Wireless Networking

Chapter 23

Overview

- **In this chapter, you will learn how to**
  - Discuss wireless networking components
  - Analyze and explain wireless networking standards
  - Install and configure wireless networks
  - Troubleshoot wireless networks

Wireless Technology Options

- **Users who want to go wireless have many options today:**
  - 802.11 (Wi-Fi) and Bluetooth use radio waves to connect devices.
  - Infrared devices connect using light waves.
  - Cellular telephone companies offer Internet connectivity through cell phone networks.

Wireless Networking Components

- **Wireless capabilities are built into many devices today.**
  - Smartphones and tablets usually come with built-in wireless.

Figure 1: Infrared transceiver ports on a laptop and PDA

Wireless Networking Components (*continued*)

- **Wireless Ethernet and Bluetooth are often integrated or can be added easily.**
  - USB, PCI, PCI Express, or PC Card adapters

Figure 2: Wireless PCI add-on card

Figure 3: External USB wireless NIC

Wireless Networking Components *(continued)*

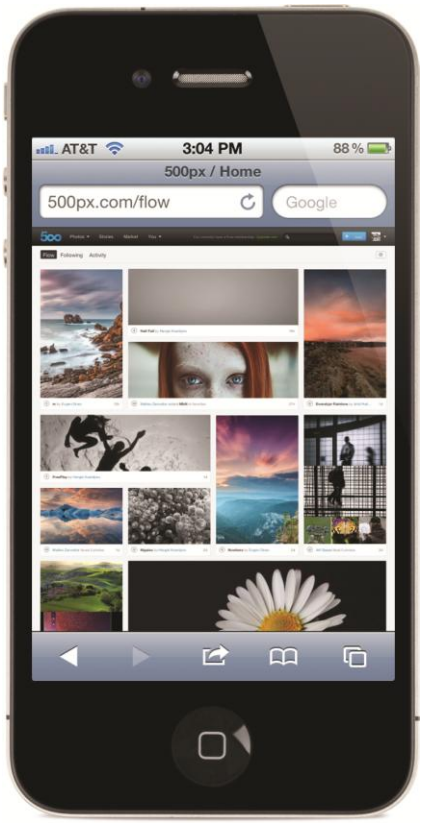

Figure 4: Smartphone with wireless capability

Wireless Networking Components *(continued)*

- **Wireless access point (WAP)**
  - Wireless Ethernet devices can connect to a WAP
  - Acts like a hub to the wireless hosts in the area
- **Bluetooth hub**
  - Built-in option on many newer PCs

Wireless Networking Components *(continued)*

Figure 5: Linksys device that acts as wireless access point, switch, and router

Figure 6: External USB Bluetooth adapter, keyboard, and mouse

Wireless Networking Components *(continued)*

- **Most WAPs draw their power from a wall outlet, like any other electronic device.**
- **More advanced WAPs, especially those used in corporate settings, can also use a feature called Power over Ethernet (PoE). Using PoE, you only need to plug a single Ethernet cable into the WAP to provide both power and a network connection.**

Wireless Networking Software

- **Wireless devices use the same networking clients and protocols as wired networks.**
  - Use CSMA/CA (CA stands for collision avoidance)
    - Another option is to use Request to Send/Clear to Send (RTS/CTS). The sending node issues an RTS to the receiving node as a request, and the receiving node replies with a CTS when it's clear. Once the data is received, the receiving node sends an ACK (acknowledgment).
    - RTS/CTS avoids collisions, but it adds significant overhead to the process and can impede performance.

Wireless Configuration Utility

- **Configure wireless networking software**
  - Use a utility to configure parameters
    - Windows built-in utility or vendor provided
    - Set parameters like network name

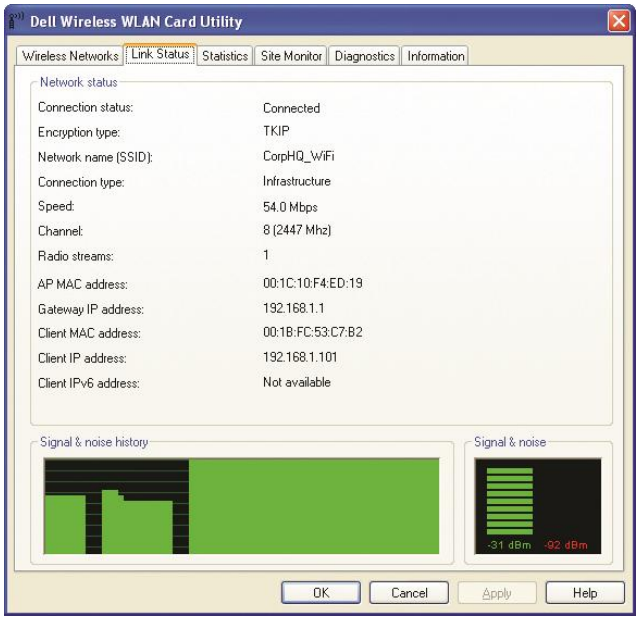

Figure 7: Wireless configuration utility

Wireless Networking Modes

- **Ad-hoc mode**
  - Each wireless node is in direct contact with every other node in a decentralized free-for-all.
  - Form an Independent Basic Service Set (IBSS)
  - Called peer-to-peer mode
  - Good for a few computers or a temporary network such as study groups or business meetings

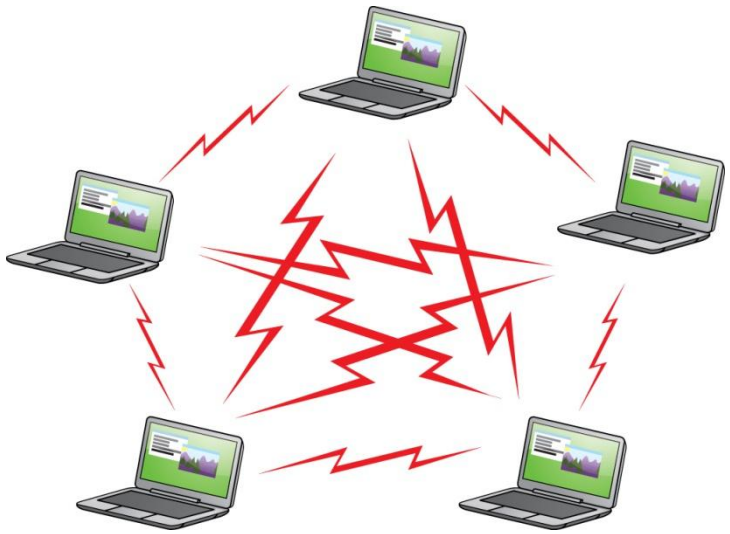

Figure 8: Wireless ad hoc mode network

Wireless Networking Modes (*continued*)

- **Infrastructure Mode**
  - Use one or more WAPs to connect wireless nodes to a wired network segment.
  - A single WAP servicing an area is called a Basic Service Set (BSS).
  - Additional WAPs create an Extended Basic Service Set (EBSS).

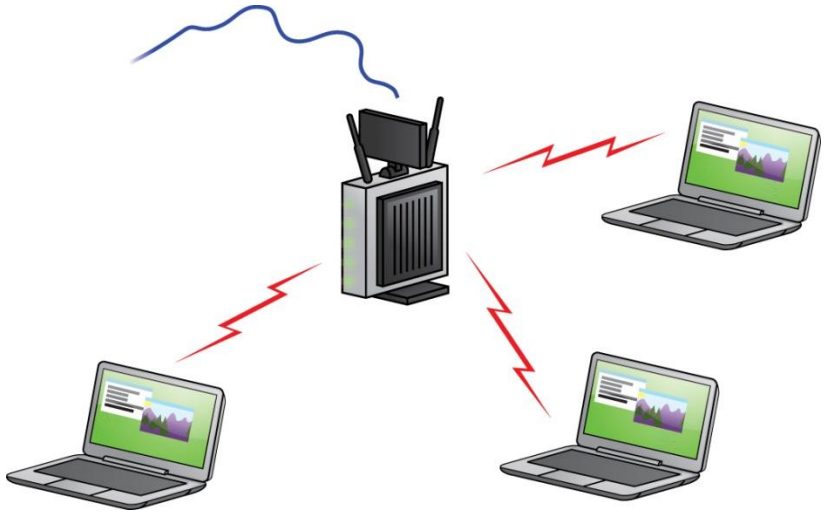

Figure 9: Wireless infrastructure mode network

Wireless Networking Security

- **Four methods used to enhance security:**
  - Change the default password on the WAP.
  - Configure Service Set Identifier (SSID).
    - That's the name of the wireless network (like a workgroup or domain name).
  - Filter by MAC address.
  - Use encryption.

- **Let's look at all four methods.**

Wireless Networking Security (*continued*)

- **The default password is common knowledge for every WAP manufacturer.**
  - Change this as soon as you start the setup.
- **Service Set Identifier (SSID)**
  - Configure a unique SSID or network name.
  - The default is often the name of the vendor, such as Linksys.
  - The name is widely known, so it's easy to guess.
  - Each node needs to have the same SSID.
  - Turning off SSID broadcasting makes it harder for people to determine your SSID name.

Wireless Networking Security (*continued*)

- **MAC filtering**
  - Filtering based on each host's unique MAC address
  - Creates a type of accepted user
  - Some WAPs enable you to blacklist specific MAC addresses too
- **WAPs use an access control list (ACL) for authentication**
  - MAC address filtering is a great example of this
  - This ACL has *nothing* to do with NTFS

Wireless Networking Security (*continued*)

- **Wired Equivalency Privacy (WEP)**
  - Encrypts data using 40-bit or 104-bit encryption
  - Provides authentication based on MAC addresses
  - Significant flaws
- **Wi-Fi Protected Access (WPA)**
  - Interim security upgrade to WEP
  - Uses encryption key integrity-checking through Extensible Authentication Protocol (EAP)
  - Uses RC4 encryption
  - WPA uses the Temporal Key Integrity Protocol (TKIP), which provides a new encryption key for every sent packet. This protects WPA from many of the attacks that make WEP vulnerable, though TKIP has flaws of its own.

Wireless Networking Security (*continued*)

- **WPA2 (IEEE 802.11i)**
  - Full security upgrade from WEP and WPA
  - Significant improvements
  - Uses AES encryption

Wireless Networking Security (*continued*)

- **Wi-Fi Protected Setup (WPS): standard created to make it easier for end users to configure secure connections.**
  - WPS works in one of two ways:
  - Some devices use a push button. First, you press the button on the WPS-compatible device for a short moment (usually two seconds). You then have a set time (usually two minutes) to press the button on the WAP. This should automatically configure a secure connection.

Wireless Networking Security (*continued*)

Figure 10: WPS button on an e2500 Router

Wireless Networking Security (*continued*)

- **Wi-Fi Protected Setup (continued):**
  - Some devices enable you to use an eight-digit numeric code printed on the device. To access the WAP, just enter the code in Windows as you would a WPA/WPA2 password.
  - WPS has a security flaw. A hacker can use a program to repeatedly guess the eight-digit code. Because of how the code is set up, it's very easy to guess. As long you have WPS enabled on your WAP, you are vulnerable. The only way to stop this hack is to shut down WPS. Check the WAP manufacturer's Web site for instructions on turning off WPS.

Wireless Networking Security (*continued*)

- **Access Point Placement and Radio Power—protect your network by hiding it from outsiders altogether.**
  - When using an omni-directional antenna, keep it near the center of your home or office
  - The closer you place it to a wall, the further away someone outside your home or office can be and still detect your wireless network.
  - Your wireless access point might also enable you to adjust the radio power levels of your antenna. Decrease the radio power until you can get reception at the furthest point inside your home or office, but not outside.

Speed and Range Issues

- **Wireless speeds range from 2 Mbps to 100+ Mbps.**
- **Speed is affected by range.**
  - Speed is dynamically negotiated.
  - Maximum throughput occurs within about 25 feet.
  - At edge of range, throughput may fall to 1 Mbps.
  - Range is not exact.
  - Range is often listed as around 150 feet or 300 feet.
  - Dead spots and interfering devices can affect signal.

Speed and Range Issues *(continued)*

- **You can increase range in a couple of ways:**
  - You can install multiple WAPs to permit "roaming" between one WAP's coverage area and another's—an EBSS.
  - You can install a replacement that increases a single WAP's signal strength, thus increasing its range.
  - There are also signal boosters are available that can give you even more power.

Wireless Networking Standards

- **802.11-based wireless networking**
  - Most common and fastest of the options for wireless networking
- **Uses different frequencies within a certain frequency range—the industrial, scientific, and medical (ISM) radio bands are 2.4 GHz and 5.8 GHz.**

Wireless Networking Standards

Standard	802.11a	802.11b	802.11g	802.11n
Max. throughput	54 Mbps	11 Mbps	54 Mbps	100+ Mbps
Max. range	150 feet	300 feet	300 feet	300+ feet
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 and 5 GHz
Security	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA	SSID, MAC filtering, industry-standard WEP, WPA
Compatibility	802.11a	802.11b	802.11b, 802.11g	802.11b, 802.11g, 802.11n, (802.11a in some cases)
Communication mode	Ad hoc or infrastructure	Ad hoc or infrastructure	Ad hoc or infrastructure	Ad hoc or infrastructure
Description	Eight available channels. Less prone to interference than 802.11b and 802.11g.	Fourteen channels available in the 2.4-GHz band (only eleven of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.	Improved security enhancements. Fourteen channels available in the 2.4-GHz band (only eleven of which can be used in the U.S. due to FCC regulations). Three non-overlapping channels.	Same as 802.11g but adds the 5-GHz band that 802.11a uses. 802.11n can also make use of multiple antennas (MIMO) to increase its range and speed.

Table 1 compares the important differences among the versions of 802.11.

Wireless Networking Standards (*continued*)

- **802.11a offers short range but high speed and low interference with other devices.**
  - ~150' range
  - 54 Mbps throughput
  - Runs at the 5-GHz frequency
  - Not compatible with any other Wi-Fi standards
- **802.11b was the first, so it has the slowest connection.**
  - ~300' range
  - 11 Mbps throughput
  - Runs at the 2.4-GHz frequency

Wireless Networking Standards (*continued*)

- **802.11g matches 802.11a's speed and provides backward compatibility for 802.11b devices.**
  - ~300' range
  - 54 Mbps throughput
  - Runs at the 2.4-GHz frequency
- **802.11n is the current standard.**
  - 300+' range
  - 100+ Mbps throughput
  - Runs at either 2.4 or 5 GHz
  - Backward-compatible with 802.11b/g devices
    - Some WAPs support 802.11a devices too

Wireless Networking Standards (*continued*)

- **Infrared wireless networking**
  - Simple way to share data without adding any additional hardware or software
  - Uses the Infrared Data Association (IrDA) protocol
  - Line-of-sight required
  - No authentication or encryption
    - You can't be more than 1 meter away

Standard	Infrared (IrDA)
Max. throughput	Up to 4 Mbps
Max. range	1 meter (39 inches)
Security	None
Compatibility	IrDA
Communication mode	Point-to-point ad hoc

Table 2: Infrared Specs

Wireless Networking Standards (*continued*)

- **Bluetooth**
  - Designed to create small wireless networks—personal area networks (PANs)—for specific jobs
    - Connecting peripherals such as keyboards, mice, and headsets to the PC
    - Decent range between devices and Bluetooth hub

Class 1	**100 mW**	**100 meters**
Class 2	**2.5 mW**	**10 meters**
Class 3	**1 mW**	**1 meter**

Wireless Networking Standards (*continued*)

- **Cellular**
  - Enables you to connect to the Internet through a network-aware smartphone, tablet, or other mobile device
  - Several different cellular standards available (covered in chapter 24)
  - Providers usually control cellular network settings – not users or administrators

Comparing Speeds

- **Wi-Fi (802.11b/a/g/n)**
  - 11, 54, or 100+ Mbps
- **IrDA**
  - ~ 56 Kbps (though some standards offer faster speeds)
- **Bluetooth**
  - 1–3 Mbps
- **GPRS**
  - 56–114 Kbps
- **Other cellular**
  - 400–700 Kbps (though some standards offer faster speeds)

Lab—What do you have?

- **Examine the laptop or workstation and answer these questions:**
  - What kind of wireless networking capabilities does the computer have (if any)?
  - What specific technology or technologies does it employ?
  - What kind of wireless networking capabilities could you add to the computer?

Installing and Configuring Wireless Networking

Configuring Wireless Networks

- **Physically installing a wireless NIC is the same as installing a wired NIC.**
  - Snap in the card and install the drivers.
- **Wireless network configuration utility**
  - Used to configure additional parameters
  - Windows XP and later OSs have this capability built in
  - Configure SSID and encryption
  - Configure communication mode
    - Ad-hoc
    - Infrastructure

Configuring Wireless Networks (continued)

- **Wi-Fi**
  - Ad hoc
    - Each wireless node needs to be configured with the same network name (SSID)
    - May need to select a common channel
    - Configure unique host IP addresses
    - Configure File and Printer Sharing

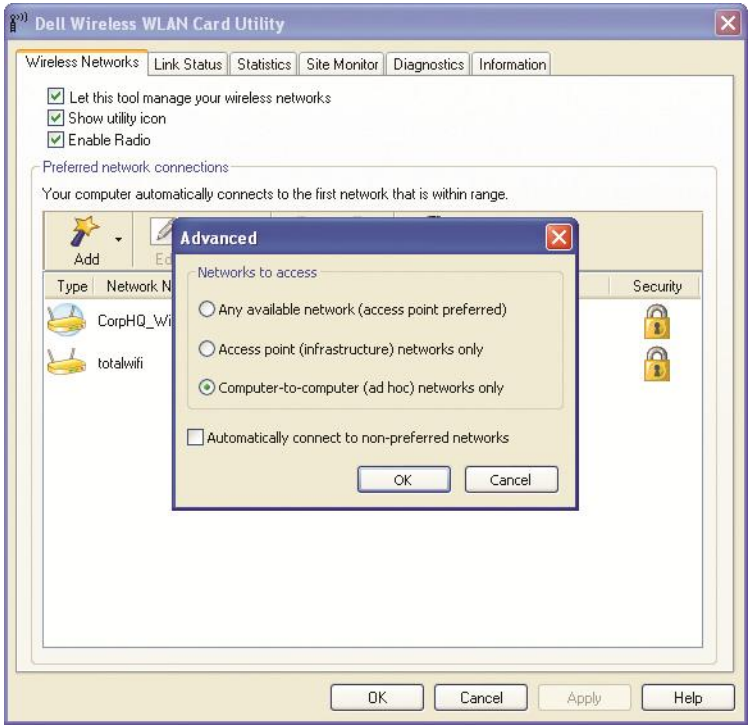

Figure 11: Selecting ad hoc mode in wireless configuration utility

Configuring Wireless Networks (*continued*)

- **Wi-Fi**
  - Infrastructure mode
    - Requires a wireless access point (WAP)
    - All nodes need to be configured with the same SSID
    - Configure the WAP with clients that match the chosen options

Figure 12: Selecting infrastructure mode in a wireless configuration utility

Configuring Wireless Networks (*continued*)

- **Configuring a wireless access point is often done through a Web browser.**
  - Enter the WAP's default IP address (see your documentation or try 192.168.1.1) in your browser.
  - Enter the default administrative password (in your documentation) to log in.
    - The next few slides show some screenshots of the configuration pages.

Configuring Wireless Networks (*continued*)

Figure 13: Security login for Linksys WAP

Configuring Wireless Networks (*continued*)

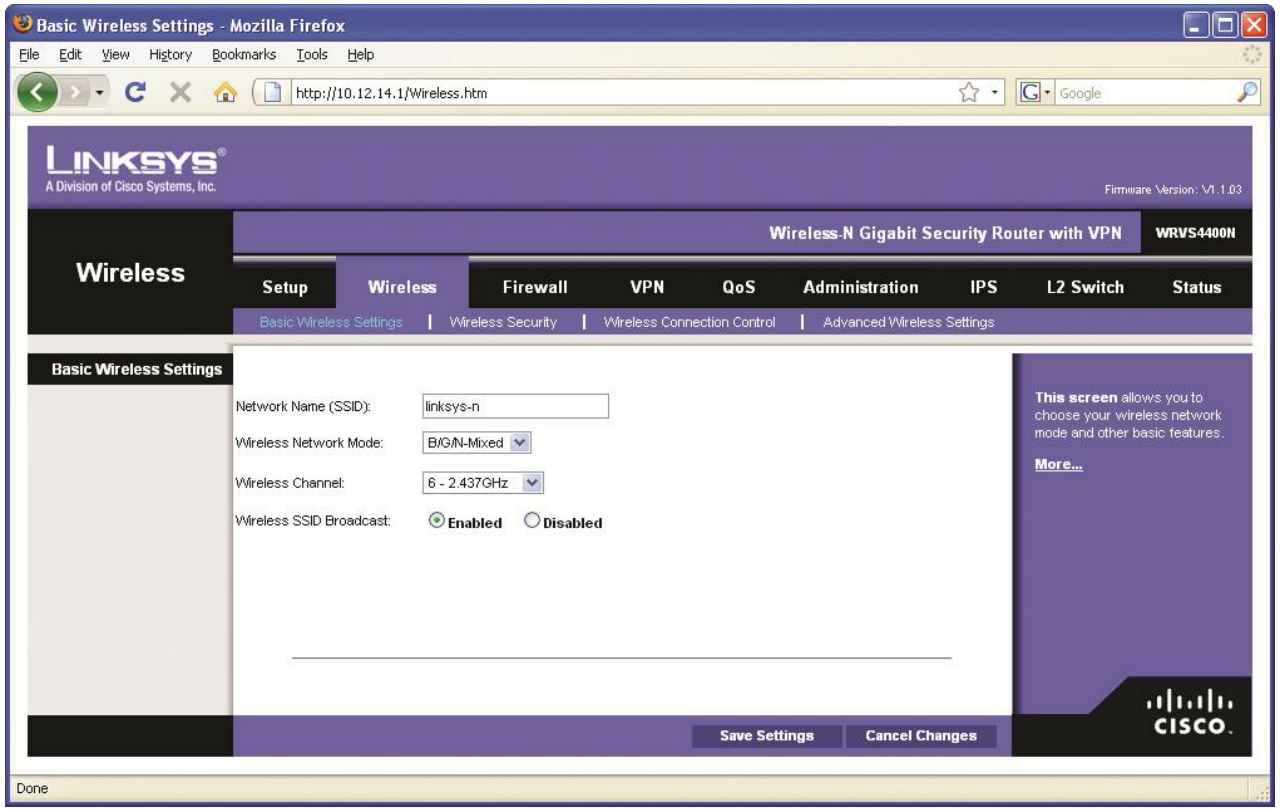

Figure 14: Linksys WAP setup screen

Configuring Wireless Networks (*continued*)

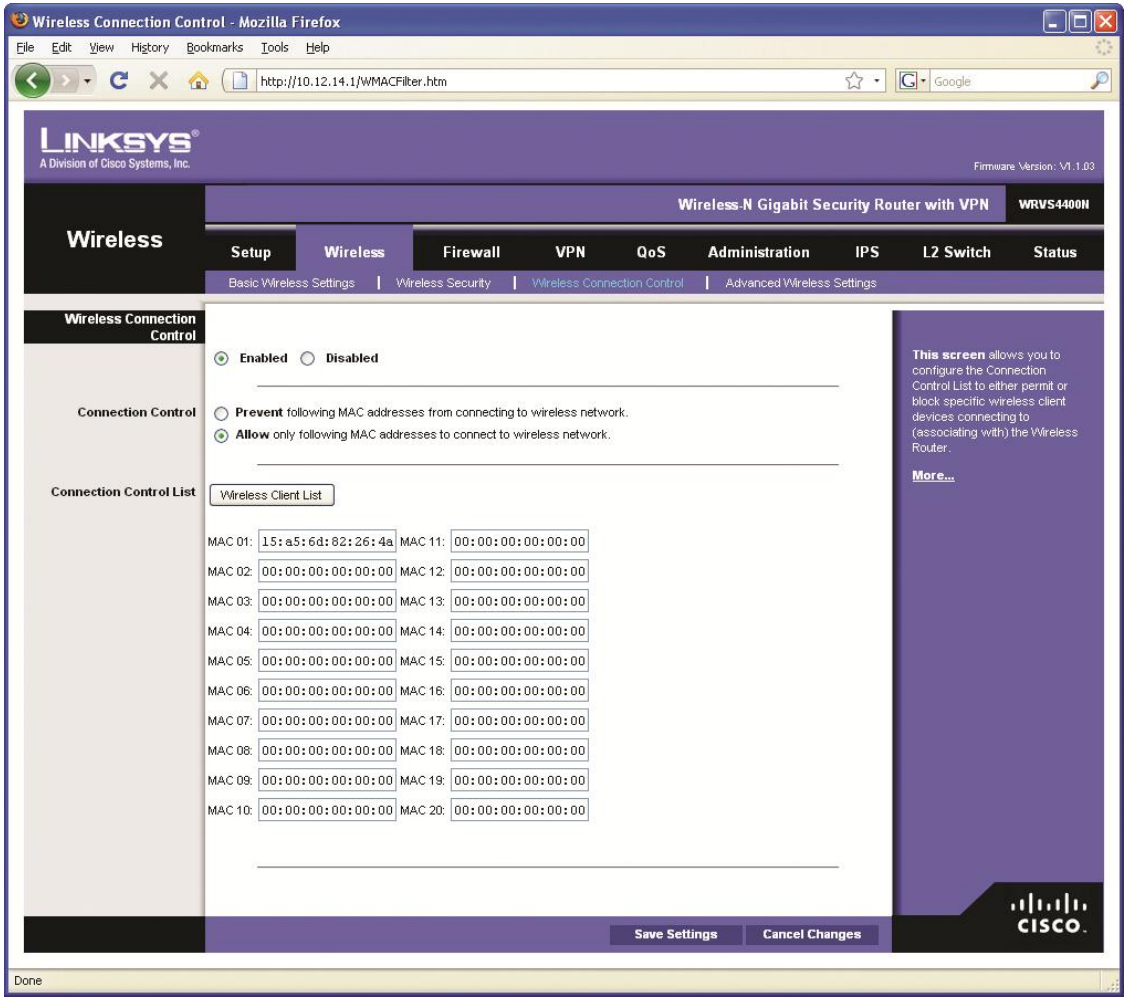

Figure 15: MAC filtering configuration screen for a Linksys WAP

Configuring Wireless Networks (*continued*)

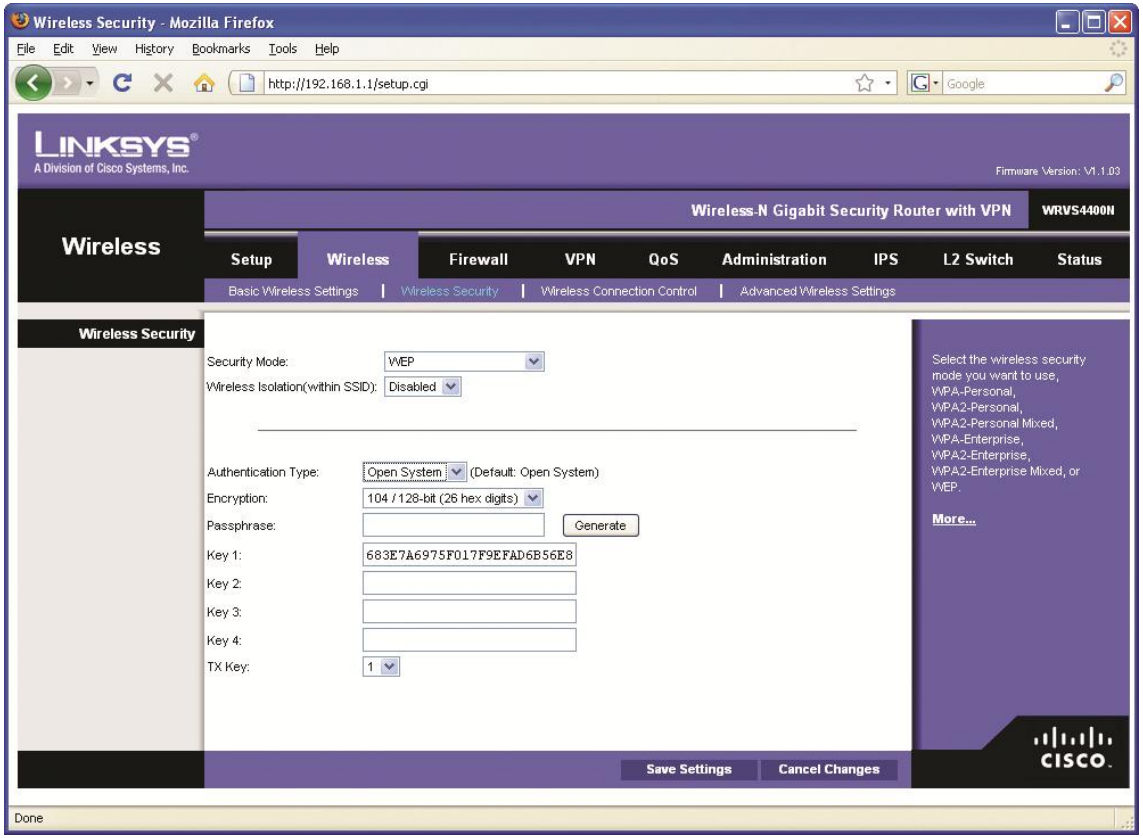

Figure 16: WEP encryption key configuration screen for a Linksys WAP

Configuring Wireless Networks (*continued*)

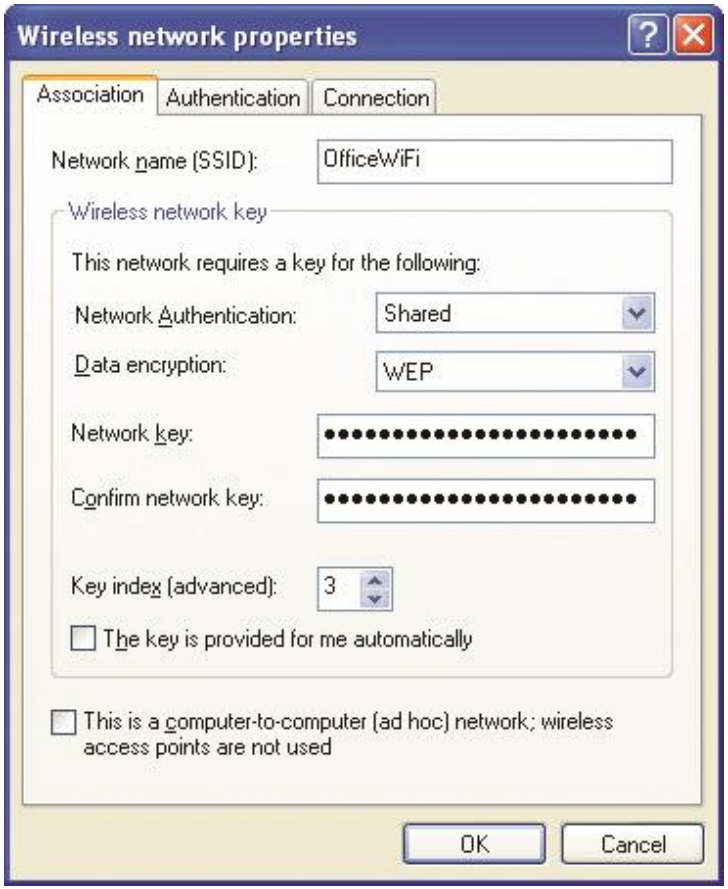

Figure 17: WEP encryption screen on client wireless network adapter configuration utility

Configuring Wireless Networks (*continued*)

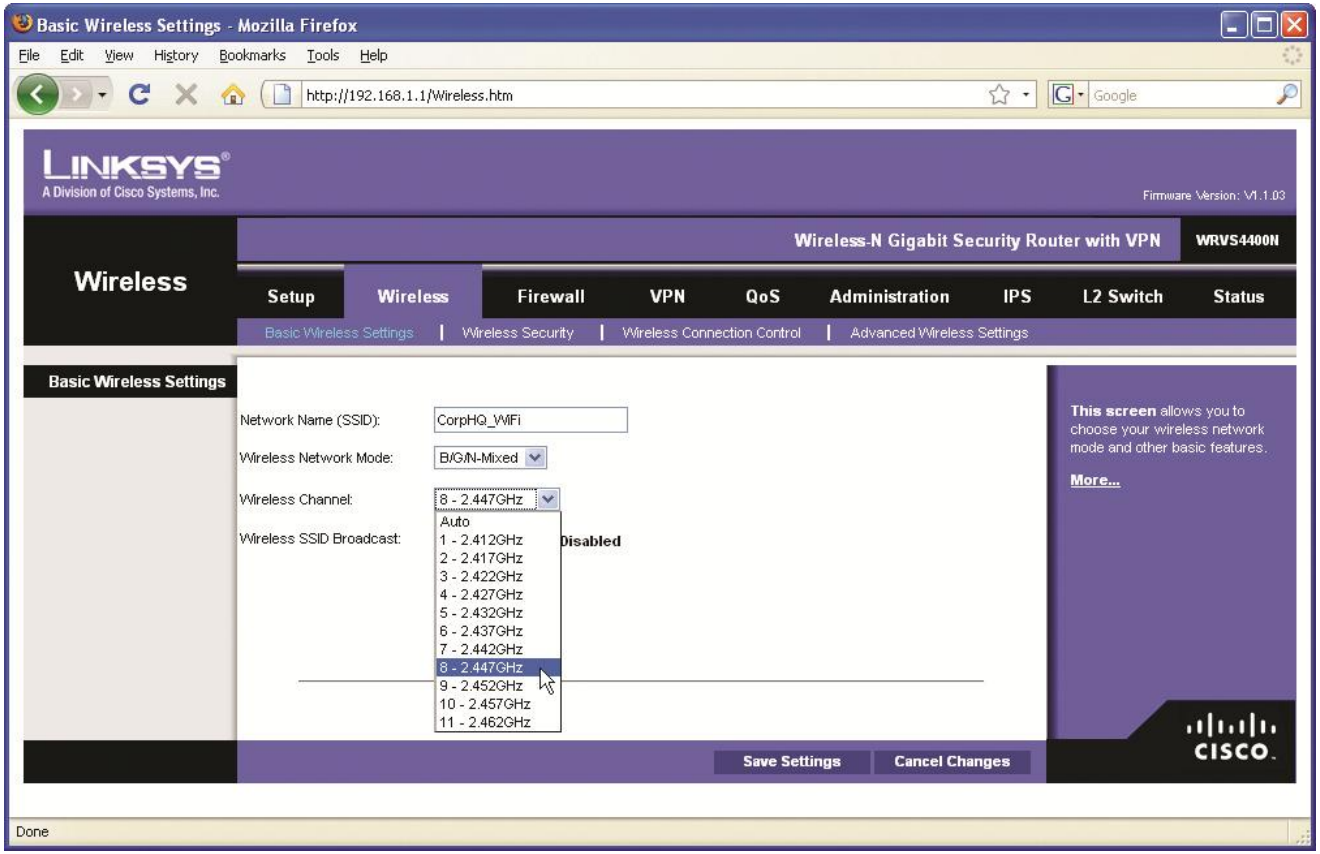

Figure 19: Changing the channel

Configuring Wireless Networks (*continued*)

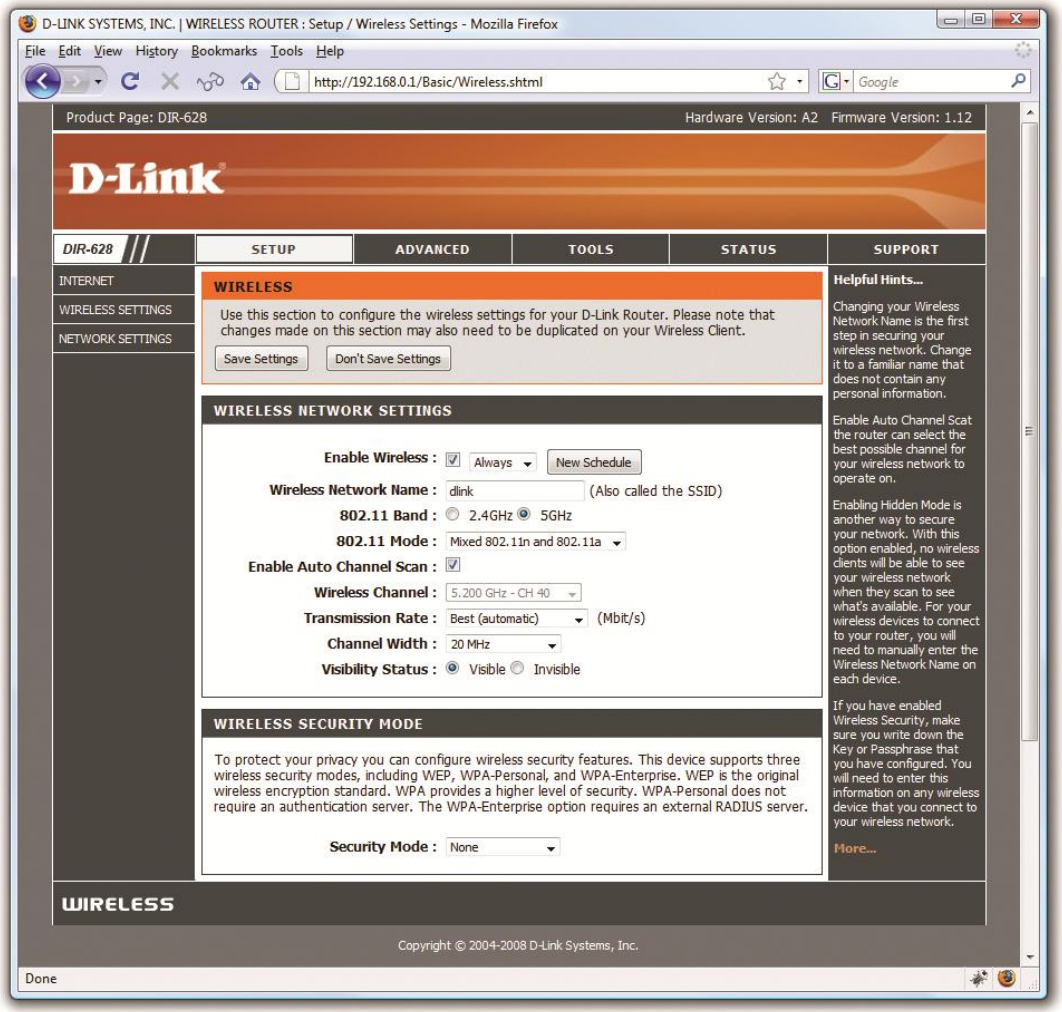

Figure 20: Selecting frequency

Lab—Configuring a WAP

1. **Connect the classroom WAP to the wired classroom network.**
2. **Access the WAP with a credential supplied by the instructor.**
3. **Seek these areas in the WAP configuration:**
   - Where do you change the SSID?
   - How can you set the encryption level?
   - What security options does the WAP offer?
   - How do you set MAC filtering?

WAP Placement

- **A typical network should have a centralized WAP**

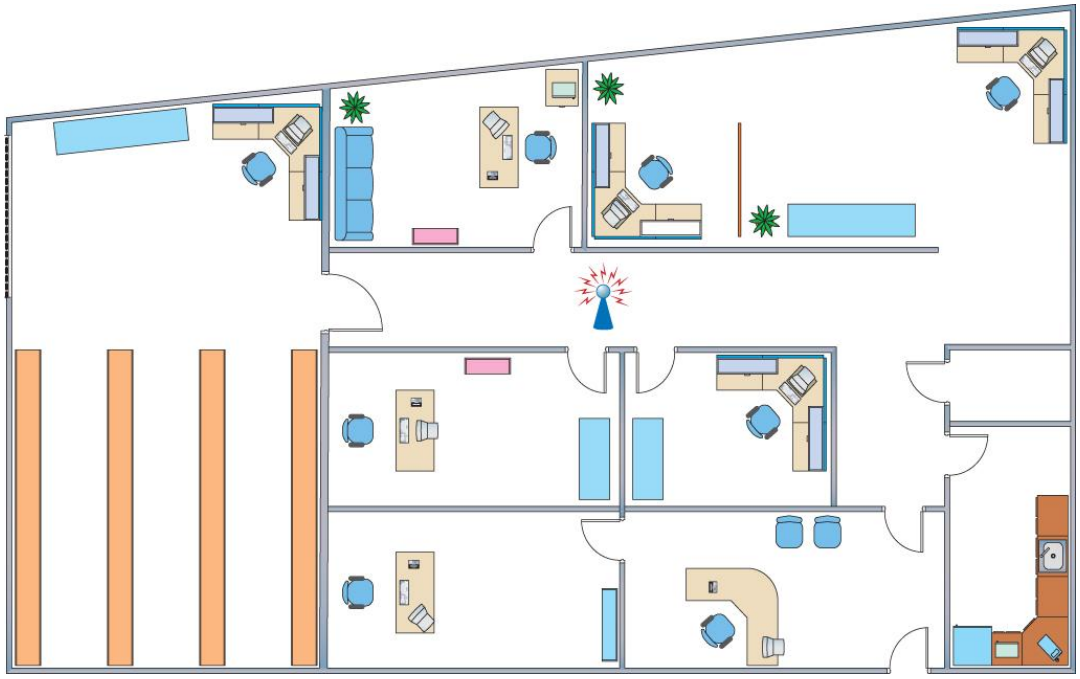

Figure 21: Room layout with WAP in the center

Antennas

- **Typical WAP uses an omnidirectional antenna called a dipole antenna.**
  - Provides blanket coverage
- **Better antennas can improve gain.**
- **Gain is measured in dBs.**
- **Third-party antennas are available.**

Figure 22: Replacement antenna on WAP

Bluetooth Configuration

- **Need two Bluetooth devices**
  - Set one as discoverable
  - Master/slave (pairing) happens automatically
  - The two devices will then determine what networking functions they can share

Bluetooth Configuration *(continued)*

Figure 23: iPAQ Bluetooth Manager software connected to Bluetooth access point

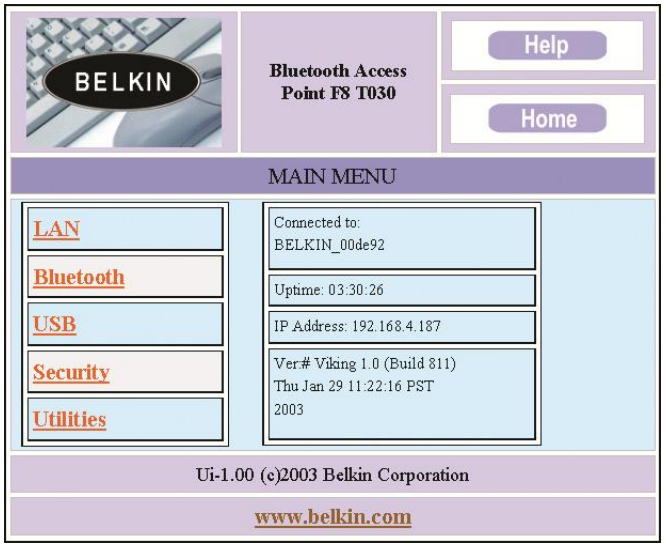

Figure 24: Belkin Bluetooth access point

Cellular Configuration

- **There is no single standard or method.**
  - Depends on vendor
  - Usually some type of configuration application

Figure 25: VZAccess Manager

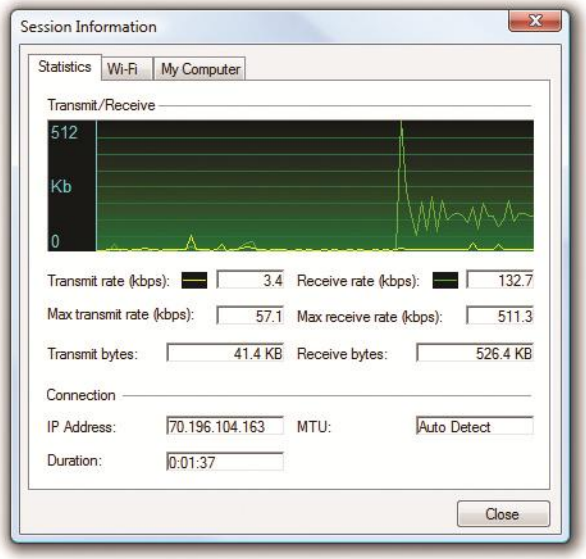

Figure 26: Session statistics for VZAccess Manager

Configuring Infrared Networks

- **Infrared**
  - Not much to configure
  - Confirm the IrDA protocol is installed
  - To transfer files
    - Use Wireless Link applet
    - Use Windows Explorer
  - To network two computers
    - Choose *Connect Directly to Another Computer*

Troubleshooting Wi-Fi

- **Who's affected by the problem?**
  - Asking this question helps localize the issue.
- **What is the nature of the network problem?**
  - Zeroing in on a particular service or application helps define the problem.
- **When did the problem start?**
  - Did some single action cause the problem?
  - Were there outside influences that caused the problem?

Troubleshooting Wi-Fi (*continued*)

- **Verify wireless NIC is functioning.**
  - Device Manager
  - Driver update
- **On portable computers with built-in cellular access, verify BIOS settings.**
  - Cellular access can be disabled in CMOS.
- **Update WAP.**
  - Many WAPs need a firmware update right out of the box.

Troubleshooting Wi-Fi (*continued*)

- **Verify network settings are correct.**
  - SSID
  - Encryption
- **Verify connectivity.**
  - Signal strength (check for low RF signal)
  - Link state
    - Enable (or disable) zeroconf service in Windows XP.
  - Interference

Figure 27: Windows XP Professional's wireless configuration utility