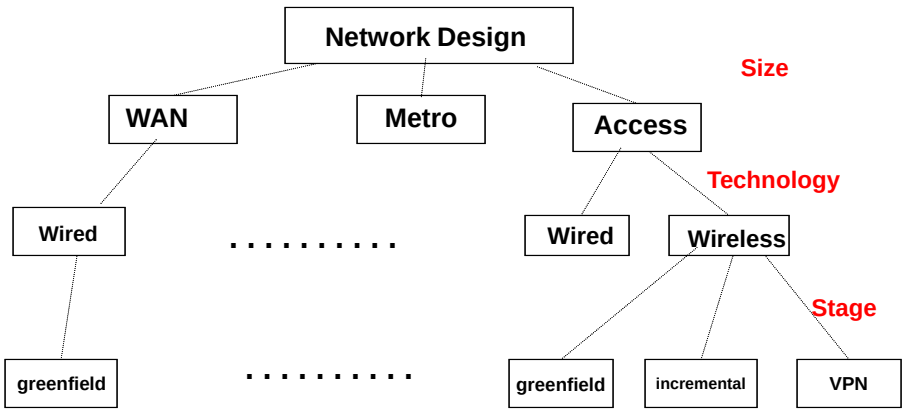
Wireless Technology in Access Networks

David Tipper
Associate Professor
Graduate Telecommunications and Networking Program
University of Pittsburgh
Slides 7

Network Design Categories

- Remember network design classifications



Techniques used to design the network will depend on the classification
Consider *Access Network Design* *wireless* for the greenfield case

Wireless in Access Networks

- Increasing use of wireless technology in access networks
  - IEEE 802.11 technology for Wireless LANS and last mile and wireless mesh networks
  - IEEE 802.16 WiMAX for MANs and last mile
  - Cellular Technology (3G, 3.5G, 4G) for mobile telephony and last mile
  - Free Space Optical for short line of sight high bandwidth connections
  - Microwave for point-to-point longer distance line of sight – high bandwidth connections
  - Proprietary solutions for wireless multi-hop mesh networks (based on 802.11 or WiMAX)
  - Variety of Speeds, Cost, Coverage Range, etc.

Why Wireless in Access Networks?

- **Two Applications**

1. Cable Replacement

- **Cheaper than wiring**
- **Example: Point to Point Microwave Link**

2. Last Hop Connectivity

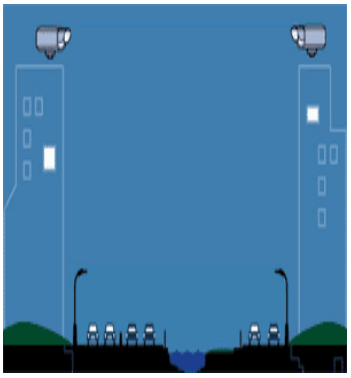
- **Link between end user/host and network is wireless – usually shared by *multiple users***
- **Normally thought of as wireless access network (Example: WLAN, cellular network)**
- **Can provide user *Mobility***
- **Cost Advantages**
- **Flexibility – ease of deployment**

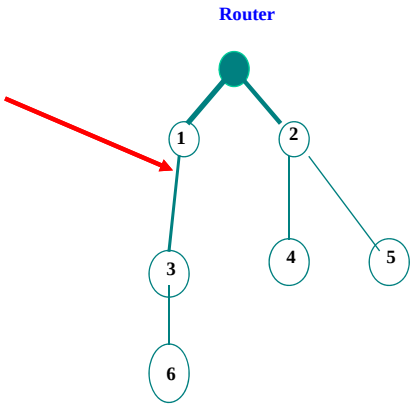
Wireless Issues

- **Wireless link implications**
  - *communications channel* is the air
    - poor quality: fading, shadowing, weather, etc.
  - *Spectrum regulated* by governments
    - frequency allocated, licensed vs. unlicensed, etc.
  - *limited bandwidth*
    - Low bit rate, frequency planning and reuse, interference
  - *power issues*
    - Power levels regulated (safety issues), conserve mobile terminal battery life
  - *security issues*
    - wireless channel is a *broadcast* medium!
    - Signal easy to intercept

Wireless for Cable Replacement

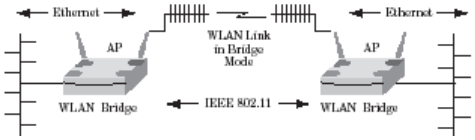
- Cable Replacement
  - Essentially using wireless link in a point-to-point fashion.
  - Typically used when too expensive to use wired cables
    - Cross a river, highway, valley, etc.
  - Basically just another technology option in *standard access network* design

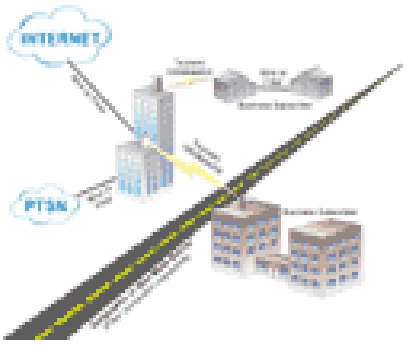




Cable Replacement

- Wireless Link Issues
  - Distance
  - Line of Sight vs. Non-Line of Sight
  - Atmospheric Effects
  - Security
  - Cost
  - Spectrum: Licensed vs. Unlicensed
  - Layer 2 interface
- In general a lower quality link then wired
  - Higher Bit Error Rate
  - Lower Availability
  - → user higher bandwidth then needed!





Cable Replacement

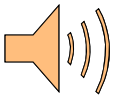
- Various Technologies available for use as cable replacement.
  - Short distances (~10M)
    - Bluetooth, IEEE 802.15, Zigbee, etc.
      - Sensors to hub, wireless access to printer, etc.
      - Unlicensed spectrum – NLOS and LOS operation
      - Data rate 10's kbps to 1Mbps
  - Medium Distances 10M-3KM
    - 802.11 (a,b,g,n),
      - 100-250M NLOS –1-5KM LOS focused antenna
      - Unlicensed spectrum
      - Data rates 1Mbps – 108Mbps
    - 802.16 (WiMAX)
      - 3-5 Km NLOS- LOS-15-30KM
      - Licensed Spectrum
      - Data rates 1-75Mbps
    - Free Space Optical
      - High data rates (100 Mbps -2.5Gbps) over short distances
      - Unlicensed, uses infrared lasers
      - LOS *required* – severely effected by weather

Cable Replacement

- Longer Distances
  - LMDS (Local Multipoint Distribution Systems)
    - Bulk of deployment focused on backhaul extension of fiber infrastructure and cellular networks
    - Operates in 28, 29 GHz spectrum
    - Range 1.5-5 miles, weather effects (500 Mbps)
  - MMDS (Multipoint Microwave Distribution Systems)
    - Operates in 2.5-2.7MHz licensed spectrum
    - Originally intended for wireless cable TV distribution
    - 20MHz spectrum → 99 10Mbps channels
    - Range ~25Km (LOS and NLOS possible)
    - Data rates ~ .5-1 Mbps on 10Mbps channel
    - Being Replaced by licensed WIMAX 802.16
  - Point to Point Microwave
    - Licensed in various bands – range up to 30Miles

How to Design Wireless Link?

- Cable Replacement Design
  1. Determine physical sites to be connected and characteristics
     - Distance, propagation environment (LOS vs. NLOS), electricity availability, physical security, etc.
  2. Determine potential frequency and equipment values
     - Licensed vs. unlicensed, interference, etc.
     - Transmit power range and receiver signal strength requirements
     - Antennas and gains, etc.
  3. Predict amount of signal lost along the path from transmitter to signal using path loss model
     - Include any weather/NLOS shadowing effects (if necessary)
     - Rule of thumb want at least 10 db System Margin
       That is received signal 10 db greater than receiver sensitivity
       System Margin = Signal Strength at Receiver – Receiver Sensitivity Threshold
  4. Evaluate *Link Budget* to ensure sufficient signal strength for desired data rate – may need to repeat 1-3 if exceed link budget
  5. Deploy trial setup and take measurements to verify design



Background

- Signal strength is expressed in decibels (dB) for ease of calculation
  - Values relative to 1 mW are expressed in dBm
  - Values relative to 1 W are expressed in dBW
  - Other values are simply expressed in dB
- Example : Express 2 W in dBm and dBW
  - dBm: 10 $\log_{10}$ (2 W / 1 mW) = 10 $\log_{10}$(2000) = 33 dBm
  - dBW: 10 $\log_{10}$ (2 W / 1 W) = 10 $\log_{10}$(2) = 3 dBW
- In general dBm value = 30 + dBW value
- Note 3 dB implies doubling/halving power
- Equipment Transmit Power, Antenna Gains, Receiver Sensitivity are expressed in W, dBW, and dBm,

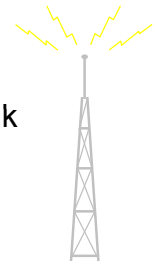
Example

- IEEE 802.11B WLan Equipment (2.4 GHz)
  - Transmit Power
    - For 802.11b in North America the possible power levels for Access Points (AP) in dBm are {24, 20, 17, 15, 13, 7, 0}
  - Antenna Gains
    - Omni-directional
      - Integrated antennas 1-3 Db
    - Directional antennas
      - Restrict coverage area –but higher gain 6-24 db

  - Receiver Sensitivity Threshold (RST)
    - For 802.11b equipment RST depends on equipment manufacturer Typical values are RSS > -80dBm for the maximum data rate.
    - Note as *signal decreases data rate goes down*
    - For example 802.11b equipment at a RSS > -80dBm get 11Mbps at -83 dBm < RSS < -80 dBm get 5.5Mbps, -85 db > RSS > -92 dBm 1 Mbps, etc.

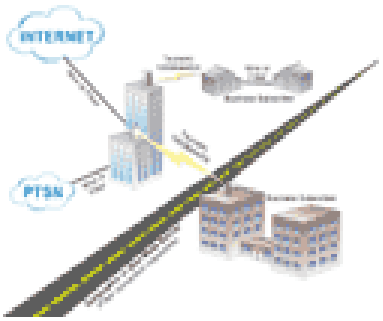
Link Budget

- Used to plan useful radio strength of link and coverage
  - Relates transmit power, path losses, margins, interference, etc.
  - Used to find max allowable path loss on each link
  - Typical Factors in Link Budget
    - Transmit Power,
    - Antenna Gain, Diversity Gain,
    - Receiver Sensitivity
    - Shadow Margin, Interference Margin, ➔ lumped into System Margin
    - Vehicle Penetration Loss, Body Loss, Building Penetration, etc.. (Typical values from measurements used)
  - Gains are added, Losses are subtracted – must balance
  - For FDD systems must do both up and down link



Example

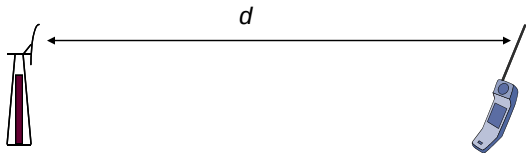
- Consider Design of a Point-to-Point link connecting LANs in separate buildings across a freeway
  - Distance 1 mile
  - Line of Sight communication
  - Spectrum Unlicensed – using 802.11b at 2.4GHz
- Given LOS is available can *approximate* propagation with Free Space Model as follows



Free Space Loss Model

- Assumptions
  - Transmitter and receiver are in free space
  - No obstructing objects in between transmitter and receiver
    clear LINE OF SIGHT (LOS) communication
  - The transmitted power is P_t
  - The received power is P_r
  - Isotropic antennas
    - Antennas radiate and receive equally in all directions with unit gain
- The *path loss* is the difference between the received signal strength and the transmitted signal strength

  $PL = P_t$ (dB) – P_r (dB)



Free space loss

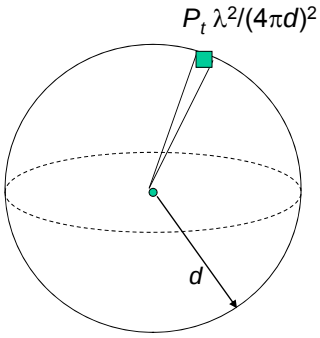
- Transmit power P_t
- Received power P_r
- Wavelength of the wireless channel is given by $\lambda = c/f = (3x10^8)/f$ where f is the frequency
- Over a distance d (in meters) the relationship between P_t and P_r is given by:

$$P_r = \frac{P_t \lambda^2}{(4\pi)^2 d^2}$$

- In dB, we have:
- P_r (dBm)= P_t (dBm) - 21.98 + 20 $\log_{10}$ (λ) – 20 $\log_{10}$ (d)
- Path Loss = PL = $P_t - P_r$ = 21.98 - 20$\log_{10}(\lambda)$ + 20$\log_{10}$ (d)

A simple explanation of free space loss

- Isotropic transmit antenna
  - Radiates signal equally in all directions
- Assume a point source
  - At a distance *d* from the transmitter, the area of the sphere enclosing the Tx is
    $A = 4\pi d^2$
  - The "power density" on this sphere is
    $P_t / 4\pi d^2$
- Isotropic receive antenna
  - Captures power equal to the density times the area of the antenna
  - Ideal area of antenna is
    $A_{ant} = \lambda^2/4\pi$
- The received power is:
  $P_r = P_t / 4\pi d^2 \times \lambda^2/4\pi = P_t \lambda^2/(4\pi d)^2$



$P_r = P_t / L_p$

Free Space Propagation

- From the Free space Path Loss formula notice that factor of 10 increase in distance => 20 dB increase in path loss (20 dB/decade)

Distance	Path Loss at 880 MHz
1km	91.29 dB
10Km	111.29 dB

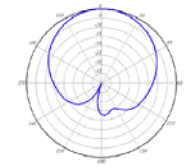
- Note that higher the frequency the greater the path loss for a fixed distance

Distance	2.4 GHz	5.7 GHz
1.6km (1mile)	104 dB	112 dB

thus 8 dB greater path loss for 5.7 WLAN band compared to 2.4GHz WLAN band

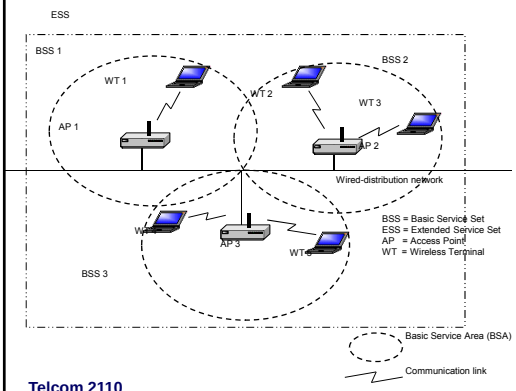
Example

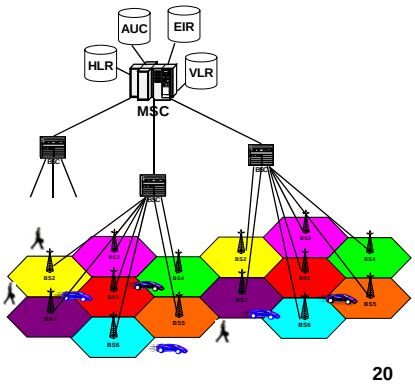
- Back to Example
  - Distance 1 mile ~ 1600m
  - Line of Sight communication
  - Spectrum Unlicensed – using 802.11b at 2.4GHz
  - Receiver Sensitivity Threshold - 80dBM for 11Mbps
- Given max transmit power of Pr = 24dBm at estimated Free Space Path loss of PL = 110 dBm the expected received signal Pr = 24 – 110 = -86dBm which is below the desired sensitivity threshold ➔ use directional Yagi antennas with with effective gain of G_t = 6 dB at transmitter and G_r = 6dB at receiver
- The resulting Pr will be
- $Pr = Pt + G_t - PL + G_r$
  $= 24 + 6 – 110 + 6 = -74dBm$
- Note that the system margin is small
  System Margin = Pr – RST = 6dB
  So 11Mbps performance is iffy – more likely to get 5.5 Mbps



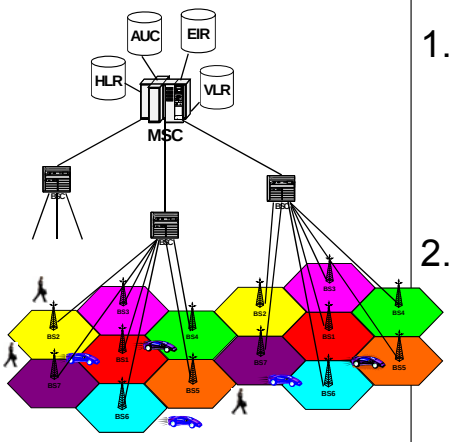
Wireless in Access Networks

- Normally what is thought of as a Wireless Access Network is using *wireless for last hop connectivity*
  - Link between end host/users to network is via wireless communication channel
  - Examples: cellular network, WLANS, WiMAX





Wireless Access Network Design



- Split Network Design problem in two parts

1. Wireless Part
   - Determine location and configuration of wireless base stations to meet
     - Coverage goals
     - Capacity requirements
2. Given base station locations solve wired access network design problem
   - One speed one center design
   - Multi-speed access design
   - Multi-center Design

Wireless Access Network Design

- Objective is to meet the network design requirements:
  - Radio signal coverage
    - Received signal strength adequate in required geographic space
    - Interference level acceptable
    - Installation restrictions
  - Data rate capacity
    - Average data rate available to users

Node (AP/BS) location problem

Frequency assignment problem

Power level assignment problem

- Solution requires knowledge of Wireless Technology constraints, signal propagation, geography of area to be covered – the exact parameter set will depend on the wireless technology used (e.g., WLANs, Cellular, WiMax)
- Consider WLANs as an example technology

Wireless LANs

- **Wireless Local Area Networks**
  - Support communication to mobile ***data*** users via wireless channel
  - Types of WLAN
    1. Infrastructure based (most popular)

       Connect users to a wired infrastructure network

       Wireless access network like cellular phone syste

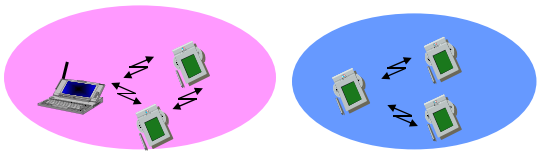
       IEEE 802.11, a, b, g, n, etc.

    2. Ad-Hoc based networks
       - Provide peer to peer communication – mobiles communicate between each other directly
       - Rapid Deployment (conference room)
       - Bluetooth, IEEE 802.11, a, b, g, n, Proprietary

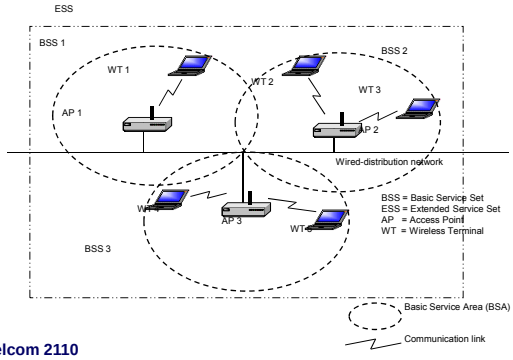
    3. Point – to –Point (cable replacement)

WLAN Topologies

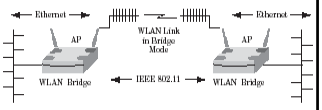
ad-hoc based architecture



Infrastructure based architecture



Point-to-point



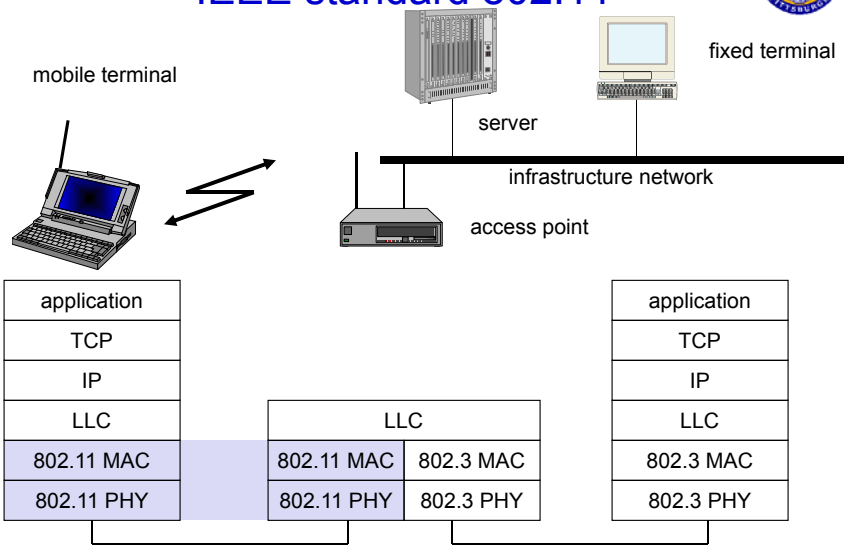
Spectrum for Wireless LANS

- Licensed Vs. Unlicensed Spectrum
  - Licensed Spectrum
    - need to buy right to use spectrum allocation in a specific geographic location from the government (e.g., AM/FM radio)
    - Prevents interference – licensee can control signal quality
  - Unlicensed Spectrum
    - Anyone can operate in the spectrum but must maintain proper behavior in spectrum (max power level and frequency leakage, etc.)
    - Can have interference problems
- Industrial Scientific and Medical bands (unlicensed)
  902-928 MHz, 2.4 – 2.4835 GHz, 5.725 – 5.875 GHz
- U-NII bands (5-6 GHz) (unlicensed)
  - Three bands of 100 MHz each
    - Band 1: 5.15 - 5.25 GHz
    - Band 2: 5.25 - 5.35 GHz
    - Band 3: 5.725 - 5.825 GHz
- 18-19 GHz licensed available in U.S.
- 17 GHz, 40 GHz and 60 GHz unlicensed under study

IEEE 802.11 Standard

- The project was initiated in 1990
- The first complete standard was released in 1997
- Supports two topologies: Infrastructure and Ad hoc
- Suite of standards for MAC layer and below
- Main standards IEEE 802.11, a, b, g, n
- Common MAC layer for all sub-standards
- Supports different physical layers at various data rates and frequencies
  - Diffused infrared (802.11)
  - Frequency hopping spread spectrum (802.11)
  - Direct sequence spread spectrum (802.11b)
  - Orthogonal Frequency Division Multiplexing (OFDM) (802.11a, g)
  - Multiple Input Multiple Output & OFDM (802.11n)
  - Is TDD for each physical layer
- Many additional sub-standards studying various aspects

IEEE standard 802.11



IEEE 802.11 Standards

Standard	Scope
802.11	Original 1,2 Mbps standard in 2.4 Ghz and IR frequency band
802.11a	54Mbps physical layer in 5GHz band
802.11b	11Mbps physical layer in 2.4GHz band
802.11d	Operation in additional regulatory domains
802.11e	Enhanced 802.11 Mac to support QoS in other standards (a,b,g,n)
802.11f	Inter-access point protocol (IAPP) to support roaming
802.11g	54Mbps physical layer in 2.4GHz band
802.11i	Enhanced security
802.11n	Extension to > 100 Mbps physical layer using MIMO
802.11s	Mesh networking
802.11u	Interworking with other networks (e.g., cellular)
802.11v	Wireless network managment

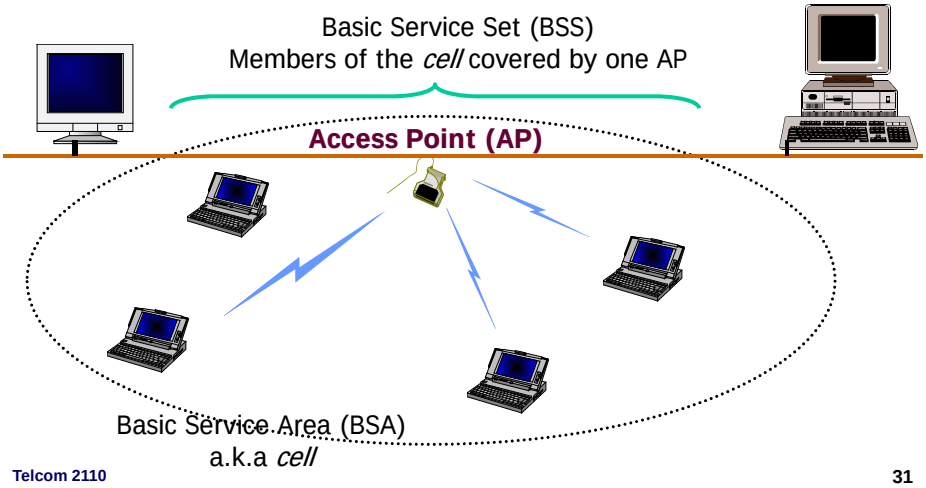
IEEE 802.11 Terminology

- Access Point (AP)
  - Acts as a base station for the wireless LAN and is a bridge between the wirless and wired network
- Basic Service Area (BSA)
  - The coverage area of one access point
- Basic Service Set (BSS)
  - A set of stations controlled by one access point
- Distribution system
  - The fixed (wired) infrastructure used to connect a set of BSS to create an **extended service set (ESS)**
- Portal(s)
  - The logical point(s) at which non-802.11 packets enter an ESS

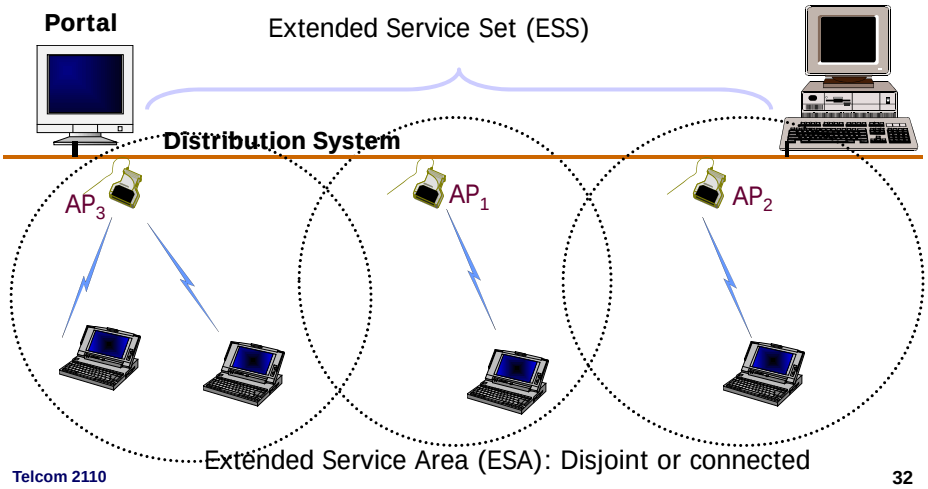
Infrastructure Network Topology

- A wired infrastructure supports communications between mobile hosts (MHs) and between MHs and fixed hosts
- Star topology
  - The BS or AP is the hub
  - Any communication from a MH to another has to be sent through the BS or AP
  - The AP manages user access to the network
  - APs typically mounted on wall or ceiling, AC power maybe a problem
  - Power over Ethernet option delivers AC power over UTP Ethernet cable
- Designed for multiple APs interconnected to cover larger areas to form ESS

Infrastructure based Architecture

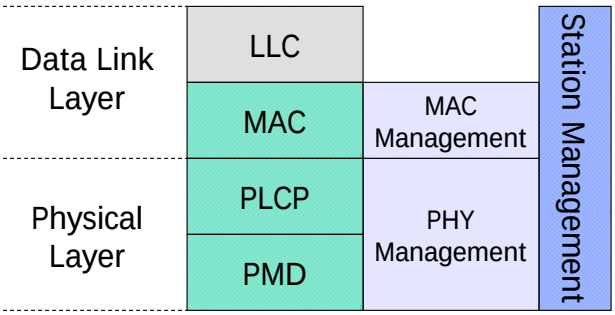


Infrastructure-based Architecture



IEEE 802.11 Protocol Architecture

MAC layer independent of Physical Layer
Physical varies with standard (802.11, 802.11a, etc.)
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent



The MAC Layer

- IEEE 802.11 data link layer has two sublayers
  - Logical Link Layer
    - determined by wired network interface
  - Media Access Control (MAC) layer :
    - security, reliable data delivery, access control
    - provides coordination among MHs sharing radio channel
- MAC Layer has two coordination techniques
  - Distributed Coordination Function (DCF)
    - based on CSMA/CA with randomized backoff
    - Asynchronous, best effort service
    - DCF with RTS/CTS (optional) avoids hidden terminal problem
  - Point Coordination Function (PCF)
    - Optional access mechanism
    - Provides “time bounded” service based on polling of MSs

Distributed Coordination Function (DCF)

- Distributed Coordination Function (DCF)
- CSMA/CD can't be used – because can't always detect collisions
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - MSs listens to channel to see if busy
    - if busy will backoff random time before checking again
    - If idle channel for duration of interframe spacing will trasmit
  - If a collision occurs, clients wait random amount of slot time after medium is clear before retransmitting
- CSMA/CA also reduces collisions by using explicit packet acknowledgement (ACK)
  - Receiving client must send back to sending client an acknowledgement packet showing that packet arrived intact
  - If ACK frame is not received by sending client, data packet is transmitted again after random waiting time

802.11 Protocol Architecture

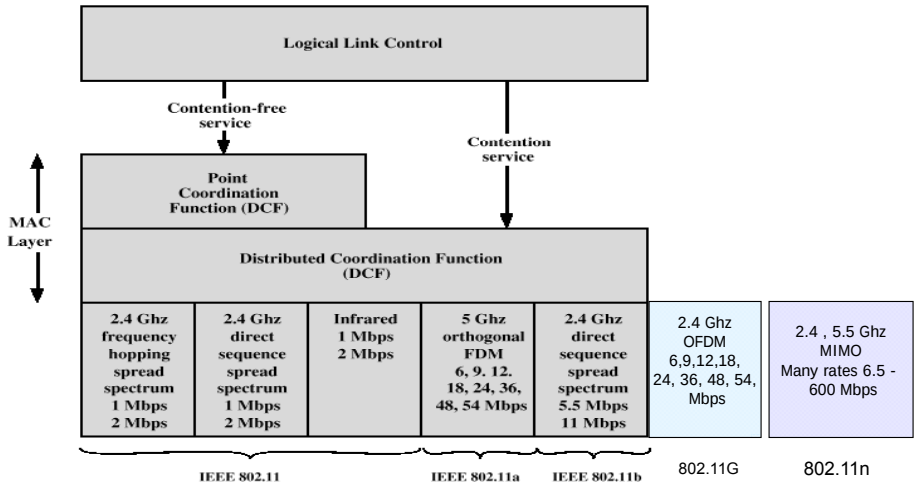
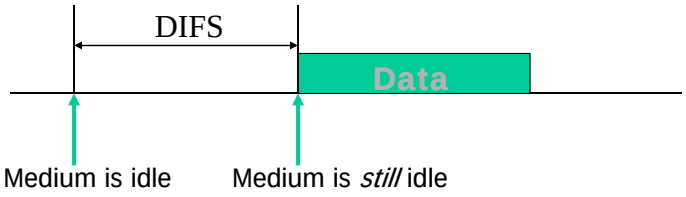


Figure 14.5 IEEE 802.11 Protocol Architecture

Physical and Virtual Carrier Sensing

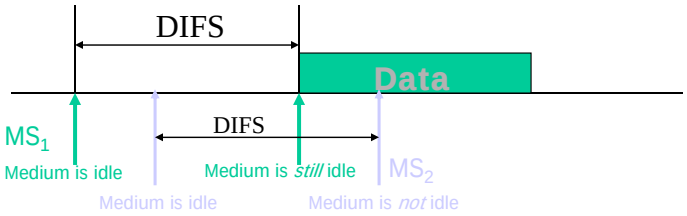
- The physical layer performs a “real” sensing of the air interface to determine if the channel is busy or idle
  - Analyzes detected packets
  - Detects carrier otherwise by RSS
- The MAC layer performs a “virtual” carrier sensing
  - The “length” in field in MAC control frame is used to set a network allocation vector (NAV)
  - The NAV indicates the amount of time that must elapse before the medium can be expected to be free again
  - The channel will be sampled only after this time elapses
- The channel is marked busy if either of the physical or virtual carrier sensing mechanisms indicate that the medium is busy

Idle Channel



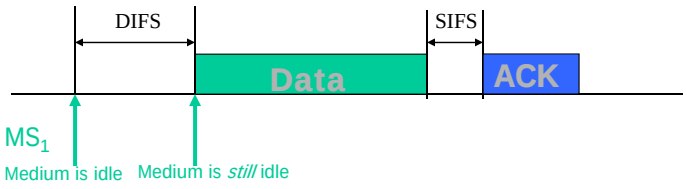
- If the medium is idle, every MS **has** to wait for a period DIFS (DCF inter-frame spacing) to send **DATA**
- After waiting for DIFS, if the medium is still idle, the MS can transmit its data frame

How does it help?



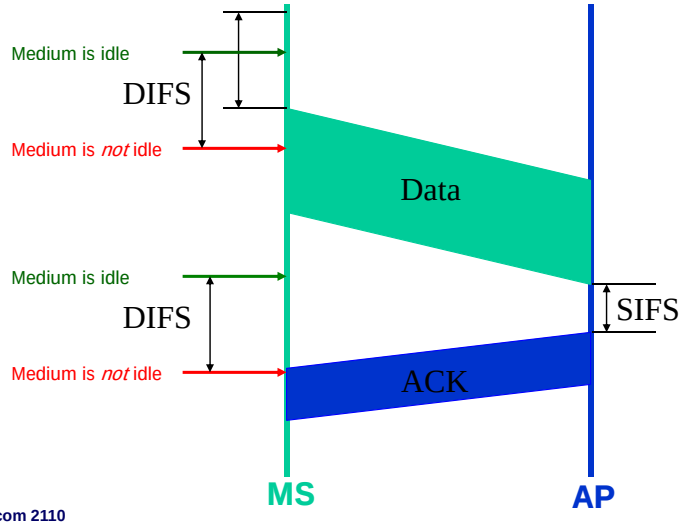
- If a second MS senses the medium to be idle after the first MS, it will find the medium to be busy after DIFS
- It will not transmit => collision is avoided

Acknowledgements

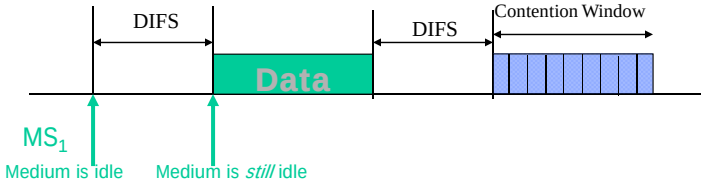


- A short inter-frame spacing (SIFS) is used
- SIFS is the ***absolute minimum*** duration that any MS should wait before transmitting anything
- It is used ONLY for acknowledgements (which will be sent by a receiving MS or AP alone)
- ACKs receive highest priority!
- ACKs will almost always be sent on time

Data Transmission And ACKs



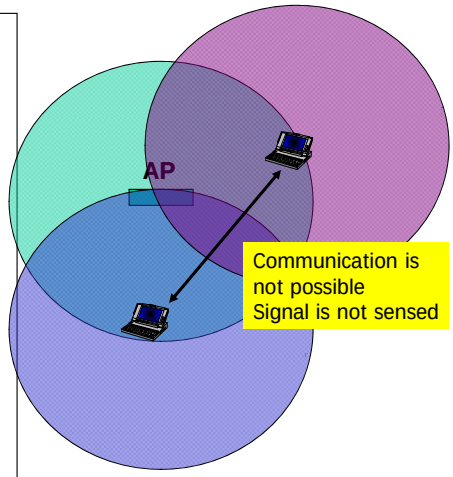
Busy Channel



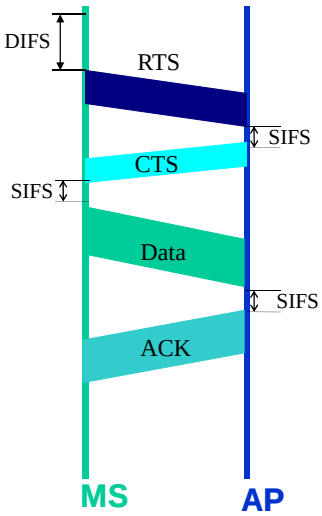
- Each MS has to still wait for a period of DIFS
- Each MS chooses a random time of **back-off** within a *contention window*
- Each MS decrements the back-off. Once the back-off value becomes zero, if the medium is idle, the MS can transmit
- The MS with the smallest back-off time will get to transmit
- All other MSs freeze their back-off timers that are “decremented” and start decrementing the timer in the next contention window from that point

When do collisions occur?

- MSs have the same value of the back-off timer
- MSs are not able to hear each other because of the “hidden terminal” effect
- MSs are not able to hear each other because of fading
- Solution: RTS/CTS
  - Also avoids excessive collision time due to long packets



RTS/CTS Mechanism

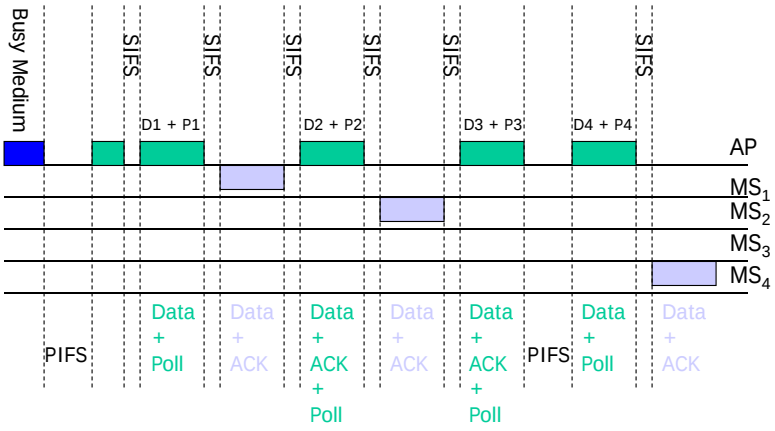


- RTS-Request to Send (20 bytes)
- CTS-Clear to Send (14 bytes)
- They can be used only prior to transmitting data
- After successful contention for the channel, a MS can send an RTS to the AP
- It gets a CTS in reply after SIFS
- CTS is received by all MSs in the BSS
- They defer to the addressed MS while it transfers data
- If there is a collision, no CTS is received and there is contention again

Point Coordination Function (PCF)

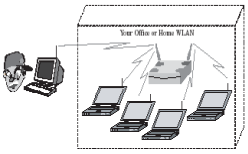
- Optional capability to provide “time-bounded” services
- It sits on top of DCF and needs DCF in order to successfully operate
- A point coordinator (the AP) polls each station and enables them to transmit without contention
  - Ad hoc networks cannot use this function
- Time (a super time slot) is divided into two parts
  - Contention Free Period (CFP)
  - Contention Period (CP)
- A MS must be CFP-aware to access the CFP
- Point coordination function IFS (PIFS)
  - Midlength IFS
  - Used by centralized controller in PCF scheme when polling MHs
- Replies to polling can occur after SIFS

PCF Continued

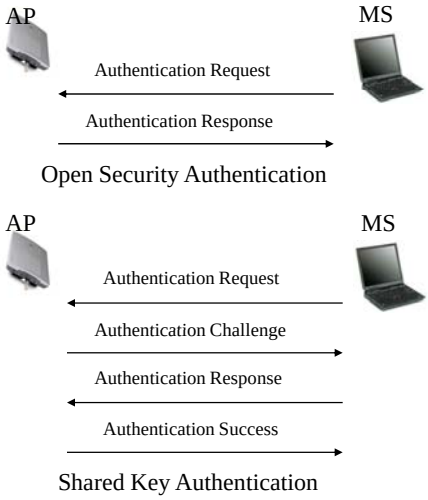


802.11 Security

- Authentication
  - Establishes identity of mobile stations to APs and vice a versa
  - Many older 802.11 networks don't use any type of authentication!
    - APs accept connections from all MSs
  - Open system authentication
    - Exchange of identities using Service Set Identifier (SSID) of network
    - SSID can be advertised by AP or entered manually into mobiles
  - Shared Key authentication
    - Uses a version of challenge/response protocol
    - Either 40 or 104 bit shared key
    - Keys are static and manually configured
  - De-authentication
    - Invoked when existing authentication is terminated



WEP Authentication



- Idea
  - Allow the AP to know that the MS possesses the right secret key
- Process
  - The AP sends a 128 byte arbitrary challenge text
  - The MS responds by encrypting the random message with the correct key
  - Algorithm used is RC-4 stream cypher
- The authentication is NOT mutual

802.11 Security

- Privacy
  - Prevents message contents from being read by unintended recipient
  - Uses Wired Equivalent Privacy (WEP) encryption (optional)
- WEP encryption
  - Each packet is encrypted separately
  - WEP based on RC4 stream cypher with 40 bit secret key
  - Secret key is combined with a 24 bit initialization vector (IV) that changes every packet to increase key size from 40 to 64
- Weakness
  - IV is transmitted in plaintext
  - IVs are reused too often (pseudorandom generator for IV repeats often (4-5 hours)
  - May start with same IV after shut down
  - Publicly available tools to hack key
    - AIRsnort , WEPcrack, etc.

Improving 802.11 Security

- Additional Security Procedures
- Wi-Fi Protected Access (WPA)

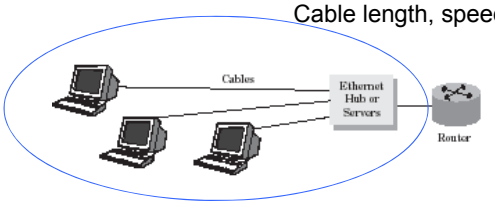
  Industry group developing techniques for existing networks
  - Use access control list with approved MAC addresses
  - Use 128 bit proprietary implementation of WEP key
  - Use VPNs (IPSec or SSL)
  - Security architecture based on 802.1x and EAP (Extensible Authentication Protocol)
    - Allows many protocols within a common framework
  - Example
    - Use a RADIUS server
    - Authenticate the access point using a variation of SSL
    - Authenticate the MS using passwords (CHAP)
- IEEE 802.11i standard
  - Use AES instead of RC4 for better security
  - Implemented on 802.11n

Design Issues in WLAN

Compare WLAN with wired LAN

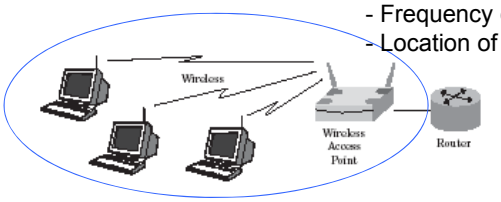
Cable length, speed

Conventional
Wired LAN



- Tx power level
- Frequency channel
- Location of access point

Typical
Wireless LAN

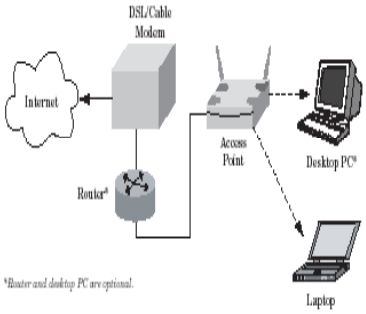


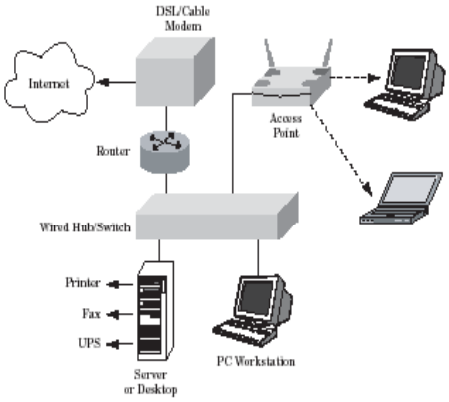
WLAN Deployment scenarios

1. Small network scenario

Ex:

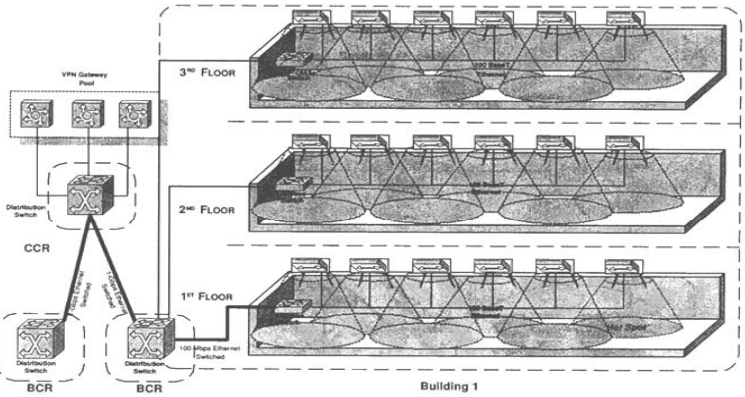
- small office, home office (SOHO)
- coffee shop





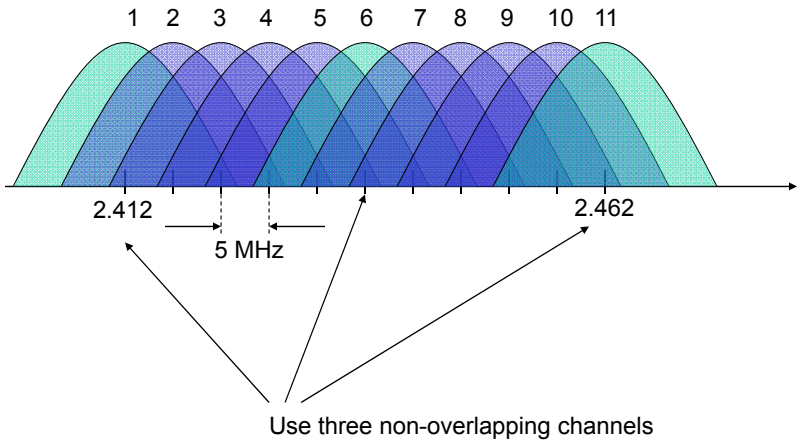
WLAN Deployment scenarios

2. Large network scenario
   - large office, warehouse
   - university campus, dormitory
   - corporate multistory buildings
   - hotels, shopping malls



BCR = Building Communication Room
CCR = Campus Communication Room

802.11
2.4 GHz specifications



802.11 Channels in 5GHz Band

- 802.11a
  - specifies 8 20 MHz channel frequencies
  - each channel divided into 52 subchannels 300KHz wide
  - 48 subchannels for data 4 subchannels for error corrections
- 802.11g
  - Ports 802.11a to 2GHz

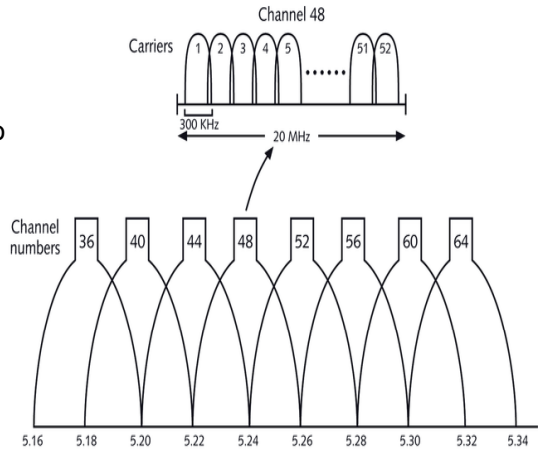


Figure 7-2 802.11a channels

802.11n Channels

- Approved recently - works in 2.4 and 5 GHz bands
  - 4 to 5 times the data rates of 802.11a,g ➔ 200-300Mbps
- Main Changes
  - Physical layer uses Multiple Input Multiple Output (MIMO) OFDM
    - Has multiple antennas at each end of the channel – provides spatial diversity
    - OFDM part about the same as 802.11a,g – uses 64QAM with 5/6 FEC rate
  - Channel Bonding
    - Combines 2 of the 20MHz 802.11a,g channels to achieve higher data rates - must be non-overlapping channels
  - Packet Aggregation
    - Reduce overhead by aggregating multiple packets from a single application/user into a common frame

Design Issues in Large WLANs

- Need to assign each AP:
  - Frequency, Power level – physical location, mode (PCF or DCF)
- In the 2.4 GHz bands
  - For 802.11b there are fourteen 20 MHz frequency bands that can be used they are spaced 5 MHz apart
  - In USA can use channels 1-11 and three are non-overlapping (1, 6, 11)
  - There are six power levels
  - For 802.11g,n there are 3 frequency bands (non-overlapping)
  - Coverage roughly 375 feet omni-directional
  - Can put up to 3 non-overlapping frequencies in one AP
- In the 5 GHz bands,
  - For 802.11a,n there are eleven channels
  - There are 8 non-overlapping channels
  - Coverage roughly 250 feet omni-directional
  - Can put up to 5 non-overlapping frequencies in one AP
- Note 802.11n allows channel bonding (use two non-overlapping frequency channels as one 40 MHz channel) to increase throughput

802.11b vs. 802.11a Max Frequency per AP

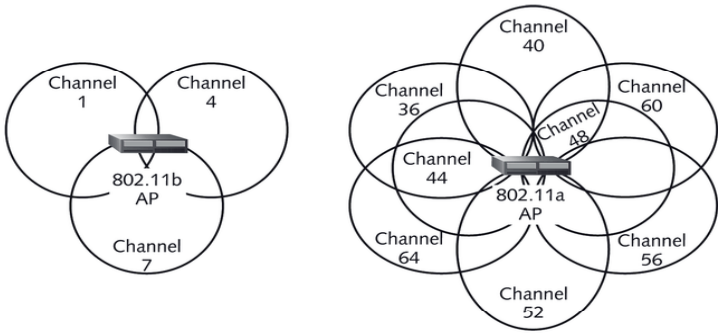


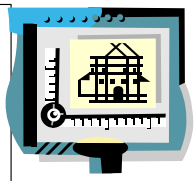
Figure 7-3 802.11b vs. 802.11a channel coverage

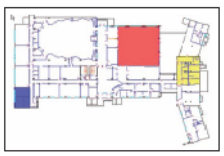
Design Issues in Large WLANs

- Network Planning of large WLAN networks require
  - *Coverage Planning*,
    - 3-D, depends on antenna pattern, building/site architecture, power level
  - Capacity Planning
    - Determining the number of APs and channels at each AP to meet the traffic demands
  - Frequency Planning
    - Frequency reuse is possible and AP can support multiple channels
    - Interference concerns

WLAN Design steps

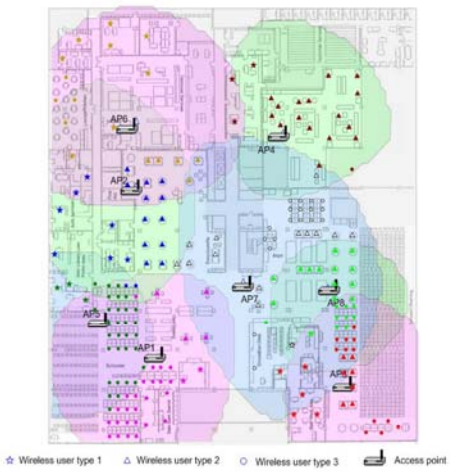
1. Obtain site and/or building drawings
2. Determine geographic coverage goals
   - What locations in the site/building need to be covered?
   - What areas need to be avoided ? (e.g., prevent unauthorized listening)
3. Determine user population, location and application requirements –
   - map into traffic demands at various locations





WLAN Design steps

4. Create WLAN design (AP locations and configurations) and installation guidelines
5. Make field measurements to verify Wireless design
6. Design wired backhaul and adjust WLAN design as required
7. Finalize design
8. Complete installation



Network design requirements

- Radio signal coverage requirement
  - Availability
  - Received signal strength
  - Interference level

Factors:
-Tx power level
- Frequency channel assignment
- location of access points
- # access points installed

- Average user data rate requirement
  - Amount of traffic user generated
    - User activity: passive or active
    - User applications: heavy or light data transaction
  - Locations where users gather

WLAN Network Design

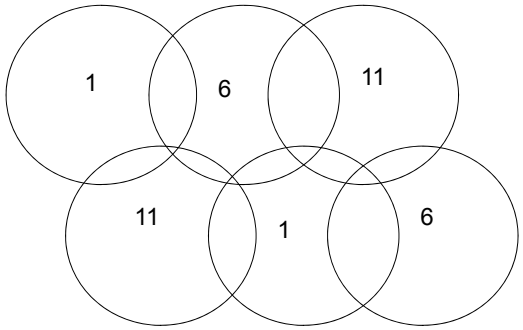
- Determine the number of APs required for the network service scenario
- Determine APs' parameters including
  - locations
  - power levels
  - frequency channels
- WLAN Coverage Design Approaches
  1. Trial and error
  2. Simple rules of thumb
  3. Signal strength prediction tools

WLAN Design approaches

- Trial and error
  - place APs at the convenient location or based on experience ("worked at other locations like that")
  - Adjust APs' locations, power levels, frequency channels based on signal strength measurement
    - Measure signal strength
    - Re-position APs, adjust power levels, freq ch.
    - Re-measure signal strength
    - …..
    - Time runs out. → leave it like that!
  - Tedious method!!
  - Based on signal coverage, not capacity considerations

WLAN design approaches

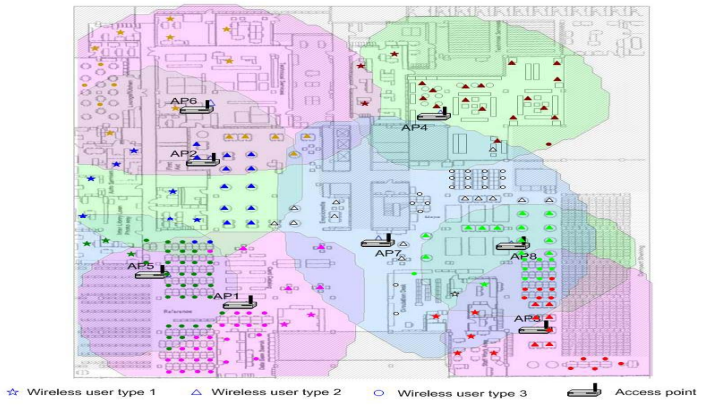
- Simple rules of thumb
  - open 160m /semi-open 50m /closed 25m



  - Reuse the three no-overlapping frequencies and verify with field measurements

WLAN design approaches

- Signal strength prediction tools
  - Path loss models can be used to predict the coverage of APs and plan locations



Radio Wave Behavior Review

- Waves may be *reflected* by stationary or moving objects, *diffracted* over large objects which block line of sight, *scattered* by small objects and *fade* with distance depending on environment and frequency – behaves in a fashion similar to light beams

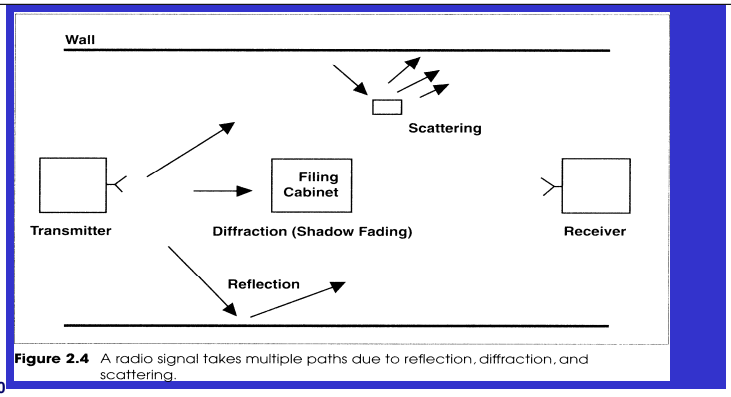
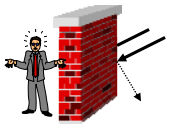
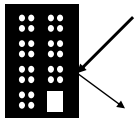


Figure 2.4 A radio signal takes multiple paths due to reflection, diffraction, and scattering.

Signal Propagation

- Received signal strength (RSS) influenced by
  - Fading – signal weakens with distance - proportional to $1/d^2$ (d = distance between sender and receiver)
  - Frequency dependent fading – signal weakens with increase in f
  - Shadowing (no line of sight path)
  - Reflection off of large obstacles
  - Scattering at small obstacles
  - Diffraction at edges

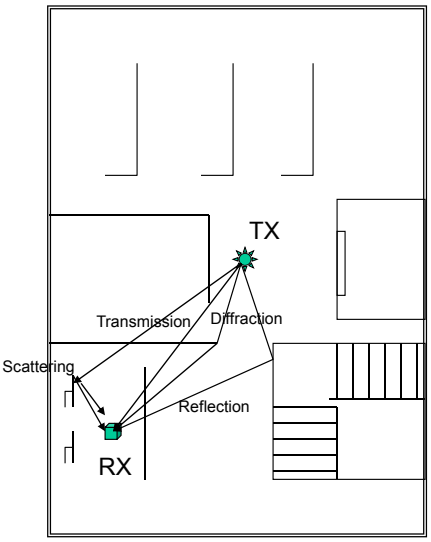

shadowing


reflection

scattering


diffraction

Signal Propagation



- Effects are similar indoors and out
- Several paths from Tx to Rx
  - Different delays, phases and amplitudes
  - Add motion – makes it very complicated
- Very difficult to look at all of the effects in a composite way
  - Breakdown phenomena into different categories
  - Here consider simple approximate measurement derived models
    1. Partition Dependent Model
    2. JTC model

Partition models

- Partition dependent model

$$L_p = L_0 + 20\log d + \sum_{type} m_{type} W_{type} + X$$

m_{type} = the number of partitions of *type*

W_{type} = the loss in dB associated with that partition

d = distance between transmitter and receiver point in meter

X = the shadow fading (depends on environment)

L_0 = the path loss at the first meter, computed by

$$L_0 = 10\log\left(\left(\frac{4\pi d_0 f}{3\times 10^8}\right)^2\right)$$

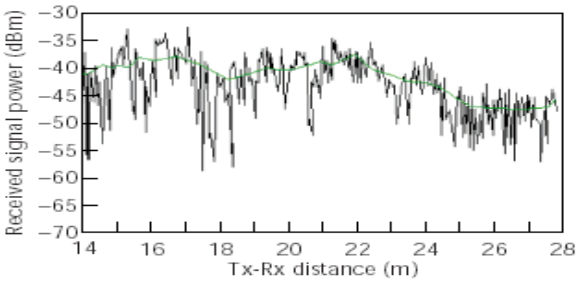
where d_0 = 1 m.

f = operating frequency of the transmitter

WLAN Partition Models

Amount of signal loss per partition is found from measured values

2.4GHz Signal attenuation through:	dB
Window in brick wall	2
Metal frame, glass wall into building	6
Office wall	6
Metal door in office wall	6
Cinder Wall	4
Metal door in brick wall	12.4
Brick wall next to metal door	3



Example Partition Model

Consider an AP operating at 2.412GHz. The distance from the AP to a receiving terminal is approximately 10 meters. There are two office walls and one metal door in office wall between the AP and the receiver. The AP operates at a power level of 100mW (20dBm). Use the partition dependent model to determine the path loss and received signal strength at the receiver location, consider a shadow fading of 13 dBm

$$L_p = L_0 + 20\log d + \sum_{type} m_{type} W_{type} + X$$

$$L_0 = 10\log\left(\left(\frac{4\pi d_0 f}{3\times 10^8}\right)^2\right)$$

$w_{office\ wall}$ = 6 dB, $w_{metaldoor\ in\ office\ wall}$ = 6 dB

X = 13 dBm

L_0 = $10\log_{10}((4\pi \times 1 \times 2.412 \times 10^9)/(3 \times 10^8))^2 = 10\log_{10}((101.034)^2) = 40.1$

L_p = 40.1 +20log(10) + (2*6 +6) +13 = 91.1 dB

Power received = $P_r = P_t - L_p$ = 20dBm – 91.1 dB = - 71.1 dBm

Note typical WLAN recievers need greater than -110 dBm RSS

The JTC Indoor Path Loss Model

$$L_{Total} = A + B \log_{10}(d) + L_f(n) + X_\sigma$$

Similar to Okumura –Hata model in cellular phone networks (curve fitting to measure values used to set up model)

- *A* is an environment dependent fixed loss factor (dB)
- *B* is the distance dependent loss coefficient,
- *d* is separation distance between the AP and portable, in meters
- L_f is a partition penetration loss factor (dB)
- *n* is the number of partitions between the access point and mobile terminal
- X_σ is a shadowing term – due to NLOS

JTC Model (Continued)

Environment	Residential	Office	Commercial
A (dB)	38	38	38
B	28	30	22
$L_f(n)$ (dB)	4n	15 + 4(n-1)	6 + 3(n-1)
X_σ Shadowing (dB)	8	10	10

JTC Model (Continued)

- Example

  Consider an AP on the first floor of a 3 floor house
  The distance to a third floor home office is approximately 8 meters
  If the AP operates at a power level of 24dBm using the JTC model determine the path loss and received signal strength in the office area

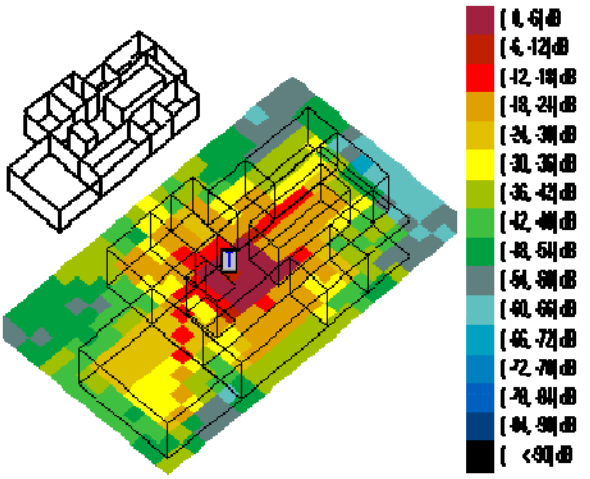
Using the JTC model with residential parameter set

$L_{total} = A + B \log_{10}(d) + L_f(n) + X_\sigma$
$= 38 + 28 \log_{10}(8) + 4x2 + 8 = 79.28$ dB

Power received = $P_r = P_t - L_{total}$ = 24 dbm – 79.28 dB = -55.28 dBm
which is well above the required -85dbm for max data rate operation.

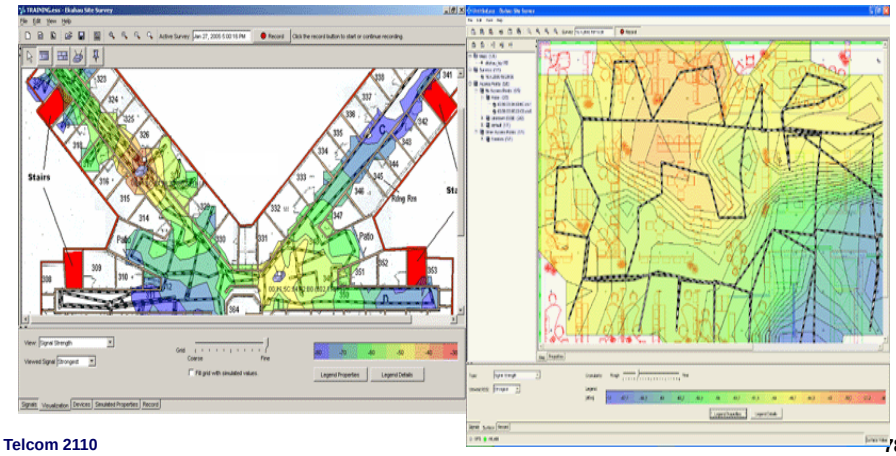
Signal strength prediction software

- Motorola LAN Planner
- Lucent: WiSE tool
- Given building/space to be covered and parameters of building and AP – predicts signal coverage



Site Survey Tools

Software to measure signal strength and recording in order to construct a coverage map of structure – must drive/walk around structure to gather data
NOKIA site survey tool, Ekahau Site Survey, Motorola LAN survey, etc.



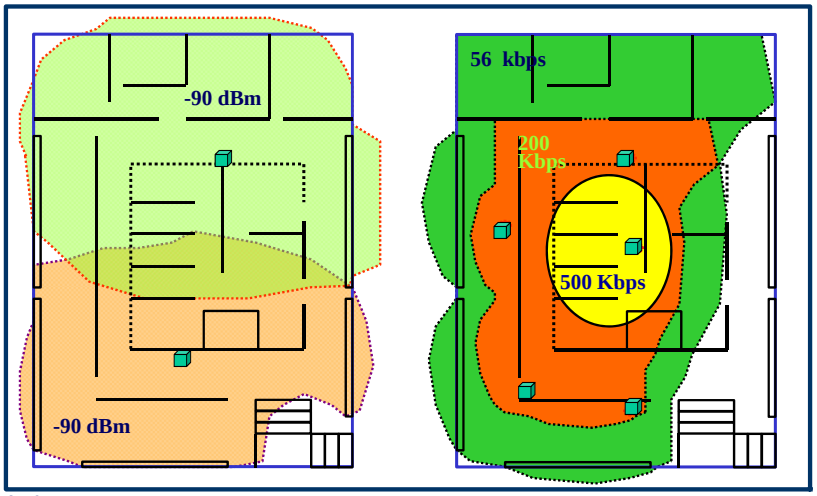
WLAN Capacity issues

- One must consider the capacity requirements as well as the coverage
- Capacity depends on # users sharing the AP and the amount of data traffic at the time
  - Heavy vs light data transfer
- Intel suggests rules of thumb for 802.11b – 1 AP can support
    - 50 nominal users who are mostly idle and occasionally check email (i.e., coffee house use) –> mean data rate ~ 100 kbps each
  - Or
    - 25 mainstream users who use a lot of email and download or upload moderately sized files -> mean data rate ~250 Kbps each
  - Or
    - 10 power users who are constantly on the network and deal with large files → mean data rate ~ 600 Kbps each
- 802.11a/g can support about four times the #users and/or traffic volume as 802.11b
- Note what is crucial is the application data rate needed not the channel rate

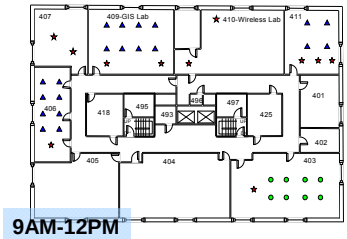
Table 1. IEEE 802.11 WLAN standards.

Standard	Spectrum	Maximum physical rate	Layer 3 data rate	Transmission	Compatible with	Major disadvantage	Major advantage(s)
802.11	2.4GHz	2 Mbps	1.2 Mbps	FHSS/DSSS	None	Limited bit rate	Higher range
802.11a	5.0GHz	54 Mbps	32 Mbps	OFDM	None	Smallest range of all 802.11 standards	Higher bit rate in less-crowed spectrum
802.11b	2.4GHz	11 Mbps	6-7 Mbps	DSSS	802.11	Bit rate too low for many emerging applications	Widely deployed; higher range
802.11g	2.4GHz	54 Mbps	32 Mbps	OFDM	802.11/802.11b due to narrow spectrum	Limited number of colocated WLANS higher range than 802.11a	Higher bit rate in 2.4-GHz spectrum
802.11n	2.4GHz And 5.GHz options	108-300 Mbps	50-75 Mbps	MIMO OFDM	802.11g	Uses two channels	Higher bit rate

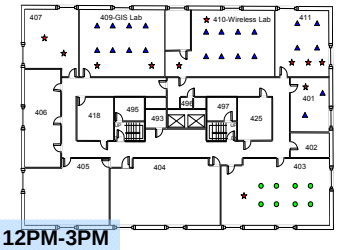
Coverage Based vs. Capacity Based



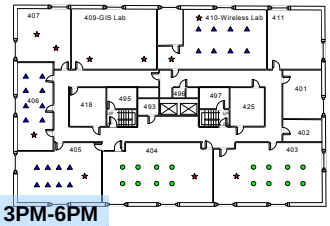
Traffic Demand Characteristics



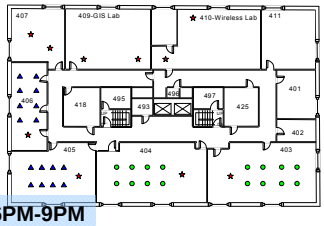
9AM-12PM



12PM-3PM

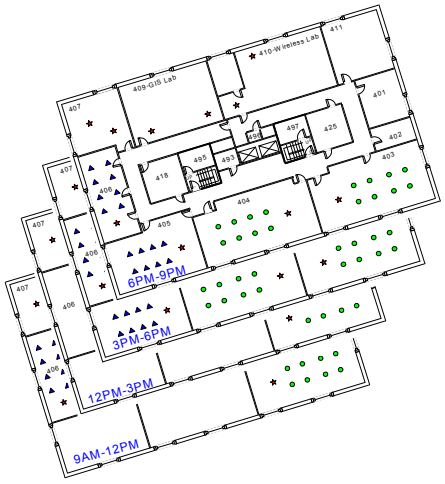


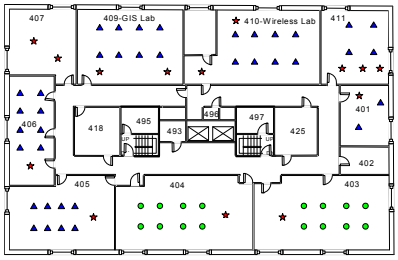
3PM-6PM



6PM-9PM

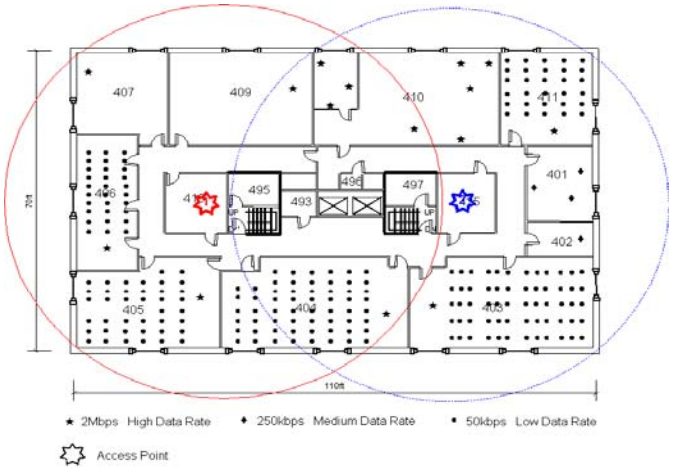
Peak Traffic load for WLAN design



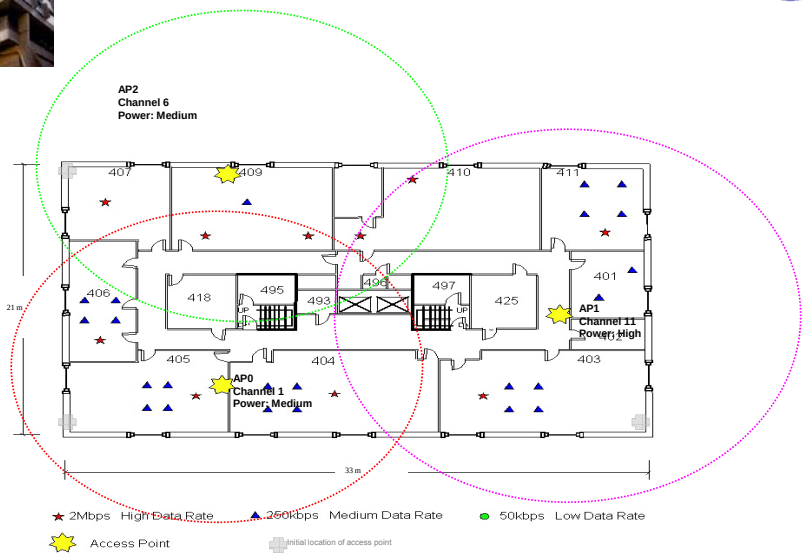


A Coverage Based Design

IS Building at
U. Pitt 4th Floor



Capacity Based WLAN Design



Heuristic Approach to WLAN Design

Following the design approach discussed earlier

1. Obtain geographic site and/or building drawings
2. Determine the geographic areas to be covered (and those not to be coveraged)
3. Estimate the coverage area (i.e., coverage square) of a AP using a signal propagation model (pick a typical power level and parameters of the propagation model)
4. Determine the minimum number of APs needed by replicating the AP coverage area throughout the required space until all areas are covered
5. Check the demand of each AP - if the demand is greater than the layer 2 capacity of the AP then add another frequency to the AP until the demand is met or split the coverage area of an AP and add another AP until the max number of APs has been reached.

Wireless in Access Networks

- Growing emphasis on wireless in access networks
- Several technical options – looked at two uses
  1. Point-to-Point cable replacement technology – design using link budget approach
  2. Last hop access technology – supports mobility
     - Design using path loss model to predict coverage
     - Include capacity requirements in design