University of Colorado **Boulder**

Fundamentals of Data Communications

Wireless Technologies

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

Review

Radio Propagation Basics

- **Electro Magnetic Waves**
  - Wavelength, frequency, amplitude, phase
  - Sign Wave
  - Cycle/Hertz
  - Positive & Negative
- **Spectrum (Licensed and Unlicensed)**
  - 2.4 and 5 Ghz
- **Interference**
- **Multi path Propagation**
- **Frequency vs. Line of Sight**
- **RF Attenuation**
- **Channel Selection**
- **Higher Frequencies / Lower Range / Noise / Throughput**

Differences Between WLAN and LAN

- WLANs use radio waves as the physical layer.
  - ***WLANs use CSMA/CA instead of CSMA/CD for media access***
  - ***Two-way radio (half-duplex) communication***
- Radio waves have problems that are not found on wires
  - ***Connectivity issues:***
    - Coverage problems
    - Interference, noise
  - ***Privacy issues***
- Access points are shared devices similar to an Ethernet hub for shared bandwidth
- WLANs must meet country-specific RF regulations

Wireless Applications

- **Wireless communications are very common in all areas**

- **Several sectors use wireless more extensively than others:**
  - Education
  - Business
  - Industry
  - Travel
  - Public safety
  - Health care

Education

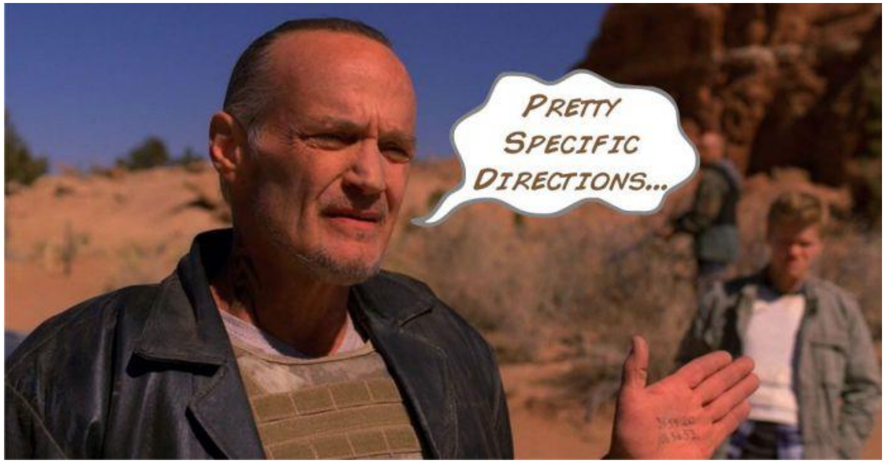
- **Educational institutions were among the first to adopt wireless technology**
  - Instructors can create presentations on a laptop and carry them into any classroom where it will connect automatically to the campus network
  - Students can easily connect wirelessly to a campus network

- **WLAN technology translates into cost savings for schools**
  - Reduces need for wiring and infrastructure
  - Fewer computer labs necessary

Business

- **The introduction of wireless access in conference rooms provides all employees with a mobile office**
- **Employees no longer have to compete for an available wired connection or carry cables with them**
- **A Cisco study showed that when wireless communications were introduced in business**
  - increased productivity by 86 minutes per day per user
- **Small office/home office (SOHO) business can also benefit from wireless data communications**

Industry



- **Examples of wireless data transmission can be found in the fields of construction, warehouse management, and manufacturing**
- **Construction examples:**
  - A problem with materials can be relayed to main office so workers can be routed to other sites to prevent idle time
  - Construction equipment (bulldozers and earth graders) have wireless devices that turn them into smart machines capable of precise positioning using a **global positioning system (GPS)**

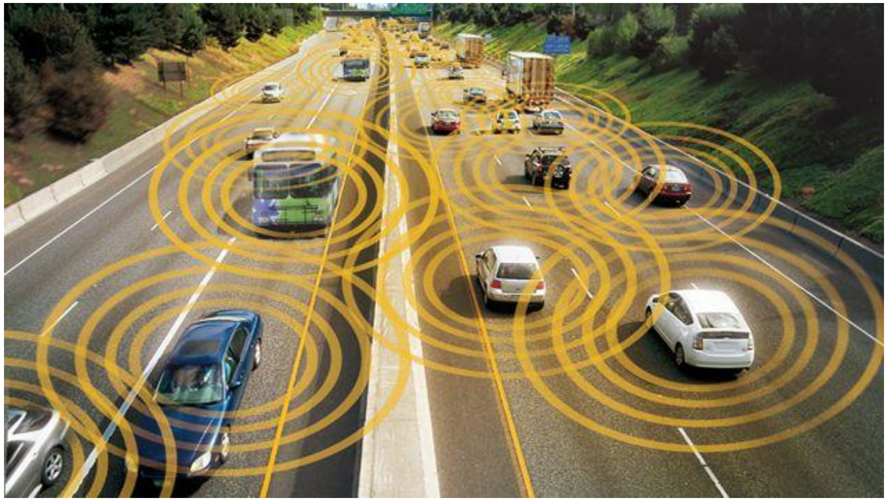
Industry

- **Warehouse Management examples:**
  - Forklift trucks can be outfitted with wireless equipment and employees can wear portable wireless inventory devices to scan bar codes
  - **Warehouse management system (WMS)** software manages all warehouse activities
    - ***WMS is tied into network so managers have ready access to up-to-the-minute statistics***
  - **Radio frequency identification (RFID)** tags emit a wireless data signal containing an ID number
    - ***Works with WMS to track inventory***

Industry

- **Manufacturing examples:**
  - – RFID tags are often used
  - – When additional parts are needed on a production line, workers press call buttons to request stock (or automate it)
  - – Battery-powered tags transmit the request wirelessly
  - – Inventory can quickly be delivered to eliminate a slow down in the production line

Travel



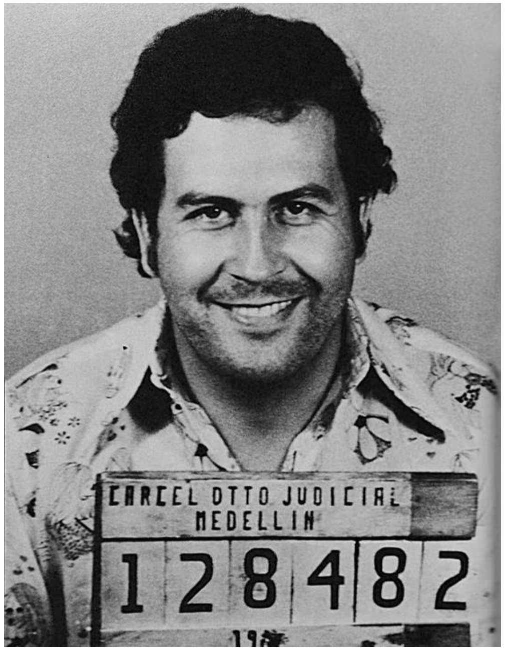
- **Airlines, commuter rail lines, and even ferry boats are now offering wireless data access**

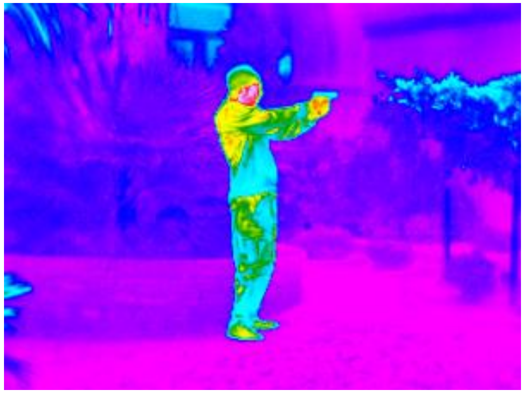
- ***Vehicle-to-vehicle (V2V)* communications uses both GPS and wireless to create a network that allows cars to communicate with one another**
  - Can alert drivers of accidents or traffic hazards ahead of them
  - Can also be used to control traffic jams

- **Self-driving vehicles**

Public Safety

- **Public safety departments using WLANs to communicate information with public safety vehicles**
  - Large volumes of data can be quickly downloaded to vehicles
    - ***e.g., building floor plans, photographs of criminal suspects, and maps***





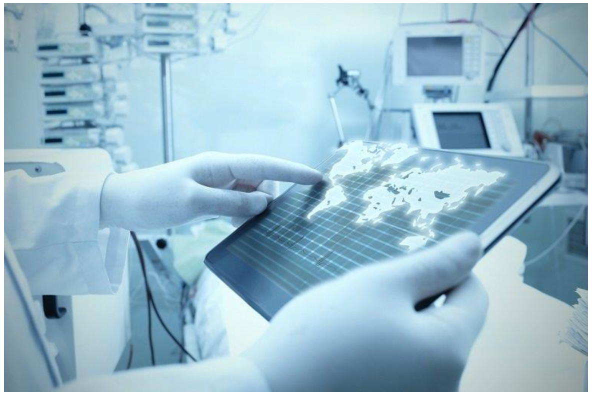
Health Care

- **Wireless LAN point-of-care computer systems allow medical staff to access and update patient records immediately**
  - Document patient's medication administration immediately
  - Extensive use of RFID tags
    - ***Identify healthcare professionals, patients, medications***
  - System verifies that medication being administered to correct patient in correct dosage
    - ***Eliminates potential errors and documentation inefficiencies***

Health Care

- **Documentation process takes place at bedside where care delivered**
  - Improves accuracy

- **Hospital personnel have real-time access to latest medication and patient status information**



- **Wireless technology also used in other medical areas:**
  - e.g., video pills

- **Security vulnerability?**
  - pacemaker

Wireless Advantages and Disadvantages: Advantages

- **Mobility: Primary advantage of wireless technology**
  - – Enables individuals to use devices no matter where users roam within range of network
  - – Increasingly mobile workforce is characteristic of today's business world
  - – WLANs give mobile workers freedom while allowing them to access network resources
  - – "Flatter" organizations: WLANs give team-based workers ability to access network resources needed while collaborating in team environment

Wireless Advantages and Disadvantages: Advantages

- **Access: wireless can provide network access to areas where previously none existed**
  - **Hotspot**: Locations where wireless data services are available
  - **Municipal networks**: hotspots typically found in downtown areas, parks and recreation areas and other high-traffic areas
  - Advantages of municipal networks:
    - ***More attractive to businesses***
    - ***Local police, fire, and municipal workers can use them***
    - ***Provide high speed Internet access for free or low cost***
  - Remote/distant locations

Wireless Advantages and Disadvantages: Advantages

- **Connectivity: Wireless technologies can provide improved service, extend the reach of networks, and provide a less expensive alternative to wired technologies**
  - **Wireless ISP**: provides wireless data access directly to the home instead of a cable or DSL provider
  - **Backhaul connection**: an organization's internal infrastructure connection between two or more remote locations
    - ***Wireless networks can be used eliminating the costs associated with leasing lines or installing fiber optic cables***

Wireless Advantages and Disadvantages: Advantages

- **Deployment: Installing network cabling in older/historic buildings difficult and costly**
  - Wireless LAN is ideal solution
  - Eliminating need for cabling results in cost savings
    - ***Significant time savings as well***
  - Allows offices to reorganize easily
  - Wireless LAN technology eliminates certain types of cable failures and increases overall network reliability
  - Disaster scenarios

Wireless Advantages and Disadvantages: Disadvantages

- **Security: Wireless signals broadcast in open air**
  - – Security for wireless LANs is prime concern
    - ***Unauthorized users might access network***
      - – Can often pick up signal outside the building
    - ***Attackers might view transmitted data***
    - ***Employees could compromise network security***
      - – Could install rogue access points
    - ***Attackers could crack existing wireless security***
      - – Older wireless products have weak security features

Wireless Advantages and Disadvantages: Disadvantages

- **Radio Signal Interference: Signals from other devices can disrupt wireless transmissions**
  - e.g., Microwave ovens, elevator motors, photocopying machines, theft protection devices, cordless telephones
  - Physical interference
    - ***Outdoor***
  - Intentional signal jamming

- **Range of Coverage: Some wireless signals only have a range of 10 feet while others extend to over 350 feet**

- **Slow Speed: a packet moving through a wireless network is slower than it would be on a wired network**

Types of Wireless Networks

- **Four broad categories:**
  - Wireless personal area networks (WPAN)
  - Wireless local area networks (WLAN)
  - Wireless metropolitan area networks (WMAN)
  - Wireless wide area networks (WWAN)

Wireless Personal Area Network (WPAN)

- **WPAN: wireless network designed for hand-held and mobile devices**
  - – Slow transmission speeds
  - – Close proximity to other devices (max distance is generally 33 feet)

- **Bluetooth – WPAN technology that uses short-range transmissions**
  - – Enables users to connect wirelessly to devices such as notebook/tablet computers, smartphones, and other portable devices

Wireless Local Area Networks (WLANs)

- **WLAN: designed to replace or supplement a wired local area network (LAN)**
- **Devices can communicate within 350 feet**
- **Transmission speeds can range up to 600 Mbps (10 Gbps)**

Wireless Metropolitan Area Network (WMAN)

- WMAN: designed for devices in a broader area of coverage or at higher speeds

- A WMAN coverage area could range from several city blocks to an entire small city

- Some WMAN technologies use light impulses to send and receive data

Wireless Wide Area Network (WWAN)

- **WWAN: wireless data network that extends beyond the range of a WMAN**
  - Can encompass multiple states, regions, or countries
  - Can even be a world-wide wireless data network

- **Long Term Evolution (LTE) modem provides wireless access several miles away from the transmission point**

Radio Propagation Basics

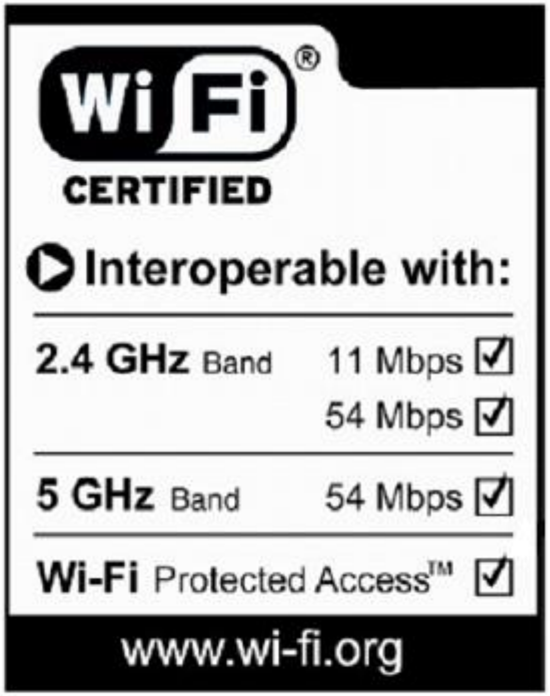
- **Electro Magnetic Waves**
  - Wavelength, frequency, amplitude, phase
  - Sign Wave
  - Cycle/Hertz
  - Positive & Negative
- **Spectrum (Licensed and Unlicensed)**
  - 2.4 and 5 Ghz
- **Interference**
- **Multi path Propagation**
- **Frequency vs. Line of Sight**
- **RF Attenuation**
- **Channel Selection**
- **Higher Frequencies / Lower Range / Noise / Throughput**

Wireless Standards Organizations and Regulatory Agencies

- **Several organizations provide direction, standards, and accountability in wireless technology**
  - International Telecommunication Union Radio Communication Sector (ITU-R)
  - US Federal Communications Commission (FCC)
  - International Organization for Standardization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Wi-Fi Alliance

Wi-Fi Certification

- **Wi-Fi Alliance certifies interoperability between products.**
  - Products include 802.11a, 802.11b, 802.11g, dual-band products, security testing, etc.
  - Provides assurance to customers of migration and integration options.
- **Cisco is a founding member of the Wi-Fi Alliance.**
- **Certified products can be found at http://www.wi-fi.com.**



Wi Fi®

CERTIFIED

Interoperable with:

2.4 GHz Band	11 Mbps	☑
	54 Mbps	☑
5 GHz Band	54 Mbps	☑
Wi-Fi Protected Access™		☑

www.wi-fi.org

Wireless Standards

- **802.11a**
  - 5GHz Spectrum / OFDM / 54Mbps / 27Mbps throughput
  - Less Interference
  - Half Range than 802.11b
  - Not Popular
  - Indoor Range (40ft - 54Mbps, 300ft - 6 Mbps)
  - Outdoor (100ft -54Mbps, 1000ft - 1 Mbps)
  - 8 non overlapping channels supported

- **802.11b**
  - 2.4GHz / DSSS / 11Mbps / 5 - 6 throughput
  - 1,2,5.5 and 11Mbps Depending on Signal Strength
  - Affordable / Popular / Hackable
  - “Sufficient Speed for Average user”
  - Indoor Range (100ft - 11Mbps, 300ft - 1 Mbps)
  - Outdoor (400ft -11Mbps, 1500ft - 1 Mbps)
  - 3 non-overlapping Channels Supported (11 available)

Wireless Standards

- **802.11g**
  - 2.4GHz / OFDM / 54Mbps / 20-25 Mbps throughput
  - Indoor Range (100ft - 54Mbps, 300ft - 1 Mbps)
  - Outdoor (400ft -11Mbps, 1500ft - 1 Mbps)
  - Backwards Compatible with 802.11b
    - ***Slower Speeds***
  - Non-overlapping channels – 1, 6, 11

- **802.11n**
  - Multiple antennas
    - ***MIMO – Multiple-input multiple-output***
  - 600 Mbps
  - 5GHz & 2.4GHz

- **802.11ac**
  - 5GHz Band
  - 1 Gbps

- **802.11ax (Wi-Fi6)**
  - 2.4 & 5 GHz & 6GHz
  - AKA “High Efficiency Wi-Fi”
    - ***Dense environments***
  - Enhances throughput and lowers latency

Wireless Standards

- **Bluetooth**
  - 2.4GHz frequency hopper (1600/sec) / 720Kbps Max
  - Personal Area Network (PAN)
  - Low Powered (1mW) - Minimal Interference to 802.11b
  - Replaces other wires

- **900MHz**
  - Baby Monitors/Phones/Video Cameras
  - Low Frequency Better Coverage (through walls easier)
  - Cisco Aironet Bridges / WaveLAN

- **Data over Cellular**
  - CDPD (TDMA)
  - 1xRTT (CDMA)
  - GPRS (GSM) EDGE Network
  - LTE
  - 5G

Wireless Equipment

- **Wireless Adapter (NIC)**
  - External / Internal

- **Wireless Access Point (WAP or AP)**
  - Connection to network
  - Bridge Behavior
  - Contain Frame on Wireless or Forward to Wired
  - L2 Forwarding / Fast!
  - Types
    - ***Point to Point (Ethernet to Wireless adapters)***
    - ***Point to Multipoint (Standards AP)***
  - Virtual Access Point (VAP)
  - 802.11F (IAPP) To track users between multiples APs

http://systems.cs.colorado.edu/downloads/802-standards/ieee-802.11f.pdf

Wireless Equipment

- **Wireless Repeater**
  - Extend the range of an existing WLAN
  - Regenerates a Network Signal
  - Does not physically connect by wire to any part of the network
  - They reduce throughput on the WLAN
  - A repeater must receive and retransmit each frame on the same RF channel, which effectively doubles the number of frames that are sent.
  - Configure SSID of Root AP to serve
  - If multiple APs, one with better signal (Configurable by MAC also)

Wireless Equipment

- **Wireless Router**
  - Connection to Multiple Networks
  - Layer 3 forwarding for every packet vs. directed traffic
  - Network Address Translation
  - DHCP
  - Port Based Control / Filtering / Firewall
    - ***MAC***
    - ***URL***
    - ***IPSec Sessions***
    - ***VPN Support***
  - Access Controller (AC)

Network Types

- **Independent (ad-hoc)**
  - Direct connection between users (hub)
  - Temporal Networks (Meetings, file exchange)

- **Infrastructure**
  - All traffic goes across AP/Router (two step communication)
  - Range to AP not between users
  - Users associated with only one AP at the time
  - No limit on the number of users an AP may serve / throughput
  - Hardware
  - Business vs. Home
    - ***Antenna not associated to device***
    - ***Multiple wireless interfaces (User density)***
    - ***IAPP***

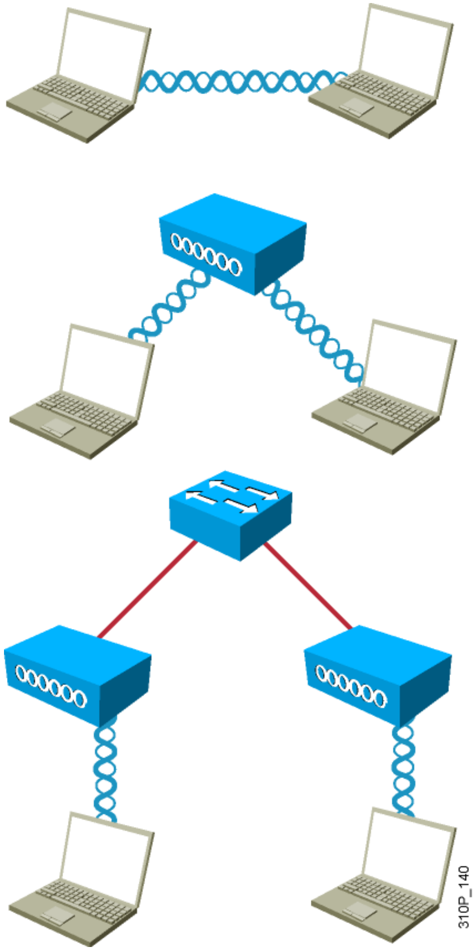
802.11 Topology Building Blocks

Ad hoc mode:

- Independent Basic Service Set (IBSS)
  - Mobile clients connect directly without an intermediate access point.

Infrastructure mode:

- Basic Service Set (BSS)
  - Mobile clients use a single access point for connecting to each other or to wired network resources.
- Extended Service Set (ESS):
  - Two or more BSSs are connected by a common distribution system .

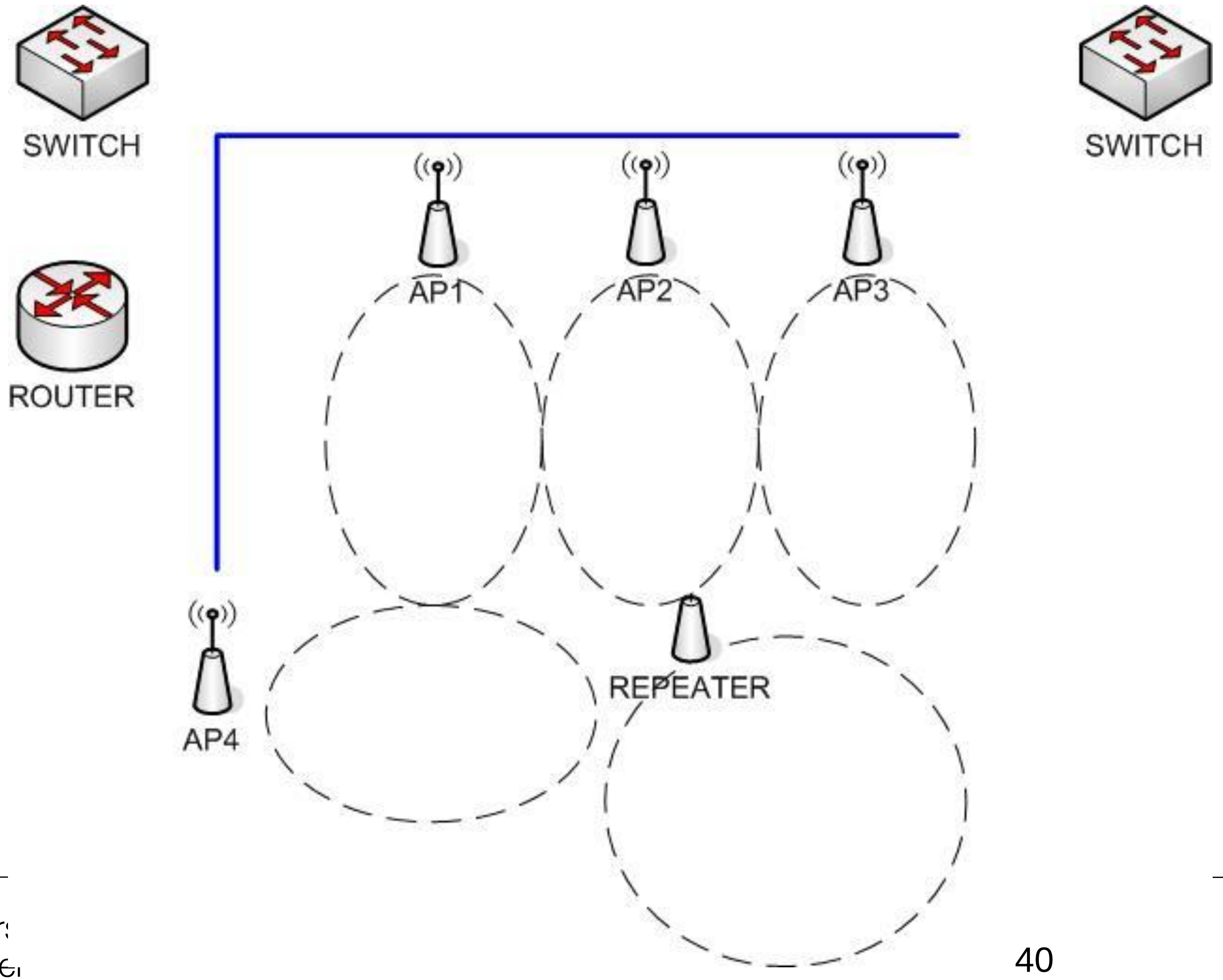


Connecting to an AP

- **SSID (Service Set Identifier)**
  - Differentiates one WLAN from another
  - VLANs
- **Frequency used (2.4 or 5)**
- **Power**
- **Channel**
- **Mode (Ad-hoc, Infrastructure)**
- **AP MAC Address**
- **Data Rate**
  - Distance reduces throughput

Distribution System

- **Wired interconnection between APs**



What is a wireless site survey?

- **Site survey: Process of planning a WLAN to meet design goals**
  - Effectiveness of a WLAN often linked to thoroughness of the site survey

- **ABSOLUTELY CRITICAL FOR SUCCESSFUL WLAN**

What is a Site Survey?

- **When installing a WLAN for an organization, areas of dead space might not be tolerated**
  - Ensure blanket coverage, meet per-user bandwidth requirements, minimize “bleeding” of signal

- **Factors affecting wireless coverage goals:**
  - Devices emitting RF signals
  - Building structure (walls, construction materials)
  - Open or closed office doors
  - Stationary versus mobile machinery/equipment
  - Movement of mobile walls (e.g., cubicles)

What is a Site Survey?

- **Factors affecting wireless coverage goals (continued):**
  - Expansion of physical plant or growth of organization
  - Existing WLANs
    - ***Both inside organization, and within nearby organizations***

Purpose of a Site Survey

- **Design goals for a site survey:**
  - Achieve best possible performance from WLAN
  - Certify that installation will operate as promised
  - Determine best location for APs
  - Develop networks optimized for variety of applications
  - Ensure coverage will fulfill organization’s requirements
  - Locate unauthorized APs

Purpose of a Site Survey

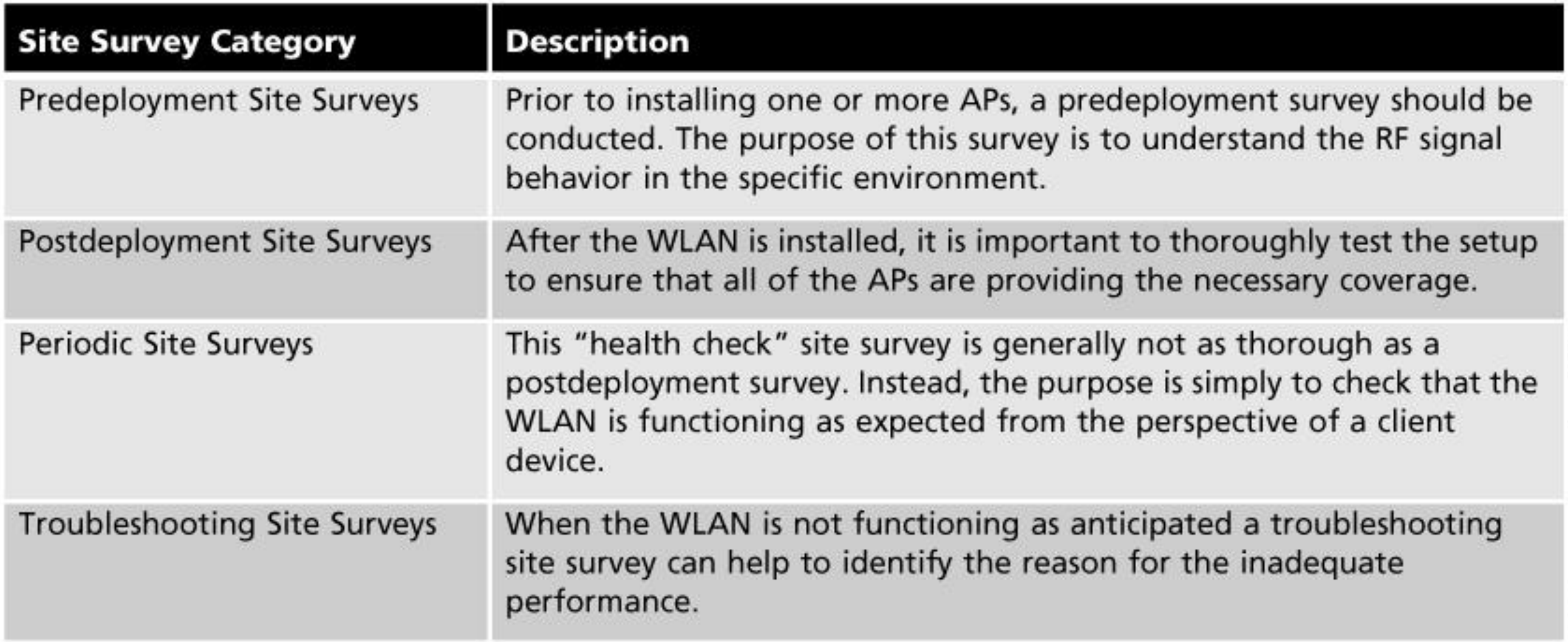
- **Design goals for a site survey (continued):**
  - Map nearby wireless networks to determine existing radio interference
  - Reduce radio interference as much as possible
  - Make wireless network secure

- **Survey provides realistic understanding of infrastructure required for proposed wireless link**
  - Assists in predicting network capability and throughput
  - Helps determine exact location of APs and power levels required

When to Perform a Site Survey

- **When to perform a site survey:**
  - Before installing a new wireless network
  - After physical changes to a building
  - After changes to an existing wireless network
  - If network needs change for the organization
  - After significant changes in personnel

- **Automated RF resource management: a dynamic self-managing WLAN**
  - the wireless devices monitor the environment and automatically adjust power levels or channels to compensate for changes



Site Survey Category	Description
Predeployment Site Surveys	Prior to installing one or more APs, a predeployment survey should be conducted. The purpose of this survey is to understand the RF signal behavior in the specific environment.
Postdeployment Site Surveys	After the WLAN is installed, it is important to thoroughly test the setup to ensure that all of the APs are providing the necessary coverage.
Periodic Site Surveys	This "health check" site survey is generally not as thorough as a postdeployment survey. Instead, the purpose is simply to check that the WLAN is functioning as expected from the perspective of a client device.
Troubleshooting Site Surveys	When the WLAN is not functioning as anticipated a troubleshooting site survey can help to identify the reason for the inadequate performance.

© Cengage Learning 2013

Procedures for Performing a Site Survey

- **Three basic steps in conducting a site survey:**
  - – Gathering background data
  - – Performing the actual survey
  - – Generating the site survey report

Wireless Deployment

- **Flexibility vs. Security**
- **Site Survey (Wireless Environment)**
  - Business Requirements
  - Number and types of clients, topology of network, types of media, etc.
  - Indoor and Outdoor Requirements
  - Infrastructure Connectivity Requirements
  - Security
  - Signal Strength / Coverage / Throughput
  - Cost
  - Antenna / AP combinations
  - Building Construction Materials
  - Identify Sources of Interference (Microwave Ovens, Phones, Other Businesses)

Wireless Deployment

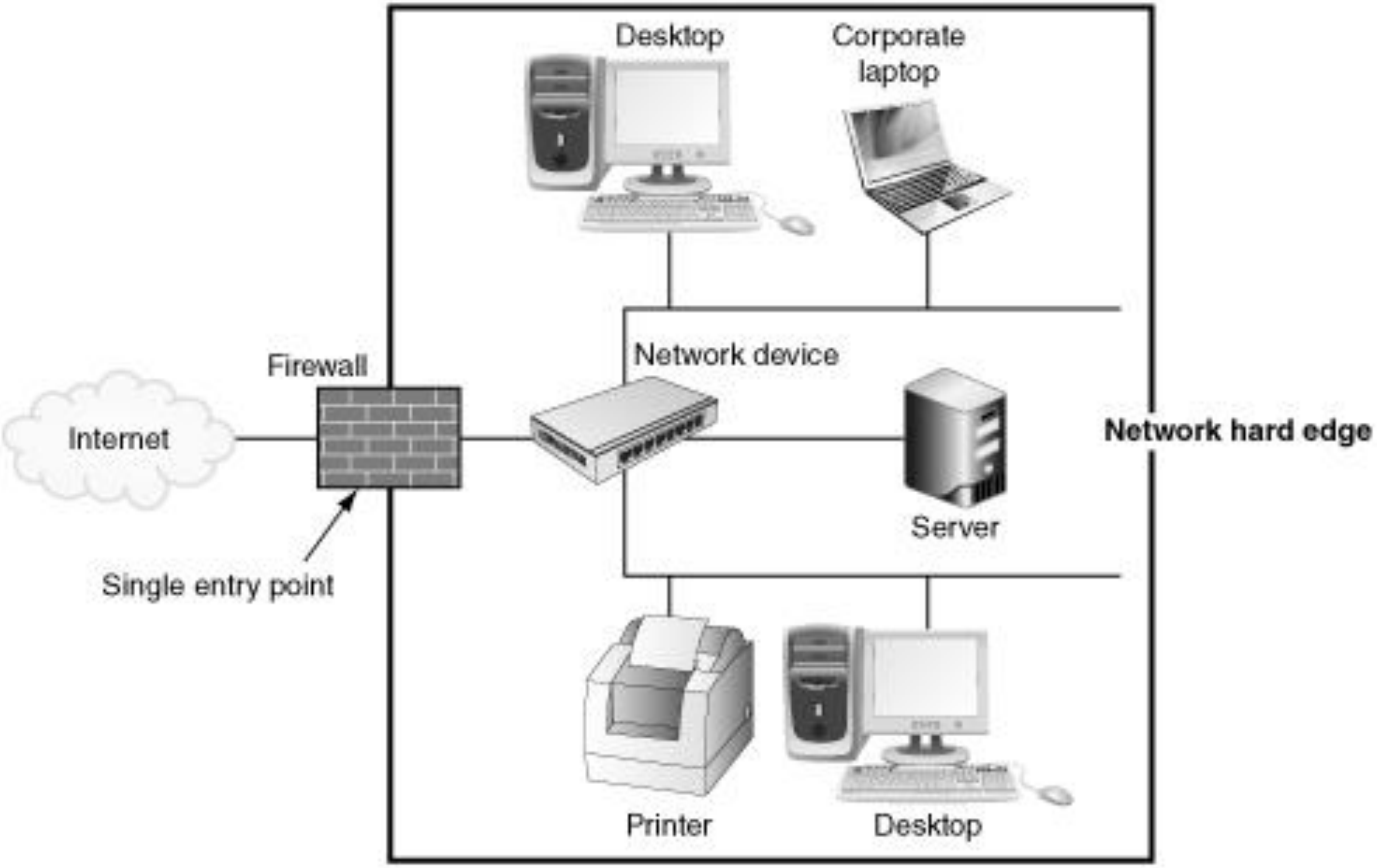
- **Security**
  - Radio Environment (antennas on parking lots)
  - SSID (Service Set Identifier)
    - ***Non-broadcast Mode***
    - ***Change from default***
    - ***Differentiates one WLAN from another***
    - ***32-character ID attached to the header of Packets ("Sniffable")***
  - WEP - Wired Equivalent Privacy
    - ***"Crackable"***
    - ***Key Renewal Cycle (Dictionary Attack)***
    - ***Only Secures the "Wireless Part" (Man in the Middle)***
  - WPA – Wi-Fi protected Access
    - ***WPA2***
  - MAC Filtering
    - ***Administration Overhead***
    - ***Sniff and Change MAC***

Wireless Attacks

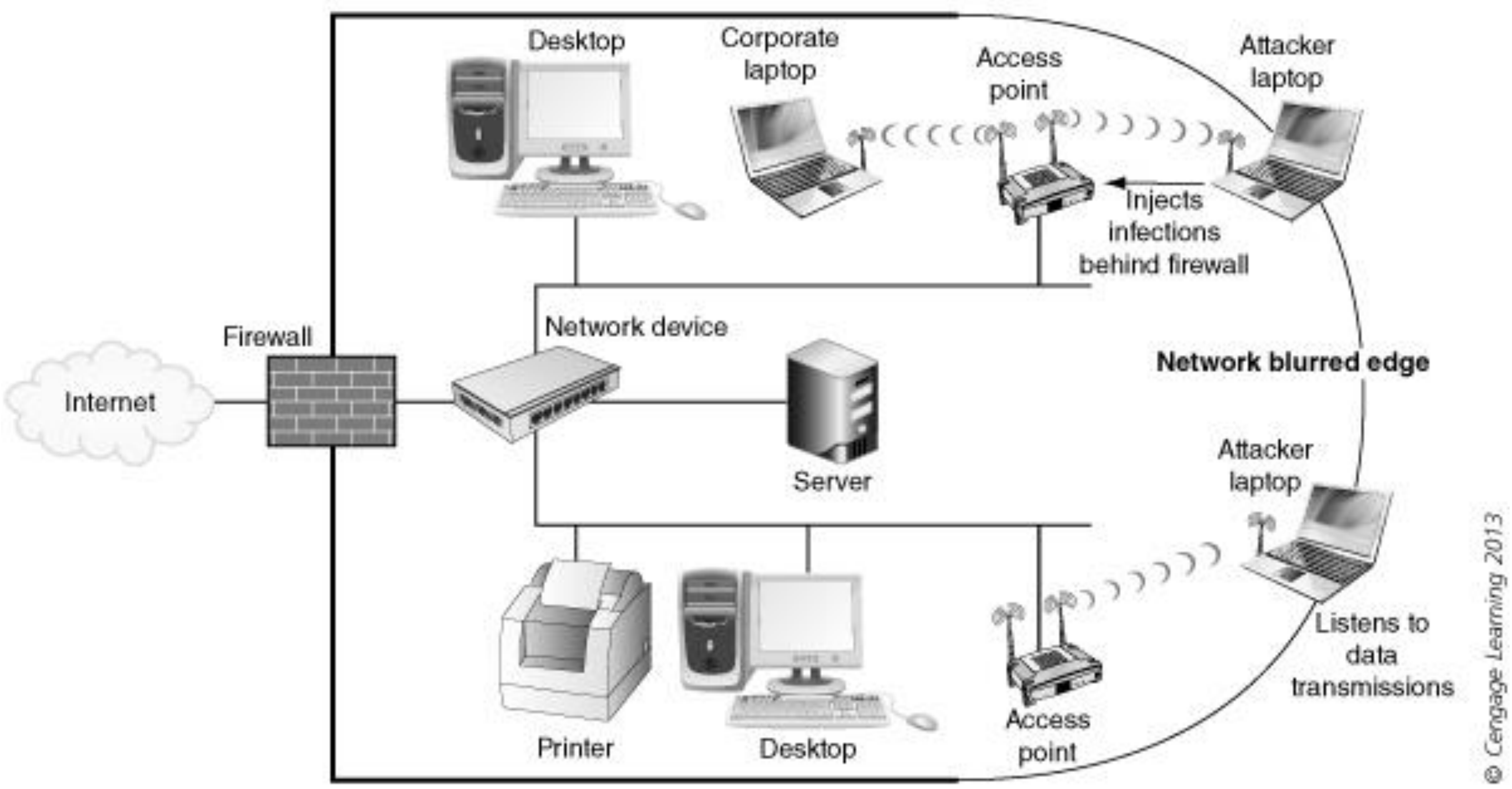
- **Attacks can be divided into three categories:**
  - – Attacks against enterprise organizations
  - – Attacks against mobile users
  - – Attacks against home users

Enterprise Attacks

- **Attack Vectors: paths that can be exploited**
  - “*Hard edge*”: well-defined boundary
  - Single entry point onto the network plus security devices that can defend it (firewall) make up a network’s hard edge
  - Physical hard edge will help keep out unauthorized personnel so that attackers cannot physically access devices
  - Introduction of wireless LANs in enterprises has changed hard edges to “blurred edges”



© Cengage Learning 2013



© Cengage Learning 2013

Enterprise Attacks

- **A wireless device may create multiple enterprise attack vectors:**
  - *Open or misconfigured AP*
  - *Rogue AP*: an employee may bring a device from home and connect it to the network
  - *Evil twin*: an AP that is set up by an attacker

Enterprise Attacks

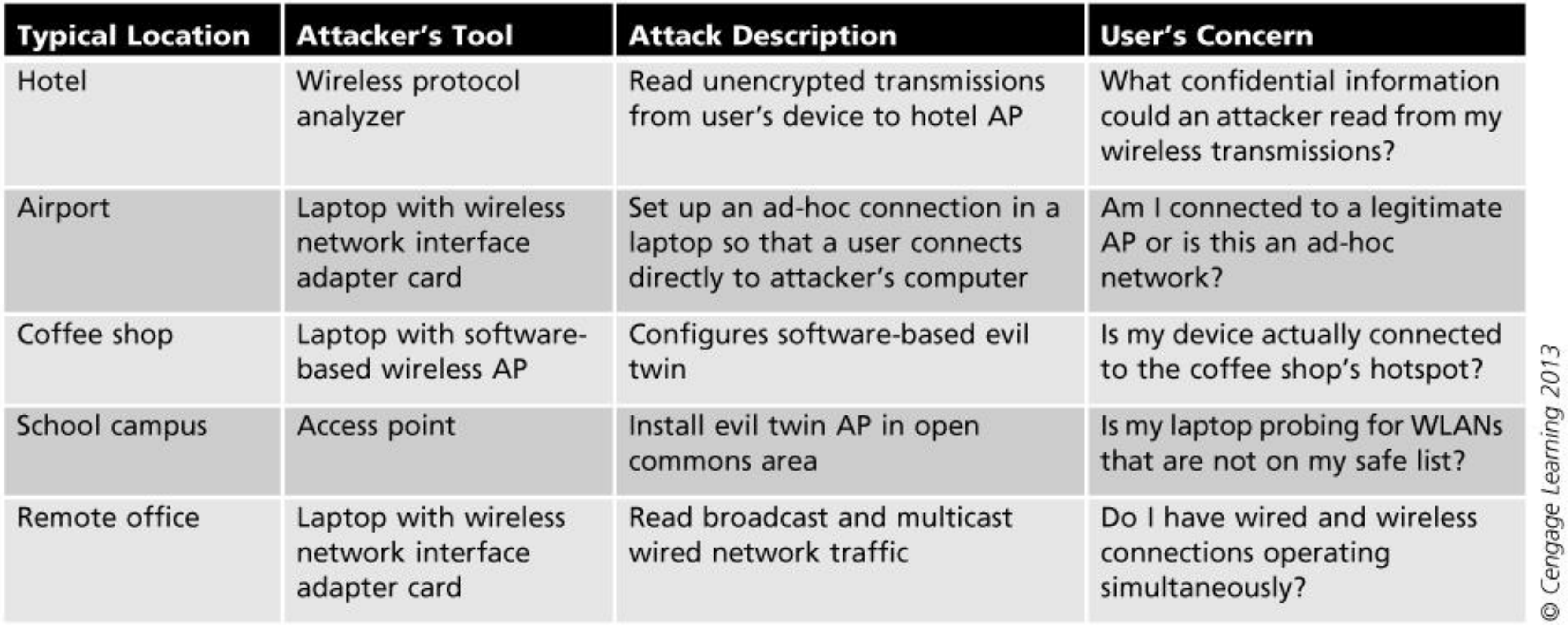
- **Wireless Enterprise Attacks:**
  - **Reading Data**: attacker can pick up the RF signal from an open or misconfigured AP and read any confidential wireless transmissions and other traffic
  - **Hijacking Wireless Connections**: an attacker can trick a corporate mobile device to connect the imposter device instead
    - ***Man-in-the-middle attack: makes it appear that the wireless device and the network computers are communicating with each other, when actually they are sending and receiving data with an evil twin AP between them***

MITM

Enterprise Attacks

- **Wireless Enterprise Attacks (continued):**
  - **Inserting Network Traffic**: injecting wireless packets into a network in order to redirect traffic to an attacker’s server
  - **Denial of Service (DoS)**: attempts to prevent a device from performing its normal functions
    - ***An attacker can flood network with RF signal noise (called RF jamming)***
    - ***An attacker can create a fictitious frame that pretends to come from a trusted client***
    - ***Manipulating duration field values to a high number thus preventing other devices from transmitting for a long period of time***

Mobile User Attacks



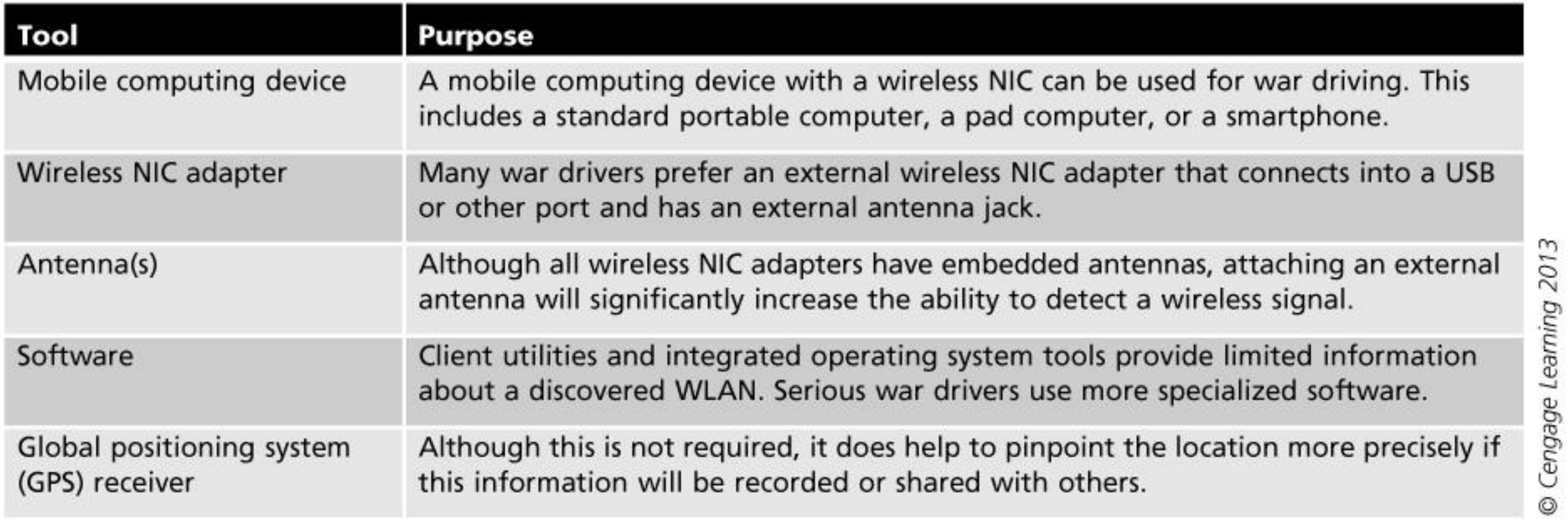
Typical Location	Attacker's Tool	Attack Description	User's Concern
Hotel	Wireless protocol analyzer	Read unencrypted transmissions from user's device to hotel AP	What confidential information could an attacker read from my wireless transmissions?
Airport	Laptop with wireless network interface adapter card	Set up an ad-hoc connection in a laptop so that a user connects directly to attacker's computer	Am I connected to a legitimate AP or is this an ad-hoc network?
Coffee shop	Laptop with software-based wireless AP	Configures software-based evil twin	Is my device actually connected to the coffee shop's hotspot?
School campus	Access point	Install evil twin AP in open commons area	Is my laptop probing for WLANs that are not on my safe list?
Remote office	Laptop with wireless network interface adapter card	Read broadcast and multicast wired network traffic	Do I have wired and wireless connections operating simultaneously?

Home Attacks

- **Attacks against home WLANs are usually easy**
  - Most home users fail to configure any security

- **Attackers can:**
  - *Steal data*
  - *Read wireless transmissions*: usernames, passwords, credit card numbers
  - *Inject malware*
  - *Download harmful content*

- **War driving: searching for wireless signals from an automobile or on foot using a portable computer**



Tool	Purpose
Mobile computing device	A mobile computing device with a wireless NIC can be used for war driving. This includes a standard portable computer, a pad computer, or a smartphone.
Wireless NIC adapter	Many war drivers prefer an external wireless NIC adapter that connects into a USB or other port and has an external antenna jack.
Antenna(s)	Although all wireless NIC adapters have embedded antennas, attaching an external antenna will significantly increase the ability to detect a wireless signal.
Software	Client utilities and integrated operating system tools provide limited information about a discovered WLAN. Serious war drivers use more specialized software.
Global positioning system (GPS) receiver	Although this is not required, it does help to pinpoint the location more precisely if this information will be recorded or shared with others.

Wireless LAN Security Threats

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network *The weakness is another reminder of the difficulty in implementing effective network security.*	

Mitigating the Threats

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Prevention System (IPS)
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Access Control

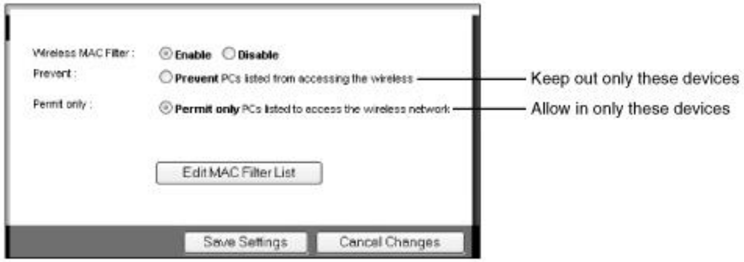
- **Access Control: granting or denying approval to use specific resources**

- **Wireless access control: Limit user’s admission to AP**

- **Media Access Control (MAC) address filtering: Based on a node’s unique MAC address**

Access Control

- **MAC address filtering considered to be a basic means of controlling access**
- **Restrictions can be implemented in one of two ways:**
  - A specific device can be permitted or the device can be blocked



Wireless MAC Filter : ● Enable ○ Disable

Prevent : ○ **Prevent** PCs listed from accessing the wireless

Permit only : ● **Permit only** PCs listed to access the wireless network

Keep out only these devices

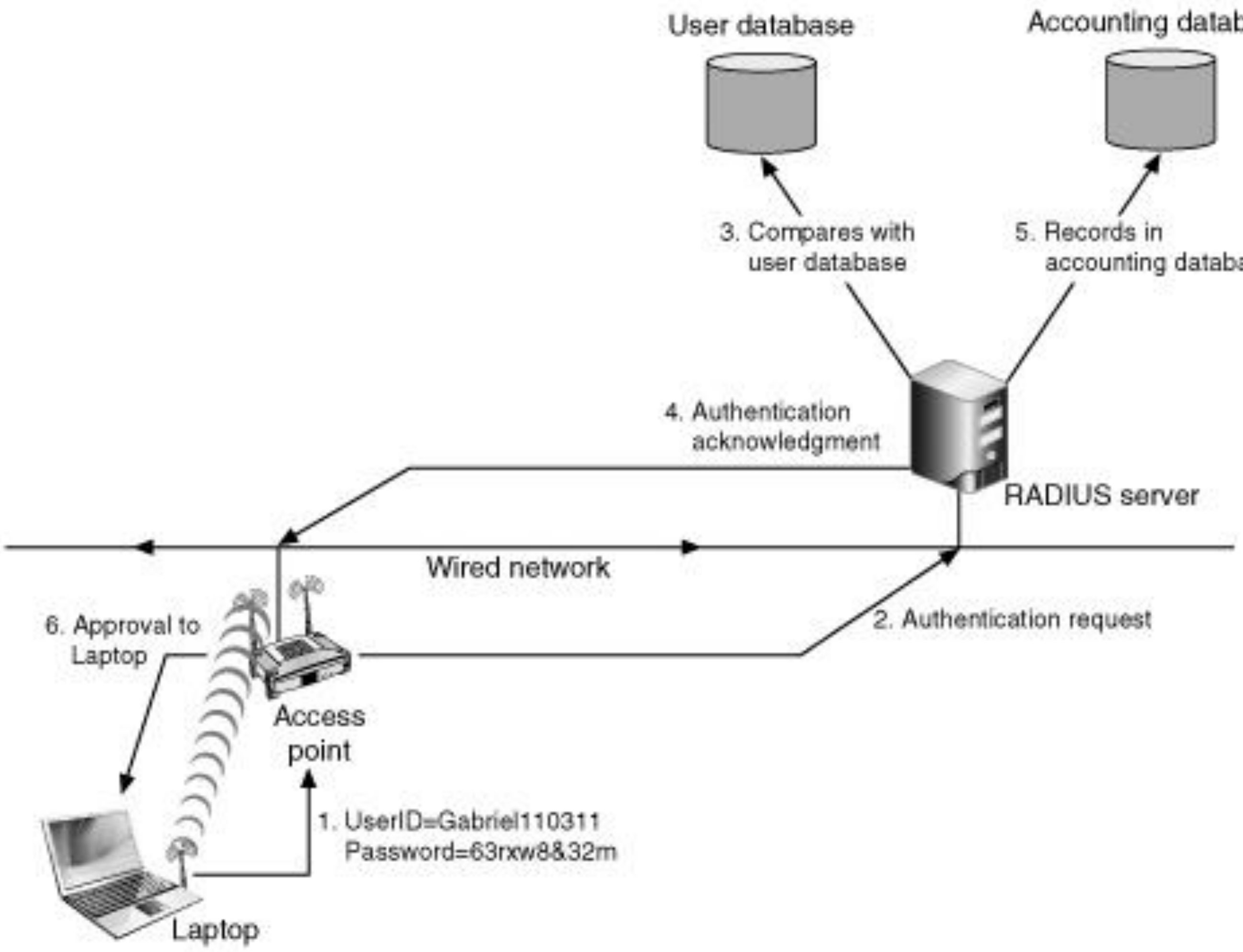
Allow in only these devices

© Cengage Learning 2013

Authentication

- **IEEE 802.11i/WPA2 authentication and key management is accomplished by IEEE 802.1X standard**
  - Implements **port security**
    - ***Blocks all traffic on port-by-port basis until client authenticated using credentials stored on authentication server***

- **802.11X is often used in conjunction with Remote Authentication Dial In User Service (RADIUS)**
  - Suitable for "high-volume service control applications"


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgment
RADIUS server
Wired network
2. Authentication request
6. Approval to Laptop
Access point
1. UserID=Gabriel110311 Password=63rxw8&32m
Laptop

© Cengage Learning 2013

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

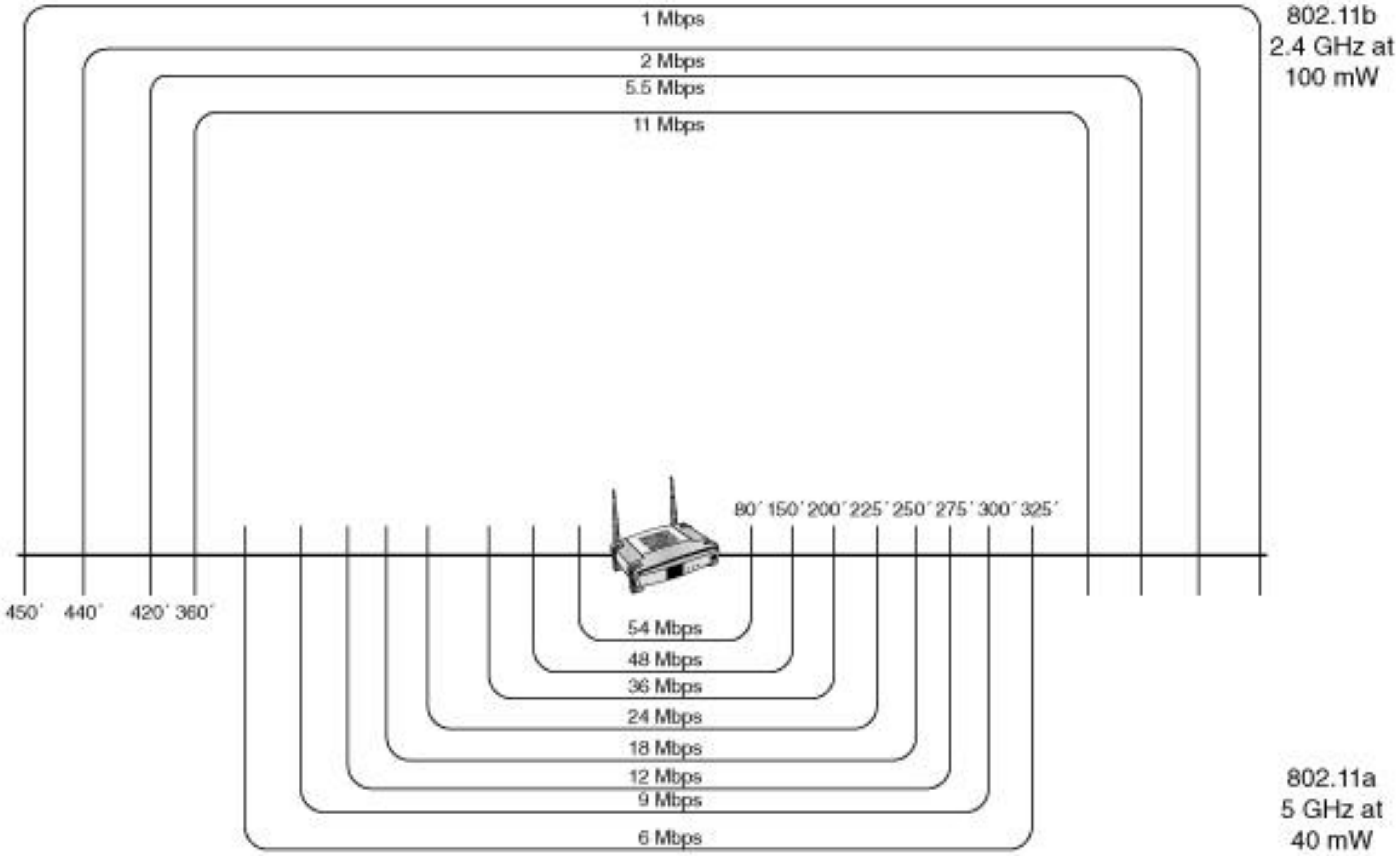
WLAN Configuration

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

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



© Cengage Learning 2013

System Throughput Problems

- **Many factors influence WLAN transmission speed (continued):**
  - Request to send/clear to send (RTS/CTS) protocol
  - Types of RF interference

- **To troubleshoot:**
  - New install or has anything changed?
  - 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

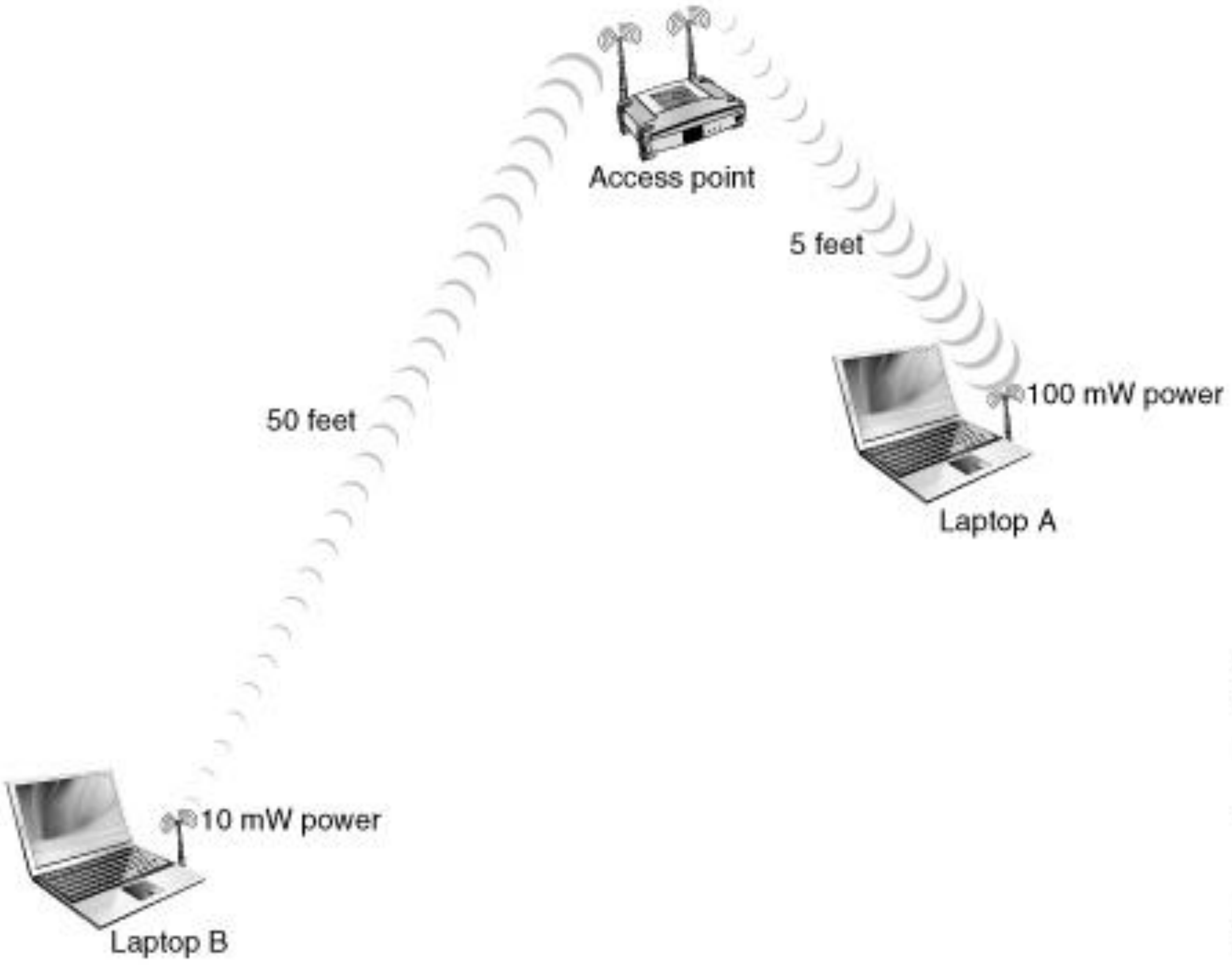
Wireless Device Troubleshooting

- **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

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

POE

- **Power over Ethernet**
  - Power IP phones or wireless AP’s using the same Ethernet cabling
  - Since copper Ethernet can reach 100 meters, POE must do so as well
  - 15Watts
  - 803.af & Cisco inline power
  - Use same pairs 1,2 3,6 or 4,5 7,8
  - Resistor between powered pairs at receiver indicate compatibility, change resistance value to indicate voltage.

  - Must have port available on the switch!

Questions?