WIFI Alliance

Tuesday, April 21, 2020 05:58 PM

- Original name: Wireless Ethernet Compatibility Alliance(WECA)
- Responsible for ensuring Wireless interoperability certification program
    - Helps conserve battery power for devices using WIFI by managing the time the client spends in the sleep mode
    - Wi-Fi Multimedia Quality of Service (WMM QoS) mechanism
        - Prioritizes wireless voice & video traffic over the WIFI link
        - Automatically enabled for the router
        - Prioritizes wireless data packets from different applications based on 4 categories:
            - Voice
            - Video
            - Best effort
            - Background
- Promotes WIFI technology
- WIFI protected setup
    - Simplifed & automatic WPA & WPA2 security configs for home & small business
- WIFI direct
    - Enables devices to connect directly without the use of an access point
- Converged Wireless Group-RF profile
    - Defines the performance metrics for WIFI & cellular radios in a converged handset to help ensure that both technologies perform well in the presence of other
- Voice personal
    - Enhanced support for voice applications in residential / small business WIFI network
    - Single AP
- Voice enterprise
    - Voice QoS highest priority
    - Seamless roaming within enterprise WIFI network (multiple APs)
- Tunneled direct link setup
    - Allows devices to establish a secure link to each other after they have joined a WIFI network
- Passpoint / Hotspot 2.0
    - Designedd to revolutionize the end user experience when connecting to a WIFI hotspot
    - Uses Extensible Authentication Protocol (EAP) to authenticate
        - Protocol for wireless networks that expands on authentication methods used by Point-to-Point(PPP)
- WMM-Admission Control
    - Allows WIFI networks to manage network traffic based upon channel conditions, network load & type of traffic
        - Voice
        - Video
        - Best effort
        - Background
- IBSS with WIFI protected setup
    - Provides easy config & strong security for ad hoc WIFI networks
    - Designed for devices with limited user interfaces
    - Features easy push button or PIN setup, task-orientated short term connections & dynamic networks that can be established anywhere
- Miracast
    - Seamlessly integrates the display of streaming video between devices
    - Core technology & security
    - WIFI multimedia
    - WMM power save

Communication Fundamentals

Tuesday, April 21, 2020 10:38 PM

- Carrier signals
  - Waveform that is modulated (modified) with a input signal for the purpose of conveying information
  - Usually a higher frequency than input signal
- Keying methods
  - Method which changes the signal into a carrier signal
  - Amplitude-Shift keying (ASK)
    - Varies the amplitude / height of a signal to represent the binary data
    - When noise occurs it normally affects amplitude of the signal meaning this keying method is more susceptible to signal loss
  - Frequency-shift keying (FSK)
    - Varies the frequency of the signal
    - 1 frequency can represent the 0 bits & another can represent the 1 bit
  - Phase-shift keying (PSK)
    - Varies the phase of signal
    - Phase change can represent the 0 & no change in phase can represent a 1

Radio frequency components

Wednesday, April 22, 2020 02:34 PM

- Transmitters
  - Initial component in the creation of wireless medium.
  - Transmitters job is to begin the RF communications
  - Transmitter starts AC signal oscillating at the RF frequency
  - Transmitter takes data provided and modifies the AC signal using a Modulation technique
- Antenna
  - Two functions when connected to the transmitter it collect the AC signal received from the Transmitter and directs or radiates it out.
  - When connected to the receiver it takes the signal and directs the AC signal to the receiver.
  - Two ways to increase the power output of an antenna
    - Generate more power at the transmitter
    - Direct or focus the RF signal that is radiating from the antenna
- Receiver
  - Takes the carrier signal received from the antenna & translate the modulated signals into 1s & 0s
    --> passes the data onto the network/computer/device
- Intentional Radiator (IR)
  - Device that intentionally generates & emits radio frequency energy by the radiation / induction
  - Regulatory bodies limit the amount of power that is aloud to be generated by an IR
  - Components of making up the IR
    - Transmitter
    - All cables
    - Connectors
    - Any other equipment (grounding, lightning, arrestors, amplifiers, attenuators, etc) between transmitter & antenna
  - Power measured at the connector that provides the input ot the antenna
    - Usually measured in Milliwtt or decibels relative to 1 Milliwatt (dBm)
- Equivalent isotopically radiated power (EIRP)
  - Highest RF signal strength that is transmitted from a particular antenna
  - Regulatory bodies limit he amount of EIRP of an antenna

Units of power & Comparison

Wednesday, April 22, 2020 02:45 PM

- Watt (W)
  - Unit of power
  - One watt is equal to 1 ampere (A) of current flowing at 1 volt (V).
  - Watt (W) = Volt (V) x Ampere (A)
- Milliwatt (mW)
  - Unit of power
  - 1 Milliwatt = 1/1,000 watts
- Decibel (dB)
  - Unit of comparison
  - Difference between two values. dB is a relative expression used to represent a difference between two values
  - In wireless networking dBs are often used to compare the power of two transmitters or more often to compare the difference or loss between the EIRP output of a transmitters antenna and the amount of power received by the receivers antenna
- dBi
  - Used to compare the output of one antenna to another
  - The gain or increase of power from an antenna when compared to what an isotropic radiator would generate is known as decibels isotropic (dBi)
- dBd
  - Relative measurement and not a unit of power
  - Antenna industry users two dB scales to describe the gain of antenna
    - dBi
    - dBd
  - dBd decibel gain relative to a dipole antenna
  - dBd value is the increase in gain of an antenna when compared to the signal of a dipole antenna
  - How to compare two antennas one in dBi and other in dBd
    - Standard dipole antenna has dBi of 2.14
    - If antenna has value of 3 dBd, this means it is 3 dB greater than a dipole antenna
    - Because value of dipole antenna is 2.13dBi all you need to do is add 3 to 2.14
      - So a 3dBd antenna is equal to a 5.14dBi antenna
- dBm
  - Compares a signal to 1 Milliwatt of power
  - Decibels relative to 1 Milliwatt
  - 0dBm = 1 Milliwatt
  - dBm = 10 x log10(PmW)
  - +6dB doubles the distance of the usable signal
  - -6dB halves the distance of the usable signal
  - dBm makes it easy to calculate the effects of antenna gain on a signal.
- Inverse Square Law
  - Law states that the change in power is equal to 1 divided by the square of the change in distance
    - As the distance from the source of the signal doubles the energy is spread out over four times the area, resulting in one-fourth of the original intensity of the signal.
  - Free space path loss formula:
    - FSPL = 36.6 + (20log10(F)) + (20log10 (D))
      - FSPL = Free space path loss
      - F = Frequency in MHz
      - D = Distance in miles between antennas
    - FSPL = 32.4 + (20log10 (F)) + (20log10 (D))
      - FSPL = Free space path loss
      - F = Frequency in MHz
      - D = Distance in Kilometres between antennas
  - FSPL is based on Newtons inverse square law

Radio Frequency Fundamentals

Tuesday, April 21, 2020 10:49 PM

Terms:

- Wavelength
  - Distance between 2 successive crescents (peaks) / 2 successive throughs (valleys)
- Frequency
  - Is how often RF signal cycles in a certain time period
  - Standard measurement of frequency is hertz (Hz)
  - Event that occurs once in a second has a frequency of 1 Hz
    - 1 Hz = 1 cycle / s
    - 1 MHz = 1 000 000 cycles / s
- Amplitude
  - Height of the wave
  - Can be characterized simply as the signal's strength / power
- Phase
  - Not a property of just one signal but instead involves the relationship between 2 or more signals that share the same frequency

Behaviors

- Wave propagation
  - The way the wave moves
  - Can vary drastically depending on the type of material the signal is traversing
- Absorption
  - Common RF behavior
  - Most materials absorb some RF signal, amount depends on the material
  - If signal does not bounce off an object, move around an object or pass through an object --> 100% absorption rate occurred
- Reflection
  - Most important RF behavior to be aware of
  - Causes serious performance problems in legacy 802.11a/b/g WLANs
  - When wave hits smooth object that is larger than the wave itself --> dependent on the material the signal may bounce in another direction
  - 2 types of reflection:
    i. Sky wave reflection
       - Signals below 1 GHz
       - Signal bounce off charged partials in the ionosphere in the earth's atmosphere

    ii. Microwave
       - Signal: 1GHz - 300GHz
       - Can bounce off smaller objects like a metal door
- Scattering
  - Described as multiple reflections
  - Reflection off an object with multiple sides
  - 2 types of scattering
    - Lower level has lessor effect on signal quality & strength
    - Occurs when RF signal encounters some type of uneven surface & is reflected into multiple directions (Chain link fences, wire mesh in stucco walls)
- Refraction
  - Signal bent into behavior
  - When signal passes through a medium with different density --> causing the wave to change direction
  - 3 most common user
    - Water vapor
    - Changes in air temperature

        - Changes in air pressure
- Diffraction
    - Signal bent around an object
    - Sitting directly behind the object s an area known as RF shadow
    - Depending on the change in direction of the signal this area can become a dead zone of coverage
- Loss (attenuation)
    - Decrease in amplitude
    - Signal may lose strength on the wire / in the air
    - Signal can be absorbed into materials it passes through
- Free space Path Loss (FSPL)
    - Signal will attenuate as it travels despite the lack of attenuation caused by obstruction, absorptions, reflection, diffraction, etc
    - Loss of signal strength caused by the natural broadening of the waves
- Multipath
    - Occurs when 2 or more signals arrive at the receiving station at the same time or within nanoseconds of each other
    - 4 results of multipath
        - Upfade
            - Multiple RF signal paths arrive at the same time & are in phase
            - Phase differences of 0 - 120 degrees will cause upfade
        - Downfade
            - Multiple RF signals arrives at the same time but are out of phase
            - Phase difference of 121 - 179 degree
            - Results in decrease signal strength
        - Nulling
            - Signal cancellation
            - Multiple RF signals arrive at the same time & are 180 degrees out of phase of each other
        - Data corruption
            - Multiple signals arriving but not at the same time the receiver might have trouble demodulating the signal
- Gain (amplification)
    - Increase in amplitude or signal strength
    - 2 types
        - Active
            - Increase to signal on the transmitter or transceivers side through the use of an amplifier --> more power is applied
        - Passive
            - Done by focusing the antenna, the inner workings of the antenna make the signal stronger

RF Mathematics

Wednesday, April 22, 2020 02:48 PM

- Rules of 10s and 3s
  - For ever 3dB of gain (relative), double the absolute power (mW)
  - For every dB of loss (relative), halve the absolute power (mW)
  - For every 10 dB of gain (relative), multiply the absolute power (mW) by a factor of 10
  - For every 10 dB of loss (relative), divide the absolute power (mW) by a factor of 10
- Noise Floor
  - Noise floor is the or background level of radio energy on a specific channel.
  - This can include modulated or encoded bits from nearby 802.11 transmitting radios or unmodulated energy coming from non-802.11 devices such as microwave ovens, Bluetooth device
  - The Amplitude of the noise floor varies in different environments.
  - 2.4GHz will have higher Noise floor than 5GHz as the bands are more crowded.
- Signal-to-Noise Ratio (SNR)
  - Is the difference in decibels between the received signal and the background noise level (noise floor), not actually a ratio.
  - Example:
    - Radio receives a signal of -85dBm and the noise floor is measured at -100dBm the difference is 15bD therefore the SNR is 15dB
- Received Signal Strength Indicator
  - The power level of an RF signal required to be successfully received by the receiver radio.
  - The lower the power level that a receiver can successfully process the better the receive sensitivity.
  - In WLAN equipment the receive sensitivity is usually defined as a function of the network speed.
- Link Budget
  - Sum of all the planned and expected gains and losses from the transmitting radio, through the RF medium, to the receiver radio
- Fade Margin / System Operating Margin
  - Fade Margin is a level of desired signal above what is required.
  - Effectively is a margin added to the required signal level to account for outside factors causing the signal level to fluctuate
  - Normally used for outdoor WLAN bridge links

Radio Frequency Signal

Wednesday, April 22, 2020 02:50 PM

Charts

- Azimuth & elevation charts (Antenna Radiation Envelopes)
    - Antenna is placed at the center of the chart
    - Azimuth chart
        - H-plane
        - Top-down view
    - Elevation chart
        - E-plane
        - Side view
- Interpreting polar charts
    - Represented in decibel (dB) mapping of the antenna coverage
    - Each concentric circle on this logarithmic chart represents a change of 5dB

Beamwidth

- Measurement of how broad / narrow the focus of an antenna is & is measured both horizontally & vertically
- Measurement from the center, the strongest point, of the antenna signal to each of the point s along the horizontal & vertical axes where the signal decreases by half power (-3dB)
    - -3dB referred to as half-power points
- Distance between the half-power point sis measured in degrees giving the horizontal & vertical beamwidth measurements
- Calculating beamwidth
    - 1st determine the scale of the Azimuth & Elevation charts
        - Complete it separately
    - 1st locate the point on the chart where the antenna signal is the strongest in order to determine the beamwidth of the antenna
    - Move along the antenna pattern away from the peak signal until you reach the point where the antenna pattern is 3dB closer to the center of the diagram
    - Draw a line from each of these points to the middle of the polar chart
    - Measure the distance in degrees between these lines to calculate the beamwidth of the antenna

Antenna Types

- Omnidirectional antenna
    - Radiate in all directions
    - Dipole antenna --> built into the AP
    - Typically found in point-to-multipoint environment
    - With higher-gain omnidirectional antennas --> vertical signals is decreased & the horizonal power is increased
    - Antennas are most effective when the length of the element is an even fraction (e.g. 1/4 or 1/2) or a multiple of the wavelength (λ)
- Semi directional antenna
    - 3 types of antennas fit into the semi directional category
        - Patch
            - Can be used effectively in libraries, warehouses & retail stores with long aisles of shelves
            - Were used indoors to reduce reflections & hopefully from the amount of multipath before 802.11 MIMO
        - Panel

        - Similar to patch
        - Terminology gets interchanged quite often
    - Yagi
        - Typically used for short - medium distance point to point connections of up to about 3.2 kms
        - Higher gain in Yagi antennas can be used to cover more distance
- Highly directional antenna
    - Used strictly for point to point communications
        - Typically between buildings
    - 2 types of highly directional antennas
        - Parabolic dish
            - Similar to cable TV satellite dishes
            - Recommended that a protective cover known as a radome is used to help offset some of the effects of the wind in a high wind situation
        - Grid antennas
            - Grill of a barbecue, with the edges slightly curved inward
            - Better in high wind environment
- Sector antenna
    - Special type of high-gain, semi-directional antenna that provides a pie-shaped coverage pattern
    - Individually, each antenna services its own piece of the pie but as a group, all of the pie pieces fit together and provide omnidirectional coverage for the entire area
    - Very small back-lobe on these antennas
    - Typically have a gain of about 10dBi
    - Use of sector antenna has increased due to the expansion of 802.11 networks in stadiums & outdoor venues
- Antenna arrays
    - A group of 2 or more antennas that are integrated together to provide coverage
    - Operate together to perform what is known as beamforming

Beamfoming

- Method of concentrating RF energy
    - Signal will be greater than the SNR at the receiver therefore providing better transition
- 3 types of beamforming
    - Static (indoor sectorized array)
        - Performed by using directional antennas to provide a fixed radiation pattern
        - Uses multiple directional antennas clustered together but all pointing away from a central point
    - Dynamic (smart antenna technology / beamsteering)
        - Focuses RF energy in a direction in a particular shape
        - Radiation pattern of the signal can change on a frame by frame basis
        - Provides optimal power & signal for each transition
        - Uses ad adaptive antenna array that manoeuvres the beam in the direction of the receiver dynamically
    - Transmit
        - Transmitting multiple phase-shifted signals with the hope & intention that they believe will arrive in-phase at the location where the transmitter believes that the receivers is located
        - Does not change antenna radiation pattern & an actual directional beam does not exist
        - Not really an antenna technology it's a digital signal processing technology
        - 2 types of transmit beamforming
            - Implicit TxBF
                - Uses an implicit channel-sounding process to optimize the phase differentials between the transmit chains

- Explict TxBF
  - Requires feedback from the stations in order to determine the amount of phase-shift required for each signal
  - 802.11ac defines Explicit TxBF requiring the use of channel measurement frames & both the transmitter & receiver to support beamforming

Visual Line of Sight (Visual LOS)

- When light travels from one point to another it travels across what is perceived to be an unobstructed straight line which is known as Visual Line of Sight
- Has no bearing whether or not a RF transition will be successful or not

RF Line of Sight

- Additional area around the visual LOS needs to remind clear of obstacles & obstructions
- Area around the visual LOS is known as Fresnel zone & is often referred to as RF Line of Sight

Fresnel Zone

- Imaginary, elongated, football-shaped area that surrounds the path of the visual LOS between 2 point-to-point antennas
- Exists above, below & to the sides of the visual LOS (in 360^{o} fashion)
- In theory, there are infinite number of Fresnel Zones
  - Closest to the center is known as the First Fresnel Zone
  - Next closest is known as the Second Fresnel Zone etc
  - Only first 2 need to be worry about
    - If 1st Fresnel Zone becomes partially / fully obstructed --> a negative influence on the RF Communication
      All of the odd-numbered Fresnel zones are in phase with the point source signal, and all of the even-numbered Fresnel zones are out of phase
    - Under no circumstances should any object or objects to encroach more than 40% into the 1st Fresnel Zone of an outdoor point-to-point bridge link --> result in unreliable P2P link, even less than 40% is likely to impair the performance of the link
      - Typical obstruction includes trees & buildings
- Fresnel Zone is related to the frequency being used
- Smaller beamwidth ≠ smaller Fresnel Zone
- All of the odd-numbered Fresnel zones are in phase with the point source signal, and all of the even-numbered Fresnel zones are out of phase
- Formula for calculating the 1st Fresnel Zone radius
  - Calculate the middle of the P2P link
    - $\text{radius} = 72.2 \times 3\sqrt{[D \div (4 \times F)]}$
      - Where
        - D = distance of the link in miles
        - F = transmitting frequency in GHz
    - optimal clearance that you eant along the signal path
      - $\text{radius}(60\%) = 43.3 \times \sqrt{[D \div (4 \times F)]}$
        - Where
          - D = distance of the link in miles
          - F = transmitting frequency in GHz
  - Calculate Fresnel Zone radius at any point along the connection
    - $\text{radius} = 72.2 \times \sqrt{\left[\left(N \times d_1 \times d_2\right) \div (\text{F} \times \text{D})\right]}$
    - Where
      - N = which Fresnel Zone are you calculating
        - Usually 1 or 2

        - d_1 = distance from one antenna to the location of the obstacles in miles
        - d_2 = distance from the obstacle to the other antenna in miles
        - D = total distance between the antennas in miles
            - $D = d_1 + d_2$
        - F = transmitting frequency in GHz

Earth Bugle

- Recommended to take into account on P2P links over 7 miles
- After 7 miles --> Earth starts to impede on the Fresnel Zone
- Formula to calculate the increased height needed to raise the antenna to account for the Earth Bugle
    - $H = D^2 \div 8$
        - Where
            - H = height of the earth bulge in feet
            - D = distance between the antennas in miles
- Formula to work out antenna height taking into account Fresnel Zone & Earth Bulge
    - $H = OB + (D^2 \div 8) + \left(43.3 \times \sqrt{[D \div (4 \times F)]}\right)$
        - Where
            - H = height of the earth bulge in feet
            - OB = obstacle in height
            - D = distance of the link in miles
            - F = transmitting frequency in GHz

Antenna Concepts

Wednesday, April 22, 2020 06:15 PM

Antenna Polarization

- Amplitude of the waves can oscillate either vertically / horizontally as wave raditate from an antenna
- Transmitting & receiving antenna needs to be oriented the same way
- Most indoor Aps with low gain omnidirectional antennas should be polarized vertically when mounting to the ceiling
- Internal antennas installed in laptops are vertically polarized as well
- Proper polarization is extremely important when aligning a point-to-point or point-to-multipoint bridge
    - Cross polarization: when best received signal level (RSL) received when aligning the antennas 15-20dB less than the estimated RSL
    - If difference exist on only 1 side & the other has a higher signal --> likely aligned to a side lobe

Antenna Diversity

- Exists when an access point has 2 or more antennas with a receiver functioning together to minimize the negative effects of multipath
- When access point senses an RF signal --> compares the signal that it is receiving on both antennas
    - uses whichever antenna has the higher signal strength to receive the frame of data
- Only 1 antenna is operational at any given time, it can't send on 1 & receive on the other

Multiple-input, Multiple-output (MIMO)

- More sophisticated form of antenna display
- Take advantage of multipath
- Can receive or transmit on multiple antennas concurrently
- 802.11n & 802.11ac radios use MIMO
- MIMO antennas
    - Indoor antennas
        - Not a common decision to make as vendors on most APs already have integrated MIMO antennas into the AP with no antennas protruding
        - If AP has external antennas these should be installed as per vendors recommendations if this isn't specified then it should be align slightly off parallel with each other
    - Outdoor antennas
        - Benefit may not be realized if the environment does not have reflective surfaces that induce multipath

Antenna Connection & Installation

Wednesday, April 22, 2020 10:33 PM

Voltage Standing Wave Ratio (VSWR)

- Measurement of the change in impedance to the AC signal
- Standard unit of measurement of electrical resistance is ohm (Ω)
- A ratio of impedance mismatch with 1:1 (no impedance) being optimal but unobtainable
- Typical values range from 1.1:1 to as much as 1.5:1
- Military specs: 1.1:1
- If VSWR --> large amount of voltage is being reflected back towards the transmitter
- May cause decreased signal strength, erratic signal strength or even transmitter failure
- Ensure that impedance of all of the wireless networking equipment is matched --> help to minimize VSWR

Signal loss

- Main objective when connecting an antenna to a transmitter: ensure that as much of the signal that is generated by the transmitter is received by the antenna to be transmitted
    - Need to pay attention to the connectors & cables between the AP & the antenna
        - If interior components are used --> these will more than likely result in AP functioning below its optimal capacity

Antenna mounting

- Key areas to achieve proper installation of an antenna
    - Placement
        - Dependent of antenna type
        - Omi antennas : normally in the middle of the area to be covered
            - High gain omni antennas are not to be placed too high above ground due to the narrow vertical coverage
        - Directional antennas : ensure that you know the horizontal & vertical beamwidths to properly aim the antenna
            - If the power is too high --> overshoot the coverage area which can be a security risk
                - Lower the transmit power
        - Outdoor directional antennas : ensure that Fresnel zone is calculated & it's clear
    - Indoor mounting considerations
        - 2 common concern
            - Aesthetics
            - Security
    - Outdoor mounting considerations
        - Ensure that wind load is taken into consideration & antennas are properly secured if it's being installed in a windy location
    - Appropriate use & environment
        - Ensure that indoor APs & antennas outdoor are not used
        - Outdoor APs & antennas are designed to withstand harsher environmental conditions (temperature, wind, rain, etc)
    - Ingress protection rating / International Protection Rating (IP Code)
        - Is represented by the letters IP followed by 2 digits / a digit & 1 /2 letters (e.g. IP66)
        - 1st number is protection against solids
            - range from 0 - 6
                - Where
                    - 0 : no protection
                    - 6 : full protection

        - 2nd number is protection against water
            - Ranges from 0 - 8
                - Where
                    - 0 : no protection
                    - 1 : dripping water
                    - 4 : water splashing from any direction
                    - 6 : powerful water jets
                    - 8 : immersion > 1 meter
    - United States National Electrical Manufacturers Association (NEMAA) enclosure rating
        - Similar to IP ratings but take other features (e.g. corrosion resistance) into account
    - Equipment for potentially explosive atmospheres (ATEX) directives
        - 2 ATEX directives
            - ATEX 95
                - pertains to equipment and protective systems that are intended to be used in potentially explosive atmospheres.
            - ATEX 137
                - pertains to the workplace and is intended to protect and improve the safety and health of workers at risk from explosive atmospheres.
    - National electrical code (NEC) hazardous locations
        - Standard for the safe installation of electrical equipment & wiring
    - Orientation & Alignment
        - Recommendations by the manufacturer needs to be read before mounting the antenna
        - Weatherproof the cables & connectors & secure them from movement
        - Document & photograph each installation of the access point & antennas
        - Can help in troubleshoot problems in the future & is able to determine if there has been movement in the installation or antenna alignment
    - Safety
        - Be wary of other antennas nearby or the antenna you are working with
            - High directional antennas are focusing high concentrations of RF energy
                - Large amount of energy can be dangerous to your health
        - Do not power on the antenna while working on it
        - Ensure APs & antennas are mounted correctly
    - Maintenance
        - Advisable to periodically perform a visual inspection of the antenna & if needed, verify its status with the installation documentation
        - 2 types of maintenance
            - Preventive
            - Diagnostic

Antenna Accessories

Wednesday, April 22, 2020 11:25 PM

- Cables
  - Introduce signal lose into communication link
  - Attenuation increases with frequency
    - If 2.4GHz WLAN is converted to 5GHz WLAN --> loss caused by the cable will be greater
  - Ensure that the right cable is chosen
    - Improper installation or selection of cables can detrimentally affect the RF communications more than just about any other component or outside influence
  - Ensure that the selected cable will support the frequencies that you will be using
  - Either purchase cables pre-cut & preinstalled with the connectors / hire a professional cabler to install the connections
- Connectors
  - Need to be of the correct impedance to match the other RF equipment
  - On average add about 1/2 dB of insertion loss
- Splitters
  - Takes an RF signal & divides it into 2 or more separate signals
  - Only used in special unique situations
    - e.g. sector antennas
- Amplifiers
  - Provides an overall increase in gain to the signal, normally referred to as active gain
  - Can be unidirectional / bidirectional
  - Increase in power is created using 1 of 2 methods
    - Fixed gain
      - Output of the transceiver is increased by the amount of the amplifier
    - Fixed output
      - Does not add to the output of the transceiver
      - Simply generates a signal equal to the output of the amplifier regardless of the power generated by the transceiver
  - Mainly used to account for signal loss through the cable
  - Required by FCC that amplifiers have unique connectors or electronic ID systems to prevent noncertified antennas from being used
- Attenuators
  - Need to decrease the signal being radiated
  - Available as fixed or variable dB loss
- Lightning arrestors
  - Redirect transient currents caused by nearby lightning strikes or ambient static away from electronic equipment & into the ground
  - Not capable of protecting against a direct strike
  - Should be installed between transceiver & the antenna
- Grounding rods & wires
  - Used to create a path of least impedance

IEEE 802.11 Standards

Wednesday, April 22, 2020 11:42 PM

Original standard

- 1st WLAN standard published
- Defined by IEEE at the physical & MAC layers of OSI model
- 3 original physical layer specifications:
  - Infrared (IR)
    - Uses light-based medium
    - Defined in the original 802.11 standard but is now obsolete
  - Frequency Hopping Spread Spectrum (FHSS)
    - Considered spread spectrum when the bandwidth is wider than what is required to carry the data
    - 802.11 radios are also called Clause 14 devices because of the clause that reference them
  - Direct Sequence Spread Spectrum (DSSS)
    - Another spread spectrum technology
    - DSSS 802.11 radios are known as Clause 16 devices
- Either FHSS or DSSS radios can transmit in the 2.4 GHz ISM band
  - DSSS 802.11 radios can transmit in channels subdivided from the entire 2.4 GHz - 2.4835 GHz ISM band
  - FHSS radios which are permitted to transmit on 1 MHz subcarriers in the 2.402 GHz - 2.480 GHz of the 2.4 GHz ISM band
- Data rates
  - defined by the original 802.11 standard were 1 Mbps & 2 Mbps regardless of which spread spectrum technology was used
  - Is the number of bits per second the Physical layer carries during a single-frame transmission, normally stated as a number of millions of bits per second (Mbps)

IEEE 802.11-2007 ratified amendments

- In 2007, the IEEE consolidated 8 ratified amendments along with the original standard, creating a single document that was published as the IEEE Std 802.11-2007
- 802.11b-1999(802.11b)
  - Physical layer medium that was defined by 802.11b is High-Rate DSSS (HR-DSSS)
  - Operates in the ISM 2.4GHz range
  - Not backwards compatible with legacy 802.11 FHSS devices, but backwards compatible with legacy 802.11 DSSS devices
  - Main Goal : achieve higher data rates in the ISM 2.4 GHz range
  - Complementary Code Keying (CCK) and modulation methods using the phase properties of the RF signal
  - Data rates of 1, 2, 5.5, and 11 Mbps
    - 1,2 Mbps are the backwards compatible ranges
    - 5.5 and 11 are known as HR-DSSS
  - Optional technology called Packet Binary Convolutional Code (PBCC)
- 802.11a-1999 (802.11a)
  - Published the same year as 802.11b
  - Uses the 5GHz spectrum using RF technology called Orthogonal Frequency Division Multiplexing (OFDM)
  - Uses 3 different 100 MHz unlicensed frequency bands in the 5 GHz range, called the Unlicensed National Information Infrastructure (U-NII)
  - 12 channels are available in the original three U-NII bands
  - Operates in the less crowded 5GHz range
  - Supported data rates of 6, 12, and 24 Mbps with a maximum of 54 Mbps
  - With the use of a technology called Orthogonal Frequency Division Multiplexing (OFDM), data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
    --> Cannot communicate with legacy 802.11, 802.11b or 802.11g clients, but can co-exist with them as they are both in different frequencies
- 802.11g-2003 (802.11g)
- new technology called Extended Rate Physical (ERP)
- Transmission : 2.4GHz ISM frequency
- Backwards compatible with 802.11b and 802.11 (DSSS)
- Two mandatory and two optional ERP physical layers (PHYs) were defined
  - 2 mandatory PHYs
    - ERP-OFDM
    - ERP-DSSS/CCK
  - 2 optional PHYs

        - ERP-PBCC
        - DSSS-OFDM
- Extended Rate Physical DSSS (ERP-DSSS/CCK)
    - Data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps using a PHY technology
- No difference between OFDM and ERP-OFDM
    - only difference is the transmit frequency
- When 802.11g was ratified it trigger huge sales in SOHO and enterprise markets because of the higher data rates and the backwards compatibility with older equipment
- ERP-OFDM and ERP-DSSS/CCK technologies can coexist, yet they cannot speak to each other.
    - protection mechanism that allows the two technologies to coexist
        - its goal was to prevent the different technologies transmitting at the same time
- 802.11d-2001
    - added requirements and definitions necessary to allow 802.11 WLAN equipment to operate in areas not served by the original standard
    - Country code information is delivered in beacons and probe responses
        - used by 802.11d compliant devices to ensure they are abiding by the countries rules and regulations for frequency and power
- 802.11h-2003
    - Defines mechanisms for dynamic frequency selection (DFS) and transmit power control (TPC)
    - Main reason : detect and avoid interference with 5 GHz satellite and radar systems
    - Introduced new frequency band called U-NII-2 Extended with 11 more channels

Band frequency range	Amendment	Channels
U-NII-1 (lower) 5.150 GHz–5.250 GHz	802.11a	4
U-NII-2 (middle) 5.250 GHz–5.350 GHz	802.11a	4
U-NII-2 Extended 5.47 GHz–5.725 GHz	802.11h	11
U-NII-3 (upper) 5.725 GHz–5.825 GHz	802.11a	4

    - DFS
        - used for spectrum management of 5 GHz channels by OFDM radio devices
        - used for radar avoidance
        - Radar-detector & radar-interference avoidance technology
        - Satisfy regulatory requirement
    - TPC
        - used to regulate the power levels used by OFDM radio cards in the 5 GHz frequency bands
        - used to meet the regulatory transmission power requirements
    - Information used by both DFS and TPC is exchanged between client stations and APs inside of management frames
- 802.11i-2004
    - Major security enhancements under 802.11i
        - Data Privacy
            - Confidentially is addressed by Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which uses the Advanced Encryption Standard (AES) algorithm
            - 802.11i also defines an optional encryption method known as Temporal Key Integrity Protocol (TKIP), which uses the RC-4 stream cipher
        - Data Integrity
            - methods to ensure that the encryption method has not been tamped with
                - WEP uses a data integrity method called the Initialization Check Value (ICV)
                - TKIIP uses a method known as the Message Integrity Check (MIC)
                - CCMP uses a much stronger MIC and other mechanisms
            - The 802.11 frames uses a 32-bit CRC known as the frame check sequence (FCS) to protect the entire frame
    - Authentication
        - 2 methods
            - Pre-shared keys (PSKs)
                - 802.1X authorization framework
                - Extensible Authentication Protocol (EAP)
                    - 802.11i amendment does not specify what EAP method to use
            - Robust Security Network (RSN)
                - Defines the entire method for authentication, generating encryption keys for clients and APs
    - Wi-Fi Alliance also has a certification known as Wi-Fi Protected Access 2 (WPA2)
        - WPS2 if fully compliant with 802.11i
    - 802.11j-2004
        - Obtain Japanese regulatory approval by enhancing the 802.11 MAC and 802.11a PHY to additionally operate in Japanese 4.9 GHz and 5 GHz bands

        - OFDM channel spacing of 10 MHz, which results in available bandwidth data rates of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps
    - 802.11e-2005
    - Layer 2 MAC methods needed to meet the QoS requirements for time-sensitive applications over IEEE 802.11 WLANs
    - The original 802.11 defined two methods to gain control of the half duplex medium:
        - Distributed Coordination Function (DCF)
            - Contention-based method determining who gets to transmit on the wireless medium next
        - Point Coordination Function (PCF)
            - Access point briefly takes control of the medium and polls the clients
            - Never adopted by WLAN vendors
    - 802.11e amendment defines enhanced medium access methods to support QoS requirements
        - Hybrid Coordination Function (HCF)
            - 2 access mechanisms to provide QOS
                - Enhanced Distributed Channel Access (EDCA)
                    - extension to DCF
                    - provide for the "prioritization of frames" based on upper-layer protocols
                - Hybrid Coordination Function Controlled Channel Access (HCCA)
                    - extension of PCF
                    - Gives the access point the ability to provide for "prioritization of stations."
                    - Like PCF never adopted by WLAN vendors
    - Wi-Fi Alliance also has a certification known as Wi-Fi Multimedia (WMM)

IEEE 802.11-2012 ratified amendments

- 802.11r-2008
    - Fast basic service set transition (FT)
    - Fast secure roaming because it defines faster handoffs when roaming occurs between cells in a WLAN using the strong security defined by a robust secure network (RSN)
    - Multiple types of fast secure roaming are implemented by different vendors
        - CCKM
        - PKC
        - OKC
        - fast session resumption
- 802.11k-2008
- radio resource measurement (RRM)
- Some of the key radio resource measurements defined under 802.11k
        - Transmit Power Control (TPC)
            - 802.11h defined this for 5GHz frequency --> 802.11k brings it in for other bands
        - Client Statistics
        - Physical layer information
            - signal-to-noise, signal strength, data rates can be reported back to the access point
        - Channel Statistics
            - Noise floor information and Channel load information can be reported back to the access point
        - Neighbor Reports
            - Ability to learn details about other access points that the client might want to roam to from the access point or the WLAN Controller
- 802.11y-2008
    - allow high-powered, shared 802.11 operations with other non-802.11 devices in the 3650 MHz–3700 MHz licensed band in the United States
    - requires content-based protocol (CBP) mechanisms to avoid interference between devices
    - defines dynamic STA enablement (DSE) procedures
- 802.11w-2009
    - Robust management frames
    - Designed to prevent DOS attacks against management frames
    - When unicast management frames are protected, frame protection is achieved by using CCMP
    - Broadcast and multicast frames are protected using the Broadcast/Multicast Integrity Protocol (BIP)
- 802.11n-2009
    - Increase the throughput in both the 2.4 GHz and 5 GHz frequency bands
    - New operation known as High Throughput (HT)
    - Provides PHY and MAC enhancements to support data rates of up to 600 Mbps
    - Multiple-input, multiple-output (MIMO) technology in unison with OFDM technology
    - 802.11n radios are also backward compatible with legacy 802.11a/b/g radios
    - 40 MHz channel width available
- 802.11p-2010
    - Support Intelligent Transportation Systems (ITS) applications

    - Data exchanges between high-speed vehicles is possible in the licensed ITS band of 5.9 GHz
    - Known as Wireless Access in Vehicular Environments (WAVE)
    - 802.11p will also be applicable to marine and rail communications
- 802.11z-2010
    - Direct Link Setup (DLS) mechanism
    - DLS allows client stations to bypass the access point and communicate with direct frame exchanges
    - DLS communications have yet to be used by enterprise WLAN vendors
- 802.11u-2011
    - Wireless Interworking with External Networks (WIEN)
    - basis for the Wi-Fi Alliance's Hotspot 2.0 specification and its Passpoint certification
    - This standard and certification is designed to provide seamless roaming for wireless devices between your Wi-Fi network and other partner networks, similar to how cellular telephone networks provide roaming
- 802.11v-2011
    - Provides for an exchange of information that can potentially ease the configuration of client stations wirelessly from a central point of management
    - Defines Wireless Network Management (WNM)
- 802.11s-2011
    - Standardizing mesh networking using the IEEE 802.11 MAC/PHY layers
    - defines the use of mesh points, which are 802.11 QoS stations that support mesh services
    - Mesh access point (MAP)
        - device that provides both mesh functionalities and AP functionalities simultaneously
    - Mesh point portal (MPP)
        - device that acts as a gateway to one or more external networks such as an 802.3 wired backbone

Post-2012 ratified amendments

- 802.11ae-2012
    - Enhancements to QoS management
    - Quality-of-service management frame (QMF) service can be enabled
- 802.11aa-2012
    - QoS enhancements to the 802.11 Media Access Control (MAC) for robust audio and video streaming for both consumer and enterprise applications
- 802.11ad-2012
    - defines Very High Throughput (VHT) enhancements using the much higher unlicensed frequency band of 60 GHz
    - higher frequency range is big enough to support data rates of up to 7 Gbps, downside is its limited to line of sight
    - Galois/Counter Mode Protocol (GCMP), which also uses AES cryptography
- 802.11ac-2013
    - Defines Very High Throughput (VHT) enhancements below 6 GHz
    - 5GHz frequency only
    - 802.11ac promises Gigabit speeds using 4 major enhancements:
        - Wider Channels
            - Ability to use 80 and 160 MHz channels
        - New Modulation
            - 256-QAM modulation
                - potential to improve increase speed by 30%
                - requires very high SNR
        - More Spatial Streams
            - Up to 8 spatial streams, although first gen 802.11ac will use 1 -4 spatial streams
        - Improved MIMO and Beamforming
            - multi-user MIMO (MU-MIMO) technology
            - utilize a simplified beamforming method called null data packet (NDP) beamforming
- 802.11af-2014
    - use of wireless in the newly opened TV white space (TVWS) frequencies between 54 MHz and 790 MHz

IEEE 802.11 draft amendments

- 802.11ah
    - Wi-Fi in frequencies below 1 GHz
        - lower frequencies will mean lower data rates but longer distances
    - Likely use is IoT sensors and a Wi-Fi back hall
- 802.11ai
    - fast initial link setup (FILS)
    - STA to establish a secure link setup in less than 100 ms
- 802.11aj
    - modifications to the IEEE 802.11ad-2012 amendment's PHY and MAC layer to provide support for operating in the Chinese Milli-Meter Wave (CMMW) frequency bands
- 802.11ak

    - referred to as General Link (GLK)
    - enhancement to 802.11 links for use in bridged networks
- 802.11aq
    - enables delivery of network service information prior to the association of stations on an 802.11 network

Defunct amendments

- Amendments considered dead in the water
    - 802.11F
    - standard mandated that vendor access points support roaming
    - was intended to address roaming interoperability between autonomous access points from different vendors
    - 802.11T
    - called Wireless Performance Prediction (WPP)

802.11m Task group

- This task group also is responsible for “rolling up” ratified amendments into a published document

Wireless Networks & Spread Spectrum Technologies

Thursday, April 23, 2020 09:55 PM

Industrial, scientific & medical bands (ISM)

- Defined by the ITU Telecommunication standardization sector (ITU-T)
- License-free
- No restrictions on what types of equipment can be used in any of them
- Frequency ranges of ISM bands are as follows
    - 900 MHz ISM bands (industrial band)
        - 26 MHz wide
        - Spans from 902 MHz - 928 MHz
        - Was used for wireless networking, but now use higher frequencies which are capable to grater throughput
        - Many parts of 900 MHz bands are issued to Global system for Mobile Communication (GSM) for used by mobile phones
        - 802.11 radios do not operate in the 900 MHz ISM bands
    - 2.4 GHz ISM band (scientific band)
        - 100 MHz wide
        - Spans from 2.4 GHz - 2.5 GHz
        - Following wireless radio uses this band
            - 802.11 (FHSS / DSSS radio)
            - 802.11b (HR-DSSS radios)
            - 802.11g (ERP radios)
            - 802.11n (HT radios)
            - Also used by microwave ovens, cordless home telephones, baby monitors & wireless video camera
            - Heavily used
            - 1 of the biggest disadvantage is the potential for interference
            - Not every regulatory body will allow transition in the entire 2.4 GHz ISM band
        - 5.8 GHz ISM band (medical band)
        - 150 MHz wide
        - spans from 5.725 GHz to 5.875 GHz
        - Used by many of the same types of consumer products
            - baby monitors
            - cordless telephones
            - cameras
        - Not uncommon to confuse the 5.8 GHz ISM band with the U-NII-3 band which spans from 5.725 GHz to 5.85 GHz
        - The United States has also always allowed OFDM transmissions on channel 165, which until April of 2014, resided in the 5.8 GHz ISM band
        - From the perspective of Wi-Fi channels, the 5.8 GHz ISM band is no longer relevant, however, many of the consumer devices that operate in the 5.8 GHz ISM band can cause RF interference with 802.11 radios that transmit in the U-NII-3 band

Unlicensed National Information Infrastructure bands (U-NII)

- Wi-Fi radios that currently transmit in the 5 GHz U-NII bands include radios that use the following technologies
    - 802.11a (OFDM radios)
    - 802.11n (HT radios)
    - 802.11ac (VHT radios)
- U-NII-1 (lower band)
    - 100 MHz wide
    - spans from 5.150 GHz to 5.250 GHz
    - Four 20 MHz 802.11 channels reside in the U-NII-1 band

    - FCC used to restrict U-NII-1 Band to indoor use – after 2004 this has been lifted
    - Prior to 2004 FCC required that Aps had permeant antennas to use this band, after 2004 allow detachable antennas, providing that the antenna connector is unique
- U-NII-2 (middle band)
    - 100 MHz wide
    - spans from 5.250 GHz to 5.350 GHz.
    - Four 20 MHz 802.11 channels reside in the U-NII-2 band.
    - Radios that transmit in the U-NII-2 band must support dynamic frequency selection (DFS)
- U-NII-2 Extended
    - 255 MHz wide
    - spans from 5.470 GHz to 5.725 GHz
    - Most 5 GHz 802.11 radios can transmit on a total of eleven 20 MHz 802.11 channels that reside in the U-NII-2 band
    - With 802.11ac , a new channel 144 has been added to the U-NII-2 Extended band – taking total to 12 channels
    - Radios that transmit in the U-NII-2 band must support dynamic frequency selection (DFS)
- U-NII-3 (upper band)
    - 125 MHz wide
    - spans from 5.725 GHz to 5.850 GHz.
    - Typically used for outdoor point-to-point communications
    - Many of the countries in Europe do not use the U-NII-3 band for WLAN unlicensed communications
    - Five 20 MHz 802.11 channels reside in the U-NII-3 band
    - In April of 2014, the FCC expanded the size of the U-NII-3 band from 100 MHz to 125 MHz. Channel 165, formerly in the 5.8 GHz ISM band, is now available as part of the U-NII-3 band

Band	Frequency	Channels
U-NII-1 (lower)	5.150 GHz–5.250 GHz	4
U-NII-2 (middle)	5.250 GHz–5.350 GHz	4
U-NII-2 Extended	5.47 GHz–5.725 GHz	12 (as channel 144 was added with 802.11ac)
U-NII-3 (upper)	5.725 GHz–5.825 GHz	4

- Future U-NII bands
    - In Jan 2013 the FCC announced that 195 MHz of additional spectrum space would be made available for unlicenced use
    - 2 proposed U-NII bands are:
    - U-NII-2B
        - 120 MHz wide band
        - spans from 5.35 GHZ to 5.47 GHz
        - Six potential 20 MHz wide channels
    - U-NII-4
        - 75 MHz wide band
        - spans from 5.85 GHZ – 5.925 GHz
        - 4 potential 20 MHz wide channels

3.6 GHz band

- Frequency range : 3.65 GHz - 3.7 GHz
- Included limitations when used near certain satellite earth stations
- Designed to operate in any 5 MHz, 10 MHz, or 20 MHz channel
- Although the project was designed for use in the United States, it was carefully designed

to be able to operate in other countries without the need to ratify a new amendment

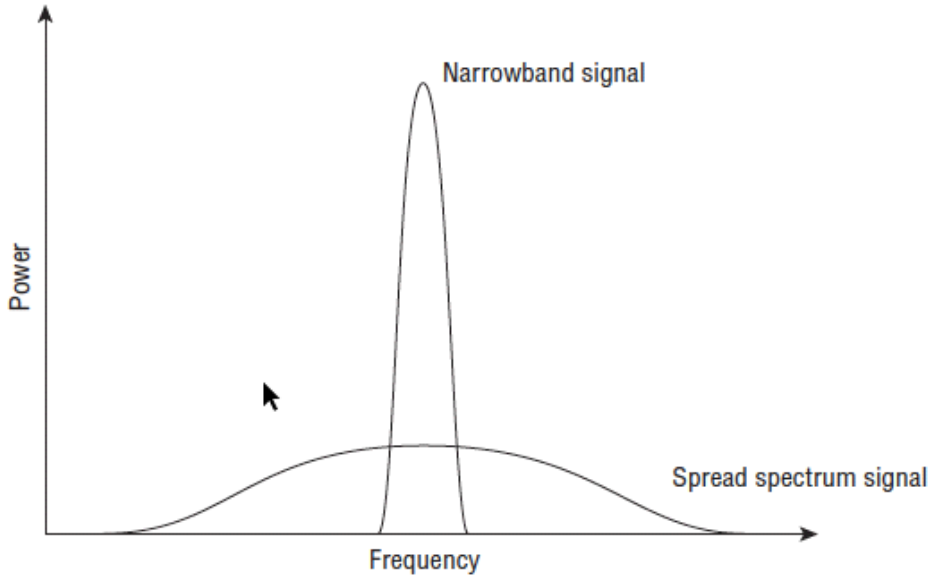
4.9 GHz band

- Frequency range of 4.94 GHz to 4.99 GHz in the United States for public safety organizations
- use for the protection of life, health, or property.
- Licensed band and is reserved strictly for public safety
- 802.11j amendment was ratified, providing support for the 4.9 GHz to 5.091 GHz frequency range for use in Japan

Future Wi-Fi frequencies

- 60 GHz
  - Speeds up to 7 Gbps
  - Difficulty penetrating through walls
  - Will not be backward compatible with other 802.11 technology
  - Wi-Fi Alliance designated the WiGig certification to test interoperability of products that operate in the 60 GHz band
- White-Fi
  - Wi-Fi technology in the unused television RF spectrum also known as TV white space

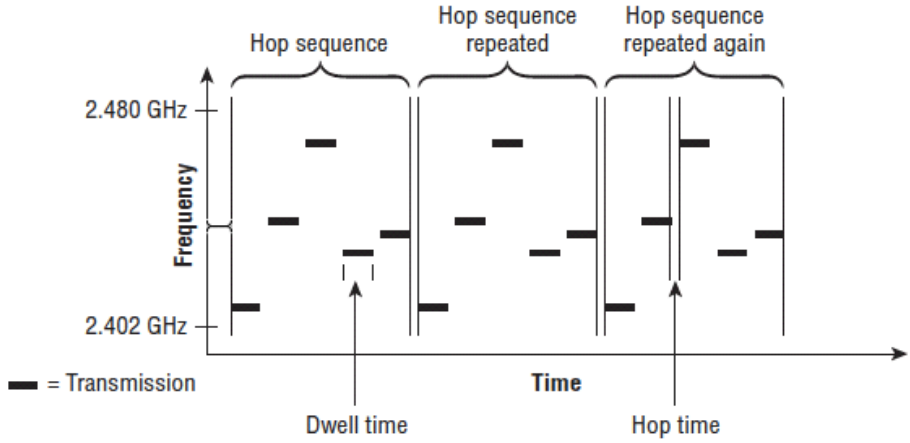
Narrowband and spread spectrum



- 2 primary radio frequency (RF) transmission methods:
  - Narrowband
    - Uses very little bandwidth to transmit the data that it is carrying
    - Intentional jamming or unintentional interference of this frequency range is likely to cause disruption in the signal
  - Spread spectrum
    - Uses more bandwidth than is necessary to carry its data
    - Typically less susceptible to intentional jamming or unintentional interference from outside sources, unless the interfering signal was also spread across the range of frequencies used by the spread spectrum communications
- Multipath interference
  - Think of Multipath interference as an Echo of your first word arriving over the top of your second word
  - If the delay spread is too great, data from the reflected signal may interfere with the same data stream from the main signal; this is referred to as intersymbol interference (ISI).
  - Spread spectrum systems are not as susceptible to ISI because they spread their signals across a range of frequencies 802.11 (DSSS) and 802.11b (HR-DSSS) can tolerate delay spread of up to 500 nanoseconds
  - Prior to 802.11n and 802.11ac MIMO technology, multipath had always been a concern

Frequency hopping spread spectrum (FHSS)

- works is that it transmits data by using a small frequency carrier space, then hops to another small frequency carrier space and transmits data, then to another frequency, and so on



- Hopping sequence
  - Uses a predefined sequence
  - Each time the hop sequence is completed, it is repeated
  - Original IEEE 802.11 standard mandates that each hop is 1 MHz in size
- Dwell time
  - Amount of time that the FHSS system transmits on a specific frequency before it switches to the next frequency in the hop set
  - Regulatory bodies typically limits the amount of dwell time
- Hop time
  - Not a specified period of time but rather a measurement of the amount of time it takes for the transmitter to change from one frequency to another
- Modulation
  - Uses Gaussian frequency shift keying (GFSK) to encode the data

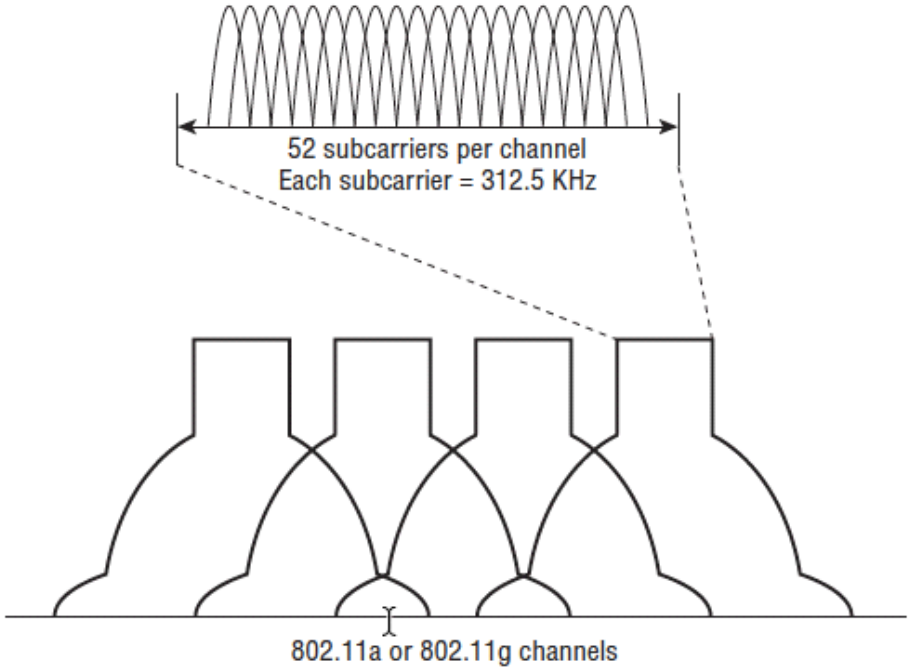
Direct sequence spread spectrum (DSSS)

- Was defined in the original 802.11 standard to provide 1 & 2 Mbps on the 2.4GHz ISM Band
- 802.11b 5.5 and 11 Mbps speeds are known as High-Rate DSSS (HR-DSSS)
- 802.11b is backwards compatible with 802.11 DSSS
- 802.11b devices are not capable of transmitting using FHSS --> not backward compatible with 802.11 FHSS devices
- Set to one channel
  - Data that is being transmitted is spread across the range of frequencies that make up the channel
- DSSS data encoding
  - To provide resilience against data corruption, each bit of data is encoded and transmitted as multiple bits of data
  - Task of adding additional, redundant information to the data is known as processing gain
  - Converts the 1 bit of data into a series of bits that are referred to as chips
  - This sequence of chips is then spread across a wider frequency space
    - Although 1 bit of data might need only 2 MHz of frequency space, the 11 chips will require 22 MHz of frequency carrier space
  - When the Barker code is used, as many as 9 of the 11 chips can be corrupted, yet the receiving radio will still be able to interpret the sequence and convert them back into a single data bit
- Modulation
  - Differential binary phase shift keying (DBPSK) utilizes two phase shifts
    - one that represents a 0 chip
    - another that represents a 1 chip

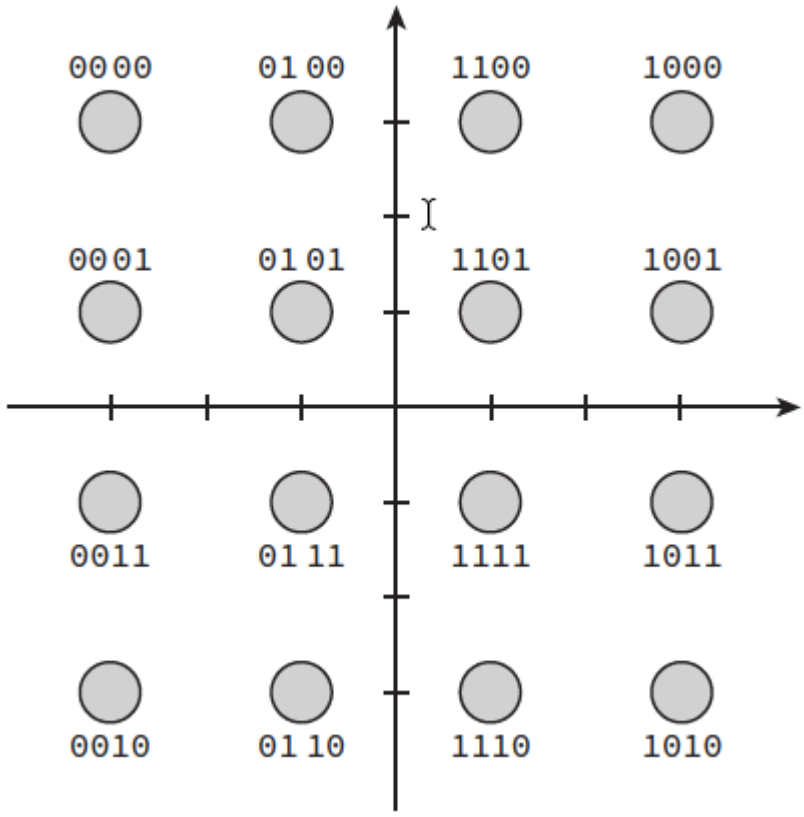
Packet Binary Convolutional Code (PBCC)

- Is a modulation technique that supports data rates of 5.5, 11, 22, and 33 Mbps
- PBCC modulation was originally defined as optional under the 802.1b amendment
- 802.11g amendment allowed for two additional optional ERP-PBCC modulation modes with payload data rates of 22 and 33 Mbps

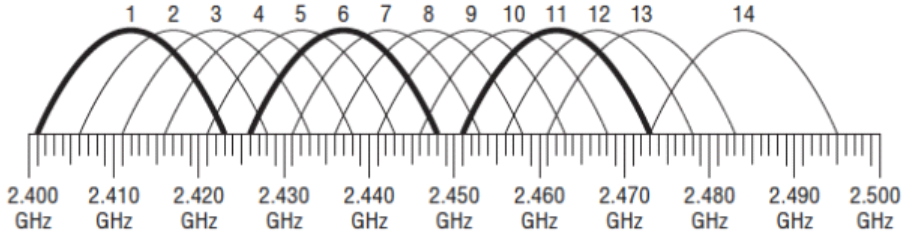
Orthogonal Frequency Division Multiplexing (OFDM)



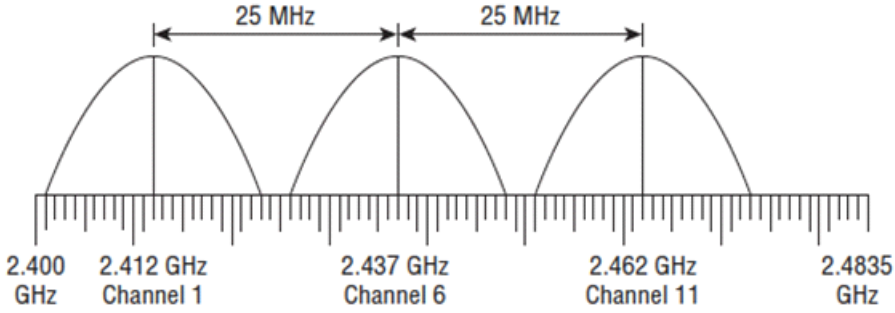
- One of the most popular communications technologies, used in both wired and wireless communications
- OFDM is not a spread spectrum technology, even though it has similar properties
- OFDM actually transmits across 52 separate, closely and precisely spaced frequencies, often referred to as subcarriers
- 48 of the subcarriers are used to transmit data
- The other four are used as references for phase and amplitude by the demodulator, allowing the receiver to synchronize itself as it demodulates the data in the other subcarriers
- Convolutional coding
  - To make OFDM more resistant to narrowband interference, a form of error correction known as convolutional coding is performed.
  - is a forward error correction (FEC) that allows the receiving system to detect and repair corrupted bits
- Modulation
  - OFDM uses binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK) phase modulation for the lower ODFM data rates
  - Higher data rates use Quadrature amplitude modulation (QAM) modulation
  - Constellation diagram, also known as a constellation map, is a two dimensional diagram often used to represent QAM modulation



- 2.4 GHz channels
  - The IEEE 802.11-2012 standard divides the 2.4 GHz ISM band into 14 separate channels
  - Regulatory bodies determine which channels are available to be used in each country
  - Channels are designated by their center frequency
  - DSSS and HR-DSSS 802.11 radios are transmitting, each channel is 22 MHz wide and is often referenced by the center frequency +/- 11 MHz
  - Within the 2.4 GHz ISM band, the distance between channel center frequencies is only 5 MHz, because of this the channels will have overlapping frequency space



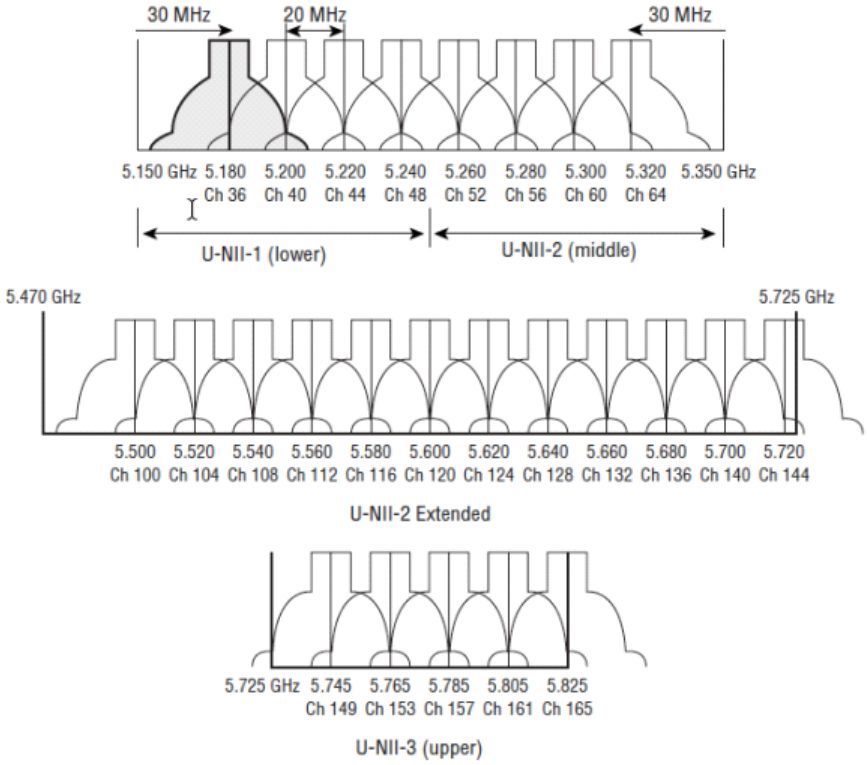
- Non overlapping channels



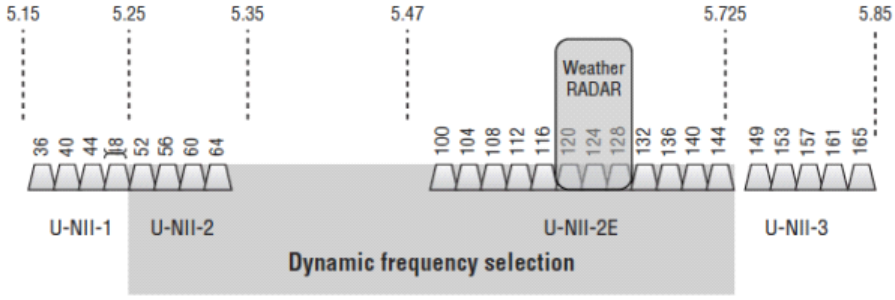
5 GHz channels

- 5 GHz U-NII bands: U-NII-1, U-NII-2, U-NII-2 Extended, and U-NII-3.
- The original three U-NII bands each had four non-overlapping channels with 20 MHz

separation between the centre frequencies
    - fifth channel was recently added to U-NII-3.
- U-NII-2 Extended band has 12 non-overlapping channels with 20 MHz of separation between the center frequencies
    - U-NII-2 Extended was 11 channels for many years until channel 144 was added with 802.11ac was released
- Channels used are regulated by local regulatory bodies



- DFS is required in U-NII-2 and U-NII-2E channels to avoid interference with radar



Adjacent, non-adjacent, and overlapping channels

- When deploying a WLAN, it is important to have overlapping cell coverage for roaming to occur. However, it is just as important for these coverage cells not to have overlapping frequency space
- A channel reuse pattern is needed because overlapping frequency space causes degradation in performance

Throughput vs. bandwidth

- Frequency band is the bandwidth
- Data encoding, modulation, medium contention, encryption, and many other factors also play a large part in data throughput
- Care should be taken not to confuse frequency bandwidth with data bandwidth
- OFDM 802.11a radios can transmit at 6, 9, 12, 18, 24, 36, 48, or 54 Mbps, yet the frequency bandwidth for all the U-NII band channels is the same for all of these speeds
- Because of the half-duplex nature of the medium and the overhead generated by CSMA/CA, the actual aggregate throughput is typically 50 percent or less of the data rates for 802.11a/b/g legacy transmissions, and 60-70 percent of the data rates for 802.11n/ac transmissions.

WLAN topologies

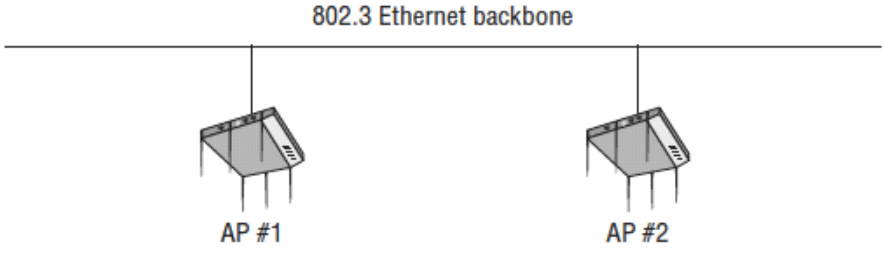
Friday, April 24, 2020 09:23 PM

- Wireless wide area network (WWAN)
  - Provides RF coverage over a vast geographical area
  - Typically use cellular telephone technologies / proprietary licensed wireless bridging technologies
    - e.g.
      - General packet radio server (GPRS)
      - Code division multiple access (CDMA)
      - Time division multiple access (TDMA)
      - Long term evolution (LTE)
      - Global system for mobile communications (GSM)
- Wireless metropolitan area network (WMAN)
  - Provides RF coverage to a metropolitan area
    - e.g. city & the surrounding suburbs
  - Worldwide interoperability for microwave access (WiMAX)
- Wireless personal area network (WPAN)
  - Wireless computer network used for communication between computer devices within close proximity of a user
  - Most common technologies in WPAN
    - Bluetooth
    - Infrared
  - Peer-to-peer connections
- Wireless local area network (WLAN)
  - Local area networks provide networking for a building or campus environment

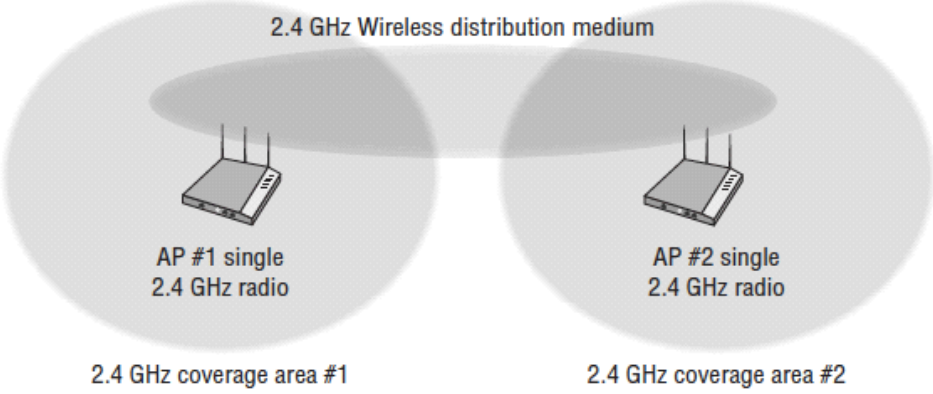
802.11 technologies

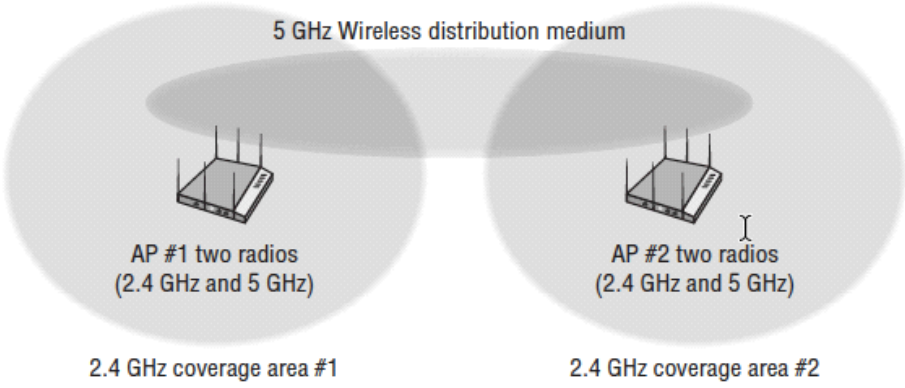
Monday, April 27, 2020 11:14 AM

- Access point (AP)
  - Half-duplex device with switchlike intelligence
    - Switchlike intelligence is defined as control & data plane mechanisms
  - 'thin/lightweight' refers to APs that are controller based for the switchlike intelligence
  - Autonomous APs also have switchlike intelligence
- Client station
  - Any radio that is not used in access point
    - e.g. laptops, tablets, scanners, smartphones
  - Must contend or the half-duplex RF medium in the same manner that an access point radio contends for the RF medium
- Integration service (IS)
  - Frame format transfer method
  - 802.11 data frame payload must be effectively transferred into an 802.3 Ethernet frame even though it uses different physical medium as compared to wired infrastructure
  - Normally takes place inside a WLAN controller when 802.11 user traffic is tunneled back to a WLAN controller
- Distribution system (DS)
  - Used to interconnect a set of basic service sets (BSS) via integrated LANs to create an extended service set (ESS)
  - Distribution system medium (DSM) is a logical physical medium used to connect access points
    - Common e.g. 802.3 medium



- Wireless distribution system (WDS)
  - Mechanism for wireless communication using a 4-MAC-address frame format
  - Can connect access points together using what is referred to as a wireless backhaul
    - Backhaul : use of wireless communications systems to get data from an end user to a node in a major network
  - Can use 1 radio for backhaul & client access but results in degraded throughput as RF is shared medium
  - Can also backhaul on 1 band & provide access on another or both





    - e.g. of WDS
        - Bridging
        - Repeaters
        - Mesh networks
- Service set identifier (SSID)
    - Logical name used to identify an 802.11 wireless network
    - Can be made up of as many as 32 characters & is case sensitive
    - Can hide SSID but is a very weak security not defined under 802.11-2012 standard
- Basic service set (BSS)
    - Cornerstone topology of an 802.11 network
    - Communicating devices that make up a BSS consist of 1 AP radio with 1 or more client stations
    - Stations that are members of a BSS have a layer 2 connection & are called associated
    - Typical BSS
        - Client stations cannot communicate directly with each other unless they go through the AP
- Basic service set identifier (BSSID)
    - 48-bit (6-octet) MAC address f an access point's radio
    - Proper definition is the layer 2 identifier of each individual BSS
- Basic service area (BSA)
    - Physical layer of coverage provided by an access point in a BSS
- Size & shape of a BSA depends on many variables, including AP transmit power, antenna gain & physical surroundings
- Extended service set (ESS)
    - 2 or more basic service sets connected by a distribution system medium
    - No requirement for BSAs to overlap to provide seamless roaming
- Independent basic service set (IBSS)
    - Radios that make up an IBSS network consist solely of client stations (STAs) & no access point is deployed
    - Can have multiple client stations in 1 physical area communicating in an ad hoc fashion
    - All of the stations transmit frames to each other directly & do not route their frames from one client to another
    - All stations must be transmitting on the same frequency channel
- Mesh basic service set (MBSS)
    - Mesh functions are used to provide wireless distribution of network traffic & the set of APs that provide mesh distribution form a mesh basic service set (MBSS)
- QoS basic service set (QoS BSS)
    - QoS mechanisms can be implemented within all of the 802.11 service set
    - QoS enhancements are available to QoS STAs associated with a QoS access point in a QoS BSS

802.11 configuration mode

Monday, April 27, 2020 01:13 PM

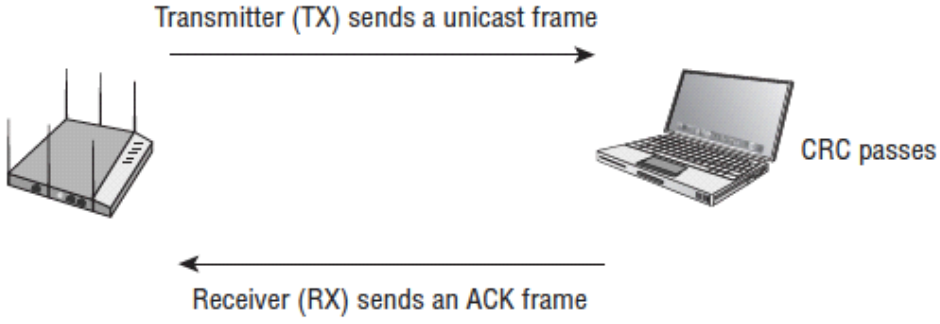
- Access point mode
  - Bridge mode
    - AP radio is converted into a wireless bridge
    - Adds extra MAC-layer intelligence to the device & gives the AP the capability to learn & maintain tables about MAC addresses from the wired side of the network
  - Workgroup bridge mode
    - Provides wireless backhaul for connected 802.3 wired clients
  - Repeater mode
    - Extends the coverage area of a portal AP on the same channel
  - Mesh mode
    - AP radio operates as a wireless backhaul radio for a mesh environment
  - Scanner mode
    - AP radio is converted into a sensor radio, allowing the AP to integrate into a wireless intrusion detection system (WIDS) architecture
- Client station mode
  - Infrastructure mode
    - Client station will allow communication via an access point
  - Ad Hoc mode
    - Participate in an IBSS topology & do not communicate via an access point

802.11 Medium Access

Monday, April 27, 2020 01:21 PM

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) vs. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

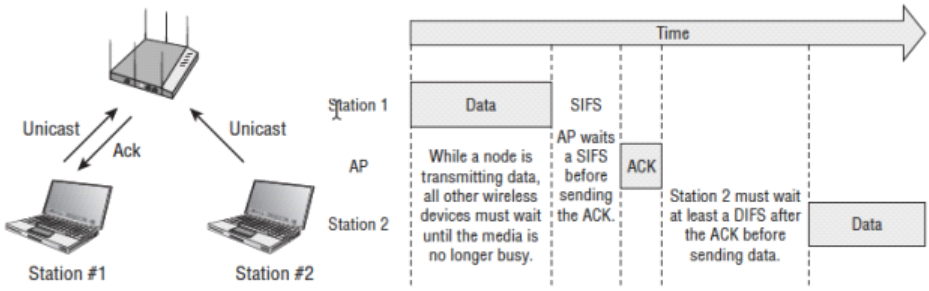
- Set of rules to provide controlled and efficient access to the network medium
- CSMA/CD
  - well known
  - Also used by Ethernet networks
- CSMA/CA
  - not as well known
  - Used by 802.11 networks
- The difference between CSMA/CD and CSMA/CA exists at the point when a client wants to transmit and no other clients are presently transmitting
- CSMA/CD
  - Nodes can immediately start transmitting
  - If a collision is detected then they temporary stop transmitting
- CSMA/CA
  - 802.11 wireless radios are not capable of transmitting and receiving at the same time
    - so they are not capable of detecting a collision during their transmission
  - Station has determined that no other stations are transmitting, the 802.11 radio will choose a random backoff value
  - Carrier sense determines whether the medium is busy
  - Multiple access ensures that every radio gets a fair shot at the medium (but only one at a time)
  - Collision avoidance means only one radio gets access to the medium at any given time, hopefully avoiding collision
- Collision detection
  - Every time an 802.11 radio transmits a unicast frame, if the frame is received properly, the 802.11 radio that received the frame will reply with an acknowledgment (ACK) frame
  - The ACK frame is a method of delivery verification of unicast frames
  - 802.11n and 802.11ac radios make use of frame aggregation –> block ACK
  - Broadcast and multicast frames do not require an acknowledgment
  - If any portion of a unicast frame is corrupted, the cyclic redundancy check (CRC) will fail and the receiving 802.11 radio will not send an ACK frame
  - if an ACK frame is not received by the original radio, there is collision assumption



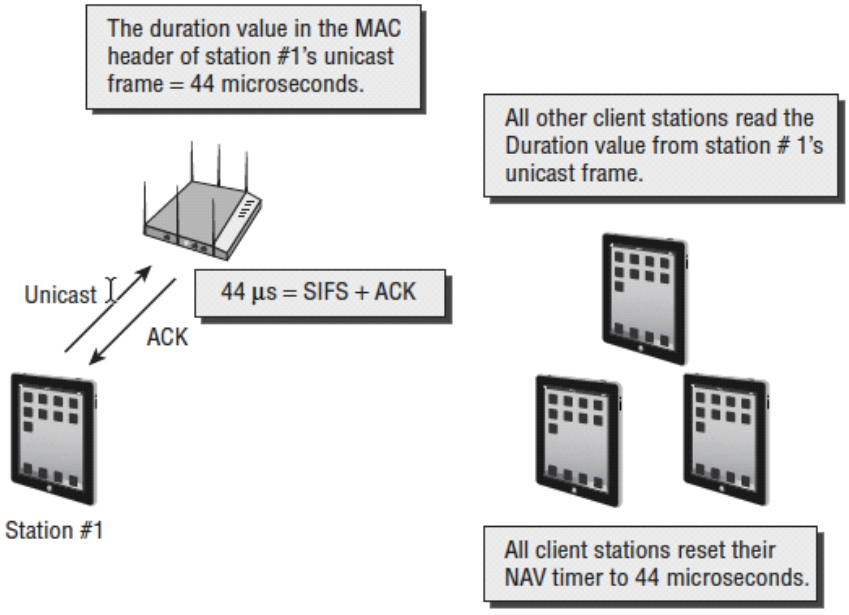
Distributed Coordination Function (DCF)

- Interframe space (IFS)
  - Is a period of time that exists between transmissions of wireless frames
  - 3 Types
    - Reduced interframe space (RIFS)
      - highest priority
    - Short interframe space (SIFS)
      - second highest priority

        - PCF interframe space (PIFS)
            - middle priority
        - DCF interframe space (DIFS)
            - lowest priority
        - Arbitration interframe space (AIFS)
            - used by QoS stations
        - Extended interframe space (EIFS)
            - used after receipt of corrupted frames
    - Interframe spaces are all about what type of 802.11 traffic is allowed next



- Duration/ID field
    - One of the fields in the MAC header of an 802.11 frame
    - Duration/ID value represents the time (in microseconds)
        - that is required to transmit an active frame exchange process so that other radios do not interrupt the process
    - Value of the Duration/ID field indicates how long the RF medium will be busy before another station can contend for the medium
- Virtual Carrier sense
    - Uses a timer mechanism known as the network allocation vector (NAV)
    - NAV timer maintains a prediction of future traffic on the medium based on Duration value information seen in a previous frame transmission



- Physical Carrier Sense
    - Mechanism to determine if the medium is busy
    - Performed constantly by all stations that are not transmitting or receiving
    - It is actually listening to the channel to see whether any other transmitters are taking up the channel
    - Physical carrier sense has 2 purposes:
        - Determine whether a frame transmission is inbound for a station to receive
            - If the medium is busy, the radio will attempt to synchronize with the transmission
        - Determine whether the medium is busy before transmitting

        - □ known as the clear channel assessment (CCA)
        - □ involves listening for RF transmissions at the Physical layer
        - □ medium must be clear before a station can transmit
- Random backoff timer
    - 802.11 station may contend for the medium during a window of time known as the backoff time
    - The station chooses a random number from a range called a contention window (CW) value
        - After the random number is chosen, the number is multiplied by the slot time value.
    - When the backoff time is equal to 0, the client can reassess the channel and, if it is clear, begin transmitting.

Point Coordination Function (PCF)

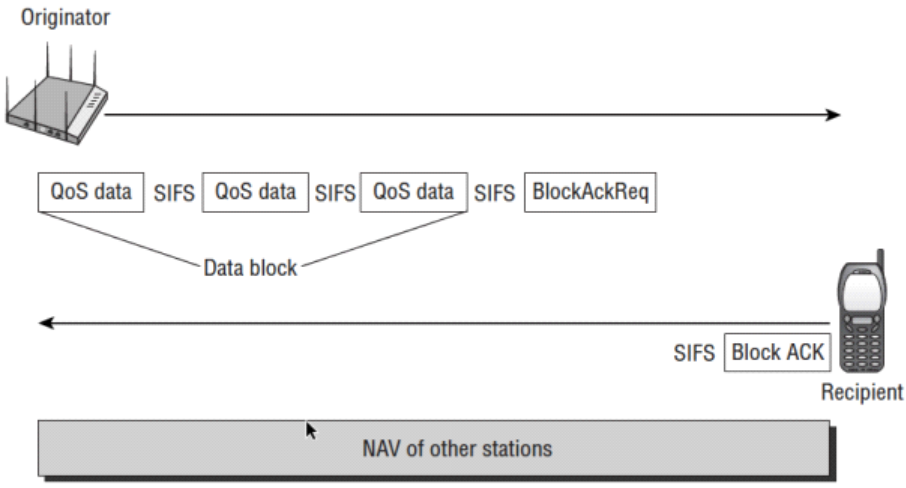
- Optional medium access
- Form of polling
- AP performs the function of the point coordinator (PC)
- PCF medium access method will work in only a basic service set (BSS)
- Because polling is performed from a central device, PCF provides managed access to the medium.
- Both the AP and the station must support it

Hybrid Coordination Function (HCF)

- Defines the ability for an 802.11 radio to send multiple frames when transmitting on the RF medium
- When an HCF-compliant radio contends for the medium, it receives an allotted amount of time to send frames.
    - Period of time is called a transmit opportunity (TXOP)
- Frame burst
    - 802.11 radio may send multiple frames
    - A short Interframe space (SIFS) is used between each frame to ensure that no other radios transmit during the frame burst
- Enhanced Distributed Channel Access (EDCA)
    - Wireless media access method that provides differentiated access that directs traffic to four access-category QoS priority queues.
    - EDCA defines four access categories
        - AC_BK (Background)
        - AC_BE (Best Effort)
        - AC_VI (Video)
        - AC_VO (Voice)
- HCF Controlled Channel Access (HCCA)
    - Is a wireless media access method that uses a QoS-aware centralized coordinator known as a hybrid coordinator (HC)

Block acknowledgment (BA)

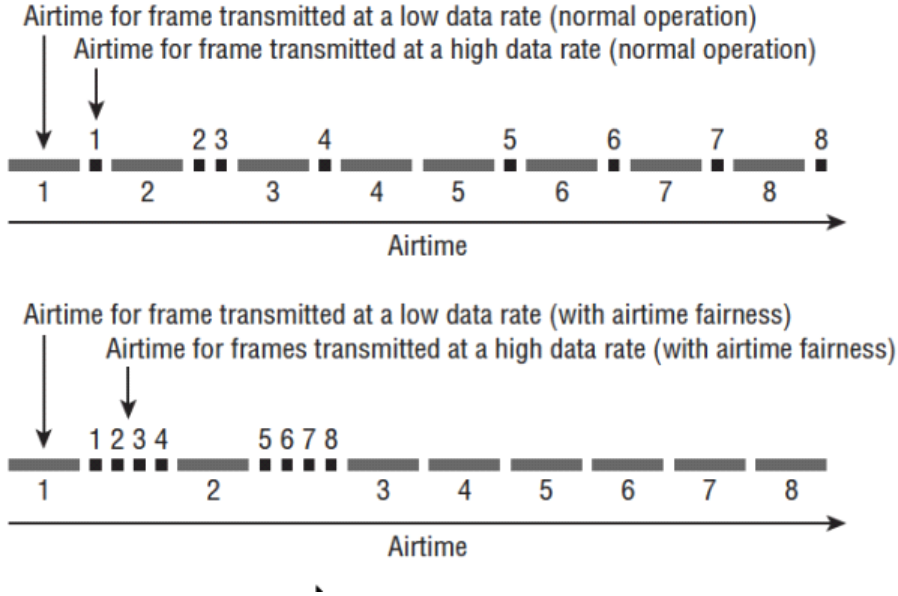
- Defined in the 802.11-2012 standard
- Improves channel efficiency by aggregating several acknowledgments into one single acknowledgment frame
- 2 Types:
    - The immediate Block ACK is designed for use with low-latency traffic
    - The delayed Block ACK is more suitable for latency-tolerant traffic



Wi-Fi Multimedia (WMM)

- Prior to 802.11e amendment, no adequate QoS procedures had been defined for the use of time-sensitive applications
- The Wi-Fi Alliance introduced the Wi-Fi Multimedia (WMM) certification as a partial mirror of 802.11e amendment

Airtime Fairness



802.11 MAC architecture

Monday, April 27, 2020 01:40 PM

Packets, frames, and bits

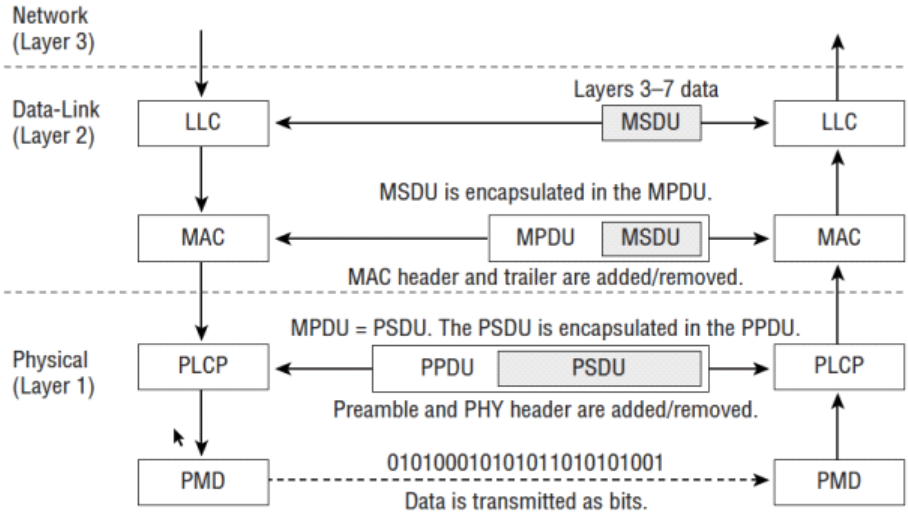
- Same as OSI Model data traverses through each layer to be transmitted to the receiver and then back up the layers

Data-Link layer

- Layer 2 of the OSI Model
- 2 sublayers:
    - MAC Service Data Unit (MSDU)
        - When the Network layer (layer 3) sends data to the Data-Link layer, that data is handed off to the LLC and becomes known as the MAC Service Data Unit (MSDU).
            - MSDU is that it is the data payload that contains the IP packet plus some LLC data.
        - maximum size of the MSDU according to 802.11-2012 standard : 2,304 bytes
        - 802.11n-2009 amendment, aggregate MSDU (A-MSDU) was introduced.
            - A-MSDU, the maximum frame body size is determined by the maximum A-MSDU size of 3,839 or 7,935 octets, depending upon the STA's capability, plus any overhead from encryption
- MAC Protocol Data Unit (MPDU)
- When the LLC sublayer sends the MSDU to the MAC sublayer, the MAC header information is added to the MSDU to identify it
- Is an 802.11 frame
- 3 basic components:
    - MAC Header
        - Consist of
            - Frame control information
            - duration information
            - MAC addressing
            - sequence control information
        - QoS data frames contain specific QoS control information
    - Frame Body
        - Variable in size
        - Contains information that is different depending on the frame type and frame subtype
        - MSDU upper layer payload is encapsulated in the frame body
        - MSDU layer 3–7 payload is protected when using encryption
    - Frame Check Sequence (FCS)
        - Comprises a 32-bit cyclic-redundancy check (CRC) that is used to validate the integrity of received frames.

Physical layer

- Layer 1 of the OSI Model
- 2 sublayers:
- PLCP Service Data Unit (PSDU)
    - Is a view of the MPDU from the Physical layer
- PLCP Protocol Data Unit (PPDU)
    - When the PLCP receives the PSDU, it then prepares the PSDU to be transmitted and creates the PLCP Protocol Data Unit (PPDU)
    - PLCP adds a preamble and PHY header to the PSDU
    - The preamble is used for synchronization between transmitting and receiving 802.11 radios



802.11 and 802.3 interoperability

- The portal is usually either an access point or a WLAN controller
- Because the wired infrastructure is a different physical medium, an 802.11 data frame payload (MSDU) must be effectively transferred into an 802.3 Ethernet frame
- All of the IEEE 802 frame formats share similar characteristics, including the 802.11 frame format
- differences between 802.3 Ethernet and 802.11 wireless frames
    - Frame size
        - 802.3 frames have a maximum size of 1,518 bytes with a maximum payload of 1,500 bytes
        - If the 802.3 frames are 802.1Q tagged for VLANs and user priority, the maximum size of the 802.3 frame is 1,522 bytes with a data payload of 1,504 bytes
        - 802.11 frames are capable of transporting frames with an MSDU payload of 2,304 bytes of upper layer data.
    - MAC addressing used by 802.11 frames is much more complex than Ethernet frames.
    - 802.3 frames have only a source address (SA) and destination address (DA) in the layer 2 header.
    - 802.11 frames have up to four address fields in the MAC header
    - 802.11 frames typically use only three of the MAC address fields (4 in WDS environment).
- TCP/IP, the most common communications protocol used on networks, typically has an IP maximum transmission unit (MTU) size of 1,500 bytes frame size
- Header of an 802.11 frame contains MAC addresses
- A MAC address is one of the following two types:
    - Individual Address
        - also known as a unicast address
    - Group Address
        - multiple destination address
        - 2 kinds of group addresses
            - Multicast-Group Address
                - An address used by an upper-layer entity to define a logical group of stations is known as a multicast-group address
            - Broadcast Address
                - A group address that indicates all stations that belong to the network is known as a broadcast address

3 802.11 frame types

- Management frames
    - Make up a majority of the frame types in a WLAN
    - Another name for an 802.11 management frame is Management MAC Protocol Data Unit (MMPDU).

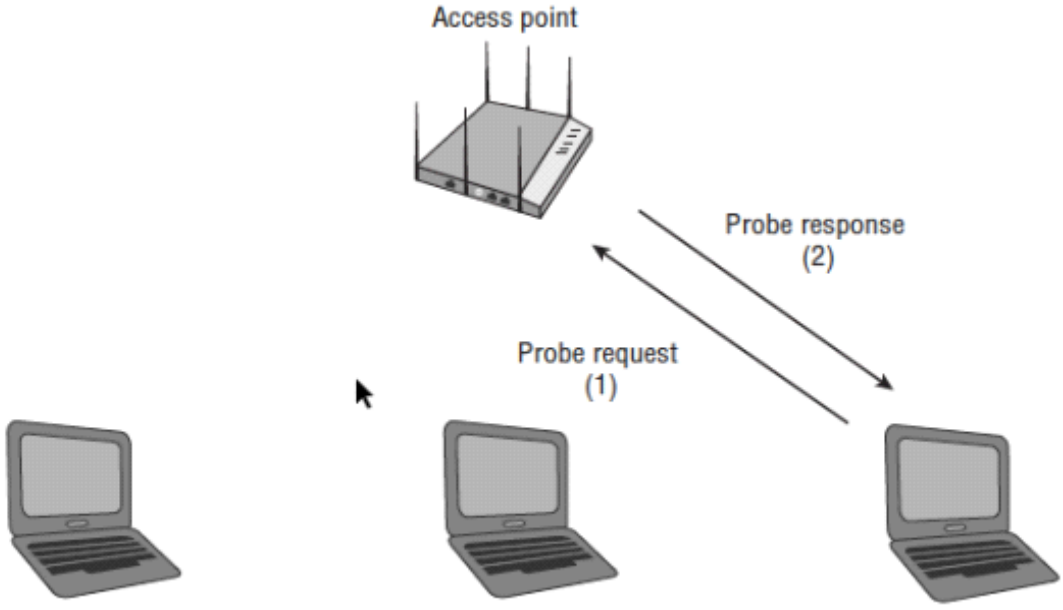
    - Do not carry any upper-layer information
    - 14 of the management frame subtypes as defined by the 802.11 standard and ratified amendments:
        - Association request
        - Association response
        - Reassociation request
        - Reassociation response
        - Probe request
        - Probe response
        - Beacon
        - Announcement traffic indication message (ATIM)
        - Disassociation
        - Authentication
        - Deauthentication
        - Action
        - Action No ACK
        - Timing advertisement
- Control frames
    - Assist with the delivery of the data frames and are transmitted at one of the basic rates
    - 9 of the control frame subtypes as defined by the 802.11 standard:
    - Power Save Poll (PS-Poll)
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgment (ACK)
    - Contention Free-End (CF-End) [PCF Only]
    - CF-End + CF-ACK [PCF Only]
    - Block ACK Request (BlockAckReq) [HCF Only]
    - Block ACK (BlockAck) [HCF Only]
    - Control wrapper
- Data frames
    - Carry the actual data that is passed down from the higher-layer protocols
    - Some 802.11 data frames carry no MSDU payload at all but do have a specific MAC control purpose within a BSS.
    - 15 data frame subtypes
        - Data (simple data frame)
        - Null function (no data)
        - Data + CF-ACK [PCF only]
        - Data + CF-Poll [PCF only]
        - Data + CF-ACK + CF-Poll [PCF only]
        - CF-ACK (no data) [PCF only]
        - CF-Poll (no data) [PCF only]
        - CF-ACK + CF-Poll (no data) [PCF only]
        - QoS Data [HCF]
        - QoS Null (no data) [HCF]
        - QoS Data + CF-ACK [HCF]
        - QoS Data + CF-Poll [HCF]
        - QoS Data + CF-ACK + CF-Poll [HCF]
        - QoS CF-Poll (no data) [HCF]
        - QoS CF-ACK + CF-Poll (no data) [HCF]

Beacon management frame (beacon)

- One of the most important frame types
- Essentially the heartbeat of the wireless network
- AP of a basic service set sends the beacons while the clients listen for the beacon frames
- Client stations only transmit beacons when participating in an independent basic service set (IBSS)
- Beacon contains a time stamp, which client stations use to keep their clocks synchronized with the AP

Passive scanning

- In order for a station to be able to connect to an AP, it must first discover an AP.
- A station discovers an AP by either listening for an AP (passive scanning) or searching for an AP (active scanning)
- Passive scanning, the client station listens for the beacon frames that are continuously being sent by the APs
- client station will listen for the beacons that contain the same SSID that has been preconfigured in the client station's software utility
- When the station hears one, it can then connect to that WLAN



Authentication

- The first of two steps required to connect to the 802.11 basic service set
- When an 802.11 device needs to communicate, it must first authenticate with the AP or with the other stations if it is configured for Ad Hoc mode
- Open System authentication
    - Provides authentication without performing any type of client verification.
    - essentially an exchange of hellos between the client and the AP
    - no exchange or verification of identity takes place between the devices
- Shared Key authentication
- Not used anymore
- Uses WEP when authenticating client stations and requires that a static WEP key be configured on both the station and the AP
- Shared Key authentication is a four-way authentication frame exchange:
    - The client station sends an authentication request to the AP.
    - The AP sends a cleartext challenge to the client station in an authentication response.
    - The client station then encrypts the cleartext challenge and sends it back to the AP in the body of another authentication request frame.
    - The AP then decrypts the station's response and compares it to the challenge text
        - If they match, the AP will respond by sending a fourth and final authentication frame the station, confirming the success
        - If they do not match, the AP will respond negatively
            - If the AP cannot decrypt the challenge, it will also respond negatively.
- Successful, the same static WEP key that was used during the Shared Key authentication process will also be used to encrypt the 802.11 data frames.

Association

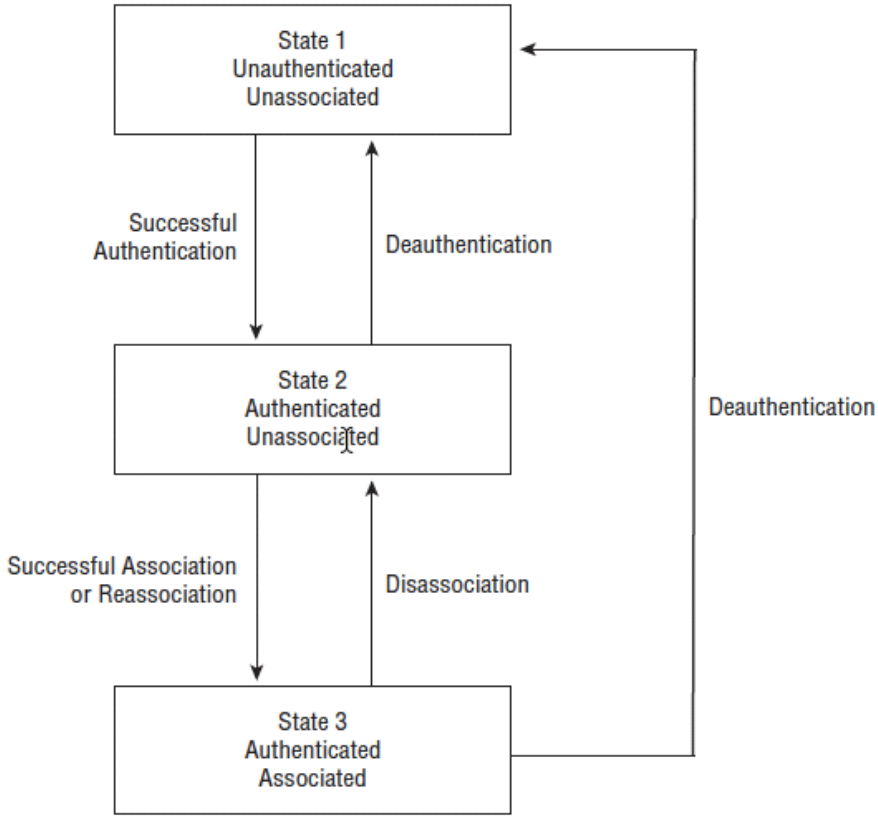
- After authenticated with the AP, the next step is for it to associate with the AP
- When associated it becomes a member of a basic service set (BSS).
- Association means that the client station can send data through the AP and on to the

distribution system medium.

- A client station sends an association request to the AP, seeking permission to join the BSS
- AP sends an association response to the client, either granting or denying permission to join the BSS.
- Occurs after Shared Key or Open System authentication

Authentication and association states

- Authentication state
  - Unauthenticated
  - Authenticated
- Association state
  - Unassociated
  - Associated



Basic and supported rates

- Specific data rates can be configured for any AP as required rates.
- The 802.11-2012 standard defines required rates as basic rates
- In order for a client station to successfully associate with an AP, the station must be capable of communicating by using the configured basic rates that the AP requires
- In addition to the basic rates, the AP defines a set of supported rates
- The supported rates are data rates that the AP offers to a client station, but the client station does not have to support all of them.

Roaming

- The 802.11 standard provided the ability for the client stations to transition from one AP to another while maintaining network connectivity for the upper-layer applications
- The 802.11 standard does not specifically define what roaming is
- The decision to roam is currently made by the client station
- A station can be authenticated to multiple APs but associated to only one AP
- Some WLAN vendors attempt to encourage or discourage roaming by manipulating the client station with the use of management frames
- As the client station roams, the original AP and the new AP should communicate with each other across the distribution system medium and help provide a clean transition between the two.

Reassociation

- When a client station decides to roam to a new AP, it will send a Reassociation request frame

to the new AP you are re-associating to the SSID of the wireless network

Disassociation

- is a notification, not a request
- If a station wants to disassociate from an AP, or an AP wants to disassociate from stations, either device can send a disassociation frame.
- Polite way of terminating the association
- Disassociation cannot be refused by either party, except when management frame protection (defined in 802.11w) is negotiated and the message integrity check (MIC) fails.

Deauthentication

- is a notification and not a request
- If a station wants to deauthenticate from an AP, or an AP wants to deauthenticate from stations, either device can send a Deauthentication frame
- Deauthentication frame will automatically cause a disassociation to occur.
- Cannot be refused by either party, except when management frame protection (defined in 802.11w) is negotiated and the message integrity check (MIC) fails.

ACK Frame

- One of the nine control frames and one of the key components of the 802.11 CSMA/CA medium access control method
- simple frame consisting of 14 octets of information
- When a station receives data, it waits for a short period of time known as a short Interframe space (SIFS)
    - receiving station copies the MAC address of the transmitting station from the data frame and places it in the Receiver Address (RA) field of the ACK frame
- Every unicast frame must be followed by an ACK frame
- If a unicast frame is not followed by an ACK, it is retransmitted.
- With a few rare exceptions, broadcast and multicast frames do not require acknowledgment.

Fragmentation

- The 802.11-2012 standard allows for fragmentation of frames
- Fragmentation breaks an 802.11 frame into smaller pieces known as fragments
    - $\Rightarrow$ adds header information to each fragment
    - $\Rightarrow$ transmits each fragment individually
- In a properly functioning 802.11 network, smaller fragments will actually decrease data throughput because of the MAC sublayer overhead of the additional header, SIFS, and ACK of each fragment

Protection Mechanism

- In order for 802.11g, 802.11b, and legacy 802.11 stations to coexist within the same BSS, the 802.11g devices enable what is referred to as the protection mechanism
- Vendors often offer three configuration modes for 802.11g Aps:
- 802.11b-Only Mode
    - Aggregate throughput will be the same as achieved in an 802.11b network
- 802.11g-Only Mode
    - APs configured as g-only will communicate with only 802.11g client stations using ERP-OFDM technology
- 802.11b/g Mode
    - The default operational mode of most 802.11g APs
    - Support for DSSS, HR-DSSS, and OFDM is enabled
- Vendor configurations are not part of the 802.11-2012 standard
- The Standard mandates support for 802.11 Clause 16 devices, 802.11b Clause 17 devices, and 802.11g Clause 19 devices within the ERP basic service set
- If an 802.11g device were to transmit a data frame, 802.11b devices would not be able to interpret the data frame or the Duration/ID value
- The 802.11b devices would not set their NAV timers and could incorrectly believe that the medium is available.
- To prevent this from happening, the 802.11g ERP stations switch into what is known as Protected mode.
- In a mixed-mode environment, when an 802.11g device wants to transmit data, it will first perform a NAV distribution by transmitting a request to send/clear to send (RTS/CTS)

exchange with the AP or by transmitting a CTS-to-Self using a data rate and modulation method that the 802.11b HR-DSSS stations can understand
    - The RTS/ CTS or CTS-to-Self will hopefully be heard and understood by all of the 802.11b and 802.11g stations
    - The RTS/CTS or CTS-to-Self will contain a Duration/ID value that will be used by all of the listening stations to set their NAV timers
- After the RTS/CTS or CTS-to-Self has been used to reserve the medium, the 802.11g station can transmit a data frame by using OFDM modulation without worrying about collisions with 802.11b HR-DSSS or legacy 802.11 DSSS stations
- The following are three scenarios that can trigger protection in an ERP basic service set:
    - An HR-DSSS (802.11b) client association will trigger protection.
    - An 802.11g AP hears a beacon frame from an 802.11 or 802.11b AP or ad hoc client
    - An ERP AP hears a management frame (other than a probe request) where the supported rate includes only 802.11 or 802.11b rates, the Non ERP Present bit may be set to 1

Request to send/clear to send (RTS/CTS)

- If a station cannot hear the other stations, or cannot be heard by the other stations, there is a greater likelihood that a collision can occur
- RTS/CTS is a mechanism that performs a NAV distribution and helps prevent collisions from occurring
- This NAV distribution reserves the medium prior to the transmission of the data frame

CTS-to-Self

- Used strictly as a protection mechanism for mixed-mode environments
- CTS notifies all other stations that they must wait until the DATA and ACK have been transmitted

Data Frames

- 15 subtypes of data frames
- most common data frame is the simple data frame
    - has MSDU upper-layer information encapsulated in the frame body
- null function frame is used by client stations to inform the AP of changes in Power Save status by changing the Power Management bit

Power Management

- Active Mode
- A legacy power-management mode used by very old 802.11 stations
- When a station is set for Active mode, the wireless station is always ready to transmit or receive data.
- Provides no battery conservation
- MAC header of an 802.11 frame, the Power Management field is 1 bit in length and is used to indicate the power-management mode of the station
    - 0 : station is in Active mode
- Power Save Mode
    - Optional mode for 802.11 stations
    - Client station is set for Power Save mode, it will shut down some of the transceiver components for a period of time to conserve power
    - Changing Power Management bit to 1
        - station is using Power Save mode
    - AP is informed that the client station is using power management, and the AP buffers all of that client's 802.11 frames.
- Traffic Indication Map (TIM)
    - If a station is part of a basic service set, it will notify the AP that it is enabling Power Save mode by changing the Power Management field to 1
    - If the AP then receives any data that is destined for the station in Power Save mode, the AP will store the information in a buffer
    - Any time a station associates to an AP, the station receives an association identifier (AID)
    - If the AP is buffering data for a station in Power Save mode, when the AP transmits its next beacon, the AID of the station will be seen in a field of the beacon frame known as the traffic indication map (TIM).

        - TIM field is a list of all stations that have undelivered data buffered on the AP
    - Every beacon will include the AID of the station until the data is delivered
    - After the station notifies the AP that it is in Power Save mode, the station shuts down part of its transceiver to conserve energy. A station can be in one of two states, either awake or doze:
        - During the awake state, the client station can receive frames and transmit frames
        - During the doze state, the client station cannot receive or transmit any frames and operates in a very low power state to conserve power.
    - When the station receives the beacon, it checks to see whether its AID is set in the TIM, indicating that a buffered unicast frame waits
        - If so, the station will remain awake and will send a PS-Poll frame to the AP
            - When the AP receives the PS-Poll frame, it will send the buffered unicast frame to the station
    - Each unicast frame contains a 1-bit field called the More Data field.
    - When the station receives a buffered unicast frame with the More Data field set to 1
        - station cannot go back to sleep yet because there is some more buffered data that it has not yet received
    - When the More Data field is set to 1, the station knows that it needs to send another PS-Poll frame and wait to receive the next buffered unicast frame.
    - After all of the buffered unicast frames have been sent, the More Data field in the last buffered frame will be set to 0, indicating that there is currently no more buffered data, and the station will go back to sleep
- Delivery Traffic Indication Message (DTIM)
    - A delivery traffic indication map (DTIM) is used to ensure that all stations using power management are awake when multicast or broadcast traffic is sent
    - DTIM is a special type of TIM
    - TIM or DTIM is transmitted as part of every beacon
    - All stations will wake up in time to receive the beacon with the DTIM
    - If the AP has multicast or broadcast traffic to be sent, it will transmit the beacon with the DTIM and then immediately send the multicast or broadcast data.
    - A misconfigured DTIM interval would cause performance issues during a push-to-talk multicast
- Announcement Traffic Indication Message (ATIM)
    - If a station is part of an IBSS, there is no central AP to buffer data while the stations are in Power Save mode
    - A station will notify the other stations that it is enabling Power Save mode by changing the Power Management field to 1.
    - When the station transmits a frame with this field set to 1, the other stations know to buffer any data that they may have for this station because this station is now in Power Save mode.
    - During the ATIM window, if a station has buffered data for another station, it will send a unicast frame known as an ATIM frame to the other station.
    - Do not confuse the ATIM frame with the TIM field
        - ATIM is a frame used for power management by ad hoc clients not communicating through an AP
- WMM Power Save and U-APSD
    - IEEE 802.11e amendment also introduced an enhanced power-management method called automatic power save delivery (APSD)
    - 2 APSD methods that are defined are:
        - Scheduled automatic power save delivery (S-APSD)
        - Unscheduled automatic power save delivery (U-APSD)
    - The Wi-Fi Alliance's WMM Power Save (WMM-PS) certification is based on U-APSD
    - Goal of WMM-PS : to have client devices spend more time in a doze state & consume less power
    - WMM-PS uses a trigger mechanism to receive buffered unicast traffic based on WMM access categories.
- 802.11n Power Management

- 802.11n-2009 amendment also defines two new power-management methods
- Spatial multiplexing power save (SM power save)
  - Purpose of SM power save : enable a MIMO 802.11n device to power down all but one of its radio chains
- Power save multi-poll (PSMP)
  - Extension of automatic power save delivery (APSD), which was defined by the 802.11e amendment

WLAN Architecture

Tuesday, April 28, 2020 09:06 PM

Wireless LAN client devices

- 802.11 Radio form factors
  - 802.11 radios are used in both client NICs and access points.
  - External Radios
    - Many form factors --> NIC comes in different shapes and sizes
      - PCMCIA adapter/PC card
      - Express Card
      - USB
  - Internal Radios
    - Installed inside the device
    - Mini PCI
    - Mini PCI Express
  - Mobile Devices
    - Smartphones
    - Tablets
    - Bar code scanners
    - VoWiFi phones
  - Wearables
    - Google Glass
    - Fitbit
  - Internet of Things (IoT)
- 802.11 Radio chipsets
  - A group of integrated circuits designed to work together is often marketed as a chipset
  - Can transmit on either the 2.4 GHz or 5 GHz unlicensed frequencies
    - Some chipsets may only support the ability to transmit on the 2.4 GHz ISM band
  - Many proprietary technologies turn up in the individual chipsets, and some of these technologies will become part of the standard in future 802.11 amendments
- Client utilities
  - End user must have the ability to configure a wireless client NIC
  - Software interface is needed in the form of client utilities
  - 3 major types, or categories, of client utilities exist:
    - Integrated operating system client utilities
    - Vendor-specific client utilities
    - Third-party client utilities
- Management, control and data planes
  - Telecommunication networks are often defined as 3 logical planes of operation:
    - Management Plane
      - WLAN Configuration
        - configurations of SSIDS, security, WMM, channel, and power settings.
      - WLAN Monitoring and Reporting
        - Monitoring of layer 2 statistics like ACKs, client associations, reassociations, and data rates occurs in the management plane
      - WLAN Firmware Management
        - Ability to upgrade access points and other WLAN devices with the latest vendor operational code is included here
    - Control Plane
      - Dynamic RF
        - Coordinated channel and power settings for multiple access points
        - Dynamic RF is also referred to by the more technical term radio resource management (RRM).
      - Roaming Mechanisms

        - Support for roaming handoffs between access points
        - L3 roaming, maintaining stateful firewall sessions of clients, and forwarding of buffered packets
    - Client Load Balancing
        - Collecting and sharing client load and performance metrics between access points to improve overall WLAN operations
    - Mesh Protocols
        - Routing user data between multiple access points requires some sort of mesh routing protocol
- Data Plane
    - Where user data is forwarded
    - A standalone AP handles all data forwarding operations locally
    - In a WLAN controller solution, data is normally forwarded from the centralized controller, but data can also be forwarded at the edge of the network by an AP

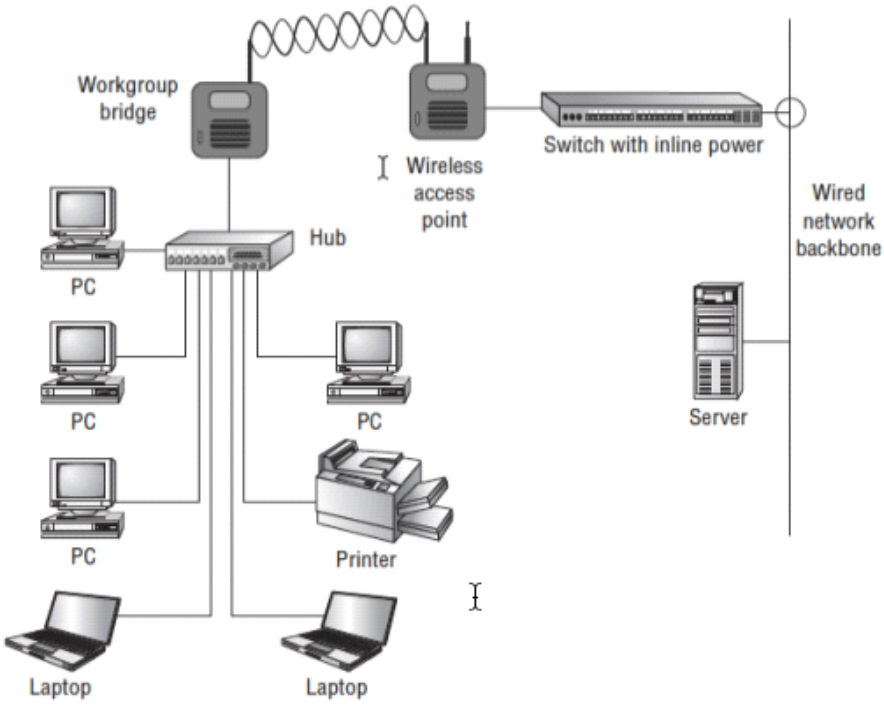
WLAN architecture

- Autonomous WLAN architecture
    - The conventional access point was a standalone WLAN portal device where all three planes of operation existed and operated on the edge of the network architecture
    - All configuration settings exist in the autonomous access point itself
    - All encryption and decryption mechanisms and MAC layer mechanisms also operate within the autonomous AP.
    - An autonomous access point contains at least 2 physical interfaces
        - usually a radio frequency (RF) radio card
        - a 10/100/1000 Ethernet port
    - Autonomous APs are deployed at the access layer and typically are powered by a PoE capable access layer switch.
- Centralized network management systems
    - A WNMS moves the management plane out of the autonomous access points.
    - Provides a central point of management to configure and maintain thousands of autonomous access points.
    - Network management server (NMS) is now used more often
- Cloud networking
    - Applications and network management, monitoring, functionality, and control are provided as a software service
    - 2 most common cloud networking models are as follows:
    - Cloud-Enabled Networking (CEN)
        - The management plane resides in the cloud, but data plane mechanisms such as switching and routing remain on the local network
    - Cloud-Based Networking (CBN)
        - The data plane is also moved to the cloud with the intent of eliminating hardware other than that used to access the Internet at the local network
- Centralized WLAN architecture
- Central WLAN controller that resides in the core of the network.
- Autonomous APs have been replaced with controller-based access points, also known as lightweight APs or thin APs
- All planes were moved out of access points and into a WLAN controller
- Encryption & decryption capabilities might reside in the centralized WLAN controller or may still be handled by the controller-based APs, depending on the vendor
- Some time-sensitive operations are still handled by the AP
- WLAN Controller:
    - Often referred to as wireless switches
    - Some vendors use proprietary protocols for communications between the WLAN controller and their controller-based
    - APs
    - Many WLAN vendors use the Control and Provisioning of Wireless Access Points (CAPWAP) protocol for managing and monitoring access points

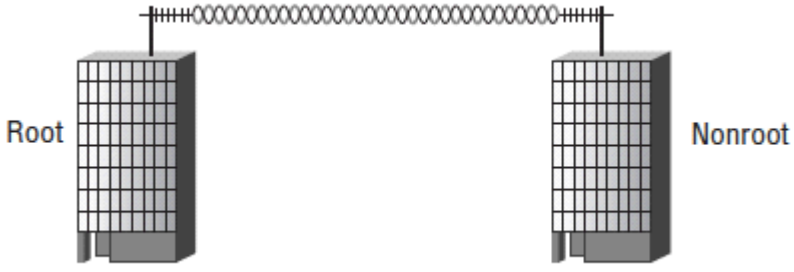
    - Can support multiple BSSIDs and VLANs
- Distributed WLAN architecture
    - Cooperative access points are used, and control plane mechanisms are enabled in the system with inter-AP communication via cooperative protocols.
    - A distributed WLAN architecture combines multiple access points with a suite of cooperative protocols, without requiring a WLAN controller
    - The control plane information is shared between the APs using proprietary protocols
- Unified WLAN architecture
    - Fully integrating WLAN controller capabilities into wired network infrastructure devices
- Hybrid architecture
    - Hybrid of any of the above

Specialty WLAN infrastructure

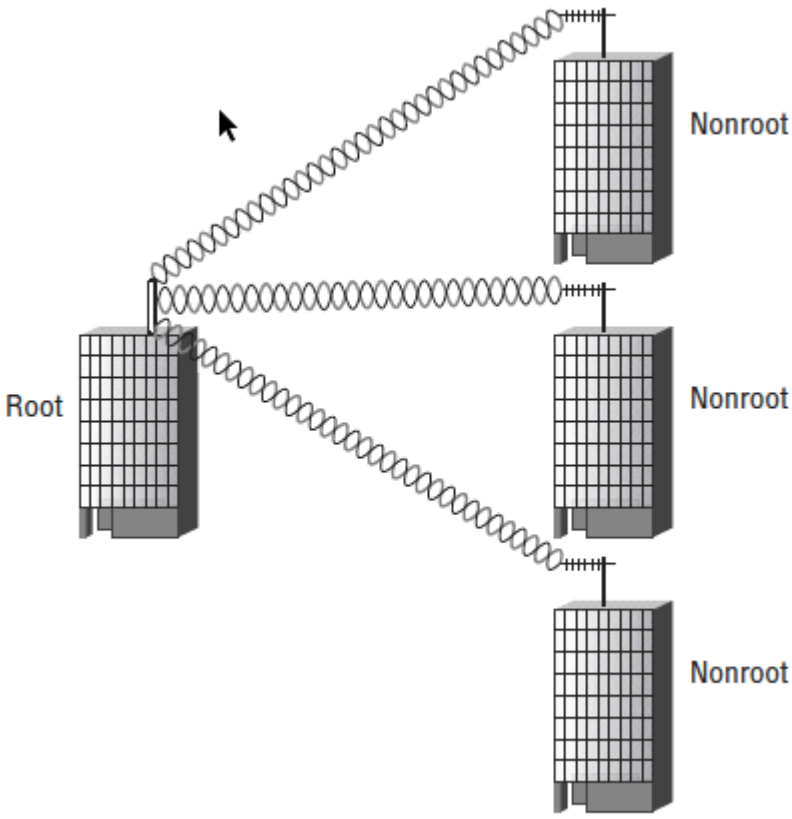
- Wireless workgroup bridge (WGB)
    - Is a wireless device that provides wireless connectivity for wired infrastructure devices that do not have radio cards.
    - Is an associated client of the access point
    - Does not provide connectivity for other wireless clients



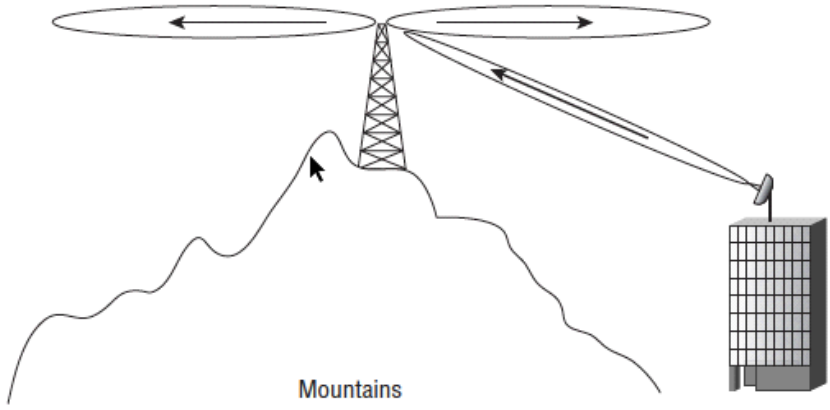
- Wireless LAN bridges
    - Purpose of bridging is to provide wireless connectivity between two or more wired networks.
    - Wireless bridges support two major configuration settings
        - root
        - Non-root
    - A bridge link that connects only two wired networks is known as a point-to-point (PtP) bridge



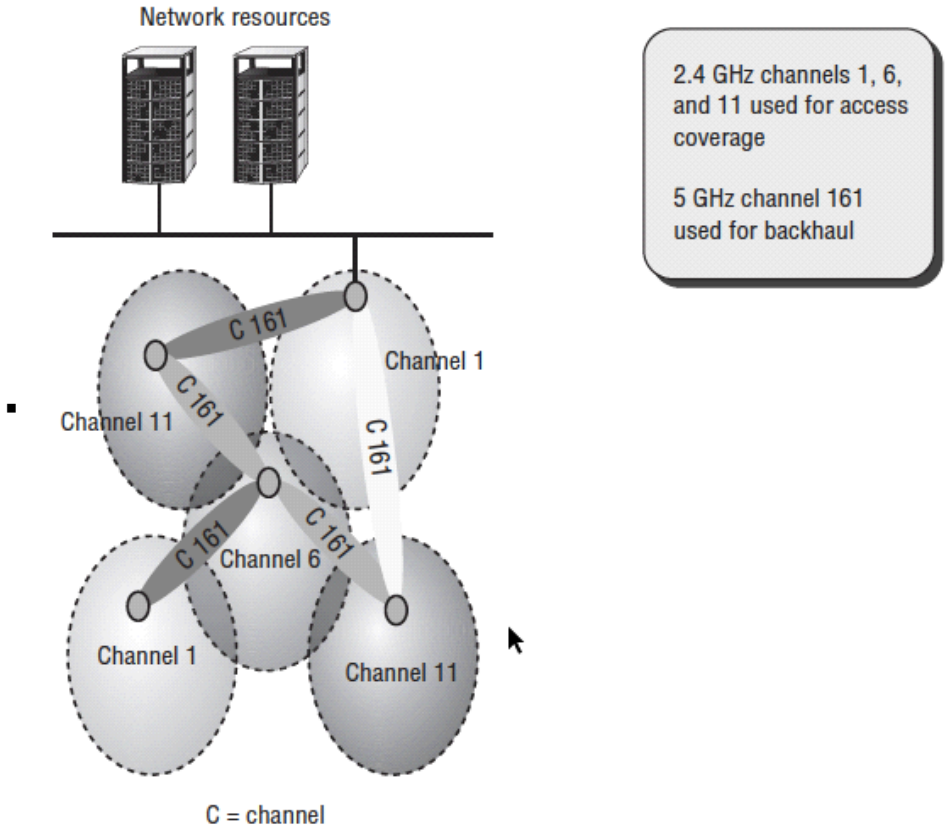
- A point-to-multipoint (PtMP) bridge link connects multiple wired networks



- Common problem with point-to-multipoint bridging
  - Mounting the high-gain omnidirectional antenna of the root bridge too high
  - Causes the vertical line of sight with the directional antennas of the nonroot bridges is not adequate.



- Enterprise WLAN router
  - A distributed solution using enterprise-grade WLAN routers at each branch office is a common choice.
  - WLAN routers are very different from access points. Unlike access points, which use a bridged virtual interface, wireless routers have separate routed interfaces
- Wireless LAN mesh access points
  - Wireless mesh APs communicate with each other by using proprietary layer 2 routing protocols and create a self-forming and self-healing wireless infrastructure (a mesh) over which edge devices can communicate



- WLAN array
  - Xirrus offers a proprietary solution that combines a WLAN controller and multiple access points in a single hardware device known as a Wi-Fi array
  - Access-point radios using sector antennas and an embedded WLAN controller all reside in one device
  - WLAN arrays are also useful in high user density environments and can also be used to reduce cable runs
- Virtual AP system
  - A virtual access point solution uses multiple access points that all share a single basic service set identifier (BSSID).
  - Clients stations believe they are connected to only a single access point, although they may be roaming across multiple physical APs
- Real-time location systems
  - Network management servers (NMSs), WLAN controllers and WIDS solutions have some integrated capabilities to track 802.11 clients by using the access points as sensors
- VoWiFi
  - VoIP over WiFi

WLAN Deployment & Vertical Markets

Thursday, April 30, 2020 04:59 PM

Deployment considerations for commonly supported WLAN applications and devices Data

- Data
  - One of the most important aspects of designing a network to handle data-oriented applications is to ensure that the network design is capable of handling the amount of data that will be transferred
  - Most data applications are forgiving of slight network delays, but problems can arise if there is not enough available data bandwidth
  - Analyze the data requirements of your users
  - Ensure that the data rates at which the users will connect are capable of handling the amount of data that they will be transmitting
- Voice
  - Not tolerant of network delays, dropped packets, or sporadic connections
  - Implementation of voice products varies between vendors
    - Each vendor has unique guidelines for designing voice applications
  - It is important to understand the best practice methods for installing your voice system
  - Voice devices are typically handheld devices that do not transmit with as much power as laptops
  - More APs will be necessary to ensure adequate coverage
- Video
  - Typically more complex than voice
  - In addition to multiple streams of data for video and voice, video often includes streams for setting up and tearing down the connection
  - In most cases, video has a higher loss tolerance than voice
  - Choppy audio during a videoconference would likely be highly disruptive, causing participants to ask the speaker to repeat what was said, whereas if the audio is clear and the video choppy, the speaker would likely be understood the first time.
  - Important to identify the type of video that is being transmitted and the function or purpose of that transmission
  - Need to evaluate the system or software that is transmitting the wireless video traffic to determine the type of traffic and protocols along with the network load
- Real-Time Location Services (RTLS)
  - Some have features that are built in, whereas others offer integration hooks to third-party vendors who specialize in location technology and have sophisticated software applications related to specific industry vertical markets
  - Location tracking is expanding incredibly quickly as more and more uses are identified
  - Can be used to locate or track people or devices on a WLAN
  - Healthcare is one of the biggest users of location-based technology
  - Each RTLS vendor is unique and will be able to provide you with recommendations and best practice documents for deploying your RTLS equipment
- Mobile devices (tablets and smartphones)
  - BYOD
  - Unlike changes in enterprise technology, which is planned and controlled by the IT department, the push for support of mobile devices is being made by the end user
  - Multiple concerns arise with integrating these devices into the network
    - Making sure that the devices are capable of connecting to the network using the proper authentication
    - Ensuring the use of encryption protocols along with the ability for these devices to be able to smoothly roam throughout the network without losing connectivity
  - Providing network access, not only based upon the identity of the user of the device but also based upon the type of device or other device or connection characteristics

    - The coverage area of any 802.11 network needs to be designed small enough so that any device can respond back to the access point with a strong enough signal

Corporate data access and end-user mobility

- With 802.11n and 802.11ac technologies, some companies are transitioning to these whilst reducing their Wired connections
- Wall outlets are expensive
    - Sometimes costing up to $200 per outlet
- Some places in company are difficult to cable to
    - e.g.
        - Warehouses
        - Conference rooms
        - Labs
- Providing continuous access and availability throughout the facility has become paramount in the past few years
- With this push toward leaner devices, Ethernet adapters have either given way to wireless radios or been bypassed all together in favor of wireless
- Wireless provides mobility, accessibility, and convenience, but if not designed and implemented properly, it can lack in performance, availability, and throughput
- Wireless should rarely be considered for distribution or core roles, except for building-to-building bridging or mesh backhaul

Network extension to remote areas

- Was one of the driving forces of home wireless networking, which also helped drive the demand for wireless in the corporate environment
- The same reasons for installing wireless networking in a home are also valid for installing wireless
    - Fewer cables are required
    - Equipment placement can often be performed without affecting the aesthetics of a building offices, warehouses, and just about any other environment

Bridging—building-to-building connectivity

- To provide network connectivity between two buildings, you can install an underground cable or fiber between the two buildings, pay for a high-speed leased data circuit, or use a building-to-building wireless bridge
- requires that the two buildings have a clear RF line of sight between them
    - Typically easy for trained professionals to perform, and there are no monthly service fees after installation, because you own the equipment.
- In addition to connecting two buildings via a PTP bridge, three or more buildings can be networked together by using a PTMP solution --> known as a hub and spoke or star

Wireless ISP (WISP)—last-mile data delivery

- Wireless Internet service providers (WISPs) deliver Internet services via wireless networking
- Instead of directly cabling each subscriber, a WISP can provide services via RF communications from central transmitters.
- WISP often use wireless technologies other than 802.11

Small office/home office (SOHO)

- Wireless networking has helped to make it easy for a SOHO employee to connect the office computers and peripheral devices together, as well as to the Internet
- Main purpose of a SOHO 802.11 network is typically to provide wireless access to an Internet gateway
- Most SOHO wireless routers provide fairly easy-to-follow installation instructions and offer reasonable performance and security, though less than what their corporate counterparts provide.

Mobile office networking

- Mobile homes or trailer offices are used for many purposes
    - As temporary offices during construction
    - After a disaster or as temporary classrooms to accommodate unplanned changes in student population
- Mobile offices are simply an extension of the office environment
- Not permanent

    - Usually easy to extend the corporate or school network to these offices
- A wireless bridge can be used to distribute wireless networking to the mobile office
    - If needed, an AP can then be used to provide wireless network access to multiple occupants of the office
- When the mobile office is no longer needed, the wireless equipment can simply be unplugged and removed

Branch offices

- A distributed solution using enterprise-grade WLAN routers at each branch office is a common choice
- Branch routers have the ability to connect back to corporate headquarters with VPN tunnels
    - corporate VLANs, SSIDs, and WLAN security can all be extended to the remote branch offices
        - The wired and wireless network access policies are seamless across the entire organization
- Most companies do not have the luxury or need to have an IT employee at each branch office --> network management server (NMS) at a central location is used to manage & monitor the entire enterprise network.

Educational/classroom use

- Wireless networking can be used to provide a safe and easy way of connecting students to a school network.
- Because the layout of most classrooms is flexible (with no permanently installed furniture), installing a wired network jack for each student is not possible.
- Wireless networking enables any classroom seating arrangement to be used, without the safety risk of networking cables being strung across the floor.
- Computer tablets are quickly becoming commonplace devices in all levels of education.
- Schools typically require more access points for coverage because of the wall materials between classrooms.
- Most classroom walls are made of cinderblock to attenuate noise between classrooms.
- Access point is often needed in at least every other classroom
- Network access control (NAC) has become an integral part of many school networks
    - NAC can be used to “fingerprint,” or identify authentication and authorization information about devices connecting to the network

Industrial—warehousing and manufacturing

- Because of the vast space and the mobile nature of the employees in these environments, companies saw the need to provide mobile network access to their employees
- Warehouse and manufacturing environments often deploy wireless handheld devices, such as bar code scanners, which are used for inventory control
- Most 802.11 networks deployed in either a warehouse or manufacturing environment are designed for coverage rather than capacity
- Wireless networks are able to provide the coverage and mobility required in a warehouse environment—and provide it cost-effectively.

Retail

- 4 key uses of wireless in retail locations
    - Wireless network that provides support relating to the operations of the store and the retail transactions
    - Tracking analytics of the retail customer
    - Location-based mapping and tracking services
    - Supplemental Internet access, often necessitated by poor cellular coverage inside the retail establishment
- Retail centers, hospitals, hotels, subways, and museums (and many other types of organizations) can provide turn-by-turn directions to visitors, along with promotions, and other location-based services.
- Providing wireless access for shoppers may make for a more pleasant and satisfied shopping experience and will likely result in more sales.

Healthcare—hospitals and offices

- Data access and end-user mobility
- Need quick, secure, and accurate access to patient and hospital or clinic data, so they can

react and make decisions
- Medical carts used to enter and monitor patient information often have wireless connections back to the nursing station
- VoWiFi is another common use of 802.11 technology in a medical environment, providing immediate access to personnel no matter where they are in the hospital
- RTLS solutions using 802.11 Wi-Fi tags for inventory control are also commonplace
- Rely on many forms of proprietary and industry-standard wireless communications that may have the potential of causing RF interference with 802.11 wireless networks.
- Many hospitals have designated a person or department to help avoid RF conflicts by keeping track of the frequencies and biomedical equipment used within the hospital

Municipal networks
- Many municipalities viewed this as a way of providing service to some of their residents who could not necessarily afford Internet access

Hotspots—public network access
- Refers to a free or pay-for-use wireless network that is provided as a service by a business
- Free hotspots have drawn much attention to the 802.11 wireless industry, helping to make more people aware of the benefits of the technology.
- Most hotspot providers perform network authentication by using a special type of web page known as a captive portal.

Stadium networks
- Fans expect and demand a complete multimedia experience when attending events, including access to replays and real-time statistics
- A well-designed stadium network can allow the venue to target sections or groups of people with directed advertisements, special offers, or customized services
- A wireless network is needed to provide event operations with services such as reliable high-speed Internet access in the press box, ticketing and point-of-sale transaction processing, and video surveillance.

Transportation networks
- Providing Wi-Fi service to any of the transportation methods is easy. Simply install one or more access points in the vehicle.
- Primary use of these networks is to provide hotspot services for end users so that they can gain access to the Internet
- Difference between a transportation network and a typical hotspot is that the network is continually moving, making it necessary for the transportation network to use some type of mobile uplink services.

Law enforcement networks
- Many law enforcement agencies are using Wi-Fi as a supplement to their public safety wireless networks
- In addition to municipalities incorporating wireless technology into law enforcement, many are adding non-Wi-Fi-based automation to utilities through the use of supervisory control and data acquisition (SCADA) equipment.
- When a police car arrives at one of these municipal Wi-Fi hotspots, the computer in the car automatically uploads the video files from the data storage in the car to the central video library

First-responder networks
- Many rescue vehicles are being equipped with either permanently mounted Wi-Fi access points or easily deployed, self-contained portable access points that can quickly and easily blanket a rescue scene with a Wi-Fi bridge to the emergency personnel's data network.

Fixed mobile convergence (FMC)
- The goal of FMC systems is to provide a single device, with a single phone number that is capable of switching between networks and always using the lowest-cost network
- FMC devices also allow you to roam across networks, so you could initiate a phone call from within your company by using the Wi-Fi network. As you walk outside, the FMC phone would roam from the Wi-Fi network to the cellular network and seamlessly transition between the two networks.

WLAN and health
- The World Health Organization and government agencies set standards that establish

exposure limits to radio waves, to which RF products must comply.

- Tests performed on WLANs have shown that they operate substantially below the required safety limits set by these organizations
- The World Health Organization has also concluded that there is no convincing scientific evidence that weak radio-frequency signals, such as those found in 802.11 communications, cause adverse health effects.

WLAN vendors

- There are many vendors in the 802.11 WLAN marketplace

WLAN Troubleshooting & Design

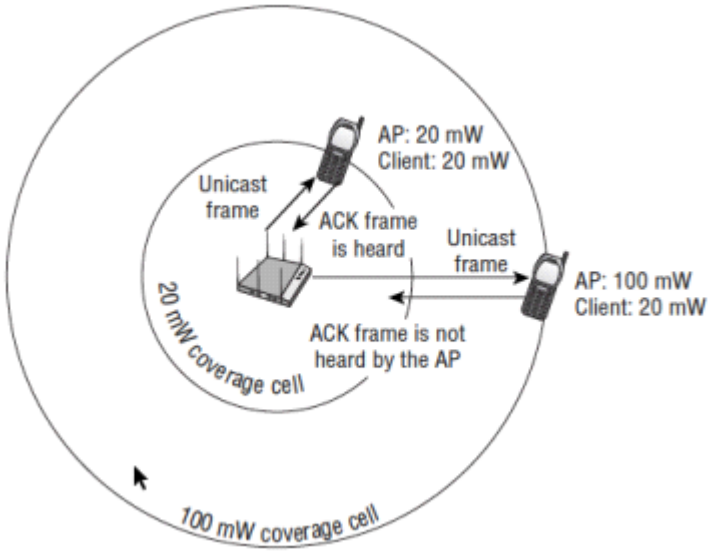
Monday, May 4, 2020 09:13 AM

Layer 2 retransmissions

- The mortal enemy of WLAN performance is layer 2 retransmissions that occur at the MAC sublayer
    - If a collision occurs or any portion of a unicast frame is corrupted, the cyclic redundancy check (CRC) will fail and the receiving 802.11 radio will not return an ACK frame to the transmitting 802.11 radio
- If an ACK frame is not received by the original transmitting radio, the unicast frame is not acknowledged and will have to be retransmitted
- Excessive layer 2 retransmissions adversely affect the WLAN in 2 ways
    - Layer 2 retransmissions increase overhead and therefore decrease throughput
    - If application data has to be retransmitted at layer 2, the delivery of application traffic becomes delayed or inconsistent.
- Excessive layer 2 retransmissions usually result in latency and jitter problems for time-sensitive applications
    - Latency
        - Time it takes to deliver a packet from the source device to the destination device
        - Delay in the delivery (increased latency) of a VoIP packet due to layer 2 retransmissions can result in echo problems.
    - Jitter
        - Variation of latency
        - Measures how much the latency of each packet varies from the average
- Most data applications in a Wi-Fi network can handle a layer 2 retransmission rate of up to 10 percent without any noticeable degradation in performance
- VoIP require that higher-layer IP packet loss be no greater than 2 percent
    - Voice over Wi-Fi (VoWiFi) networks need to limit layer 2 retransmissions to 5 percent or less to ensure the timely and consistent delivery of VoIP packets
- Layer 2 retransmissions are a result of many possible problems
    - Multipath, RF interference, and low signal-to-noise ratio (SNR) are problems that exist at layer 1 yet result in layer 2 retransmissions
    - Other causes of layer 2 retransmissions include hidden nodes, near/far problems, mismatched power settings, and adjacent channel interference, which are all usually a symptom of improper WLAN design
- RF interference
    - Interfering devices may prevent an 802.11 radio from transmitting --> causing a denial of service
    - Several different types of interference
        - Narrowband Interference
            - Will not cause a denial of service (DoS) for an entire band
            - Signal usually have a very high amplitude and will absolutely disrupt communications in the frequency space in which it is being transmitted
            - Can disrupt one or several 802.11 channels
            - Can also result in corrupted frames and layer 2 retransmissions
            - Only way to eliminate narrowband interference is to locate the source of the interfering device with a spectrum analyzer
        - Wideband Interference
            - If the transmitting signal has the capability to disrupt the communications of an entire frequency band --> typically considered wideband
            - Only way to eliminate wideband interference is to locate the source of the interfering device with a spectrum analyzer and remove the

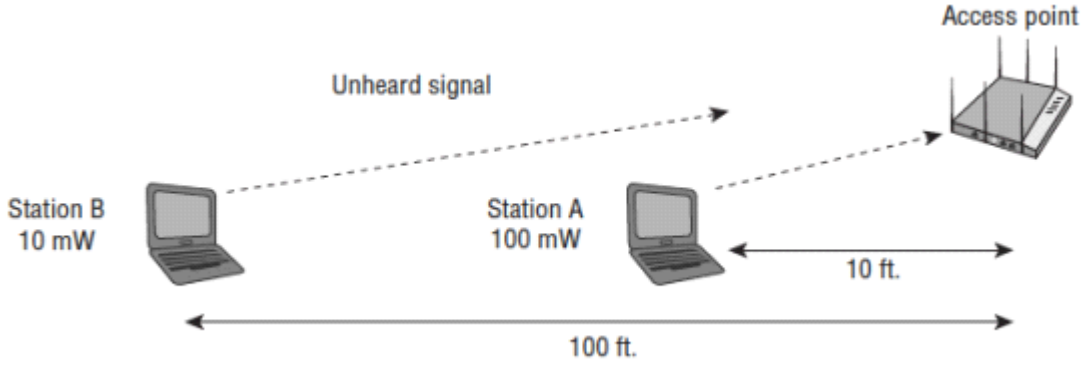
interfering device
        - All-Band Interference
        - Typically associated with frequency hopping spread spectrum (FHSS) communications that usually disrupt the 802.11 communications at 2.4 GHz
        - Although an FHSS device will not typically cause a denial of service, the frame transmissions from the 802.11b/g/n devices can be corrupted from the all-band transmissions of a legacy 802.11 FHSS interfering radio.
        - Bluetooth (BT) is a short-distance RF technology used in WPANs
            - Uses FHSS and hops across the 2.4 GHz ISM band at 1,600 hops per second
        - Digital Enhanced Cordless Telecommunications (DECT) cordless telephones also use frequency hopping transmissions.
        - Frequency hopping transmitters do not usually result in as much data corruption as fixed-channel transmitters
            - However, the existence of a high number of frequency hopping transmitters in a finite space can result in a high amount of 802.11 data corruption and is especially devastating to VoWiFi communications
- Multipath
    - Can cause intersymbol interference (ISI), which causes data corruption
    - If the data is corrupted because of multipath --> layer 2 retransmissions
    - Can be a serious problem when working with legacy 802.11a/b/g equipment
    - Use of directional antennas will often reduce the number of reflections
    - Antenna diversity can also be used to compensate for the negative effects of multipath
    - Does not affect 802.11n or 802.11ac technology
    - Multipath has a constructive effect with 802.11n/ac transmissions that utilize multiple-input, multiple-output (MIMO) antennas and maximum ratio combining (MRC) signal processing techniques.
    - There is no way to fix multipath indoors because some reflection will always occur, and thus there will always be multiple paths of the same signal
    - Using a semi-directional antenna will cut down on reflections and thereby decrease data corruption and layer 2 retransmissions
- Adjacent channel interference
    - Refers to degradation of performance resulting from overlapping frequency space that occurs due to an improper channel reuse design
    - When designing a wireless LAN, you need overlapping coverage cells in order to provide for roaming.
        - Overlapping cells should not have overlapping frequencies
            - Overlapping coverage cells with overlapping frequencies cause what is known as adjacent channel interference
- Low Signal-to-noise ratio (SNR)
    - Important value because if the background noise is too close to the received signal or the received signal level is too low, data can be corrupted and retransmissions will increase
    - Not actually a ratio
        - Is simply the difference in decibels between the received signal and the background noise (noise floor)
    - Data transmissions can become corrupted with a very low SNR
    - SNR of 25 dB or greater is considered good signal quality
    - SNR of 10 dB or lower is considered poor signal quality
    - When designing for coverage during a site survey, the normal recommended best practice is to provide for a –70 dBm or stronger received signal that is well above the noise floor
    - When designing for WLANs with VoWiFi clients, a –67 dBm or stronger signal that is even higher above the noise is recommended
- Mismatched power settings
    - Between an access point and a client radio

- Communications can break down if a client station's transmit power level is less than the transmit power level of the access point
- The ACK frame is not "heard" by the AP, which then must retransmit the unicast frame. All of the client's transmissions are effectively seen as noise by the AP, and layer 2 retransmissions are the result.



- Best solution is to ensure that all of the client transmit power settings match the access point's transmit power
- One way to test whether the mismatched AP/client power problem exists is to listen with a protocol analyzer
  - An AP/client power problem exists if the frame transmissions of the client station are corrupted when you listen near the access point but are not corrupted when you listen near the client station.
- A high-gain antenna on an access point will amplify the AP's transmitted signal and extend the range at which the client is capable of hearing the signal.

- Near/Far
  - Disproportionate transmit power settings between multiple clients may also cause communication problems within a basic service set (BSS)
  - A low-powered client station that is at a great distance from the access point could become an unheard client if other high-powered stations are very close to that access point
    - Transmissions of the high-powered stations could raise the noise floor near the AP to a higher level
  - Half-duplex nature of the medium usually prevents most near/far occurrences
  - Able to use the same method to troubleshoot the mismatched AP/client power problem to troubleshoot near/far problems with a protocol analyzer

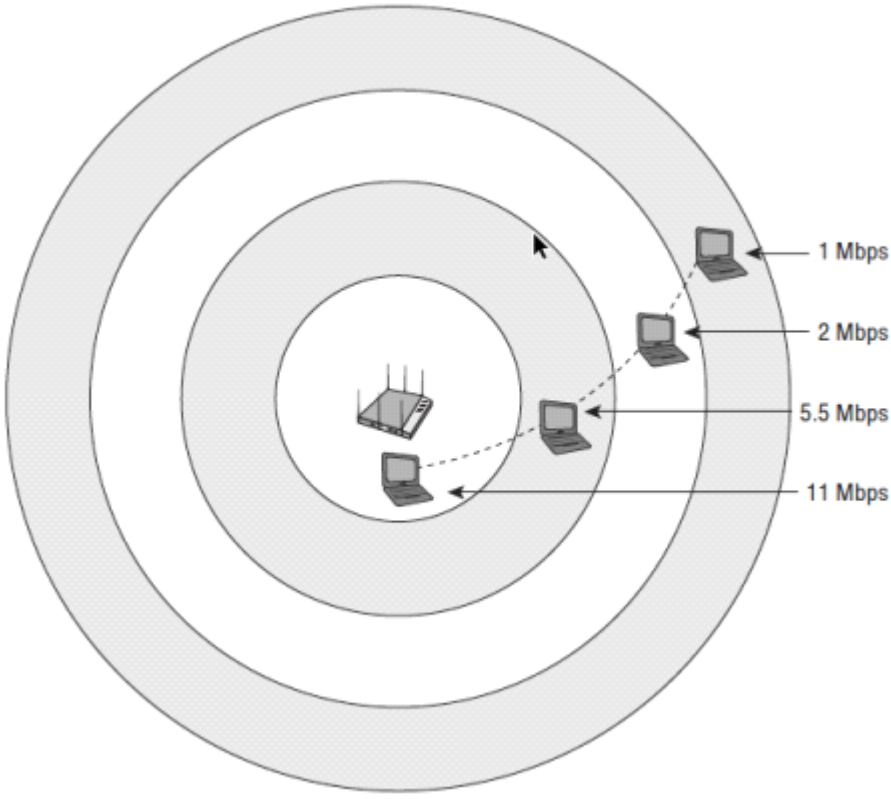


- Hidden node
  - Clear Channel Assessment (CCA) involves listening for 802.11 RF transmissions at the Physical layer
    - medium must be clear before a station can transmit
  - The problem with physical carrier sense is that all stations may not be able to hear

each other.
    - If the station that was about to transmit did not detect any RF energy during its CCA, it would transmit
        - Often occur 2 stations to transmit at the same time
    - The hidden node problem occurs when one client station's transmissions are heard by the access point but are not heard by any or all of the other client stations in the basic service set (BSS).
    - The hidden node problem may exist for several reasons—for example, poor WLAN design or obstructions such as a newly constructed wall or a newly installed bookcase
    - If your end users complain of a degradation of throughput, one possible cause is a hidden node
        - Protocol analyzer is a useful tool in determining hidden node issues.

802.11 coverage considerations

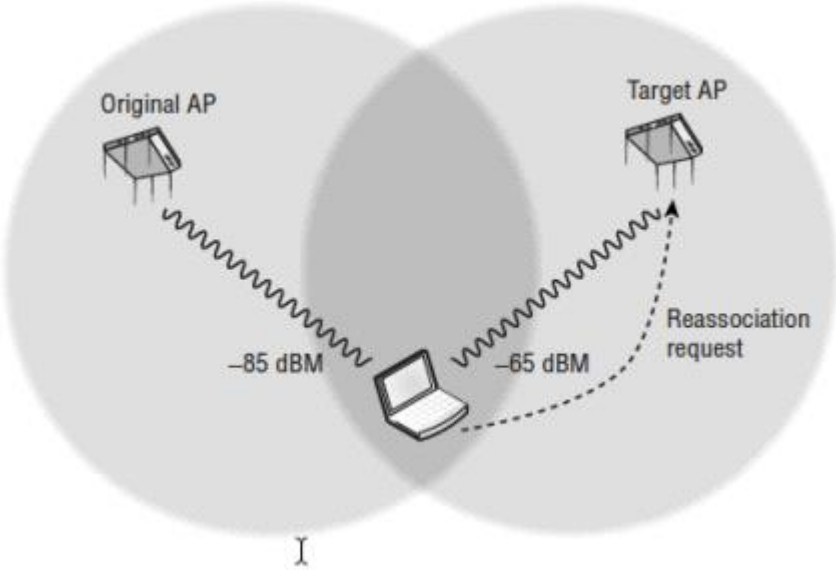
- Dynamic rate switching (DRS)
    - As client station radios move away from an access point, they will shift down to lower bandwidth capabilities by using a process known as dynamic rate switching (DRS)
    - Data rate transmissions between the access point and the client stations will shift down or up depending on the quality of the signal between the two radios
    - There is a correlation between signal quality and distance from the AP.



    - Referred to as dynamic rate shifting, adaptive rate selection, and automatic rate selection
    - Objective of DRS is upshifting and downshifting for rate optimization and improved performance
        - Lower data rates will have larger concentric zones of coverage than the higher data rates
    - The thresholds used for dynamic rate switching are proprietary and are defined by 802.11 radio manufacturers
    - Because vendors implement DRS differently, you may have two different vendor client radios at the same location, while one is communicating with the access
    - All WLAN radios use dynamic rate switching

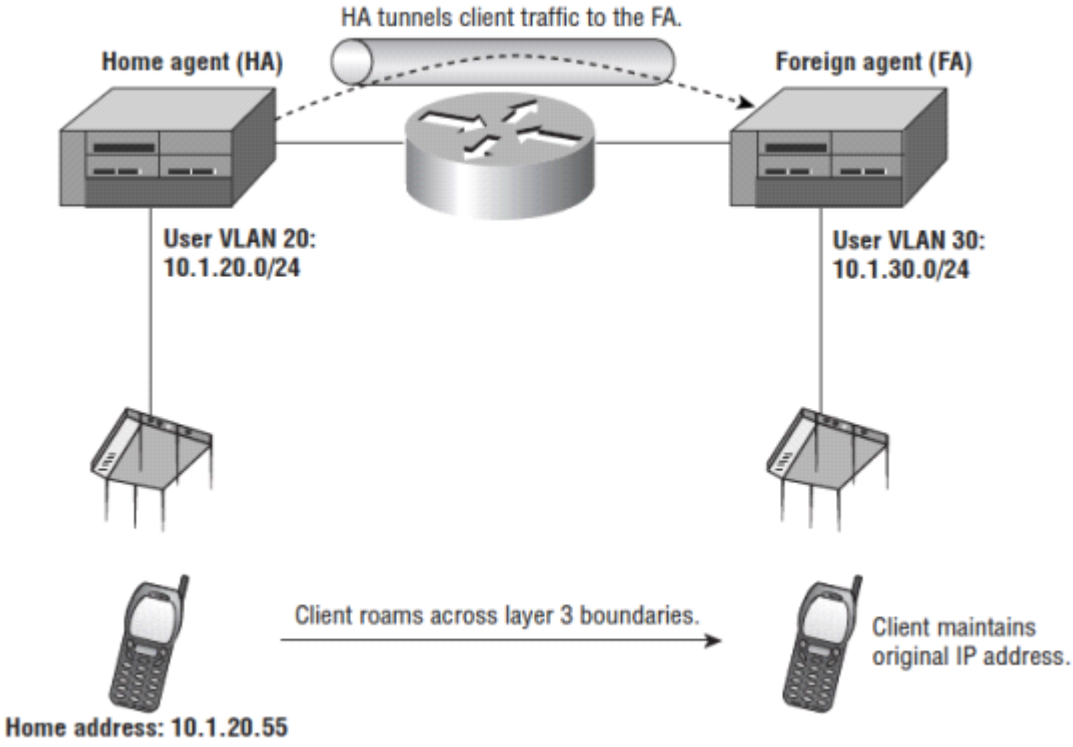
- It is often a recommend practice to turn off the two lowest data rates of 1 and 2 Mbps when designing a 2.4 GHz 802.11b/g/n network
  - Reasons to disable lower data rates
    - Sticky client roaming problems
    - Medium contention
    - Hidden node problem
- When 802.11 radios transmit at very low data rates such as 1 Mbps and 2 Mbps, effectively they cause medium-contention overhead for higher data rate transmitters due to the long wait time
- Turning off the lower data rates is also a common practice to limit cell size when designing high-density WLANs

- Roaming
  - Is the method by which client stations move between RF coverage cells in a seamless manner
  - Seamless communications for client stations moving between the coverage zones within an extended service set (ESS) is vital for uninterrupted mobility.
  - Roaming problems are usually caused by poor network design or faulty client device drivers
  - Client stations, and not the access point, make the decision on whether or not to roam between access points
  - The method by which a client station decides to roam is a set of proprietary rules determined by the manufacturer of the 802.11 radio, usually defined by receive signal strength indicator (RSSI) thresholds
  - As the received signal from the original AP grows weaker and a station hears a stronger signal from another known access point, the station will initiate the roaming process



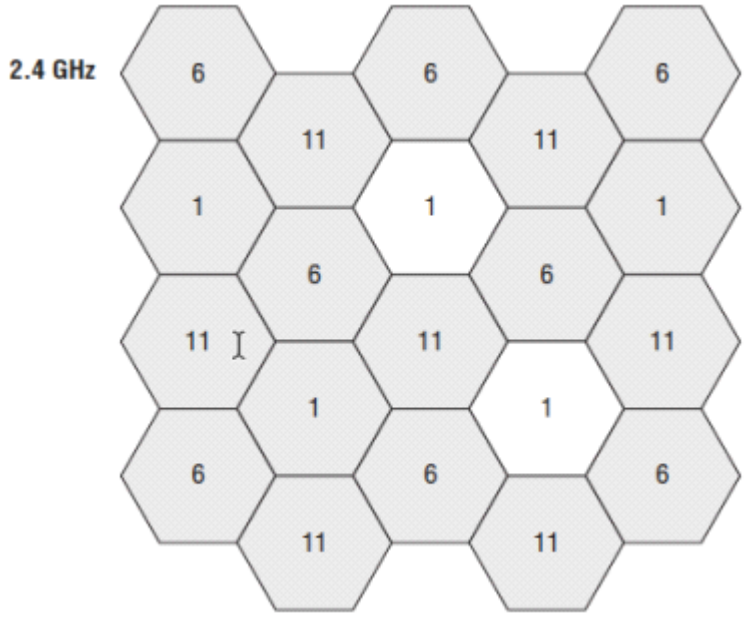
  - The ratified 802.11r amendment also defines faster secure handoffs when roaming occurs between cells in a wireless LAN using the strong security defined in a robust security network (RSN).
  - The best way to ensure that seamless roaming will commence is proper design and a thorough site survey.
  - A proper site survey should be conducted to make sure that a client always has adequate duplicate coverage from multiple access points
  - Roaming problems will occur if there is not enough duplicate cell coverage. Too little duplicate coverage will effectively create a roaming dead zone, and connectivity might even temporarily be lost.
- Layer 3 roaming
  - Because 802.11 wireless networks are usually integrated into pre-existing wired topologies, crossing layer 3 boundaries is often a necessity, especially in large

deployments
    - The only way to maintain upper-layer communications when crossing layer 3 subnets is to provide a layer 3 roaming solution that is based on the Mobile IP standard
    - Mobile IP is an Internet Engineering Task Force (IETF) standard protocol that allows mobile device users to move from one layer 3 network to another while maintaining their original IP address
    - Layer 3 roaming solutions based on Mobile IP use some type of tunneling method and IP header encapsulation to allow packets to traverse between separate layer 3 domains with the goal of maintaining upper-layer communications

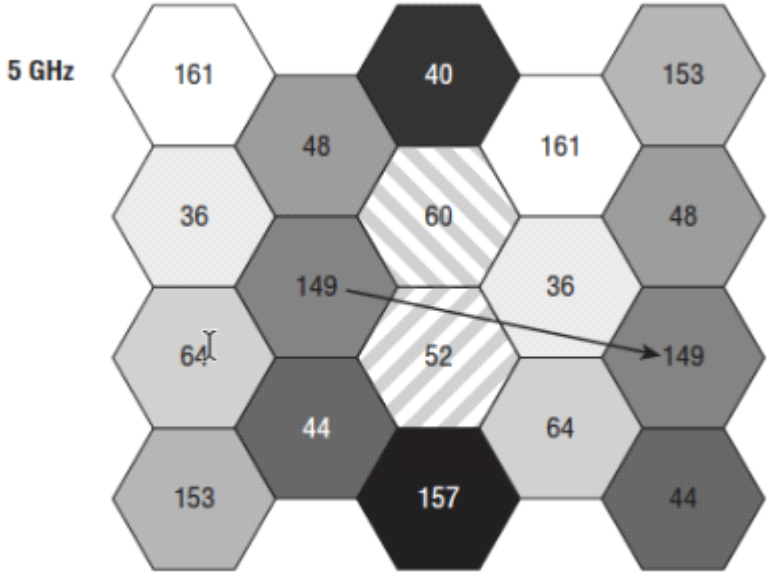


    - The foreign agent is another WLAN controller that handles all Mobile IP communications with the home agent on behalf of the client
    - The foreign agent's IP address is known as the care-of address.
    - The FA uses the HAT tables to locate the HA of the mobile client station
    - Although maintaining upper-layer connectivity is possible with these layer 3 roaming solutions, increased latency is sometimes an issue
- Co-channel interference
    - If all of the APs are on the same channel, unnecessary medium contention overhead occurs.
    - If an AP on channel 1 is transmitting, all nearby access points and clients on the same channel will defer transmissions.
    - The result is that throughput is adversely affected
        - Nearby APs and clients have to wait much longer to transmit because they have to take their turn
    - Unnecessary medium contention overhead that occurs because all the APs are on the same channel is called co-channel interference (CCI)
    - The unnecessary medium contention overhead caused by co-channel interference is a result of improper channel reuse design
    - Do not confuse adjacent channel interference with co-channel interference
        - Adjacent channel interference is also a result of improper channel reuse design
            - Much more serious problem than co-channel interference because of the corrupted data and layer 2 retries
    - Proper channel reuse design is the answer to both co-channel and adjacent channel interference

- Channel reuse/multiple channel architecture
  - To avoid co-channel and adjacent channel interference, a channel reuse design is necessary.
  - The only three channels that meet these criteria in the 2.4 GHz ISM band are channels 1, 6, and 11 in the United States
  - Overlapping coverage cells, therefore, should be placed in a channel reuse pattern

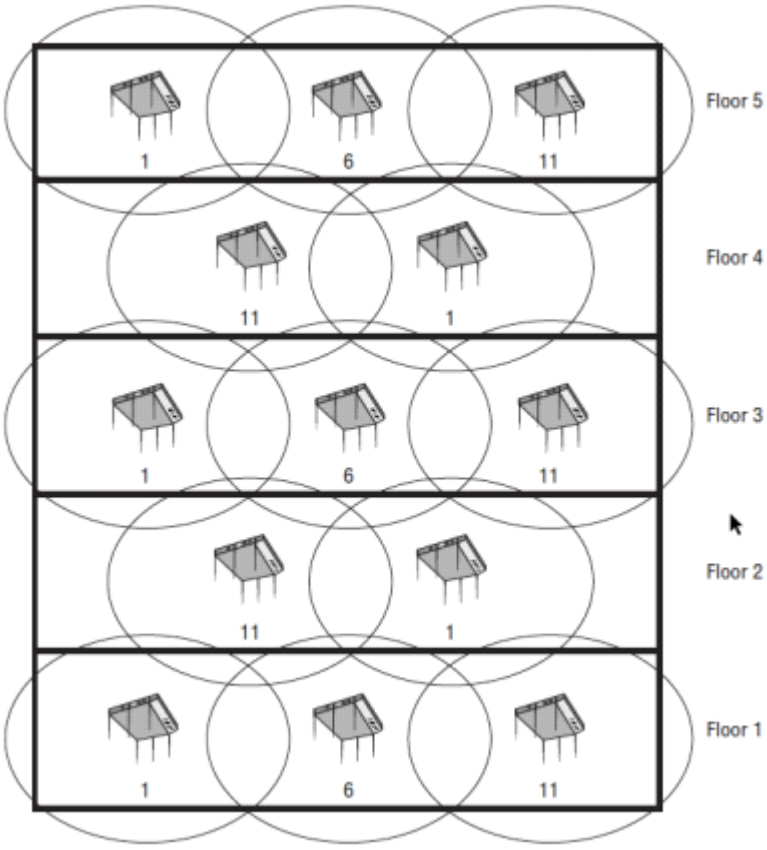


  - A WLAN channel reuse pattern also goes by the name of multiple-channel architecture (MCA).
  - In Europe, a WLAN four-channel reuse pattern of channels 1, 5, 9 and 13 is sometimes deployed
  - Channel reuse patterns should also be used in the 5 GHz frequency bands
    - If all the 5 GHz channels are legally available for transmissions, a total of 25 channels may be available for a channel reuse pattern at 5 GHz
  - Depending on the region, and other considerations, 8 channels, 12 channels, 17 channels, 22 channels, or other combinations may be used for 5 GHz channel reuse patterns.
  - It is a recommended practice that any adjacent coverage cells use a frequency that is at least two channels apart and not use an adjacent frequency



  - The second recommended practice for 5 GHz channel reuse design is that there should be at least two cells of coverage space distance between any two
- Access points transmitting on the same channel

- It is necessary to always think three-dimensionally when designing a multiple-channel architecture reuse pattern
- A site survey must be performed on all floors, and the access points often need to be staggered to allow for a three-dimensional reuse pattern.



- Channel reuse/channel bonding
  - 802.11n technology introduced the capability of bonding two 20 MHz channels to create a larger 40 MHz channel.
  - Channel bonding effectively doubles the frequency bandwidth, meaning double the data rates that can be available to 802.11n radios
  - 802.11n radios that have 40 MHz channel bonding enabled are backward compatible with legacy 80211a radios that only support 20 MHz radios
- Single channel architecture
  - Imagine a WLAN network with multiple access points all transmitting on the same channel and all sharing the same BSSID
  - The client stations see transmissions on only a single channel with one SSID (logical WLAN identifier) and one BSSID (layer 2 identifier)
  - From the prospective of the client station, only one access point exists.
  - Uplink and downlink transmissions are coordinated by a WLAN controller on a single 802.11 channel in such a manner that the effects of co-channel interference are minimized.
  - In a single-channel architecture (SCA) system, the clients think they are associated to only one AP, so they never initiate a layer 2 roaming exchange
  - All of the roaming handoffs are handled by a central WLAN controller
  - The main advantage is that clients experience a zero handoff time, and the latency issues associated with roaming times are resolved.
- Capacity vs. Coverage
  - When a wireless network is designed, two concepts that typically compete with each other are capacity and coverage
  - Proper network design now entails providing necessary coverage while trying to limit the number of devices connected to any single access point at the same time
  - it is important to design the network to try to limit the number of stations that are

simultaneously connected to a single access point
    - WLANs with high user density are becoming a greater concern due to the client population explosion that has occurred.
    - Most WLAN vendors implement proprietary load balancing, band steering, and other MAC layer mechanisms to further assist capacity needs in a high-density user environment.
- Band steering
    - The unlicensed 5 GHz frequency spectrum offers many advantages over the unlicensed 2.4 GHz frequency spectrum for Wi-Fi communications
    - Band steering is not an IEEE 802.11–developed technology
    - When a dual-frequency client first starts up, it will transmit probe requests on both the 2.4 and 5 GHz bands looking for an AP.
    - When a dual-frequency AP hears probe requests on both bands originating from the same client radio, the AP knows that the client is capable of operating in the 5 GHz band
    - AP will then try to steer the client to the 5 GHz band by responding to the client using only 5 GHz transmissions
    - If the client radio continues to try to connect to the AP using the 2.4 GHz radio, the AP will ultimately allow the connection
    - It should be noted that some client device vendors may also implement proprietary client-side band steering.
    - In environments where a high density of client devices exists, band steering to both frequencies can be used to balance an almost equal number of clients to both of the radios in the AP
- Load balancing
    - WLAN vendors also use methods to manipulate the MAC sublayer to balance clients between multiple access points
    - load balancing clients between access points ensures that a single AP is not overloaded with too many clients and that the total client population can be served by numerous APs with the final result being better performance.
    - Load balancing between access points is typically implemented in areas where there is a high density of clients and roaming is not necessarily the priority
    - In areas where roaming is needed, load balancing is usually not a good idea because the mechanisms may cause clients to become sticky and stay associated to the AP too long
- High Density WLANs
    - Once you have determined the types of devices that are being used and the types of applications, you can then calculate the amount of airtime consumption
    - To estimate the number of devices supported on a single AP radio, divide the individual airtime required per device into 80 percent.
        - 80 / single device airtime consumption = # devices per AP radio
- Oversized coverage cells
    - A mistake often made when deploying access points is to have the APs transmit at full power.
    - Oversized coverage usually will not meet your capacity needs
    - Oversized coverage cells can cause hidden node problems.
    - Access points at full power will most likely also increase the odds of co-channel interference due to bleed-over transmissions
    - In some cases, APs at full power may not be able to hear the transmissions of client stations with lower transmit power
    - If the access point coverage and range is a concern, the best method of extending range is to increase the AP antenna gain instead of increasing transmit power.
- Physical environment
    - Although physical environment does not cause RF interference, physical obstructions can indeed disrupt and corrupt an 802.11 signal
    - An example of this is the scattering effect caused by a chain-link fence or safety glass with wire mesh

- The only ways to eliminate physical interference is to remove the obstruction or add more APs.
- The best method of dealing with the physical environment is to perform a proper site survey

Voice vs. data

- Most data applications in a Wi-Fi network can handle a layer 2 retransmission rate of up to 10 percent without any noticeable degradation in performance
- However, time-sensitive applications such as VoIP require that higher-layer IP packet loss be no greater than 2 percent
- Therefore, Voice over Wi-Fi (VoWiFi) networks need to limit layer 2 retransmissions to 5 percent or less to guarantee the timely and consistent delivery of VoIP packets
- Most enterprise data applications will operate within a poorly designed WLAN but will not run optimally
  - Lack of a site survey or an improper survey results in the poor design
- Adding voice to the WLAN often exposes existing problems
  - Because data applications can withstand a much higher layer 2 retransmission rate, problems that existed within the WLAN may have gone unnoticed
- Optimizing the WLAN to support voice traffic will optimize the network for all wireless clients, including the clients running data applications other than voice

Performance

- Various factors can affect the coverage range of a wireless cell, and just as many factors can affect the aggregate throughput in an 802.11 WLAN
- The following variables can affect the range of a WLAN
  - Transmission Power Rates
    - The original transmission amplitude (power) will have an impact on the range of an RF cell
    - APs with too much transmission amplitude can cause many problems
  - Antenna Gain
    - Antennas are passive-gain devices that focus the original signal
    - If you want to increase the range for the clients, the best solution is to increase the antenna gain of the access point.
  - Antenna Type
    - Antennas have different coverage patterns
    - Using the right antenna will give the proper coverage and reduce multipath and nearby interference
  - Wavelength
    - Higher frequency signals have a smaller wavelength property and will attenuate faster than a lower-frequency signal with a larger wavelength
    - 2.4GHz goes further than 5GHz
  - Free Space Path Loss
    - In any RF environment, free space path loss (FSPL) attenuates the signal as a function of distance and frequency
  - Physical Environment
    - Walls and other obstacles will attenuate an RF signal because of absorption and other RF propagation behaviors
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
    - The medium access method that uses interframe spacing, physical carrier sense, virtual carrier sense, and the random back-off timer creates overhead and consumes bandwidth
  - Encryption
    - Extra overhead is added to the body of an 802.11 data frame whenever encryption is implemented
  - Application Use
    - Different types of applications have variable effects on bandwidth consumption
  - Number of Clients
    - Remember that the WLAN is a shared medium

- Layer 2 Retransmissions
  - various problems can cause frames to become corrupted
    - If frames are corrupted, they will need to be retransmitted and throughput will be affected

Weather

- When deploying 802.11 outdoors as mesh or bridge configurations
- Following weather conditions must be considered
  - Lightning
    - Direct and indirect lightning strikes can damage WLAN equipment
    - Lightning arrestors should be used for protection against transient currents
  - Wind
    - Because of the long distances and narrow beamwidths, highly directional antennas are susceptible to movement or shifting caused by wind
    - Even slight movement of a highly directional antenna can cause the RF beam to be aimed away from the receiving antenna, interrupting the communications.
  - Water
    - Conditions such as rain, snow, and fog present two unique challenges.
    - outdoor equipment must be protected from damage caused by exposure to water
    - Consider National Electrical Manufacturers Association (NEMA)
    - Cables and connectors should be checked on a regular basis for damage
    - A torrential downpour can attenuate a signal as much as 0.08 dB per mile (0.05 dB per kilometre) in both the 2.4 GHz and 5 GHz frequency ranges.
  - Air Stratification
    - A change in air temperature at high altitudes is known as air stratification (layering).
    - Changes in air temperature can cause refraction.
  - UV/Sun
    - UV rays and ambient heat from rooftops can damage cables over time if proper cable types are not used.

Upper layer troubleshooting

- WLANs very often get blamed for causing problems that actually exist in the wired network at higher layers
- If it can be determined that the problem is not a layer 1 or layer 2 problem, then the problem is usually a networking issue or problems with an application.
- If a VLAN was to fail, the various points of failure include a misconfigured switch, incorrect IP helper address, and DHCP scope with no remaining leases
- If the Wi-Fi network is not the problem, troubleshooting layers 3–7 will be necessary

802.11 network security architecture

Sunday, May 10, 2020 09:23 PM

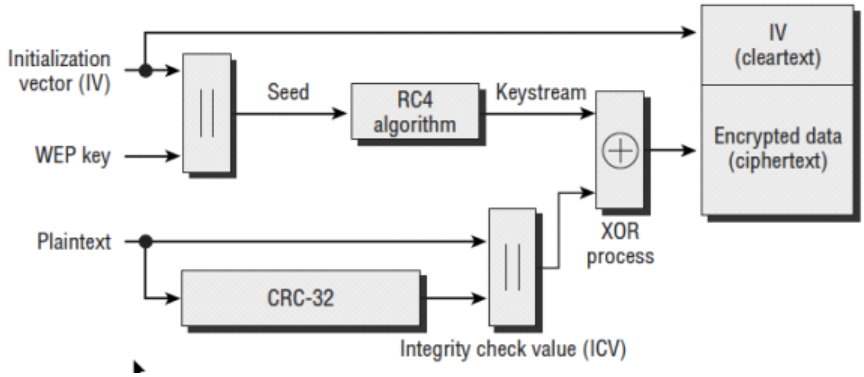
802.11 security basics

- Data privacy and integrity
  - All data transmissions travel in the open air
  - Protecting data privacy in a wired network is much easier because physical access to the wired medium is more restricted, whereas access to wireless transmissions is available to anyone in listening range
    - Therefore, using cipher encryption technologies to obscure information is mandatory to provide proper data privacy.
  - 2 most common algorithms used to protect data are:
    - RC4 algorithm (RC stands for Ron's Code or Rivest Cipher) Algorithm
      - Is a streaming cipher used in technologies that are often used to protect Internet traffic, such as Secure Sockets Layer (SSL)
      - Is incorporated into two legacy encryption methods known as WEP and TKIP
    - Advanced Encryption Standard Algorithm (AES)
      - Originally named the Rijndael algorithm
      - is a block cipher that offers much stronger protection than the RC4 streaming cipher
      - Used to encrypt 802.11 wireless data by using an encryption method known as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
      - Encrypts data in fixed data blocks with choices in encryption key strength of 128, 192, or 256 bits.
      - AES cipher is the mandated algorithm of the U.S. government for protecting both sensitive and classified information
  - WEP, TKIP and CCMP all use a data integrity check to ensure that the data has not been maliciously altered
- Authentication, authorization, and accounting (AAA)
  - Authentication
    - Is the verification of identity and credentials
    - Users or devices must identify themselves and present credentials
    - More secure authentication systems use multifactor authentication
  - Authorization
    - Determines if the device or user is authorized to have access to network resources
    - Can be based on
      - Type of device
      - Time of day restrictions
      - Location
    - Authentication must be completed before authorization takes place
  - Accounting
    - Is tracking the use of network resources by users and devices
    - A record is kept of user identity, which resource was accessed, and at what time
    - Often a requirement of many industry regulations, such as the payment card industry (PCI)
- Segmentation
  - Is the chosen method of separating user traffic within a network
  - can be achieved through a variety of means, including firewalls, routers, VPNs, and VLANs
  - Segmentation is also intertwined with role-based access control (RBAC)
- Monitoring and policy
  - A full-time monitoring solution is also needed to protect against possible attacks that target the WLAN

- Be monitored by a wireless intrusion detection system (WIDS) possible attacks that target the WLAN
- Depending on the level of risk assessment, not all businesses require a monitoring solution but WLAN monitoring solution is highly recommended

Legacy 802.11 security

- Legacy authentication
  - The original 802.11 standard specified 2 methods of authentication
    - Open System authentication
    - Shared Key authentication
  - These legacy authentication methods were not so much an authentication of user identity, but more of an authentication of capability
  - Open System authentication does not require the use of any credentials, every client gets authenticated and therefore authorized onto network resources after they have been associated
- Static WEP encryption
- is a layer 2 encryption method that uses the RC4 streaming cipher
- 3 main goals of WEP encryption
  - Confidentiality
  - Access Control
  - Data Integrity
- 64-bit WEP uses a secret 40-bit static key, which is combined with a 24-bit number selected by the radio's device drivers
  - This 24-bit number, known as the initialization vector (IV), is sent in cleartext & is different on every frame
- How does WEP work?
  - Runs a cyclic redundancy check (CRC) on the plaintext data that is to be encrypted
  - Appends the integrity check value (ICV) to the end of the plaintext data
  - 24-bit cleartext initialization vector (IV) is then generated & combined with the static secret key
  - Uses both the static key & the IV as seeding material through a pseudorandom algorithm that generates random bits of data known as a keystream
    - These pseudorandom bits are equal in length to the plaintext data that is to be encrypted
  - The pseudorandom bits in the keystream are then combined with the plaintext data bits by using a Boolean XOR process
  - End result is the WEP ciphertext, which is the encrypted data
  - The encrypted data is then prefixed with the cleartext IV



- WEP weaknesses:
  - IV Collisions Attack
    - Because of the limited size of the IV space, IV collisions occur, and an attacker can recover the secret key much easier when IV collisions occur in wireless networks.
  - Weak Key Attack
    - An attacker can recover the secret key much easier by recovering the known weak IV keys
  - Reinjection Attack
    - Hacker tools exist that implement a packet reinjection attack to accelerate the

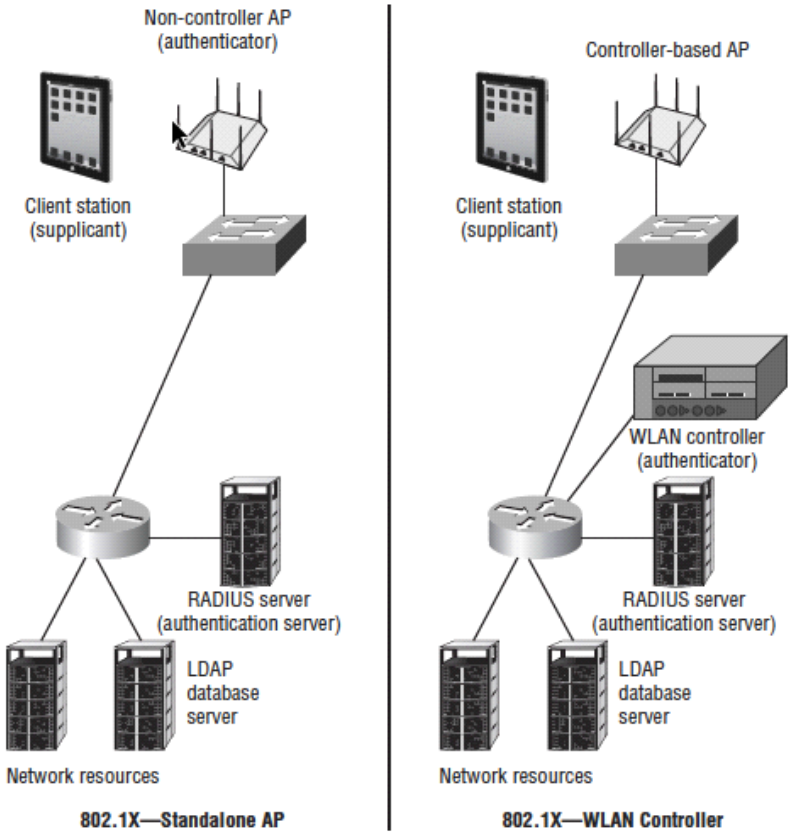
collection of weak IVs on a network with little traffic
    - Bit-Flipping Attack
        - The ICV data integrity check is considered weak
        - WEP encrypted packets can be tampered with
- WEP cracking tools have been available for many years
    - May use a combination of the first 3 mentioned attacks and can crack WEP in less than 5 minutes
- After an attacker has compromised the static WEP key, any data frame can be decrypted with the newly discovered key.
- MAC filters
    - Every network card has a physical address known as a MAC address (a 12-digit hexadecimal number)
    - MAC filters can be configured to either allow or deny traffic from specific client MAC addresses to associate and connect to an AP.
    - The 802.11 standard does not define MAC filtering, and any implementation of MAC filtering is vendor specific.
    - It should be noted that MAC addresses can be spoofed, or impersonated, and any amateur hacker can easily bypass any MAC filter by spoofing an allowed client MAC address.
    - MAC filtering is not considered a reliable means of security for wireless enterprise networks
- SSID cloaking
    - Access points typically have a setting called Closed Network or Broadcast SSID
    - By either enabling a closed network or disabling the broadcast SSID feature, you can hide, or cloak, your wireless network name
    - implement a closed network, the SSID field in the beacon frame is null (empty), and therefore passive scanning will not reveal the SSID to client stations that are listening to beacons
    - Note that an access point in a closed network will respond to any configured client station that transmits directed probe requests with the properly configured SSID
    - Although implementing a closed network may hide your SSID from some of these WLAN discovery tools, anyone with a layer 2 wireless protocol analyzer can capture the frames transmitted by any legitimate end user and discover the SSID, which is transmitted in cleartext
    - SSID cloaking is by no means an end-all wireless security solution
        - 802.11 standard does not define SSID cloaking, and therefore, all implementations of a closed network are vendor specific

Robust security

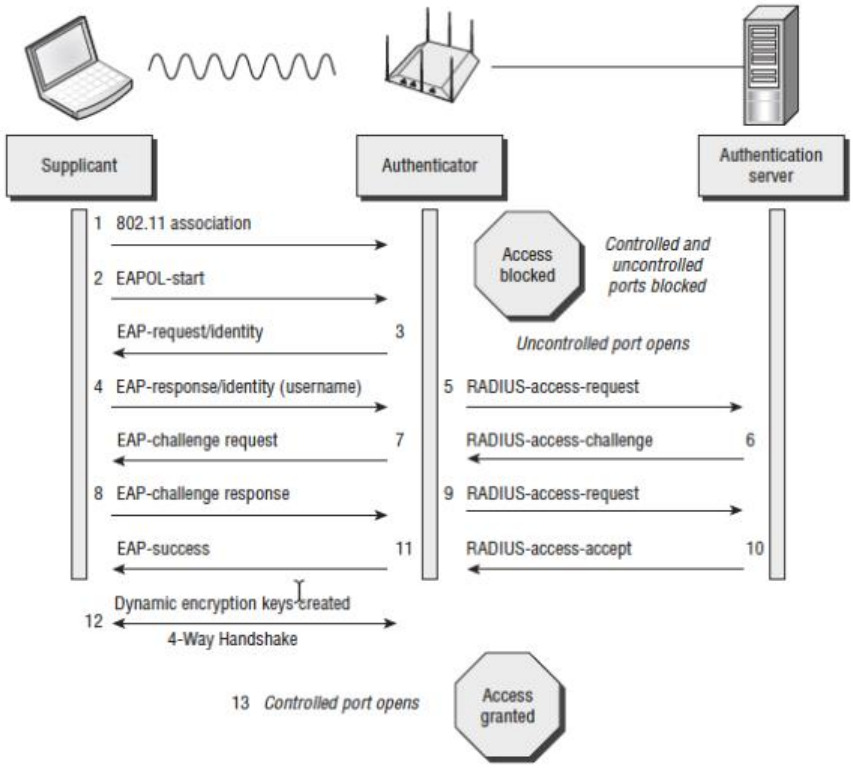
- Robust security network (RSN)
    - 2 stations (STAs) must authenticate and associate with each other, as well as create dynamic encryption keys through a process known as the 4-Way Handshake
        - Referred to as an Robust Security Network Association (RSNA)
    - Counter Mode with Cipher Block Chaining Message Authentication (CCMP/AES) encryption is the mandated encryption method
        - Temporal Key Integrity Protocol (TKIP/RC4) is an optional encryption method
    - An RSN can be identified by a field found in beacons, probe response frames, association request frames, and reassociation request frames. This field is known as the RSN Information Element (IE).
- Authentication and authorization
    - Authentication is the verification of user identity
    - Authorization involves whether a device or user is granted access to network resources and services credentials
- PSK authentication
    - The 802.11-2012 standard defines authentication and key management (AKM) services.
    - An authentication and key management protocol (AKMP) can be either a pre-shared (PSK) or an EAP protocol used during 802.1X authentication
    - PSK authentication is meant to be used in SOHO environments because the stronger

enterprise 802.1X authentication solutions are not available.
    - WPA/WPA2-Personal utilizes PSK authentication
        - Prior to the IEEE ratification of the 802.11i amendment, the Wi-Fi Alliance introduced the Wi-Fi Protected Access (WPA) certification
        - The intended goal of WPA-Personal was to move away from static encryption keys to dynamically generated keys using a simple passphrase as a seed
        - WPA/WPA2-Personal allows an end user to enter a simple ASCII character string, dubbed a passphrase, anywhere from 8 to 63 characters in size
        - The only practical difference between WPA (TKIP/RC4) and WPA2 (CCMP/AES) has to do with the encryption cipher
        - If PSK authentication is the chosen security method, WPA2-Personal should always be used
    - Proprietary PSK authentication
        - The biggest problem with using PSK authentication in the enterprise is social engineering
        - The PSK is the same on all WLAN devices. If an end user accidentally gives the PSK to a hacker, WLAN security is compromised
        - If an employee leaves the company, to maintain a secure environment all of the devices have to be reconfigured with a new 256-bit PSK.
        - Several enterprise WLAN vendors have come up with a creative solution to using WPA/ WPA2-Personal that solves some of the biggest problems of using a single passphrase for WLAN access
            - Each computing device or user will have their own unique PSK for the WLAN
            - Individual users can be mapped to a unique WPA/WPA2-Personal passphrase
            - Individual users are then assigned a unique PSK that is created either dynamically or manually
            - The PSKs that are generated can also have an expiration date
            - Unique time-based PSKs can also be used in a guest WLAN environment as a replacement for more traditional username/ password credentials.
                - If a unique PSK is compromised, an administrator only has to revoke the single PSK credential and no longer has to reconfigure all access points and end user devices.
        - A proprietary PSK solution provides unique user credentials that standard PSK cannot provide
        - Additionally, proprietary PSK solutions with unique credentials do not require anywhere near the complex configuration needed for 802.1X/EAP.
- 802.1X/EAP framework
- The IEEE 802.1X standard is not specifically a wireless standard and is often mistakenly referred to as 802.11x
    - The 802.1X standard is a port-based access control standard.
- An 802.1X framework may be implemented in either a wireless or wired environment
- Consists of three main components
    - Supplicant
        - A host with software that requests authentication and access to network resources is known as a supplicant
        - Would be a client station requesting access to network resources
- Authenticator
    - Blocks traffic or allows traffic to pass through its port entity
    - Authentication traffic is normally allowed to pass through the authenticator, whereas all other traffic is blocked until the identity of the supplicant has been verified
    - The authenticator maintains 2 virtual ports
        - Uncontrolled port
        - Controlled port
    - Uncontrolled allows EAP traffic to pass through
    - Controlled blocks all other traffic until supplicant is authenticated
    - A standalone access point or WLAN controller would be the authenticator

- Authentication Server (AS)
  - Validates the credentials of the supplicant that is requesting access and notifies the authenticator that the supplicant has been authorized.
  - Maintains a user database or may proxy with an external database, such as an LDAP database, to authenticate user credentials.
  - Typically a Remote Authentication Dial-In User Service (RADIUS) server



  - Note that some WLAN vendors offer solutions where either a standalone AP or a WLAN controller can dual-function as a RADIUS server and perform direct LDAP queries, thus eliminating the need for an external RADIUS server
  - Although the supplicant, authenticator, and authentication server work together to provide the framework for 802.1X port-based access control, an authentication protocol is needed to perform the authentication process.
    - Extensible Authentication Protocol (EAP) is used to provide user authentication
  - AP is a flexible layer 2 authentication protocol used by the supplicant and the authentication server to communicate
  - The authenticator allows the EAP traffic to pass through its virtual uncontrolled port.
  - After the authentication server has verified the credentials of the supplicant, the server sends a message to the authenticator that the supplicant has been authenticated
  - The authenticator is then authorized to open the virtual controlled port and allow all other traffic to pass through.

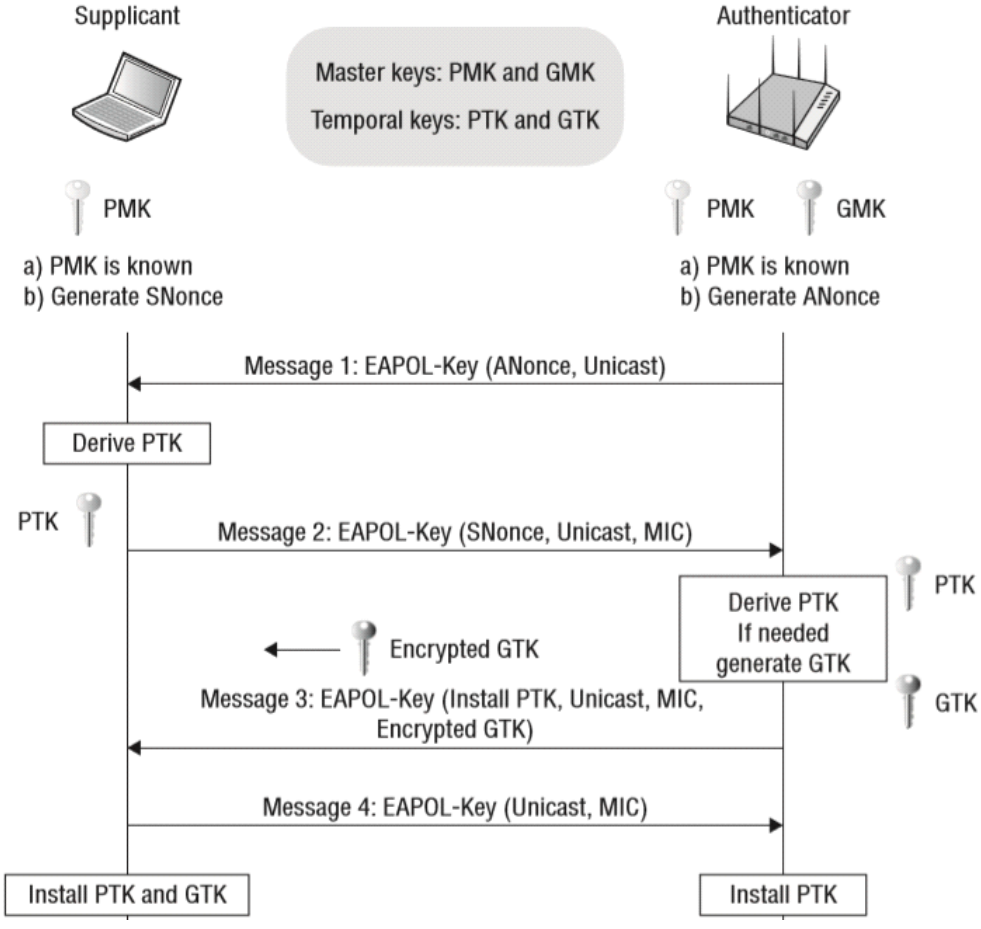


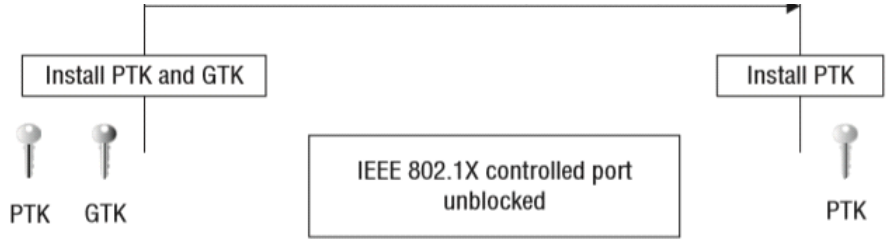
- EAP types
  - EAP is a layer 2 protocol that is very flexible, and many different flavors of EAP exist.
  - Some, such as Cisco's Lightweight Extensible Authentication Protocol (LEAP), are proprietary, whereas others, such as Protected Extensible Authentication Protocol (PEAP), are considered standards based
  - Some provide for only one-way authentication; others provide two-way authentication.
  - Mutual authentication not only requires that the authentication server validate the client credentials, but the supplicant must also authenticate the validity of the authentication server.
  - Most types of EAP that require mutual authentication use a server-side digital certificate to validate the authentication server.
  - A server-side certificate is installed on the RADIUS server, while the certificate authority (CA) root certificate resides on the supplicant
  - The Certificate exchange also creates an encrypted Secure Sockets Layer (SSL) / Transport Layer Security (TSL) tunnel in which the supplicant's username/password credentials or client certificate can be exchanged.

TABLE 4.3 EAP Comparison Chart

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco proprietary	RFC-2716	IETF draft	IETF draft	IETF draft	IETF draft	IETF draft
Digital Certificates—Client	No	No	Yes	Optional	No	Yes	Optional	No
Digital Certificates—Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password Authentication	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs—Client	No	No	No	No	No	No	No	Yes
PACs—Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Debatable	Yes	Yes	Yes	Yes	Yes	Yes
Tunneled Authentication	No	No	Optional	Yes	Yes	Yes	Yes	Yes
Wi-Fi Alliance supported	No	No	Yes	Yes	Yes	No	Yes	Yes
Man-in-the-Middle Protection	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Dictionary Attack Resistance	No	No	Yes	Yes	Yes	N/A	Yes	Yes
Token support	No	No	Yes	Yes	No	Yes	Yes	Yes

- Dynamic encryption-key generation
    - 802.1X/EAP framework does not require encryption, the use of encryption is recommended.
    - However, a by-product of 802.1X/EAP is the generation and distribution of dynamic encryption keys
    - EAP protocols that utilize mutual authentication provide “seeding material” that can be used to generate encryption keys dynamically.
    - The advantage of dynamic keys is that every user has a different and unique key that cannot be compromised by social engineering attacks.
    - These dynamic keys are generated per session per user, meaning that every time a client station authenticates, a new key is generated and every user has a unique and separate key.
- 4-Way Handshake
    - Two stations (STAs) must establish a procedure to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the 4-Way Handshake.
    - RSNAs utilize a dynamic encryption-key management method that involves the creation of five separate keys.
    - Part of the RSNA process involves the creation of two master keys known as the Group Master Key (GMK) and the Pairwise Master Key (PMK).
    - The PMK is created as a result of the 802.1X/EAP authentication
    - These master keys are the seeding material used to create the final dynamic keys that are used for encryption and decryption
    - The final encryption keys are known as the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK)
    - The PTK is used to encrypt/decrypt unicast traffic, and the GTK is used to encrypt/decrypt broadcast and multicast traffic.
    - The 4-Way Handshake will always be the final four frames exchanged during either an 802.1X/EAP authentication or a PSK authentication
    - Also, every time a client radio roams from one AP to another, a new 4-Way Handshake must occur so that new unique dynamic keys can be generated





- WPA/WPA2-Personal
  - If you do not own a RADIUS server, 802.1X/EAP authentication will not be possible.
    - Because most of us do not have a RADIUS server, the 802.11-2012 standard offers a simpler method of authentication using a PSK
  - This method involves manually typing matching passphrases on both the access point and all client stations that will need to be able to associate to the wireless network
  - A formula is run that converts the passphrase to a Pairwise Master Key (PMK) used with the 4-Way Handshake to create the final dynamic encryption keys.
  - still requires significant administrative overhead and has potential social engineering issues in a corporate or enterprise environment
  - An 802.1X/EAP solution as defined by WPA/WPA2-Enterprise is the preferred method of security in a corporate and workplace environment
- Temporal Key Integrity Protocol (TKIP) encryption
  - This method uses the RC4 cipher just as WEP encryption does
  - The problem with WEP was not the RC4 cipher but how the encryption key was created
  - TKIP was developed to rectify the problems that were inherent in WEP.
  - TKIP starts with a 128-bit temporal key that is combined with a 48-bit initialization vector (IV) and source and destination MAC addresses in a complicated process known as per-packet key mixing
  - This key-mixing process mitigates the known IV collision and weak key attacks used against WEP
  - Additionally, TKIP uses a stronger data integrity check known as the message integrity check (MIC) to mitigate known bit-flipping attacks against WEP.
  - All TKIP encryption keys are dynamically generated as a final result of the 4-Way Handshake.
  - The 802.11n and higher amendments do not permit the use of WEP encryption or TKIP encryption for the High Throughput (HT) and Very High Throughput (VHT) data rates
- CCMP encryption
  - The default encryption method defined under the 802.11i amendment is known as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - This method uses the Advanced Encryption Standard (AES) algorithm (Rijndael algorithm)
    - CCMP/AES uses a 128-bit encryption-key size and encrypts in 128-bit fixed-length blocks.
  - All CCMP encryption keys are dynamically generated as a final result of the 4-Way Handshake.
  - CCMP/AES encryption will add an extra 16 bytes of overhead to the body of an 802.11 data frame
  - Because the AES cipher is processor intensive, older legacy 802.11 devices do not have the processing power necessary to perform AES calculations

Traffic segmentation

- VLANs
  - are used to create separate broadcast domains in a layer 2 network and are often used to restrict access to network resources without regard to physical topology of the network.
  - VLANs are a layer 2 concept and are used extensively in switched 802.3 networks for both security and segmentation purposes.

    - VLANs are used to support multiple layer 3 networks on the same layer 2 switch
    - individual SSIDs can be mapped to individual VLANs, and users can be segmented by the SSID/VLAN pair, all while communicating through a single access point.
    - Each SSID can also be configured with separate security settings.
    - A common strategy is to create a guest, voice, and employee SSID/VLAN pair
    - Management access to the WLAN controllers or APs should also be isolated on a separate VLAN.
    - The way VLANs are deployed in a WLAN environment depends on the design of the network as well as the type of WLAN architecture that is in place
- RBAC
    - Role-based access control (RBAC) is another approach to restricting system access to authorized users.
    - The three main components of an RBAC approach are users, roles, and permissions.
    - Permissions can be defined as layer 2 permissions (VLANS or MAC filters), layer 3 permissions (access control lists), layers 4–7 permissions (stateful firewall rules), and bandwidth permissions
    - When wireless users authenticate via the WLAN, they inherit the permissions of whatever roles they have been assigned.
    - When used in a WLAN environment, role-based access control can provide granular wireless user management

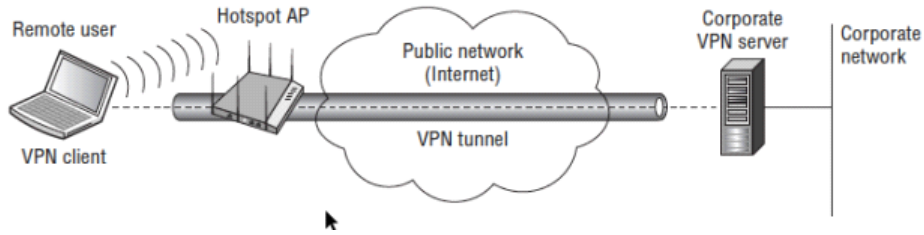
Infrastructure security

- Physical security
    - Access points and other WLAN hardware can be quite expensive
    - Although access points are usually mounted in or near the ceiling, theft can be a problem
    - Enclosure units with locks can be mounted in the ceiling or to the wall
    - Secure enclosure units may also meet aesthetic demands by keeping the access point out of plain sight.
- Interface security
    - All wireless infrastructure devices must be able to be accessed by administrators through a management interface
    - Any interface that is not used should be turned off
    - At a minimum, all the passwords for these configuration options should be changed from the factory defaults.
    - Most infrastructure devices should also support some type of encrypted management capabilities.
    - It is also a highly recommended practice to configure your infrastructure devices from only the wired side and never configure them wirelessly
    - If devices are configured from the wireless side, an intruder might be able to capture your wireless packets and be able to watch what you are doing

VPN wireless security

- Layer 3 VPNs
    - The use of upper-layer virtual private network (VPN) solutions can also be deployed with WLANs
    - VPNs are typically not recommended to provide wireless security in the enterprise due to the overhead and because faster, more secure layer 2 solutions are now available.
    - VPNs do have their place in Wi-Fi security and should definitely be used for remote access
    - Sometimes used in wireless bridging environments
    - Use of VPN technology is mandatory for remote access. Your end users will take their laptops off site and will most likely use public access Wi-Fi hotspots. Because there is no security at most hotspots, a VPN solution is needed.
    - It is imperative that users implement a VPN solution coupled with a personal firewall whenever accessing any public access Wi-Fi networks.
    - VPNs have several major characteristics
        - Provide encryption, encapsulation, authentication, and data integrity
    - Use secure tunneling

        - Process of encapsulating one IP packet within another IP packet
    - The original destination and source IP address of the first packet is encrypted along with the data payload of the first packet
    - VPN tunneling, therefore, protects your original private layer 3 addresses and also protects the data payload of the original packet.
    - The most commonly used layer 3 VPN technology is Internet Protocol Security (IPsec). IPsec VPNs use stronger encryption methods and more secure methods of authentication and are the most commonly deployed VPN solution
    - Most IPsec VPNS are NAT-transversal, but any firewalls at a remote site require (at a minimum) that UDP ports 4500 and 500 be open.
- SSL VPN
    - VPN technologies do exist that operate at other layers of the OSI model, including SSL tunneling
    - Unlike an IPsec VPN, an SSL VPN does not require the installation and configuration of client software on the end user's computer
    - A user connects to a Secure Sockets Layer (SSL) VPN server via a web browser.
    - The traffic between the web browser and the SSL VPN server is encrypted with the SSL protocol or Transport Layer Security (TLS).
    - SSL VPNs are often chosen because of issues with NAT or restrictive firewall policies at remote locations.
- VPN deployment
    - VPNs are most often used for client-based security when connected to public access WLANs and hotspots that do not provide security.
    - VPN technology can provide the necessary level of security for remote access when end users connect to public access WLAN
    - Another common use of VPN technology is to provide site-to-site connectively between a remote office and a corporate office.
    - Most WLAN vendors now offer VPN client-server capabilities in either their APs or WLAN controllers



- Guest WLAN security
    - Guest wireless networks allow Internet access to visitors, such as contractors, students, or salespeople.
    - Therefore, many organizations provide WLAN guest access with a unique SSID and guest VLAN
    - Firewalls are also often used to further restrict the guest user capabilities and even the bandwidth that is available to guests
    - The main security goal of a guest WLAN is to provide guests with an easily accessible wireless portal to the Internet, while at the same time restricting guest user access from the rest of the company network.
    - The security components of a guest WLAN normally consist of the following
        - Guest SSID
            - Normally an open network that has no WPA/WPA2 encryption security
            - Encrypted guest access can also be provided with 802.1X with Hotspot 2.0 using Wi-Fi CERTIFIED Passport client devices
        - Guest VLAN
            - Guest user traffic should be segmented into a unique VLAN tied to an IP subnet that does not mix with the employee user VLAN
            - Guest traffic is often also routed to a demilitarized zone (DMZ).
        - Firewall Policy
            - Guest WLAN firewall policies tend to be very restrictive

        - Guest firewall policies typically allow for DHCP and DNS but restrict access to private networks
        - The guest firewall policy normally routes all user traffic straight to an Internet gateway and away from corporate network infrastructure.
    - Captive Web Portal
        - Guest users must normally log in through a captive web portal page before they can proceed to the Internet
        - One of the most important aspects of the captive web portal page is the legal disclaimer.
        - Businesses are also legally protected if something bad should happen to a guest user's WLAN device, such as being infected by a computer virus
        - A captive portal solution effectively turns a web browser into an authentication service
        - Captive portals can redirect unauthenticated users to a login page using an IP redirect, DNS redirection, or redirection by HTTP.
    - Guest Management Solution
        - Most guest WLANS require a guest user to authenticate with credentials via a captive web portal
        - Therefore, a database of user credentials must be created.
- Captive portal
    - Most hotspots and guest networks are secured by a captive portal
    - A captive portal is essentially the integration of a firewall with an authentication web page.
    - When a user connects to the guest network, whether wired or wireless, any packets that the user transmits are intercepted and blocked from accessing a gateway to the network resources until the user has authenticated through the captive portal.
    - Captive portals are available as standalone software solutions, but most WLAN vendors offer integrated captive portal solutions
    - You can typically personalize the page by adding graphics, such as a company logo, inserting an acceptable use policy, or configuring the logon requirements.
    - Not all captive portal pages require a username and password for authentication. Some vendors have begun to use unique dynamic PSKs as user credentials
    - Captive web portals that do not require credentials still provide an acceptable use policy, which functions as a legal disclaimer for the guest network

Wireless Attacks, Intrusion Monitoring & Policy

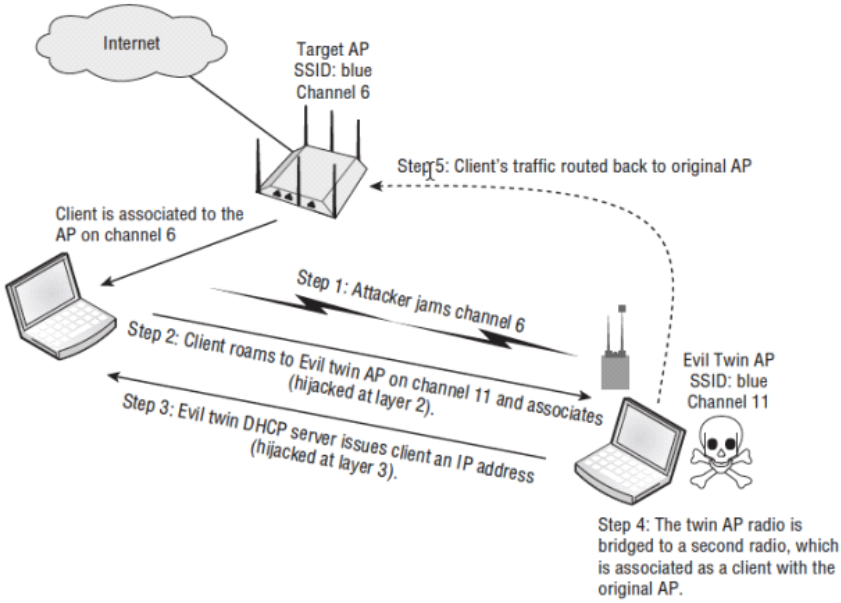
Monday, May 11, 2020 12:02 PM

Wireless attacks

- Rogue wireless devices
  - Rogue access point is any unauthorized Wi-Fi device that is not under the management of the proper network administrators
  - The individuals most responsible for installing rogue access points are typically not hackers
    - but are employees not realizing the consequences of their actions
  - Ad hoc wireless connections also have the potential of providing rogue access into the corporate network
  - The Ethernet connection and the Wi-Fi network interface controller (NIC) can be bridged together
    - Intruder might access the ad hoc wireless network and then potentially route their way to the Ethernet connection and get onto the wired network.
      - Many government agencies and corporations ban the use of ad hoc networks for this very reason
  - On some computers, it is possible to limit the use of multiple NICs simultaneously
  - When the user plugs an Ethernet cable into the computer, the wireless adapter is automatically disabled, eliminating the risk of an intentional or unintentional bridged network
  - Furthermore, besides physical security, there is nothing to prevent an intruder from also connecting their own rogue access point via an Ethernet cable into any live data port provided in a wall plate.
  - If an 802.1X solution is deployed for the wireless network, it can also be used to secure the network ports on the wired network
  - In that case, any new device, including APs, would need to be authenticated to the network prior to being given access
- Peer-to-peer attacks
  - A commonly overlooked risk
  - 802.11 client station can be configured in either Infrastructure mode or Ad Hoc mode.
  - Because an IBSS is by nature a peer-to-peer connection, any user who can connect wirelessly with another user can potentially gain access to any resource available on either computer
  - Users that are associated to the same access point are potentially just as vulnerable to peer-to-peer attacks as IBSS users.
  - Properly securing your wireless network often involves protecting authorized users from each other, because hacking at companies is often performed internally by employees.
  - In most WLAN deployments, Wi-Fi clients communicate only with devices on the wired network, such as email or web servers, and peer-to-peer communications are not needed.
  - If connections are required to other wireless peers, the traffic is routed through a layer 3 switch or other network device before passing to the desired destination station.
  - Client isolation is a feature that can often be enabled on WLAN access points or controllers to block wireless clients from communicating with other wireless clients on the same wireless VLAN
  - Some applications require peer-to-peer connectivity. Many VoWiFi phones offer push-to talk capabilities that use multicasting
- Eavesdropping
  - 802.11 wireless networks operate in license free frequency bands, and all data transmissions travel in the open air
  - Access to wireless transmissions is available to anyone within listening range, and therefore strong encryption is mandatory
  - Wireless communications can be monitored via two eavesdropping methods:
    - Casual eavesdropping
      - Is sometimes referred to as WLAN discovery
      - Is accomplished by simply exploiting the 802.11 frame exchange methods that are clearly defined by the 802.11-2012 standard
      - Software utilities known as WLAN discovery tools exist for the purpose of finding open WLAN networks.
      - Many popular and freely available WLAN discovery software programs, such as inSSIDer, WiFiFoFum, and iStumbler, that can be used by individuals to discover wireless networks
      - WLAN discovery tools send out null probe requests across all license-free 802.11 channels with the hope of receiving probe response frames containing wireless network information, such as SSID, channel, encryption, and so on
      - WLAN discovery is typically considered harmless and in the past was referred to as wardriving

        - Malicious eavesdropping
            - The unauthorized use of 802.11 protocol analyzers to capture wireless communications, is typically considered illegal
            - Most countries have laws making it illegal to listen in on any type of electromagnetic communications, including 802.11 wireless transmissions
            - Many commercial and freeware 802.11 protocol analyzers exist that allow wireless network administrators to capture 802.11 traffic for the purpose of analyzing and troubleshooting their own wireless networks
            - The problem is that anyone with malicious intent can also capture 802.11 traffic from any Wi-Fi network.
            - A wireless intrusion detection system (WIDS) cannot detect malicious eavesdropping
            - For this reason, a strong, dynamic encryption solution such as TKIP/RC4—or even better, CCMP/AES—is mandatory
            - Malicious eavesdropping of this nature is highly illegal.
            - Because of the passive and undetectable nature of this attack, encryption must always be implemented to provide data privacy.
            - The most common targets of malicious eavesdropping attacks are public access hotspots
- Encryption cracking
    - The current WEP-cracking tools that are freely available on the Internet can crack WEP encryption in as little as 5 minutes
    - an attacker usually needs only to capture several hundred thousand encrypted packets with a protocol analyzer and then run the captured data through a WEP-cracking software program
    - The software utility will usually then be able to derive the secret 40-bit or 104-bit key in a matter of seconds
    - After the secret key has been revealed, the attacker can decrypt any and all encrypted traffic
    - Because the attacker can decrypt the traffic, they can reassemble the data and read it as if there was no encryption whatsoever
- Authentication attacks
    - The 802.11-2012 standard does not define which type of EAP authentication method to use, and all flavors of EAP are not created equal
    - Lightweight Extensible Authentication Protocol (LEAP), once one of the most commonly deployed 802.1X/EAP solutions, is susceptible to offline dictionary attacks.
    - The hashed password response during the LEAP authentication process is crackable
    - An attacker merely has to capture a frame exchange when a LEAP user authenticates and then run the capture fi le through an offline dictionary attack tool
    - Password can be derived in a matter of seconds & username is also seen in cleartext during the LEAP authentication process
        - Stronger EAP authentication protocols that use tunneled authentication are not susceptible to offline dictionary attacks
    - If an authorized WLAN portal can be compromised and the authentication credentials can be obtained, network resources are exposed
    - WPA/WPA2-Personal, also known as PSK authentication, is a weak authentication method that is vulnerable to an offline brute-force dictionary attack
    - If a hacker has the passphrase and captures the 4-Way Handshake, they can re-create the dynamic encryption keys and decrypt traffic.
    - A policy mandating very strong passphrases of 20 characters or more should always be in place whenever a WPA/WPA2-Personal solution is deployed
- MAC spoofing
    - Usually, MAC filters are configured to apply restrictions that will allow traffic only from specific client stations to pass through.
    - Unfortunately, MAC addresses can be spoofed, or impersonated, and any amateur hacker can easily bypass any MAC filter by spoofing an allowed client station's address
    - Because of spoofing and because of all of the administrative work involved with setting up MAC filters
        - MAC filtering is not considered a reliable means of security for wireless enterprise networks
        - Should be implemented only as a last resort
- Management interface exploits
    - Interfaces that are not used should be disabled.
    - Strong passwords should be used, and encrypted login capabilities using SSH (Secure Shell) or Hypertext Transfer Protocol Secure (HTTPS) should always be utilized.
    - It is not uncommon for attackers to use security holes left in management interfaces to reconfigure APs.
    - After gaining access via a management interface, an attacker might even be able to initiate a firmware upgrade of the wireless hardware and, while the upgrade is being performed, power off the equipment.

- Wireless hijacking
  - Also known as the evil twin attack
  - The attacker configures access point software on a laptop, effectively turning a Wi-Fi client radio into an access point
  - The access point software is configured with the same SSID that is used by a public hotspot access point
  - The attacker then sends spoofed disassociation or de-authentication frames, forcing users associated with the hotspot AP to roam to the evil twin AP
  - At this point, the attacker has effectively hijacked wireless clients at layer 2 from the original AP.
  - The evil twin will typically be configured with a Dynamic Host Configuration Protocol (DHCP) server available to issue IP addresses to the clients
  - The attacker may also be using a second wireless NIC with their laptop to execute what is known as a man-in-the-middle attack



  - These attacks can take another form in what is known as a Wi-Fi phishing attack. The attacker may also have web server software and captive portal software.
  - Then the attacker's fake login page may request a credit card number from the hijacked user. Phishing attacks are common on the Internet and are now appearing at your local hotspot.
  - The only way to prevent a hijacking, man-in-the-middle, or Wi-Fi phishing attack : use a mutual authentication solution
    - 802.1X/EAP authentication solutions require that mutual authentication credentials be exchanged before a user can be authorized. A user cannot get an IP address unless authorized; therefore, users cannot be hijacked.
- Denial of service (DoS)
  - The attack on wireless networks that seems to receive the least amount of attention is the denial of service (DoS)
  - With the proper tools, any individual with ill intent can temporarily disable a Wi-Fi network by preventing legitimate users from accessing network resources.
  - monitoring systems exist that can detect and identify DoS attacks immediately
  - usually nothing can be done to prevent DoS attacks other than locating and removing the source of the attack.
  - DoS attacks can occur at either layer 1 or layer 2 of the OSI model. Layer 1 attacks are known as RF jamming attacks.
  - 2 types of jamming attacks:
    - Intentional Jamming
      - occur when an attacker uses some type of signal generator to cause interference in the unlicensed frequency space
      - Narrowband and wideband jammers exist
      - Either causing all data to become corrupted or causing the 802.11 radios to continuously defer when performing a clear channel assessment (CCA).
    - Unintentional Jamming
      - More common
      - Microwave ovens, cordless phones, and other devices can also cause denial of service.
      - not necessarily an attack, it can cause as much harm as an intentional jamming attack.
  - The best tool to detect any type of layer 1 interference, whether intentional or unintentional, is a spectrum

analyzer
    - The more common type of denial-of-service attacks that originate from hackers are layer 2 DoS attacks
        - A wide variety of layer 2 DoS attacks exist that are a result of manipulating 802.11 frames
        - most common involves spoofing disassociation or de-authentication frames
    - Many more types of layer 2 DoS attacks exist, including association floods, authentication floods, PS-Poll floods, and virtual carrier attacks
    - management frame protection (MFP) mechanisms for the prevention of spoofing certain types of 802.11 management frames
    - A spectrum analyzer is your best tool to detect a layer 1 DoS attack, and a protocol analyzer or wireless IDS is your best tool to detect a layer 2 DoS attack
    - The best way to prevent any type of denial-of-service attack is physical security.
- Vendor-specific attacks
    - Hackers often find holes in the firmware code used by specific WLAN access point and WLAN controller vendors
    - Most of these vendor-specific exploits are in the form of buffer overflow attacks.
    - Fix normally via firmware update
- Social engineering
    - Is a technique used to manipulate people into divulging confidential information, such as computer passwords.
    - The best defense against social engineering attacks are strictly enforced policies to prevent confidential information from being shared.
    - Any information that is static is extremely susceptible to social engineering attacks

Intrusion monitoring

- Wireless intrusion detection system (WIDS)
    - might be necessary even if there is no authorized 802.11 Wi-Fi network on site
    - After an 802.11 network is installed for access, it has become almost mandatory to also have a WIDS because of the other numerous attacks against Wi-Fi, such as DoS, hijacking, and so on.
    - The typical WIDS is a client-server model that consists of three components:
        - WIDS Server
            - is a software server or hardware server appliance acting as
            - Uses signature analysis, behavior analysis, protocol analysis, and RF spectrum analysis to detect potential threats a central point of monitoring security and performance data collection
                - Behavior analysis looks for 802.11 anomalies
        - Management Consoles
            - A software-based management console is used to communicate back to a WIDS server from a desktop station
            - used for administration and configuration of the server and sensors.
            - The management console can also be used for 24/7 monitoring of 802.11 wireless networks
        - Sensors (Hardware or software)
            - May be placed strategically to listen to and capture all 802.11 communications.
            - The eyes and ears of a WIDS monitoring solution
            - Basically radio devices that are in a constant listening mode as passive devices
            - Are usually hardware based and resemble an access point
            - Standalone sensors do not provide access to WLAN clients because they are configured in a listen-only mode
            - The sensors constantly scan all 14 channels in the 2.4 GHz ISM band, as well as all of the channels in the 5 GHz U-NII bands
            - Access points can also be used as part-time sensors.
            - WIDS are best at monitoring layer 2 attacks, such as MAC spoofing, disassociation attacks, and de-authentication attacks
    - Currently, three WIDS design models exist
        - Overlay
            - The most secure model
            - WIDS that is deployed on top of the existing wireless network.
            - uses an independent vendor's WIDS and can be deployed to monitor any existing or planned WLAN
            - The overlay solution consists of a WIDS server and sensors that are not part of the WLAN solution that provides access to clients.
            - Dedicated overlay systems are not as common as they used to be as WIDS features been rolled into enterprise wireless solutions
        - Integrated

        - A centralized WLAN controller or a centralized network management server (NMS) functions as the IDS server
        - Access points can be configured in a full-time sensor-only mode or can act as part-time sensors when not transmitting as access points
        - A recommended practice would be to also deploy some APs as fulltime sensors
        - less expensive solution but may not have all the capabilities that are offered in an overlay WIDS
      - Integration Enabled
        - APs integrate software code that can be used to turn the APs into sensors that will communicate with the third-party WIDS server
- Wireless intrusion prevention system (WIPS)
  - Most WIDS vendors prefer to call their product a wireless intrusion prevention system
  - The reason that they prefer the term prevention systems is that they are all now capable of mitigating attacks from rogue APs and rogue clients
  - A WIPS characterizes access points and client radios in four or more classifications
    - Infrastructure Device
      - Refers to any client station or AP that is an authorized member of the company's wireless network
    - Unknown Device
      - Is assigned automatically to any new 802.11 radios that have been detected but not classified as a rogue or infrastructure device yet
    - Known Device
      - Refers to any client station or AP that is detected
      - The known device label is typically manually assigned by an administrator to radio devices of neighboring businesses that are not considered a threat WIPS and whose identity is known.
    - Rogue Device
      - Refers to any client station or AP that is considered an interfering device and a potential threat
      - Most WIPS define rogue APs as devices that are actually plugged into the network backbone and are not known or managed by the organization
      - Most WIPS vendors use different terminology when classifying devices
- Mobile WIDS
  - Laptop versions of a WIDS
  - The software program is a protocol analyzer capable of decoding frames with some layer 1 analysis capabilities as well
  - Most 802.11 protocol analyzer software offers standalone mobile security and performance analysis tools
  - Think of a mobile WIDS as a single sensor, server, and console built into one unit
  - One useful feature of a mobile WIDS is that it can detect a rogue AP and client and then be used to track them down
- Spectrum analyzer
  - Is a frequency domain tool that can detect any RF signal in the frequency range that is being scanned.
  - A spectrum analyzer that monitors the 2.4 GHz ISM band will be able to detect both intentional jamming and unintentional jamming devices.
  - 2 forms of spectrum analysis systems are available
    - mobile
    - distributed

Wireless security policy

- General security policy
  - When establishing a wireless security policy, you must first define a general policy
  - A general wireless security policy defines the following items
    - Statement of Authority
      - Defines who put the wireless policy in place and the executive management that backs the policy.
    - Applicable Audience
      - Audience to whom the policy applies, such as employees, visitors, and contractors.
    - Violation Reporting Procedures
      - Define how the wireless security policy will be enforced, including what actions should be taken and who is in charge of enforcement
    - Risk Assessment and Threat Analysis
      - Defines the potential wireless security risks and threats and what the financial impact will be on the company if a successful attack occurs.
    - Security Auditing
      - Internal auditing procedures, as well as the need for independent outside audits, should also be

defined.

- Functional security policy
    - Define the technical aspects of wireless security
    - Establishes how to secure the wireless network in terms of what solutions and actions are needed
    - A functional wireless security policy will define the following items:
    - Policy Essentials
        - Basic security procedures, such as password policies, training, and proper usage of the wireless network, are policy essentials and should be defined
    - Baseline Practices
        - Define minimum wireless security practices such as configuration checklists, staging and testing procedures, etc.
    - Design and Implementation
        - The actual authentication, encryption, and segmentation solutions that are to be put in place are defined
    - Monitoring and Response
        - All wireless intrusion detection procedures and the appropriate response to alarms are defined.
- Legislative compliance
    - In most countries, there are mandated regulations on how to protect and secure data communications within all government agencies
    - In the United States, NIST maintains the Federal Information Processing Standards (FIPS).
    - In the United States, other legislation exists for protecting information and communications in certain industries. These include the following:
        - HIPAA
            - The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards for electronic healthcare transactions and national standards for providers, health insurance plans, and employers
        - Sarbanes-Oxley
            - Defines stringent controls on corporate accounting and auditing procedures with a goal of corporate responsibility and enhanced financial disclosure.
        - GLBA
            - The Gramm-Leach-Bliley Act (GLBA) requires banks and financial institutions to notify customers of policies and practices disclosing customer information
- PCI compliance
    - The Payment Card Industry (PCI) realizes that in order to sustain continued business growth, measures must be taken to protect customer data and card numbers.
    - The PCI Security Standards Council (SSC) has implemented regulations for organizations processing and storing cardholder information.
    - commonly referred to as the PCI Standard.
    - Within this standard are components governing the use of wireless devices
    - 802.11 wireless policy recommendations
        - Although a detailed and thorough policy document should be created, it is highly recommend these six wireless security policies:
            - BYOD Policy
                - Each employer needs to define a bring your own device (BYOD) policy that clearly states how personal devices will be on boarded onto the secure corporate WLAN
                - The policy should also state how the personal devices can be used while connected to the company WLAN and which corporate network resources are accessible
            - Remote-Access WLAN Policy
                - End users take their laptops and handheld devices off site and away from company grounds
                - This policy should include the required use of an IPsec or SSL VPN solution to provide device authentication, user authentication, and strong encryption of all wireless data traffic
            - Rogue AP Policy
                - No end users should ever be permitted to install their own wireless devices on the corporate network
                - This policy should be strictly enforced.
            - Ad Hoc Policy
                - End users should not be permitted to set up ad hoc or peer-to-peer networks.
            - Wireless LAN Proper Use Policy
                - This policy should include proper installation procedures, proper security

implementations, and allowed application use on the wireless LAN

- IDS Policy
  - Policies should be written defining how to properly respond to alerts generated by the wireless intrusion detection system

Radio Frequency Site Survey Fundamentals

Monday, May 11, 2020 02:20 PM

WLAN site survey interview

- Customer briefing
  - If a wireless network is being planned for your company or for a prospective client, it is highly recommended that you sit management down, give them an overview of 802.11 wireless networking, and talk with them about how and why site surveys are conducted
  - Do not need to explain the inner workings of orthogonal frequency division multiplexing or the Distributed Coordination Function; however, a conversation about the advantages of Wi-Fi, as well as the limitations of a WLAN, is a good idea.
  - Chances are that a wireless network is already being considered because the company's end users have requested wireless access to the company network using their own personal devices such as smartphones and tablets
  - Just as important is a discussion about the bandwidth and throughput capabilities of 802.11a/b/g/n/ac technology.
  - It should also be explained that the medium is a half-duplex shared medium and not full-duplex.
  - Another appropriate discussion is why a site survey is needed.
  - A very brief explanation on how RF signals propagate and attenuate will provide management with a better understanding of why an RF site survey is needed to ensure the proper coverage and enhance performance.
  - If management is properly briefed on the basics of Wi-Fi as well as the importance of a site survey, the forthcoming technical questions will be answered in a more suitable fashion
- Business requirements
  - What is the purpose of the WLAN?
  - If you have a complete understanding of the intended use of a wireless network, the result will be a better-designed WLAN
  - VoWiFi network has very different requirements than a heavily used data network
  - Here are some of the business requirement questions that should be asked:
  - What applications will be used over the WLAN?
    - This question could have both capacity and quality of service (QoS) implications
  - Who will be using the WLAN?
    - Different types of users have different capacity and performance needs.
    - Users may also need to be separated for organizational purposes.
    - This is also an important consideration for security roles.
  - What types of devices will be connecting to the WLAN?
    - Will employees be allowed to connect their personal devices to the network?
    - Does the company have a bring your own device (BYOD) strategy and is a mobile device management (MDM) solution needed?
    - The capabilities of the devices may also force decisions in security, frequency, technology, and data rates.
- Capacity and coverage requirements
  - After the purpose of the WLAN has been clearly defined, the next step is to begin asking all the necessary questions for planning the site survey and designing the wireless network.
  - You will need to sit down with a copy of the building's floor plan and ask the customer where they want RF coverage
  - Do they really need coverage everywhere? Do laptop data users need access in a storage area? Do they need connectivity in the outdoor courtyard? Do handheld bar code scanners used in a warehouse area need access in the front office?
  - If you can determine that certain areas of the facility do not require coverage, you will save the customer money and yourself time when conducting the physical survey

- Depending on the layout and the materials used inside the building, some preplanning might need to be done as to what type of antennas to use in certain areas of the facility
- When the survey is performed, this will be confirmed or adjusted accordingly.
- You must not just consider coverage; you must also plan for capacity
- The following are among the many factors that need to be considered when planning for capacity:
- Data Applications
  - The applications that are used will have a direct impact on the number of Wi-Fi devices that should be communicating on average through an access point.
  - What is a good average number of connected devices per access point?
  - it depends entirely on the purpose of the WLAN and the applications being used
  - 35 to 50 active Wi-Fi devices per radio on a dual-frequency 802.11n access point is realistic with average application use, such as web browsing.
- User and Device Density
  - Three important questions need to be asked with regard to users.
    - How many users currently need wireless access and how many Wi-Fi devices will they be using?
    - How many users and devices may need wireless access in the future?
      - These first two questions will help you to begin adequately planning for a good ratio of devices per access point while allowing for future growth
    - The third question of great significance is, Where are the users?
  - Sit down with network management and indicate on the floor plan of the building any areas of high user density.
  - Plan to conduct the physical survey when the users are present and not during off-hours. A high concentration of human bodies can attenuate the RF signal because of absorption
- Peak On/Off Use
  - Be sure to ask what the peak times are—that is, when access to the WLAN is heaviest
  - Certain applications might be heavily accessed through the WLAN at specified times. Another peak period could be when one shift leaves and another arrives.
- Existing Transmitters
  - Does not refer just to previously installed 802.11 networks
  - Rather, it refers to interfering devices such as microwaves, cordless headsets, cordless phones, wireless machinery, and so on
  - If you don’t know that the employees are using 2.4 GHz cordless headsets or Bluetooth keyboards and mice, you may be designing a network destined for failure
- Portability vs. Mobility
  - There are two types of mobility
    - First is related to being portable and the other is true mobility
  - Portable think moving laptop from desk to meeting room and back, you don’t need access whilst in transit.
  - True mobility means that a user remains connected 100 percent of the time while traveling through the facility
  - Most users now carry some sort of personal mobile device, such as a smartphone; therefore, true mobility is almost always an understood requirement
  - Determining which type of connectivity is necessary can be key for not only troubleshooting an existing network but also for designing a new one.
- Backward Compatibility for Legacy Devices
  - It should be understood in advance that if there is any requirement for backward compatibility with legacy clients, the 802.11 protection mechanisms will always adversely affect throughput
  - Enterprise deployments will almost always require some level of backward compatibility to provide access for older 802.11a/b/g radios found in handhelds, VoWiFi phones, or older laptops

- Existing wireless network
    - Quite often the reason you are conducting a WLAN site survey is that you have been called in as a consultant to fix an existing deployment
    - Sadly, many untrained integrators or customers just install the access points wherever they can mount them and leave the default power and channel settings on every AP.
    - Usually, site surveys must be conducted either because of performance problems or difficulty roaming
    - Performance problems are often caused by RF interference, low SNR, adjacent cell interference, or cochannel cooperation
    - Roaming problems may also be interference related or caused by a lack of adequate coverage and/or by a lack of proper duplicate cell coverage for roaming
    - Here are some of the questions that should be asked prior to the reparative site survey:
    - What are the current problems with the existing WLAN?
        - Ask the customer to clarify the problems.
        - Are they throughput related?
        - Are there frequent disconnects?
        - Is there any difficulty roaming?
        - In what part of the building do the problems occur most often?
        - Is the problem happening with one WLAN device or multiple devices?
        - How often do the problems occur, and have any steps been taken to duplicate the troubles?
    - Are there any known sources of RF interference?
        - More than likely the customer will have no idea, but it does not hurt to ask.
        - Are there any microwave ovens? Do people use cordless phones or headsets? Does anyone use Bluetooth for keyboards or mice?
        - After asking these interference questions, you should always perform a spectrum analysis
    - Are there any known coverage dead zones?
        - This is related to the roaming questions, and areas probably exist where proper coverage is not being provided
    - Does prior site survey data exist?
        - Chances are that an original site survey was not even conducted. However, if old site survey documentation exists, it may be helpful when troubleshooting existing problems
        - Unless quantifiable data was collected that shows dBm strengths, the survey report should be viewed with extreme caution
    - What equipment is currently installed?
        - Ask what type of equipment is being used, such as 802.11a (5 GHz) or 802.11b/g (2.4 GHz), and which vendor has been used
        - Is the customer looking to upgrade to an 802.11n or 802.11ac network?
        - check the configurations of the devices, including service set identifiers (SSIDs), WEP or WPA keys, channels, power levels, and firmware versions.
    - Depending on the level of troubleshooting that is required on the existing wireless network, a second site survey consisting of coverage and spectrum analysis will often be necessary.
    - Adjustments to the existing WLAN equipment typically are adequate. However, the worst-case scenario would involve a complete redesign of the WLAN
    - If wireless usage requirements have changed, a redesign might be the best course of action.
- Infrastructure connectivity
    - Asking for a copy of the wired network topology map is highly recommended.
    - For security reasons, the customer may not want to disclose the wired topology, and you may need to sign a nondisclosure agreement
    - Understanding the existing topology will also be of help when planning WLAN segmentation and security proposals and recommendations
    - With or without a topology map, the following topics are important to ensure the desired infrastructure connectivity:

- Roaming
  - Is roaming required?
  - Any devices that run connection-oriented applications will need seamless roaming
  - Seamless roaming is mandatory if handheld devices and/or VoWiFi phones are deployed
  - With the advent of smartphones and tablets, most end users expect mobility. Providing for secure seamless roaming is pretty much an afterthought.
  - It should also be understood that there might be certain areas where the WLAN was designed so that roaming is a very low priority, such as areas with a high density of users
  - This is a WLAN design with high density as the priority, as opposed to mobility and roaming whether users will need to roam across layer 3 boundaries.
  - A Mobile IP solution or a proprietary layer 3 roaming solution will be needed if client stations need to roam across subnets
  - With regard to the existing network, it is imperative that you determine whether the wired network infrastructure will support all the new wireless features.
- Wiring Closets
  - Where are the wiring closets located?
  - Will the locations that are being considered for AP installation be within a 100-meter (328-foot) cable drop from the wiring closets?
- Antenna Structure
  - If an outdoor network or point-to-point bridging application is requested, some additional structure might have to be built to mount the antennas
  - Asking for building diagrams of the roof to locate structural beams and existing roof penetrations is a good idea.
  - Depending on the weight of the installation, you may also need to consult a structural engineer.
- Switches
  - Will the access points be connected by category 5 (CAT5) cabling to unmanaged switches or managed switches?
  - CAT5e or higher grade cabling is usually needed to maximize 802.3af PoE.
  - An unmanaged switch will only support a single VLAN.
  - Are there enough switch ports?
  - What is the power budget of the switch?
  - Who will be responsible for configuring the VLANs?
- PoE
  - How will the access points be powered?
  - Very often the customer will not yet have a PoE solution in place, and further investment will be needed.
  - the customer already does have a PoE solution installed, it must be determined whether the PoE solution is compliant with 802.3af or 802.3at (PoE Plus).
  - it is important to make sure that it is compatible with the system you are proposing to install.
  - If PoE injectors need to be installed, you will need to make sure there are sufficient power outlets.
- Segmentation
  - How will the WLAN and/or users of the WLAN be segmented from the wired network?
  - Will the entire wireless network be on a separate IP subnet tied to unique
  - Will firewalls or VPNs be used for segmentation? VLANs?
  - Or will the wireless network be a natural extension to the wired
  - network and follow the same wiring, VLAN numbering, and design schemes as the wired infrastructure?
- Naming Convention
  - Does the customer already have a naming convention for cabling and network infrastructure equipment, and will one need to be created for the WLAN?
- User Management

        - Considerations regarding RBAC, bandwidth throttling, and load balancing should be discussed
        - Do they have an existing RADIUS server or does one need to be installed?
        - What type of LDAP user database is being used?
        - Where will usernames and passwords be stored?
        - Will usernames and passwords be used for authentication, or will they be using client certificates?
        - Will guest user access be provided?
    - Device Management
        - Will employees be allowed to access the WLAN with their own personal devices?
        - How will personal and company-issued mobile devices be managed?
        - Do they want to provide different levels of access based upon device type
    - Infrastructure Management
        - How will the WLAN remote access points be managed?
        - Is a central management solution a requirement?
        - Will devices be managed using SSH2, SNMP, or HTTP/HTTPS?
        - Do they have standard credentials that they would like to use to access these management interfaces?
- Security expectations
    - All data privacy and encryption needs should be discussed
    - All AAA requirements must be documented
    - It should be determined whether the customer plans to implement a wireless intrusion detection or prevention system (WIDS or WIPS) for protection against rogue APs and the many other types of wireless attacks.
    - A comprehensive interview regarding security expectations will provide the necessary information to make competent security recommendations after the site survey has been conducted and prior to deployment
    - Industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, and Payment Card Industry (PCI) may have to be taken into account when making security recommendations
    - All of these answers should also assist in determining whether the necessary hardware and software exists to perform these functions
- Guest access
    - Most companies offer some sort of wireless guest access to the Internet.
    - Guest users access the WLAN via the same access points.
    - However, they usually connect via a guest SSID that redirects the guest users to a captive portal.
    - The guest captive portal serves two purposes:
        - The login screen forces guest users to accept the corporate legal disclaimer.
        - After logging in, the guest users are provided with a gateway to the Internet.
    - It should be noted that all users who connect with the guest SSID should be allowed to go only to the Internet gateway and should be properly segmented from all other network
    - Resources in a separate guest VLAN
    - Firewall restrictions and bandwidth throttling are also common when deploying guest WLANs

Documentation and reports

- Forms and customer documentation
- Before the site survey interview, you must obtain some critical documentation from the customer:
- Blueprints
    - You need a floor plan layout in order to discuss coverage and capacity needs with network administration personnel
    - Some software survey tools allow you to import floor plans, and the software will record the survey results on the floor plan for you
    - These are highly recommended and make the final report much easier to compile
    - What to do if no blueprints:

        - The original architect of the building will probably still have a copy of the blueprints.
        - Many public and private buildings' floor plans might also be located at a public government resource such as city hall or the fi re department.
        - Businesses are usually required to post a fire escape plan
- Topographic Map
    - If an outdoor site survey is planned, a topographic map, also called a contour map, will be needed
    - Contour maps display terrain information, such as elevations, forest cover, and the locations of streams and other bodies of water
    - topographic map will be a necessity when performing bridging calculations, such as Fresnel zone clearance.
- Network Topology Map
    - Understanding the layout of the customer's current wired network infrastructure will speed up the site survey process and allow for better planning of the WLAN during the design phase
    - Acquiring a network topology map from the customer is a highly recommended practice that will result in a well-designed and properly integrated WLAN
- Security Credentials
    - You might need proper security authorization to access facilities when conducting the site survey
    - A meeting with security personnel and/or the facilities manager in advance of the survey will be necessary in order to meet all physical security requirements
    - Regardless of the security requirements, it is always a good idea to have the network administrator alert everyone that you will be in the area.
- Interview Checklist
    - A detailed checklist containing all the questions to be asked during the site survey interview should be created in advance
- Installation Checklist
    - Many site survey professionals prefer to record all installation details on the floor plan documents
    - An installation checklist detailing hardware placement and mounting for each individual access point is also an option.
    - Information about AP location, antenna type, antenna orientation, mounting devices, and power sources may be logged
- Equipment Checklist
    - A checklist of all the hardware and software tools used during the survey might also be a good idea
- Deliverables
    - After the interview process has been completed and the survey has been conducted, a final report must be delivered to the customer
    - Compiled information contained in the deliverables will include the following:
    - Purpose Statement
        - The final report should begin with a WLAN purpose statement that stipulates the customer requirements and business justification for the WLAN.
    - Spectrum Analysis
        - Be sure to identify potential sources of interference
    - RF Coverage Analysis
        - Define RF cell boundaries
    - Hardware Placement and Configuration
        - Recommend AP placement, antenna orientation, channel reuse pattern, power settings, and any other AP-specific information such as installation techniques and cable routing
    - Capacity and Performance Analysis
        - Include results from application throughput testing, which is sometimes an optional analysis report included with the final survey report
- Additional reports

- Along with the survey report, other recommendations will be made to the customer so that appropriate equipment and security are deployed
- The person conducting the survey might not be doing the installation
- Regardless of who handles the installation work, other recommendations and reports will be provided along with the site survey report:
  - Vendor Recommendations
    - It is a highly recommended practice to conduct the site survey using equipment from the same vendor who will supply the equipment that will later be deployed on site
    - The mere fact that every vendor's radios use proprietary RSSI thresholds is reason enough to stick with the same vendor during surveying and installation.
    - It is not unheard of for a survey company to conduct two surveys with equipment from two different vendors and present the customer with two separate options.
    - However, the interview process will usually determine in advance the vendor recommendations that will be made to the customer.
  - Implementation Diagrams
    - The implementation diagram is basically a wireless topology map that illustrates where the access points will be installed and how the wireless network will be integrated into the existing wired infrastructure.
    - AP placement, VLANs, and layer 3 boundaries will all be clearly defined.
  - Bill of Materials
    - Itemizes every hardware and software component necessary for the final installation of the wireless network
    - The model number and quantity of each piece of equipment will be necessary
  - Project Schedule and Costs
    - Outlines all timelines, equipment costs, and labor costs
    - Particular attention should be paid to the schedule dependencies, such as delivery times and licensing, if applicable.
  - Security Solution Recommendations
    - Comprehensive wireless security recommendations
    - All aspects of authentication, authorization, accounting, encryption, and segmentation should be included in the security recommendations documentation
  - Wireless Policy Recommendations
    - An addendum to the security recommendations might be corporate wireless policy recommendations
  - Training Recommendations
    - One of the most overlooked areas
    - It is highly recommended that wireless administration and security training sessions be scheduled with the customer's network personnel

Vertical market considerations

- Outdoor surveys
  - Calculations necessary for outdoor bridging surveys are numerous, including the Fresnel zone, earth bulge, free space path loss, link budget, and fade margin.
  - outdoor site surveys for the purpose of providing general outdoor wireless access for users are becoming more commonplace
  - Outdoor site survey kits using outdoor mesh APs will be needed.
  - Weather conditions, such as lightning, snow and ice, heat, and wind, must also be contemplated
  - Unless the hardware is designed for outdoor use, the outdoor equipment must ultimately be protected from the weather elements by using NEMA-rated enclosure units (NEMA stands for National Electrical Manufacturers Association)
  - Safety is also a big concern for outdoor deployments. Consideration should be given to hiring professional installers.

    - All RF power regulations, as defined by the regulatory body of your country, will need to be considered
    - If towers are to be used, you may have to contact several government agencies
    - you must contact the proper RF regulatory authority and aviation authority to find out the details
- Aesthetics
    - An important aspect of the installation of wireless equipment is the “pretty factor.”
    - Many businesses prefer that all wireless hardware remain completely out of sight.
    - Extremely important in retail environments and in the hospitality industry
    - WLAN vendors continue to design more aesthetic-looking access points and antennas
- Government
    - The key concern during government wireless site surveys is security.
    - Be sure to check export restrictions before traveling to other countries with certain equipment.
    - Obtaining the proper security credentials will most likely be a requirement before conducting the government survey
    - An identification badge or pass often is required.
    - In some government facilities, an escort is needed in certain sensitive areas
- Education
    - As with government facilities, obtaining the proper security credentials in an education environment usually is necessary.
    - Properly securing access points in lockable enclosure units is also necessary to prevent theft or tampering user density should be accounted for during capacity and coverage planning.
    - In campus environments, wireless access is required in most buildings, and very often bridging solutions are needed between buildings across the campus
    - Most school buildings use dense wall materials such as cinderblock or brick to attenuate the sound between classrooms. These materials also heavily attenuate RF signals.
- Healthcare
    - One of the biggest concerns in a healthcare environment is sources of interference from the biomedical equipment that exists on site.
    - A thorough spectrum analysis survey using a spectrum analyzer is extremely important.
    - Hospitals are usually large in scale, and a site survey may take many weeks; a predictive site survey can save a lot of time.
    - The applications used in the medical environment should all be considered during the interview and the survey.
    - VoWiFi phone deployments are commonplace in hospitals because of the communication mobility that they provide to nurses
    - Wi-Fi real-time location systems (RTLSs) using active 802.11 RFID tags are commonplace in hospitals for asset management tracking
    - Because of the presence of medical patients, proper security credentials and/or an escort will often be necessary
    - Many applications are connection oriented, and drops in connectivity can be detrimental to the operation of these applications
- Hotspots
    - Security solutions at hotspots are usually limited to a captive portal solution for user authentication against a customer database.
- Retail
    - A retail environment often has many potential sources of 2.4 GHz interference.
    - The inventory storage racks and bins and the inventory itself are all potential sources of multipath problems
    - Heavy user density should also be considered, and a retail site survey should be done in the height of the shopping season as opposed to the offseason when the malls are empty.
    - Wireless applications that are used in retail stores include handheld scanners used for data collection and inventory control
    - Coverage is usually a greater concern than capacity because wireless data-collection

devices require very little bandwidth, and the number used in a particular area is typically limited.

- Warehouses
    - 2.4 GHz WLAN will likely be deployed because most handheld devices currently use 2.4 GHz radios.
    - Coverage, not capacity, is usually the main objective when designing a wireless network in a warehouse
    - Warehouses are filled with metal racks and all sorts of inventory that can cause reflections and multipath
    - High ceilings often cause mounting problems as well as coverage issues
    - Indoor chain-link fences that are often used to secure certain areas will scatter and block a 2.4 GHz RF signal
    - Seamless roaming is also mandatory
    - Handheld WLAN barcode scanners are now often being replaced with smart phones that use barcode scanning applications.
- Manufacturing
    - Often similar to a warehouse environment in terms of multipath interference and coverage design.
    - A manufacturing plant presents many unique site survey challenges, including safety and the presence of employee unions
    - Heavy machinery and robotics may present safety concerns to the surveyor, and special care should be taken so as not to mount access points where they might be damaged by other machines.
    - Proper protection gear may need to be worn, and ruggedized access points or enclosures may have to be installed
    - Many manufacturing plants are union shops with union employees. A meeting with the plant's union representative may be necessary to make sure that no union policies will be violated by the site surveyor team.
- Multitenant buildings
    - The biggest issue when conducting a survey in a multitenant building is the presence of other WLAN equipment used by nearby businesses
    - Almost assuredly all of the other tenants' WLANs will be powered to full strength, and some equipment will be on nonstandard channels such as 2 and 8, which will likely interfere with your WLAN equipment
    - If at all possible, strong consideration should be given to deploying a WLAN using the 5 GHz U-NII bands.

Site Survey Systems and Devices

Thursday, May 14, 2020 09:21 PM

Site survey defined

- Protocol and spectrum analysis
  - A spectrum analyzer will help identify whether there is any type of RF interference from 802.11 devices or other devices that could interfere with your WLAN
  - Wi-Fi-based protocol analyzers can examine 802.11 frames and identify SSID and BSSID information along with packet and security information.
  - Some Wi-Fi protocol analyzers are specifically designed for performing site surveys.
- Standalone
  - Wi-Fi cards and spectrum analyzer cards go about seeing the RF world in slightly different ways
  - The Wi-Fi card can see frames and modulated bits going across the RF medium. Protocol analyzers take the data received by the Wi-Fi cards and provide packet analysis of that data
  - Spectrum analyzers monitor the RF signal itself.
  - Because the Wi-Fi receiver and the spectrum analyzer receiver are separate devices that monitor different pieces of information, historically they have been standalone devices, each performing a dedicated task.
- Integrated
  - By correlating the raw RF with the data from the Wi-Fi card, you can better understand the effects of various scenarios on your wireless network
  - Look to spectrum and protocol analyzer vendors to be adding more integration between both the spectrum analysis cards and Wi-Fi cards
- Spectrum analysis
  - are frequency domain measurement devices that can measure the amplitude and frequency space of electromagnetic signals
  - To conduct a proper 802.11 spectrum analysis survey, the spectrum analyzer needs to be capable of scanning both the 2.4 GHz ISM band and the 5 GHz U-NII bands
  - A true spectrum analyzer picks up RF energy regardless of the source.
  - If the background noise level exceeds –85 dBm in either the 2.4 GHz ISM band or the 5 GHz U-NII bands, the performance of the wireless network can be severely degraded
  - A noisy environment can cause the data in 802.11 transmissions to become corrupted
  - Interfering devices might also prevent an 802.11 radio from transmitting
  - It is a recommended practice to conduct spectrum analysis of all frequency ranges, especially in the 2.4 GHz ISM band
  - The following are potential sources of interference in the 2.4 GHz ISM band:
    - Microwave ovens
    - 2.4 GHz cordless phones, DSSS and FHSS
    - Fluorescent bulbs
    - 2.4 GHz video cameras
    - Elevator motors
    - Cauterizing devices
    - Plasma cutters
    - Bluetooth radios
    - Nearby 802.11, 802.11b, 802.11g, or 802.11n (2.4 GHz) WLANs
  - A common everyday interfering item that should be documented during the site survey interview is the location of any microwave ovens
  - Current potential sources of interference in 5 GHz U-NII bands include the following:
    - 5 GHz cordless phones
    - Radar
    - Perimeter sensors
    - Digital satellite

        - Nearby 5 GHz WLANs
        - Outdoor wireless 5 GHz bridges
    - The 802.11-2012 standard defines dynamic frequency selection (DFS) and transmit power control (TPC) mechanisms to satisfy regulatory requirements for operation in the 5 GHz band to avoid interference with 5 GHz radar systems
    - Using a 5 GHz spectrum analyzer during a site survey may help determine in advance whether radar transmissions exist in the area where the WLAN deployment is planned.
    - After locating the sources of interference, the best and simplest solution is to eliminate them entirely.
    - If interfering devices cannot be eradicated in the 2.4 GHz bands, consider moving to the less crowded 5 GHz U-NII bands.
    - If your WLAN is being used for either data or voice or for both, a proper and thorough spectrum analysis is mandatory in an enterprise environment.
- Coverage analysis
    - The next step is the all-important determination of proper 802.11 RF coverage inside your facility
    - During the site survey interview, capacity and coverage requirements are discussed and determined before the actual site survey is performed
    - In certain areas of your facility, smaller cells or co-location may be required because of a high density of users or heavy application bandwidth requirements
    - RF measurements must be taken to guarantee that these needs are met and to determine the proper placement and configuration of the access points and antennas.
    - Proper coverage analysis must be performed using some type of received signal strength measurement tool or planning tool
    - how do you conduct proper coverage analysis?
    - One mistake that many people make during the site survey is leaving the access point radio at the default full-power setting.
    - A good starting point for a 2.4 GHz access point is 25 mW transmit power.
    - The hardest part of physically performing a coverage analysis site survey is often finding where to place the first access point and determining the boundaries of the first RF cell.
    - It is important to avoid excessive overlap because it can cause frequent roaming and performance degradation.
    - The shape and size of the building and the attenuation caused by the various materials of walls and obstacles will require you to change the distances between access points to ensure proper cell overlap
    - WLAN design guides and white papers from various WLAN vendors often reference 15 percent to 30 percent coverage cell overlap for roaming purposes.
    - Coverage overlap is really duplicate coverage from the perspective of a Wi-Fi client station
    - A proper site survey should be conducted to make sure that a client always has proper duplicate coverage from multiple access points
    - The SNR is an important value because, if the background noise is too close to the received signal, data can be corrupted and retransmissions will increase
    - Many vendors recommend a minimum SNR of 18 dB for data networks and a minimum of 25 dB for voice networks.
- AP placement and configuration
    - Coverage analysis also determines the proper placement of access points and power settings.
    - When the site survey is conducted, all the cell edge measurements will be recorded and written on a copy of the floor plan of the building.
    - An entry with the exact location of each access point must also be recorded.
    - The location of all the wiring closets will also be noted on the floor plan, and care should be taken to ensure that the placement of any access point is within a 100-meter (328-foot) cable run back to the wiring closet because of copper Ethernet cabling distance limitations
    - A good site survey kit should have a variety of antennas, both omnidirectional and semi directional.

    - Do not be afraid to provide coverage in a building by using a combination of both low-gain omnidirectional antennas and indoor semi directional antennas
- Application analysis
    - With the proliferation of Wi-Fi networks along with the importance of these networks in the enterprise, capacity planning has become an integral part of the site survey process
    - This takes into account not only the user capacity but the bandwidth capacity as well.
    - Software tools exist that can perform application stress testing of a WLAN
    - Several companies offer 802.11a/b/g/n/ac multistation emulation hardware that can simulate multiple concurrent virtual wireless client stations
    - Roaming performance can also be tested.

Site survey tools

- Indoor site survey tools
    - Here are some of the tools that you might use for an indoor site survey:
        - Spectrum Analyzer
            - Is needed for frequency spectrum analysis.
        - Blueprints
            - Are needed to map coverage and mark RF measurements.
        - Signal Strength Measurement Software
            - For RF coverage analysis.
        - 802.11 Client Card
            - Used with the signal measurement software
        - Access Point
            - At least one AP is needed, preferably two
        - WLAN Controller
            - If autonomous access point is not available, controller will be required to manage the survey AP
        - Battery Pack
            - Necessity because the site survey engineer does not want to have to run electrical extension cords to power the access point while it is temporarily mounted for the site survey
        - Binoculars
            - Can be very useful in tall warehouses and convention center
        - Flashlight
            - A powerful, directional flashlight can come in handy in a dark corner or in a ceiling.
        - Walkie-Talkies or Mobile Phones
            - Walkie-talkies or cell phones are typically preferred over yelling across the room
        - Antennas
            - A variety of both indoor omnidirectional and indoor directional antennas historically has been common in indoor Wi-Fi site survey kits.
            - If the internal antennas do not meet your design needs, most enterprise AP vendors also have AP models that support external antennas.
        - Temporary Mounting Gear
            - you will be temporarily mounting the access point—often high up, just below the ceiling
        - Digital Camera
            - used to record the exact location of the access point placement.
        - Measuring Wheel or Laser Measuring Meter
            - A tool is needed to make sure the access point will in fact be close enough for a 100-meter cable run back to the wiring closet.
        - Colored Electrical Tape
            - The colored tape can be used to leave a trail back to where you want to mount the access points
        - Ladder or Forklift
            - Ladders and/or forklifts may be needed to temporarily mount the access point to the ceiling.

- Outdoor site survey tools
    - The following list includes some of the tools that you might use for an outdoor bridging site survey:
        - Topographic Map
            - A map that outlines elevations and positions will be needed.
        - Link Analysis Software
            - Point-to-point link analysis software can be used with topographic maps to generate a bridge link profile and also perform many of the necessary calculations, such as Fresnel zone and EIRP.
        - Calculators
            - Software calculators and spreadsheets can be used to provide necessary calculations for link budget, Fresnel zone, free space path loss, and fade margin.
            - Other calculators can provide information about cable attenuation and voltage standing wave ratio (VSWR).
        - Maximum Tree Growth Data
            - Trees are a potential source of obstruction of the Fresnel zone, and unless a tree is fully mature, it will likely grow taller
            - A chainsaw is not always the answer, and planning antenna height based on potential tree growth might be necessary.
        - Binoculars
            - Visual line of sight can be established with the aid of binoculars.
        - Walkie-Talkies or Cell Phones
            - 802.11 bridge links may span up to (or at times exceed) a mile. Two site survey engineers working as a team will need some type of device for communicating during the survey.
        - Signal Generator and Wattmeter
            - Also known as a Bird meter, to test cabling, connectors, and accessories for signal loss and VSWR
            - This testing gear can be used for testing cabling and connectors before deployment
        - Variable-Loss Attenuator
            - A variable-loss attenuator has a dial that enables you to adjust the amount of energy that is absorbed.
            - Used simulate different cable lengths or cable losses.
        - Inclinometer
            - Used to determine the height of obstructions.
            - Doing so is crucial when you need to ensure that a link path is clear of obstructions.
        - GPS
            - Recording the latitude and longitude of the transmit sites and any obstructions or points of interest along the path is important for planning
        - Digital Camera
            - Used to take pictures of outdoor mounting locations, cable paths, grounding locations, obstructions, and so on.
        - Spectrum Analyzer
            - Used to test ambient RF levels at transmit sites.
        - High-Power Spotlight or Sunlight Reflector
            - In the case of a wireless bridge, you will need to make sure you are surveying in the right direction. As the path gets farther away, the ability to identify a specific rooftop or tower becomes harder and harder.
            - Because light travels so well, it can be used to narrow in on the actual remote site and ensure that the survey is conducted in the right direction

Coverage analysis

- Manual
    - Used to find the cell boundaries.
    - 2 major types of manual coverage analysis surveys:

        - Passive
            - The radio collects RF measurements, including received signal strength (dBm), noise level (dBm), and signal-to-noise ratio (dB).
            - Although the client adapter is not associated to the access point during the survey, information is received from radio signals that exist at layer 1 and layer 2.
        - Active
            - The radio is associated to the access point and has layer 2 connectivity, allowing for low-level frame transmissions.
            - If layer 3 connectivity is also established, low-level data traffic such as Internet Control Message Protocol (ICMP) pings are sent in 802.11 data frame transmissions.
            - Layer 1 RF measurements can also be recorded during the active survey.
            - Most vendors recommend that both passive and active manual site surveys be conducted.
- Predictive
    - Applications that provide RF simulations and modelling design capabilities
    - Is accomplished using an application that creates visual models of RF coverage cells, bypassing the need for actually capturing RF measurements.
    - Predictive applications are an excellent tool to use with blueprints of buildings that have yet to be built.
- Dynamic RF
    - Radio resource management (RRM), where access points can dynamically change their configuration based on accumulated RF information gathered from the access points radios.
    - RRM can address isolated WLAN capacity needs by utilizing dynamic load balancing of clients between the access points
    - When implemented, RRM provides automatic cell sizing, automatic monitoring, troubleshooting, and optimization of the RF environment, which can best be described as a self-organizing wireless LAN
    - RRM cannot make up for a poorly planned network, but it can help adjust and adapt to periodic or isolated surges in network usage and demand.
- Wireless network validation
    - Immediately after a wireless network has been installed, it is important to audit or validate the installation
    - This validation allows you to verify the RF coverage and data rates that are being provided by the installed network; you can then compare the actual values with expected values from your network design plans.
    - A wireless network validation is typically performed by systematically walking through the building or coverage area of the wireless network and taking RF and network measurements.
    - These measurements are then documented on the floor plan or map.
    - This information should help you to identify where and why your problem exists.

Power over Ethernet (PoE)

Thursday, May 14, 2020 09:31 PM

- Nonstandard PoE
  - The initial PoE products were proprietary solutions created by individual companies that recognized the need for the technology
  - The IEEE process to create a PoE standard began in 1999; however, it would take about four years before the standard became a reality.
  - Proprietary PoE solutions often used different voltages, and mixing proprietary solutions could result in damaged equipment
- IEEE 802.3af
  - PoE amendment to the 802.3 standard
  - Defined how to provide PoE to 10BaseT (Ethernet), 100BaseT (Fast Ethernet), and 1000BaseT (Gigabit Ethernet) devices.
- IEEE Std 802.3-2005, Clause 33
  - 802.3af amendment was one of four amendments that were incorporated into this revised standard
- IEEE 802.3at-2009
  - The IEEE 802.3at amendment was ratifi ed in 2009. 802.3at is also known as PoE+ or PoE plus, since it extends the capabilities of PoE
  - Two of the main objectives of the 802.3at Task Group were to be able to provide more power to powered devices and to maintain backward compatibility with Clause 33 devices
  - As APs become faster and incorporate newer technologies, such as multiple input, multiple output (MIMO), they require more power to operate
  - The IEEE 802.3at amendment is able to provide up to 30 watts of power using two pairs of wires in an Ethernet cable
  - The 802.3at amendment defines PoE devices as either Type 1 or Type 2. Devices capable of supporting the higher power defined in the 802.3at amendment are defined as Type 2 devices, and devices not capable of supporting the higher power are defined as Type 1 devices
- IEEE Std 802.3-2012, Clause 33
  - The IEEE revised the 802.3 standard again and created IEEE Std 802.3-2012
- Overview
  - PoE standard defines two types of PoE devices which communicate with each other and provide the PoE infrastructure
    - powered devices (PDs)
    - power-sourcing equipment (PSE)
  - Powered device (PD)
    - Either requests or draws power from the power-sourcing equipment.
    - must be capable of accepting up to 57 volts from either the data lines or the unused pairs of the Ethernet cable
    - must also be able to accept power with either polarity from the power supply in what is known as mode A or mode B

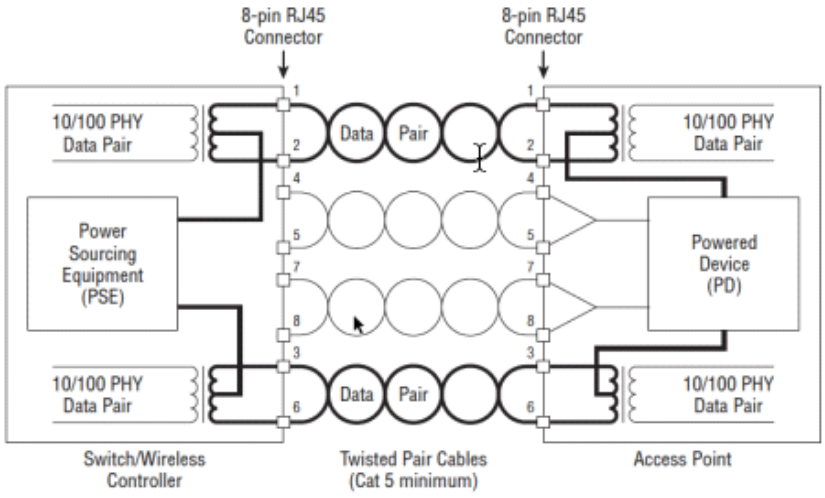
Conductor	**Mode A**	**Mode B**
1	Positive voltage, negative voltage	
2	Positive voltage, negative voltage	
3	Negative voltage, positive voltage	
4		Positive voltage, negative

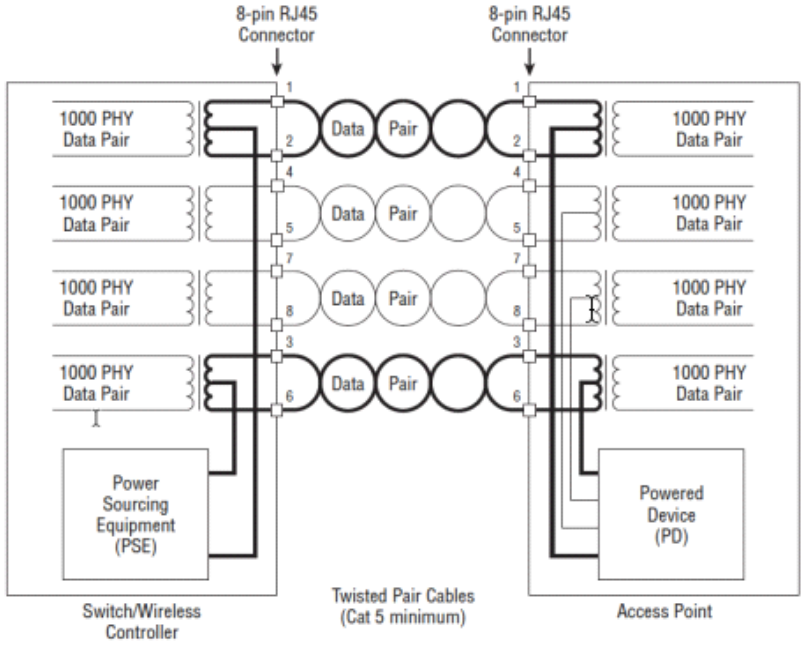
		voltage
5		Positive voltage, negative voltage
6	Negative voltage, positive voltage	
7		Negative voltage, positive voltage
8		Negative voltage, positive voltage

- The PD must reply to the power-sourcing equipment with a detection signature and notify the power-sourcing equipment whether it is in a state in which it will accept power or will not accept power.
- If the device is determined not to be compliant, power to the device will be withheld
- If the device is in a state in which it will accept power, the PD can optionally provide a classification signature
- Type 2 devices perform a two-event Physical layer classification or Data-Link layer classification, which allows a Type 2 PD to identify whether it is connected to a Type 1 or a Type 2 PSE
- If mutual identification cannot be completed, the device can only operate as a Type 1 device
- If the device is not identified, the PSE does not know how much power the device needs; therefore, it allocates the maximum power
- If the device is classified, the PSE has to allocate only the amount of power needed by the PD, thus providing better power management.
- Link Layer Discovery Protocol (LLDP) is a standards-based layer 2 neighbor discovery protocol that can also be used for more detailed power classification.
- The maximum power draw of an 802.3af-compliant device is 12.95 watts, and the maximum power draw of an 802.3at-compliant device is 25.5 watts.

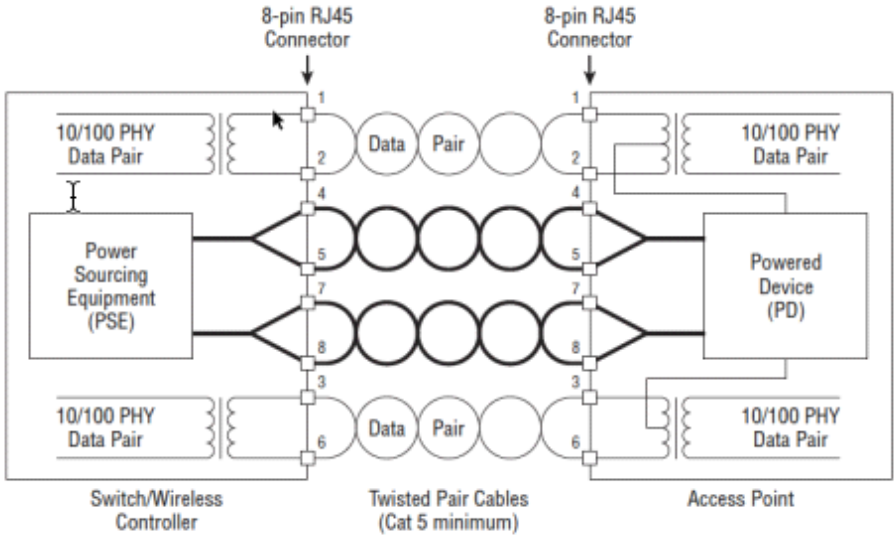
○ Power-sourcing equipment (PSE)
- Provides power to the PD.
- Searches for powered devices by using a direct current (DC) detection signal
- After a PoE-compliant device is identified, the PSE will provide power to that device
- The amount of power provided by the PSE is greater than what is used by the PD
  - This is because the PSE needs to account for the worst case scenario, in which there may be power loss due to the cables and connectors between the PSE and the PD.
- Once connected, the PSE continuously checks the connection status of the PD along with monitoring for other electrical conditions, such as short circuits
- When power is no longer required, the PSE will stop providing it
- Power-sourcing equipment is divided into two types of equipment endpoint and midspan.

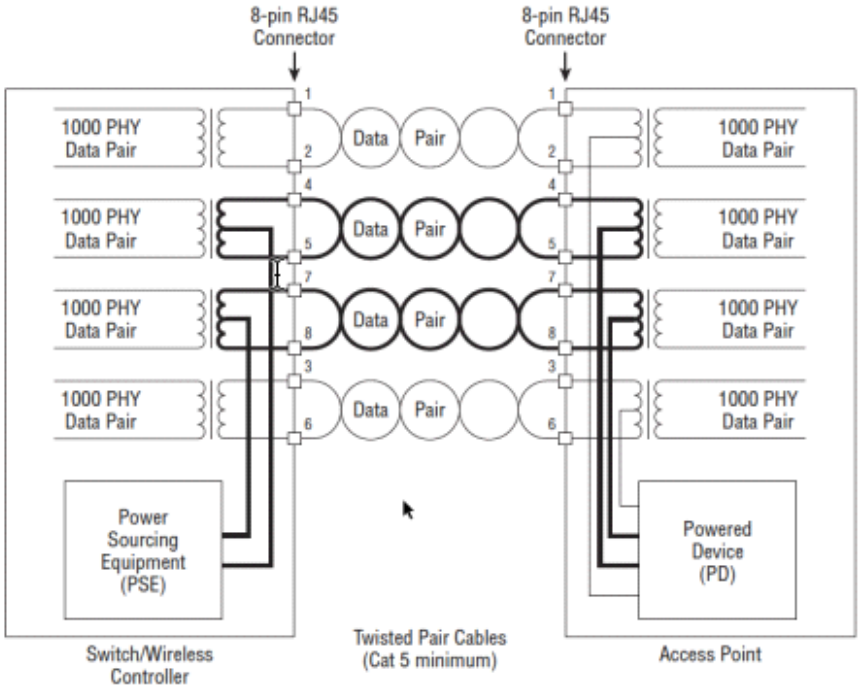
○ Endpoint PSE
- Provides power and Ethernet data signals from the same device
- Are typically PoE-enabled Ethernet switches
- The switches are typically access layer switches
- Some specialty devices, such as WLAN controllers may also function as endpoint PSE equipment
- Endpoint equipment can provide power using two methods
  - Alternative A
    - The PSE places power on the data pair





- Alternative B
  - Originally, Alternative B was designed to provide power on the spare unused pair of wires in a 10BaseT/100BaseTX cable,
  - A 1000BaseT endpoint PSE can also use Alternative B to provide power to a PD by placing the power on two of the data 1000BaseT data pairs
  - When 802.3af was initially ratified, 1000BaseT (Gigabit Ethernet) devices could receive PoE from only endpoint devices.





- Midspan PSE
  - Acts as a pass-through device, adding power to an Ethernet segment.
  - Enables you to provide PoE to existing networks without having to replace the existing Ethernet switches
  - midspan PSE is placed between an Ethernet source (such as an Ethernet switch) and a PD
  - acts as an Ethernet repeater while adding power to the Ethernet cable
  - Originally with 802.3af, midspan devices were only capable of using Alternative B—and only with 10BaseT and 100BaseTX PDs
  - With the ratification of 802.3at, midspan devices were able to use either Alternative A or Alternative B and they could provide support for 1000BaseT devices.
- Power-sourcing equipment pin assignments
  - The PSE must have a medium dependent interface (MDI) to carry the current to the powered device (PD).
  - MDI is essentially the technical term for the Ethernet cabling connector
  - There are two valid four-wire pin connections used to provide PoE
  - In each of these configurations, the two pairs of conductors carry the same nominal current in both magnitude and polarity
  - Many devices are capable of automatically identifying and providing the crossover connection if needed

- Planning & deploying PoE
  - Power planning
    - At maximum power for a PD, the PSE must be capable of providing 15.4 W or 30 W of power to each PoE device, depending on whether your devices require PoE+.
    - This does not include the amount of power necessary for the switch to perform its networking duties
    - A simple way of determining whether the power supply of the switch is powerful enough is to determine the size of the power supply for the equivalent non-PoE switch and add 15.4 watts for each PoE device that you will be connecting to the switch, or 30 watts for each PoE+ device you will be connecting to the switch.
    - Careful planning is needed to ensure that enough power is available for all the PDs.
    - When reading the power budget specifications of a switch, be sure to

determine how many ports are PoE-capable.
        - PoE ports can often also be configured with a priority level. Higher priority PoE ports take precedence for receiving power in the event that the PoE budget is exceeded
        - Proper planning of the PoE budget to ensure that the budget is never exceeded is best practice.
        - As the demand for PoE devices increases, the need to manage and troubleshoot PoE problems will also increase
        - The more PoE devices that you add to the network, the more you concentrate the power requirements in the data center or wiring closet
        - As your power needs increase, electrical circuits supplying power to the PoE switches might have to be increased
    - Redundancy
        - Even when there was an electrical failure, the telephone still worked and provided the ability to call someone
        - This is a level of service that we have come to expect.
        - As VoIP and VoWiFi telephones replace traditional telephone systems, it is important to still provide this same level of continuous service.
        - To achieve this, you should make sure that all of your PoE PSE equipment is connected to uninterruptible power sources
    - 802.11n or 802.11ac and PoE
        - When 802.3at not available The most common method was to downgrade the MIMO capability of the 802.11n access points so that 802.3af power could be used
        - The downside was that not all of the MIMO transmitter capabilities were being used by the APs.
        - The good news is that almost all of the current generation of 3×3:3 dual-frequency 802.11n APs are indeed capable of running with full transmitter capabilities using 802.3af PoE.
        - There is no reason you cannot use an available power outlet to provide electrical current to an AP. The downside is that most APs are deployed in areas where a power outlet is not conveniently accessible.
        - The best way to power 802.11n and 802.11ac APs is to deploy a PoE+ (802.3at) PSE that is capable of providing 30 watts via an Ethernet cable

802.11n

Thursday, May 14, 2020 09:40 PM

802.11n-2009 amendment

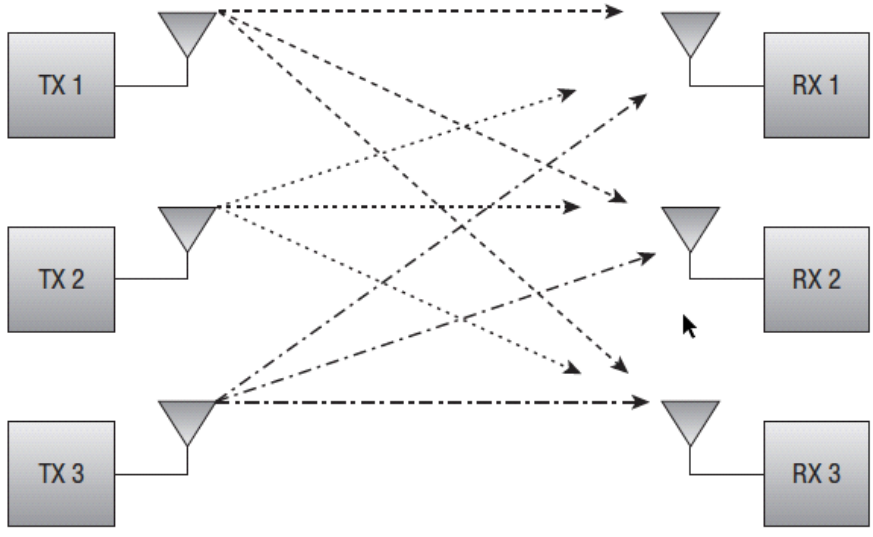
- Defines High Throughput (HT) Clause 20 radios that use multiple-input, multiple-output (MIMO) technology in unison with Orthogonal Frequency Division Multiplexing (OFDM) technology
- Benefits of using MIMO are increased throughput and even greater range
- 802.11n radios are backward compatible with legacy 802.11a/b/g radios
- A dual-frequency 802.11n Wi-Fi radio is usually referred to as an 802.11a/b/g/n radio. It should be noted that the technology defined for use by 802.11n radios is not frequency dependent

Wi-Fi Alliance certification

- 802.11n products are tested for both mandatory and optional baseline capabilities
- All certified products must also support both Wi-Fi Multimedia (WMM) quality of service (QoS) mechanisms and WPA/WPA2 security mechanisms
- Wi-Fi CERTIFIED n devices can operate in both the 2.4 GHz and 5 GHz frequency bands and are also backward compatible with 802.11a/b/g certified devices.

Multiple-Input, Multiple-Output (MIMO)

- Requires the use of multiple radios and antennas, called radio chains
- transmit multiple radio signals at the same time to take advantage of multipath.
- Multipath is a propagation phenomenon that results in two or more paths of the same signal arriving at a receiving antenna at the same time or within nanoseconds of each other.
- MIMO systems, however, take advantage of multipath and, believe it or not, multipath then becomes your friend.
- The MIMO receiver will then use advanced digital signal processing (DSP) techniques to sort out the originally transmitted signals.
- Transmitting multiple streams of data with a method called spatial multiplexing (SM) provides for greater throughput and takes advantage of the old enemy known as multipath.



- Radio chains
  - Conventional 802.11 radios transmit and receive RF signals by using a single-input single output (SISO) system
  - SISO systems use a single radio chain
  - A radio chain is defined as a single radio and all of its supporting architecture, including mixers, amplifiers, and analogue/ digital converters
  - A MIMO system consists of multiple radio chains, with each radio chain having its own antenna
  - A MIMO system is characterized by the number of transmitters and receivers used by

the multiple radio chains
    - or example, a 2Å~3 MIMO system would consist of three radio chains with two transmitters and three receivers. A 3Å~3 MIMO system would use three radio chains with three transmitters and three receivers
    - In a MIMO system, the first number always references the transmitters (TX), and the second number references the receivers (RX).
    - The use of multiple transmitters in a MIMO system provides for the transmission of more data via spatial multiplexing
    - The 802.11n standard allows for MIMO systems up to 4Å~4 using four radio chains
- Spatial multiplexing (SM)
    - A MIMO radio also has the ability to send independent unique data streams.
    - Each independent data stream is known as a spatial stream, and each unique stream can contain data that is different from the other streams transmitted by one or more of the other radio chains
    - The fact that the multiple streams follow different paths to the receiver because of the space between the transmitting antennas is known as spatial diversity
    - Sending multiple independent streams of unique data using spatial diversity is often also referred to as spatial multiplexing (SM) or spatial diversity multiplexing (SDM).
    - Do not confuse the independent unique streams of data with the number of transmitters.
    - In a MIMO system, the first number always references the transmitters (TX), and the second number references the receivers (RX). The third number represents how many unique streams of data can be sent or received.
    - For example, a 3X:2 MIMO system would use three transmitters and three receivers, but only two unique data streams are utilized.
    - not all 802.11n radios have the same MIMO capabilities
    - If good RF conditions exist, when a 3Å~3:3 access point and a 3X3:3 client device are communicating with each other, three spatial streams can be used for unicast transmissions.
    - However, when a 3X3:3 access point and a 2X2:2 client device are communicating with each other, only two spatial streams will be used for unicast transmissions
    - The 802.11n amendment does allow for the use of up to a 4X4:4 MIMO system
    - Multiple spatial streams can be sent with the same (equal) modulation or they can be sent using different (unequal) modulation
    - Although unequal modulation is theoretically and technically possible, WLAN vendors have never implemented unequal modulation with 802.11n radios
- MIMO diversity
    - MIMO systems employ advanced antenna diversity capabilities
    - Simple antenna diversity is a method of compensating for multipath as opposed to utilizing multipath.
    - When receive diversity is used, the signals may also be linearly combined by using a signal processing technique called maximal ratio combining (MRC).
    - MRC algorithms are used to combine multiple received signals by looking at each unique signal and optimally combining the signals in a method that is additive as opposed to destructive.
    - MIMO systems using MRC will effectively raise the SNR level of the received signal.
    - MRC uses a receive-combining function that assesses the phase and SNR of each incoming signal.
    - Each received signal is phase-shifted so that they can be combined.
    - The amplitude of the incoming signals is also modified to focus on the signal with the best SNR.
- Space-time block coding (STBC)
    - Is a method where the same information is transmitted on two or more antennas.
    - It is a type of transmit diversity.
    - can be used when the number of radio chains exceeds the number of spatial streams.
    - STBC does, however, increase the receiver's ability to detect signals at a lower SNR than would be otherwise possible

    - TBC and cyclic shift diversity (CSD) are transmit diversity techniques where the same transmit data is sent out of multiple antennas
    - STBC communication is possible only between 802.11n devices
- Cyclic shift diversity (CSD)
    - Is another transmit diversity technique specified in the 802.11n standard
    - CSD diversity signals can be received by either 802.11n or legacy devices.
    - For mixed mode deployments, where 802.11n coexists with 802.11g and 802.11a devices, there is a need to have a way of transmitting the symbols in the legacy OFDM preamble over multiple transmit antennas
    - The cyclic delay is chosen to be within the limits of the guard interval (GI) so that it does not cause excessive inter-symbol interference (ISI)
    - An 802.11n system has no problem using the multiple signals to improve the overall SNR of the preamble
- Transmit beamforming (TxBF)
    - The 802.11n amendment also proposes an optional PHY capability called transmit beamforming (TxBF), which uses phase adjustments.
    - Transmit beamforming can be used when there are more transmitting antennas than there are spatial data streams
    - Transmit beamforming is a method that allows a MIMO transmitter using multiple antennas to adjust the phase and amplitude of the outgoing transmissions in a coordinated method.
    - If the transmitter (TX) knows about the RF characteristic of the receiver's location, the phase of the multiple signals sent by a MIMO transmitter can be adjusted. When the multiple signals arrive at the receiver, they are in phase, resulting in constructive multipath instead of the destructive multipath caused by out-of-phase signals.
    - Transmit beamforming will also result in higher throughput because of the higher SNR that allows for the use of more complex modulation methods that can encode more data bits.
    - The higher SNR also results in fewer layer 2 retransmissions.
    - Transmit beamforming could be used together with spatial multiplexing (SM)
    - In practice, transmit beamforming will probably be used when spatial multiplexing is not the best option
    - Transmitters that use beamforming will try to adjust the phase of the signals based on feedback from the receiver by using sounding frames.
    - The transmitter is considered the beamformer, while the receiver is considered the beamformee
    - Transmit beamforming relies on implicit feedback or explicit feedback from both the transmitter and receiver
    - With some vendor-specific exceptions, 802.11n transmit beamforming has not been utilized due to the lack of client-side support for the technology
    - Even though transmit beamforming never really caught on with 802.11n radios, it is widely believed that 802.11ac will make use of the technology in the near future.

HT channels

- 20 MHz non-HT and HT channels
    - 802.11n (HT) radios also use the same OFDM technology and have the capability of using either 20 MHz channels or 40 MHz channels
- 40 MHz channels
    - 802.11n (HT) radios also have the capability of using 40 MHz OFDM channels
    - The 40 MHz HT channels use 128 OFDM subcarriers; 108 of the subcarriers transmit data, whereas 6 of the subcarriers are used as pilot tones for dynamic calibration between the transmitter and receiver.
    - The 40 MHz channels used by HT radios are essentially two 20 MHz OFDM channels that are bonded together
    - Deploying 40 MHz HT channels at 2.4 GHz unfortunately does not scale well in multiple channel architecture.
- 40 MHz Intolerant
    - Any 802.11n AP using a 40 MHz channel will be forced to switch back to using only 20

MHz channels if they receive the frames from nearby 802.11n 2.4 GHz stations that are intolerant.

- Guard interval (GI)
  - Data is modulated onto the carrier signal in bits or collections of bits called symbols
  - 802.11a/g radios use an 800-nanosecond guard interval (GI) between OFDM symbols.
  - In a multipath environment, symbols travel different paths, and therefore some symbols arrive later. A “new” symbol may arrive at a receiver before a “late” symbol has been completely received. This is known as inter-symbol interference (ISI) and often results in data corruption.
  - 802.11n also uses an 800-nanosecond guard interval; however, a shorter 400-nanosecond guard interval is optional. A shorter guard interval results in a shorter symbol time, which has the effect of increasing data rates by about 10 percent.
- Modulation and coding scheme (MCS)
- HT PHY
  - The 802.11n amendment defines the use of three PPDU structures that use three different preambles. One of the preambles is a legacy format, and two are newly defined HT preamble formats.
- Non-HT legacy
  - Often also referred to as a legacy format because it was originally defined by Clause 18 of the 802.11-2012 standard for OFDM transmissions.
  - The header contains the signal field, which indicates the time needed to transmit the payload of the non-HT PPDU, which of course is the MPDU (802.11 frame).
  - Support for the non-HT legacy format is mandatory for 802.11n radios, and transmissions can occur in only 20 MHz channels
  - The non-HT format effectively is the same format used by legacy 802.11a and 802.11g radios
- HT Mixed
  - PPDU formats defined in the 802.11n amendment is the HT Mixed format.
  - the beginning of the preamble contains the non-HT training symbols and legacy signal field that can be decoded by legacy 802.11a and 802.11g radios.
  - The rest of the HT Mixed preamble and header cannot be decoded by legacy 802.11a/g devices
  - The HT Signal (HT-SIG) contains information about the MCS, frame length, 20 MHz or 40 MHz channel size, frame aggregation, guard interval, and STBC. The HT Short
  - Training Field (HT-STF) and HT Long Training Field (HT-LTF) are used for synchronization between MIMO radios
- HT Greenfield
  - An 802.11n radio in HT Greenfield mode can receive frames from legacy devices; however, legacy devices cannot understand the HT Greenfield preamble.
  - Therefore, any legacy device will interpret an HT Greenfield transmission as noise.

HT MAC

- A-MSDU
  - Every time a unicast 802.11 frame is transmitted, a certain amount of fixed overhead exists as a result of the PHY header, MAC header, MAC trailer, Interframe spacing, and acknowledgment frame.
  - Medium contention overhead also exists because of the time required when each frame must contend for the medium.
  - Frame aggregation is a method of combining multiple frames into a single frame transmission.
  - The fixed MAC layer overhead is reduced, and overhead caused by the random backoff timer during medium contention is also minimized.
- A-MPDU
  - Aggregate MAC Protocol Data Unit (A-MPDU).
- Block Acknowledgment
  - An A-MSDU contains multiple MSDUs all wrapped in a single frame with one MAC header and one destination.
  - Block ACKs were first introduced by the 802.11e amendment as a method of

acknowledging multiple individual 802.11 frames during a frame burst

- RIFS
  - 802.11e QoS amendment introduced the capability for a transmitting radio to send a burst of frames during a transmit opportunity (TXOP).
  - The 802.11n amendment defines a new Interframe space that is even shorter in time, called a reduced Interframe space (RIFS)
  - A RIFS interval can be used in place of a SIFS interval, resulting is less overhead during a frame burst.
  - It should be noted that RIFS intervals can be used only when a Greenfield HT network is in place.
- HT power management
  - The 802.11e QoS amendment introduced unscheduled automatic power save delivery (U-APSD), which is the mechanism used by WMM Power Save (WMM-PS).
  - The 802.11n power-management mechanisms are meant as supplements to WMM-PS when MIMO radios are used.
  - spatial multiplexing power save (SM power save). The purpose of SM power save is to allow a MIMO 802.11n device to power down all but one of its radios
  - Power Save Multi Poll (PSMP), has also been defined for use by 802.11n (HT) radios. PSMP is an extension of automatic power save delivery (APSD) that was defined by the 802.11e amendment

HT operation

- 20/40 channel operation
  - 802.11n radios can operate in either a 20 MHz–only channel mode or a 20/40 MHz channel operation mode
  - The HT radios that are 20/40 capable can use 40 MHz transmissions when communicating with each other; however, they would need to use 20 MHz transmissions when communicating with the legacy stations
  - The 802.11n access point must declare 20-only or 20/40 support in the beacon management frame.
  - 802.11n client stations must declare 20-only or 20/40 in the association or reassociation frames.
  - Client stations must re-associate when switching between 20-only and 20/40 modes.
  - If 20/40-capable stations transmit by using a single 20 MHz channel, they must transmit on the primary channel and not the secondary channel.
- HT protection modes (0–3)
  - To ensure backward compatibility with older 802.11a/b/g radios, 802.11n (HT) access points may signal to other 802.11n stations when to use one of four HT protection modes:
    - Mode 0—Greenfield (No Protection) Mode
      - Only HT radios are in use.
      - All the HT client stations must also have the same operational capabilities.
    - Mode 1—HT Non-member Protection Mode
      - In this mode, all the stations in the BSS must be HT stations. Protection mechanisms kick in when a non-HT client station or non-HT access point is heard that is not a member of the BSS
    - Mode 2—HT 20 MHz Protection Mode
      - In this mode, all the stations in the BSS must be HT stations and are associated to a 20/40 MHz access point.
      - If a 20 MHz–only HT station associates to the 20/40 MHz AP, protection must be used.
    - Mode 3—Non-HT Mixed Mode
      - This protection mode is used when one or more non-HT stations are associated to the HT access point
      - If any 802.11a/b/g radios associate to the BSS, protection will be used.
      - Mode 3 will probably be the most commonly used protection mode because most basic service sets will most likely have legacy 802.11a/b/g devices as members

- RTS/CTS and CTS-to-self
    - When HT protection is enabled within an HT BSS, an HT STA will precede HT transmissions with either an RTS/CTS control frame exchange or a CTS-to-Self-control frame using modulation and coding understandable to the STAs that are being protected against Duration ID within these control frames causes STAs to update their network allocation vector (NAV).

Very High Throughput (VHT) & 802.11ac

Thursday, May 14, 2020 10:06 PM

802.11ac-2013 amendment

- 802.11ac technology does not operate in the 2.4 GHz ISM band, only the 5 GHz U-NII bands.

5 GHz only

- 802.11ac expands channel widths even further than 802.11n, with channel widths of 80 MHz and 160 MHz.
- Due to the limited frequency space in the 2.4 GHz band, 802.11ac is designed to operate only in the 5 GHz band where much more frequency space is available.

20, 40, 80, and 160 MHz channels

- 802.11ac introduced two new channel widths: 80 MHz and 160 MHz
- 40 MHz channel is created by combining two 20 MHz channels, an 80 MHz channel combines two 40 MHz channels
- The two 40 MHz channels that make up the 80 MHz channel must be adjacent.
- the 160 MHz channel is made up of two 80 MHz channels; however, the two 80 MHz channels do not have to be adjacent
    - If the channels are adjacent, then it is referred to as a 160 MHz channel.
    - If they are not adjacent, then it is referred to as an 80+80 MHz channel.
- With 802.11ac, a new feature has been added that allows the AP to choose the channel width on a per-frame basis. This feature is known as dynamic bandwidth operation.

256-QAM modulation

- 256-QAM is an evolutionary upgrade that was introduced with 802.11ac
- 256-QAM identifies 256 unique values, using 16 different levels of phase shift and 16 different levels of amplitude shift.
- Because there are 256 distinct values, each value is able to represent 8 bits
- 256-QAM is more sensitive to noise and interference. Because of this, 802.11ac receiver performance requires about 5 dB of additional gain as compared to 64-QAM
- 256-QAM is used for the highest modulation coding sets. To achieve these higher data rates, higher signal-to-noise ratios are needed

Modulation and coding schemes

- 802.11n (HT) defined 77 different modulation and coding schemes (MCSs)
- 802.11ac simplified this by defining only 10 MCS options
- The first eight modulation and coding schemes are mandatory; however, most vendors will support the last two, which provide 256-QAM modulation

Single-user MIMO

- To distinguish the MIMO technology that was introduced with 802.11n from MU-MIMO, we will refer to it as single-user MIMO (SU-MIMO)
- The 802.11ac amendment doubles the total number of supported spatial streams to eight.

802.11ac data rates

- The first enhancement toward the increased data rates of 802.11ac is 256-QAM
- The second enhancement is the increase in data rates is the increase in the number of spatial streams
- Third is the channel width

VHT MAC

- A-MPDU
    - All 802.11ac frames are transmitted using the Aggregate MAC Protocol Data Unit (A-MPDU) frame format, even if only a single frame is being transmitted
    - Aggregation also shifts some of the frame information from the Physical Layer Convergence Protocol (PLCP) header to the MPDU header.
    - Since PLCP information is transmitted at the lowest supported data rate, and the MPDU information is transmitted at the higher data rates, this will improve performance
    - The higher transmission speeds of 802.11ac make Reduced Interframe Space (RIFS) obsolete

    - An A-MPDU frame reduces the per-frame overhead and only requires a single block ACK
- RTS/CTS
    - 802.11ac can use RTS/CTS to perform dynamic bandwidth operations
    - Uses it to dynamically change channel width

Beamforming

- Explicit beamforming
    - 802.11ac only uses explicit beamforming and requires support by both the transmitter and receiver in order for beamforming to be used
    - To begin the process, the beamformer transmits a null data packet (NDP) announcement frame, which notifies the beamformee of the intent to send a beamformed transmission.
    - The beamformer then follows this with an NDP frame
    - The beamformee processes each OFDM subcarrier and creates feedback information. The feedback contains information regarding power and the phase shift between each pair of transmit and receive antennas
    - The beamformer uses the feedback matrix to calculate a steering matrix that is used to direct the data transmission to the beamformee.
- Multiuser MIMO
    - The 802.11ac technology that changes one of the fundamental concepts of wireless networks, multiuser MIMO (MU-MIMO).
    - Up until now, an 802.11 AP was only able to communicate with one device at a time.
    - With 802.11ac, it is possible to communicate with up to four devices
    - The goal of MU-MIMO is to use as many spatial streams as possible, whether the transmission is with one client using four spatial streams or with four clients using one spatial stream each.
    - Due to the advanced signal processing that is required, MU-MIMO is only supported for downstream transmission from an AP to multiple clients
    - Beamforming is a critical part of MU-MIMO
- Multiuser beamforming
    - With MU-MIMO, the task of beamforming is not just performed for transmitting to a single client, it's performed for transmitting to up to four clients at a time.
    - To begin the MU-MIMO beamforming process, the AP performs a channel sounding procedure, similar but more complex than with SU-MIMO
    - the AP transmits a null data packet (NDP) announcement frame, notifying multiple beamformees of the intent to send a beamformed transmission
    - As with beamforming to a single user, each beamformee processes each OFDM subcarrier and creates feedback information, creating a compressed feedback matrix
    - The first beamformee responds to the AP with its compressed feedback matrix.
    - The AP then polls each additional beamformee sequentially using Beamforming Report Poll frames
    - The AP then uses the feedback matrix from each of the beamformees to create a single steering matrix
    - the AP is sending 16 transmissions, 4 from each antenna. Of those 16 transmissions, the receiving antenna needs to be able to distinguish and interpret the signal that is directed toward it while trying to ignore the other 12 transmissions.
    - Beamformees that are too close to each other could experience inter-user interference from signals directed toward other users
    - After the AP transmits the multiuser frame, the client stations must each acknowledge its frame
    - The AP keeps track of the capabilities of each client and goes through the beamforming and block acknowledgment processes for each transmission that it performs
    - The AP will periodically need to update its steering matrix in order to redirect or refocus the signal to the new location of a moving beamformee
- Quality of service
    - With the implementation of MU-MIMO, the implementation of the queuing and transmission of QoS frames is handled differently than in single-user wireless environments

    - The AP takes the first AC_VO frame for Station 1 and begins to construct a multiuser frame.
    - The AP takes frames for the other stations and adds them to the multiuser frame, providing that the stations are spatially distinct and the frames are shorter than the primary frame.
    - These other frames can be from the primary or secondary access category. Any shorter frames are padded
    - After the multiuser frame is transmitted to the three stations, block ACKs are used to confirm their successful transmission

Infrastructure requirements

- Ethernet
    - With the transition to the second phase of 802.11ac, the data throughput of the wireless network may exceed Gigabit Ethernet speeds.
    - So, if second phase 802.11ac is capable of data rates of up to 1.3 Gbps, what options are available for providing this throughput on the distribution system?
        - 10Gig copper
        - 10 Gig Fibre
        - 2 x 1Gig Cooper
        - mGig (NBaseT)
- Power
    - The greater the performance of the AP, the more likely that additional power will be needed.
    - The industry is transitioning to PoE+.
    - Upgrading the network to provide 802.3at (PoE+) power of 30 watts is highly recommended and most likely will become a necessity.

802.11ac in a SOHO or home

- Device radios
    - One of the first things to determine is whether the client devices that you will be using support 802.11ac
    - If you do plan to upgrade, you will need to purchase a dual-radio AP to continue to provide support for older 2.4 GHz devices
- Data flow/usage
    - Unless you have an unusual network configuration, your communications will be either between your client device and the Internet or between your client device and some type of server within your network
    - If communications with the Internet, it is not likely that your Internet connection is fast enough to support the throughput that an 802.11ac AP can provide.
    - If it can, you will need to ensure that the entire data path between the AP and the server supports at least 1 Gbps Ethernet.
- Spatial streams
    - Many personal mobile devices do not support multiple spatial streams due to the power requirements.
    - You will need to consider how your faster devices are affected and whether the performance you achieve is worth the upgrade costs
- Wider 802.11ac channels
    - With channel widths up to 80 MHz and 160 MHz with the second phase of 802.11ac, the wider channel width is a technology that all 802.11ac devices can benefit from
- MU-MIMO
    - MU-MIMO does have the potential of improving performance in the SOHO or home environment
    - With MU-MIMO, the AP can transmit to up to four devices simultaneously
    - You need to remember that this can only occur if the devices are spatially separated, since beamforming will not work properly if two devices are near each other

Wi-Fi Alliance certification

- Prior to the ratification of the 802.11ac amendment, the Wi-Fi Alliance published its vendor certification program for 802.11ac, Wi-Fi CERTIFIED ac.
- Wi-Fi CERTIFIED ac products must support both Wi-Fi Multimedia (WMM) quality-of-service

mechanisms and WPA2/WPA2 security mechanisms

- They only need to be backward compatible with 5 GHz 802.11a/n certified devices

Bring Your Own Device (BYOD)

Thursday, May 14, 2020 10:06 PM

Mobile Device Management

- Company-issued devices versus personal devices
    - An MDM solution can be used to manage both company-issued devices and personal devices.
    - the management of CID and BYOD is quite different.
    - The management strategy for company mobile devices usually entails more in-depth security because very often the CIDs have company documents and information stored on them.
    - When company devices are provisioned with an MDM solution, many configuration settings such as virtual private network (VPN) client access, email account settings, Wi-Fi, profile settings, passwords, and encryption settings are enabled.
    - The ability for employees to remove MDM profiles from a CID is disabled and the MDM administrator can remotely wipe company mobile devices if they are lost or stolen.
    - Because these devices are not personal devices, the IT department can also dictate which applications can or cannot be installed on tablets and/or smartphones.
    - The concept of BYOD emerged because personal mobile devices are much more difficult to manage unless a proper MDM solution has been deployed.
    - Every company should have its own unique BYOD containment strategy while still allowing access to the corporate WLAN
    - For example, when the personal devices are provisioned with an MDM solution, the camera may be disabled so that pictures cannot be taken within the building
- MDM architecture
    - The basic architecture of any MDM solution consists of four main components:
        - Mobile Device
            - The mobile Wi-Fi device requires access to the corporate WLAN
            - can be either a company-owned or employee-owned device.
            - The mobile devices are not allowed onto the corporate network until an enrolment process has been completed and an MDM profile has been installed
        - AP/WLAN Controller
            - All Wi-Fi communications are between the mobile devices and the access point to which they connected
            - If the devices have not been enrolled via the MDM server, the AP or WLAN controller quarantines the mobile devices within a restricted area of the network known as a walled garden
        - MDM Server
            - The MDM server is responsible for enrolling client devices
            - provisions the mobile devices with MDM profiles that define client device restrictions as well as configuration settings
            - Certificates can be provisioned from the MDM server
            - Whitelisting policies restrict enrolment to a list of specific devices and operating systems.
            - Blacklisting policies allow all devices and operating systems to enrol except for those that are specifically prohibited by the blacklist.
            - Device inventory control and application management are key components of any MDM solution
        - Push Notification Servers
            - The MDM server communicates with push notification servers such as Apple Push Notification service (APNs) and Google Cloud Messaging (GCM) for over-the-air management of mobile Wi-Fi devices
- MDM enrolment

- Mobile devices must go through an enrolment process in order to access network resources
    1. Mobile device connects with the access point
        - The mobile device must first establish an association with an AP.
        - The Wi-Fi security could be open, but usually the CID or personal devices are trying to establish a connection with a secure corporate SSID that is using 802.1X or pre-shared key (PSK) security
        - At this point, the AP holds the mobile client device inside a walled garden.
    2. AP checks if the device is enrolled.
        - The next step is to determine if the mobile device has been enrolled.
        - If the mobile device is already enrolled, the MDM server will send a message to the AP to release the device from the walled garden.
        - Unenrolled devices will remain quarantined inside the walled garden.
    3. MDM server queries LDAP
        - The MDM server queries an existing LDAP database, such as Active Directory.
        - The LDAP server responds to the query, and then the MDM enrolment can proceed
    4. Device is redirected to the MDM server
        - When the user opens a browser on the mobile device, it is redirected to the captive web portal for the MDM server
        - The enrolment process can then proceed.
        - For legal and privacy reasons, captive web portals contain a legal disclaimer agreement that gives the MDM administrator the ability to restrict settings and remotely change the capabilities of the mobile device.
        - If the user does not agree to the legal disclaimer, they cannot proceed with the enrolment process and will not be released from the walled garden.
    5. Devices installs certificate and MDM profile
        - Once enrolment begins, a secure over-the-air provisioning process for installing the MDM profile is needed
        - Over-the-air provisioning differs between different device operating systems, but using trusted certificates and SSL encryption is the norm.
    6. MDM server releases mobile device
        - once the device has completed the MDM enrolment, the MDM server sends a message to the AP or WLAN controller to release the mobile device from the walled garden.
    7. Mobile device exits the walled garden
        - The mobile device now abides by the restrictions and configuration settings defined by the MDM profile

- MDM profiles
    - MDM profiles are used for mobile device restrictions
    - MDM profiles can also be used to globally configure various components of a mobile device.
    - MDM profiles can include device restrictions, email settings, VPN settings, LDAP directory service settings, and Wi-Fi settings
- MDM agent software
    - The operating systems of some mobile devices require MDM agent application software.
    - An MDM agent must support multiple Android device manufacturers.
    - The MDM agent on the iOS device could potentially send information back to the MDM server that is not defined by the Apple MDM APIs
- Over-the-air management
    - The MDM server can monitor device information including device name, serial number, capacity, battery life, and the applications that are installed on the device
    - Information that cannot be seen includes SMS messages, personal emails, calendars, and browser history.
    - The mobile device can still be managed remotely, even if the mobile device is no longer connected to the corporate WLAN

    - The communication between the MDM server and the mobile devices requires push notifications from a third-party service.
    - Both Google and Apple have APIs that allow applications to send push notifications to mobile devices.
    - What kind of remote actions can an MDM administrator accomplish over the Internet
        - Make changes to the configuration.
        - Make changes to the device restrictions.
        - Deliver a message to the device.
        - Lock the device.
        - Wipe the device.
        - Make application management changes.
- Application management
    - Enterprise MDM solutions also offer various levels of management of the applications that run on mobile devices.
    - Managing applications on company-owned devices is commonplace; however, application management on employee's personal devices is not as prevalent.
- Wi-Fi client onboarding
    - The main purpose of these onboarding solutions is to give the customer an inexpensive and simple way to provision mobile devices onto the secure corporate SSID.

Guest WLAN access

- Guest SSID
    - In the past, a common SSID strategy was to segment different types of users—even employees— on separate SSIDs; each SSID was mapped to an independent VLAN
    - That strategy is rarely recommended now because of the layer 2 overhead created
    - What has not changed over time is the recommendation that all guest user traffic be segmented onto a separate SSID by having many SSIDs
    - The guest SSID will always have different security parameters than the employee SSID, and therefore the necessity of a separate guest SSID continues
    - Although encryption is not usually provided for guest users, some WLAN vendors have begun to offer encrypted guest access and provide data privacy using dynamic PSK credentials. Encrypted guest access can also be provided with 802.1X/EAP with Hotspot 2.0
- Guest VLAN
    - Guest user traffic should be segmented into a unique VLAN tied to an IP subnet that does not mix with the employee VLAN
    - Segmenting your guest users into a unique VLAN is a security and management best practice.
    - Although isolating the guest VLAN in a DMZ has been a common practice for many years, it is no longer necessary if guest firewall policies are being enforced at the edge of the network.
- Guest firewall policy
    - The most important security component of a guest WLAN is the firewall policy
    - The guest WLAN firewall policy prevents guest user traffic from getting near the company network infrastructure and resources
    - The guest firewall policy should simply route all guest traffic straight to an Internet gateway and away from the corporate network infrastructure.
    - It really is up to the security policy of the company to determine what ports need to be blocked on the guest VLAN
- Captive web portals
    - Often, guest users must log in through a captive web portal page before they are provided access to the Internet
    - One of the most important aspects of the captive web portal page is the legal disclaimer.
    - A captive portal solution effectively turns a web browser into an authentication service.
- Client isolation, rate limiting, and web content filtering
    - Client isolation is a feature that can be enabled on WLAN access points or controllers to block wireless clients from communicating directly with other wireless clients on the

same wireless VLAN.
    - Client isolation is highly recommended on guest WLANs to prevent peer-to-peer attacks.
    - Enterprise WLAN vendors also offer the capability to throttle bandwidth of user traffic.
    - Enterprise companies often deploy web content filter solutions to restrict the type of websites that their employees can view while at the workplace.
- Guest management
    - Most guest WLANS require a guest user to authenticate with credentials via a captive web portal
    - Unlike a pre-existing Active Directory database, guest user databases are normally created on-the-fly
    - Someone has to be in charge of managing the database and creating the guest user accounts
    - IT administrators are typically too busy to manage a guest database; therefore, the individual who manages the database is often a receptionist or the person who greets guests at the front door
- Guest self-registration
    - A good guest management solution allows the receptionist to register a single guest user or groups of users
    - Over the past few years, there has also been a greater push for guest users to create their own account, what is commonly referred to as self-registration.
    - When the guest is redirected to the captive web portal, if they do not already have a guest account, a link on the logon web page redirects the guest to a self-registration page.
    - Self-registration via a kiosk is quite useful when the kiosk is deployed in the main lobby or at the entrance to the company
    - An advantage of self-registration kiosks is that the receptionist does not have to provision the users and can concentrate on other work duties.
- Employee sponsorship
    - Guest users can also be required to enter the email address of an employee, who in turn must approve and sponsor the guest
    - Employee sponsorship ensures that only authorized guest users are allowed onto the guest WLAN and that the company employees are actively involved in the guest user authorization process.
- Social login
    - A new trend in guest networks in retail and service industries is social login
    - Social login is a method of using existing logon credentials from a social networking service (such as Twitter, Facebook, or LinkedIn)
    - Social login is often enabled using the OAuth protocol.
        - OAuth is a secure authorization protocol that allows access tokens to be issued to third-party clients by an authorization server
    - The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service and can be used for social login for Wi-Fi guest networks
- Encrypted guest access
    - The problem is that the many consumers and guest users are not savvy enough to know how to use a VPN solution when connected to an open guest WLAN
    - However, if a company can also provide encryption on the guest SSID, the protection provided to the guest user is a value added service.
    - Another growing trend with public access networks is the use of 802.1X/EAP with Hotspot 2.0
    - Hotspot 2.0 is a Wi-Fi Alliance technical specification that is supported by the Passpoint certification program
    - Though open networks are still the norm today, growing interest in security and automated connectivity in public access networks will motivate adoption and use of Hotspot 2.0

Network access control (NAC)

- Posture
    - Network access control (NAC) began as a response to computer viruses, worms, and malware that appeared in the early 2000s
    - Posture is a process that applies a set of rules to check the health and configuration of a computer and determine whether it should be allowed access to the network.
    - NAC products do not perform the health checks themselves but rather validate that the policy is adhered to.
    - Essentially, posture assessment “checks the checkers.”
    - After the posture check is performed, if a computer is considered unhealthy, the ideal scenario would be for the posture agent to automatically fi x or remediate the problem so
    - that the computer can pass the check and gain network access.
- NAC and BYOD
    - With the proliferation of personal Wi-Fi-enabled devices, enterprises were forced to decide if these devices would be allowed to connect to the enterprise network and if so, what type of access would be allowed.
    - Allows you to set device and user to be looked at if device is allowed onto network
    - NAC uses various monitoring and fingerprinting techniques to identify different devices so that access can be controlled.
- OS fingerprinting
    - The operating system of WLAN client devices can be determined by a variety of fingerprinting methods, including DHCP snooping.
    - An extensive list of DHCP fingerprints can be found at www.fingerbank.org.
    - Another OS detection method is HTTP fingerprinting. The user-agent header within an HTTP packet identifies the client operating system
- AAA
    - Authentication obviously is used to identify the user who is connecting to the network
    - Authorization is used to process information such as the following:
        - User type (admin, help desk, staff)
        - Location, connection type (wireless, wired, VPN)
        - Time of day
        - Device type (smartphone, tablet, computer)
        - Operating system
        - Posture
    - By utilizing both authentication and authorization, a NAC can distinguish between John using his smartphone and John using his personal laptop.
- RADIUS change of authorization
    - Prior to RADIUS Change of Authorization (CoA), if a client was authenticated and assigned a set of permissions on the network, the client authorization would not change
    - until the client logged out and logged back in.
    - RADIUS accounting (the final A in AAA) is used to monitor the user connection
    - RADIUS CoA can dynamically change the permissions that the user has on the network