. If the Setup CD is unavailable, download the Setup program from http://Linksys.com/support.

## Step 1: Insert the Linksys EA-Series Setup CD into the PC.

When prompted, select **Set up your Linksys Router**. You will be asked to read and accept the License Terms for using the software. Click **Next >** after accepting the license terms.

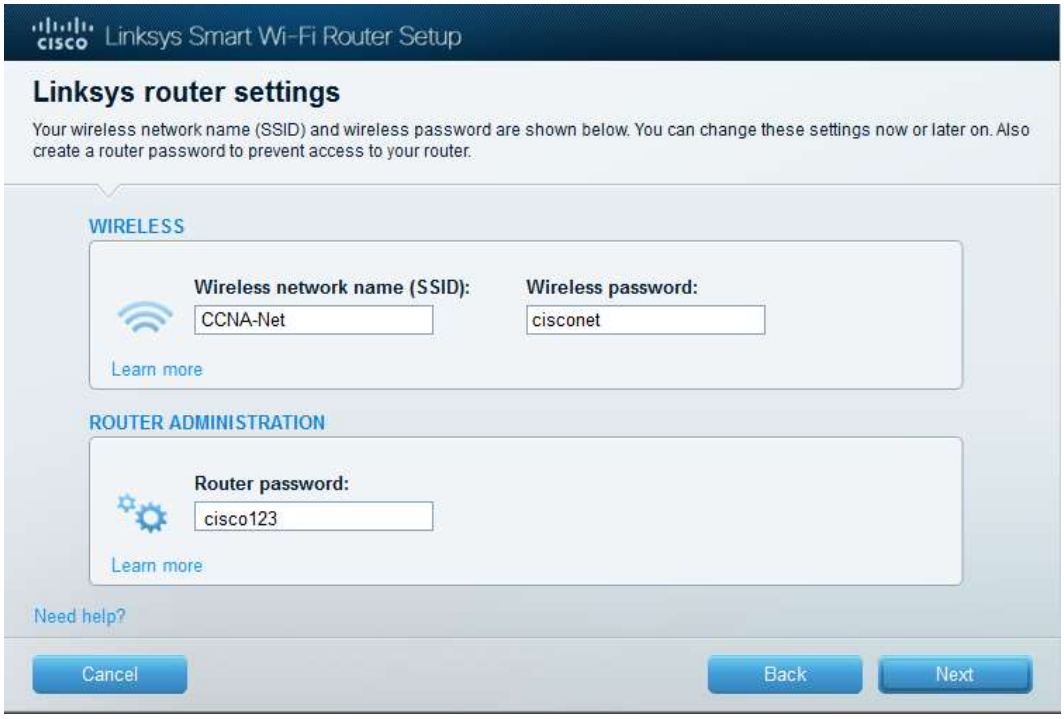



## Step 2: Cable the network as shown in the topology.

Follow the directions in the next window for connecting the power cable and Ethernet cable from your cable modem or DSL modem. You may connect the PC to one of the four unused Ethernet ports on the back of the router. After you have connected everything, click **Next >**.


## Step 3: Configure Linksys router settings.

a. Allow time for the **Linksys router settings** window to display. Use the **Linksys Router Settings** table at the beginning of this lab to fill in the fields in this window. Click **Next** to display the summary router settings screen. Click **Next**.

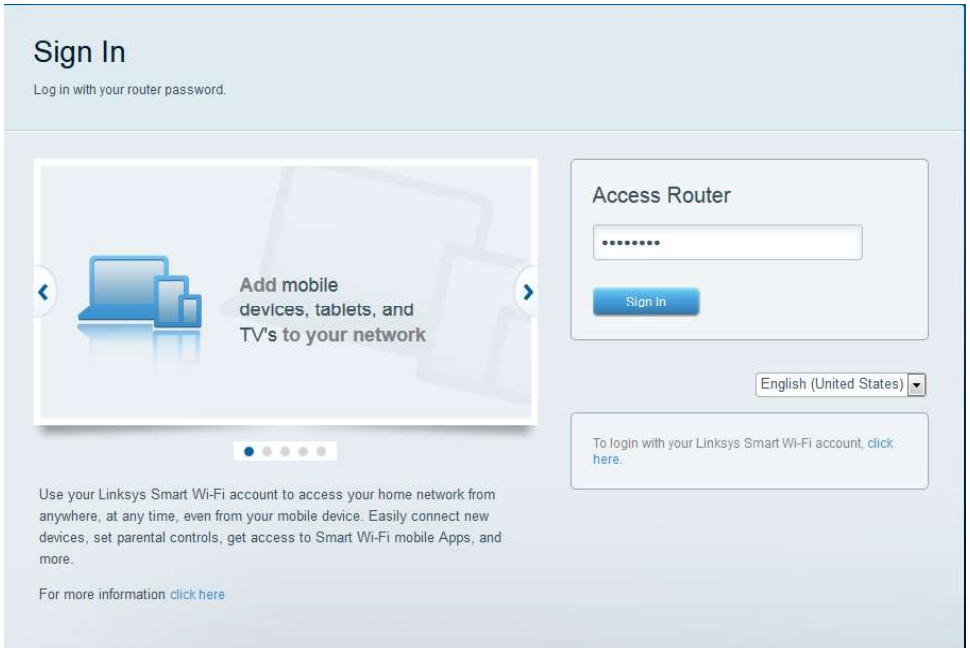



b. The **Create your Linksys Smart Wi-Fi account** window displays. A Linksys Smart Wi-Fi account associates your router to the account, allowing you to remotely manage the router using a browser or

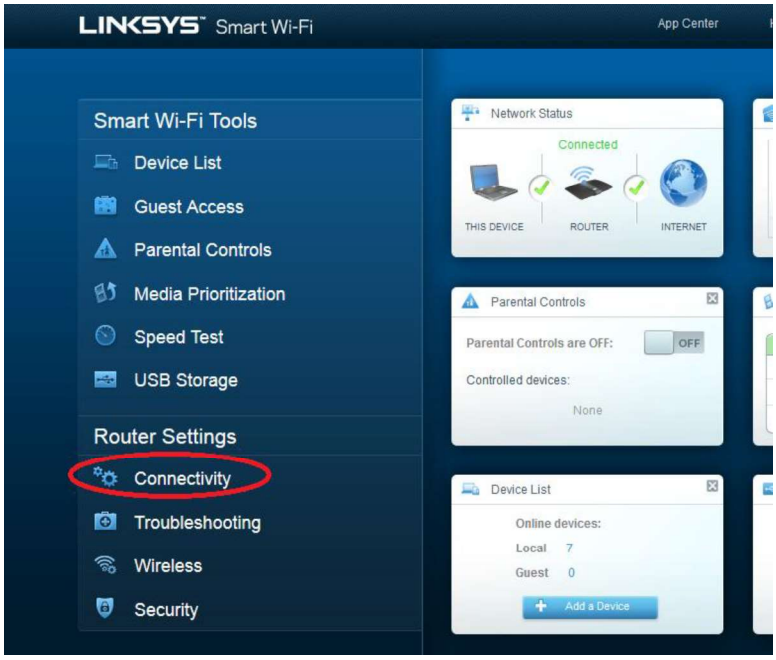
mobile device running the Smart Wi-Fi app. For this lab, bypass the account setup process. Click the **No thanks** box and press **Continue**.

**Note**: An account can be setup by browsing to www.linksyssmartwifi.com.

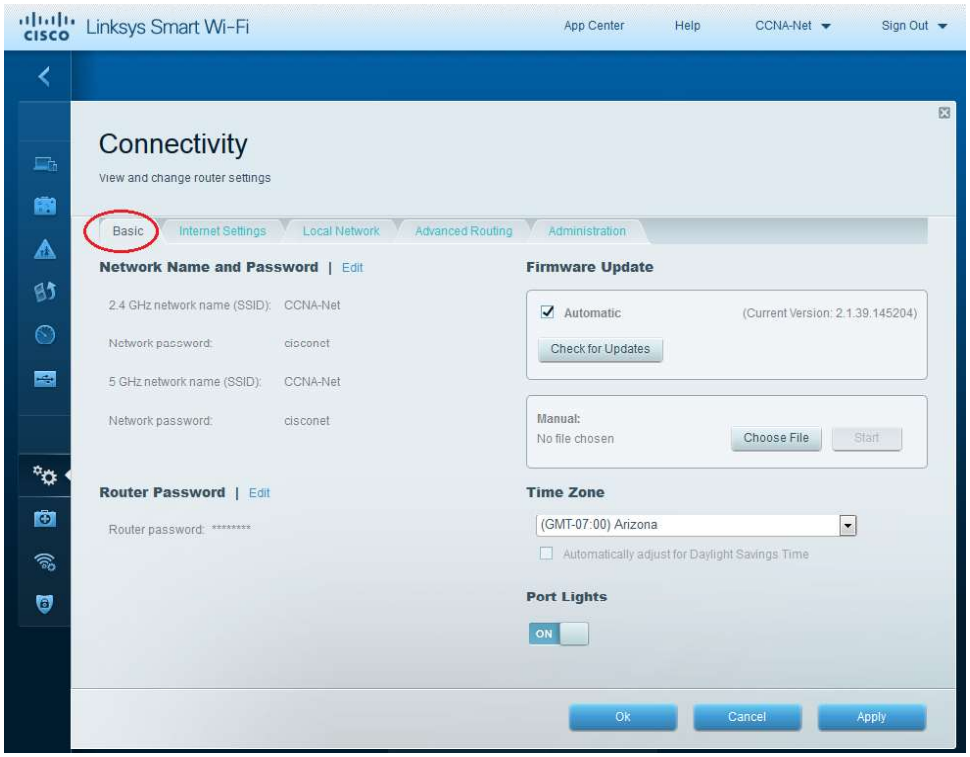

c. A **Sign In** window displays. In the **Access Router** field, enter **cisco123,** and click **Sign In**.



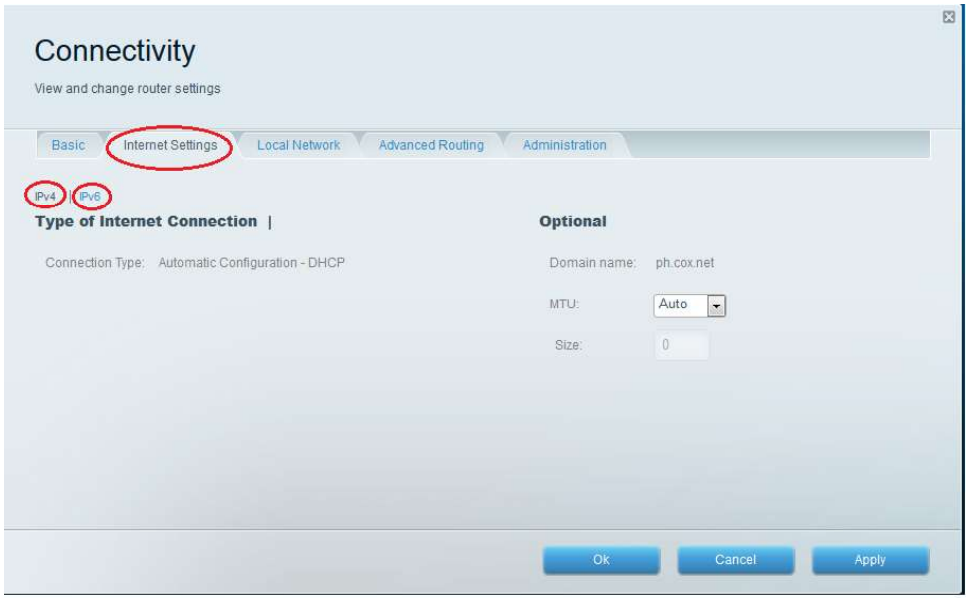

d. On the Linksys Smart Wi-Fi home page, click **Connectivity** to view and change basic router settings.




e. On the **Basic** tab, you can edit the SSID name and password, change the router password, perform firmware updates, and set the time zone for your router. (The router password and SSID information was set in Step 3a.) Select the correct time zone for your router from the drop-down box and click **Apply**.

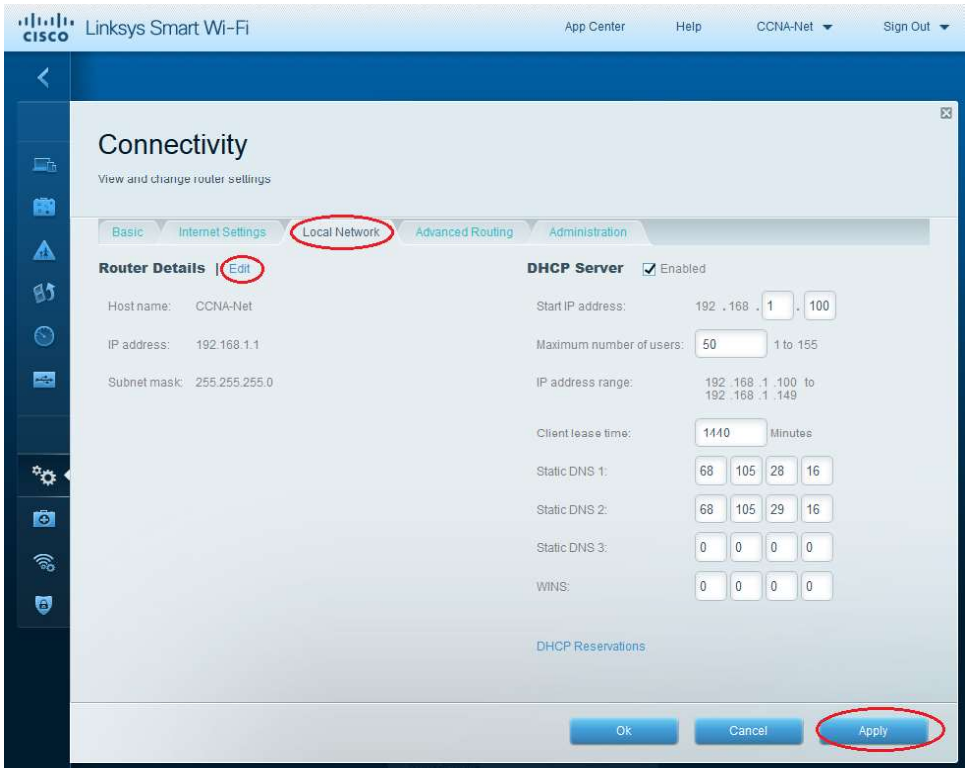



f. The **Internet Settings** tab provides information about the Internet connection. In the example, the router automatically configured the connection for DHCP. Both IPv4 and IPv6 information can be displayed from this screen.

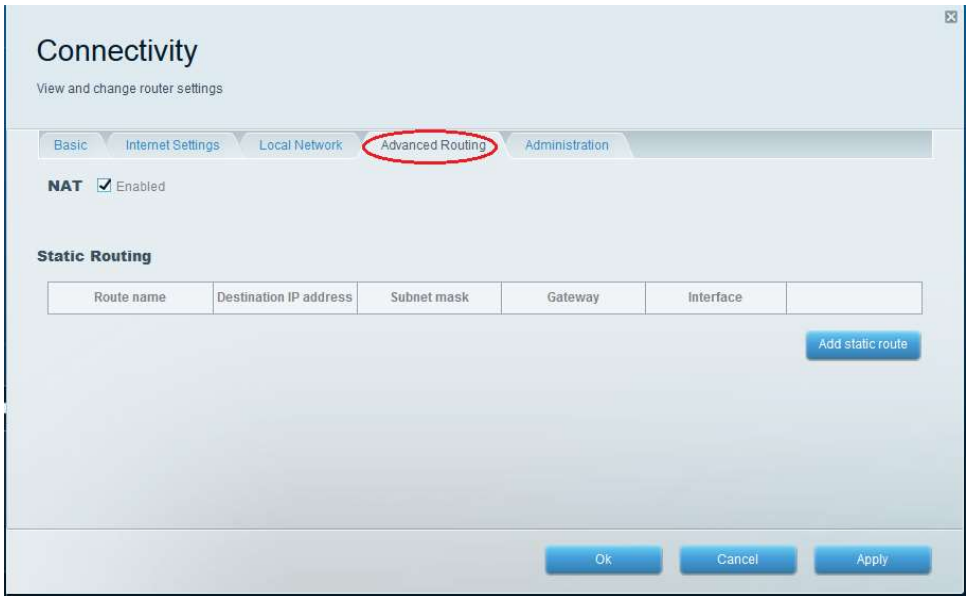



g. The **Local Network** tab controls the local DHCP server settings. The default local network settings specify the 192.168.1.0/24 network and the local IP address of the default router is 192.168.1.1. This can be changed by clicking **Edit** next to **Router Details**. DHCP Server settings can be changed on this screen. You can set the DHCP starting address, maximum number of DHCP users, client lease time, and static DNS servers. Click **Apply** to accept all changes made on this screen.

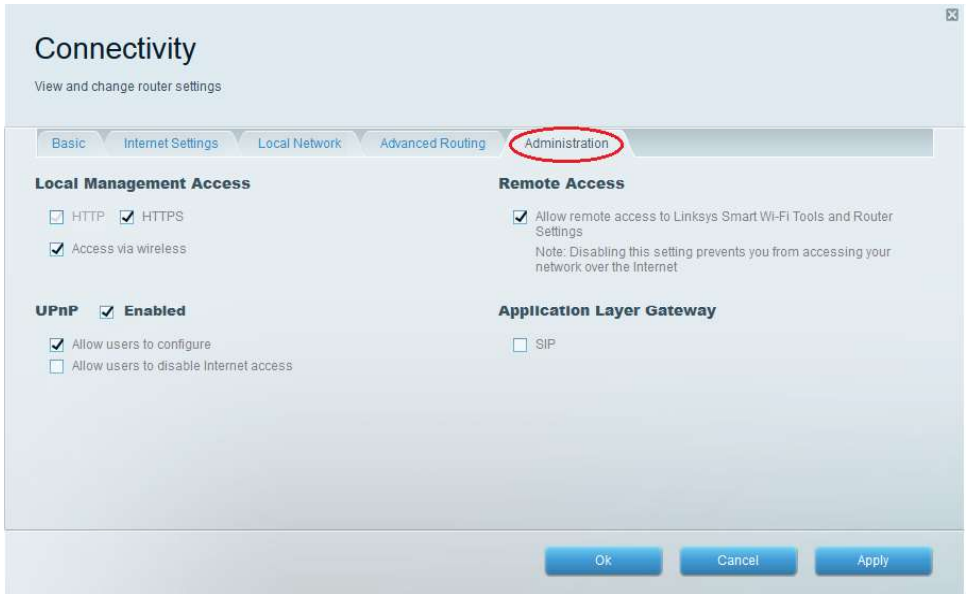
**Note**: If DHCP is used to obtain ISP connection information, these DNS addresses will most likely be populated with the ISP's DNS server information.



h. The **Advanced Routing** tab allows you to disable Network Address translation (NAT), which is enabled by default. This screen also allows you to add static routes. Click **Apply** to accept any desired changes made on this screen.




i. The **Administration** tab provides controls for the management of the Smart Wi-Fi software. By chicking the appropriate box, you can activate remote management access to the router. You can also activate HTTPS access and restrict wireless management. Universal Plug and Play (UPnP) and Application Layer Gateway controls are also available on this screen. Click **Apply** to accept any desired changes made on this screen.



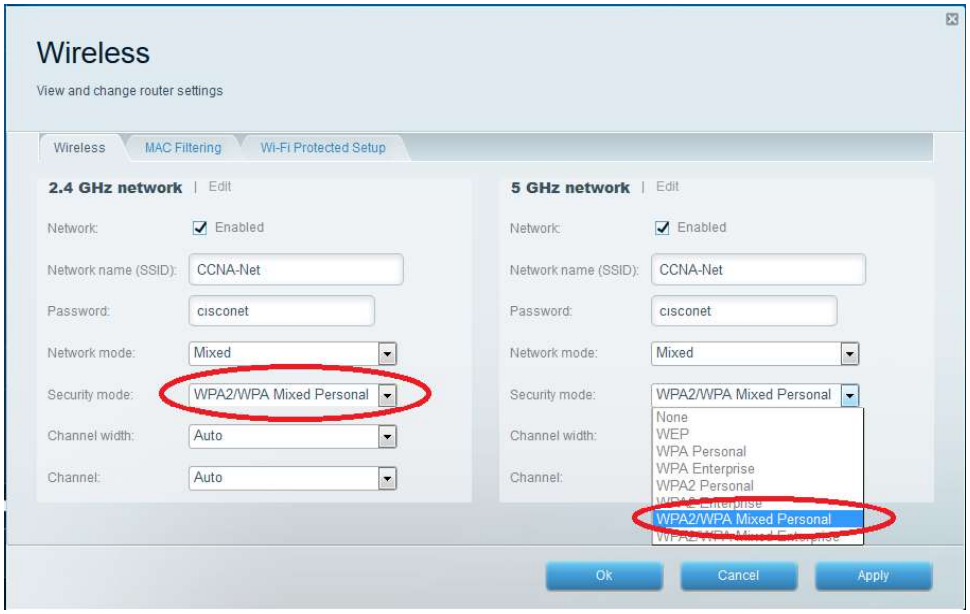

# Part 2: Secure the Wireless Network

In Part 2, you will secure the Linksys EA series router wireless network and review firewall and port forwarding options on a Linksys Smart Wi-Fi router.

## Step 1: Add WPA security on the wireless routers.

a. From the Linksys Smart Wi-Fi home page, click **Wireless**.

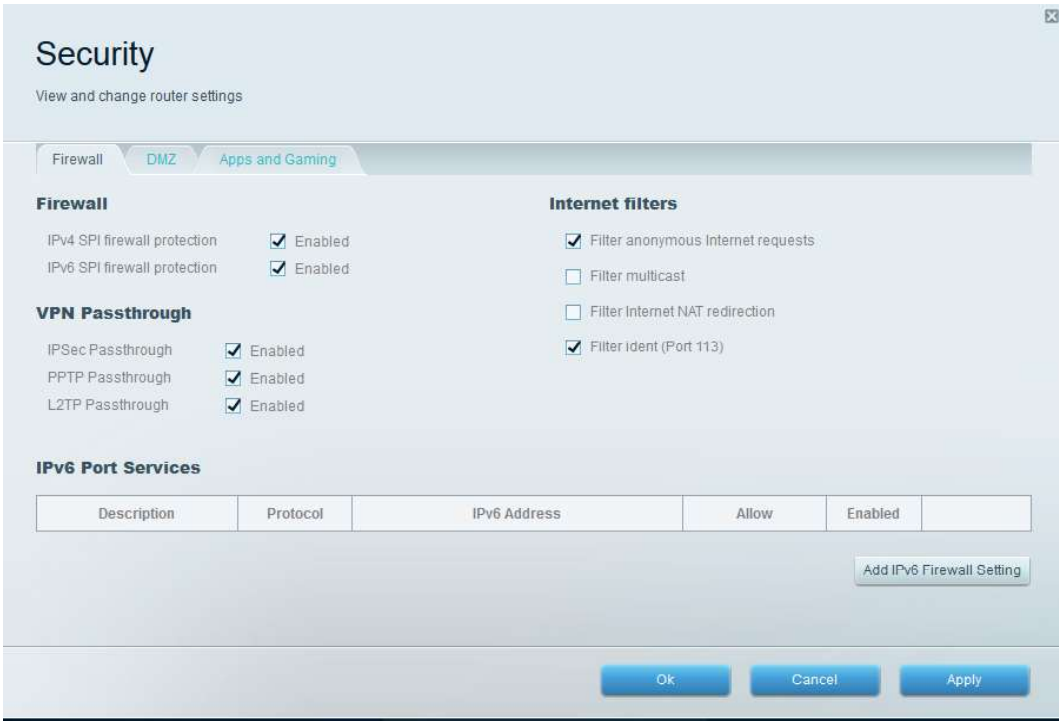

b. The **Wireless** window displays the settings for both the 2.4 and 5 GHz radios. Use the **Edit** button next to each column to modify the security setting on each wireless frequency range. (The SSID and password were previously set in Part 1.) Click the **Security mode** drop-down list to select the **WPA2/WPA Mixed Personal** option for each range. Click **Apply** to save your settings, and then click **OK**.



## Step 2: Apply firewall and port forwarding settings.

a. From the Linksys Smart Wi-Fi home page, click **Security**. In the **Security** windows, the **Firewall**, **DMZ**, and **Apps and Gaming** tabs are available to view and change router security settings.


b. The **Firewall** tab displays firewall settings, where you can enable or disable IPv4 and IPv6 Stateful Packet Inspection (SPI) firewall protection, Virtual Private Network (VPN) Passthrough options, and Internet filters. Click **Apply** to accept any desired changes made on this screen.




c. The **Apps and Gaming** tab provides port forwarding capabilities. In the example, ports 5060 and 5061 have been opened for a VoIP Softphone application running on a local device at IP address 192.168.1.126. Click **Apply** to accept any desired changes made on this screen.

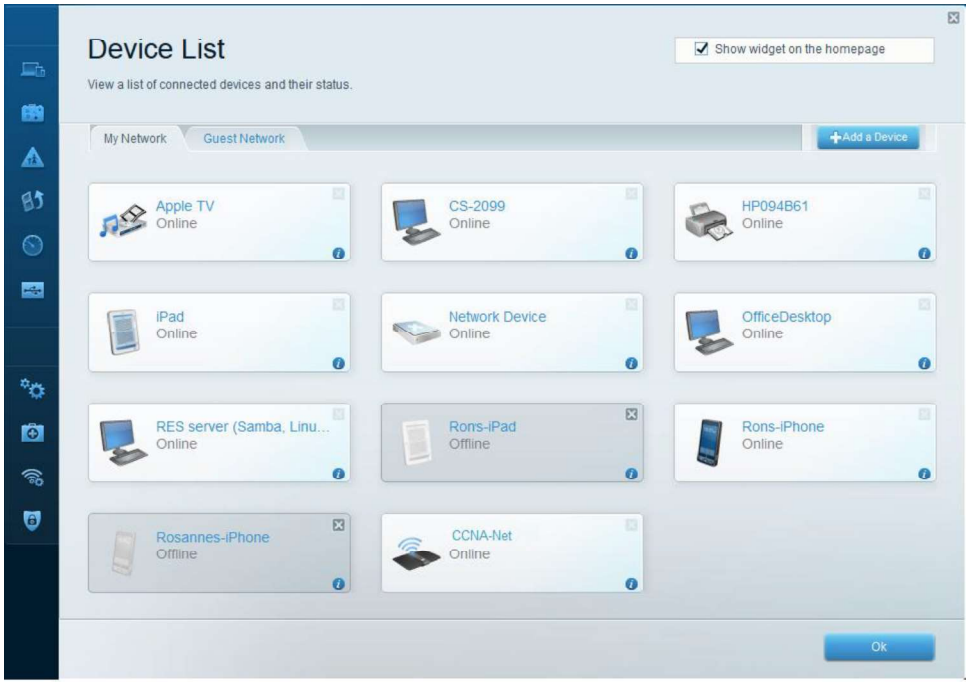

# Part 3: Review Additional Features on a Linksys EA Series Router

In Part 3, you will review some of the additional features available on the Linksys EA series router.

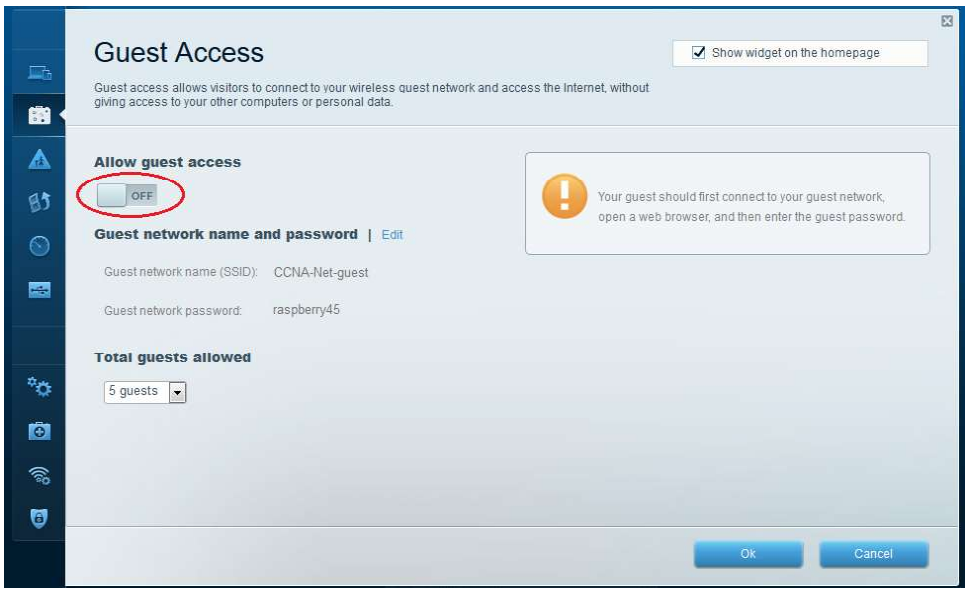
## Step 1: Review Smart Wi-Fi Tools.

a. From the Linksys Smart Wi-Fi home page, click **Device List**.

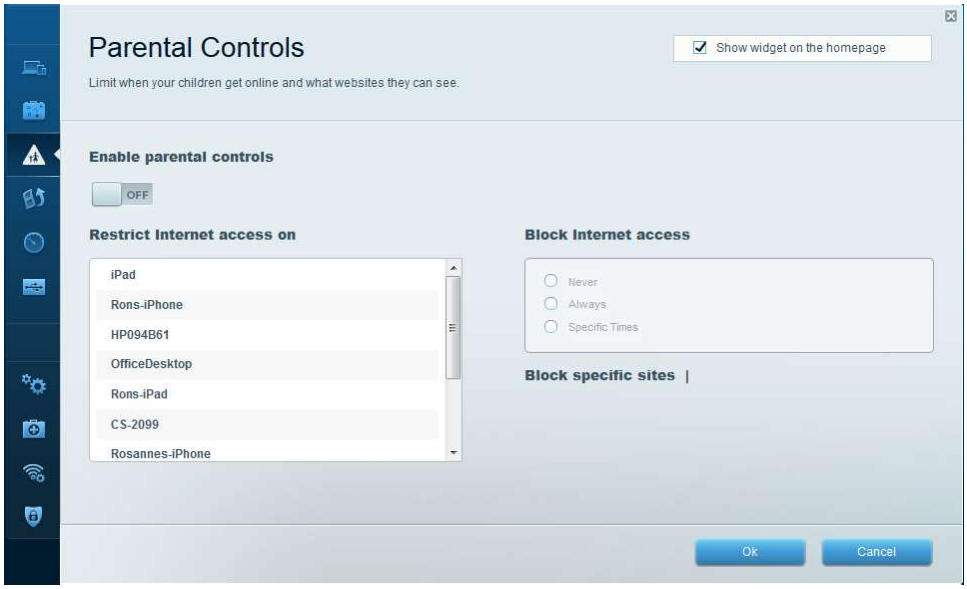

The **Device List** window displays the list of clients on the local network. Notice that there is a tab for the **Guest Network**. If the Guest network was activated, clients on that network would be displayed in the **Guest Network** tab.



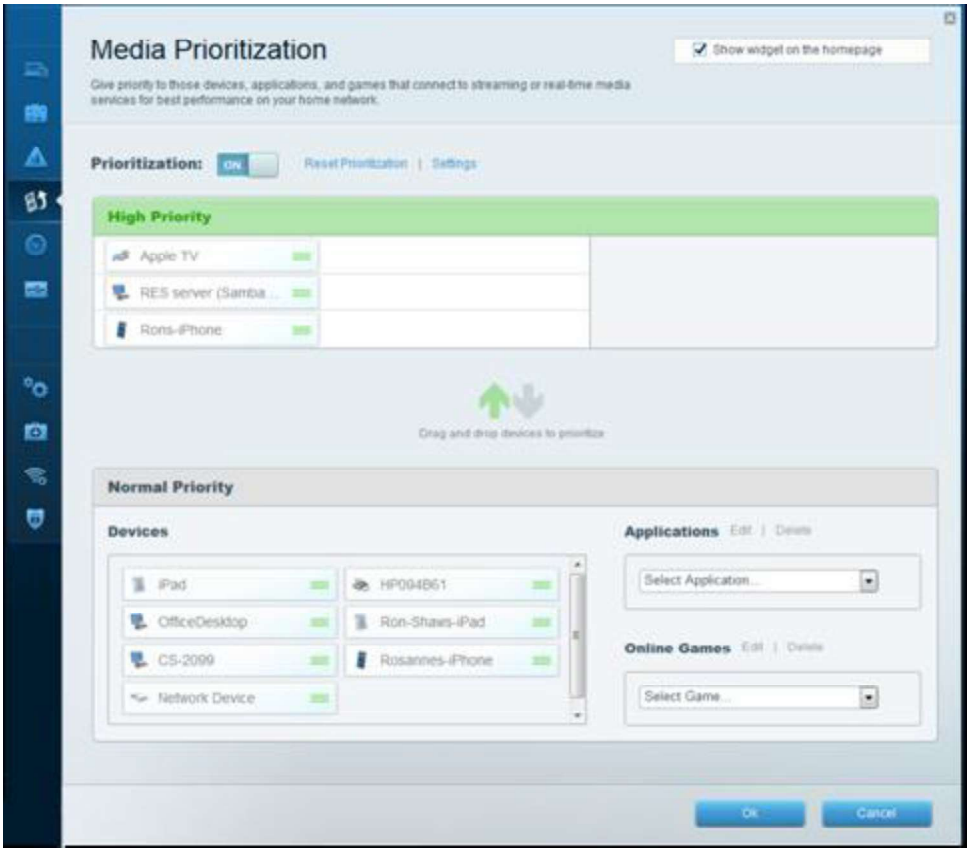

b. From the Linksys Smart Wi-Fi home page, click **Guest Access**. Clients on the guest network only have access to the Internet and are unable to access other clients on the local network. To allow guest access, click on the **Allow guest access** toggle button. Click **Edit** link (next to the Guest network name and password) to change the Guest network password and click **OK** to accept the changes.




c. From the Linksys Smart Wi-Fi home page, click **Parental Controls**. Use these settings to restrict Internet access on selected devices and to restrict time and websites. Click **OK** to save the settings.

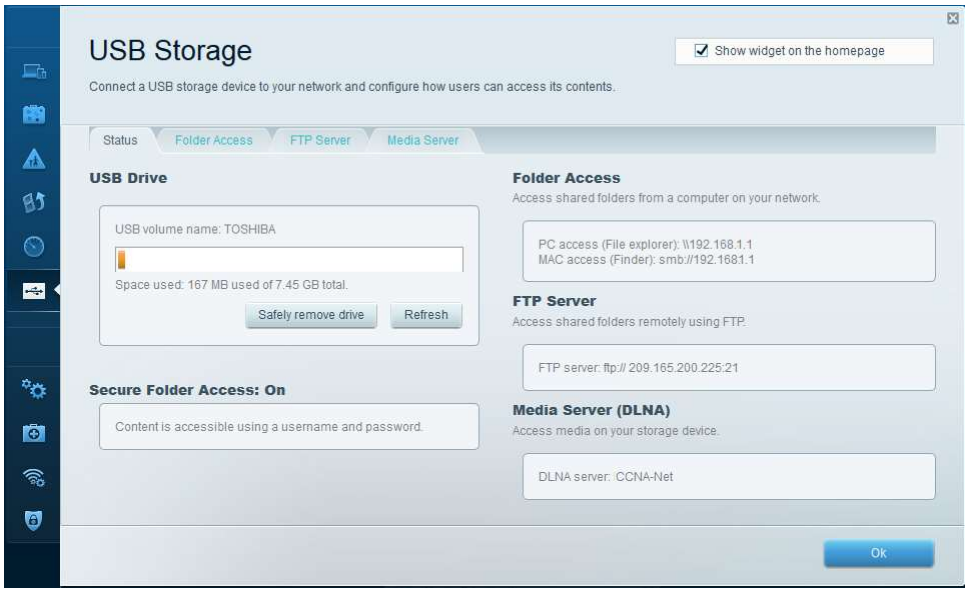



d. From the Linksys Smart Wi-Fi home page, click on **Media Prioritization**. These settings allows you to assign network bandwidth prioritization to selected devices on the local network. In the example, the device labeled Apple TV has been given the highest priority for network resources. To make prioritization changes, just drag and drop the listed devices, and click **OK** to save your settings.



e. From the Linksys Smart Wi-Fi home page, click **Speed Test**. Use this utility to test your Internet access speeds. The example shows the results of the speed test. The router stores the results of each speed tests and allows you to display that history.

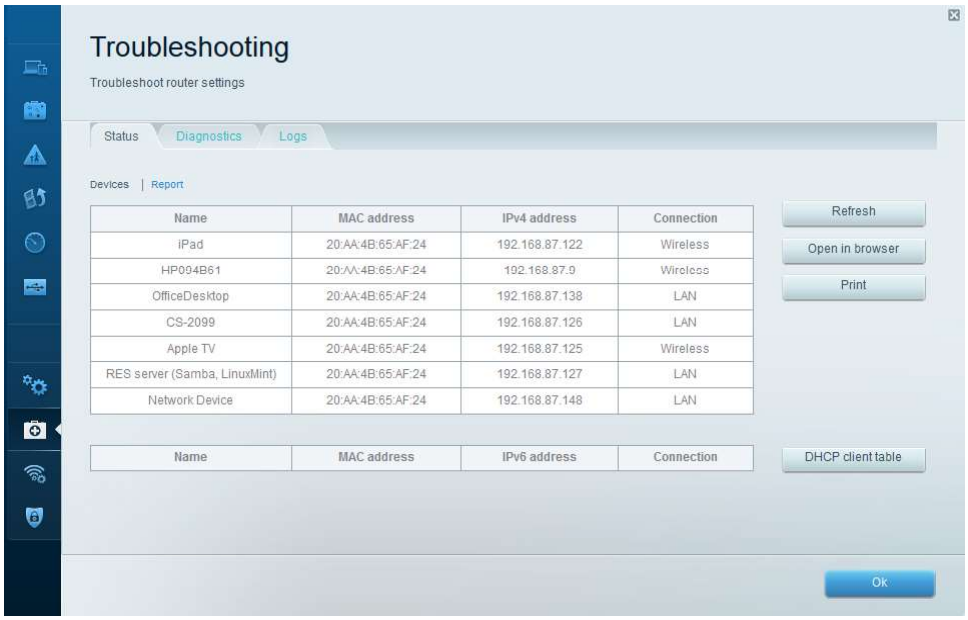

f. From the Linksys Smart Wi-Fi home page, click **USB Storage**. Use this screen to review your USB drive settings. From here, you can click on the appropriate tab to set up FTP and Media Servers. You can also set up individual user accounts for access to these servers by clicking the tabs at the top of this screen. A USB storage device is plugged into the back of the router to use this option. Click **OK** to save any desired changes.



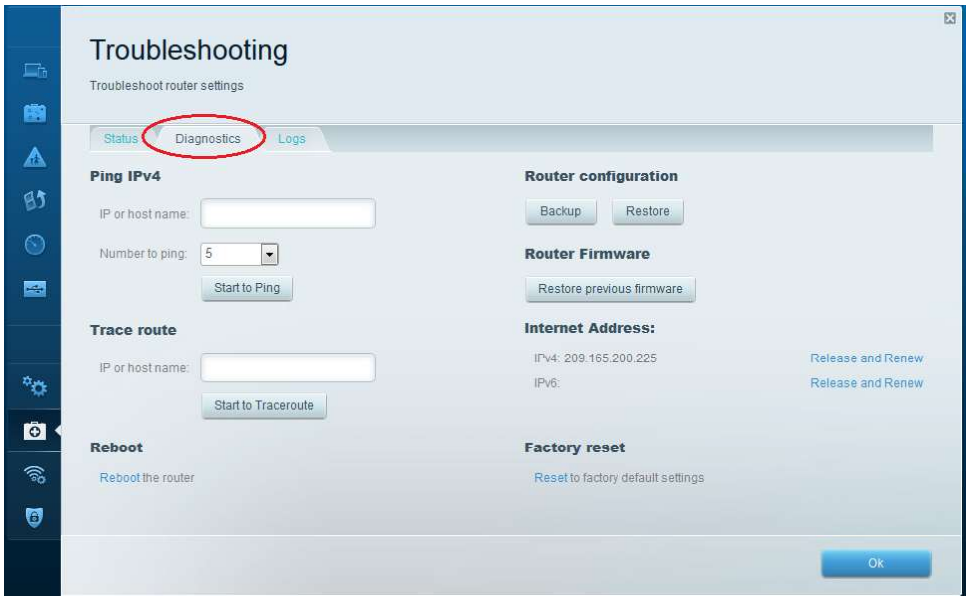

## Step 2: Troubleshoot the router.

From the Linksys Smart Wi-Fi home page, click **Troubleshooting**.

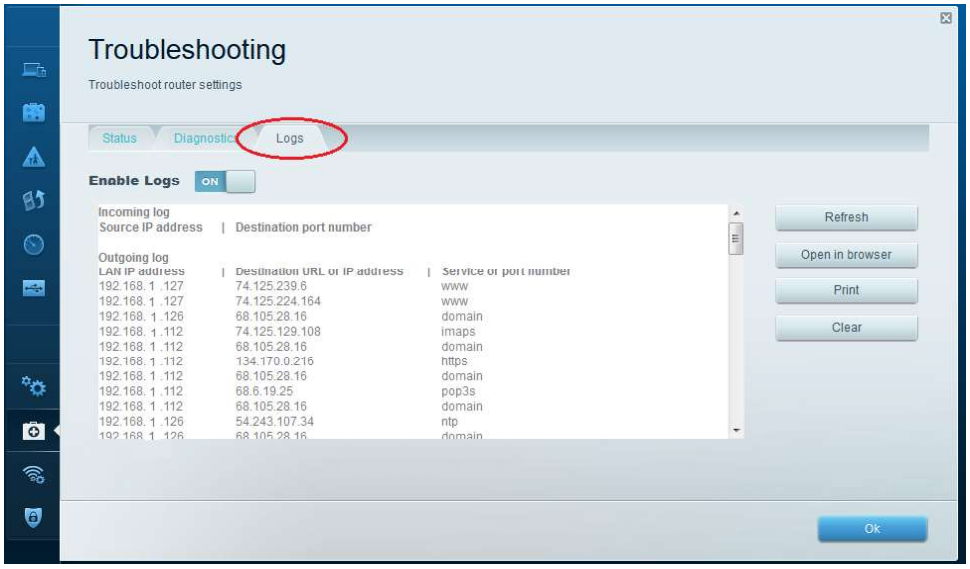
a. The **Status** tab provides a list of clients on the local network along with their NIC MAC and IP addresses. It also displays how they are connected to the network. Click **OK** to save any desired changes.




b. The **Diagnostics** tab provides the ping and traceroute utilities. It also allows you to reboot the router, backup and restore the router configuration, restore a previous firmware version, release and renew the Internet addresses on your router, and reset to factory default settings. Click **OK** to save any desired changes.




c. The **Logs** tab provides Incoming and Outgoing, Security, and DHCP logs. You can print and clear these logs from this screen. Click **OK** to save any desired changes.




# Part 4: Connect a Wireless Client

In Part 4, you will configure the PC's wireless NIC to connect to the Linksys EA Series Router.

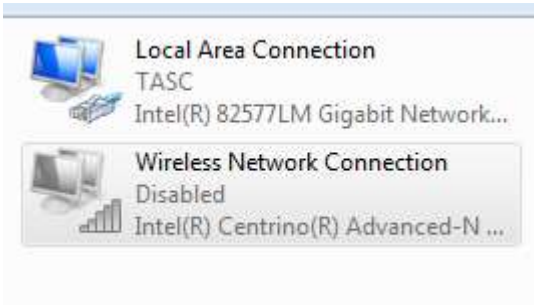
**Note**: This lab was performed using a PC running the Windows 7 operating system. You should be able to perform the lab with other Windows operating systems listed; however, menu selections and screens may vary.

## Step 1: Use the Network and Sharing Center.

a. Open the **Network and Sharing Center** by clicking the Windows **Start** button > **Control Panel** > **View network status and tasks** under Network and Internet heading in the Category View.

b. In the left pane, click the **Change adapter settings** link.

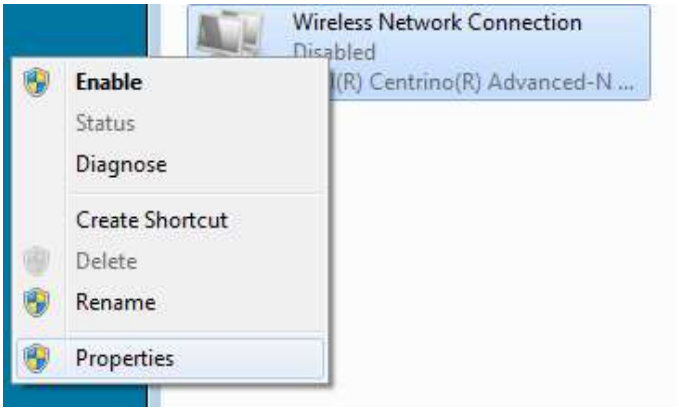
The **Network Connections** window provides the list of NICs available on this PC. Look for your **Local Area Connection** and **Wireless Network Connection** adapters in this window.




**Note**: VPN adapters and other types of network connections may also be displayed in this window.

## Step 2: Work with your wireless NIC.

a. Select and right-click the **Wireless Network Connection** option to display a drop-down list. If your wireless NIC is disabled, you must **Enable** it.




b. Right-click the **Wireless Network Connection**, and then click **Connect/Disconnect**. This displays a list of SSIDs in range of your wireless NIC. Select **CCNA-Net**, then click the **Connect**.


c. When prompted, enter **cisconet** to supply the network security key, and then click **OK**.


d. The wireless icon should display in your taskbar when you have a wireless connection. Click this icon to display the list of SSIDs in range of your PC.

e. The SSID **CCNA-Net** should now show that you are connected to the CCNA-Net wireless network.


## Reflection

Why would you not want to use WEP security for your wireless network?

_____

WEP uses RC4 encryption, which can be easily hacked. WPA2 use Advanced Encryption Standard (AES), which is considered the strongest encryption protocol.

# Inside and Outside Control (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

## Objective

Explain how wireless LAN components are deployed in a small- to medium-sized business.

Instructor Notes: This activity can be completed individually, in small groups, or as a class.

## Scenario

An assessment has been completed to validate the need for an upgrade to your small- to medium-sized wireless network. Approved for purchase are indoor and outdoor access points and one wireless controller. You must compare equipment models and their specifications before you purchase.

Therefore, you visit the Wireless Compare Products and Services web site and see a features chart for indoor and outdoor wireless access points and controller devices. After reviewing the chart, you note there is some terminology with which you are unfamiliar:

- Federal Information Processing Standard (FIPS)
- MIMO
- Cisco CleanAir Technology
- Cisco FlexConnect
- Band Select

Research the above terms. Prepare your own chart with your company's most important requirements listed for purchasing the indoor and outdoor wireless access points and wireless controller. This chart will assist in validating your purchase order to your accounting manager and CEO.

## Resources

Internet access to the World Wide Web

# Part 1: Secure Background Knowledge of Wireless Terminology

### Step 1: Define unfamiliar wireless terms.

a. FIPS

b. MIMO

c. Cisco CleanAir Technology

d. Cisco FlexConnect

e. Band Select

### Step 2: Visit the Wireless Compare Products and Services web site.

a. Compare the devices in each category based on their feature sets.

b. Choose one model from each category: indoor, outdoor, and controller categories for the upgrades for your business.

### Step 3: Create a chart for each device chosen in Step 2b to include:

a. The main type of selected device (indoor access point, outdoor access point, or controller).

b. A graphic of each selected device.

c. Five of the most beneficial features that the selected models would provide your business.

**Step 4: After research is complete, explain, and justify your choices with another student, class group, or entire class.**

## Suggested Activity Completion Examples

# Part 1:

**Wireless device features definitions**

| | |
|---|---|
| **FIPS** | FIPS is the Federal Information Processing Standard regarding security for wireless devices. |
| **MIMO** | Unlike SISO (Single Input, Single Output), MIMO technology uses multiple radio bands and paths to transfer network data through multiple signals. Multiple antennas are used to send multiple spatial streams at the same time allowing for higher data transmission speeds and data delivery payloads. |
| **Cisco CleanAir Technology** | CleanAir Technology allows Cisco devices to:<br>• provide continual, system-wide wireless network discovery without wireless performance impact<br>• identify source, location and interference of wireless signals<br>take automatic steps to avoid current and future wireless interference while recording what steps were taken to do so |
| **Cisco FlexConnect** | FlexConnect (previously known as Hybrid Remote Edge Access Point or H-REAP) is a wireless solution which enables network administrators to configure and control access points located at remote locations. This is performed by using a local wireless controller through a WAN connection. |
| **Band Select** | Band Select is a Cisco-selected frequency range technology based upon the ISM (industrial, scientific, and medical) unlicensed usage. These include:<br>• 900 MHz<br>• 2.4 GHz (802.11b, g, and n standards) – better range but lower data rates<br>• 5 GHz (802.11a, n, and ac standards) – less range but higher data rates |

# Part 2:

## Cisco 2600 Series Indoor Access Point

| | |
|---|---|
| **Wi-Fi Standards** | 802.11 a, b, g, n<br>(supports Dual paths/radio rates of 2.4 and 5 GHz)<br>Data rate capabilities of 450 Mbps |
| **FIPS** | In process |
| **CleanAir Technology** | Yes |
| **FlexConnect** | Yes |
| **Antennas** | Internal and external |

## Cisco 1552I Series Outdoor Access Point


| | |
|---|---|
| **Wi-Fi Standards** | 802.11 a, b, g, n<br>(supports Dual paths/radio rates of 2.4 and 5 GHz)<br>Data rate capabilities of 300 Mbps downstream with 10/100/1000 Mbps upstream |

| | |
|---|---|
| **FIPS** | In process |
| **CleanAir Technology** | Yes |
| **FlexConnect** | Yes |
| **Antennas** | Internal |

**Cisco Wireless Controller Module for ISR G2**

| | |
|---|---|
| **Data Throughput** | 500 Mbps |
| **Wireless Guest Services** | Yes (up to 500 clients supported by 50 APs)<br>16 WLANs supported with 16 maximum VLANs allowed |
| **CleanAir Technology** | Yes |
| **FlexConnect** | Yes |
| **Access Control Lists (ACLs for security)** | Yes |

## Identify elements of the model that map to IT-related content:

- Wireless terminology
- Inside and outside wireless access points
- Wireless controllers
- Wireless device capabilities