Wireless LANs

Panko Chapter 6 and Chapter 7

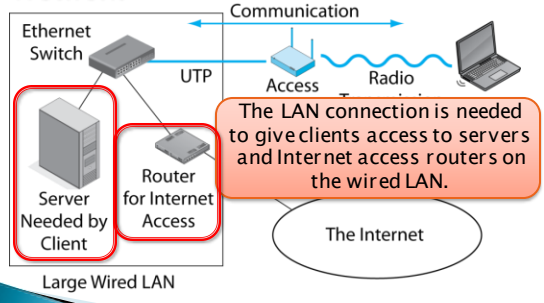
Panko and Panko
Business Data Networks and Security, 10th Edition, Global Edition

- Introduction
- Radio Signal Propagation
- Radio Bands and Bandwidth
- Spread Spectrum Transmission
- 802.11 WLAN Operation
- 802.11 Transmission Standards
- Wireless Mesh Networking

6.1 802.11/Wi-Fi WLAN Technology

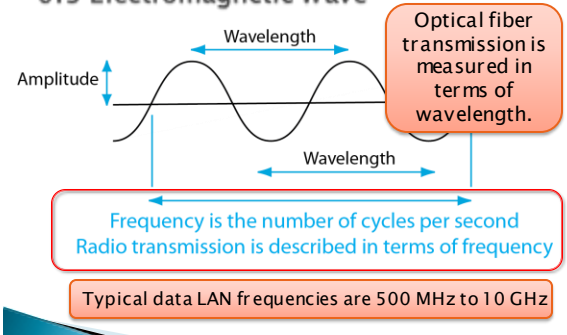
- 802.11 Wireless LAN Technology
  - The dominant WLAN technology today
  - Standardized by the 802.11 Working Group of the IEEE 802 Committee

6.2 Hybrid Switched/Wireless 802.11 Network

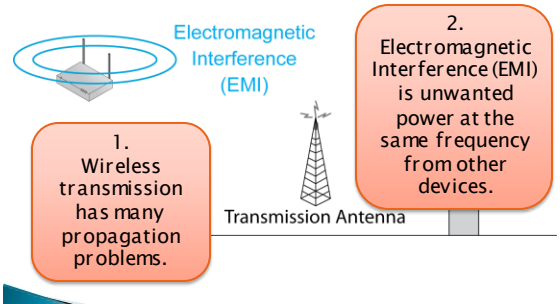


- Introduction
- Radio Signal Propagation
- Radio Bands and Bandwidth
- Spread Spectrum Transmission
- 802.11 WLAN Operation
- 802.11 Transmission Standards
- Wireless Mesh Networking

6.3 Electromagnetic Wave



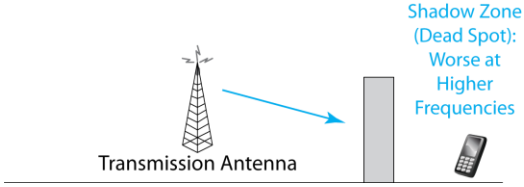
6.5: Wireless Propagation Problems



1. Wireless transmission has many propagation problems.

2. Electromagnetic Interference (EMI) is unwanted power at the same frequency from other devices.

6.5: Wireless Propagation Problems



Shadow zones are places the signal cannot penetrate because of obstacles in its path.

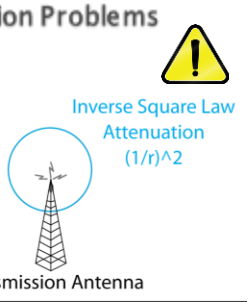
Shadow zones, also called dead spots, grow worse as frequency increases.

6.5: Wireless Propagation Problems

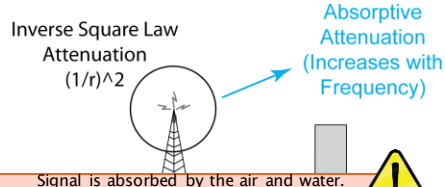
The signal strength spreads out as the surface of a sphere.

This means that its strength falls as $(1/r^2)$, where r is the radius.

If you double the distance, you only get ¼ the signal strength



6.5: Wireless Propagation Problems

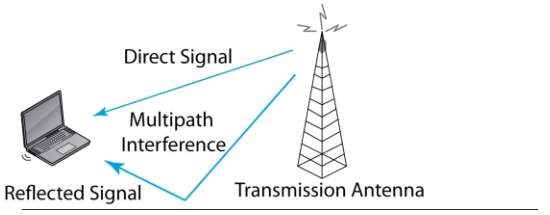


Signal is absorbed by the air and water.
e.g. bathrooms, plants, people

Note that there are two types of attenuation: Inverse square law and absorptive attenuation.

Note that this is different to shadow zones.

6.5: Wireless Propagation Problems

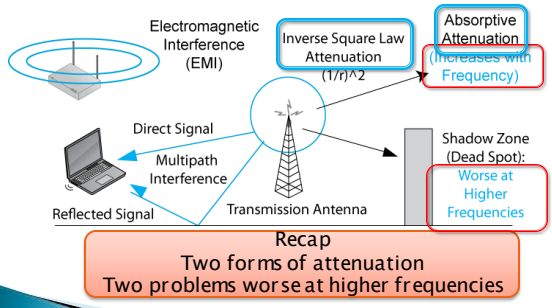


Direct and reflected signals may interfere.
Most serious propagation problem at WLAN frequencies.

Q:

- Who solved the multipath interference problem for WLAN frequencies?

6.5: Wireless Propagation Problems



Recap
Two forms of attenuation
Two problems worse at higher frequencies

6.8 Frequency Spectrum, Service Band, Channels

Frequency Spectrum

The frequency spectrum is all possible frequencies from 0 Hz to infinity.

0 Hz

6.8 Frequency Spectrum, Service Band, Channels

Service Band

The frequency spectrum is divided into blocks of fequencies called service bands.

Service bands are dedicated to individual services:

- Broadcast television
- FM Radio
- Emergency services
- GPS
- Cellular telephony
- etc.

6.8 Frequency Spectrum, Service Band, Channels

Service Band

- Channel 5
- Channel 4
- Channel 3
- Channel 2
- Channel 1

Each service band is divided into channels.

A signal is sent in a single channel (for instance, a television channel).

Signals sent in different channels do not interfere with one another.

6.10: Channel Bandwidth and Transmission Speed

- Channel Bandwidth
  - Channel bandwidth is the highest frequency in a channel minus the lowest frequency.
  - An 88.0 MHz to 88.2 MHz channel has a bandwidth of 0.2 MHz (200 kHz).
  - Higher-speed signals need wider channel bandwidths.
  - Multiply bandwidth by N can multiply transmission speed by N

6.10 Channel Bandwidth and Transmission Speed

- Broadband Channels
  - Broadband means wide radio channel bandwidth and therefore high speed
  - Popularly, fast systems are called "broadband" even if they are not radio systems

6.11 2.4 GHz and 5 GHz Service Band

- The 2.4 GHz Service Band
  - 2.4 GHz to 2.485 GHz
  - Propagation characteristics are good
  - For 20 MHz wide 802.11 channels, only three nonoverlapping channels are possible
  - Channels 1, 6, and 11

6.11 2.4 GHz and 5 GHz Service Band

- The 2.4 GHz Service Band
  - Co-channel interference between nearby access points transmitting in the same channel degrades performance
  - Except in very small networks, difficult or impossible to put nearby access points on different channels (Figure 6-12)

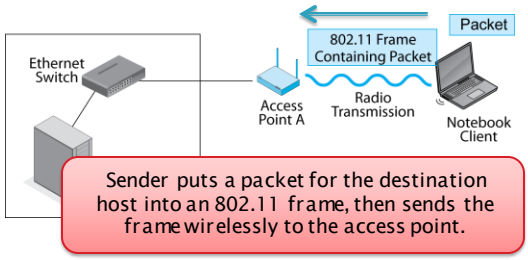
6.11 2.4 GHz and 5 GHz Service Band

- The 5 GHz Service Band
  - More bandwidth, so between 11 and 24 non-overlapping 20 MHz channels
  - Makes it easy to have nearby access points operate on non-overlapping channels
  - Increasing channel bandwidth in newer standards reduces the number of possible channels

6.11 2.4 GHz and 5 GHz Service Band

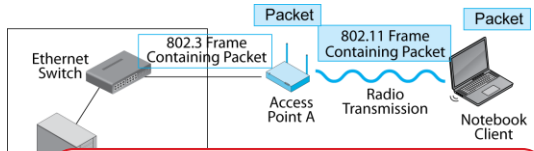
- What is the main advantage of 2.4 GHz operation?
- What is the main advantage of 5 GHz operation?

6.16 Typical 802.11 Wi-Fi Operation



Sender puts a packet for the destination host into an 802.11 frame, then sends the frame wirelessly to the access point.

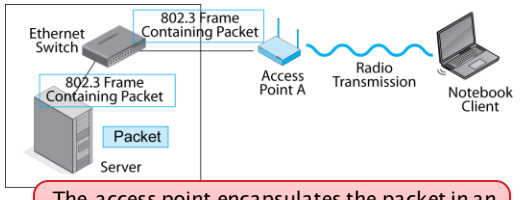
6.16 Typical 802.11 Wi-Fi Operation



The 802.11 frame has the wrong frame format to travel over an 802.3 Ethernet network. The switches and destination host would not know what to do with it.

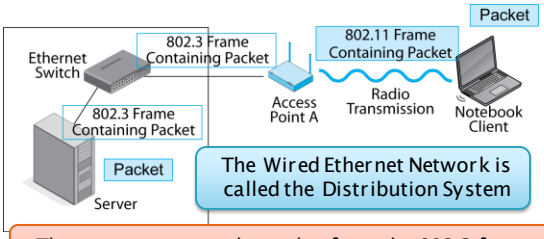
The access point removes the packet from the 802.11 frame and discards the frame.

6.16 Typical 802.11 Wi-Fi Operation



The access point encapsulates the packet in an 802.3 frame and sends this frame on to the destination host via Ethernet switches.

6.16 Typical 802.11 Wi-Fi Operation



The Wired Ethernet Network is called the Distribution System

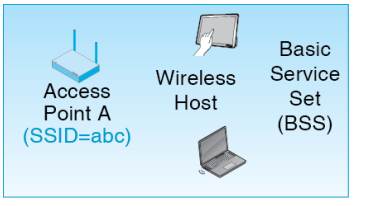
The server removes the packet from the 802.3 frame.

6.16 Typical 802.11 Wi-Fi Operation

- Does the IP packet travel all the way to the destination host?
- Does the 802.11 frame travel all the way to the destination host? Why or why not?

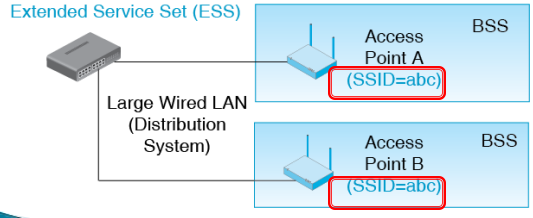
6-17: Basic Service Set (BSS)

- An access point and its wireless hosts
- Service Set ID (SSID) is the name of the network (abc)



6-17: Extended Service Set (ESS)

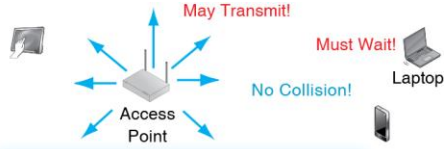
- Collection of access points that all have the same SSID
- "Handoff" to another AP is also called "roaming": 802.11r



6.18: Transmitting in a Single Channel

Channel Sharing:
The access point and all the hosts it serves transmit in a single channel. If two devices transmit at the same time, their signals will collide, becoming unreadable.

6.18: Transmitting in a Single Channel



Media Access Control (MAC)
MAC methods govern when devices transmit so that only one device transmits at a time.

Comparison Box

- CSMA/CA+ACK is Mandatory
  - Carrier Sense Multiple Access/Collision Avoidance+Acknowledgement
  - It is the default MAC method.
  - It is more efficient than RTS/CTS.
  - Is includes and "ACK" and so is reliable
- RTS/CTS
  - Is optional alternative.

6.21 Major 802.11 Wi-Fi Standards

Standard	Rated Speed
802.11g	54 Mbps; **obsolete** but used
802.11a	54 Mbps; **obsolete** but used
802.11n	100 to 600 Mbps 150 to 300 Mbps common; **dominant use**
802.11ac	433 Mbps to 6.93 Gbps 433 to 1.3 Gbps common; **dominant sales**

6.21 Major 802.11 Wi-Fi Standards

Standard	MIMO?	Maximum Spatial Streams	MU-MIMO?
802.1g	No	NA	No
802.11a	No	NA	No
802.1n	Yes	4	No
802.1ac	Yes	8	Yes

6.24 Speed, Distance, and Throughput

- Rated Speed versus Throughput
  - Rated speed is the speed the standard specifies
  - Throughput is the speed that is actually delivered
  - Total throughput is substantially lower than rated speed—sometimes 50% lower
  - Access point throughput is aggregate throughput for all devices transmitting and receiving
  - Speed drops with modulation methods to reduce errors at distance
  - So device throughput may be 25%

6.25 Backward Compatibility

- Devices Built for Newer Standards Still Implement Older Standards
  - This is called backward compatibility
  - This Allows Older and Newer Devices to Communicate

Chapter 7

- Introduction
- 802.11i LAN Security
- 802.11i Security is Not Enough
- 802.11 Wi-Fi WLAN Management
- Decibels
- Bluetooth
- Other Local Wireless Technologies

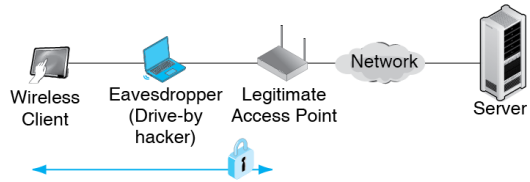
- The TJX Breach
- **Introduction**
- 802.11i LAN Security
- 802.11i Security is Not Enough
- 802.11 Wi-Fi WLAN Management
- Decibels
- Bluetooth
- Other Local Wireless Technologies

7.1 Wireless LAN Security Threats

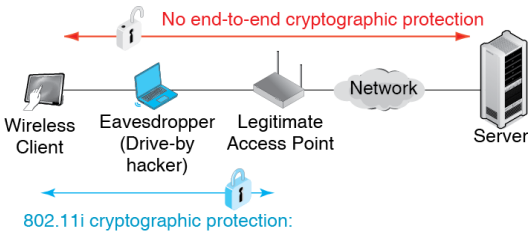
War Drivers (??)	Drive-By Hackers
Lurk Outside Building	Lurk Outside Building
Collect Access Point Data SSID, strength of signal, security	Collect Access Point Data SSID, strength of signal, security
May publicize findings Do not read messages Do not send attacks	Read messages Send attacks that bypass the firewall
Legal: Used for localization services!	Illegal

- The TJX Breach
- Introduction
- 802.11i LAN Security
- 802.11i Security is Not Enough
- 802.11 Wi-Fi WLAN Management
- Decibels
- Bluetooth
- Other Local Wireless Technologies

7.2 Scope of 802.11i Security Protection



7.2 Scope of 802.11i Security Protection



7.3 802.11i Security

- 802.11i Provides Security between the Wireless Host and the Wireless Access Point
  - Initial authentication
  - Encryption of messages for confidentiality, authentication, and message integrity
  - Uses strong cryptographic standards, including AES for encryption for confidentiality

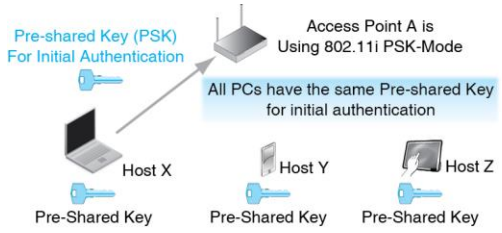
7.3 802.11i Security

- Configuring an Access Point
  - Select 802.11i (sometimes called **WPA2**)
  - Do not select Wireless Protected Access (WPA), an earlier, weaker security standard created by the Wi-Fi Alliance
  - **Never ever** select Wired Equivalent Privacy (WEP), an earlier security standard created by the 802.11 Working Group
  - Earlier standards do not provide acceptable security

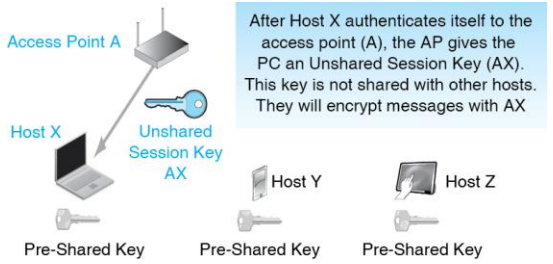
7.4 802.11i Modes of Operation

	Pre-Shared Key (PSK) Mode	802.1X Mode
Environment	Home, Business with a single access point	Companies with multiple access points
Uses a Central Authentication Server?	No	Yes
Authentication	Knowledge of Pre-Shared Key	Credentials on authentication server
Technical Security	Strong	Very Strong
Human Security	Vulnerable	Very Strong

7.5 802.11i PSK Mode: Initial Authentication



7.6 802.11i PSK Mode: Unshared Session Key



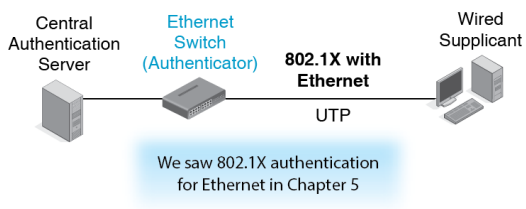
7.7 Security Threats in 802.11i PSK Mode

- Someone may give the PSK to unauthorized people
  - It does not seem secret, so employees tend to share it
- PSKs are generated from passphrases
  - Passphrases must be at least 20 characters long
- Wireless Protected Setup (WPS)
  - Created by Wi-Fi Alliance to make PSK setup easier
  - User enters an 8-digit PIN for a particular access point
  - Unfortunately, easily cracked and should be turned off on the access point if possible

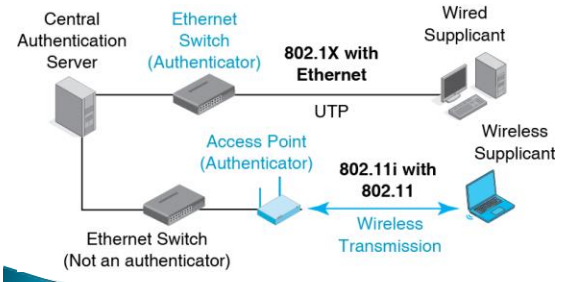
Question?

- Does WPA2/PSK use symmetric or asymmetric encryption over the wireless link?

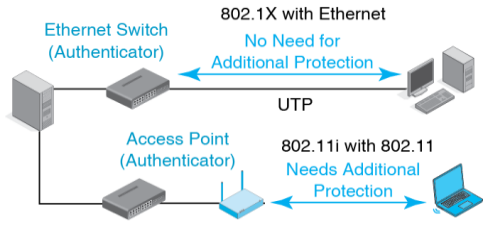
7-8: 802.11i in 802.1X mode



7-8: 802.11i in 802.1X mode



7-8: 802.11i in 802.1X mode



802.1X requires a confidential client-authenticator link
Not a problem with UTP, big problem with wireless

7-8: 802.11i in 802.1X mode

- Create an SSL/TLS VPN between the access point/authenticator and the client/supplicant
- This will protect the confidentiality of subsequent 802.1X message exchanges
- The most popular standard for using SSL/TLS with 802.1X is the PEAP standard.

Bluetooth

- Created for relatively low-speed transmission over small distances
- Cable replacement technology for devices around your body or desk
- Not a full WLAN technology
- Classic Bluetooth gives only about 3 Mbps, but gives a long battery life

7.20 Bluetooth Modes of Operation

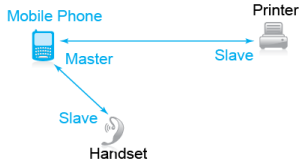
Operating Mode	Classic Bluetooth	High-Speed Bluetooth Uses a 2nd 802.11 radio!
Principal Benefit	Decent speed at low power (Long battery life)	High-Speed transfers available when needed. Longer distance.
Speed	Up to 3 Mbps	Up to about 24 Mbps
Expected Duty Cycle	Low to High	Low (only use occasionally)
Power Required	Low	High
Maximum Distance	About 10 m	About 30 m

7.14: Bluetooth Operation

All Bluetooth connections are one-to-one connections

A master and its slaves is called, collectively, a piconet.

A master may have up to 7 slaves, so a piconet may have up to 8 devices.



7.22 Bluetooth Profiles

- Bluetooth Profiles
  - Specify how devices will work together for different applications
  - Nothing like this in 802.11 Wi-Fi
  - Includes Headset, Hands-free, Basic Printing, Synchronisation

- The TJX Breach
- Introduction
- 802.11i LAN Security
- 802.11i Security is Not Enough
- 802.11 Wi-Fi WLAN Management
- Decibels
- Bluetooth
- **Other Local Wireless Technologies**

7-23 Near Field Communication (NFC)

- For Very Small Distances and Low Speed
  - Up to 4 cm (about 2 inches)
  - Limited to 424 kbps
  - So uses very little battery power
- Operation in the 13.56 kHz Band
  - Dedicated for this use
  - Also gives low power consumption

7-23 Near Field Communication (NFC)

- Sample Applications
  - Payment of bus fares (already popular in some countries)
  - Unlocking car doors and turning on the ignition
  - Building door entry control
  - Sharing electronic business cards and other files between mobile devices
  - Retail payments, including loyalty points and coupons (beginning to be popular)

7-23 Near Field Communication (NFC)

- Passive Radio Frequency ID (RFID) Tags
  - Goal: to replace bar codes
  - Tags are electronic but have no power source
  - When scanned by a reader, use power of the scan to generate a reply
  - Inexpensive compared to powered devices
  - Can only send a small amount of information
  - Cannot do encryption