CHAPTER 1: OVERVIEW OF WIRELESS STANDARDS, ORGANIZATIONS, & FUNDAMENTALS

Standards organizations:
FCC - a government entity that regulates, among other things, content and properties of wireless communications including frequency, bandwidth, max power of internal radiator, EIRP, and use of communications. They publish regulations in the CRF (code of federal regulations) that standards organizations have to follow.
International telecommunication union radio communication sector (ITU-R) - maintains database of worldwide frequency assignments. Manages 5 regions.
Institute of Electrical and Electronics Engineers (IEEE) - creates technological standards for cross-platform interoperability. Made 802.11 wireless standard.
Wi-Fi Alliance - global industry trade association, committed to help WLANs grow, also to ensure interoperability of WLAN products by certification testing.
International Organization for Standardization (ISO) - made OSI model, a nongovt'l org that identifies needs of gov't, business, society, then develops standards w/ ppl who will use them.
OSI model: 7.Application; 6.Presentation; 5.Session; 4.Transport; 3. Network; 2.Data-Link; 1.Physical

Physics of Carrier Signals
AC or DC signal modulated = carrier signal, which can be interpreted as a 0 or 1. Modulation options: amplitude, frequency, and phase.
How data is encoded: Amplitude and Wavelength are physical characteristics of waves. Frequency is # of waves/unit of time. Phase: relative measure 1 wave to another, measured in degrees.
Keying method: method of manipulating a signal so it represents multiple pieces of data (0 or 1).
Amplitude Shift Keying (ASK): Making amplitude larger or smaller to represent a 0 or 1. Unreliable if high interference is taking place. (AM radio??)
Frequency Shift Keying (FSK): Higher or lower frequency can indicate a 1 or 0. Used in earlier 802.11 (think FM radio??)
Phase Shift Keying (PSK): Used extensively in 802.11. 0 is when a phase change at a certain sample point does not occur, 1 is when phase change does occur. if 4 phases are used instead of 2, we can represent 2 binary values (ie 00, 01, 10, 11). Called Multiple PSK
Techniques to represent data: Current State: current value of a signal is checked at a certain time/each interval of specific time. Door metaphor: open=1 closed=0. State Transition: The change (or no change) of a signal is used to distinguish between a 0 and a 1. Door metaphor: moving=0 still=1.

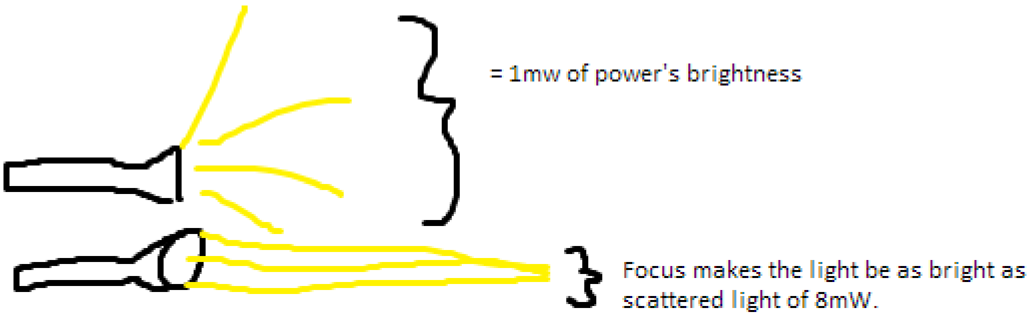
CHAPTER 2 - RADIO FREQUENCY FUNDAMENTALS

Wireless communications travel across an unbounded medium, lets signal radiate in all directions.
A RF starts out as an Alternating Current (AC), radiated out of antenna in form of electromagnetic wireless signal. Shape of AC signal is the likes of a sine curve, defined as "the waveform". Can travel up to the speed of light.
RF characteristics defined by laws of physics:
Polarity: Orientation of the antenna affects the polarity of the signal. The E-field is parallel to the plane of the antenna element. The plane that is perpendicular is known as the H-plane (consists of the H-field which is magnetic.
Wavelength: distance btw two crests or troughs of a wave. Represented by Greek symbol lambda λ. Higher frequency (shorter wavelength) = shorter distance a propagated wave will travel.
A 2.45GHz signal has a 4.82 inch (12.24cm) wavelength. A 5.775GHz has a 2.04 (5.19cm) wavelength.
Frequency: Measured in Hertz. 1 Event occurring/ 1 second = 1Hz
1KHz = 1k cycles/sec. 1 mega Hz (MHz) = 1 million cycles/sec. 1 gigahertz(GHz) = 1 billion cycles/sec. wavelength = c/f (c=speed of light~300 billion m/s)
Amplitude: size of trough or crest from center of curve. Usually measured with a y, as in coordinate plane is the y axis.
Phase: relationship between 2 waves. If 180 degree separation in phase occurs, then the two waves end up cancelling out one another.

RF Behaviors
Wave propagation: The material through which RF waves move can change the properties of propagation dramatically.
Absorption: When RF signal does not bounce off, move around, or pass through an object, 100% absorption occurs. Most materials usually absorb some of a RF. Leading cause of attenuation. Water causes pretty high levels of absorption.
Reflection: sky wave reflection happens with frequencies below 1 GHz (large wavelength) when they bounce off charged particles of ionosphere. Microwave reflection exists between 1GHz and 300 GHz; bouncing off of smaller objects such as metal doors, buildings, roads, bodies of water, walls, file cabinets. Metal will absolutely cause reflection; glass and concrete may do so too. New Technology MIMO takes advantage of reflecting RF Signals.
Scattering: multiple reflections occurring when EM signal's wavelength is greater than pieces of the medium it is passing through. 2 kinds of scattering: smaller level; reflection off of tiny particles (i.e. smog and sandstorms can cause this kind of scattering. Larger level; RF signal scattered by uneven surface. Caused by stuff like rocky terrain, chain link fences. Substantial signal attenuation can result. Like light hitting a disco ball.
Refraction: Bending of RF signal while passing through a medium. Causes: water vapor, changes in air temp, and changes in air pressure. Typically, RF signals refract towards the earth's surface.
Diffraction: Bending of RF signal around an object. Dependent on shape, size, and material of obstructing object, and also chars of RF signal. Space directly behind object becomes a "dead zone"
Loss (Attenuation): Decrease of amplitude or signal strength.
Free Space Path Loss: Loss of signal purely because of travel. The property of this loss is logarithmic with distance, so more distance will cause more loss, but the change isn't as great as in the first couple meters.
Multipath: Multiple instances of signal arrive at receiver within nanoseconds of each other. Results: Downfade (decreased signal strength, phase differences between 121 and 179 degrees), Upfade (increased signal strength; phase difference of 0 to 120 degrees), Nulling, (signal cancellation; phase differences around 180), Data corruption (intersymbol interference *ISI*).
Gain (Amplification): Increase of amplitude or signal strength. Active: use of amplifier with external power source; Passive: focusing RF signal w/ use of antenna.

Chapter 3: Radio frequency components, measurements, and mathematics

Three components to any communication: 1. Want or need of communication *2. Medium or means of communications* 3.A set of rules for this communication to exist.
Transmitter: Data which is pumped into it from computer is converted into an AC signal, according to 802.11b, and g, this signal oscillates at 2.4 billion times per second. 802.11a does so at 5 billion times/sec. The transmitter applies the corresponding modulation technique and power (amplitude) and sends it to the antenna.
Antenna: Radiation or Reception of radio waves, power is a lot less coming in than going out;often referenced to an *isotropic radiator* (a point source) – like the sun that radiates RFs in all directions equally. Ways to increase power from antenna: 1. Increase power 2. Focus waves. Flashlight metaphor: 1. Stronger batteries 2. Use lens to focus light.
Receiver: Gets AC waves from antenna, transforms them into digital (0s and 1s)
Intentional radiator (IR): everything from transmitter to antenna (not including the antenna). Is measured and regulated at the point where the current gets to the antenna. Power level measured in milliwatts(mW)

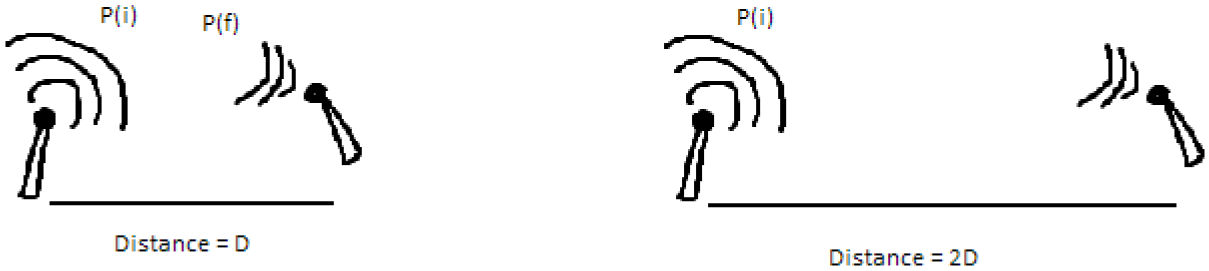

= 1mw of power's brightness
Focus makes the light be as bright as scattered light of 8mW.

Equivalent Isotropically Radiated Power (EIRP) is the highest RF signal strength that is radiated from a specific antenna. The above example, the same measured 1mW of both flashlight instances, the first one without lens/bulb (the antenna's effect) has only 1mW, but with lens and bulb, the focused light (at same distance) makes the EIRP=8mW. This quantity is also regulated by FCC.

Units of Power	Units of comparison
1 Watt = 1 amp of current flowing at 1 volt. Watts = Amps*Volts. (Metaphor: Power washer-pressure applied and volume of water used/time; success of washer = pressure*volume of water)	Decibel (dB): Comparison between power of two transmitters or to compare loss btw EIRP of transmitting antenna to amt of power received at other end. $1bel = \log_{10}\frac{10}{1}$. The 10/1 represents a ratio of 10:1 of outgoing to incoming power. Decibel = 10*1 bel.
Milliwatt (mW): 1/1000 of a Watt. 802.11 equipment usually 1mW to 100mW of power transmitted. Decibel	Decibels isotropic (dBi): The gain of power from an antenna when compared to what a theoretical ("perfect world") isotropic radiator would generate (flashlight without the lens to focus power).
Decibels relative to 1 milliwatt (dBm): 0dBm=1mW of amplitude. $dBm = 10 \times \log_{10} P_{mW}$ *6dB rule*: +6dB doubles distance of usable signal; -6dB halves the distance of usable signal.	Decibel dipole (dBd): decibel gain (dBi) as compared to a dipole antenna. Standard dipole antenna has value of 2.14. If an antenna has 3dBd: means the antenna is 3dB more powerful than a dipole antenna; this antenna has dBi = 5.14.

Inverse Square Law:

$$P(f2) = P(f) * \frac{1}{(2D)^2}$$



<u>Free Space Loss (FSPL)</u> in dB = 32.4 + 20log$_{10}$(*f in MHz*) +20log$_{10}$(*km btw antennas*)
36.6+ … for miles.

RF Mathematics
3dB of Gain? Absolute power (mW) *2
3dB of Loss? Absolute power(mW) /2
10dB of Gain? Absolute power (mW)*10
10dB of Loss? Absolute power(mW)/10

Using logs:

$$dBm = 10\log_{10}(Power\ in\ mW)$$

$$dB = 10\log_{10}\frac{P_f}{P_o}$$

Where P_f is final power and P_o is original power

Received Signal Strength Indicator (RSSI)
<u>Receive sensitivity</u>: the power level needed for a receiver to process data. Usually measured in terms of the speed of the network. More speed = more sensitivity. RSSI goes from 0 to 255 mapped todBm values.
Signal Quality and Signal-to-Noise ratio are used to sell products. RSSI is a proprietary measure
Link Budget
Sum of all gains and losses from the transmitting radio through RF medium to the receiver radio; purpose being to ensure that the signal gets across successfully (above receiver sensitivity threshold)
Gain: RF amplifiers and antennas
Loss: attenuators, FSPL, insertion loss (*i.e.* connectors, cables)
Fade Margin (or system operating margin (SOM))
Level of desired signal above what is required.*i.e.* if sensitivity threshold is -80dBm and signal comes in at -65dBm, the fade margin is 15dBm. Fade margin minimum is 10dBm. 25dBm recommended for distances >5miles.

CHAPTER 4: RADIO FREQUENCY SIGNAL AND ANTENNA CONCEPTS

<u>Active Gain</u>: Gain attained from increasing power coming from transmitter.
<u>Passive Gain</u>: Gain resulting from focusing the power through the antenna.
<u>Azimuth and Elevation charts</u>: radiation pattern charts based on a logarithmic scale using dB as a relative measure. Azimuth (H-plane) is a chart viewing antenna in birds-eye-view. Elevation (E-plane) is from the side.
<u>Beamwidth</u>: Like with a flashlight, light is focused more on one setting than another. It is the measure of how wide the focus of an antenna is vertically and horizontally from the center point to -3dB out vertically and horizontally (where the power is half of what it is in the center).

Antenna Types:
<u>Omnidirectional</u>: 360 horizontal RF radiation, designed to provide coverage in all directions.
Ie:collinear, dipole antenna. For 2.4GHz, a dipole antenna is ¼λ, which is about 1 inch.
Higher gain antennas increase the horizontal spread, vertical spread decreased.
<u>Semidirectional</u>: RF radiation to 180 directional spread, away from antenna. Like a streetlamp.
Short to medium distance use.
i.e. Patch, Panel(Planar antennas good for warehouses, libraries where there are large shelves. Can have up to 1 mile of coverage point-to-point), and Yagi (like tv antennas, except that they receive rf that are very close in wavelength so instead

of all the different lengths of antennas, there's only 1 length. For short and medium distance; max 2 miles, high gain used for longer distances.)

Highly Directional: More like a spotlight, focus on a small area.Ideal for longer distances of up to 35miles point-to-point. Can be affected by high winds; moving the antenna b/c of small Beamwidth can disrupt the beam of antenna & will miss the receiving antenna.i.e. Parabolic Dish, grid antennas

The more directional a signal, the more the amplification of RF signals going in and coming out.

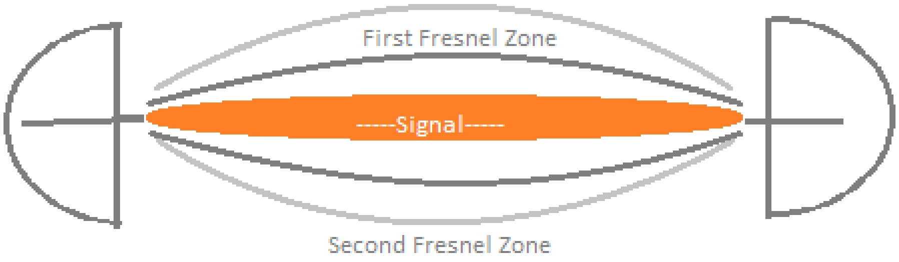
Phased Array Antenna: multiple antennas hooked up with a single processor, can send multiple signals simultaneously. Regulated differently than single-signal antennas.

Sector Antennas: High gain antennas (coverage can reach far) that cover a "piece of the pie" Many of these mounted on a taller tower can cover 360 degrees, each can be adjusted for corresponding terrain. Used for cellular coverage, now being used for 802.11 as well.

Fresnel Zone:

Line of Sight: usually a straight line on which the center of focus is; RF's success has nothing to do with visual Line of Sight

RF Line of Sight: LOS needs to be clear as well as the area around it. This area is called the Fresnel Zone; shaped like an American football in every direction (3D) around the signal beam.



Anything more than 40% into the first Fresnel zone will most likely make the link fail. Most common obstacles in a point-to-point link are trees and buildings.

1st Fresnel zone Radius = *72.2 ×√[D ÷ (4 ×F)]*| D = distance of the link in miles | F = transmitting frequency in GHz

60 % of above Radius (the largest radius) is *43.3 ×√[D ÷ (4 ×F)]*

It is also useful to find the radius of the first or second Fresnel zone at a certain point btw the two antennas.

Radius = *72.2 ×√[(N × d1 × d2) ÷ (F × D)]*

N = which Fresnel zone you are calculating (usually 1 or 2)

d1 = distance from one antenna to the location of the obstacle in miles

d2 = distance from the obstacle to the other antenna in miles

D = total distance between the antennas in miles (D = d1 + d2)

F= Frequency in GHz

Size of Fresnel zone is dependent on D and F only, not the beamwidth of the signal or the type of antenna.

Waves in odd numbered Fresnel zones are *in phase* with the point signal, waves in even numbered ones are *out of phase*. Out of phase waves from the second Fresnel zone can interfere and degrade the signal by reflecting off of flat surfaces or metal rooftops. Not too common.

Earth Bulge

We must account for the curvature of the earth; rule of thumb: p2p connections farther than 7 miles from each other.

$H = D^2 \div 8$| H = height of the earth bulge in feet | D = distance between the antennas in miles

Antenna Height = Obstacle + Earth Bulge + Fresnel Zone

$H = OB + (D^2 \div 8) + (43.3\sqrt{[D \div (4 \times F)]})$ | OB = Height of obstruction

Antenna Polarization

Important that sending and receiving antennas are both either in vertical or horizontal positions

Antenna Diversity

In order to avoid multipath, two or more antennas are mounted and work together to sample the waves, compare them and then use the one that has better strength. Also known as *receive diversity*. The distance between the antennas should be a factor of the wavelength (¼, ½, 1, 2). *Transmit diversity* refers to the AP transferring data out the same antenna as it received the signal for a request. Useful b/c we don't know where the receiving antenna is always, esp. with moving receivers.

MIMO

Takes advantage of multipath uses techniques such as Space Time Coding (STC), basically uses multiple antennas at the same time at both receiving and transmitting end of the communication link.

Antenna installation

Voltage Standing Wave Ratio (VSWR): a ratio of impedance mismatch *max voltage:min voltage* Along a line. Ideal (but unobtainable) would be a 1:1 ratio. A large VSWR is bad, meaning large loss in power (amplitude). This loss is reflected back to transmitter; can damage it.

Signal Loss: can be avoided with proper and well maintained equipment.

Mounting of Antenna, Placement, orientation/alignment, safety, maintenance, and appropriate use are needed for proper function.

Chapter 5: Overview of the IEEE 802.11 Standard

802.11 group is responsible for LAN communications using radio frequencies.

Original 802.11 standard published in 1997, referred to as 802.11 Prime. Latest revision was in 2007. Technologies are defined to be at physical and data link layers. Physical Layer (original) specifications: Infrared (IR), Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS)

Spread spectrum: a bandwidth that is wider than what is required to transport data.

Ratified Amendments

802.11b: *High-Rate DSSS* operates in 2.4 to 2.4835 GHz ISM band.

Use of *Complementary Code Keying (CCK)*, phase modulation. Support data rates 1, 2, 5.5, 11 Mbps. 1,2 are backwards compatible with 802.11 legacy equip. 5.5 & 11 known as HR-DSSS. *Packet Binary Convolutional Code (PBCC)* optional.

802.11a:*Orthogonal Frequency Division Multiplexing (OFDM)*

Operates in 5 GHz *Unlicensed National Information Infrastructure(UNII)* band. Data rates required: 6, 12, 24. Rates of: 6,9,12,18,24,36,48,54 Mbps are sometimes supported through OFDM. Cannot communicate with 802.11 legacy or 802.11b/g. 1) Different spread spectrum technology used. 2)b operates in 5GHz, while 802.11/b/g operate in 2.4GHz.

802.11g: *Extended Rate Physical (ERP)* 2.4 to 2.4835 GHz ISM band.

ERP-OFDM (data rates 6, 12, 24 mandatory) and ERP-DSSS/CCK (1, 2, 5.5, and 11Mbps) are mandatory for backwards compatibility. ERP-PBCC optional.

802.11d: Standard in order to ensure compatibility with frequency and power rules, and FHSS parameters internationally.

802.11F: A standard that is considered as “recommended practice,” but not mandatory.

Recommendation is to support Roaming: Seamless “hop” from one AP to another while communicating with the underlying network using *Inter-Access Point Protocol (IAPP)*. A rec. only b/c of vendor-interoperability issues.

802.11h:Defined mechanisms for Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC),

Avoid interference w/ 5GHz satellite and radar transmissions. TPC used to meet regulatory transmission power reqmts
Extended # of channels from 4 to 11 (UNII-2 Extended).

802.11i: Better security through Robust Security Network (RSN). Now is synonymous to *WPA2*, an Wi-Fi certification.

Data Privacy: Encryption methods *CCMP* – uses *AES* algorithm. Abbreviated as CCMP/AES, CCMP AES or CCMP. Optional encryption method: *TKIP* (an enhancement of *WEP*)

Authentication: PSKs, Extensible Authentication Protocol (EAP).

802.11j: Japanese altercations to 802.11a.

802.11e: QoS requirements

Hybrid Coordination Function (HCF): Prioritization of stations transmitting to AP.

Enhanced Distributed Channel Access (EDCA): Prioritization of frames based on upper layer protocols aka VOIP or VOWIP packets get delivered high priority.

802.11k: Provides means of Radio Resource Measurement

Transmit Power Control (TPC): Reduction of interference for the 5 GHz bands, will also be used in other bands

Client Statistics: Physical (signal-to-noise ratio, sig strength) and MAC (errs, frame transm) info reported back to APs.

Channel Stats: Noise-floor information reported back to AP

Neighbor Reports: Mobile Assisted Handover (MAHO) to get better handover between cells. Improves roaming perf.

802.11r: fast basic service set transition (FT) amendment. Faster handoffs for better roaming between cells in WLAN.

Speed needed in security protocols especially with VoWIP.

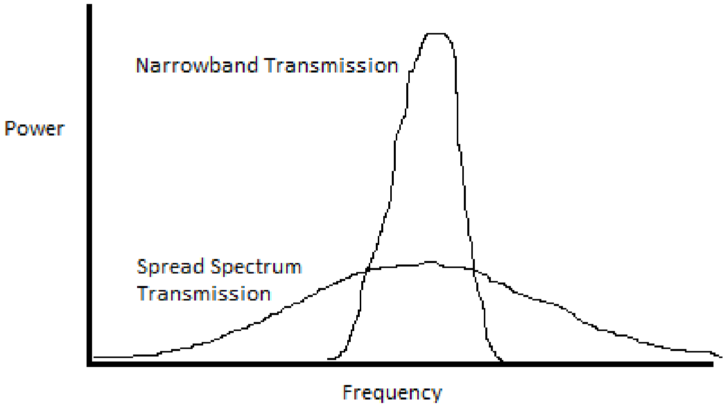
Draft Amendments

The merge of voice, data, video over wireless medium is in the works through recently ratified k, r, and coming n, and v.
802.11m: The “housekeeping” clause.
802.11n: High Throughput (HT) use of MIMO technology along with OFDM. Use of multiple receiving and transmitting antennas; takes advantage of multipath.
802.11p: Support of Intelligent Transportation Systems (ITS) apps. (Wireless in moving vehicles, future use in traffic jam alerts, collision avoidance, adaptive traffic light control, vehicle safety services, etc.
802.11s: Standardization of Wireless Distribution System (WDS) thru *Hybrid Wireless Mesh Protocol*. Includes *MAP, MPP*
802.11T: Wireless Performance Prediction (WPP), benchmarks used by independent test labs, manufacturers, end users.
802.11u:Interworking with external networks (WIEN) such as handoff to internet, cellular networks, and WiMax.
802.11v: Ability to config client stations wirelessly from a central pt of mgmt. Load balancing, ntwk selection, virtual APs
802.11w: To prevent DoS attacks by making more secure management frames.
802.11y: Standardization of shared 802.11 operation with users in the 3650 MHz-3700MHz band in USA, etc.
802.11z: Enhancements to Direct Link Setup (DLS): allows stations to bypass AP & communicate direct w/frame xchanges.
802.11aa: Enhancements for MAC for better audio video streaming; coexistence with other traffic.

CHAPTER 6: WIRELESS NETWORKS AND SPREAD SPECTRUM TECHNOLOGIES

There are two standard bands, the Industrial, Scientific, and Medical **(ISM) Bands**, and the Unlicensed National Information Infrastructure **(UNII) Bands**. In the ISM bands, there are three frequency ranges: *902-928 MHz (26MHz wide), 2.4-2.4835 GHz (83.5MHz wide)*, and *5.725-5.875 GHz (150 MHz wide)*. Most WLAN radios are in the 2.4 GHz ISM band. The UNII Bands include *UNII-1 (5.15-5.25 GHz with 4 channels)*, *UNII-2 (5.25-5.35 GHz with 4 channels)*, *UNII-3 (5.725-5.825 GHz with 4 channels)*, and *UNII-2 Extended (5.47-5.725 GHz with 11 channels)*. Each non-extended are 100MHz wide.

Transmission Methods



Narrowband: More susceptible to jamming/interference because of the narrow range of frequencies. Usually licensed by regulatory bodies so two freq. in same area are not interfering with one another. i.e. FM and AM radio
Multipath interference: Just like an echo in a canyon, it is hard to tell what person is saying if the echo interferes with the next coming word. Want the *delay spread(time difference between main and reflected signal)* to be as small as possible, otherwise transmission rate needs to slow down in order to get fewer errors. Intersymbol interference (ISI): When the delay spread is too long thus causing interference of the echo with the next piece of data.
Spread Spectrum: Less susceptible to above problem, as frequencies are more spread out.
Frequency Hopping Spread Spectrum (FHSS): Transmission includes a sequence, dwell time, and hop time. The sequence is repeated in cycles, using the same frequency sequence over and over again. Dwell time is for how long the antenna transmits the signal at a certain frequency inside of the hopping sequence. Hop Time (good if less) is how long the transmitter takes to switch from one frequency to the next within the hopping sequence. Usually “insignificant” compared to the dwell time, but it adds up, and can increase overhead. Uses Gaussian Frequency Shift Keying (GFSK) modulation to encode.
Direct Sequence Spread Spectrum (DSSS): Instead of hopping frequencies, DSSS stays in the same frequency channel. It takes a bit (1 or 0) and applies XOR to it using a *pseudo-random number (PN)* (or CCK code- more complicated, works at faster frequencies). PN represents 1 as 10110111000 and 0 as 01001000111. The advantage: up to 9 out of 11 of these “chips” can be corrupted, but de-spreader (receiving radio card) can still figure out what the original bit was from the ones not

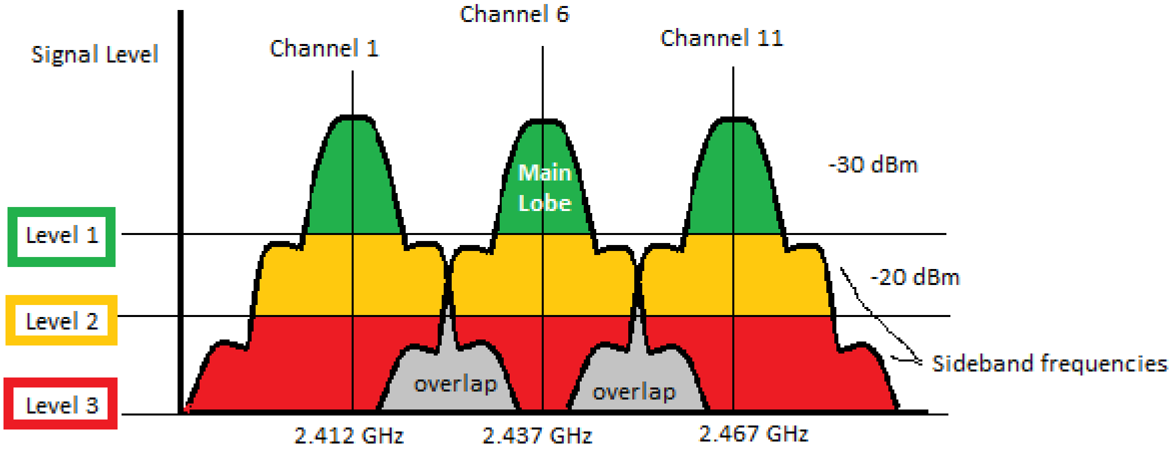
corrupted. Data rates supported: 1 and 2 Mbps. With CCK, HR-DSSS is achieved, w/data rates 5.5 and 11 Mbps. Modulation used: DBPSK and DQPSK.

Modulation Techniques: Packet Binary Convolutional Code (PBCC): Not used at enterprise level; originally defined in 802.11b, optional in g, need both receiver and transmitter to support technology.

Orthogonal Frequency Division Multiplexing (OFDM): Most commonly used in wired and wireless. Also low power, wider frequency range. Transmits across 52 subcarriers, each with a width of 312.5 KHz. Singular data rates lower, but because there are so many subcarriers, the overall DR is higher than FHSS and DSSS. Because individual data rates are lower, there's less chance of ISI. OFDM is more resistant to narrowband interference b/c of the use of error correction *Convolutional Coding*. Sometimes referred to as a spread spectrum technology, but really is different.

2.4 GHz Channels

14 ranging from 2.412 to 2.484 GHz (the center values); 1-11 are used in USA. Each is 22MHz wide, referenced by center freq ±11 MHz; clearly, overlapping occurs. Channels 1, 6, 11 do not overlap (they must be at least 25MHz away from each other not to.) It is necessary to put AP-s at least 5 to 10 feet away from each other to avoid *sideband frequency interference*:



2.4 GHz Band nonoverlapping channels - at least 25 MHz apart at Level 1: + or - 11 around center frequency.

5 GHz Channels

802.11-2007 defines the bands of 5 GHz as UNII-1, UNII-2, UNII-3, and UNII-2 Extended. 1, 2, 3 have 4 non-overlapping channels with 20 MHz separation between the center frequencies. UNII-2 ext has 11 non-overlapping channels w/20 MHz separation btw center freq. Sideband frequencies don't drop off as quickly as 2.4 GHz

Adjacent, Nonadjacent, and Overlapping Channels

	DSSS	HR-DSSS	ERP	OFDM
Frequency band	2.4GHz ISM	2.4GHz ISM	2.4GHz ISM	UNII bands
Adjacent means	≥ 30 MHz	≥ 25 MHz	= 25 MHz	= 20 MHz
Non-adjacent	N/A	N/A	> 25 MHz	> 20 MHz
Overlapping	< 30 MHz	<25 MHz	<25 MHz	N/A

Throughput vs. Bandwidth: Throughput is actually a lot lower due to CSMA/CA, at least 50% lower, especially when the medium is shared between multiple stations; i.e. multiple people are downloading a file at the same time, reduces throughput.

Chapter 7: Wireless LAN Topologies

This chapter details the following topologies, and the technologies used to pull them off.

Wireless Wide Area Network (WWAN) Covers large areas – i.e. cellular networks; technologies such as GPRS, CDMA, TDMA, GSM, data sent to PDAs, cell phones, and cellular networking cards.

W. Metropolitan Area Network (WMAN) To cover larger metropolitan areas with 802.11, especially in and around cities. Not too realistic because WiFi was never intended to be used in this way.
W. Personal A. N. (WPAN) Close Proximity communication such as Bluetooth and infrared.
W. Local A. N. (WLAN) Used in enterprises w/use of multiple access points. Provides users gateway to internet.

802.11 Topologies

Anything with a radio card is referred to as a *station* (STA); sometimes these are inside Access Points (APs). *Client Station* is radio card that is not in an AP.
The 802.11 standard defines 3 topologies known as *service sets*: Basic Service Set (BSS), Extended Service Set (ESS), and independent basic service set (IBSS)
Basic Service Set (BSS): A basic unit that makes up a wireless topology. Typically consists of 1 AP and some client stations connected to it. Stations with layer 2 connection that are part of a BSS are called *associated*.
Extended Service Set (ESS): A collection of BSSs, with or without overlapping AP coverage. With nonoverlapping coverage, when stations move from one AP to another, it is called *nomadic roaming*. Totally overlapping coverage is called *colocation,* used to increase client capacity. Network name of ESS is usually called *ESSID – technically the same thing as SSID*.
Independent Basic Service Set (IBSS): I.e. Ad-Hoc; basically peer-to-peer connections with no access point involved.

Connection types
Simplex: one radio is just receiver, one is transmitter, doesn't work other way around (i.e. FM and AM radios)
Half-duplex: both radios can transmit and receive, but only one at a time (i.e. 802.11 wireless networks, walkie-talkies)
Full-duplex: both radios can transmit and receive at same time (i.e. telephone conversation)

Access Point: Half duplex device with switch-like intelligence (autonomous AP), or half-d lightweight AP(controlled by remote from a WLAN controller) These keep track of MAC Service Data Unit (MSDU)

Integration Service (IS): delivery service of MSDUs btw distribution system and non 802.11 LAN. Basically the job of IS is to effectively transfer 802.11 data frames into an 802.3 Ethernet frame (generally), but could be between wireless and token ring.
Distribution System (DS): to interconnect set of BSSs via integrated LAN to make an ESS. Components: *Distribution System Medium (DSM)*: connects access points (most common is 802.3), and *Distribution System Services (DSS)*: connects client stations; uses layer 2 addressing to eventually forward layer 3-7 info to IS or another wireless client station.
Wireless DS: replacing the standard 802.3 backbone, it is possible to use wireless backbone to connecting APs (Called *wireless backhaul*); can use *single or dual radios*, as well as repeaters for connection of APs. Single radio can decrease throughput because 802.11 is a half-duplex medium, thus when APs are talking to each other, client stations are turned away from communicating. On contrary, dual radios (using 2.4GHz and 5GHz antennas simultaneously avoids this half-duplex problem). *Repeaters* extend service to places that an AP may not reach. Repeater is not connected to backbone. However, it also add extra overhead/extra hop; usually not as effective for real-time applications.
Service Set Identifier (SSID): Logical name used to identify a 802.11 wireless network. Max 32 characters and is case sensitive. Admins can cloak SSID so the name is hidden from nonlegit users, but is not a very strong security measure at all.
Basic Service Set Identifier (BSSID): basically another name for the Layer 2 MAC address of an AP provided by the hardware manufacturer.
Basic Service Area (BSA): Physical Area of Coverage provided by AP. Some APs can move between data rates known as *dynamic rate switching*. Size and shape of BSA depends on power, gain of antenna, and physical surrondings.
Basic Service Set (BSS): A basic unit that makes up a wireless topology. Typically consists of 1 AP and some client stations connected to it. Stations with layer 2 connection that are part of a BSS are called *associated*.
Extended Service Set (ESS): A collection of BSSs, with or without overlapping AP coverage. With nonoverlapping coverage, when stations move from one AP to another, it is called *nomadic roaming*. Totally overlapping coverage is called *colocation,* used to increase client capacity. Network name of ESS is usually called *ESSID – technically the same thing as SSID*.
Independent Basic Service Set (IBSS): I.e. Ad-Hoc; basically peer-to-peer connections with no access point involved.

802.11 Configuration modes

AP modes: Root mode (only one in the 802.11 standard) other nonstandard ones available: Bridge mode, workgroup bridge mode, repeater mode, scanner mode.
Client Station modes: Infrastructure: the most common; used when connecting to an AP. OR Ad Hoc mode: for participation in IBSS topology.

The **Mathias Paper** was an analysis of different kinds of interferences in a typical WLAN network using a microwave, cordless phone, Bluetooth technology, and a video camera, among others. They found that the worst offender (obliterating throughput of the WLAN) was the TDD cordless phone. The video camera was the next worst offender, especially in short range interference. In conclusion, they say that although interference is a problem, and is likely to become more of a problem as more and more devices take to the air, it is something that WLANs will learn to deal with, and won't cause the death of WLANs.

CHAPTER 8: MEDIUM ACCESS

CSMA/CD: Carrier Sense Multiple Access /Collision Detection
Used in Ethernet networks. A contention method for packets entering the shared access medium; Collisions are actually detected and packets resent.
CSMA/CA: Carrier Sense Multiple Access /Collision Avoidance
Less known, used in Wireless network; difference is that Collisions are merely assumed to have happened when an ACK message doesn't make it back to the sender. Is a result of the half-duplex nature of 802.11. STAs are constantly listening for transmission (when in active mode) in medium, when determined that no other stations are transmitting, it chooses a random back-off value before beginning transmission. All Unicast 802.11 Frames must be acknowledged by receiving radio. In case of corruption the CRC fails and no ACK is sent to transmitting radio. Frames that do not need acknowledgement: Broadcast and Multicast frames.

Distributed Coordination Function (DCF) Mandatory access method for 802.11 standard
Interframe Space(IFS): Short period of time that exists between frames during wireless transmission.
Short Interframe Space: Highest priority; comes before an ACK.
DCF interframe Space: Most common besides SIFS, is used for most other 802.11 frames.
Arbitration IS: used by QoS Stations
Extended IS: Used with retransmissions
Shortest to Longest time period *SIFS*<PIFS<*DIFS*<AIFS<EIFS
Duration/ID Field: in the 802.11 MAC header, indicates how long RF Medium will be busy with transmission of following data. Used to reset NAV timers of other STAs +Legacy power management.
Virtual Carrier Sense: Uses timer mechanism called network allocation vector (NAV) used as count-down timer. Medium is assumed to be busy until timer reaches 0. Considered "First line of defense for carrier sense (when is medium busy)."Layer 2 (OSI) of defense.
Physical Carrier Sense: The constant monitoring of medium. Purpose is (a) see if frame is incoming (b) to determine if medium is busy before transmission; known as *clear channel assessment (CCA)*. Layer 1 line of defense.
V and P Carrier Sense always happening concurrently
Random Back-Off Timer: A randomly chosen amount of time between 0 and a predetermined contention window called back-off value; is multiplied by the slot time. This sets off the Back-Off Timer. After time is up, reassessment of medium follows; if still busy, process is repeated.

Point Coordination Function (PCF): Optional for 802.11. AP acts as Point Coordinator (PC), all STAs must support function. Polls the clients in PCF mode about intention to send data to prioritize clients. Known as *contention-free period(CFP*); otherwise when in DCF it is known as *contention period (CP)*.

Hybrid Coordination Function (HFC): Combination of DCF and PCF, created two channel-access methods
Enhanced Distributed Channel Access (EDCA): Extension of DCF; uses 8 user priority levels. Uses 802.1D priority tags, defines 4 access categories based on user priorities: AC_VO (Voice), AC_VI (Video), AC_BE (Best Effort), AC_BK (Background). Higher priority has lowest back-off values, so most time to get at transmitting or TXOP
Controlled Channel Access (HCCA): Uses Hybrid Coordinator (HC) that is a QoS-aware coordinator. Built into the access point and can allocate TXOPs to itself or other higher-priority stations.

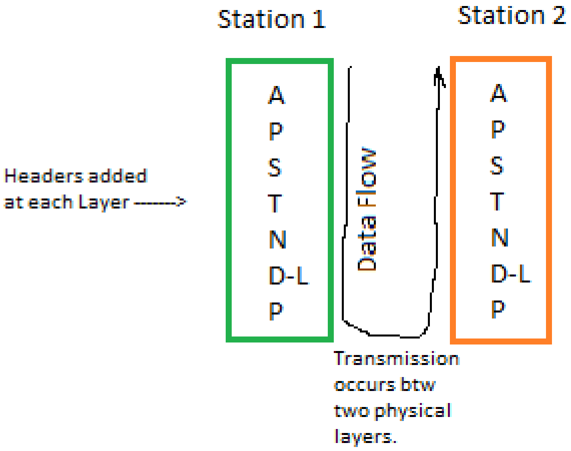
Block Acknowledgement (BA)
Under the 802.11e amendment, defined in 802.11-2007 standard. 2 kinds: Immediate for low-latency traffic, and Delayed for latency-tolerant traffic. The Block ACK is more efficient and cuts down on overhead caused by contention for the medium by putting multiple ACKs into one frame.

Wi-Fi Multimedia (WMM)

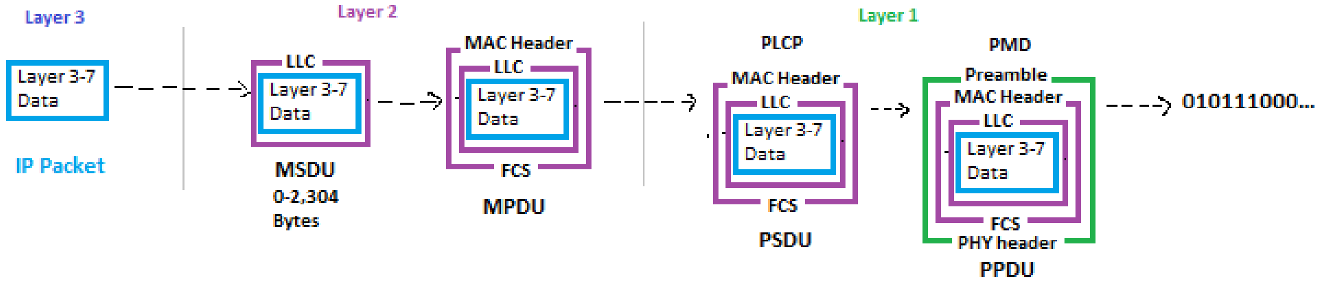
In order to meet QoS requirements for low-latency applications like VOIP, the 802.1D priority tags from Ethernet are passed into the same four categories, each marked with a tag: WMM Voice with 6,7; Vid Priority (Like HDTV video streams): 5,4; Best Effort (i.e. Internet browsing): 0,3 ; Background priority(file transfers/print jobs): 2,1.

CHAPTER 9: 802.11 MAC ARCHITECTURE

As data travels down OSI model to eventually be transmitted, each layer adds header information, then after transmitted is "decapsulated" layers 4-7 encapsulated into an IP packet, then at DL layer, MAC header added and then encapsulated into a frame. Last header to be added is at the Physical Layer.



The Data-Link Layer has MAC, Logical Link Control sublayers.
Frames from IP packet to bits:



802.3 to 802.11
802.3 has max frame size of 1,518 bytes; an 802.11 frame may be too large for 802.3 medum.
802.3 has only Source Address and Destination Address in header, 802.11 has Frame control, Duration/ID, Sequence ctrl, and QoS control in the header, along with 4 MAC addresses: Receiver Address, Transmitter Address, BSSID, and Destination Address.
802.11 Frame types:
Management Frame: Makes up majority of frames. They do not carry upper-layer (3-7) information. Used by stations to Join or Leave a BSS. Only exist in wireless networks because it is an unbound medium. 12 Subtypes*: Association request & response (second step in connection to a network), Reassociation request & response (used during roaming; should happen invisibly to user), Probe request & respond (part of active scanning), Beacon, Announcement Traffic indication message (ATIM), Disassociation (notification, cannot be refused), Authentication (first step in connecting to a network), Deauthentication(notification, also causes disassociation), Action.*
Control Frame: Assist with delivery of data frames. Transmitted at one of the basic rates so that it can be heard by all stations; they contain only headers. *8 Subtypes: Power Save (PS)-Poll, Request-to-Send(RTS), Clear to Send (CTS), ACK (Contains FC, Duration, Receiver address, FCS), Contention Free (CF)-END [PCF only], CF-End + CF-ACK [PCF-only], Block ACK Request [HCF], Block ACK [HCF].*
Data frames: These carry actual data from layers 3-7. 15 Subtypes, Important ones*: Data (simple data frame), Null function (no data-indicates power save status change)*
Fragmentation of frames adds overhead but if interference occurs, it can reduce retransmission overhead. Fragmentation is thus more useful in a more interference-prone environment.

ERP Protection Mechanism used for seamless coexistence btw 802.11 g, b and legacy DSSS devices. In mixed mode environment, a RTS/CTS or CTS-to-self is sent to all stations so that even the legacy ones can understand and reset NAV timers to avoid collision. Then data intended for g STAs is sent at faster rates when CTS-to-self is used usually by an AP; throughput is higher because fewer frames are sent.

Power management

Traffic Indication Map (TIM) A field that is changed to 1 when STA in BSS changes to Power Save Mode (Wireless card takes a nap). Information intended for that STA is stored in a buffer until it changes back to 0 or it sends a PS-Poll frame. When there is stuff in the buffer for that client taking a nap, its AID is inside the AP's TIM, so the station knows to send the PS-Poll frame to receive the data.

Delivery Traffic Indication Message (DTIM) Used when there needs to be a Multicast or Broadcast sent out, and causes all the clients to eventually wake up to receive the message in time.

Announcement Traffic Indication Message (ATIM) Used in an IBSS only, serves similar purpose to TIM in a BSS.

WMM Power Save (WMM-PS) Goal is to have clients in doze (power saving) state to save power instead of legacy "ping pong" with TIM, PS-Poll, ACK, Data transfer, more ACK, etc at random times. Instead WMM sends trigger frames eliminating need for PS-Poll Frames

CHAPTER 10: WIRELESS DEVICES

WLAN Client Devices: Half-Duplex radio transceivers come in many flavors, and work on one or more OS's. Different drivers are needed for most of them; usually malfunctioning radio is caused by corrupt/bad driver.

Radio Cards

Used in all kinds of stations, come in many sizes, connect to multiple I/O devices. Most widely used: Mini PCI. Almost any laptop out there has one integrated into it. PDAs need smaller, lower power card formats such as SD & *Compact Flash* (CF). PC adapters used in desktops, can have extendible antenna, or USB interface.

Client Utilities – the software that finds and manages networks, as well as configures WLAN card.

4kinds: SOHO, Enterprise-class utilities (more configurations available), Integrated Operating system utilities, third party client utilities (usually costs xtra $).

WLAN Architecture

Autonomous AP – intelligent edge architecture

Have radio card and Ethernet port. It is capable of configuration alterations, management. Also called "fat AP" or "stand-alone AP;" they have many capabilities including WPA2 security, PoE, Adjustable transmit power, multiple mgmt interfaces.

Wireless Network Management System (WNMS)

To manage large number of APs, can control autonomous APs too, can have RF spectrum mgmt and planning, as well as intrusion detection. However, does not help in roaming like a WLAN controller does.

Centralized WLAN architecture and Lightweight APs

Limited software capabilities connected to a central system. APs work faster not bogged down by all the stuff an autonomous AP would have to do.

WLAN Controller

"Wireless Switches" operate at Layer 2 of OSI, but can also route traffic at the Network Layer. They have many roles: AP management, 802.11 traffic tunneling (sending an 802.11 frame through Ethernet using Generic Routing Encapsulation (GRE); the Protocol can create an IP tunnel making a p2p link btw lightweight AP and WLAN controller. AP group profiles, WLAN Profiles: Multiple WLAN profiles can be supported by 1 AP, however, an AP can alone belong to one AP group. Virtual BSSID: To create wireless VLANs even when there is only 1. User Mgmt, Layer 2 security, automatic load balancing, WIDS, Dynamic RF spectrum mgmt., Bandwidth management, Firewalls, Layer 3 roaming support, PoE

Split MACMAC layer services could be split between controller and AP

Remote Office WLAN Controller To allow remote and branch offices to be managed from central location. Communicates with central WLAN controller over a WAN link. Only allows for small no of lightweight APs.

Distributed WLAN Architecture

Scalability schema: adding multiple WLAN controllers, each in control of a group of APs. This lets us add more APs, and also will provide more gateway and network resources (less overhead)

Distributed WLAN Hybrid WLAN controller that controls both fat and thin APs

Unified WLAN Architecture: make wired devices at core or edge have WLAN controllers, combining the two networks.

Specialty WLAN Infrastructure

Wireless Workgroup Bridge (WGB): connects wired devices and collectively provides wireless access to them by joining them to a BSS as a client station. The WGB does not provide connectivity to other clients, only acts as a liaison between AP and wired devices. Only the WGB participates in CSMA/CA, medium contention, the wired clients do not do this individually.

Wireless LAN bridges: Provides connectivity between 2+ wired networks. Can be used in or outdoors (more common). Bridges can have other modes: AP mode, WGB mode, Repeater mode, Root with clients, Nonroot with clients. The last two are not encouraged since they are a security issue and they can cause unnecessary overhead. Problems: long P2P links can cause ARP timeouts, or are placed too high for the omnidirectional antenna to reach lower altitude.
Enterprise Wireless Gateway:Legacy Middleware device used to segregate autonomous access points from protected wired network infrastructure.
Residential Wireless Gateway:Aka: home wireless router. Not very expensive but have many features such as: configurable 802.11 radio card, simple routing protocols, NAT, Port AT, Firewall, L2 security WPA2, DHCP.
VPN Wireless Router:Similar as the home router, but can support VPN protocols, typically used as edge routers in remote/branch offices to connect to the main/central office.
Wireless Mesh Access Points:Wireless APs communicating with one another using layer 2 routing protocols creating a self-forming and self-healing infrastructure. Usually 5GHz are used for this purpose, while 2.4 GHz radios used to provide connectivity to clients.
Enterprise Encryption Gateway(EEG): Middleware device that divides encrypted network side and unencrypted other side. APs managed from unencrypted side.
WLAN Array: Combination of a WLAN controller and multiple access points in one hardware device.
Cooperative Control: Autonomous AP combined with *cooperative control* protocols to eliminate need for WLAN controller.
Virtual AP system: Multiple APs advertising only one MAC address, makes for zero handoff during roaming,no latency issues.
Real-Time Location Systems: using APs as sensors to track where a piece of equipment is. Useful in hospitals and RTLS application that provides detailed maps of where the radio is; Kind of like GPS but locally?
VoWiFi: *Phones* supporting 2.4GHz (and more recently 5GHz), now developing OFDM on VoWiFi phones to replace HR-DSSS.

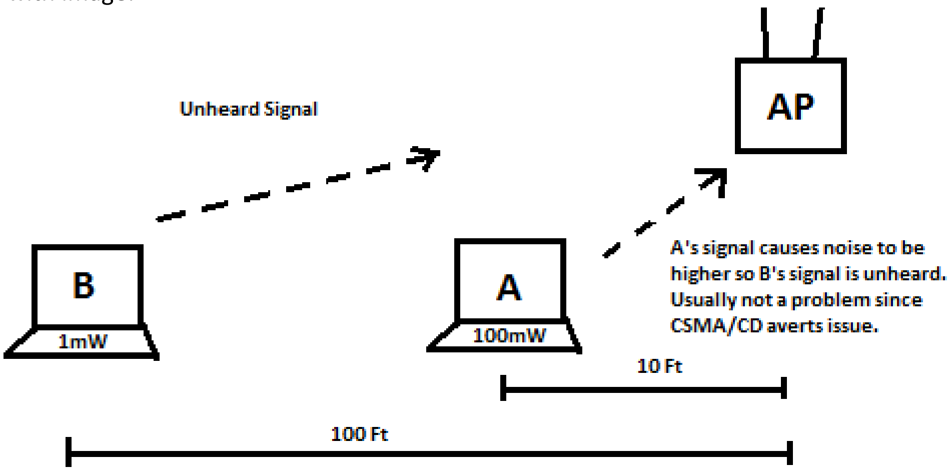
CHAPTER 11: WLAN DEPLOYMENT AND VERTICAL MARKETS

This chapter explores many markets where Wireless is an opportune solution versus wired. Generally, the reasons are for mobility, less cables thus easier installation and repair and aesthetics. However, they are not as good in performance and throughput. Wireless should only be used for Access layers, not core except for building to building bridges.
Markets: Network extension to remote areas, bridging-building-to-building connectivity (other solutions include installing underground copper wire, or pay for high speed leased lines), Last mile delivery, SOHO, Mobile offices (temporary situations or highly mobile ones like military maneuvers), Classroom use, Warehouses in industrial/manufacturing sector, Healthcare in Hospitals, and Offices, Municipal networks (most have failed, only used in smaller radius town centers), Hotspots, free or using *captive portal*s that require logon to access any webpage, Transportation (trains, buses, airplanes), Law Enforcement Networks (security!!), First Responder Networks, Fixed Mobile Convergence (Phones that can migrate from 802.11 to cellular coverage seamlessly).
WHO has established that RFs used for 802.11 are too weak to cause any negative effects on health.
List of Vendors for all kinds of services such as Security, Troubleshooting, Mesh networking solutions, etc.

CHAPTER 12: WLAN TROUBLESHOOTING

Layer 2 Retransmissions cause decrease in throughput by increasing overhead, and also timely delivery of critical applications like VoIP become delayed thus causing a negative user experience (*jitter*: caused by delay in delivery, measure of how much delay varies from the average, *Latency*: time it takes to deliver a VoIP packet from source to dest., ultimately these cause jumps in flow of data and reduced battery life.)
Causes of retransmissions:
RF interference (a) Narrowband: Not cause DoS, but high amplitude and disrupt in a specific channel or channels. (b) Wideband: Can jam all channels in an ISM band. (c) All-band interference: usually caused by FHSS because it hops all over the place. Older Bluetooth caused this type of interference.
Multipath causes interframe symbol interference (ISI) thus corruption which leads to retransmissions. Can be compensated for by using antenna diversity, multipath is something that can't always be fixed because it is caused by the physical environment; i.e. reflections and refractions off walls, ceilings, shelves, etc. Now MIMO is a fix for this too, actually taking advantage of these reflected signals.
Adjacent Cell Interference Use of channels too near each other within a ISM band, causing interference of one channel on the next. Aka: overlapping channels
Low SNR Background noise too close to the received signal or the signal is too low, thus too close to the noise floor. Signal-to-Noise-Ratio is not actually a ratio; it is the difference in dB between received signal and background noise (aka noise

floor). The lower the number of SNR, the more retransmissions occur. SNR of 25+ is very good, SNR of 10dB or less is bad. Recommendation is 18 to 25 dB SNR.
Mismatched Power settings between client and AP; most commonly, it occurs when client can hear AP, but AP can't hear client. To fix, make sure AP's power is same as clients' or make the AP's power the same as the lowest powered client. Way to detect: using a protocol analyzer, frame retransmissions of client STA are corrupted when listening near the AP, but not when you listen near client. Increasing range of AP is usually done by putting AP to full power, but best solution is not that, but increasing antenna gain of AP, which takes advantage of *Antenna reciprocity*.
Near/Far explained with image:


AP
Unheard Signal
B
1mW
A
100mW
A's signal causes noise to be higher so B's signal is unheard. Usually not a problem since CSMA/CD averts issue.
10 Ft
100 Ft

Hidden Node A wall or other object "hides" transmissions of 1 client from other ones, thus collisions occur when both try to transmit at the same time. Solution: disable 1 and 2 mbps data rates of AP, try lowering the RTS/CTS threshold on a suspected hidden node to about 500bytes or so, Remove obstacles, move the hidden node STA, and even add another AP if the previous things don't help. Detection if retransmission rate of one STA is way higher than all of the other stations' retransmission rates.

Coverage Considerations

Dynamic Rate Switching: Also called adaptive rate selection, automatic rate selection. As an AP moves away from AP, it dynamically lowers bandwidth capabilities. Algorithms used for this are proprietary; usually based on RSSI thresholds, packet error rates, and retransmissions. Turn off 1, 2 Mbps to avoid slow connection by closer clients because so many clients farther away are occupying medium for longer.
Roaming: The proprietary nature and the environment can cause roaming hiccups. Client stations make the decision on whether to roam or not. Recommended 15-25% overlap between APs for seamless roaming. Too much overlap is not good either because then client will roam too often, or switch between APs when it isn't really necessary. Authentication process can take 700 milliseconds or more, but seamless VoWiFi requires 150 milliseconds or less when roaming. *Fast Secure Roaming (FSR):* solution to use when 802.1X/EAP security and time-sensitive apps are used.
Layer 3 Roaming: roaming between two access points that are on different subnets, requiring client to acquire a different IP address. VoIP would disconnect in this scenario. Only way to maintain connectivity in this case is either with a Mobile IP solution or proprietary layer 3 roaming solution.
Co-channel interference: adjacent APs configured on the same channel, creating unnecessary medium contention overhead.
Channel Reuse/Multiple channel architecture: Use a tessellation of channels within a network to reduce co-channel interference.
Single Channel Architecture: Many APs on the same channel, but all of them use the same SSID so client thinks it's connected to the same AP even though it may be "roaming" from one AP to another. These roams are handled by a central WLAN controller. Each AP has its own MAC address on the radio card, but they share 1 virtual MAC address. Advantage: 0 handoff time, thus no latency issues associated with roaming; great for VoWiFi and 802.1X/EAP solutions; also, adjacent cell interference no longer an issue.

Capacity vs. Coverage

Legacy method: fewer APs set to maximum level. Now: more APs with lower levels (cell sizing) to provide for capacity.
Colocation: Placing multiple APs in the same physical space to provide for more capacity (each one on a different channel). APs should actually be physically separated by 15 feet to avoid sideband interference; useful in really crowed situations like a university lecture hall.
Colocation with a single channel architecture: channel stacking where each level can be a different channel in a multiple story building.

Oversized Coverage Cells: problem caused by max range settings on AP but will not meet capacity needs, and can cause hidden node problems, as well as co-channel interference; increase antenna gain instead.

Voice vs. Data

IP Voice (Canary)	IP data (cockroach)
Small, uniform-size packets	Variable size packets
Even, predictable deliver	Bursty delivery
Highly affected by late or inconsistent packet delivery	Minimally affected by late or inconsistent packet delivery
"Better never than late"	"Better late than never"

Performance the following can affect the range of a WLAN
Transmission power rates, Antenna gain, antenna type, wavelength, free space path loss, physical environment, CSMA/CA, Encryption, application use, # of clients, Layer 2 retransmissions.

Weather Lighting can fry equipment, Wind shifting highly directional antennas, Precipitation can cause RF attenuation and damage to equipment, Air stratification (change in air temps can cause refraction), UV/sun can damage cables over time.

Chapter 13: 802.11 Network Security Architecture

Required for Adequate Security

Data privacy: Encrypting the data streams; there are multiple cipher encryptions. Most common: RC4 algorithm (Used in TKIP and WEP), Advanced Encryption Standard (AES) algorithm (Used in CCMP). Encryption happens in a continuous stream or in blocks.

AAA

Authentication: Verification of User identity and credentials. Use of username/password is most common. There's also verification by digital certificate or by multifactor authentication where there are multiple credentials required.

Authorization: Granting access to network. Authentication must always happen before authorization.

Accounting: Tracking network use, like a video camera in front of a store.

Segmentation: Separation of users into separate groups, achieved through firewalls, routers, VPNs, and VLANs. Most common: layer 3 segmentation using VLANs. Also through role-based access control.

Monitoring and Policy: Implementing a schedule and set of rules to maintain the WLAN using wireless intrusion detection systems (WIDS).

Legacy 802.11 Security

Legacy Authentication: Open (let anyone into network) and Shared Key (very insecure key sent in cleartext, then encrypted).

Static WEP Encryption: *Wired Equivalent Privacy*. Layer 2 encryption, uses RC4 cipher using 64 or 128 bit. Each has a 24-bit Initialization Vector which is sent in cleartext. The rest of the bits are utilized in a 40-bit static key, which must match on both the AP and client STA. How it works: a CRC is run on plaintext data, attaches *Integrity Check Value* (ICV) to the end, 24-bit cleartext IV is generated and combined with static secret key. The static key and IV run through pseudorandom algorithm that generates a keystream which is equal to length of plaintext data, which is then combined with the data using Boolean/XOR logical process. The result is encrypted data, which is prefixed with IV before sent off.

WEP is susceptible to many attacks including IV collisions attack, weak key attack, reinjection attack, bit-flipping attack.

MAC Filters: MAC addresses can be spoofed thus appearing to be another client that may have more credentials in a network than the actual machine hiding behind the fake MAC address, thus let into a "filtered area".

SSID Cloaking: When broadcasting a network, the AP cloaks, or hides the SSID, which makes it harder for the client station to associate to the network. This really doesn't do much; it just takes extra steps to find the SSID of a network. Perhaps just prevents any non-hacker from associating with network.

Robust Security

Requirement of 802.1X/EAP authentication method in an enterprise, and use of preshared key or password in SOHO. CCMP/AES default, TKIP/RC4 optional.

Robust Security Network (RSN): 2 STAs to establish authentication procedure then associate with each other, as well as make dynamic encryption keys through a process known as 4-Way handshake..

802.1X/EAP Framework: A port-based access control standard. Basically it allows or denies traffic to pass through a port based on credentials, content. Does not require encryption

Supplicant: Host that requests authentication and access to the specific network, each has a unique id credential to be verified by the server. I.e. desktop host

Authenticator: The Device that allows or denies traffic through a port. EAP Authentication traffic is generally always allowed through the uncontrolled port; the controlled port blocks all other traffic until supplicant is authenticated. I.e. managed switch.

Authentication Server (AS): Server that validates supplicant's credentials. Notifies authenticator that supplicant has/has not been authorized. The server maintains a database locally or through a proxy to authenticate credentials. I.e. RADIUS server.

EAP Types: Extensible Authorization Protocol is layer 2 protocol, very flexible with multiple flavors. LEAP (cisco proprietary), PEAP (protected extensible..), one-way/two-way validation.

Dynamic Encryption-Key Generation: generation /session/user. Dynamic WEP was used before WPA came along, was a by-product of EAP authentication process. Still better than static; if compromised, only 1 user's traffic could be decrypted.

4-Way Handshake: The last 4 frames exchanged during EAP or PSK authentication.

WPA/WPA2-Personal: For networks without a RADIUS server. Involves matching passphrases on the AP and client stations to associate; the passphrase is converted into a Pairwise Master Key (PMK) which is then used with the 4-Way Handshake. Involves heavy admin overhead, could have social engineering problems with compromise of passcode and should be avoided in enterprise environment.

TKIP Encryption: An enhancement of WEP. 128-bit temporal key combined with 48-bit Initialization Vector (IV), src, dest MAC addresses in a process known as per-packet mixing. Uses a stronger integrity check known as MIC. Total of 20 bytes of overhead.

CCMP Encryption: Counter mode with Cipher Block Chaining Message Authentication Code Protocol. Uses Advanced Encryption Standard (AES) algorithm (Rijndael Algorithm) with 128-bit encryption-key size, and encrypts in 128-bit blocks. 8-byte MIC is used (much stronger than for TKIP). Extra 16 bytes of overhead.

Segmentation: Key part of network DESIGN.

VLANs: For separate broadcast domains in layer 2 network; used to restrict access to nwk resources w/o regard to physical topology of network. Individual SSIDs mapped to each VLAN; users can be given different SSID /VLAN pairs (w/varying security settings) while still going through the same AP. Common use is separate VLANs for Guest, Voice, Data access.

RBAC: *Role based access control* is an approach to the restriction of system access to authorized users. Components- Users, Roles, Permissions (layer 2 [MAC filters], L3 [Access Ctrl Lists], L4-7 [stateful firewall rules, time, and bandwidth permissions). Permissions can be mapped to roles; users can be assigned to roles. Through authentication to network, they inherit permissions of the role they are assigned to.

Infrastructure Security

Physical Security (locks on APs in boxes, enclosure units around cables or jacks.)

Infrastructure Security: unused interfaces should be turned off, passwords to be changed from factory defaults, use encrypted management capabilities, practice configuring devices from only wired side, not wireless (more secure, and less chance of locking self out).

VPN Wireless Security

Not recommended for use in wireless security, 2 types: router to router and client/server based. Mandatory for remote access usually coupled with a firewall when using VPN in public networks.

Layer 3 VPNs: Provide encryption, encapsulation, authentication, and data integrity. VPN uses *secure tunneling* (encapsulating an IP packet within another IP packet). The original dest and src IP address of 1st packet is encrypted with the data. Technologies include *Point-to-Point Tunneling Protocol (PPTP)* and *Internet Protocol Security (IPSec) –Supports DES, 3DES, AES ciphers*. PPTP uses *MPPE (Microsoft P2P Encryption)*-uses RC4*, MS-CHAP for authentication which is vulnerable to dictionary attacks*, used in SOHO environments.

CHAPTER 14: WIRELESS ATTACKS, INTRUSION MONITORING, AND POLICY

Wireless Attacks: risks are access to insider databases, corporate trade secrets, personal health info, as well as damage of network resources, software theft, remote hacking.

Rouge Wireless Devices | *Rouge AP*: any Wi-Fi device that is connected to the wired infrastructure but not under management of proper network admins. It may be employees unknowingly creating this risk by plugging in an AP unsecured by default. Or an AdHoc network with one node connected to a wired portal. With 802.1X, an AP that plugs into the wired infrastructure must be authenticated into the network before it is granted access.

Peer-to-Peer Attacks | These can occur within an IBSS where a peer has access to any resource available on the connected computer, or within a VLAN on a BSS because they can share layer 2 and 3 domains, unless they are disabled by routing traffic through L3 switches. Or use of *Public Secure Packet Forwarding (PSPF)* enabled on APs to block wi-fi clients to communicate with other STAs on same VLAN. However, this will disable push-to-talk multicasting for VoWiFi to work.

Eavesdropping | Listening in on wireless transmissions; if not encrypted can be read. *Casual Eavesdropping*: harmless, known also as *wardriving*: looking for wireless networks, usually while in moving vehicle. Common freeware tool: NetStumbler. *Malicious Eavesdropping*: unauthorized use of protocol analyzers to capture wireless communications, considered illegal by wiretapping laws. Cannot be detected by WIDS because of the passive nature of PAs which is why TKIP or CCMP is highly suggested so any eavesdroppers can't reassemble emails, VoIP packets, etc.

Encryption Cracking | Mainly concerning WEP encryption.

Authentication Attacks | some versions of EAP can be cracked using offline dictionary attacks (LEAP). Once they get the password, attacker can impersonate user by authenticating under his/her name. WPA/WPA2-Personal also vulnerable to offline dictionary attacks; when password is compromised, it can lead to easier discovery of the generated TKIP or CCMP encryption key, as well as the Pairwise Master Key (PMK).

MAC Spoofing | Windows lets you edit the wireless card's MAC address through the registry or in device manager, as well as using 3rd party utilities. Then the computer can impersonate someone's whose MAC is authenticated in the network.

Managing Interface Exploits | Access to Devices through web interface, command line interface, serial port, console connection, Simple Network Management Protocol need to be either turned off if not used, or secured with long, complicated passwords and secured with HTTPS if available. Attacks of this sort can cause DoS or cause software changes that make hardware useless.

Wireless Hijacking | is usually easiest to configure on an unsecured hotspot. *Evil Twin Attack*: A laptop configured as an AP with same SSID as the real network, sends deauthentication packets that causes clients to roam to the Evil Twin, whereupon the attacker can execute peer-to-peer attacks on hijacked computers. *Man-in-the-Middle Attack*: On top of hijacking, this one configures a second wireless card to connect to original hot-spot, then to the evil twin. This way, the victims are rerouted back to the original gateway, thus making the man-in-the-middle virtually undetectable. *Wi-Fi-Phishing Attack*: Adding on to previous situations, the Phishing occurs when the attacker displays a fake, but identical looking gateway as the original hotspot had and asks for login and credit card information. Only way to prevent hijacking is through mutual authentication methods such as 802.1X/EAP.

Denial of Service (DoS) | Disabling of Wireless network through Layer 1 (Jamming attacks) or Layer 2. Intentional Jamming: Use of signal generator to cause interference in unlicensed frequency space. Unintentional Jamming: more common; can be caused by microwave ovens, cordless phones, video cameras. To detect; use a spectrum analyzer. L2 DoS usually come from hackers: spoofing diassociation/deauthentication frames repeatedly, or sending authentication/association floods, PS-Poll floods, virtual carrier attacks. Protocol analyzer or Wireless IDS can be used to detect layer 2 attacks. To prevent: Physical security; i.e. Barbed wire and guard dogs ☺

Vendor-Specific Attacks | Caused by firmware code holes in proprietary equipment.

Social Engineering | Technique used to manipulate people into divulging confidential information like passwords.

Intrusion Monitoring

Wireless Intrusion Detection System (WIDS) | Should be implemented when there is no official Wi-Fi network installed. Best at monitoring L2 attacks and WIDS can have alarms for many potential security risks. False positive are often a problem, thus proper policies and thresholds need to be defined. WIDS can also have performance-monitoring capabilities, alerting admin of excessive bandwidth use or excessive reassociation/roaming of VoWiFi phones.

Consists of client/server model with 3 components:

WIDS server: central pt of mgmt

Management consoles: Software-based mgmt. consoles that connect to WIDS server as clients; can (and should) be used 24/7 for monitoring of wireless networks

Sensors: Hard/Software –based sensors placed strategically to listen to and capture all 802.11 communications; usually are radio devices in a constant listening mode as passive devices.

Models that exist:

Overlay: Employed onto an existing wi-fi network; more expensive in general, extensive features, components are not a part of the WLAN that provides access to clients.

Integrated: WLAN integrated with WIDS. Wireless controller also acts as centralized IDS server, lightweight access points can be configured in full time sensor-only modes; can act like part-time sensors. Less expensive but may not have all capabilities as an Overlay model.

Integration Enabled: Wi-fi vendors sometimes integrate AP and mgmt. systems with major WIDS vendors. Light-weight APs in WLAN can be converted into full-time sensors that communicate directly with a separate WIDS server, and no longer communicate directly with WLAN controller; The integration-enabled WIDS server can then communicate directly with the WLAN controller to get stats from sensor APs.

Wireless Intrusion Prevention System (WIPS)

Infrastructure Device: Client/AP that is authorized member of company's wireless network.

Unknown Device: Assigned automatically to any new 802.11 radios detected but not classified as rogues. These are considered interfering devices and usually investigated further to identify any potential future threat.

Known Device: any client/AP detected by WIPS and identity is known. Initially considered an interfering device, then manually assigned by admin to radio devices of neighboring business that are not considered threats.

Rogue Device: Client/AP that is considered interference and potential threat. After identification of such a device, WIPS can effectively mitigate an attack, usually by creating a DoS attack on the rogue device, or by using the SNMP and disabling the managed switch port that is connected to the rogue AP.

*Note a WIPS can't detect everything; a common hacker strategy is to enable a rogue device on 2.4 GHz channel 14, which is not permitted in most countries.

Mobile WIDS: Advantage is that after detection, the mobility allows the rogue AP to be tracked down immediately.

Spectrum Analyzer: Tool that can detect RF signal in a specific frequency range; they can detect both intentional and unintentional jamming devices, and can sometimes classify the device. SAs are usually stand-alone mobile solutions, but can also be integrated with a WIPS.

Wireless Security Policy Absolutely needed along with any WIDS or WIPS or any security protocol, otherwise there is no real point in the latter.

General Security Policy | Establishment of why a wireless security policy is needed. Items involved:

Statement of Authority: who put wireless policy in place, who backs the policy.

Applicable Audience: Defines who the policy applies to, such as employees, visitors, contractors.

Violation Reporting Procedure: Defines specifics of enforcement, what happens in case of violation, and who is in charge of the enforcement.

Risk Assessment and Threat Analysis: Identifies risks and threats, and what kind of loss is possible if a successful attack is launched.

Security Auditing: Identifies auditing procedures.

Functional Security Policy | The technical aspects of wireless security; how it will be implemented

Policy Essentials: Basic procedures i.e. passwords policies, training, and proper use of wireless ntwk

Baseline Practices: minimum wireless security practices i.e. config checklists, staging, testing procedure.

Design and Implementation: Actual authentication, encryption, segmentation solutions to be put in place.

Monitoring Response: Wireless intrusion detection procedures, definition of response to alarms.

Legislative Compliance | Governmental agencies usually have a policy set for them; in the US, NIST maintains the Federal Information Processing Standards (FIPS). The standards define things like security modules for cryptography. Other legislative policies:

HIPAA Health Insurance Portability and Accountability Act: Standards for electronically transferred health records, and national standards for insurance providers, insurance plans, etc. Goal is to protect patient information and maintain privacy.

Sarbanes-Oxley: Auditing procedures, goal of corporate responsibility and financial disclosure.

GLBA The Gramm-Leach_Bliley Act: Requires banks and financial institutions to notify customer of any policies and practices that may disclose customer info. Goal: to protect SSNs, Credit card no. addresses, other private information.

802.11 Policy Recommendations

Remote-access WLAN policy | When accessing network remotely, ensure proper securities are in place such as VPNs, firewalls. Most needed in public-access hotspots.

Rogue AP policy | End Users should not be allowed to install their own wireless devices on the network because that could open unsecured portals to attackers.

Ad Hoc policy | Recommended to not allow users to use peer-to-peer connections because they rarely use encryption and can offer an attacker unauthorized access to the wired portion of the network.

Wireless Lan proper use policy | Outline of how to properly use the network. Include installation procedures, applications allowed, security implemenations.

IDS policy | defining proper responses to alerts raised by an IDS.

CHAPTER 15: RADIO FREQUENCY SITE SURVEY FUNDAMENTALS

Site Survey Interview

Customer Briefing | Explain the advantages of Wi-Fi and the limitations of a WLAN, discussion about bandwidth and throughput with relation to the current 802.11 a/b/g technology. Throughput vs. Data rate. 802.11g (ERP) protection mechanism. Why site survey is needed… the nature of RF signals 2.4 vs. 5GHz.

Business requirements | Why does the business need a WLAN; what would it be used for (which applications/in what environment), any VLAN needed? What devices will be connecting to WLAN?

Capacity and Coverage Requirements | Should look at floor plan of building, ask about capacity vs. coverage. Where should there be wireless coverage within a building? How about outside in yard? Will determine the type of antennas needed/save money if some places do not require wireless coverage.
Capacity planning | *Data applications*; often on average, 12-15 data users/AP is recommended. *User Density*: how many users currently need wifi, how many will need it in the future, where are the users? RF signal is attenuated by high concentration of Human Bodies. *Peak on/off use*: what is max capacity needed and when; could change settings for those times. *Existing Transmitters*: not just existing APs, but also microwaves, and other interfering devices. *Mobile vs. Mobility*: using laptop, turning off, moving to another place, turning it on again vs. like VoWiFi. *802.11g (ERP) protection mechanism*: throughput effected with backwards compatibility.
Existing WLAN | Problems are usually caused by existing APs with default settings causing co-channel interference and multipath interference. Qs to ask: Current probs, what are they? Any known sources of RF interference… like microwave, Bluetooth, cordless phones? Known dead zones? Prior site survey data? What equipment is currently installed?
Infrastructure Connectivity | to integrate WLAN into existing wired architecture, ask for copy of wired network topology map. Required seamless roaming? Restrictions on certain floors… what exactly? VLAN capability with customer's switches? Layer 3 roaming? Where are wiring closets? Antenna structure; p2p bridging needed? Hubs vs. Switches; recommended not to use hubs b/c of security and performance degradation. PoE needed? Segmentation by VLAN, VPN, firewall? Any naming conventions? Consideration of RBAC, bandwidth throttling, load balancing, where are passwords/usernames stored? Management of network through SSH2, SNMP, HTTPS/HTTP?
Security Expectations | Authorization, Authentication, accounting (AAA) requirements to be discussed/documented.
Guest Access | usually have redirection to a captive portal, should be segmented off from rest of the resources in a guest VLAN. Other commonalities: Firewall restrictions, and bandwidth throttling.

Documents and Reports

Form & Customer Documentation
Deliverables
Additional Reports

CHAPTER 16: SITE SURVEY SYSTEMS AND DEVICES

Spectrum analysis as well as **coverage analysis** is important. Variables such as walls, floors, doors, plumbing, windows, elevators, buildings, trees, and mountains can have direct effect on coverage on access point or wireless bridge.

Site Survey

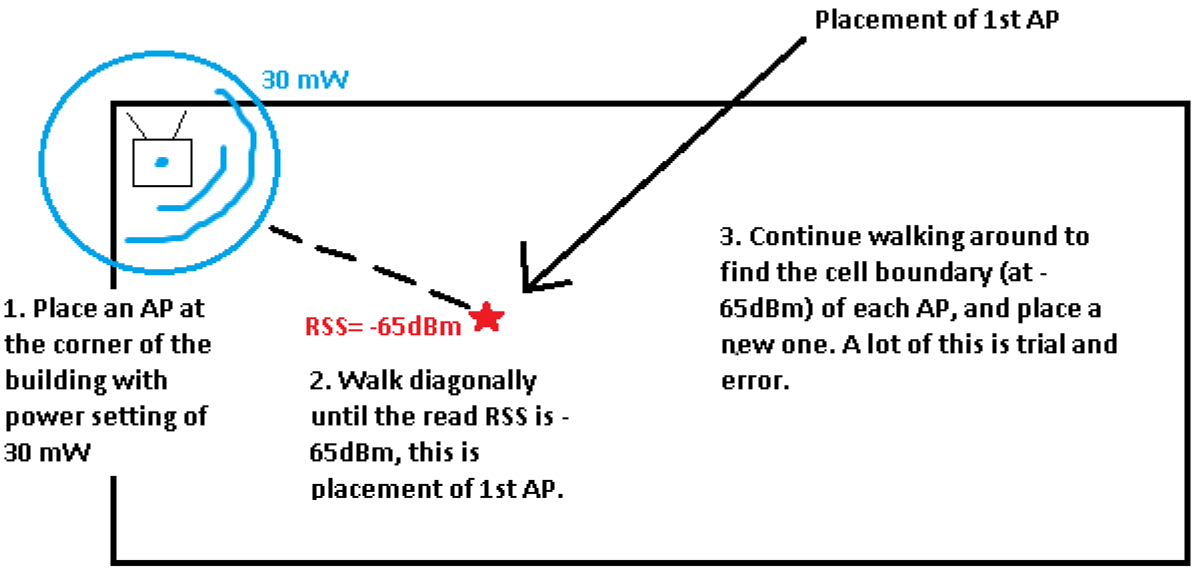
Purpose is not only to determine RF coverage, but also to look for potential sources of interference, as well as proper placement, installation, and configuration of 802.11 hardware and components. Optional requirement is capacity performance and application testing.

Mandatory Spectrum Analysis

Before coverage analysis survey, a highly overlooked, but important part of site survey is spectrum analysis; i.e. finding potential interferences. Mostly not done because spectrum analyzers are very expensive
Necessary because if noise floor exceeds -85dBm in 2.4GHz or 5GHz, the performance of wireless network can be severely degraded from the high number of retransmissions from the failed CRC, and no ACK frame return. Retransmissions above 10% will highly degrade performance. With VOIP, retransmissions over 2% will show degradation. In addition, a strong RF interference can prevent 802.11 client stations to transmit at all.
Interference in 2.4 GHz ISM band: Microwave ovens, cordless phones, fluorescent bulbs, video cameras, elevator motors, cauterizing devices, plasmas cutters, Bluetooth radios, nearby 802.11 b/g/n WLANs, Wireless ISPs. i.e. if a 1k watt microwave is 0.0000001% leaky, it still will interfere with 802.11 radio.
Interference in 5 GHz UNII bands: cordless phones, radar, perimeter sensors, digital satellite, nearby 802.11a/n WLANs, outdoor wireless 5 GHz bridges.
To limit interference: switch to 5GHz UNII band – cleaner, get a commercial grade microwave oven- an microwave oven's interference lays smack-dab in the middle of the 2.4 GHz spectrum, policy to remove cordless phones that interfere with wireless.

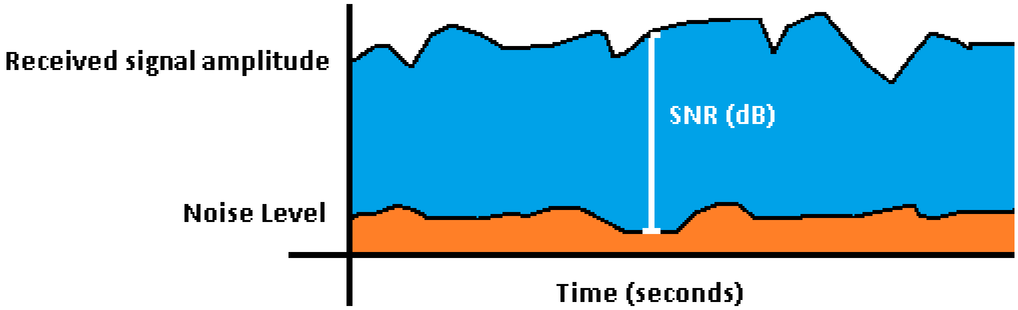
Mandatory Coverage Analysis

Capacity and Coverage requirements need to be discussed and determined before site survey is to be performed. Then, RF measurements need to be taken to guarantee the needs are met/ if not, then what to do to meet them. Coverage analysis must be performed with a *received signal strength* measurement tool- sometimes could be as easy as the RSS meter in your wireless card's client utility.


Placement of 1st AP
30 mW
1. Place an AP at the corner of the building with power setting of 30 mW
RSS= -65dBm
2. Walk diagonally until the read RSS is -65dBm, this is placement of 1st AP.
3. Continue walking around to find the cell boundary (at -65dBm) of each AP, and place a new one. A lot of this is trial and error.

* The description of a coverage analysis. It is important to avoid too much overlap because it can cause frequent roaming and performance degradation. Shape/size of building as well as material of walls and obstacles will require changes to distances btw access points, repeat of procedure.

Cell edge measurements: Received Signal Strength (RSS) in dBm, also known as RSL, Noise level (in dBm), and Signal to Noise Ratio (SNR in dB) If coverage is more important than capacity, the edge RSS can be reduced to -85dBm.



Recommendation for SNR is min of 18 dBm for data networks, and 25 dBm for Voice networks if data rate is to stay at 54Mbps. For VoWiFi, cell recommendations are cell radii of -60dBm, cells on same channel should have at least 20 dB separation – aka, if the cell boundary is at -60dBm, the next cell's boundary using the same channel should be -80dBm far away.

AP placement and Configuration

Each AP should be no more than 100 m cables distance away from wiring closet. Use semidirectional antennas in hallway- can cut down on reflections, negative effects of multipath (data corruption caused by delay spread and intersymbol interference)

Optional Application Analysis

Applications that simulate stress of a full-capacity network, as well as concurrent virtual wireless client stations. Roaming performance can also be tested, along with a multistation emulator that can test hundreds of protocols and generate traffic bidirectionally, along with VoIP traffic.

Site Survey Tools

Indoor Main tool: a RSS measurement tool. In addition: Spectrum analyzer, Blueprints of building, Signal strength measurement software, 802.11 client card, AP, WLAN controller, Battery pack, binoculars, Walkie-talkies/cell phones, antennas, temporary mounting gear, digital camera, measuring wheel/laser measuring meter, ladder or forklift, colored electrical tape.

Outdoor(bridging site survey) Topographic map, link analysis software, calculators, max tree growth data, binoculars, walkie-talkies/cell phones, signal generator and wattmeter, variable-loss attenuator, inclinometer, GPS, digital camera, sectrum analyser, high power spotlight or sunlight reflector

Coverage analysis

Manual | Passive: Radio card collects RF measurements, including RSS, noise level, and SNR. Client adapter is NOT associated to the AP during survey, all info is received from radio signals at layer 1. Active: Radio card is associated to AP, data link and Network layer data can be passed (such as pings). Upper layer info such as packet loss and layer 2 retransmissions can be measured. Main point of active is to look at % of L2 retransmissions.

Info from active and passive modes can be merged and visual representation of RF footprints is displayed over graphic floor plan. Some applications allow for "what-if" scenarios to be created (like increase/decrease power setting, changing channels)

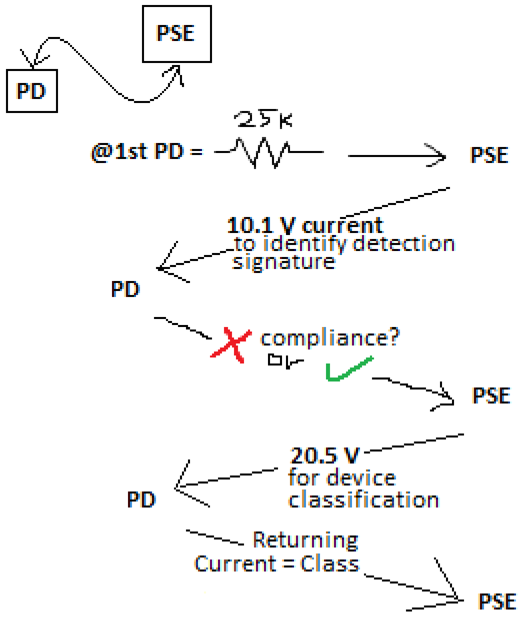
Assisted | After AP installations, a Wireless Network Management System or WLAN controller scans the AP radio cards and collects the RF information, then used for visualization of coverage cells and for optimizing AP configs (channels and pwr settings). Often used as a starting point before final deployment and used as calibration/planning tool with WLAN controllers.

Predictive | Uses an application that creates visual models of RF coverage cells. Projected cell coverage zones are created using modeling algorithms. Usually these are stand-alone programs that use blueprints and floor plans that contain layer info on type of building materials. Modeling forecast can include following: Channel reuse patterns, coverage cell boundaries, ap placement, ap power settings, number of APs, data rates. Vendors claim up to 85% accuracy.

Self-Organizing Wireless LANs

Could eliminate need for manual or other type of site surveys by the use of radio frequency spectrum management (RFSM), where a centralized device can dynamically change the configs of a thin or fat AP based on accumulated RF info gathered from AP's radio cards. Some of these are defined under 802.11h amendment.

CHAPTER 17: POWER OVER ETHERNET (POE)



History of PoE

Concept of power over data lines came since the telephone, where power needed to operate the device was delivered directly over the data lines. Typically, PoE devices today include VoIP phones, cameras, and APs. The power sent to them are through the Ethernet cable, the use of PoE alleviates need to run electrical wires to the device; greatly improves flexibility of placing the devices, moving is also easier.

Nonstandard PoE | aka proprietary solutions before IEEE created the standards (began in 1999). Problem: use of different voltages, mixing proprietary solutions could damage equipment.

IEEE 802.3af | Defines how to provide PoE to 10BaseT (Ethernet), 100BaseT (Fast Ethernet), 1000BaseT(Gigabit Ethernet) devices. Approved on June 12, 2003.

IEEE 802.3-2005, Clause 33 | Specifically defines PoE. Four amendments incorporated into 1 clause: 802.ak - 10 Gigabit Ethernet, 802.3af - PoE, 802.3ah - Ethernet in the First Mile, 802.3ak - 10GBase-CX4.

IEEE 802.3at | Not yet ratified in 2009..., also known as PoE+ extends capabilities of PoE. 1) More power provided (as much as 30 watts of power to devices vs. 15.4) 2)Be backwards compatible with Clause 33 devices.

PoE Devices

Powered Device (PD) | Requests/Draws power from Power Sourcing Equipment. MUST be able to accept 57 Volts of power from data lines or unused pairs of Ethernet cable. MUST be able to accept power with either polarity from power supply (mode A or B). Need minimum of Cat5 Ethernet Cable. Detection Signal - reply to PSE; used to see if power can be accepted and to see if PD is compliant with Clause 33. Classification Signature - tells PSE the level of power needed. When PD is first connected to PSE, it presents itself as a 25k-ohm resistance

Drawing outlines detection of compliance/state of device (able to accept power?) and of classification (how much power is needed to operate).

Returning Current between 14.5 and 20.5 V
Class 0 : 0-4 mA
Class 1: 9-12mA
Class 2: 17-20mA

Class 3: 26-30mA
Class 4: 36-44mA.
Power classification(max power used)- Class 0 Default: 0.44W-12.95W, Class 1: 0.44-3.84W, Class 2: 3.84-6.49W, Class 3: 6.49-12.95W, Class 4: Reserved for Future Use.

Power-Sourcing Equipment (PSE) | provides power to the PD. Power supplied is at a nominal 48 volts (44-57). Uses a DC detection signal. Power provided is greater than what is used by the PD, need to account for worst case scenario, plus loss of power from cables/connectors. Max draw of any PD is 12.95 Watts so max of PSE output is 15.4 Watts. When power is not required anymore, PSE will stop providing. There are two types of equipment:

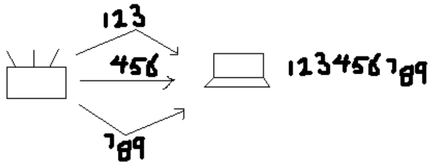
Endpoint - provides power and ethernet data from SAME DEVICE. Typically are PoE-enabled switches or WLAN controllers
2 alternatives: A - puts pwr on data pair: 1,2 & 3,6 (only alternative Gig Ethernet can use) B - places power on the spare pair 4,5 & 7,8.
Midspan - power sourcing equipment that acts as a pass-through device, adding power to Ethernet segment between PSE and PD. Can only use alternative B, only works with 10BaseT and 100BaseT.

Power-Sourcing Equipment Pin Assignments | Using Alt. A, positive voltage is matched to the transmit pair of the PSE. if PSE uses crossover ethernet, port may choose have opposite configurations (positive voltage to 1,2 and negative to 3,6). Alternative B can only have positive to 4,5 and negative to 7,8.

Planning and Deploying PoE
Power planning | Power sourcing equipment must be able to provide 15.4 Watts. I.e. a 24-port switch must be able to provide 15.4*24 = 369.4 watts collectively. A 110-volt power supply can provide up to 3300 watts. The need for more PoE can cause there not to be enough power to go around to all PDs. Thus, there's a need for a power budget. PDs with classification really help reduce power consumption because only the amount of power necessary is expended. More power = more heat, thus need for climate controlled equip rooms.
Redundancy | A power outage didn't bring down phones' power in the past, we expect the same from VoIP, so you need redundant power sources or a backup to turn on if there is a power outage.

Chapter 18: High Throughput (HT) and 802.11n

Main objective was to increase data rates and throughput in both 2.4 and 5 GHz RF bands. 802.11n draft defines *High Throughput (HT)* which provides PHY and MAC layer enhancements potentially making rates up to 600mbps.
Physical Layer is dramatically different using MIMO technology which takes advantage of multipath.
Wi-Fi Certification requires Support for 2 spatial streams in transmit mode (only AP) and receive mode (AP and client except handheld), support for MPDU and MSDU, support for block ACK. 2.4GHz and 5GHz bands can operate in dual or single mode on 1 device, can contain Greenfield preamble, 40MHz channels in 5GHz band optional.
MIMO
Heart/Soul of 802.11n in the PHY Layer. Use of multiple radios and antennas = a radio chain. Transmit beamforming is optional to steer beams for better throughput and greater range.
Radio Chains: SISO means single radio chain (single radio and all of its supporting arch. Incl. mixers, amps, analog/digital converters. 2X3 MIMO means 3 chains with 2 transmitters (TX) and 3 receivers (RX). These also allow for spatial multiplexing. More radios/antennas = more power needed.



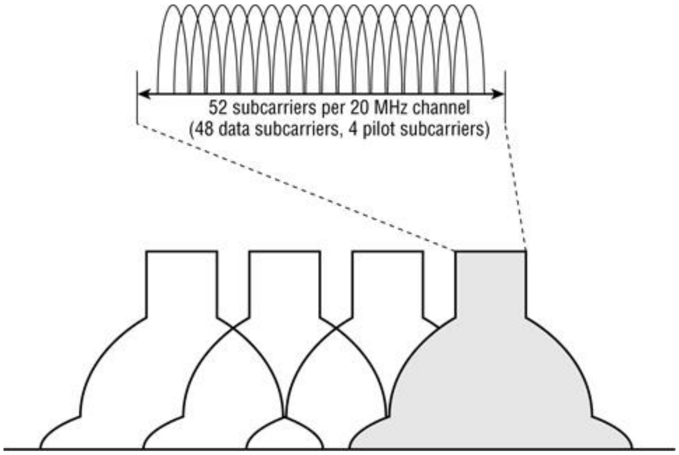
Spatial Multiplexing: Basically multiple streams sent simultaneously, even using different kinds of modulation. Although using (equal) same kind of modulation is faster. Both receiver and transmitter must be MIMO supporting.

MIMO Diversity Antenna Diversity: method of compensating for multipath as opposed to using it. Without MIMO, *switched diversity* means multiple antennas listen, but only the best quality stream of information is used, all others ignored. *Maximal Ratio combining (MRC*): combines multiple received signals into one by looking at each one and optimally combining constructively. MIMO uses both MRC and switched diversity.
Transmit Beamforming Allows MIMO transmitter to focus transmissions in a coordinated method using multiple antennas; works if transmitter knows about receiver's location. Use of constructive multipath by sending initial signals out of phase so

they combine to a whole healthy signal at RX. Emulates high-gain unidirectional antenna. Relies on implicit/explicit feedback between RX and TX (think sonar technology?)

HT Channels HT Clause 20 radios can operate in either frequency.

20MHz Non-HT and HT Channels: NON HT: Each channel 52 subcarriers. 48 transmit data, 4 used as pilot tones for calibration btw TX and RX. HT: Each Channel 56 subcarriers, 52 transmit data, 4 pilots.


52 subcarriers per 20 MHz channel
(48 data subcarriers, 4 pilot subcarriers)

Non-HT: Each “blob” is a channel of 20 MHz.

40MHz Channels have 114 OFDM subcarriers 108 data carriers, 6 pilots; doubles frequency bandwidth avail for TX. Essentially two 20MHz channels bonded. Really can only be implemented in 5GHz because there’s more Frequency range. In 2.4GHz, any two 40 GHz channels would overlap severely. => Only supported in 5GHz UNII bands.

Guard Interval: 54Mbps radio transmission by OFDM, each *symbol* (a collection of bits) contains 288 bits; 216 are data, 72 are error-correction bits. Each OFDM symbol has an 800 nanosecond Guard Interval (GI) Purpose: to accommodate for late arrival of symbols over long distances. *Intersymbol Interference (ISI)*: A new symbol may get to RX before a late symbol has been completely received. 802.11n allows for optional 400 nanosecond GI to improve data rates by ~10%, but chances of ISI increase.

Modulation and Coding Scheme (MCS): Data rates previously were dependent on what modulation was used (6-54Mbps). HT radios use many factors including modulation, number of spatial streams, channel size and guard interval. Each MCS is a variation of these factors. 77 exist, 8 are mandatory for 20MHz HT:

Mandatory MCS Indexes 0 to 7 using 1 spatial stream; Datarates of each depend on 800 GI and 400 GI – 0 is 6.5|7.2Mbps, 1 is 13.0|14.4Mbps, 2 is 19.5|21.7Mbps… 7 is 65|72.2Mbps. 0 is BPSK Modulation | 1,2 are QPSK Modulation | 3,4 are 16-QAM | 5-7 are 64-QAM

There are tables depicting these for 20MHz 4 Spatial Streams, 40MHz 1 spatial and 4 spatial streams, with the best being MCS 31 with 64 QAM, 4 Spacial Stream, 400ns GI at 600Mbps.

HT PHY

Purpose of preamble is to synchronize TX at PHY layer btw 2 802.11 radios. Purpose of PHY header is to use a signal field to indicate how long it will take to transmit the 802.11 frame (MPDU). THREE PPDU structures that use 3 different preambles: Non-HT (Legacy), HT Mixed (Contains both Legacy and Greenfield format), HT Greenfield.

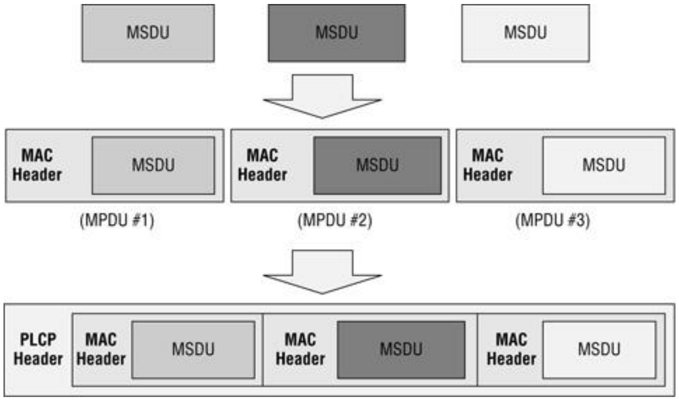
HT MAC

Medium contention overhead addressed by using 2 methods of frame aggregation; new methods of interframe spacing and Block ACKs, plus methods of power management.

Frame Aggregation: combining multiple frames into single TX. (Hey, like a train with many truckloads on it!)

TYPE A) *Aggregate MAC Service Data Unit (A-MSDU)* AP gets 802.3, takes off headers/trailers, puts all in one 802.11 Frame. Entire frame can be secured using TKIP or CCMP. *Note: all MSDUs must be of same QoS type (i.e. UDP and TCP shouldn’t be mixed.)

TYPE B) *Aggregate MAC Protocol Data Unit (A-MPDU)* Each MSDU has a MAC header/trailer inside the MPDU.



MTBA (Multiple Traffic ID block ACK) The ACK used for A-MPDUs because each MPDU has its own header.
RIFS (Reduced Interframe Space): 1/8th of a SIFS interval, reduces overhead when used instead of SIFS. Can only be used in Greenfield HT.

HT Power Management

Spatial Multiplexing Power Save (SM power save): allows MIMO radios to power down all but 1 radios. Static mode: power down to 802.11 a/b/g radio mode (one on receiving 1 spatial stream). Dynamic Mode: Powers down to all but one but can bring up others much faster. An AP can trigger to wake up other radios by sending a request-to-send frame.
Power Save Multi Poll (PSMP): Extension of automatic power save delivery. Yeah.

HT Operation

20/40 Channel Operation: Rules – HT AP must declare 20 or 20/40 support in beacon| Client stations must declare 20 or 20/40 in association/reassociation frames | Client must reassociate when switching btw 20 and 20/40 | if 20/40 capable STA TX by using single 20MHz, must transmit on primary channel.
HT Protection Modes:
0 – Greenfield only: HT radios in use. Same channel type operation.
1 – HT nonmember protection mode: All stations in BSS must be HT, protection mechanism kick in when non-HT STA or AP is heard that is not a member of BSS.
2 – HT 20MHz protection mode: All stations in BSS must be HT and are associated to a 20/40 AP. If 20MHz only HT station associates to 20/40 AP, protection is used to prevent 20MHz STA to transmit at the same time.
3 – HT Mixed Mode: 1 or more Non-HT radios are in BSS; most common today, as there are many legacy devices out there.
Dual-CTS Protection: RTS/CTS frames sent in both HT and non-HT formats so both legacy and HT devices can understand. Resets NAV timers within the HT cell and any neighboring clients or APs that hear RTS/CTS.
Phased Coexistence Operation (PCO): optional. Divides time and alternates btw 20/40 MHz channels. Adv: no protection mechanism needed during 40 MHz operation phase. So could increase throughput in some situations.