CWNA Guide to Wireless LANs, Third Edition

Chapter 12: Wireless Network Troubleshooting and Optimization

Objectives

- Describe the steps in troubleshooting RF interference
- Explain the techniques in troubleshooting a WLAN configuration
- List the steps in troubleshooting wireless devices
- Describe how to optimize a WLAN

Troubleshooting a Wireless Network

- Many WLAN problem sources can be grouped into three categories:
  - RF interference
  - WLAN configuration settings
  - Problems related to the wireless device itself

RF Interference

- RF interference is one of the main sources of WLAN problems
- Interference can be the result of:
  - External interference
  - Intersymbol interference

External Interference

- **Electromagnetic interference (EMI)**: electronic disturbance which causes an undesirable degrading in the performance of electrical equipment
- **Radio frequency interference (RFI)**: any undesirable electrical energy emitted within the frequency range dedicated to RF transmissions
- **Noise**: unwanted RF signals
- **Noise floor**: measure of the total of all the noise from different systems

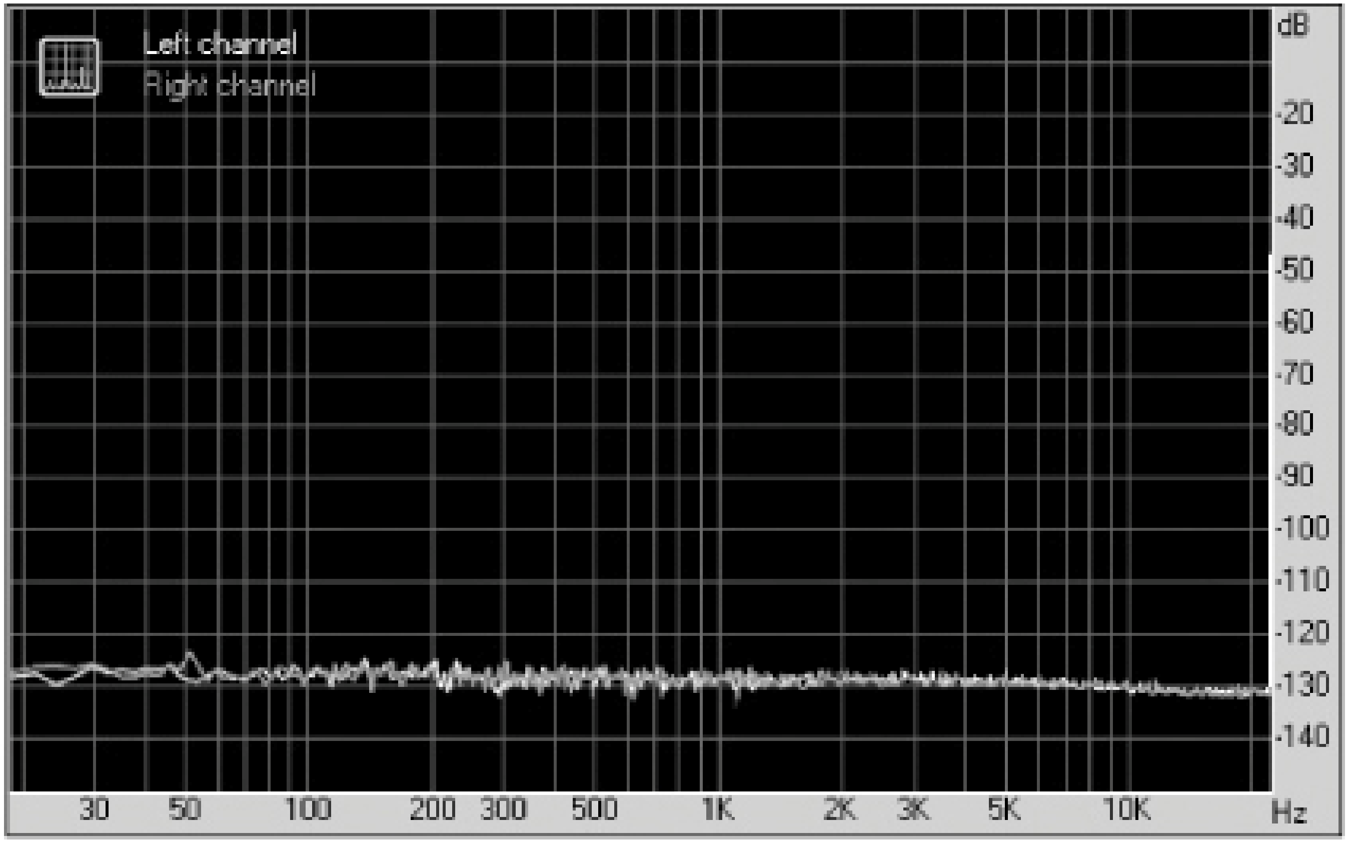


Figure 12-1 Noise Floor

External Interference

- There are four categories of external noise interference on a WLAN
  - Narrowband
  - Wideband
  - All-band
  - Weather

Narrowband Interference

- Narrowband interference: RF interference that is usually generated by television, radio, and satellite transmitters
  - Impacts only a narrow portion of the spectrum
  - Generally constant and so strong that it completely disrupts all communication
  - To troubleshoot, use a spectrum analyzer to determine the affected WLAN channel
  - Often an alternative channel can be chosen

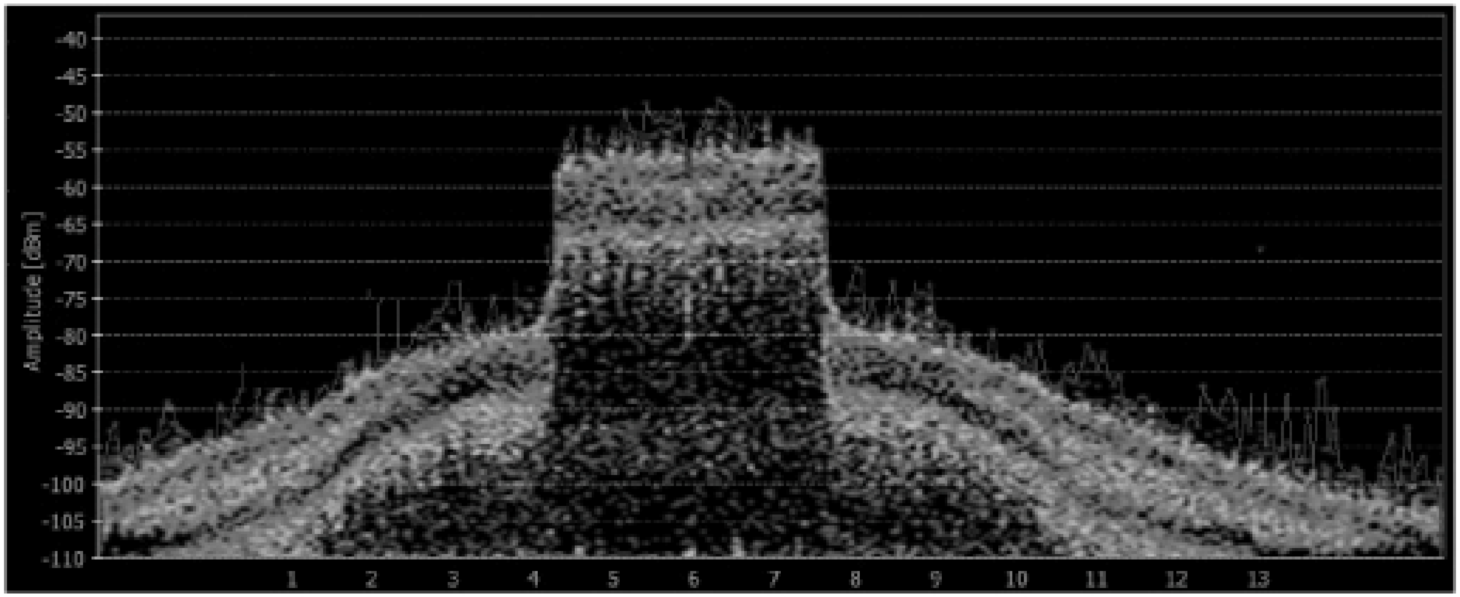


Figure 12-2 Narrowband interference

Wideband Interference

- Wideband interference: RF interference that affects the entire frequency band
  - Because entire band is impacted changing to an alternate channel is not a solution
  - Must locate the source of the interfering signal and remove it

All-Band Interference

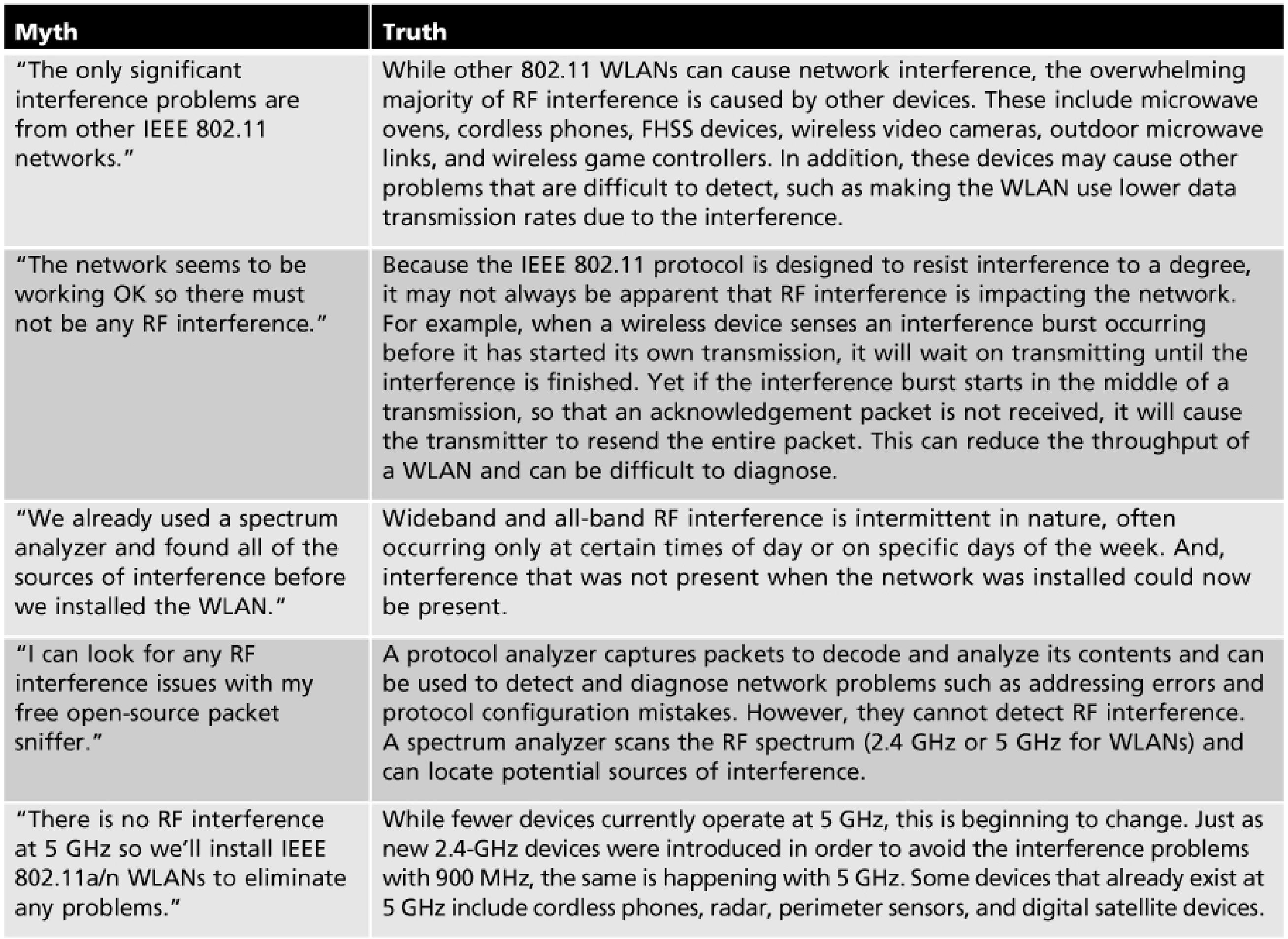
- All-band interference: RF interference that covers all bands of the RF spectrum
- Frequency-hopping spread spectrum (FHSS) uses range of frequencies that change during transmission
- Several solutions have been proposed:
  - Change the RF spectrum used
  - Modify power levels
  - Add switching software
  - Change the MAC layer
  - Change PHY layer

Weather Interference

- RF signals may move through different atmospheric conditions
- When an RF signal moves from one medium to another of a different density(such as cold, damp air) the signal bends instead of traveling in a straight line
  - Known as refraction
- Little can be done regarding the impact of weather on RF interference

RF Interference Troubleshooting

- Best practices to consider in order to reduce RF interference:
  - Be wary of noise and recognize situations where noise may impact transmissions
  - Maintain a system operating margin (SOM)
    - SOM is the difference measured in decibels between the received signal level and the signal level that is required so there are no errors
  - Maintain proper power
  - Separate antennas as much as possible



Myth	Truth
"The only significant interference problems are from other IEEE 802.11 networks."	While other 802.11 WLANs can cause network interference, the overwhelming majority of RF interference is caused by other devices. These include microwave ovens, cordless phones, FHSS devices, wireless video cameras, outdoor microwave links, and wireless game controllers. In addition, these devices may cause other problems that are difficult to detect, such as making the WLAN use lower data transmission rates due to the interference.
"The network seems to be working OK so there must not be any RF interference."	Because the IEEE 802.11 protocol is designed to resist interference to a degree, it may not always be apparent that RF interference is impacting the network. For example, when a wireless device senses an interference burst occurring before it has started its own transmission, it will wait on transmitting until the interference is finished. Yet if the interference burst starts in the middle of a transmission, so that an acknowledgement packet is not received, it will cause the transmitter to resend the entire packet. This can reduce the throughput of a WLAN and can be difficult to diagnose.
"We already used a spectrum analyzer and found all of the sources of interference before we installed the WLAN."	Wideband and all-band RF interference is intermittent in nature, often occurring only at certain times of day or on specific days of the week. And, interference that was not present when the network was installed could now be present.
"I can look for any RF interference issues with my free open-source packet sniffer."	A protocol analyzer captures packets to decode and analyze its contents and can be used to detect and diagnose network problems such as addressing errors and protocol configuration mistakes. However, they cannot detect RF interference. A spectrum analyzer scans the RF spectrum (2.4 GHz or 5 GHz for WLANs) and can locate potential sources of interference.
"There is no RF interference at 5 GHz so we'll install IEEE 802.11a/n WLANs to eliminate any problems."	While fewer devices currently operate at 5 GHz, this is beginning to change. Just as new 2.4-GHz devices were introduced in order to avoid the interference problems with 900 MHz, the same is happening with 5 GHz. Some devices that already exist at 5 GHz include cordless phones, radar, perimeter sensors, and digital satellite devices.

© Cengage Learning 2013

Table 12-1 Myths and truths about RF interference

Intersymbol Interference

- When an RF signal is transmitted, multiple copies of the signal are transmitted (known as multipath)
  - These copies are "added" to the primary signal
- Intersymbol interference (ISI) is the adding of signals to the primary signal
  - Can result in downfade, corruption, or nulling
- Two ways to reduce the impact of ISI:
  - Switch to a WLAN that supports MIMO
    - Will cause signals to take different paths
  - Use the correct antenna

WLAN Configuration

- WLAN configuration settings that may cause problems:
  - Cochannel interference
  - Adjacent-channel interference
  - Power settings
  - System throughput
  - Incorrect AP configuration settings

Cochannel Interference

- Cochannel interference: can result when two or more networks attempt to use the same channel
  - If all APs were set to the same channel throughput would be reduced
- Solution:
  - Use an application to identify if any other WLANs are in the area and on which channel they are transmitting
  - If cochannel interference exists with no free channels available, moving to a protocol with more non-overlapping channels may be the only option

Adjacent Channel Interference

- Adjacent interference occurs when one transmission on one channel encroaches upon another channel
- Solution:
  - Identify the channel that is being used by a nearby WLAN and switch to a different channel

Incorrect Power Settings

- An AP should not have an output power level higher than the output power level of the wireless device
- In a WLAN, the output power of the AP must be matched to that of the lowest-powered mobile device
- To troubleshoot incorrect power settings, use a spectrum analyzer

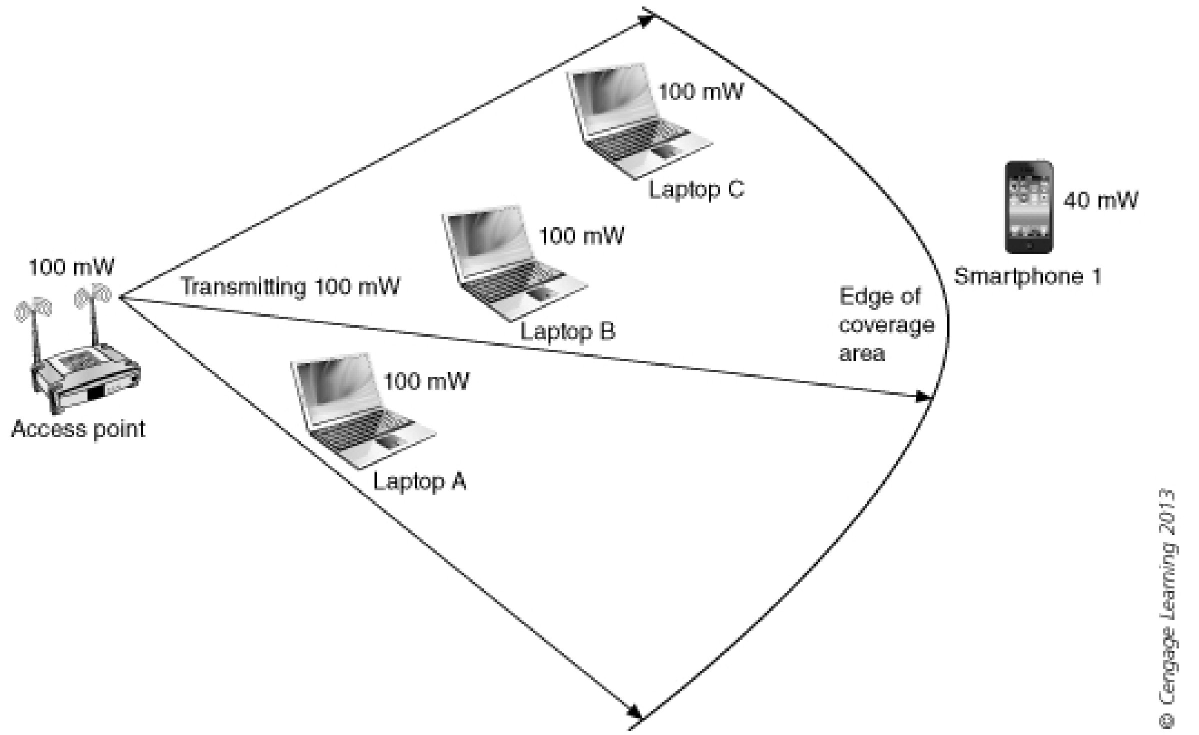


Figure 12-3 100 mW AP

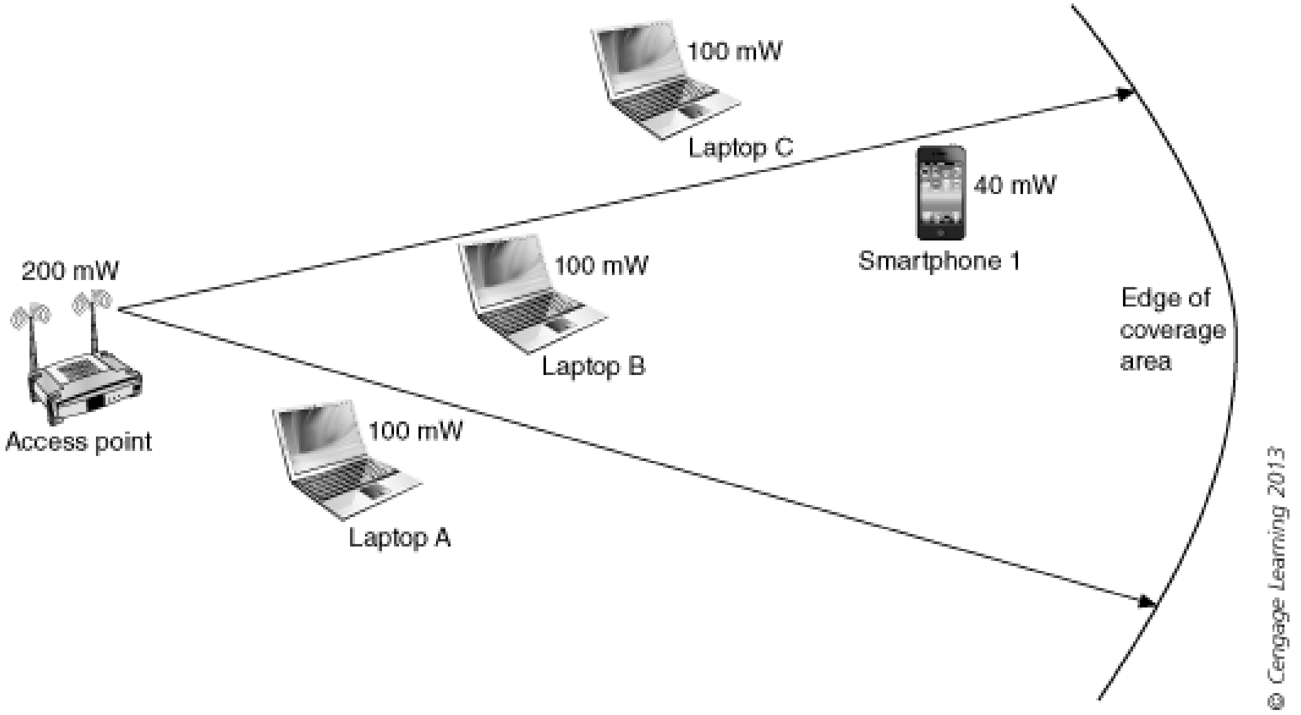


Figure 12-4 200 mW AP

System Throughput Problems

- Throughput is the measure of how much actual data can be sent per unit of time across a network
- Many factors influence WLAN transmission speed:
  - AP processor speed
  - Distance from AP
  - Implementing security solutions
  - Number of users associated with an AP
  - Packet size

System Throughput Problems

- Many factors influence WLAN transmission speed (continued):
  - Request to send/clear to send (RTS/CTS) protocol
  - Types of RF interference
  - Using Point Coordination Functions (PCF) protocol
- To troubleshoot:
  - Determine if all devices experiencing problem or only a single device
  - Identify potential causes that may have least impact on system if changed

AP Configuration Settings

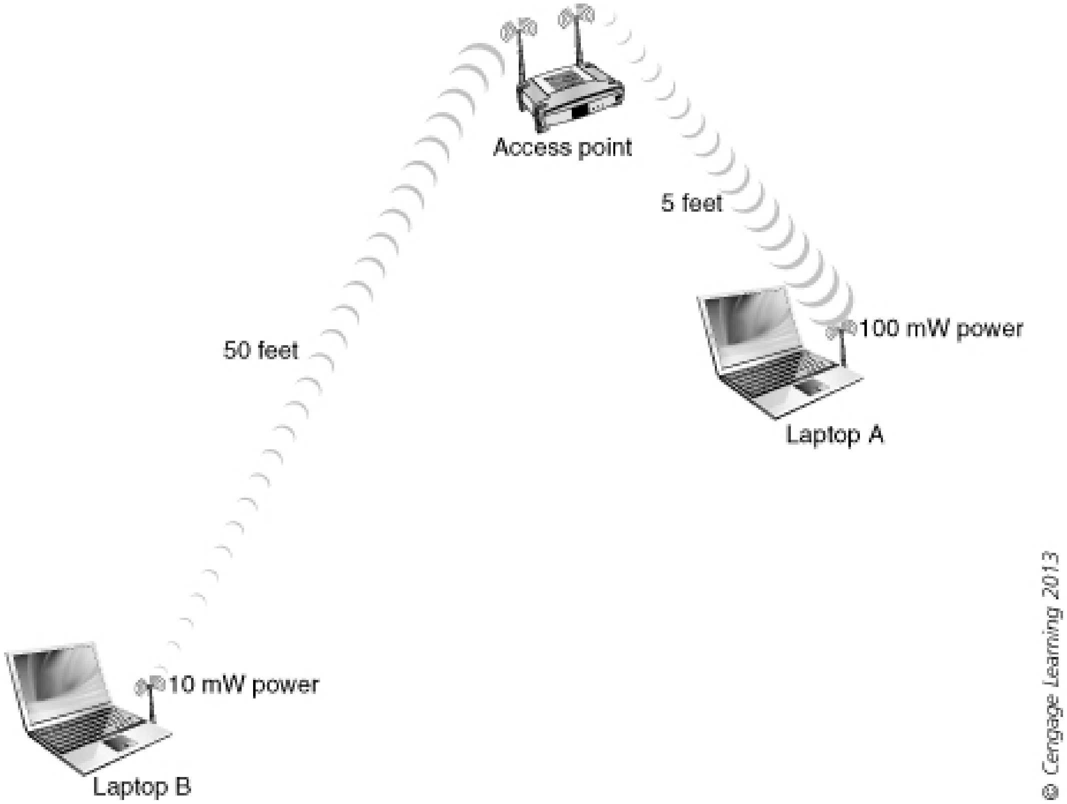
- Some WLAN problems are the result of incorrect or incompatible AP settings with other devices
- If there is no connectivity the following two areas are the primary sources:
  - SSID: If a client's device's SSID does not match the SSID of an AP the client device will not associate
  - Security settings: clients attempting to authenticate with AP must support the same security options configured in the AP

Wireless Device Troubleshooting

- Potential problems include:
  - Device location
  - Resolving connectivity issues

Device Location

- Near/Far: a transmission problem involving two wireless devices
  - The wireless device closest to the AP transmits at a higher power than the other, overwhelming the weaker signal from the distant device
- Possible solutions:
  - Move the device with the stronger power farther away
  - Reduce the transmission power of the devices that are closer to the AP
  - Increase the transmission power of devices that are farther away from the AP



© Cengage Learning 2013

Figure 12-5 Near/far

Device Location

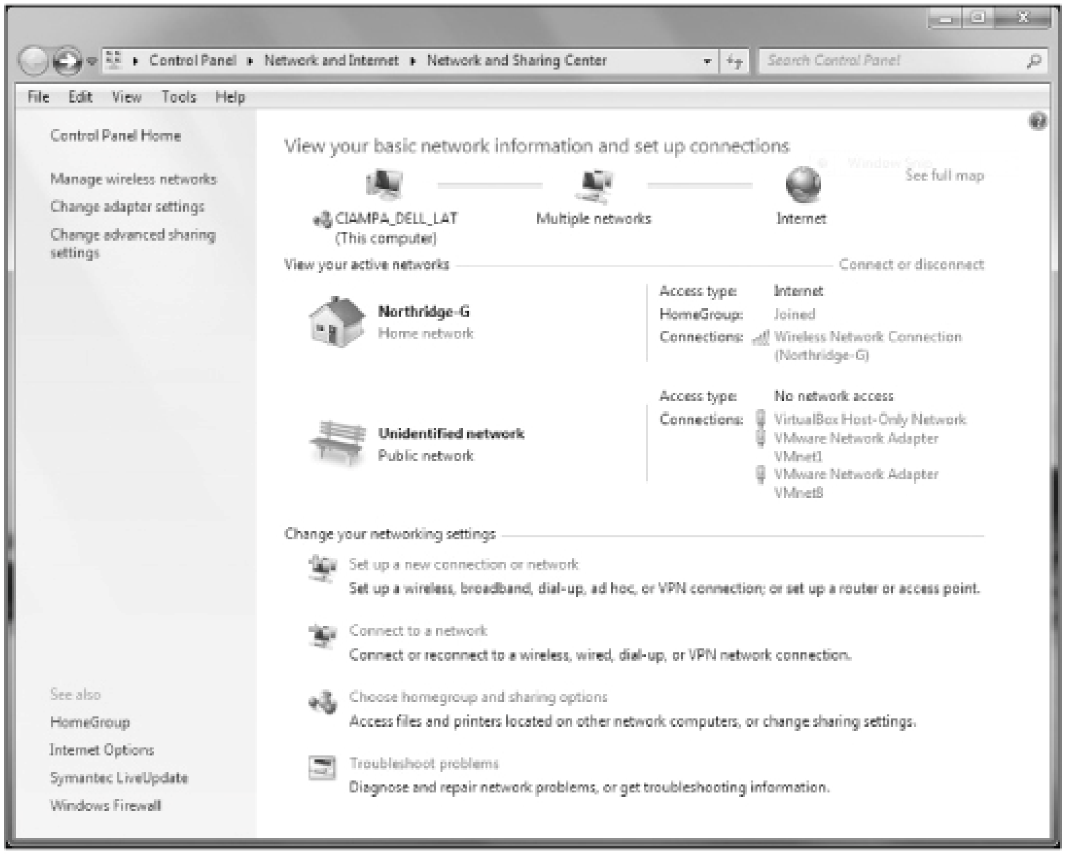
- Hidden Nodes: a station that is within range of an AP but not another station
- Several ways to resolve a hidden node problem:
  - Move the hidden node device
  - Remove any physical obstacles that may be interfering with devices communicating with each other
  - Add an additional AP to the WLAN

Resolving Connectivity Issues

- Windows Connection Process:
  - *Scan for wireless networks*
    - Wireless network adapter sends series of Probe Request frames
    - APs within range respond with Beacon frame that contains the capabilities of the wireless AP
  - *Choose an AP*
    - Decision based on:
      - Wireless AP capabilities
      - Preferred networks
      - Signal strength

Resolving Connectivity Issues

- Windows Connection Process (continued):
  - *Authenticate*
    - Type of authentication depends on security capabilities of AP and how wireless device has configured to authenticate with AP
  - *Associate*
    - Network adapter creates an association with the AP
  - *Obtain an IP address*
    - Manual addressing
    - DHCP addressing
    - APIPA addressing


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Symantec LiveUpdate

Windows Firewall

View your basic network information and set up connections

See full map

CIAMPA_DELL_LAT (This computer) — Multiple networks — Internet

View your active networks — Connect or disconnect

Northridge-G
Home network

Access type: Internet
HomeGroup: Joined
Connections: Wireless Network Connection (Northridge-G)

Unidentified network
Public network

Access type: No network access
Connections: VirtualBox Host-Only Network
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

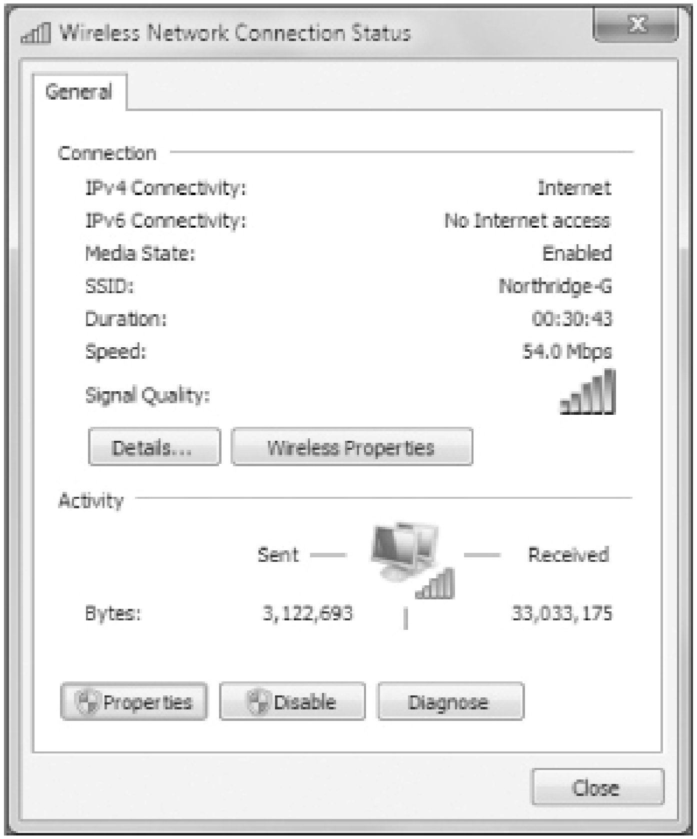
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

© Cengage Learning 2013

Figure 12-6 Windows Network and Sharing Center

Resolving Connectivity Issues

- Wireless Network Connection Status dialog box in Windows 7
  - Provides an overview of the current status by displaying the Layer 3 connectivity status, media state, SSID being used, length of time the connection has been active, negotiated connection speed, and signal quality
  - The Details button gives more information including addressing information



Wireless Network Connection Status

Connection

IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
SSID: Northridge-G
Duration: 00:30:43
Speed: 54.0 Mbps
Signal Quality:

Activity

Sent — — Received

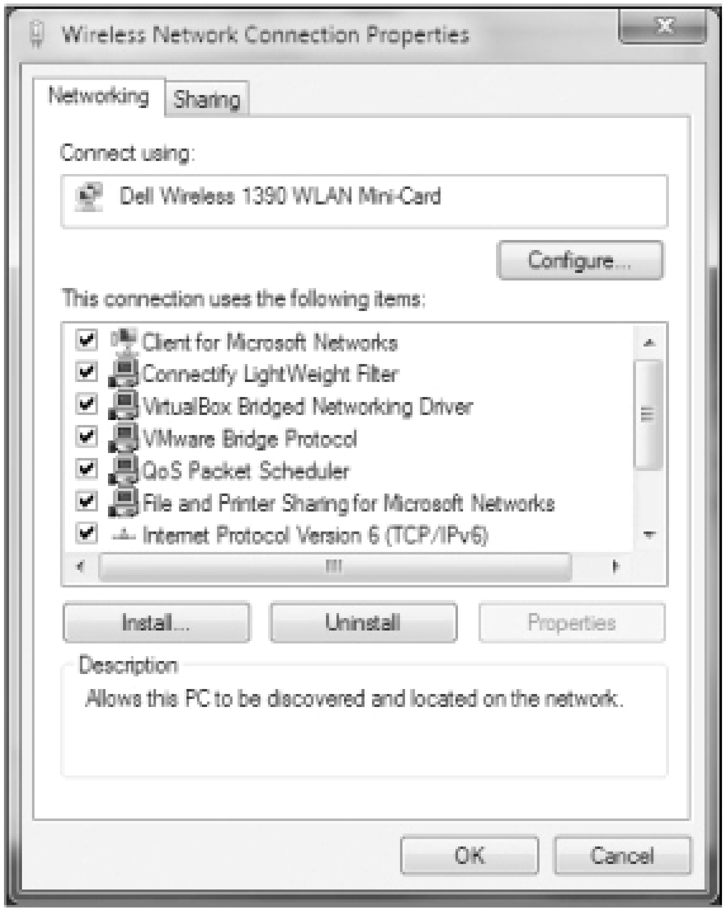
Bytes: 3,122,693 | 33,033,175

© Cengage Learning 2013

Figure 12-7 Wireless Network Connection Status

Resolving Connectivity Issues

- Wireless Network Connection Properties dialog box in Windows 7
  - Provides comprehensive information and the ability to adjust configurations
  - Important areas of this dialog box:
    - Networking tab
    - Sharing tab
    - This connection uses the following items list



Connect using:

Dell Wireless 1390 WLAN Mini-Card

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Connectify LightWeight Filter
- ☑ VirtualBox Bridged Networking Driver
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows this PC to be discovered and located on the network.

© Cengage Learning 2013

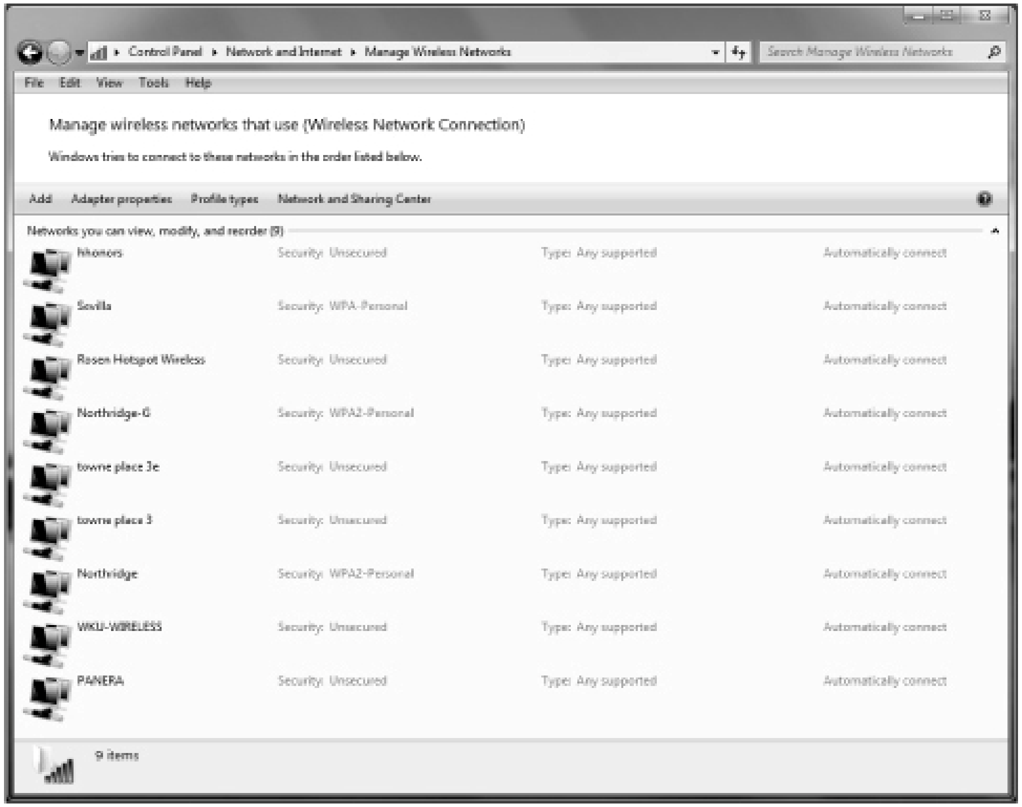
Figure 12-9 Wireless Network Connection Properties

Resolving Connectivity Issues

- Windows 8 operating system:
  - Uses a simpler, more integrated radio and connection management interface
  - Allows user to turn on and off installed wireless radios
  - Support native radio management to eliminate conflicts between applications
  - Will automatically disconnect a device from the user's mobile broadband network and power it down
  - Supports different WLAN hotspot authentication types

Troubleshooting Steps

- Possible causes if problems makings connection:
  - Incompatible IEEE 802.11 standards
  - Mismatched authentication methods
  - Mismatched pre-shared key
  - Conflict between operating system configuration and a third-party configuration tool
  - Incorrect MAC address
  - Disabled wireless adapter
  - Legacy wireless NIC driver
  - Outdated profiles


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Search Manage Wireless Networks
File
Edit
View
Tools
Help
Add
Adapter properties
Profile types
Network and Sharing Center

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

Networks you can view, modify, and reorder (9)

hhonors	Security: Unsecured	Type: Any supported	Automatically connect
Sevilla	Security: WPA-Personal	Type: Any supported	Automatically connect
Rosen Hotspot Wireless	Security: Unsecured	Type: Any supported	Automatically connect
Northridge-G	Security: WPA2-Personal	Type: Any supported	Automatically connect
towne place 3e	Security: Unsecured	Type: Any supported	Automatically connect
towne place 3	Security: Unsecured	Type: Any supported	Automatically connect
Northridge	Security: WPA2-Personal	Type: Any supported	Automatically connect
WKU-WIRELESS	Security: Unsecured	Type: Any supported	Automatically connect
PANERA	Security: Unsecured	Type: Any supported	Automatically connect

9 items

© Cengage Learning 2013

Figure 12-10 Network profiles

Troubleshooting Steps

- Possible causes if wireless device intermittently disconnects from AP:
  - Incompatible 802.1x authentication
  - Duplicate SSID
    - Generally result of default SSID being used on APs
  - Interference from nontraditional devices
    - Game consoles and streaming television Internet devices

WLAN Optimization

- WLAN optimization includes:
  - Channel optimization
  - Access point optimization
  - Wireless device optimization

Channel Optimization

- Optimizing the channel for roaming is a primary concern
- A device can only roam from the coverage area of one AP to another AP if the SSID and security settings are identical
- Cell overlap: area between two APs in which a wireless device begins to search for a new AP with which to associate

Channel Optimization

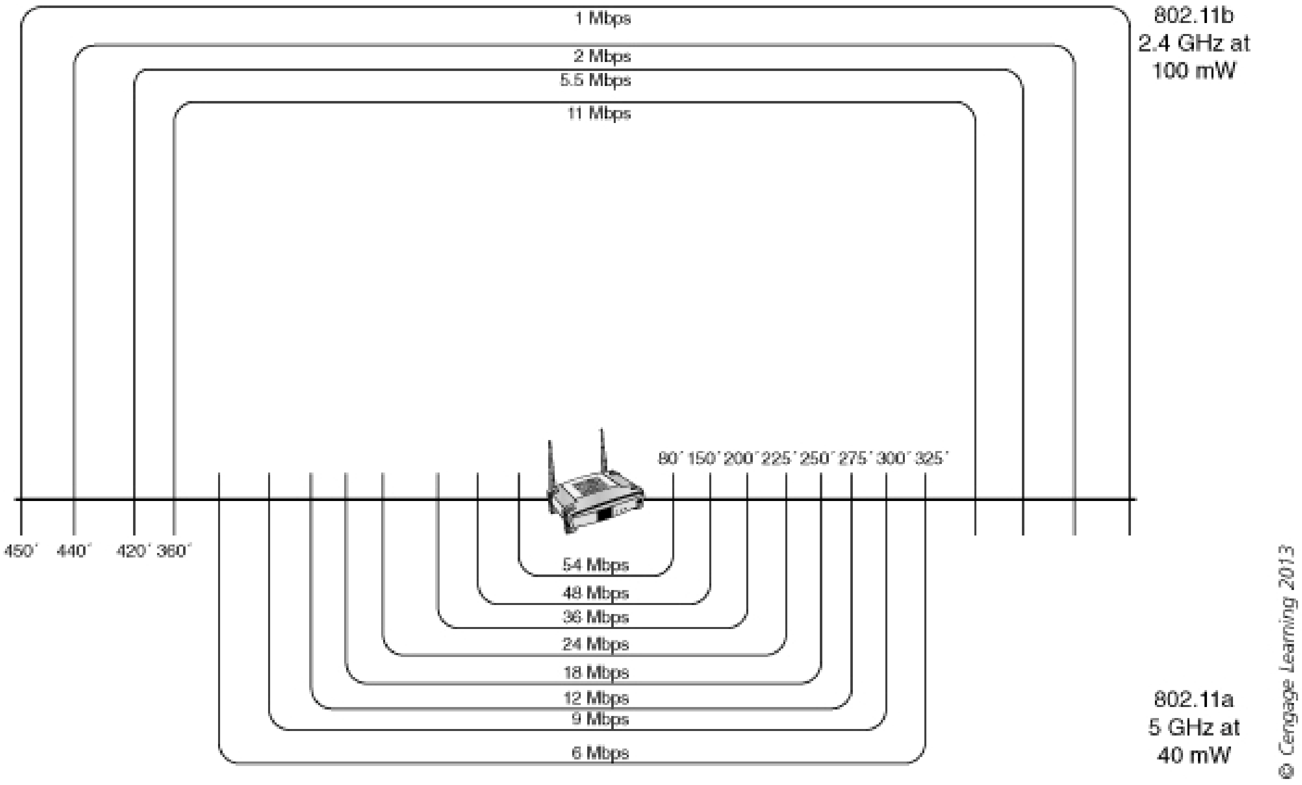
- In areas where wireless usage might be clustered together, such as a lecture hall or auditorium on a school campus, the solution is to optimize the channel by installing high-density WLANs
- High-density WLAN characteristics:
  - More APs are clustered together in order to provide the resources to users
  - APs are positioned in different locations
  - Newer standards are utilized to maximize throughput
  - Older standards are not implemented

Access Point Optimization

- Steps for optimizing APs include:
  - Never accept default configuration of an AP
    - Configure a unique SSID and set the highest level of security authentication and encryption settings
  - Install lightweight APs to minimize the total cost of ownership (TCO)
  - Configure wireless VLANs for additional security
  - Use wireless network management systems (WNMS)

Access Point Optimization

- Steps for optimizing APs (continued):
  - Use a captive portal AP for guest accounts
  - Use picocells when necessary
    - Picocell is a WLAN that uses a reduced power output from the AP that results in a smaller coverage but can allow for increased performance due to channel reuse
  - Size the coverage area to the corresponding standard (see next slide)



© Cengage Learning 2013

Figure 12-12 Coverage area comparison

Wireless Device Optimization

- Devices that rely on time-dependent applications, such as voice or video streaming, perform better with les roaming
  - Devices may be configured as “conservative roaming”
  - Other devices that do not normally use these applications can be set to “aggressive roaming”
- Whenever possible, devices should be set to “disable upon wired connect”
  - Provides a higher degree of security so the device cannot be used as a rogue AP

Summary

- One of the main sources of WLAN problems is RF interference
- Four categories of external noise interference are narrowband, wideband, all-band, and weather interference
- Intersymbol interference (ISI) can result in downfade, corruption, or nulling
- Another category of WLAN problem sources has to do with WLAN configuration
- Cochannel and adjacent channel interference may lead to changing an APs channel configuration

Summary

- An AP should not have an output power level higher than the output power level of the wireless device
- Some WLAN problems are the result of incorrect AP settings or AP settings that are incompatible with other devices
- A device that is transmitting at higher signal strength and is located closer to the access point will drown out a weaker signal from a device that is farther away and is using less power

Summary

- Microsoft Windows operating system provides tools that can be used to view and make changes to the wireless connection
- Ensuring smooth roaming between WLANs is based on cell overlap
- Wireless networks that are used in areas in which large numbers of devices are clustered close together are known as high-density WLANs
- Optimizing APs and wireless devices can lead to a more efficient WLAN