

Certified Wireless Network Administrator

Module 01 – Overview of Wireless

Communications

WORKBOOK

Module Introduction

- Overview of Wireless History
 - Standards
 - The FCC
 - ITU-R
 - IETF
 - ISOC Hierarchy
 - WiFi Alliance
 - IEEE
 - OSI Model Review
 - The Hierarchical Model
 - Carrier Signals
 - Communication Fundamentals

Overview of Wireless History

- ☐ Wireless communications have been worked with since the 19th century
 - ☐ In the 1970's Hawaii had a wireless communication model for transmitting between the islands
 - This medium was called Aloha, operating at 400 MHz
 - ☐ In the 1990's we saw commercial wireless communications operating at the 900 MHz range

Standards

- The International Telecommunication Union Radio Communication Sector (ITU-R) and local entities such as the Federal Communications Commission (FCC) set the rules for what a user can do with a radio transmitter
 - These organizations manage and regulate frequencies, power levels, and transmission methods
 - They also work together to help guide the growth and expansion that is being demanded by wireless users

Standards (Cont.)

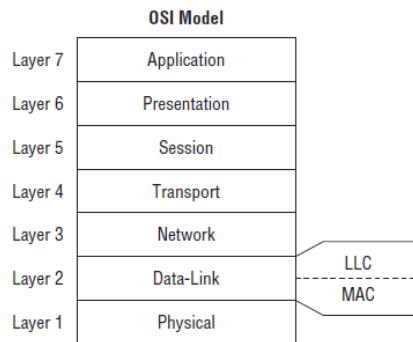
- The Institute of Electrical and Electronics Engineers (IEEE) creates standards for compatibility and coexistence between networking equipment
 - They still must adhere to the FCC's rules and regulations

Standards (Cont.)

- The Internet Engineering Task Force (IETF) is responsible for creating Internet standards
 - Many of these standards are integrated into the wireless networking and security protocols and standards
- The Wi-Fi Alliance performs certification testing to make sure wireless networking equipment conforms to the 802.11 WLAN communication guidelines

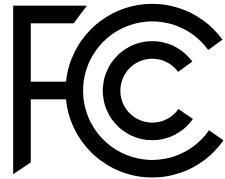
Standards (Cont.)

- Let's not forget the ISO designed the OSI model to aid in how the technologies can interconnect



The FCC

- ☐ Established by the Communications Act of 1934
 - ☐ The FCC is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable
 - ☐ They regulate licensed spectrum and unlicensed spectrum
 - ☐ Unlicensed means we don't have to acquire a license to use this medium



The FCC (Cont.)

- Both licensed and unlicensed communications are generally regulated by:
 - Frequency
 - Bandwidth
 - Maximum power of the Intentional Radiator (IR)
 - Maximum Equivalent Isotropically Radiated Power (EIRP)
 - Use (indoor and/or outdoor)
 - Spectrum sharing rules

ITU-R

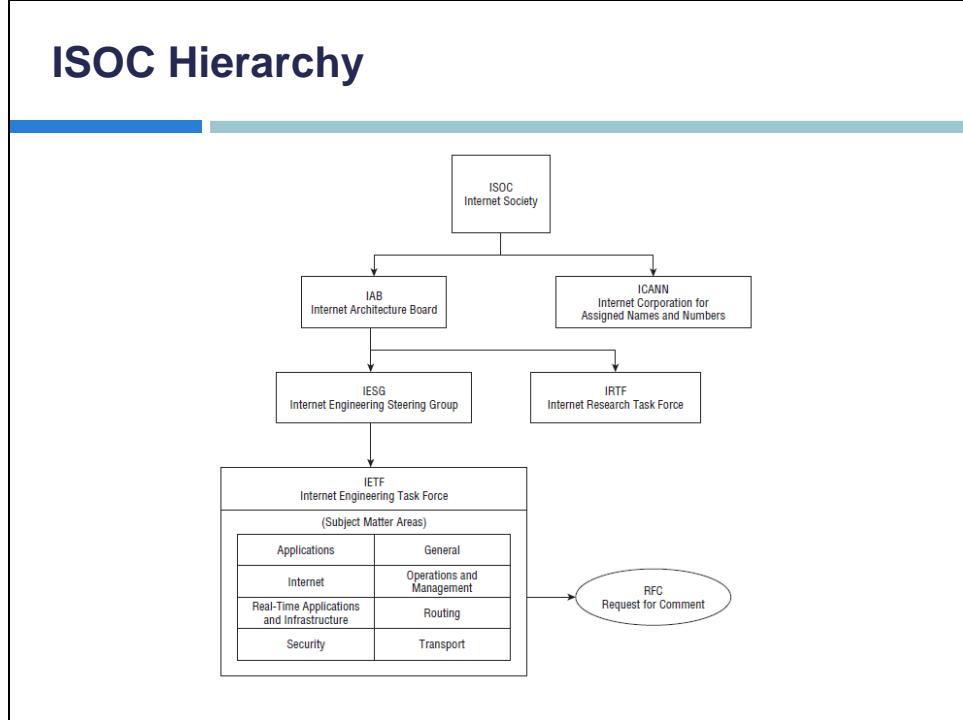
- The United Nations has tasked the *International Telecommunication Union Radio communication Sector (ITU-R) with global spectrum management*
 - This is broken down into 5 regions
 - Region A: The Americas, Inter-American Telecommunication Commission (CITEL) www.citel.oas.org
 - Region B: Western Europe, European Conference of Postal and Telecommunications Administrations (CEPT) www.cept.org
 - Region C: Eastern Europe and Northern Asia, Regional Commonwealth in the field of Communications (RCC) www.en.rcc.org.ru
 - Region D: Africa, African Telecommunications Union (ATU) www.atu-uat.org
 - Region E: Asia and Australia, Asia-Pacific Telecommunity (APT) www.aptsec.org

IETF

- IETF is one of five main groups that are part of the Internet Society (ISOC)
 - Internet Engineering Task Force (IETF)
 - Internet Architecture Board (IAB)
 - Internet Corporation for Assigned Names and Numbers (ICANN)
 - Internet Engineering Steering Group (IESG)
 - Internet Research Task Force (IRTF)

IETF (Cont.)

- RFC 3935, states the purpose of the IETF is as follows:
 - “...to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds.”



Wi-Fi Alliance

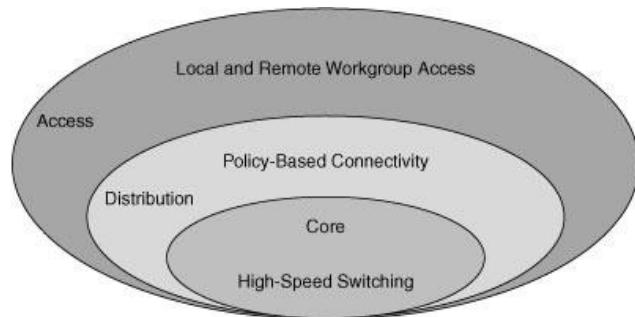
- ❑ A global non-profit organization of over 550 vendors devoted to improving the equipment used with 802.11
 - ❑ Any vendor equipment with this logo has been certified with any other vendor's equipment as long as they have the same logo



IEEE

- *Institute of Electrical and Electronics Engineers*
 - About 400,000 members in 160 countries
 - It is important to remember that the IEEE standards, like many other standards, are written documents describing how technical processes and equipment should function

The Hierarchical Model

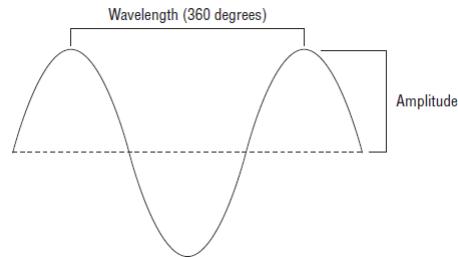


Carrier Signals

- Data is sent as a series of 1's and 0's
 - Therefore the transmitter needs a way of sending both 0's and 1's to transmit data from one location to another
 - If a signal fluctuates or is altered, even slightly, the signal can be interpreted so that data can be properly sent and received
 - This is then called the carrier signal

Communication Fundamentals

- Wireless communications use some sort of modulation to transmit data
 - Two terms used for the RF signal is Wavelength and Amplitude

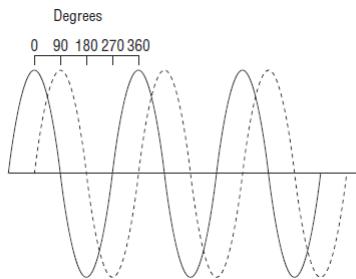


Communication Fundamentals (Cont.)

- *Frequency describes a behavior of waves*
 - Waves travel away from the source that generates them
 - How fast the waves travel, or more specifically, how many waves are generated over 1-second period of time, is known as frequency

Communication Fundamentals (Cont.)

- Phase is a relative term. It is the relationship between two waves with the same frequency.



Communication Fundamentals (Cont.)

- A keying method is what changes a signal into a carrier signal
 - It provides the signal with the ability to encode data so that it can be communicated or transported



Communication Fundamentals (Cont.)

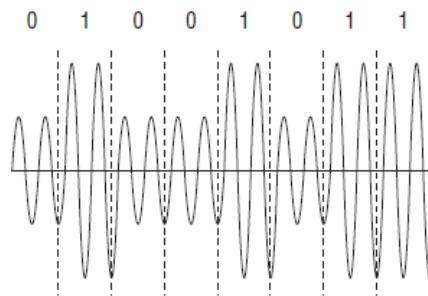
- Keying methods are used to transmit the data
- There are three current types used:
 - Amplitude-Shift Keying (ASK)
 - Frequency-Shift Keying (FSK)
 - Phase-Shift Keying (PSK)
- Note: These will be covered in more detail

Communication Fundamentals (Cont.)

- Current State: This method of determining if a 1/0 is being transmitted is to notice the state of the signal at an expected point in time
- State Transition: This method will determine a 1/0 based on whether or not the transmitted signal changed state, such as going out of phase

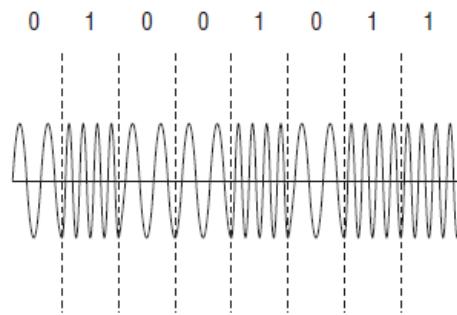
Communication Fundamentals (Cont.)

□ Amplitude-Shift Keying:



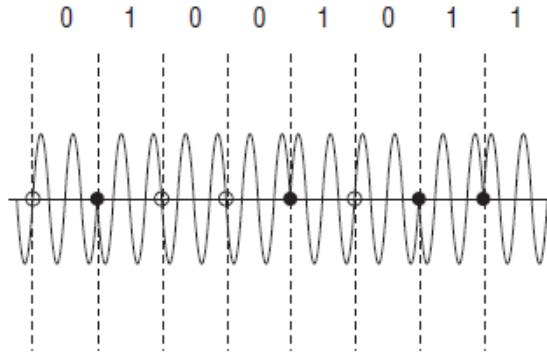
Communication Fundamentals (Cont.)

□ Frequency-Shift Keying:



Communication Fundamentals (Cont.)

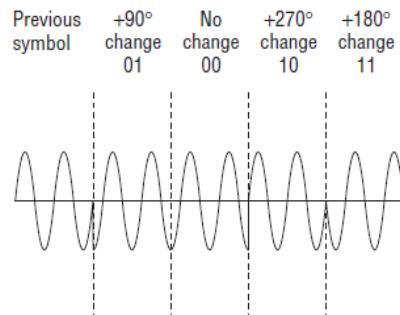
□ Phase-Shift Keying:



- No phase change occurred
 - Phase change occurred

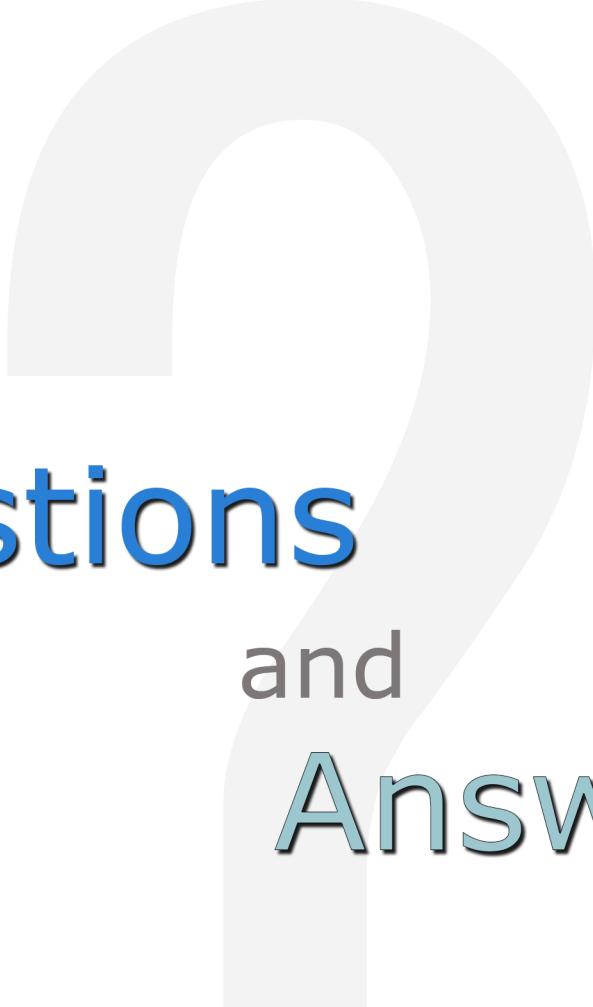
Communication Fundamentals (Cont.)

- Multiple-Phase-Shift Keying:
 - Advanced versions of PSK can encode multiple bits per symbol
 - Instead of using 2 phases for a single 1/0, we can use four phases, which is capable of representing two binary values (00, 01, 10, or 11)



Module Review

- Overview of Wireless History
 - Standards
 - The FCC
 - ITU-R
 - IETF
 - ISOC Hierarchy
 - WiFi Allowance
 - IEEE
 - OSI Model Review
 - The Hierarchical Model
 - Carrier Signals
 - Communication Fundamentals



Questions and Answers

Review Questions:

1. In the 1970's _____ had a wireless communication model for transmitting between islands.
 - A. China
 - B. Hawaii
 - C. Alaska
 - D. Russia

2. True or False: In the 1990's we saw commercial wireless communications operating at the 1900 MHz range.
 - A. True
 - B. False

3. What does FCC stand for?
 - A. Federal Castration Commission
 - B. Foreign Colonization Congress
 - C. Freight Coordination Capital
 - D. Federal Communications Commission

4. True or False: The Institute of Electrical and Electronics Engineers (IEEE) creates standards for compatibility and coexistence between networking equipment.
 - A. True
 - B. False

5. True or False: Wi-Fi Alliance is a global non-profit organization of over 550 vendors devoted to improving the equipment used with 802.11.
 - A. True
 - B. False

Answer Key:

1. B
In the 1970's Hawaii had a wireless communication model for transmitting between islands.
2. B
False. In the 1990's we saw commercial wireless communications operating at the 900 MHz range.
3. D
FCC stands for Federal Communications Commission.
4. A
True. The Institute of Electrical and Electronics Engineers (IEEE) creates standards for compatibility and coexistence between networking equipment.
5. A
True. Wi-Fi Alliance is a global non-profit organization of over 550 vendors devoted to improving the equipment used with 802.11.

Certified Wireless Network Administrator
Module 02 - Fundamentals of RF

WORKBOOK

Module Introduction

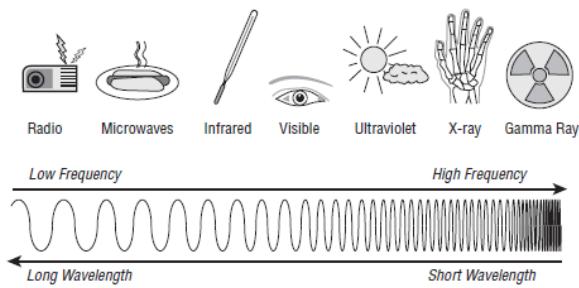
- What is an RF Signal?
 - Characteristics of RF
 - Wavelength
 - Frequency
 - Amplitude
 - Phase
 - RF Behaviors
 - Absorption
 - Reflection
 - Scattering
 - Refraction
 - Diffraction
 - Attenuation
 - Multipath
 - Gain

What is an RF Signal?

- The electromagnetic (EM) spectrum, which is usually simply referred to as spectrum, is the range of all possible electromagnetic radiation
 - These signals can move through matter or space
 - You may know these signals from:
 - AM/FM
 - X-Rays
 - Visible light

What is an RF Signal? (Cont.)

□ Electromagnetic Spectrum



What is an RF Signal? (Cont.)

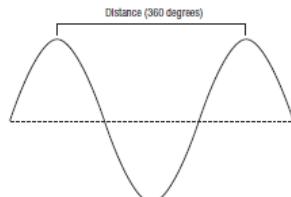
- An RF signal starts out as an electrical alternating current (AC) signal that is originally generated by a power source
 - This AC signal is sent through a copper conductor (typically a coaxial cable) and radiated out of an antenna element in the form of an electromagnetic wave
 - This electromagnetic wave is the wireless signal
 - Changes of electron flow in an antenna, otherwise known as *current*, produce changes in the electromagnetic fields around the antenna.
 - The shape and form of the AC signal—defined as the *waveform*—is known as a sine wave

Characteristics of RF

- A study in physics would show the following characteristics of RF
 - Wavelength
 - Amplitude
 - Frequency
 - Phase

Wavelength

- As stated earlier, an RF signal is an alternating current (AC) that continuously changes between a positive and negative voltage
 - Wavelength is the distance between the two successive crests



Wavelength (Cont.)

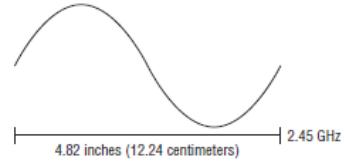
- The three components of this inverse relationship are:
 - Frequency (f , measured in hertz, or Hz)
 - Wavelength (λ , measured in meters, or m)
 - Speed of light (c , which is a constant value of 300,000,000 m/sec)
 - Reference formulas:
 - To illustrate the relationship: $\lambda = c/f$ and $f = c/\lambda$
 - A simplified explanation is that the higher the frequency of an RF signal, the smaller the wavelength of that signal
 - The larger the wavelength of an RF signal, the lower the frequency of that signal

Wavelength (Cont.)

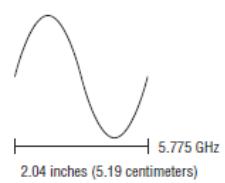
- Commonly, we hear that a lower frequency signal will travel farther than a higher frequency
 - Think of the pebble thrown into a clear lake, the energy doesn't stop, it's just harder to detect over a greater distance

Wavelength (Cont.)

□ 2.4 GHz



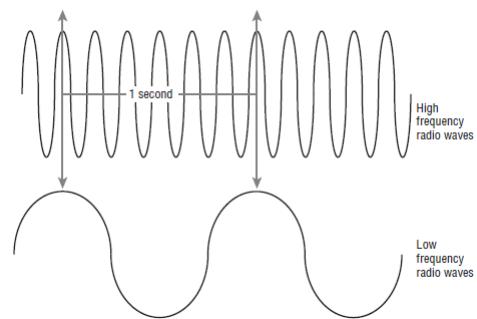
□ 5.0 GHz



Frequency

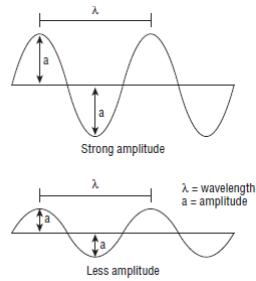
- Frequency is the number of times a specified event occurs within a specified time interval
 - A standard measurement of frequency is *hertz* (Hz)
 - 1 hertz (Hz) = 1 cycle per second
 - 1 kilohertz (KHz) = 1,000 cycles per second
 - 1 megahertz (MHz) = 1,000,000 (million) cycles per second
 - 1 gigahertz (GHz) = 1,000,000,000 (billion) cycles per second

Frequency (Cont.)



Amplitude

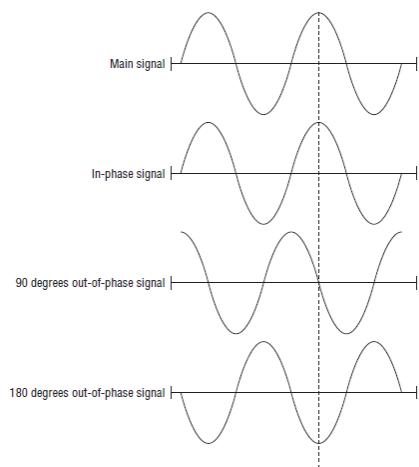
- This is the strength or power of the signal
 - When you look at an RF signal using an oscilloscope, the amplitude is represented by the positive crests and negative troughs of the sine wave



Phase

- This is a relationship between 2 or more signals with the same frequency
 - The phase involves the relationship between the position of the amplitude crests and troughs of two waveforms
 - If 2 signals have a 0 degree difference in phase, then the amplitude may increase as much as double
 - If 2 signals have a 180 degree difference in phase, then they would cancel each other out
 - This is if these signals were of the same frequency

Phase (Cont.)



RF Behaviors

- As an RF signal travels through the air and other mediums, it can move and behave in different manners
- RF propagation behaviors include:
 - Absorption
 - Reflection
 - Scattering
 - Refraction
 - Diffraction
 - Free-Space-Path-Loss
 - Multipath
 - Attenuation
 - Gain

Absorption

- If a signal does not bounce off, or move around an object, and it cannot move through the object then you'd have 100% absorption
- Example:
 - A 2.4 GHz signal will be 1/16 the original power after propagating through a brick wall
 - That same signal will only lose 1/2 the original power after passing though drywall material

Reflection

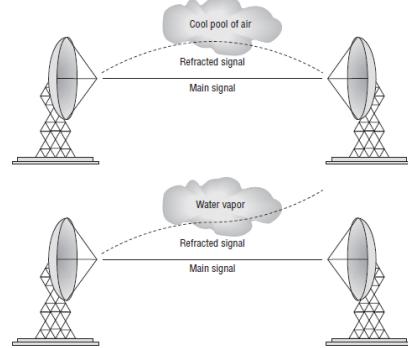
- ☐ A wave can bounce off a flat smooth surface that is larger than the wave
 - ☐ This will change the direction of the wave
 - ☐ There are two major types of reflection:
 - ☐ Sky wave reflection:
 - This is usually frequencies below 1GHz, such as AM radio, and a reason why you can hear a radio station that is 100's of miles away on a clear night
 - The signal is bouncing off of the ionosphere
 - ☐ Microwave reflection:
 - Microwave signals exist between 1 GHz and 300 GHz
 - These can bounce off of much smaller objects like a metal door

Scattering

- With scattering, you could almost think of multiple reflections at once
 - Such as why the sky appears blue
 - When a signal is passing through a medium of smaller particles then scattering could become an issue to the strength of the signal

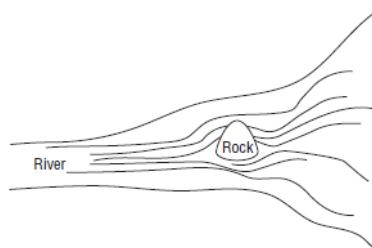
Refraction

- When a signal passes through a different type of medium (such as liquid) this medium could cause the signal to be “bent”



Diffraction

- Like Refraction, a signal is bent, but in this case around an object, not passing through a different medium



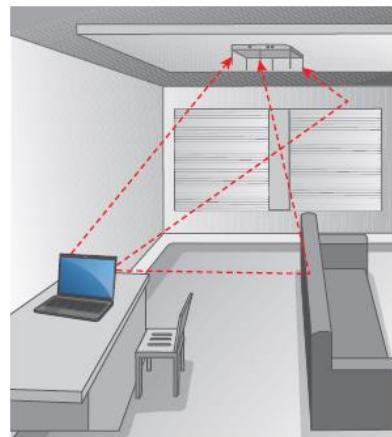
Attenuation

- This is the loss of signal strength over distance
 - If you think again, about the ripple effect, the amount of energy is still the same, but it's having to spread the energy over a greater distance
 - At some point the amount of energy is too low for the receiving antenna to detect
 - This could also be known as free-space-path-loss

Multipath

- Multipath is a propagation phenomenon that results in two or more paths of a signal arriving at a receiving antenna at the same time or within nanoseconds of each other
 - This can often be caused by reflection
 - Multipath is most often destructive:
 - Cancelling or weakening other signals (nulling / down fade)
 - Increasing the amplitude (up fade)
 - Causing corruption (data corruption)

Multipath (Cont.)

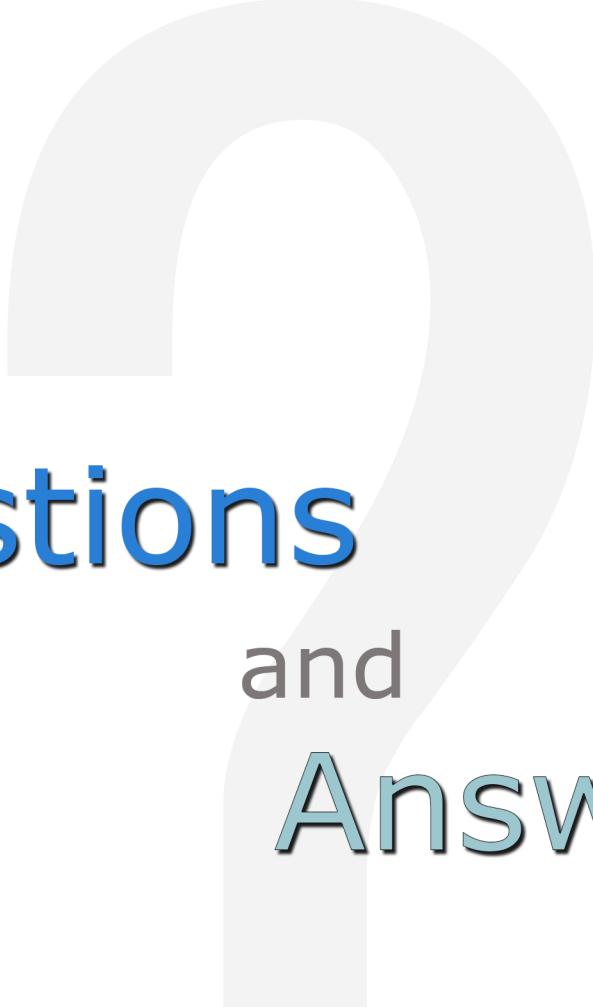


Gain

- Known as amplification or increased amplitude
 - A signal's amplitude can be boosted by the use of external devices
 - Active gain is usually caused by the transceiver or the use of an amplifier on the wire that connects the transceiver to the antenna
 - Passive gain is accomplished by focusing the RF signal with the use of an antenna

Module Review

- What is an RF Signal
- Characteristics of RF
- Wavelength
- Frequency
- Amplitude
- Phase
- RF Behaviors
- Absorption
- Reflection
- Scattering
- Refraction
- Diffraction
- Attenuation
- Multipath
- Gain



Questions and Answers

Review Questions:

1. True or False: The electromagnetic (EM) spectrum, which is usually simply referred to as spectrum, is the subset range of possible electromagnetic radiation.
 - A. True
 - B. False

2. Which of the following is not an example of an RF signal?
 - A. Infrared
 - B. AM \ FM
 - C. Sound waves
 - D. X-Rays

3. Which of the following are characteristics of RF? (Choose two)
 - A. Wavelength
 - B. Latitude
 - C. Frequency
 - D. Pulse

4. _____ is the number of times a specified event occurs within a specified time interval.
 - A. Wavelength
 - B. Signal
 - C. Amplitude
 - D. Frequency

5. _____ is the strength or power of the signal.
 - A. Signal
 - B. Amplitude
 - C. Frequency
 - D. Phase

Answer Key:

1. B
False. The electromagnetic (EM) spectrum, which is usually simply referred to as spectrum, is the range of all possible electromagnetic radiation.
2. C
Sound waves are not an example of an RF signal.
3. A, C
Latitude and pulse are not characteristics of RF.
4. D
Frequency is the number of times a specified event occurs within a specified time interval.
5. B
Amplitude is the strength or power of the signal.

Certified Wireless Network Administrator
Module 03 – Components and
Measurements of RF

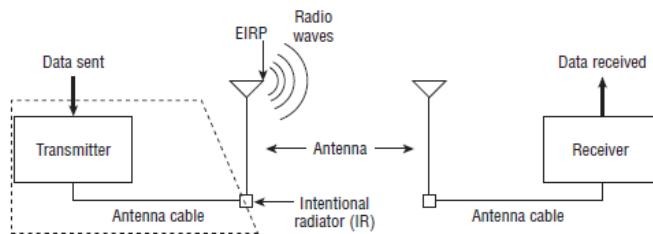
WORKBOOK

Module Introduction

- Components of RF Communications
 - Units of Power and Comparison
 - RF Mathematics
 - Rule of 10s and 3s

Components of RF Communications

- Many components contribute to the successful transmission and reception of an RF signal



Transmitter

- The transmitter is the initial component in the creation of the wireless medium
- The computer hands the data off to the transmitter, and it is the transmitter's job to begin the RF communication
 - When the transmitter receives data, it then generates the AC current to start this transmission
 - The transmitter determines the power to be used

Antenna

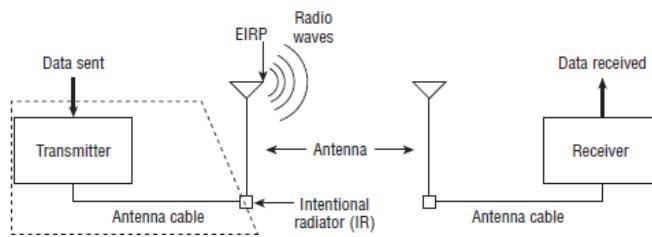
- ❑ An antenna provides two functions in a communication system
 - ❑ Connected to the transmitter, it collects the AC signal that it receives and directs, or radiates, the RF waves away from the antenna in a pattern specific to the antenna type
 - Often called an isotropic radiator (IR)
 - ❑ When connected to the receiver, the antenna takes the RF waves that it receives through the air and directs the AC signal to the receiver
 - ❑ The receiver converts the AC signal to bits and bytes

Antenna (Cont.)

- There are two ways to increase the power output from an antenna
 1. To generate more power at the transmitter
 2. To direct, or focus, the RF signal that is radiating from the antenna

Receiver

- The receiver is the final component in the wireless medium
 - The receiver takes the carrier signal that is received from the antenna and translates the modulated signals into 1s and 0s



Intentional Radiator (IR)

- The FCC defines this as:
 - Something that is specifically designed to generate RF, as opposed to something that generates RF as a by-product of its main function
 - The FCC regulates the power level
 - It is typically measured in milliwatts (mW) or decibels relative to 1 milliwatt (dBm)

Equivalent Isotropically Radiated Power (EIRP)

- EIRP is the highest RF signal strength that is transmitted from a particular antenna
 - EIRP can be increased based on the type of antenna
 - Think of a flashlight

Units of Power and Comparison

- When an 802.11 wireless network is designed, two key components are coverage and performance
 - A good understanding of RF power, comparison, and RF mathematics can be very helpful during the network design phase

Units of Power

- **Units of Power (Absolute)**

- Watt (W)
- Milliwatt (mW)
- Decibels relative to 1 milliwatt (dBm)

- **Units of Comparison (Relative)**

- Decibel (dB)
- Decibels relative to an isotropic radiator (dBi)
- Decibels relative to a half-wave dipole antenna (dBd)

Watt

- A watt (W) is the basic unit of power
 - A watt is very similar to the output of the power washer
 - Instead of the pressure generated by the machine, electrical systems have voltage
 - Instead of water flow, electrical systems have current, which is measured in amps
 - So the amount of watts generated is equal to the volts times the amps

Watt (Cont.)

- A milliwatt (mW) is also a unit of power
 - A milliwatt is 1/1,000 of a watt
 - The reason you need to be concerned with milliwatts is because most of the indoor 802.11 equipment that you will be using transmits at power levels between 1 mW and 100 mW

Decibel (dB)

- The first thing you should know about the *decibel (dB)* is that it is a unit of comparison, not a unit of power
 - It is used to represent a difference between two values
 - In other words, a dB is a relative expression and a measurement of change in power
 - dB compares the difference or loss between the EIRP output of a transmitter's antenna and the amount of power received by the receiver's antenna

Decibel (Cont.)

- A bel is defined as the ratio of 10 to 1 between the power of two sounds
 - Example: An access point transmits data at 100 mW Laptop1 receives the signal from the AP at a power level of 10 mW
 - This is a ratio of 10:1 or 1 bel

dB Mathematics

- $10^1 = 10 \log_{10}(10) = 1$
- $10^2 = 100 \log_{10}(100) = 2$
- $10^3 = 1,000 \log_{10}(1,000) = 3$
- $10^4 = 10,000 \log_{10}(10,000) = 4$
- A dB is 1/100 of a bel
- To calculate dB:
 - Decibels = $10 \times \log_{10}(P1/P2)$

dB_i

- It is important to be able to calculate the radiating power of the antenna so that you can determine how strong a signal is at a certain distance from the antenna
 - This measurement is decibels isotropic (dB_i)
 - Comparing measurements from an Isotropic Radiator
 - Another way of phrasing this is decibel gain referenced to an isotropic radiator or change in power relative to an antenna

dB_i (Cont.)

- Since antennas are measured in gain, not power, you can conclude that dB_i is a relative measurement and not an absolute power measurement
 - dB_i is simply a measurement of antenna gain
 - The dB_i value is measured at the strongest point, or the focus point, of the antenna signal

dBd

- The antenna industry uses two dB scales to describe the gain of antennas
 - The first scale, is dBi
 - The second scale is dipole (dBd), or decibel gain relative to a dipole antenna
 - So a dBd value is the increase in gain of an antenna when it is compared to the signal of a dipole antenna

dBd (Cont.)

- The definition of dBd seems simple enough
 - How do you compare two antennas when one is represented with dBi and the other with dBd?
 - This is actually quite simple. A standard dipole antenna has a dBi value of 2.14. If an antenna has a value of 3 dBd, this means that it is 3 dB greater than a dipole antenna.
 - Again think of the flashlight
 - If the dipole antenna is 2.14 dBi, all you need to do is add 3 to 2.14
 - A 3 dBd antenna is equal to a 5.14 dBi antenna

dBm

- ❑ dBm also provides a comparison
 - ❑ Instead of comparing a signal to another signal, it is used to compare a signal to 1 milliwatt of power
 - ❑ dBm means decibels relative to 1 milliwatt
 - ❑ 0 dBm is equal to 1 milliwatt
 - ❑ Using the formula $\text{dBm} = 10 \times \log_{10}(P_{\text{mW}})$, you can determine that 100 mW of power is equal to +20 dBm

The 6dB Rule

- ☐ Known as the “Inverse Square Law”
 - ☐ By doubling the distance from the RF source, the signal will decrease by about 6 dB
 - ☐ If you double the distance between the transmitter and the receiver, the received signal will decrease by 6 dB
 - ☐ This rule also implies that if you increase the amplitude by 6 dB, the usable distance will double
 - ☐ This 6 dB rule is very useful for comparing cell sizes or estimating the coverage of a transmitter
 - Also useful for understanding antenna gain
 - Every 6 dB of extra antenna gain will double the usable distance of an RF signal

RF Mathematics

- These logarithmic functions can look scary
- If you want to refresh yourself on some of your math skills before going on, then review the following:
 - Addition and subtraction using the numbers 3 and 10
 - Multiplication and division using the numbers 2 and 10
- Although not technically accurate doing this type of math will be close

Rule of 10s and 3s

- For every 3 dB of gain (relative), double the absolute power (mW)
- For every 3 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

Rule of 10s and 3s (Cont.)

□ Example:

- ❑ If your access point is configured to transmit at 100 mW and the antenna is rated for 3 dBi of passive gain, the amount of power that will radiate out of the antenna (EIRP) will be 200 mW
 - Following the rule learned, the 3 dB of gain from the antenna caused the 100 mW signal from the access point to double
 - ❑ If your access point is configured to transmit at 100 mW and is attached to a cable that introduces 3 dB of loss, the amount of absolute amplitude at the end of the cable will be 50 mW
 - Here the 3 dB of loss from the cable caused the 100 mW signal from the access point to be halved

AM1

Math Examples (eNotes)

$\checkmark \frac{10}{\text{dBm}} + \frac{0}{\text{dBm}}$

$$\begin{array}{r} 1 \\ + \\ 3 \\ + \\ 3 \\ + \\ 6 \\ + \\ 2 \\ \hline 9 \end{array}$$

$\frac{mW}{1} \div \frac{2}{10}$

$$\begin{array}{r} 1 \\ \times 2 \\ \hline 2 \end{array}$$

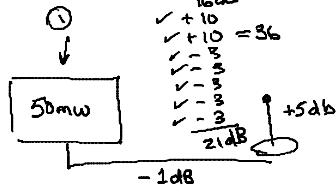
$\frac{(10)}{\text{dBm}} + \frac{0}{\text{dBm}}$

$$\begin{array}{r} 10 \\ + \\ 10 \\ + \\ 20 \text{ dBm} \\ - \\ 3 \\ \hline 17 \text{ dBm} \\ + \\ 10 \text{ dBm} \\ \hline 27 \text{ dBm} \end{array}$$

$\frac{mW}{1} \div \frac{2}{10}$

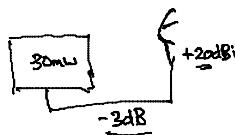
$$\begin{array}{r} 1 \\ \times 10 \\ \times 10 \\ \hline 100 \text{ mW} \\ 2 \\ \hline 50 \text{ mW} \\ \times 10 \\ \hline 500 \text{ mW} \end{array}$$

Math Examples (eNotes)



Math Examples (eNotes)

$$\begin{array}{r} 3 \uparrow \\ 10 - \end{array} \quad \begin{array}{l} \text{dBm} \\ \text{UNK} \\ \text{UNK-3} \\ +10 \text{ UNK+7} \\ +10 \text{ UNK+17} \end{array}$$
$$\begin{array}{r} \text{mW} \times 2 \\ \hline 30\text{mW} \\ 15\text{mW} \\ 150 \\ 1500 \end{array} \quad \begin{array}{r} \text{dB} \\ 0 \\ \hline 1 \\ +10 \\ +10 \end{array}$$

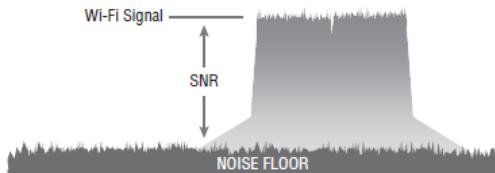


Noise Floor

- The noise floor is the ambient or background level of radio energy on a specific channel
 - This could be caused by another transmitter
 - This could be caused by non-transmitters such as a microwave oven

SNR

- Many Wi-Fi vendors define signal quality as the *Signal-to-Noise Ratio (SNR)*
 - If a radio receives a signal of -85 dBm and the noise floor is measured at -100 dBm, the difference between the received signal and the background noise is 15 dB
 - The SNR is 15 dB



Received Signal Strength Indicator (RSSI)

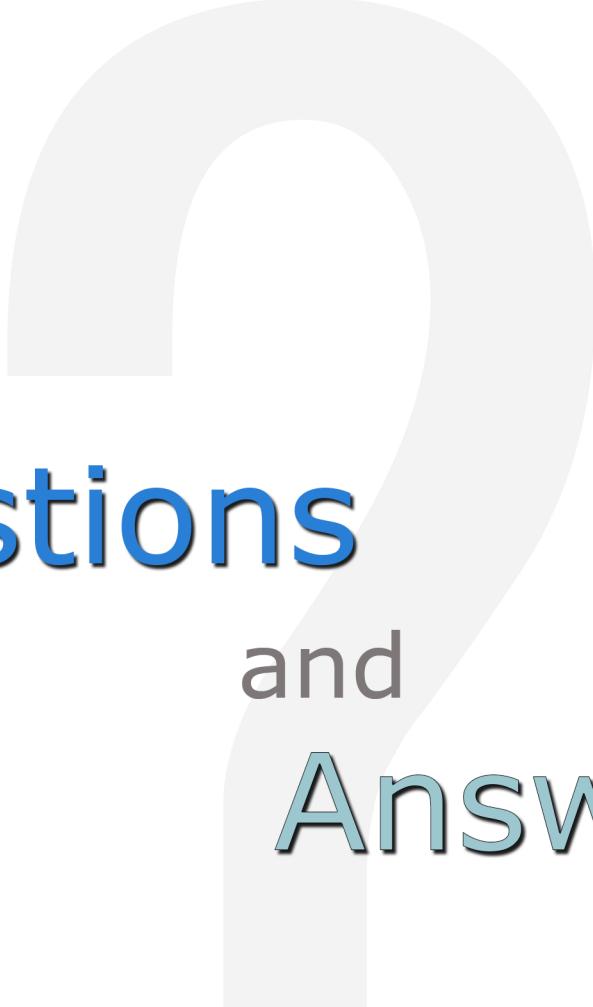
- Receive sensitivity refers to the power level of an RF signal required to be successfully received by the receiver radio
 - ▣ The lower the power level that the receiver can successfully process, the better the receive sensitivity
 - This is like being a concert
 - How loud (at minimum) must your friend speak for you to understand their speech

RSSI Example

- 54 Mbps –79 dBm
 - 48 Mbps –80 dBm
 - 36 Mbps –85 dBm
 - 24 Mbps –87 dBm
 - 18 Mbps –90 dBm
 - 12 Mbps –91 dBm
 - 9 Mbps –91 dBm
 - 6 Mbps –91 dBm

Module Review

- Components of RF Communications
 - Units of Power and Comparison
 - RF Mathematics
 - Rule of 10s and 3s



Questions and Answers

Review Questions:

1. The _____ is the initial component in the creation of the wireless medium.
 - A. Antenna
 - B. Receiver
 - C. Transmitter
 - D. Intentional Radiator

2. What provides two functions in a communication system?
 - A. Antenna
 - B. Transmitter
 - C. Receiver
 - D. Intentional Radiator

3. The _____ is the final component in the wireless medium.
 - A. Antenna
 - B. Intentional Radiator
 - C. Receiver
 - D. Transmitter

4. What are the two key components when designing an 802.11 wireless network?
 - A. Coverage
 - B. Maintenance
 - C. Ceiling height
 - D. Performance

5. The _____ is the ambient or background level of radio energy on a specific channel.
 - A. Received Signal Strength Indicator
 - B. Noise Floor
 - C. RF Mathematics
 - D. SNR

Answer Key:

1. C
The transmitter is the initial component in the creation of the wireless medium.
2. A
An antenna provides two functions in a communication system.
3. C
The receiver is the final component in the wireless medium.
4. A, D
When an 802.11 wireless network is designed, two key components are coverage and performance.
5. B
The noise floor is the ambient or background level of radio energy on a specific channel.

Certified Wireless Network Administrator
Module 04 – RF Signal and Antenna
Concepts

WORKBOOK

Module Introduction

- Azimuth and elevation charts (antenna radiation envelopes)
- Omnidirectional antennas
- Semidirectional antennas
- Highly directional antennas
- Sector antennas
- Antenna arrays
- Static beamforming
- Dynamic beamforming
- Transmit beamforming

Azimuth and Elevation Charts (Antenna Radiation Envelopes)

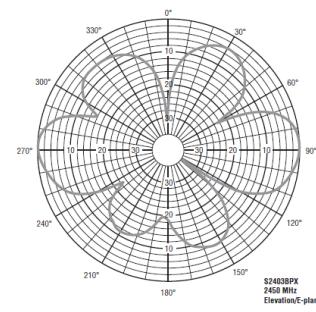
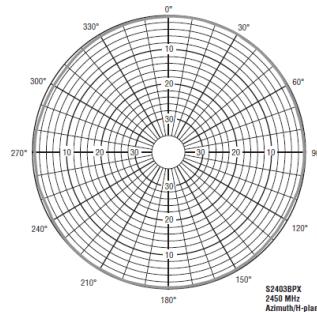
- Actual side-by-side comparison of antennas requires you to:
 - Walk around the antenna with an RF meter
 - Take numerous signal measurements
 - Plot the measurements
 - On the ground
 - On a piece of paper that represents the environment

Azimuth and Elevation Charts (Antenna Radiation Envelopes) (Cont.)

- Antenna manufacturers create Azimuth charts and elevation charts, commonly known as radiation patterns, for their antennas
 - These charts are commonly known as polar charts or antenna radiation envelopes

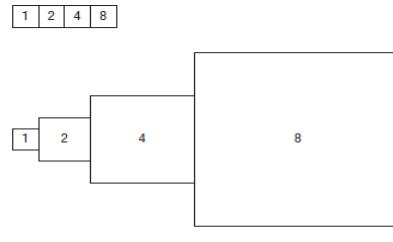
Azimuth and Elevation Charts (Antenna Radiation Envelopes) (Cont.)

- In these charts, the antenna is placed at the center of the chart
 - Azimuth chart = H-plane = top-down view
 - Elevation chart = E-plane = side view



Azimuth and Elevation Charts (Antenna Radiation Envelopes) (Cont.)

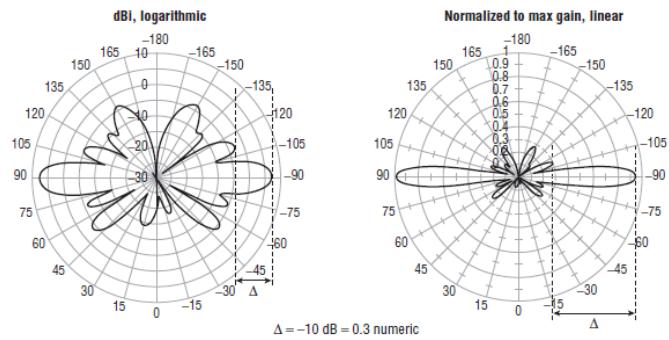
- These charts are often misinterpreted and misread
 - One of the biggest reasons these charts are misinterpreted is that they represent the decibel (dB) mapping of the antenna coverage



1 2 4 8 16 32 64 128 256 512

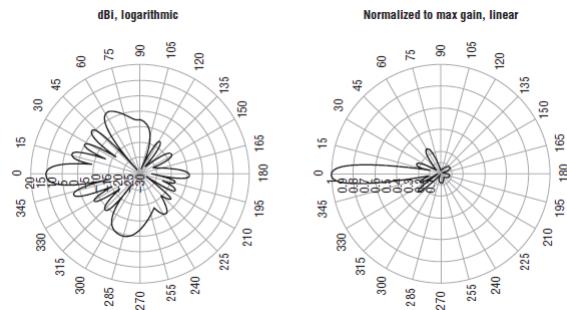
Azimuth and Elevation Charts (Antenna Radiation Envelopes) (Cont.)

- Example of logarithmic chart E-plane



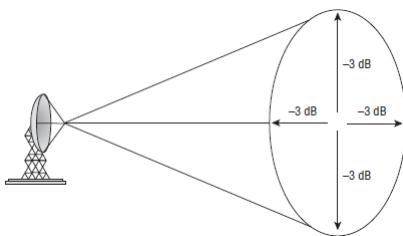
Azimuth and Elevation Charts (Antenna Radiation Envelopes) (Cont.)

□ Directional Antenna E-plane

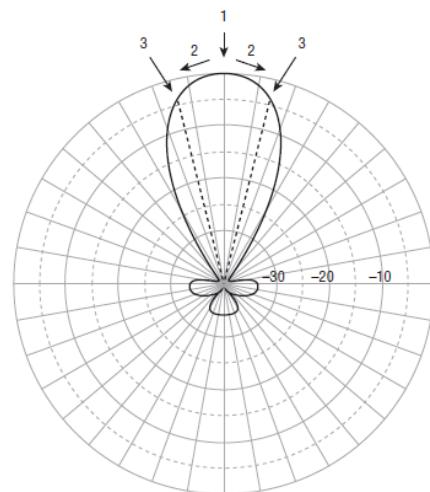


Beamwidth

- Measurement of how broad or narrow the focus of an antenna
- Measured both horizontally and vertically
 - From the center, or strongest point, of the antenna signal to each of the points along the horizontal and vertical axes where the signal decreases by half power



Beamwidth (Cont.)

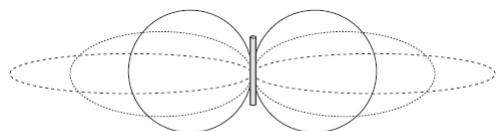


Antenna Types

- There are three main categories of antennas:
 - Omnidirectional: radiate RF in a fashion similar to the way a typical lamp radiates light
 - Designed to provide general coverage in all directions
 - Semidirectional: radiate RF in a fashion similar to the way a street lamp shines light
 - Highly directional: radiate RF in a fashion similar to the way a spotlight focuses light on a flag or a sign

Omnidirectional Antenna

- Omnidirectional antennas radiate RF signal in all directions
 - Small, rubber-coated dipole antenna, often referred to as a rubber duck antenna
 - The default antenna of many access points

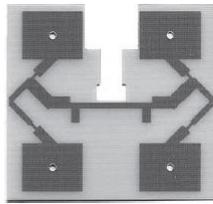


Semidirectional Antenna

- Semidirectional antennas are designed to direct a signal in a specific direction
 - Used for short- to medium-distance communications
 - Three types of antennas fit into the semidirectional category:
 - Patch
 - Panel
 - Yagi (pronounced YAH-gee)

Patch Antenna

- Used for outdoor point-to-point communications up to about a mile
- More commonly used as a central device to provide unidirectional coverage from the access point to the clients in an indoor environment



Planar Antenna

- Planar antennas are also often used to provide coverage for long hallways with offices on each side

Yagi Antenna

- They are typically used for short- to medium-distance point-to-point communications of up to about 2 miles, although high-gain Yagi antennas can be used for longer distances
 - Another benefit of semidirectional antennas is that they can be installed high on a wall and tilted downward toward the area to be covered



Highly Directional Antenna

- ❑ Highly directional antennas are strictly used for point-to-point communications, typically to provide network bridging between two buildings
 - ❑ They provide the most focused, narrow beamwidth of any of the antenna types
 - ❑ Two types:
 - ❑ Parabolic Dish Antenna:
 - The parabolic dish antenna is similar in appearance to the small digital satellite TV antennas that can be seen on the roofs of many houses
 - ❑ Grid Antenna:
 - The spacing of the wires on a grid antenna is determined by the wavelength of the frequencies that the antenna is designed for

Antenna Arrays

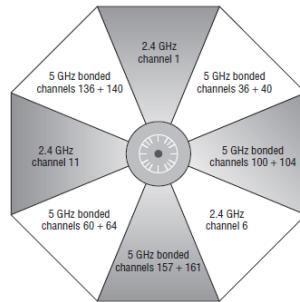
- A group of two or more antennas that are integrated together to provide coverage
 - These operate together to perform what is known as beamforming

Beamforming

- Beamforming is a method of concentrating RF energy
 - Concentrating a signal means that the power of the signal will be greater and the SNR at the receiver should therefore also be greater, providing a better transmission

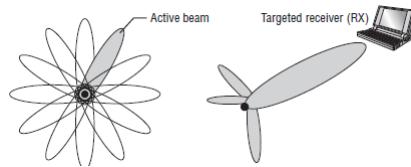
Static Beamforming

- Performed by using directional antennas to provide a fixed radiation pattern
 - Static beamforming uses multiple directional antennas, all clustered together but aimed away from a center point or location



Dynamic Beamforming

- Dynamic beamforming focuses the RF energy in a specific direction and in a particular shape
 - Like static beamforming, the direction and shape of the signal is focused
 - Unlike static beamforming, the radiation pattern of the signal can change on a frame-by-frame basis



Transmit Beamforming

- Transmit beamforming (TxBF) is performed by transmitting multiple phase-shifted signals with the hope and intention that they will arrive in-phase at the location where the transmitter believes that the receiver is located

Antenna Polarization

- As waves radiate from an antenna, the amplitude of the waves can oscillate either vertically or horizontally
 - ▣ It is important to have the polarization of the transmitting and receiving antennas oriented the same in order to receive the strongest possible signal
 - ▣ Polarization is not as important for indoor communications because the polarization of the RF signal often changes when it is reflected, which is a common occurrence indoors

Antenna Diversity

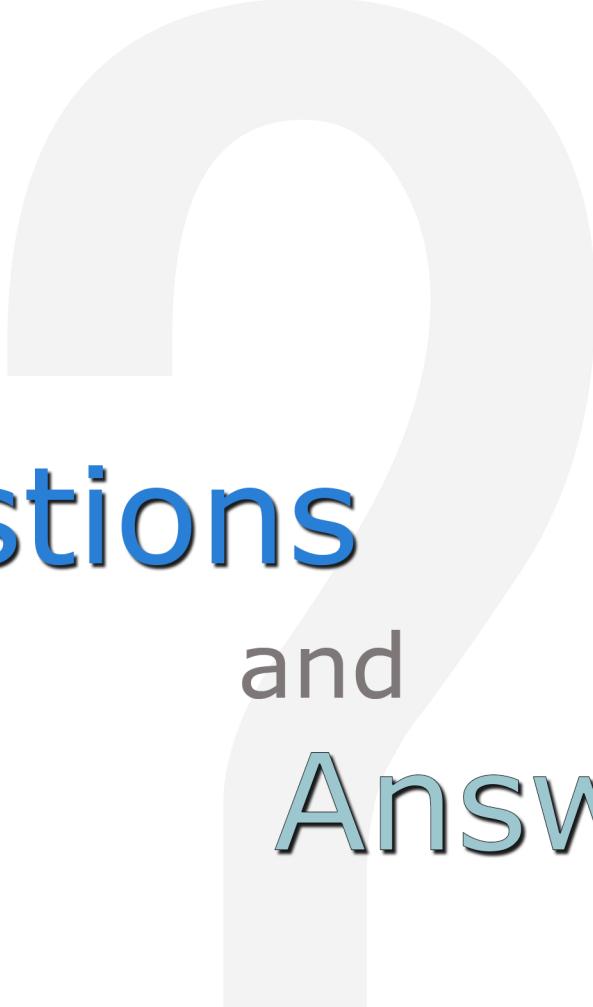
- ❑ Antenna diversity exists when an access point has two or more antennas with a receiver functioning together to minimize the negative effects of multipath
 - ❑ When the access point senses an RF signal, it compares the signal that it is receiving on both antennas and uses whichever antenna has the higher signal strength to receive the frame of data
 - ❑ This sampling is performed on a frame-by-frame basis, choosing whichever antenna has the higher signal strength
 - ❑ Called switched diversity, often seen before 802.11n

Multiple-Input, Multiple-Output

- Multiple-input, multiple-output (MIMO) is another, more sophisticated form of antenna diversity
 - Takes advantage of Multipath
 - Wireless radio architecture that can receive or transmit using multiple antennas concurrently
 - These techniques send data by using multiple simultaneous RF signals, and the receiver then reconstructs the data from those signals
 - 802.11n and 802.11ac radios use MIMO technology

Module Review

- Azimuth and elevation charts (antenna radiation envelopes)
- Omnidirectional antennas
- Semidirectional antennas
- Highly directional antennas
- Sector antennas
- Antenna arrays
- Static beamforming
- Dynamic beamforming
- Transmit beamforming



Questions and Answers

Review Questions:

1. Antenna manufacturers create _____ charts and elevation charts, commonly known as radiation patterns, for their antennas.
 - A. Azimuth
 - B. Relation
 - C. Kizmit
 - D. Distance

2. _____ is the measurement of how broad or narrow the focus of an antenna is.
 - A. Radiation envelopes
 - B. Static beamforming
 - C. Transmit beamforming
 - D. Beamwidth

3. _____ antennas radiate RF signals in all directions.
 - A. Omnidirectional
 - B. Semidirectional
 - C. Patch antenna
 - D. Highly directional

4. _____ antennas are designed to direct a signal in a specific direction.
 - A. Patch
 - B. Omnidirectional
 - C. Semidirectional
 - D. Planar

5. True or False: A Yagi antenna is typically used for long range distance communications of up to about 5 miles, although high-gain Yagi antennas can be used for longer distances.
 - A. True
 - B. False

Answer Key:

1. A
Antenna manufacturers create azimuth charts and elevation charts, commonly known as radiation patterns, for their antennas.
2. D
Beamwidth is the measurement of how broad or narrow the focus of an antenna is.
3. A
Omnidirectional antennas radiate RF signals in all directions.
4. C
Semidirectional antennas are designed to direct a signal in a specific direction.
5. B
False. A Yagi antenna is typically used for short to medium-distance point-to-point communications of up to about 2 miles, although high-gain Yagi antennas can be used for longer distances.

Certified Wireless Network Administrator
Module 05 – IEEE 802.11

WORKBOOK

Module Introduction

- ❑ Original IEEE 802.11 standard
 - ❑ IEEE 802.11-2007 ratified amendments
 - ❑ IEEE 802.11-2012 ratified amendments
 - ❑ Post-2012 ratified amendments
 - ❑ IEEE 802.11 draft amendments

Original IEEE 802.11 Standard

- The IEEE specifically defines 802.11 technologies at the Physical layer and the MAC sublayer of the Data-Link layer
 - Infrared (IR) technology uses a light-based medium. Although an infrared medium was indeed defined in the original 802.11 standard, the implementation is obsolete
 - Frequency Hopping Spread Spectrum (FHSS) radio frequency signals can be defined as narrowband signals or as spread spectrum signals
 - An RF signal is considered spread spectrum when the bandwidth is wider than what is required to carry the data
 - Direct Sequence Spread Spectrum (DSSS) is another spread spectrum technology that uses fixed channels

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*
 - The IEEE Std 802.11-2007 document included the following:
 - IEEE Std 802.11-1999 (R2003)
 - IEEE Std 802.11a-1999
 - IEEE Std 802.11b-1999
 - IEEE Std 802.11g-2003
 - IEEE Std 802.11i-2004

802.11b

- 802.11b is *High-Rate DSSS (HR-DSSS)*
 - The frequency space in which 802.11b radio cards can operate is the unlicensed 2.4 GHz to 2.4835 GHz ISM band

802.11a

- 802.11 technologies would operate in the 5 GHz frequency space using an RF technology called *Orthogonal Frequency Division Multiplexing (OFDM)*
- 802.11a radios initially were meant to transmit in three different 100 MHz unlicensed frequency bands in the 5 GHz range

802.11a (Cont.)

- These three bands are called:
 - *Unlicensed National Information Infrastructure (U-NII)* frequency bands
 - A total of 12 channels are available

802.11g

- Used a new technology called *Extended Rate Physical* (ERP) but were still meant to transmit in the 2.4 GHz to 2.4835 GHz ISM Frequency band
 - Data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps are possible using this technology
 - Although once again the IEEE requires only the data rates of 6, 12, and 24 Mbps To maintain backward compatibility

802.11 Review

	802.11 legacy	802.11b	802.11g	802.11a
Frequency	2.4 GHz ISM band	2.4 GHz ISM band	2.4 GHz ISM band	5 GHz U-NII-1, U-NII-2, and U-NII-3 bands
Spread spectrum technology	FHSS or DSSS	HR-DSSS	ERP: ERP-OFDM and ERP-DSSS/CCK are mandatory. PBCC is optional.	OFDM
Data rates	1, 2 Mbps	DSSS: 1, 2 Mbps HR-DSSS: 5.5 and 11 Mbps	ERP-DSSS/CCK: 1, 2, 5.5, and 11 Mbps	6, 12, and 24 Mbps are mandatory. ERP-OFDM: 6, 12, and 24 Mbps are mandatory. Also supported are 9, 18, 36, 48, and 54 Mbps. ERP-PBCC: 22 and 33 Mbps
Backward compatibility	N/A	802.11 DSSS only	802.11b HR-DSSS and 802.11 DSSS	None
Ratified	1997	1999	2003	1999

802.11i

- From 1997 to 2004, not much was defined in terms of security in the original 802.11 standard
 - Three key components of any wireless security solution are:
 - Data privacy (encryption)
 - Data integrity (protection from modification)
 - Authentication (identity verification)
 - For seven years, the only defined method of encryption in an 802.11 network was the use of 64-bit static encryption called Wired Equivalent Privacy (WEP)

802.11i (Cont.)

- The 802.11i amendment defined a Robust Security Network (RSN)
 - The intended goal of an RSN was to better hide the data flying through the air while at the same time placing a bigger guard at the front door

802.11i (Cont.)

- ❑ Data Privacy Confidentiality needs have been addressed in 802.11i with the use of a stronger encryption method called Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
 - ❑ This uses the Advanced Encryption Standard (AES) algorithm
 - ❑ Often abbreviated as CCMP/AES, AES CCMP, or often just CCMP
 - ❑ Authentication 802.11i defines two methods of authentication using either an IEEE 802.1X authorization framework or preshared keys (PSKs)
 - ❑ An 802.1X solution requires the use of an Extensible Authentication Protocol (EAP)
 - ❑ The 802.11i amendment does not specify what EAP method to use
 - ❑ Robust Security Network (RSN) defines the entire method of establishing authentication, negotiating security associations, and dynamically generating encryption keys for client stations and access points

802.11r-2008

- ❑ The technology is more often referred to as 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)
 - ❑ Under 802.11r, a client station is able to establish a QoS stream and set up a security association with a new access point in an efficient manner that allows bypassing 802.1X authentication when roaming to a new access point
 - From 700ms to 100ms

802.11w

- The goal of the IEEE Task Group (TGw) was to provide a way of delivering management frames in a secure manner
 - Preventing the management frames from being able to be spoofed
 - These 802.11w frames are referred to as robust management frames
 - Robust management frames can be protected by the management frame protection service and include disassociation, deauthentication, and robust action frames

802.11n

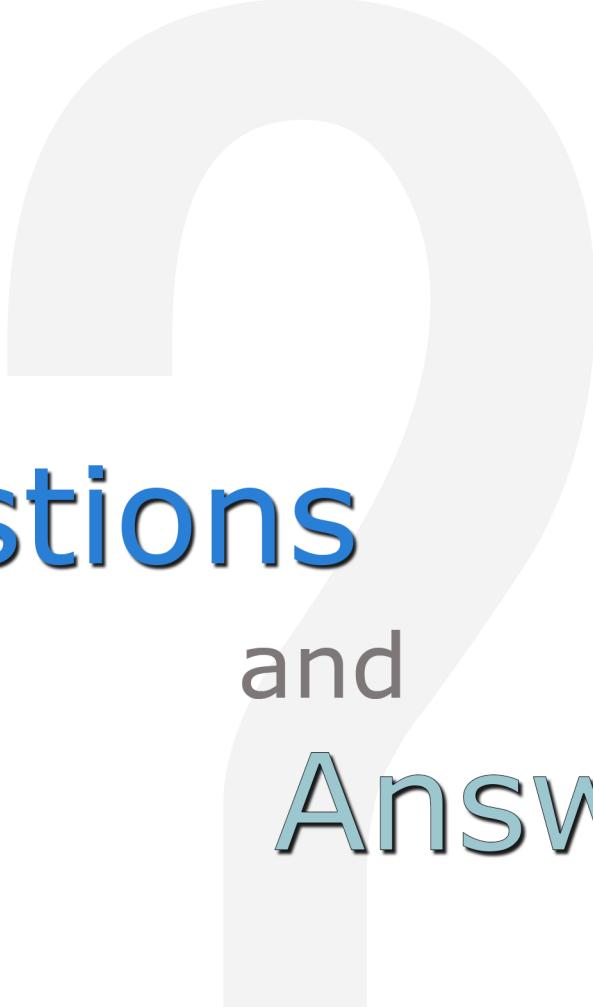
- The 802.11n- 2009 amendment defines a new operation known as *High Throughput (HT)*
 - This provides PHY and MAC enhancements to support data rates of up to 600 Mbps and therefore aggregate throughput above 100 Mbps

802.11ac

- ❑ The 802.11ac-2013 amendment defines Very High Throughput (VHT) enhancements
 - ❑ 6 GHz. The technology will only be used in the 5 GHz frequency bands where 802.11a/n radios already operate
 - ❑ Wider Channels 802.11n introduced the capability of 40 MHz channels, which effectively doubled the data rates
 - ❑ 802.11ac brings us the capability of 80 MHz and 160 MHz channels
 - ❑ This is the main reason that enterprise 802.11ac radios will operate at 5 GHz as opposed to the 2.4 GHz ISM band

Module Review

- ❑ Original IEEE 802.11 standard
 - ❑ IEEE 802.11-2007 ratified amendments
 - ❑ IEEE 802.11-2012 ratified amendments
 - ❑ Post-2012 ratified amendments
 - ❑ IEEE 802.11 draft amendments



Questions and Answers

Review Questions:

1. The IEEE specifically defines 802.11 technologies at the _____ layer and the MAC sublayer of the Data-Link layer.
 - A. Network
 - B. Transport
 - C. Physical
 - D. Session

2. True or False: The frequency space in which 802.11b radio cards can operate is the unlicensed 5 GHz to 5.4835 GHz ISM band.
 - A. True
 - B. False

3. True or False: 802.11g used a new technology called Extended Rate Physical (ERP) but was still meant to transmit in the 2.4 GHz to 2.4835 GHz ISM frequency band.
 - A. True
 - B. False

4. 802.11g has a maximum transmission rate of _____ Mbps when using (ERP) technology.
 - A. 12
 - B. 24
 - C. 120
 - D. 54

5. True or False: The 802.11i amendment defined a Robust Security Network (RSN) that was intended to better hide the data flying through the air while at the same time placing a bigger guard at the front door.
 - A. True
 - B. False

Answer Key:

1. C
The IEEE specifically defines 802.11 technologies at the Physical layer and the MAC sublayer of the Data-Link layer.
2. B
False. The frequency space in which 802.11b radio cards can operate is the unlicensed 2.4 GHz to 2.4835 GHz ISM band.
3. A
True. 802.11g used a new technology called Extended Rate Physical (ERP) but was still meant to transmit in the 2.4 GHz to 2.4835 GHz ISM frequency band.
4. D
802.11g has data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps that are possible when using (ERP) technology.
5. A
True. The 802.11i amendment defined a Robust Security Network (RSN) that was intended to better hide the data flying through the air while at the same time placing a bigger guard at the front door.

Certified Wireless Network Administrator
Module 06 – Spread Spectrum
Technologies

WORKBOOK

Module Introduction

- ❑ Industrial, Scientific, and Medical bands (ISM)
 - ❑ Unlicensed National Information Infrastructure bands (U-NII)
 - ❑ Narrowband and spread spectrum
 - ❑ Frequency hopping spread spectrum (FHSS)
 - ❑ Direct sequence spread spectrum (DSSS)
 - ❑ Orthogonal Frequency Division Multiplexing (OFDM)
 - ❑ 2.4 GHz channels
 - ❑ 5 GHz channels
 - ❑ Adjacent, nonadjacent, and overlapping channels
 - ❑ Throughput vs. bandwidth

Industrial, Scientific, and Medical Bands

- The IEEE 802.11 standard and the subsequent 802.11b, 802.11g, and 802.11n amendments all define communications in the frequency range between 2.4 GHz and 2.4835 GHz
- The frequency ranges of the ISM bands are as follows:
 - 902 MHz – 928 MHz (26 MHz wide)
 - 2.4 GHz – 2.5 GHz (100 MHz wide)
 - 5.725 GHz – 5.875 GHz (150 MHz wide)
- The 900 MHz band is known as the industrial band, the 2.4 GHz band is known as the scientific band, and the 5.8 GHz band is known as the medical band

900 MHz

- The 900 MHz ISM band is 26 MHz wide and spans from 902 MHz to 928 MHz
 - A factor limiting the use of the 900 MHz ISM band is that in many parts of the world, part of the 900 MHz frequency range has already been allocated to the Global System for Mobile Communications (GSM)

2.4 GHz

- ❑ The 2.4 GHz ISM band is the most common band used for wireless networking communications
 - ❑ The 2.4 GHz ISM band is 100 MHz wide and spans from 2.4 GHz to 2.5 GHz
 - ❑ The following wireless radios use this band:
 - ❑ 802.11 (FHSS radios or DSSS radios)
 - ❑ 802.11b (HR-DSSS radios)
 - ❑ 802.11g (ERP radios)
 - ❑ 802.11n (HT radios)
 - ❑ Also used by microwave ovens, cordless home telephones, baby monitors, and wireless video cameras

5.0 GHz

- The 5.8 GHz ISM band is 150 MHz wide and spans from 5.725 GHz to 5.875 GHz
 - Used by many of the same types of consumer products:
 - Baby monitors
 - Cordless telephones
 - Cameras

Unlicensed National Information Infrastructure Bands

- ❑ The IEEE 802.11a amendment designated WLAN transmissions within the frequency space of the three 5 GHz bands, each with four channels
 - ❑ These frequency ranges are known as:
 - ❑ Unlicensed National Information Infrastructure (U-NII) bands
 - ❑ There are three groupings:
 - ❑ Lower
 - ❑ Middle
 - ❑ Upper
 - U-NII-1 (lower)
 - U-NII-2 (middle)
 - U-NII-3 (upper)
 - 802.11a (OFDM radios)
 - 802.11n (HT radios)
 - 802.11ac (VHT radios)

U-NII Review

Band	Frequency	Channels
U-NII-1	5.15 GHz – 5.25 GHz	4 channels
U-NII-2	5.25 GHZ – 5.35 GHz	4 channels
U-NII-2 Extended	5.47 GHZ – 5.725 GHz	12 channels*
U-NII-3	5.725 GHz – 5.85 GHz	5 channels

60 GHz

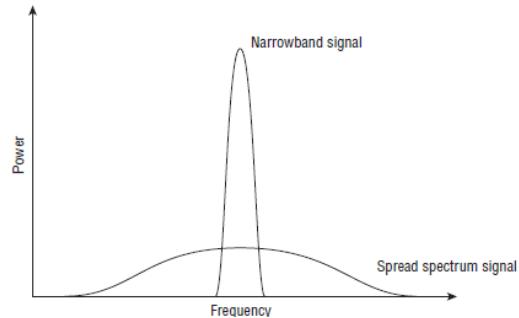
- Very High Throughput (VHT) technology that will operate in the unlicensed 60 GHz frequency band
 - New PHY and MAC layer enhancements have the potential of accomplishing speeds of future Wi-Fi frequencies
 - Up to 7 Gbps
 - Since these ultrahigh frequencies have difficulty penetrating through walls, the technology will most likely be used to provide bandwidth-intensive and short distance communications indoors

Narrowband and Spread Spectrum

- There are two primary radio frequency (RF) transmission methods:
 - Narrowband
 - Uses very little bandwidth to transmit the data that it is carrying
 - Example: a narrowband radio might transmit data on 2 MHz of frequency space at 80 watts
 - Spread spectrum
 - Uses more bandwidth than is necessary to carry its data
 - Takes the data that is to be transmitted and spreads it across the frequencies that it is using
 - Example: a spread spectrum radio might transmit data over a 22 MHz frequency space at 100 milliwatts

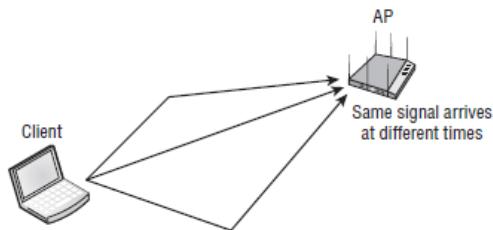
Narrowband and Spread Spectrum

- Typically, the FCC or other local regulatory bodies require that narrowband transmitters be licensed to minimize the risk of two narrowband transmitters interfering with each other
- AM and FM radio stations are examples of narrowband transmitters



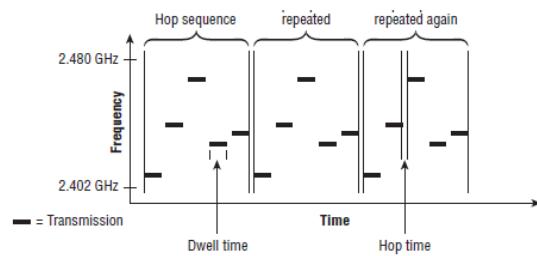
Multipath Interference

- One of the problems that can occur with RF communications is multipath interference
 - Multipath occurs when a reflected signal arrives at the receiving antenna after the primary signal



Frequency Hopping Spread Spectrum

- ❑ Generally, the way 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

- FHSS radios use a predefined hopping sequence (also called a hopping pattern or hopping set)
 - This comprises a series of small carrier frequencies, or hops
 - Instead of transmitting on one set channel or finite frequency space, an FHSS radio transmits on a sequence of subchannels called hops

Dwell Time

- Dwell time is a defined amount of time that the FHSS system transmits on a specific Frequency before it switches to the next frequency in the hop set
 - The FCC specifies a maximum dwell Time of 400 milliseconds (ms) per carrier frequency during any 30-second period of time
 - Typical dwell times are around 100 ms to 200 ms
 - The IEEE 802.11 standard specifies that A hopping sequence must consist of at least 75 frequencies, 1 MHz wide

Hop Time

- Hop time is 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
- Hop time is typically a fairly small number, often about 200 to 300 microseconds (μs)

Direct Sequence Spread Spectrum

- Direct Sequence Spread Spectrum (DSSS) was originally specified in the primary, or root, 802.11 standard and provides 1 and 2 Mbps RF communications using the 2.4 GHz ISM band
 - 802.11b addendum and provides 5.5 and 11 Mbps RF communications using the same 2.4 GHz ISM band
 - The 802.11b 5.5 and 11 Mbps speeds are known as High-Rate DSSS (HR-DSSS)
 - DSSS is set to one channel
 - The data that is being transmitted is spread across the range of frequencies that make up the channel

Direct Sequence Spread Spectrum (Cont.)

- The task of adding additional, redundant information to the data is known as processing gain
 - In this day and age of data compression, it seems strange that we would use a technology that adds data to our transmission, but by doing so, the communication is more resistant to data corruption
 - The system converts the 1 bit of data into a series of bits that are referred to as chips
 - To create the chips, a Boolean XOR is performed on the data bit and a fixed-length bit sequence pseudorandom number (PN) code
 - Using a PN code known as the Barker code, the binary data 1 and 0 are represented by the following chip sequences:
 - Binary data 1 = 1 0 1 1 0 1 1 1 0 0 0
 - Binary data 0 = 0 1 0 0 1 0 0 0 1 1 1

Direct Sequence Spread Spectrum (Cont.)

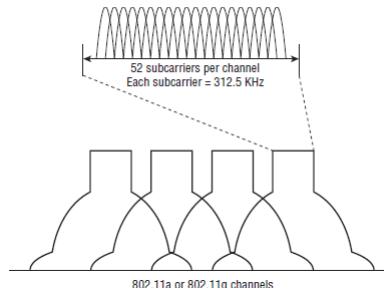
- This sequence of chips is then spread across a wider frequency space
 - Although 1 bit of data might need only 2 MHz of frequency space, the 11 chips will require 22 MHz of frequency carrier space
 - This process of converting a single data bit into a sequence is often called spreading or chipping
 - 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

Direct Sequence Spread Spectrum (Cont.)

- After the data has been encoded using a chipping method, the transmitter needs to modulate the signal to create a carrier signal containing the chips
 - Differential binary phase shift keying (DBPSK) utilizes two phase shifts, one that represents a 0 chip and another that represents a 1 chip
 - To provide faster throughput, differential quadrature phase shift keying (DQPSK) utilizes four phase shifts, allowing each of the four phase shifts to modulate 2 chips (00, 01, 10, 11) instead of just 1 chip, doubling the speed

Orthogonal Frequency Division Multiplexing

- Orthogonal Frequency Division Multiplexing (OFDM) is 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 to spread spectrum, such as low transmit power and using more bandwidth than is required to transmit data

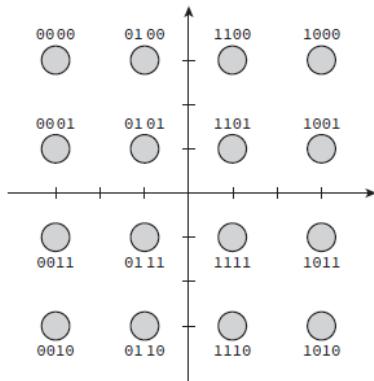


Orthogonal Frequency Division Multiplexing (Cont.)

- OFDM uses binary phase shift keying (BPSK) and quadrature phase shift keying (QPSK) phase modulation for the lower ODFM data rates
- The higher OFDM data rates use 16-QAM and 64-QAM modulation
 - Quadrature amplitude modulation (QAM) is a hybrid of phase and amplitude modulation

Orthogonal Frequency Division Multiplexing (Cont.)

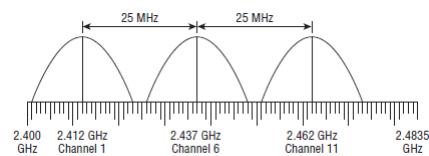
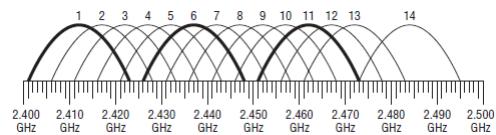
- ❑ A constellation diagram is divided into four quadrants, and different locations in each quadrant can be used to represent data bits
 - ❑ Areas on the quadrant relative to the horizontal axis can be used to represent various phase shifts



2.4 GHz

- The IEEE 802.11-2012 standard divides the 2.4 GHz ISM band into 14 separate channels
 - Channels are designated by their center frequency
 - How wide the channel is depends on the technology used by the 802.11 transmitter.
 - When DSSS and HR-DSSS 802.11 radios are transmitting, each channel is 22 MHz wide and is often referenced by the center frequency \pm 11 MHz
 - For example, channel 1 is 2.412 GHz \pm 11 MHz, which means that channel 1 spans from 2.401 GHz to 2.423 GHz. It should also be noted that within the 2.4 GHz ISM band, the distance between channel center frequencies is only 5 MHz. Because each channel is 22 MHz wide, and because the separation between center frequencies of each channel is only 5 MHz, the channels will have overlapping frequency space.
 - With the introduction of OFDM in 802.11a, along with its expanded use in 802.11g, 802.11n, and 802.11ac, the frequency width used by an OFDM channel is approximately 20 MHz

2.4 GHz (Cont.)



5.0 GHz

- ❑ 802.11a/n and 802.11ac radios transmit in the 5 GHz U-NII bands:
 - ❑ U-NII-1, U-NII-2, U-NII-2 Extended, and U-NII-3
 - To prevent interference with other possible bands, extra bandwidth is used as a guard
 - ❑ In the U-NII-1 and U-NII-2 bands, the centers of the outermost channels of each band must be 30 MHz from the band's edge
 - ❑ An extra 20 MHz of bandwidth exists in the U-NII-3 band

5.0 GHz (Cont.)

- 802.11n technology introduced the capability of bonding together 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

Adjacent, Nonadjacent, and Overlapping Channels

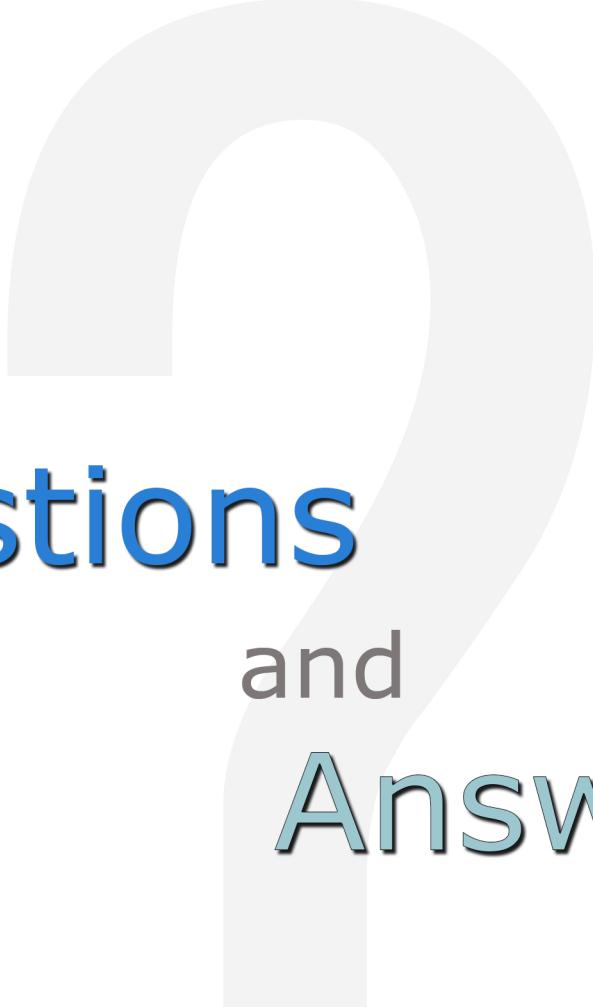
- When deploying a WLAN, it is important to have overlapping cell coverage for roaming to occur
 - However, it is just as important for these coverage cells not to have overlapping frequency space

Throughput vs. Bandwidth

- Wireless communication is typically performed within a constrained set of frequencies known as a frequency band
 - ▣ This frequency band is the bandwidth
 - ▣ Plays a part in the eventual throughput of the data
 - ▣ Do not confuse frequency bandwidth with data bandwidth
 - ▣ Changes in speed due to modulation and coding is known as data rates
 - Also often referred to as data bandwidth

Module Review

- Industrial, Scientific, and Medical bands (ISM)
- Unlicensed National Information Infrastructure bands (U-NII)
- Narrowband and spread spectrum
- Frequency hopping spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)
- 2.4 GHz channels
- 5 GHz channels
- Adjacent, nonadjacent, and overlapping channels
- Throughput vs. bandwidth



Questions and Answers

Review Questions:

1. True or False: The IEEE 802.11 standard and the subsequent 802.11b, 802.11g, and 802.11n amendments all define communications in the frequency range between 3.4 GHz and 3.4835 GHz.
 - A. True
 - B. False
2. True or False: The 2.4 GHz ISM band is the most common band used for wireless networking communications.
 - A. True
 - B. False
3. What two ISM bands are used by microwave ovens, cordless home telephones, baby monitors, and wireless video cameras? (Choose two)
 - A. 902 MHz
 - B. 2.4 GHz
 - C. 5.8 GHz
 - D. 7.6 GHz
4. _____ uses very little bandwidth to transmit the data that it is carrying.
 - A. Multipath Interference
 - B. Spread Spectrum
 - C. Hopping Sequence
 - D. Narrowband
5. _____ uses more bandwidth than is necessary to carry its data.
 - A. Narrowband
 - B. Spread Spectrum
 - C. Multipath Interference
 - D. Frequency Hopping

Answer Key:

1. B
False. The IEEE 802.11 standard and the subsequent 802.11b, 802.11g, and 802.11n amendments all define communications in the frequency range between 2.4 GHz and 2.4835 GHz.
2. A
True. The 2.4 GHz ISM band is the most common band used for wireless networking communications.
3. B, C
The 2.4 GHz and 5.8 GHz ISM bands are used by microwave ovens, cordless home telephones, baby monitors, and wireless video cameras.
4. D
Narrowband uses very little bandwidth to transmit the data that it is carrying.
5. B
Spread spectrum uses more bandwidth than is necessary to carry its data.

Certified Wireless Network Administrator
Module 07 – WLAN Topologies

WORKBOOK

Module Introduction

- Wireless networking topologies
- 802.11 topologies
- 802.11 configuration modes

Wireless Networking Topologies

- We've only talked about WLAN technologies but other wireless technologies are cellular, Bluetooth, and ZigBee
- All can be arranged into four major wireless topologies:
 - Wireless Wide Area Network (WWAN)
 - Wireless Metropolitan Area Network (WMAN)
 - Wireless Personal Area Network (WPAN)
 - Wireless Local Area Network (WLAN)

Wireless Wide Area Network (WWAN)

- ❑ A Wide Area Network (WAN) provides RF coverage over a vast geographical area
 - ❑ A WAN might traverse an entire state, region, or country or even span worldwide
 - ❑ A Wireless Wide Area Network (WWAN) also covers broad geographical boundaries but obviously uses a wireless medium instead of a wired medium
 - ❑ Cellular providers such as Sprint, Verizon, and Vodafone use a variety of competing technologies to carry data
 - ❑ Examples of these cellular technologies are:
 - General Packet Radio Service (GPRS)
 - Code Division Multiple Access (CDMA)
 - Time Division Multiple Access (TDMA)
 - Long Term Evolution (LTE)

Wireless Metropolitan Area Network (WMAN)

- A Wireless Metropolitan Area Network (WMAN) provides RF coverage to a metropolitan area such as a city and the surrounding suburbs
 - One wireless technology that is often associated with a WMAN is defined by the 802.16 standard
 - This standard defines broadband wireless access and is sometimes referred to as Worldwide Interoperability for Microwave Access (WiMAX)

Wireless Personal Area Network (WPAN)

- A Wireless Personal Area Network (WPAN) is a wireless computer network used for communication between computer devices within close proximity of a user.
- The most common technologies in WPANs are Bluetooth and infrared
 - Infrared is a light-based medium
 - Bluetooth is a radio-frequency medium that uses Frequency Hopping Spread Spectrum (FHSS) technology

Wireless Local Area Network (WLAN)

- Local Area Networks provide networking for a building or campus environment
 - The 802.11 wireless medium is a perfect fit for local area networking simply because of the range and speeds that are defined by the 802.11-2012 standard and future amendments
 - This makes up the majority of 802.11 wireless network deployments

802.11 Topologies

- The main component of an 802.11 wireless network is the radio, which is referred to by the 802.11 standard as a *station (STA)*
- 802.11 topologies are known as *service sets*:
 - basic service set (BSS)
 - extended service set (ESS)
 - independent basic service set (IBSS)
 - mesh basic service set (MBSS)
- Think about duplex settings

Access Points

- ❑ A wired infrastructure device typically associated with half-duplex communications is an Ethernet hub
 - ❑ A wired hub is effectively a shared medium in which only one host device can transmit data at a time
 - ❑ The original CWNP definition of an access point (AP) was a half-duplex device with switch-like intelligence
 - ❑ That definition can still be used to characterize autonomous access points and cooperative access points
 - ❑ The best example of switch-like intelligence used by access points or WLAN controllers is the ability to address and direct wireless traffic at layer 2
 - ❑ The upper-layer information that is contained in the body of an 802.11 wireless data frame is called a MAC Service Data Unit (MSDU)

Distribution Service

- The 802.11-2012 standard also defines a distribution system (DS) that is used to interconnect a set of basic service sets (BSSs) via integrated LANs to create an extended service set (ESS)
 - A logical physical medium used to connect access points is known as a distribution system medium (DSM)
 - The distribution system services (DSS) provide the switch-like intelligence

SSID

- The service set identifier (SSID) is a logical name used to identify an 802.11 wireless network
 - The SSID wireless network name is comparable to a Windows workgroup name
 - Most access points have the ability to cloak an SSID and keep the network name hidden from illegitimate end users.
 - Hiding the SSID is a very weak attempt at security

BSS

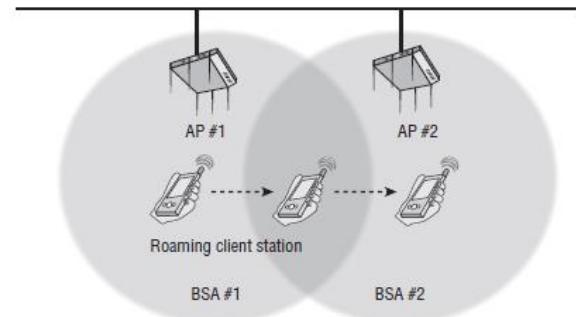
- The Basic Service Set (BSS) is the cornerstone topology of an 802.11 network
 - The communicating devices that make up a BSS consist of one AP radio with one or more client stations



ESS

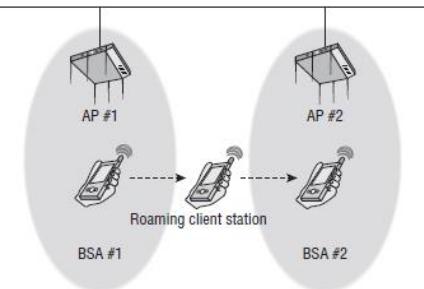
- An Extended Service Set is two or more basic service sets connected by a Distribution System Medium
 - Usually an ESS is a collection of multiple access points and their associated client stations, all united by a single DSM
 - The most common example of an ESS has access points with partially overlapping coverage cells

ESS (Cont.)



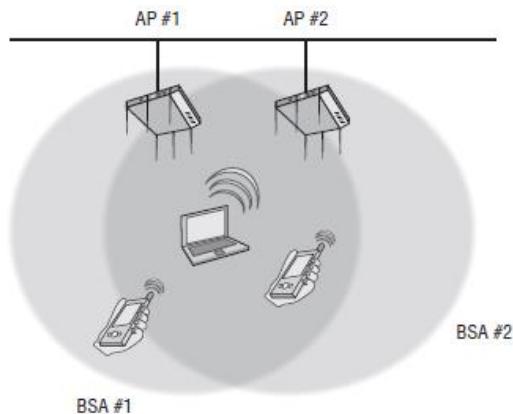
Roaming

- Although seamless roaming is usually a key aspect of WLAN design, there is no requirement for an ESS to guarantee uninterrupted communications

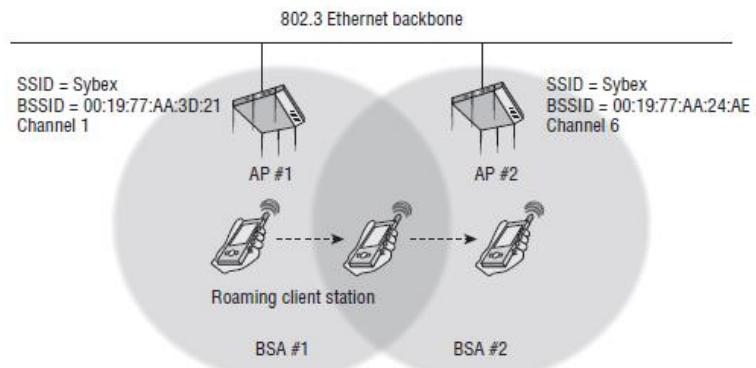


Roaming (Cont.)

□ Co-location



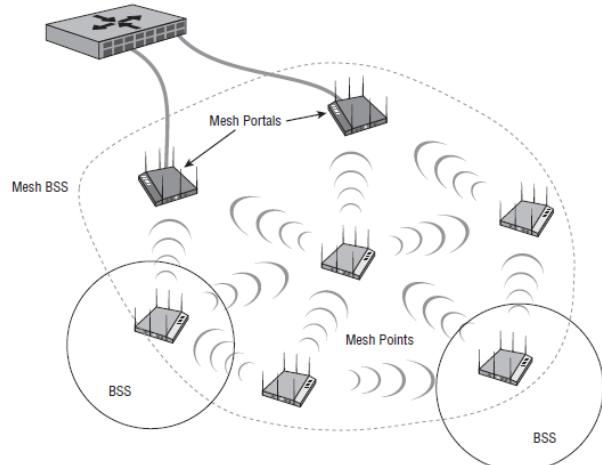
Roaming (Cont.)



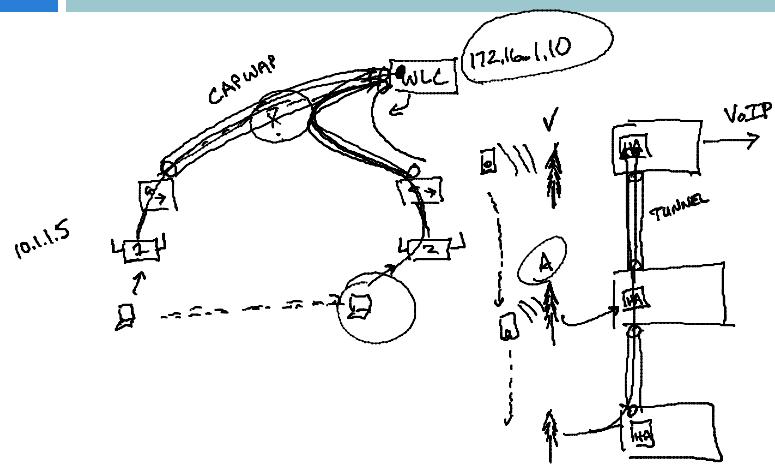
Mesh BSS

- A Hybrid Wireless Mesh Protocol (HWMP) is defined as the Default Path Selection Protocol for an MBSS
 - ▣ HWMP is both proactive and reactive and is effectively a dynamic layer 2 routing protocol

Mesh BSS (Cont.)



WLC Roaming (eNotes)



Access Point Modes

- Bridge Mode
 - Converted into a wireless bridge
 - Adds extra MAC-layer intelligence to the device and gives the AP the capability to learn and maintain tables about MAC addresses from the wired side of the network
 - Workgroup Bridge Mode
 - Transformed into a workgroup bridge, providing wireless backhaul for connected 802.3 wired clients
 - Repeater Mode
 - Performs as a repeater AP which extends the coverage area of a portal AP on the same channel
 - Mesh Mode
 - Operates as a wireless backhaul radio for a mesh environment
 - The backhaul radio may also allow for client access
 - Scanner Mode
 - Converted into a sensor radio, allowing integration into a Wireless Intrusion Detection System (WIDS) architecture
 - In a continuous listening state while hopping between multiple channels
 - Often referred to as monitor mode

Client Station Modes

- ☐ May operate in one of two states
 - ☐ The default mode for an 802.11 client radio is typically infrastructure mode
 - ☐ When running in Infrastructure mode, the client station will allow communication via an access point

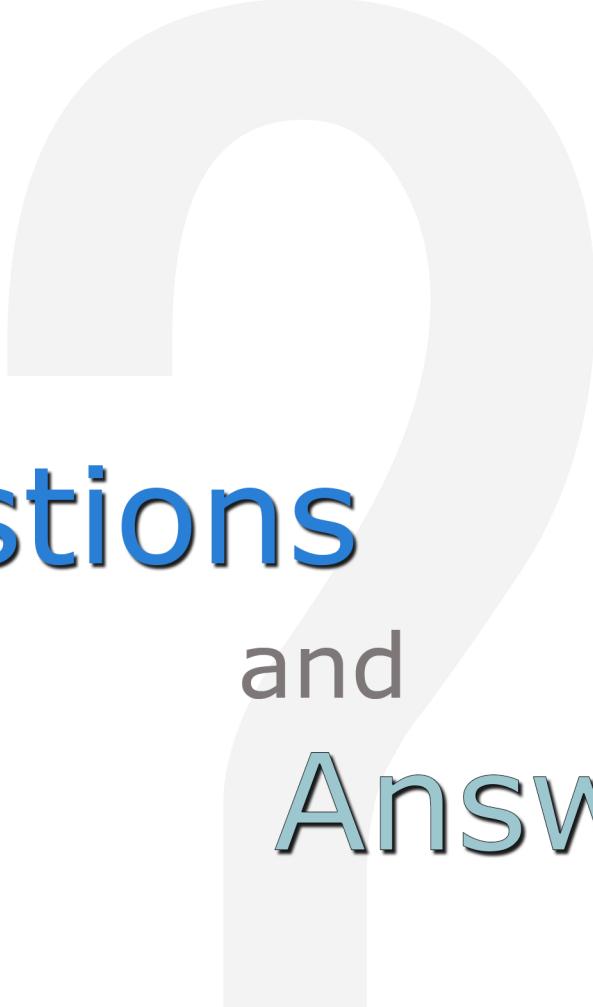


Client Station Modes (Cont.)

- The second client station mode is called Ad Hoc mode
 - Other vendors may refer to this as Peer-to-Peer mode
 - 802.11 client stations set to Ad Hoc mode participate in an IBSS topology and do not communicate via an access point
 - All station transmissions and frame exchanges are peer-to-peer

Module Review

- Wireless networking topologies
- 802.11 topologies
- 802.11 configuration modes



Questions and Answers

Review Questions:

1. Which of the following is a type of wireless topology? (Choose two)
 - A. Wireless World Area Network (WWAN)
 - B. Wireless Metropolitan Area Network (WMAN)
 - C. Wireless Perimeter Area Network (WPAN)
 - D. Wireless Local Area Network (WLAN)
2. True or False: A Wide Area Network (WAN) provides RF coverage over a vast geographical area.
 - A. True
 - B. False
3. True or False: One wireless technology that is often associated with a WMAN is defined by the 802.13 standard.
 - A. True
 - B. False
4. The most common technologies in WPANs are _____ and _____. (Choose two)
 - A. Bluetooth
 - B. Cellular
 - C. Infrared
 - D. WiMAX
5. True or False: Most access points have the ability to cloak an SSID and keep the network name hidden from illegitimate end users.
 - A. True
 - B. False

Answer Key:

1. B, D
Wireless Metropolitan Area Network (WMAN) and Wireless Local Area Network (WLAN) are two types of wireless topologies.
2. A
True. A Wide Area Network (WAN) provides RF coverage over a vast geographical area.
3. B
False. One wireless technology that is often associated with a WMAN is defined by the 802.16 standard.
4. A, C
The most common technologies in WPANs are bluetooth and infrared.
5. A
True. Most access points have the ability to cloak an SSID and keep the network name hidden from illegitimate end users.

Certified Wireless Network Administrator
Module 08 – Wi-Fi Access

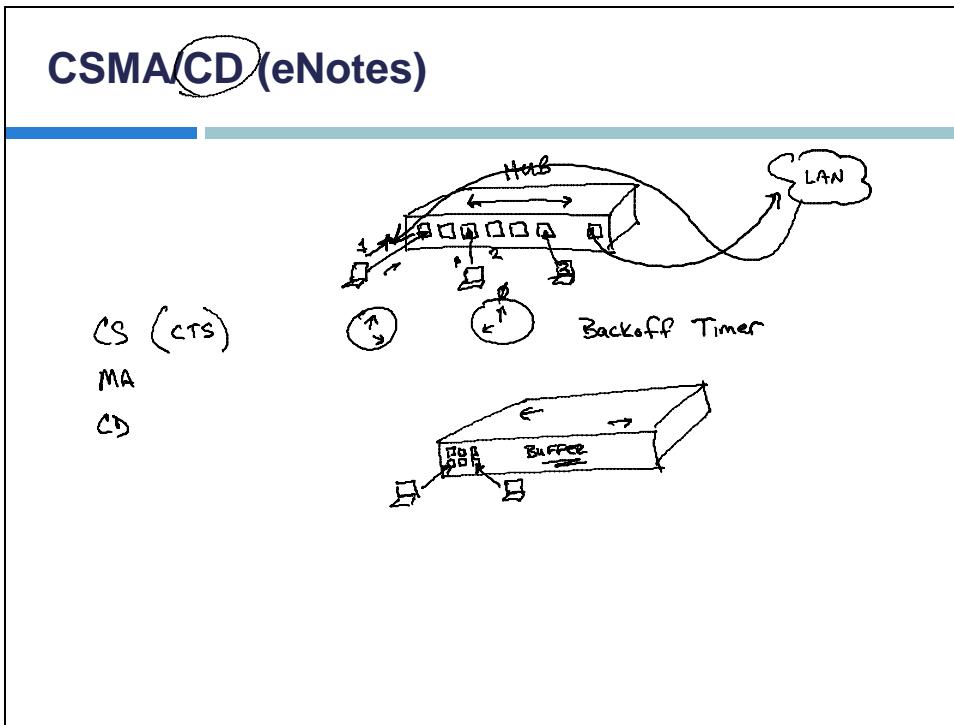
WORKBOOK

Module Introduction

- CSMA/CA vs. CSMA/CD
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- Hybrid Coordination Function (HCF)
- Block acknowledgment (BA)
- Wi-Fi Multimedia (WMM)
- Airtime Fairness

CSMA/CA vs. CSMA/CD

- Network communication requires a set of rules to provide controlled and efficient access to the network medium
 - ▣ Media Access Control (MAC) is the generic term used when discussing the general concept of access
- Two forms of contention that are heavily used in today's networks are
 - ▣ Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
 - ▣ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

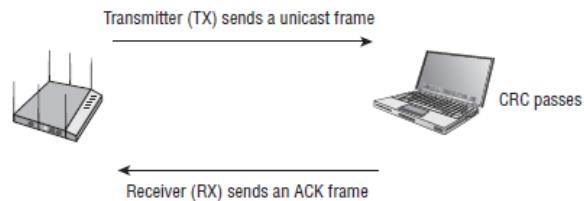


CSMA/CA

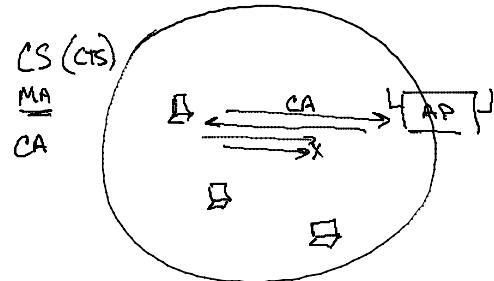
- ❑ CSMA/CA is a process used to ensure that only one 802.11 radio is transmitting at a time
 - ❑ The IEEE 802.11-2012 standard defines a function called Distributed Coordination Function (DCF)
 - ❑ Medium access method that utilizes multiple checks and balances to try to minimize collisions
 - ❑ This process does not specifically determine whether a collision occurs
 - ❑ In other words, there is no collision detection
 - ❑ However, if an ACK frame is not received by the original radio, there is collision assumption

CSMA/CA (Cont.)

- Distributed Coordination Function (DCF) is the fundamental access method of 802.11 communications
 - ▣ DCF is the mandatory access method of the 802.11 standard



CSMA/CA (eNotes)



Distributed Coordination Function

- Distributed Coordination Function (DCF) is the fundamental access method of 802.11 communications
 - ▣ DCF is the mandatory access method of the 802.11 standard
- The 802.11 standard also has an optional access method known as Point Coordination Function
- Hybrid Coordination Function (HCF) has also been added

Distributed Coordination Function (Cont.)

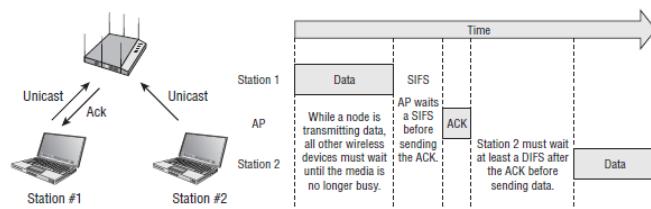
- Some of the components that are part of the CSMA/CA process
- Here are the four main components of DCF:
 - Interframe Space
 - Duration/ID Field
 - Carrier Sense
 - Random Backoff Timer
- Think of these four components as checks and balances that work together at the same time to ensure that only one 802.11 radio is transmitting on the half-duplex medium

Interframe Space (IFS)

- Interframe Space (IFS) is a period of time that exists between transmissions of wireless frames
- There are six types of interframe spaces, which are listed here in order of shortest to longest:
 - 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

SIFS/DIFS

- As an example, only ACK frames, block ACK frames, data frames, and clear-to-send (CTS) frames may follow a SIFS
- The two most common interframe spaces used are the SIFS and the DIFS

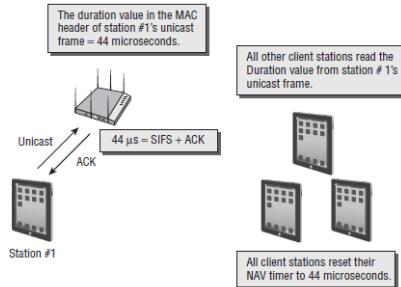


SIFS/DIFS (Cont.)

- When a client transmits a unicast frame, the Duration/ID field contains a value from 0 to 32,767
 - ▣ This 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

Carrier Sense

- Virtual carrier sense uses a timer mechanism known as the network allocation vector (NAV)
 - The NAV timer maintains a prediction of future traffic on the medium based on Duration value information seen in a previous frame transmission



Carrier Sense (Cont.)

- Physical carrier sense has two purposes:
 - To 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
 - To determine whether the medium is busy before transmitting
 - This is known as the clear channel assessment (CCA)
 - The CCA involves listening for RF transmissions at the Physical layer
 - The medium must be clear before a station can transmit

Carrier Sense (Cont.)

- ❑ An OFDM station selects a random number from a contention window of 0–15
 - ❑ For this example, the number chosen is 4
 - ❑ The station multiplies the random number of 4 by a slot time of 9 μ s
 - ❑ The random backoff timer has a value of 36 μ s (4 slots)
 - ❑ For every slot time during which there is no medium activity, the backoff time is decremented by a slot time
 - ❑ The station decrements the backoff timer until the timer is zero
 - ❑ The station transmits if the medium is clear

Point Coordination Function (PCF)

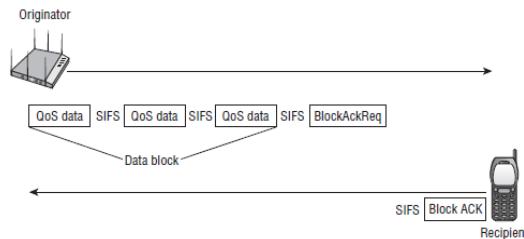
- This access method is a form of polling
 - The AP performs the function of the Point Coordinator (PC) because the AP is taking on this role
 - PCF medium access method will work in only a Basic Service Set (BSS)

Block Acknowledgment

- ❑ The 802.11e amendment also introduced a Block Acknowledgment (BA) mechanism that is defined in the 802.11-2012 standard
 - ❑ Block ACK improves channel efficiency by aggregating several acknowledgments into one single acknowledgment frame
 - ❑ Two types of Block ACK mechanisms:
 - ❑ Immediate
 - Designed for use with low-latency traffic
 - ❑ Delayed
 - More suitable for latency-tolerant traffic

Block Acknowledgment

- An originator station sends a block of QoS data frames to a recipient station
 - The originator requests acknowledgment of all the QoS data frames by sending a BlockAckReq frame
 - Instead of acknowledging each unicast frame independently, the block of QoS data frames are all acknowledged by a single Block ACK

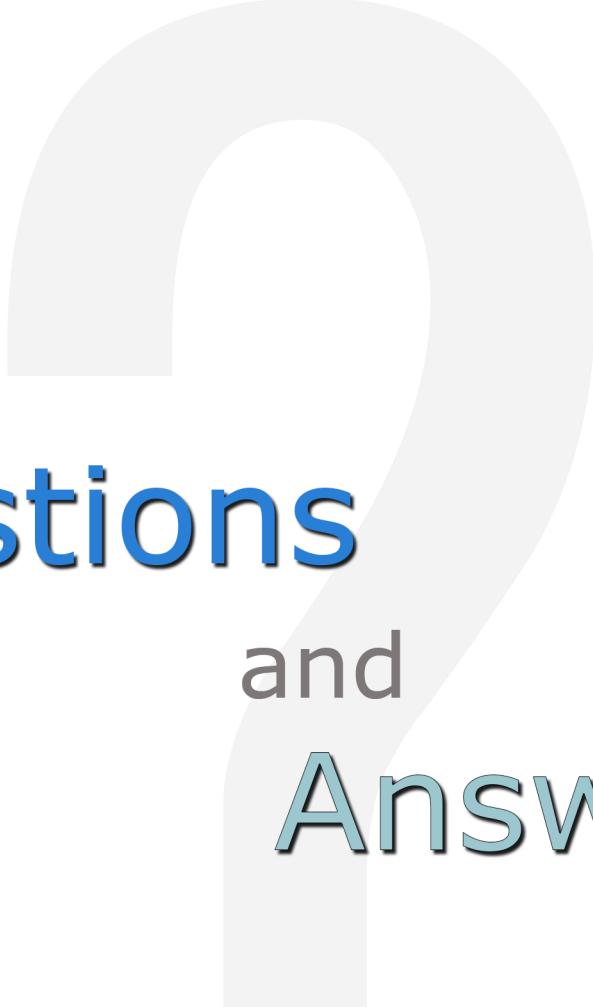


Airtime Fairness

- ❑ One of the important features of 802.11 is its ability to support many different data rates
 - ❑ Allows older technologies to still communicate alongside newer devices, along with enabling devices to maintain communications by shifting to slower data rates as they move away from an access point
 - ❑ The ability to use these slower data rates is paramount to 802.11 communications
 - ❑ It can also be a huge hindrance to the overall performance of the network and to individual devices operating at faster data rates
 - ❑ Instead of allocating equal access to the network between devices, the goal of airtime fairness is to allocate equal time, as opposed to equal opportunity

Module Review

- CSMA/CA vs. CSMA/CD
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- Hybrid Coordination Function (HCF)
- Block acknowledgment (BA)
- Wi-Fi Multimedia (WMM)
- Airtime Fairness



Questions and Answers

Review Questions:

1. True or False: Network communication requires a set of rules to provide controlled and efficient access to the network medium.
 - A. True
 - B. False

2. _____ and _____ are two forms of contention that are heavily used in today's networks. (Choose two)
 - A. Carrier Sense Multiple Access with Collision Detection (CSMA \ CD)
 - B. Carrier Sense Minimal Access with Collision Acceptance (CSMA \ CA)
 - C. Carrier Sense Minimal Access with Collision Division (CSMA \ CD)
 - D. Carrier Sense Multiple Access with Collision Avoidance (CSMA \ CA)

3. True or False: The 802.11 standard also has an optional access method known as Point Coordination Function.
 - A. True
 - B. False

4. _____ is a period of time that exists between transmissions of wireless frames.
 - A. Interframe Space
 - B. Distributed Coordination
 - C. Carrier Sense
 - D. Point Coordination Function

5. True or False: One of the important features of 802.11 is its ability to support many different data rates.
 - A. True
 - B. False

Answer Key:

1. A
True. Network communication requires a set of rules to provide controlled and efficient access to the network medium.
2. A, D
Carrier Sense Multiple Access with Collision Detection (CSMA \ CD) and Carrier Sense Multiple Access with Collision Avoidance (CSMA \ CA) are two forms of contention that are heavily used in today's networks.
3. A
True. The 802.11 standard also has an optional access method known as Point Coordination Function.
4. A
Interframe Space (IFS) is a period of time that exists between transmissions of wireless frames.
5. A
True. One of the important features of 802.11 is its ability to support many different data rates.

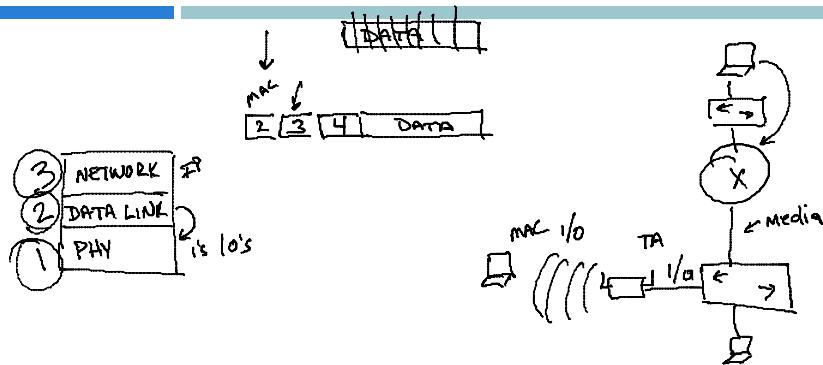
Certified Wireless Network Administrator
Module 09 – MAC Architecture

WORKBOOK

Module Introduction

- Packets, frames, and bits
 - Data-Link layer
 - Physical layer
 - 802.11 and 802.3 interoperability
 - Three 802.11 frame types
 - Beacon management frame (beacon)
 - Passive scanning
 - Active scanning
 - Authentication
 - Association
 - Authentication and association states
 - Basic and supported rates

Packets, Frames, and Bits (eNotes)



Data-Link Layer

- The 802.11 Data-Link Layer is divided into two sublayers
 - The upper portion is the IEEE 802.2 Logical Link Control (LLC) sublayer
 - Identical for all 802 based networks, although it is not used by all IEEE 802 networks
 - The bottom portion of the Data-Link Layer is the Media Access Control (MAC) sublayer
 - The 802.11 standard defines operations at the MAC sublayer

MAC

- When the LLC sublayer sends the MSDU to the MAC sublayer, the MAC header information is added to the MSDU to identify it
 - The MSDU is now encapsulated in a MAC Protocol Data Unit (MPDU)
 - A simple definition of an 802.11 MPDU is that it is an 802.11 frame
 - MAC Header Frame control information, duration information, MAC addressing, and sequence control information are all found in the MAC header
 - Frame Body
 - This component can be variable in size and contains information that is different depending on the frame type and frame subtype

Ethernet Connectivity

- “Wireless LAN Topologies,” the 802.11-2012 standard defines:
 - An Integration Service (IS) that enables delivery of MSDUs between the Distribution System (DS) and a non-IEEE-802.11 Local Area Network (LAN)
 - The payload of a wireless 802.11 data frame is the upper layer 3–7 information known as the MSDU
 - The job of the integration service is to first remove the 802.11 header and trailer and then encase the MSDU VoIP payload inside an 802.3 Ethernet frame

Frame Information

- Source Address (SA)
 - The MAC address of the original sending station
 - Can originate from either a wireless station or the wired network
- Destination Address (DA)
 - The MAC address that is the final destination of the layer 2 frame
 - May be a wireless station or could be a destination on the wired network such as a server or a router
- Transmitter Address (TA)
 - The MAC address of an 802.11 radio that is transmitting the frame onto the half-duplex 802.11 medium
- Receiver Address (RA)
 - The MAC address of the 802.11 radio that is intended to receive the incoming transmission from the transmitting station

Management Frames

- ❑ All 14 of the management frame subtypes 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

- Following is a list of all 9 of the control frame subtypes 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 Frame Subtypes

- The following is a list of all 15 of the data frame subtypes defined by the 802.11 standard:
 - 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]

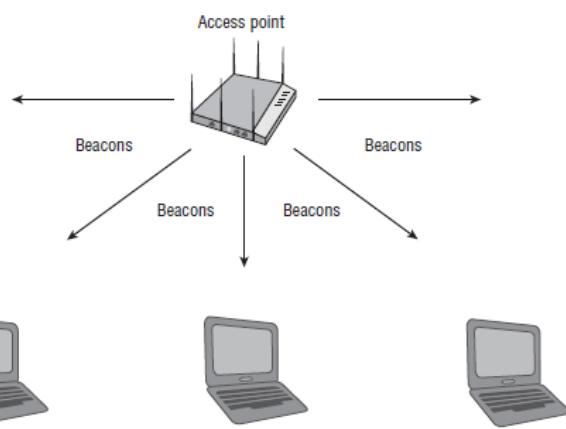
Beacon Frames

- One of the most important frame types is the beacon management frame, commonly referred to as the beacon.
 - Beacons are essentially the heartbeat of the wireless network
 - The AP of a basic service set sends the beacons while the clients listen for the beacon frames

Beacon Frame Types

Information Type	Description
Time Stamp	Synchronization information
Spread Spectrum Parameter Sets	FHSS-, DSSS-, HR-DSSS-, ERP-, OFDM-, HT-, or VHT-specific information
Channel Information	Channel used by the AP or IBSS
Data Rates	Basic and supported rates
Service Set Capabilities	Extra BSS or IBSS parameters
SSID	Logical WLAN name
Traffic Indication Map (TIM)	A field used during the Power Save process
QoS Capabilities	Quality of service and Enhanced Distributed Channel Access (EDCA) information
Robust Security Network (RSN) Capabilities	TKIP or CCMP cipher information and authentication method
Vendor Proprietary Information	Vendor-unique or vendor-specific information

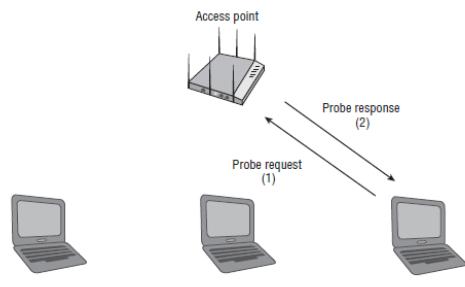
Passive Scanning



Active Scanning

- In addition to passively scanning for APs, client stations can actively scan for them
 - In active scanning, the client station transmits management frames known as probe requests
 - These probe requests either can contain the SSID of the specific WLAN that the client station is looking for or can look for any SSID

Active Scanning



- One drawback to passive scanning is that beacon management frames are broadcast only on the same channel as the AP
- In contrast, active scanning uses probe request frames that are sent out across all available channels by the client station

Authentication

- Authentication is the first of two steps required to connect to the 802.11 Basic Service Set
 - Both authentication and association must occur, in that order, before an 802.11 client can pass traffic through the AP to another device on the network

Open System Authentication

- Open System Authentication is the simpler of the two authentication methods
 - It provides authentication without performing any type of client verification
 - It is essentially an exchange of hellos between the client and the AP
 - It is considered a null authentication because no exchange or verification of identity takes place between the devices
 - Open System Authentication occurs with an exchange of frames between the client and the AP

WEP Authentication

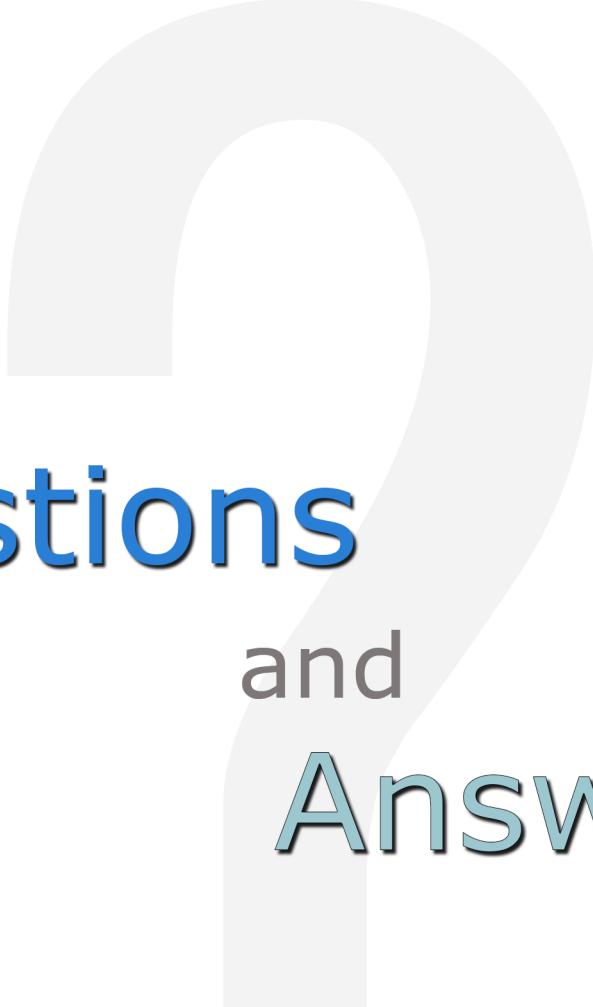
- ❑ Shared Key Authentication uses WEP when authenticating client stations and requires that a static WEP key be configured on both the station and the AP
 - ❑ In addition to WEP being mandatory, authentication will not work if the static WEP keys do not match
 - ❑ Shared Key Authentication is a four-way authentication frame exchange:
 1. The client station sends an authentication request to the AP
 2. The AP sends a clear text challenge to the client station in an authentication response
 3. The client station then encrypts the clear text challenge and sends it back to the AP in the body of another authentication request frame
 4. 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 to 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

Association

- After the station has authenticated with the AP, the next step is for it to associate with the AP
 - When a client station associates, 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.
 - The client station sends an association request to the AP, seeking permission to join the BSS

Module Review

- Packets, frames, and bits
- Data-Link layer
- Physical layer
- 802.11 and 802.3 interoperability
- Three 802.11 frame types
- Beacon management frame (beacon)
- Passive scanning
- Active scanning
- Authentication
- Association
- Authentication and association states
- Basic and supported rates



Questions and Answers

Review Questions:

1. True or False: The 802.11 Data-Link Layer is divided into four sublayers.
 - A. True
 - B. False

2. True or False: The job of the integration service is to first add the 802.11 footer then encase the MSDU VoIP payload inside an 802.3 Ethernet frame.
 - A. True
 - B. False

3. True or False: One of the most important frame types is the beacon management frame, commonly referred to as the beacon.
 - A. True
 - B. False

4. True or False: In active scanning, the client station transmits management frames known as beacon requests.
 - A. True
 - B. False

5. True or False: In passive scanning the beacon management frames are broadcast on different channels.
 - A. True
 - B. False

Answer Key:

1. B
False. The 802.11 Data-Link Layer is divided into two sublayers.
2. B
False. The job of the integration service is to first remove the 802.11 header and trailer and then encase the MSDU VoIP payload inside an 802.3 Ethernet frame.
3. A
True. One of the most important frame types is the beacon management frame, commonly referred to as the beacon.
4. B
False. In active scanning, the client station transmits management frames known as probe requests.
5. B
False. In passive scanning the beacon management frames are broadcast only on the same channel as the AP. This is a drawback of passive scanning.

Certified Wireless Network Administrator
Module 10 – WLAN Architecture

WORKBOOK

Module Introduction

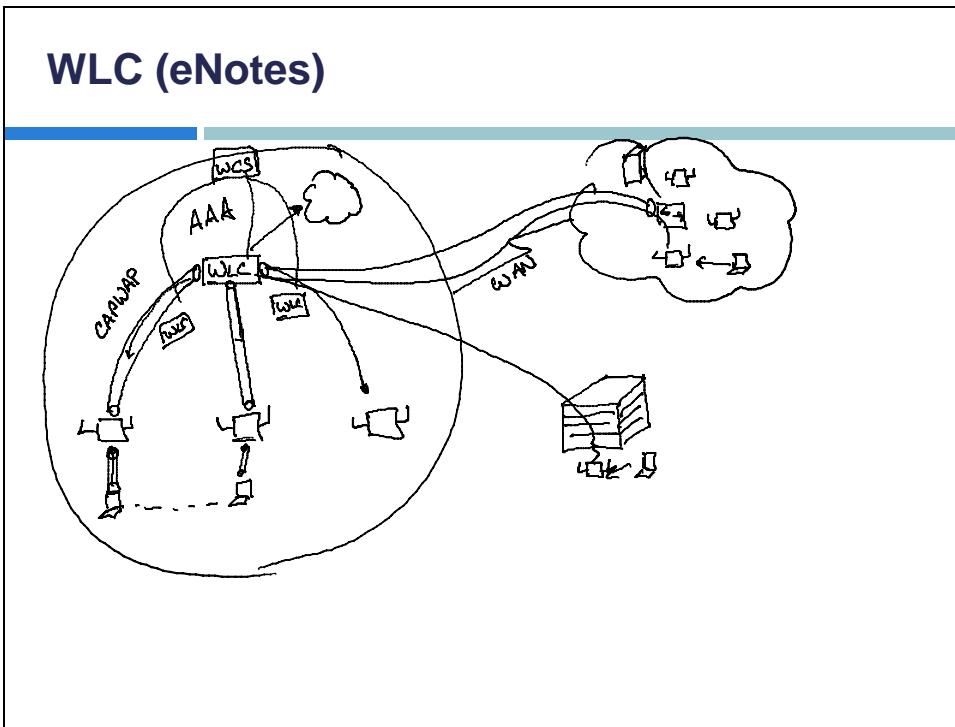
- Wireless LAN client devices
 - WLAN architecture
 - Specialty WLAN infrastructure

Management, Control, and Data Planes

- Telecommunication networks are defined as 3 logical planes of operation:
 - Management Plane
 - Defined by administrative network management, administration, and monitoring
 - Example: Any network management solution that can be used to monitor routers and switches and other wired network infrastructure
 - A centralized network management server can be used to push both configuration settings and firmware upgrades to network devices
 - Control Plane
 - Consists of control or signaling information and is often defined as network intelligence or protocols
 - Example: Control plane intelligence found in routers would be dynamic layer 3 routing protocols, such as OSPF or BGP, used to forward data
 - Content Addressable Memory (CAM) tables and Spanning Tree Protocol (STP) are control plane mechanisms used by layer 2 switches for data forwarding
 - Data Plane (User Plane)
 - The location in a network where user traffic is actually forwarded
 - Example: An individual router where packets are forwarded
 - Example: An individual switch forwarding an 802.3 Ethernet frame

Management Plane

- The functions of the management plane within an 802.11 WLAN are as follows:
 - WLAN Configuration examples include the configurations of SSIDS, security, WMM, channel, and power settings
 - WLAN Monitoring and Reporting Monitoring of layer 2 statistics like ACKs, client associations, re-associations, and data rates occurs in the management plane
 - Examples of upper-layer monitoring and reporting include application visibility, IP connectivity, TCP throughput, latency statistics, and stateful firewall sessions
 - WLAN Firmware Management is the ability to upgrade access points and other WLAN devices with the latest vendor operational code



Control Plane

- Often defined by protocols that provide the intelligence and interaction between equipment in a network
- Examples of control plane intelligence:
 - Dynamic RF
 - Coordinated channel and power settings for multiple access points are provided by the control plane
 - The majority of WLAN vendors implement some type of dynamic RF capability
 - Dynamic RF is also referred to by the more technical term radio resource management (RRM)
 - Roaming Mechanisms
 - The control plane also provides support for roaming handoffs between access points
 - Capabilities may include L3 roaming, maintaining stateful firewall sessions of clients, and forwarding of buffered packets
 - Fast secure roaming mechanisms, such as opportunistic key caching (OKC), may also be used to forward client master encryption keys between access points
 - Client Load Balancing
 - Collecting and sharing client load and performance metrics between access points to improve overall WLAN operations happens in the control plane
 - Mesh Protocols
 - Routing user data between multiple access points requires some sort of mesh routing protocol
 - Most WLAN vendors use layer 2 routing methods to move user data between mesh access points (some vendors are using layer 3 mesh routing)
 - The 802.11s amendment has defined standardized mesh routing mechanisms

Data Plane

- Where user data is forwarded
- Two devices that usually participate are the AP and a WLAN Controller
 - 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
 - As with the management and control planes, each vendor has a unique method and recommendations for handling data forwarding

Autonomous WLAN Architecture

- For many years, 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
 - These APs are often referred to as fat APs, or standalone APs
 - However, the most common industry term for the traditional access point is autonomous AP
 - All configuration settings exist in the autonomous access point itself, and therefore, the management plane resides individually in each autonomous AP
 - All encryption and decryption mechanisms and MAC layer mechanisms also operate within the autonomous AP

Centralized Network Management Systems

- One of the challenges for a WLAN administrator using a large WLAN autonomous architecture is management
 - As an administrator, would you want to configure 300 autonomous APs individually?
 - One major disadvantage of using the traditional autonomous access point is that there is no central point of management

Cloud Networking

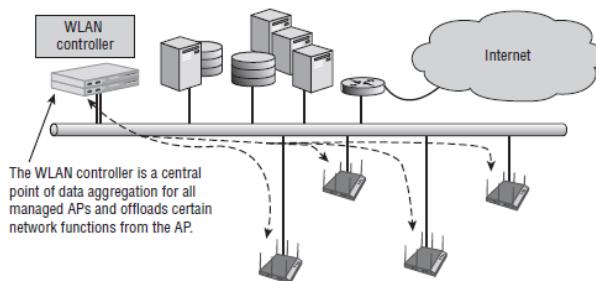
- Cloud computing and cloud networking are catchphrases used to describe the advantages of computer networking functionality when provided under a Software as a Service (SaaS) model
 - The idea behind cloud networking is that applications and network management, monitoring, functionality, and control are provided as a software service

Centralized WLAN Architecture

- The next progression in the development of WLAN integration is the centralized WLAN architecture
 - Uses a central WLAN controller that resides in the core of the network
 - In the centralized WLAN architecture, autonomous APs have been replaced with controller-based access points, also known as lightweight APs or thin APs
 - The encryption and decryption capabilities might reside in the centralized WLAN controller or may still be handled by the controller-based APs, depending on the vendor

WLAN Controller

- At the heart of the centralized WLAN architecture model is the WLAN controller



WLAN Controller (Cont.)

- ❑ Multiple WLAN controllers that communicate with each other may be deployed at different network layers, providing they can communicate with each other
 - ❑ AP Group Profiles
 - Defines the configuration settings for a single AP or group of access points
 - Settings such as channel, transmit power, and supported data rates are configured here
 - An AP can belong to only one AP group profile but may support multiple WLAN profiles
 - ❑ WLAN Profiles
 - WLAN controllers are capable of supporting multiple WLANs, which are often called WLAN profiles
 - Different groups of 802.11 clients can connect to a different SSID which is unique to each profile
 - The WLAN profile is a set of configuration parameters that are configured on the WLAN controller
 - Parameters can include the WLAN logical name(SSID), WLAN security settings, VLAN assignment, and quality-of-service (QoS)

WLC Options

- Internal Wireless Intrusion Detection Systems
 - Some WLAN controllers have integrated WIDS capabilities for security monitoring
 - Dynamic RF Spectrum Management
 - The majority of WLAN controllers implement some type of dynamic RF capability
 - A WLAN controller is a centralized device that can dynamically change the configuration of the controller-based access points based on accumulated RF information gathered from the access points' radios

WLC Options (Cont.)

- ❑ When implemented, dynamic RF provides automatic cell sizing, automatic monitoring, troubleshooting, and optimization of the RF environment
 - ❑ Best described as a self-organizing and self-healing wireless LAN
 - ❑ Bandwidth Management: bandwidth pipes can be restricted upstream or downstream
 - ❑ Firewall Capabilities: stateful packet inspection is available with an internal firewall in some WLAN controllers
 - ❑ Layer 3 Roaming Support: capabilities to allow seamless roaming across layer 3 routed boundaries are fully supported
 - Power over Ethernet (PoE)
 - ❑ When deployed at the access layer, WLAN controllers can provide direct power to controller-based APs via PoE
 - ❑ However, most controller-based APs are powered by third-party edge switches

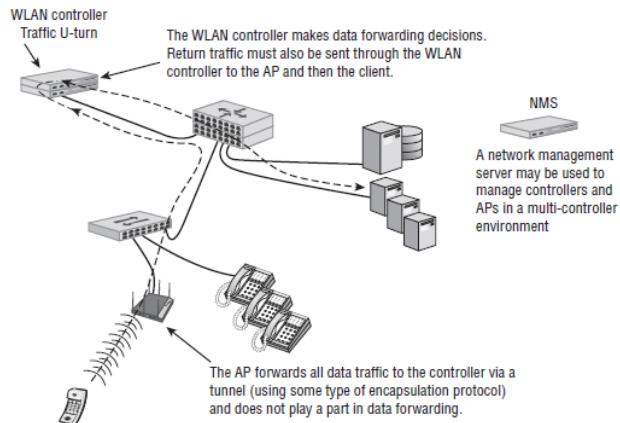
Split MAC

- The majority of WLAN controller vendors implement what is known as a split MAC architecture
 - With this type of WLAN architecture, some of the MAC services are handled by the WLAN controller, and some are handled by the access point

Controller Data Forwarding Models

- The centralized WLAN architecture usually means that the data plane exists in the WLAN controller because all user traffic is sent from the access points to the WLAN controller using IP encapsulation
- However, there are two types of data forwarding methods when using WLAN controllers:
 - **Centralized Data Forwarding**
 - Where all data is forwarded from the AP to the WLAN controller for processing, it may be used in many cases, especially when the WLAN controller manages encryption and decryption or applies security and QoS policies
 - **Distributed Data Forwarding**
 - Where the AP performs data forwarding locally, it may be used in situations where it is advantageous to perform forwarding at the edge and to avoid a central location in the network for all data, which may require significant processor and memory capacity at the controller
 - Distributed Local Data Forwarding is also used to avoid high-latency WAN links and to provide traffic with the most efficient forwarding path when communications do not involve centralized resources

Controller Data Forwarding Models



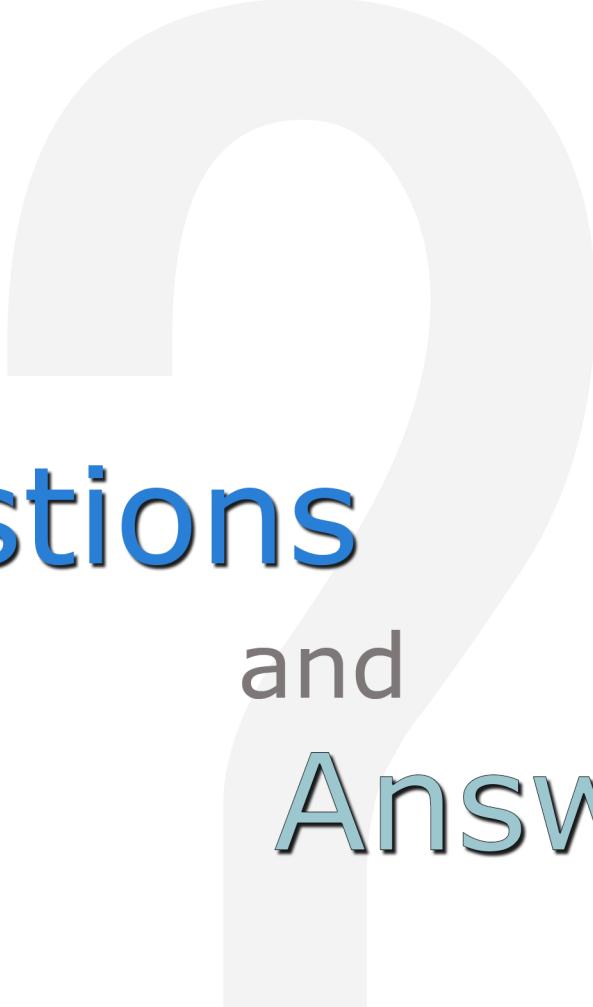
Controller Data Forwarding Models

□ Remote Office WLAN Controller

- ❑ Although WLAN controllers typically reside on the core of the network, they can also be deployed at the access layer, usually in the form of a remote office WLAN controller
 - ❑ A remote office WLAN controller typically has much less processing power than a core WLAN controller and is also less expensive
 - The purpose of a remote office WLAN controller is to allow remote and branch offices to be managed from a single location

Module Review

- Wireless LAN client devices
 - WLAN architecture
 - Specialty WLAN infrastructure



Questions and Answers

Review Questions:

1. True or False: WLAN Firmware Management is the ability to upgrade access points and other WLAN devices with the latest vendor operational code.
 - A. True
 - B. False
2. Please choose examples of upper-layer monitoring and reporting. (Choose three)
 - A. Application visibility
 - B. IP connectivity
 - C. TCP throughput
 - D. Packet timestamps
3. What are some examples of control plane intelligence? (Choose three)
 - A. Dynamic RF
 - B. Roaming mechanisms
 - C. Port filtering
 - D. Mesh protocols
4. True or False: One major disadvantage of using the traditional autonomous access point is that there is a central point of management.
 - A. True
 - B. False
5. True or False: Although WLAN controllers typically reside on the core of the network, they can also be deployed at the access layer, usually in the form of a remote office WLAN controller.
 - A. True
 - B. False

Answer Key:

1. A
True. WLAN Firmware Management is the ability to upgrade access points and other WLAN devices with the latest vendor operational code.
2. A, B, C
Examples of upper-layer monitoring and reporting include application visibility, IP connectivity, and TCP throughput.
3. A, B, D
Some examples of control plane intelligence are dynamic RF, roaming mechanisms, and mesh protocols.
4. B
False. One major disadvantage of using the traditional autonomous access point is that there is no central point of management.
5. A
True. Although WLAN controllers typically reside on the core of the network, they can also be deployed at the access layer, usually in the form of a remote office WLAN controller.

Certified Wireless Network Administrator
Module 11 – WLAN Deployment

WORKBOOK

Module Introduction

- Deployment considerations for commonly supported
- WLAN applications and devices
- Corporate data access and end-user mobility
- Network extension to remote areas
- Bridging—building-to-building connectivity
- Wireless ISP (WISP)—last-mile data delivery
- Small office/home office (SOHO)
- Mobile office networking
- Branch offices

Deployment Considerations for Commonly Supported WLAN Applications and Devices

□ Data

- When data-oriented applications are discussed, email and web browsing are two of the most common applications that come to mind
 - When planning for network traffic over any type of network, wireless or wired, you need to first look at the protocols that are being implemented
 - Protocols are communications methods or techniques used to communicate between devices on a network
 - Protocols can be well designed, based on documented standards, or they can be proprietary, using unique communications methods

Deployment Considerations for Commonly Supported WLAN Applications and Devices (Cont.)

Voice

- When designing a WLAN to support voice communications, keep in mind that, unlike data communications, voice communications are not tolerant of network delays, dropped packets, or sporadic connections
 - Designing a WLAN to support voice communications can also be a challenge because there are so many differences in how vendors implement their voice products

Deployment Considerations for Commonly Supported WLAN Applications and Devices (Cont.)

Video

- ❑ The transmission of video is 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
 - ❑ Unless you are using the WLAN for a real-time videoconference, video can likely take a backseat to audio

Real-Time Location Services

- Most manufacturers of enterprise WLAN systems tout some sort of location capability with their products



Mobile Devices

- The primary devices that people are requesting access for are cell phones and tablets that are also capable of communicating using 802.11 radios
- 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

Corporate Data Access and End-User Mobility

- With the increased throughput provided by 802.11n and now 802.11ac technology, many organizations have been transitioning to these higher-speed wireless networks while reducing the number of devices connecting to the network via wired connections
- Providing continuous access and availability throughout the facility has become paramount in the past few years

Network Extension to Remote Areas

- Bridging: Building-to-Building Connectivity
 - To provide network connectivity between two buildings, you can install an underground cable or fiber between the two buildings, you can pay for a high-speed leased data circuit, or you can use a building-to-building wireless bridge
 - A wireless building-to-building bridge requires that the two buildings have a clear RF line of sight between them
 - Point-to-point (PTP) or point-to-multipoint (PTMP) transceiver and antenna can be installed
 - The installation is typically easy for trained professionals to perform, and there are no monthly service fees after installation, because you own the equipment

Wireless ISP: Last-Mile Data Delivery

- The term last-mile is often used by phone and cable companies to refer to the last segment of their service that connects a home subscriber to their network
 - The last-mile of service can often be the most difficult and costly to run because at this point a cable must be run individually to every subscriber
 - 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

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
 - The main purpose of a SOHO 802.11 network is typically to provide wireless access to an Internet gateway



ROBO

- A company might have branch offices across a region, an entire country, or even around the world
 - 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

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
 - 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

Health Care

- Although healthcare facilities such as hospitals, clinics, and doctors' offices may seem very different from other businesses, they have many of the same networking needs as other companies: data access and end-user mobility
 - WoWs



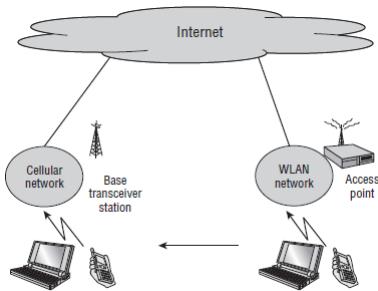
Hotspots

- Most hotspot providers perform network authentication by using a special type of web page known as a captive portal
 - When a user connects to the hotspot, the user must open up a web browser

 <h2>iBAHN</h2> <p>Sign up Customer plan Payment terms Authentication</p>	
<h1>Welcome to iBAHN - Please Choose a Connection Plan</h1>	
<p>PUBLIC INTERNET</p> <p>Provide premium high speed Internet access</p> <p>Identify:</p> <ul style="list-style-type: none"> = VPM connection • Downloading large files • Video and music streaming • 24 hours - 5-12.99 	<p>SPECIAL PROGRAMS</p> <p>Choose from one of our special Programs</p> <ul style="list-style-type: none"> <input type="radio"/> Subscription Service <input type="radio"/> Connected Code
<input type="button" value="Next"/>	<input type="button" value="Next"/>
<p>By proceeding, you agree to the Terms of Use (Read)</p>	
<p><small>© 2008 iBAHN. All rights reserved. iBAHN is a registered trademark or service mark of iBAHN, Inc. as well as their third party partners. Unauthorized copying or distribution is illegal for security of these parts. Please choose your preferred service.</small></p>	

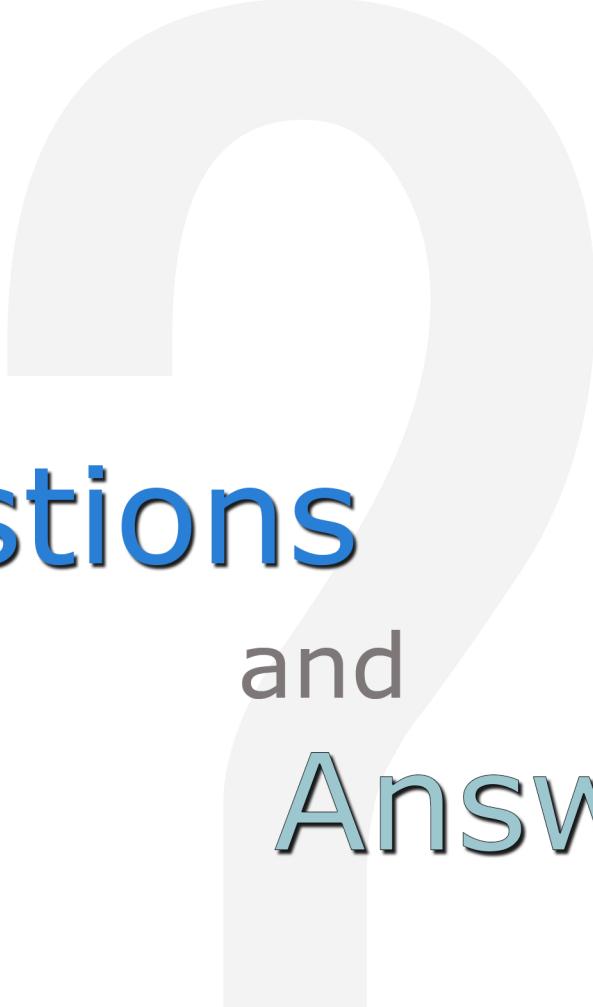
Fixed Mobile Convergence

- One of the hot topics relating to Wi-Fi is known as 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



Module Review

- Deployment considerations for commonly supported
- WLAN applications and devices
- Corporate data access and end-user mobility
- Network extension to remote areas
- Bridging—building-to-building connectivity
- Wireless ISP (WISP)—last-mile data delivery
- Small office/home office (SOHO)
- Mobile office networking
- Branch offices



Questions and Answers

Review Questions:

1. True or False: When data-oriented applications are discussed, email and web browsing are two of the most common applications that come to mind.
 - A. True
 - B. False

2. True or False: When planning for network traffic over any type of network, wireless or wired, you need to first look at the protocols that are being implemented.
 - A. True
 - B. False

3. True or False: When designing a WLAN to support voice communications, you should keep in mind that, unlike data communications, voice communications are tolerant of network delays, dropped packets, or sporadic connections.
 - A. True
 - B. False

4. True or False: Designing a WLAN to support voice communications can also be a challenge because there are so many differences in how vendors implement their voice products.
 - A. True
 - B. False

5. True or False: Unless you are using the WLAN for a real-time video conference, audio can likely take a backseat to video.
 - A. True
 - B. False

Answer Key:

1. A
True. When data-oriented applications are discussed, email and web browsing are two of the most common applications that come to mind.
2. A
True. When planning for network traffic over any type of network, wireless or wired, you need to first look at the protocols that are being implemented.
3. B
False. When designing a WLAN to support voice communications, you should keep in mind that, unlike data communications, voice communications are not tolerant of network delays, dropped packets, or sporadic connections.
4. A
True. Designing a WLAN to support voice communications can also be a challenge because there are so many differences in how vendors implement their voice products.
5. B
False. Unless you are using the WLAN for a real-time video conference, video can likely take a backseat to audio.

Certified Wireless Network Administrator
Module 12 - Troubleshooting

WORKBOOK

Module Introduction

- Layer 2 retransmissions
 - 802.11 coverage considerations
 - Voice vs. data
 - Performance
 - Weather
 - Upper layer troubleshooting

Layer 2 Retransmissions

- Unicast 802.11 frames must be acknowledged
 - 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
 - Excessive layer 2 retransmissions adversely affect the WLAN in two ways
 - First, layer 2 retransmissions increase overhead and therefore decrease throughput
 - Second, if application data has to be retransmitted at layer 2, the delivery of application traffic becomes delayed or inconsistent
 - Applications such as VoIP depend on the timely and consistent delivery of the IP packet
 - Latency and Jitter

RF Interference

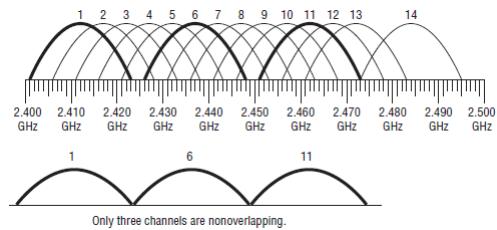
- ❑ Various types of RF interference can greatly affect the performance of an 802.11 WLAN
 - ❑ Interfering devices may prevent an 802.11 radio from transmitting, thereby causing a denial of service
 - ❑ A narrowband RF signal occupies a smaller and finite frequency space and will not cause a denial of service (DoS) for an entire band, such as the 2.4 GHz ISM band
 - ❑ A narrowband signal is usually very high amplitude and will absolutely disrupt communications in the frequency space in which it is being transmitted
 - ❑ A source of interference is typically considered wideband if the transmitting signal has the capability to disrupt the communications of an entire frequency band

RF Interference (Cont.)

- ❑ The term all-band interference is typically associated with frequency hopping spread spectrum (FHSS) communications that usually disrupt the 802.11 communications at 2.4 GHz
 - ❑ Multipath can cause intersymbol interference (ISI), which causes data corruption
 - ❑ Because of the difference in time between the primary signal and the reflected signals, known as the delay spread, the receiver can have problems demodulating the RF signal's information
 - ❑ Now that MIMO technology is prevalent, patch and panel antennas are no longer needed because multipath is constructive
 - ❑ 802.11n and 802.11ac MIMO patch antennas are still used indoors but for a much different reason

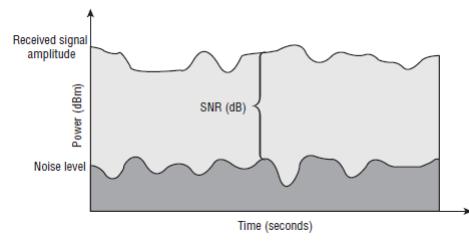
RF Interference (Cont.)

- Most Wi-Fi vendors use the term *adjacent channel interference* to refer to degradation of performance resulting from overlapping frequency space that occurs due to an improper channel reuse design
- In the WLAN industry, an adjacent channel is considered to be the next or previous numbered channel



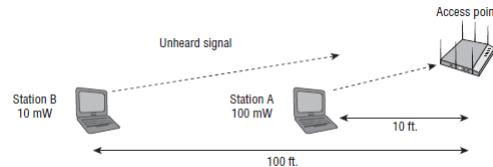
RF Interference (Cont.)

- The signal-to-noise ratio (SNR) is an 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
- The SNR is not actually a ratio
 - It is simply the difference in decibels between the received signal and the background noise (noise floor)



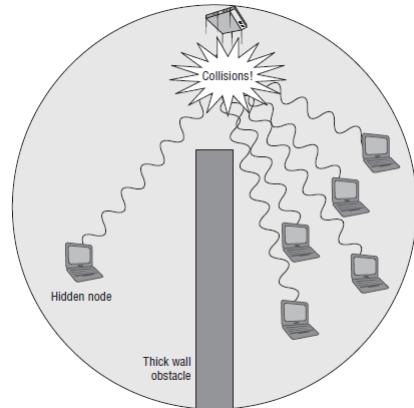
RF Interference (Cont.)

- 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
 - The transmissions of the high-powered stations could raise the noise floor near the AP to a higher level
 - The higher noise floor would corrupt the far station's incoming frame transmissions and prevent this lower-powered station from being heard



RF Interference (Cont.)

- CCA involves listening for 802.11 RF transmissions at the Physical layer
 - The 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

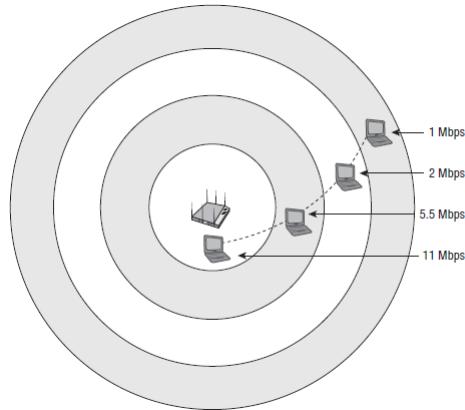


802.11 Coverage Considerations

- Providing for both coverage and capacity in a WLAN design solves many problems
 - Roaming problems and interference issues will often be mitigated in advance if proper WLAN design techniques are performed and a thorough site survey is conducted

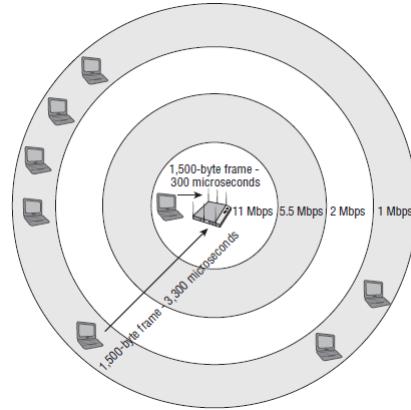
802.11 Coverage Considerations (Cont.)

- 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)
- Access points can support multiple data rates depending on the spread spectrum technology used by the AP radio



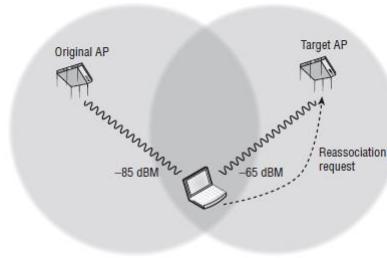
802.11 Coverage Considerations (Cont.)

- ❑ It is often a recommended 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
 - ❑ A WLAN network administrator should consider disabling the two lowest rates on a 2.4 GHz access point for three reasons:
 - Sticky client roaming problems
 - Medium contention
 - Hidden node problem



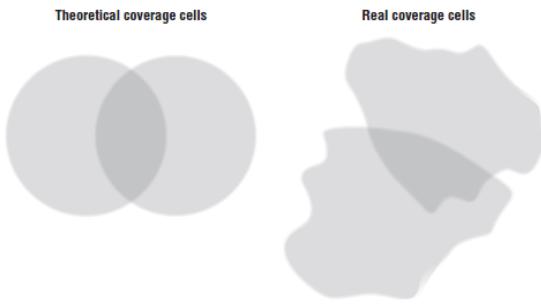
802.11 Coverage Considerations (Cont.)

- Roaming is the method by which client stations move between RF coverage cells in a seamless manner
 - Client stations switch communications through different access points
 - Seamless communications for client stations moving between the coverage zones within an Extended Service Set (ESS) is vital for uninterrupted mobility



802.11 Coverage Considerations (Cont.)

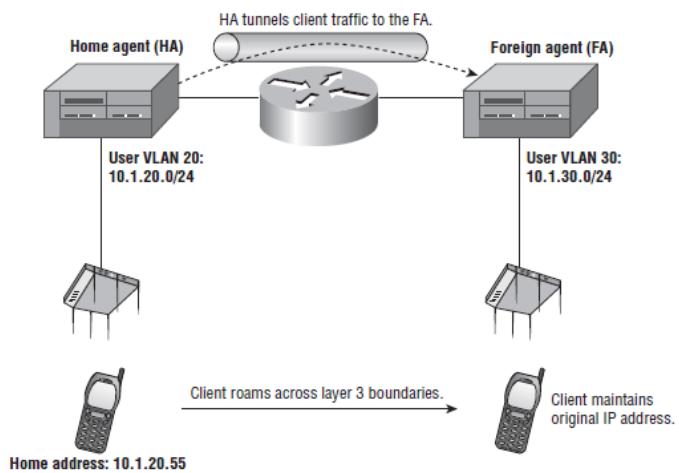
- The best way to ensure that seamless roaming will commence is proper design and a thorough site survey
- When you're designing an 802.11 WLAN, most vendors recommend 15 to 30 percent overlap of -70 dBm coverage cells



802.11 Coverage Considerations (Cont.)

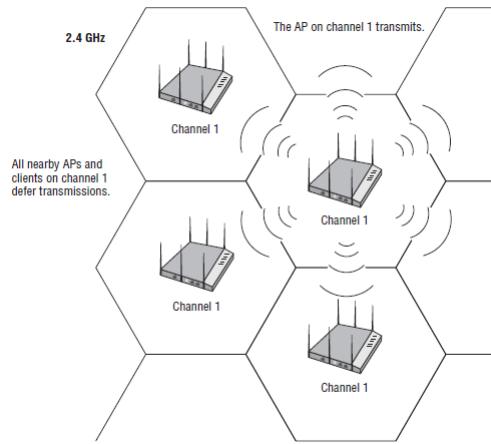
- One major consideration when designing a WLAN is what happens when client stations roam across layer 3 boundaries
 - Wi-Fi operates at layer 2 and roaming is essentially a layer 2 process
 - The client station will lose layer 3 connectivity and must acquire a new IP address
 - Any connection-oriented applications that are running when the client reestablishes layer 3 connectivity will have to be restarted

802.11 Coverage Considerations (Cont.)

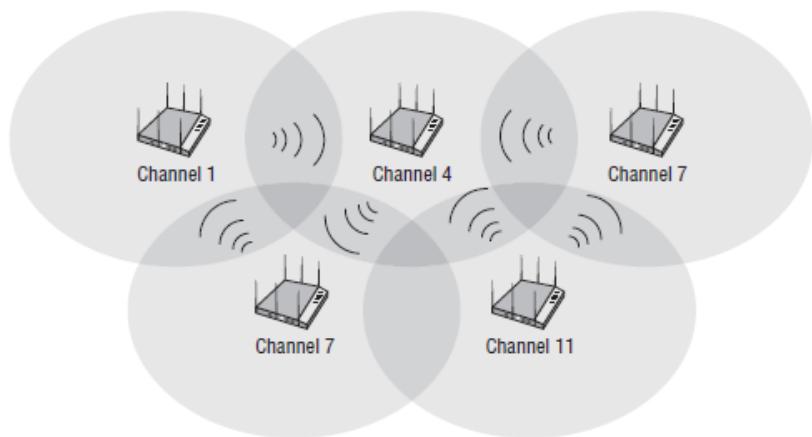


802.11 Coverage Considerations (Cont.)

- ❑ One of the most common mistakes many businesses make when first deploying a WLAN is to configure multiple access points all on the same channel
 - ❑ If all of the APs are on the same channel, unnecessary medium contention overhead occurs



802.11 Coverage Considerations (Cont.)



802.11 Coverage Considerations (Cont.)

□ Channel Reuse/Channel Bonding

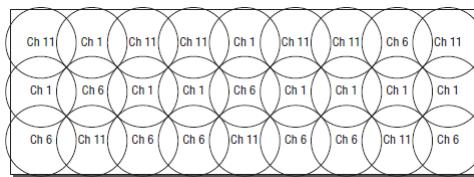
- 802.11n technology introduced the capability of bonding two 20 MHz channels to create a larger 40 MHz channel
- Channel bonding effectively doubles the frequency bandwidth, meaning double the data rates that can be available to 802.11n radios

Capacity vs. Coverage

- When a wireless network is designed, two concepts that typically compete with each other are capacity and coverage
 - In the early days of wireless networks, it was common to install an access point with the power set to the maximum level to provide the largest coverage area possible
 - This was typically acceptable because there were very few wireless devices

Capacity vs. Coverage (Cont.)

- With the proliferation of wireless devices, network design has changed drastically from the early days
 - 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
 - This is what is meant by *capacity vs. coverage*

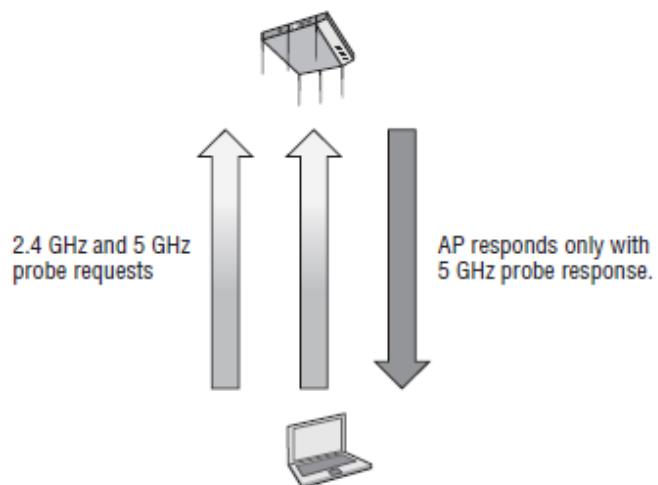


Capacity vs. Coverage (Cont.)

□ Band Steering

- The unlicensed 5 GHz frequency spectrum offers many advantages over the unlicensed 2.4 GHz frequency spectrum for Wi-Fi communications
 - The 5 GHZ U-NII bands offer a wider range of frequency space and many more channels
 - A proper 5 GHz channel reuse pattern using multiple channels will greatly decrease medium contention overhead caused by co-channel interference

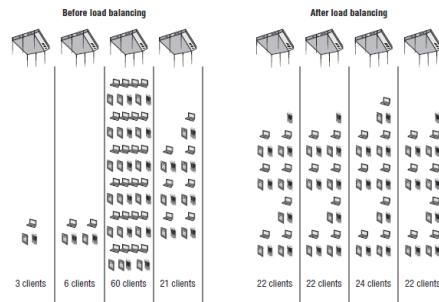
Capacity vs. Coverage (Cont.)



Capacity vs. Coverage (Cont.)

□ Load Balancing

- WLAN vendors also use methods to manipulate the MAC sublayer to balance clients between multiple access points



Voice vs. Data

- All too often, WLANs are deployed in an enterprise without any type of site survey
 - Also, many WLANs are initially designed to provide coverage only for data applications and not for voice
 - Most enterprise data applications will operate within a poorly designed WLAN but will not run optimally

IP voice	IP data
Small, uniform-size packets	Variable-size packets
Even, predictable delivery	Bursty delivery
Highly affected by late or inconsistent packet delivery	Minimally affected by late or inconsistent packet delivery
"Better never than late"	"Better late than never"

Performance

□ Transmission Power Rates

- ❑ The original transmission amplitude (power) will have an impact on the range of an RF cell
 - An access point transmitting at 30 mW will have a larger coverage zone than an access point transmitting at 1 mW if the same antenna is used
 - APs with too much transmission amplitude can cause many problems
 - ❑ Antenna Gain Antennas are passive-gain devices that focus the original signal
 - An access point transmitting at 30 mW with a 6 dBi antenna will have greater range than it would if it used only a 3 dBi antenna
 - 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
 - ❑ All things being equal, 2.4 GHz access points have a greater range than 5 GHz access points due to the difference in the length of their waves

Performance (Cont.)

- 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
 - A building with concrete walls will require more access points than a building with drywall because concrete is denser and attenuates the signal faster than drywall

Performance (Cont.)

- Applications Use
 - Different types of applications have variable affects on bandwidth consumption
 - Wi-Fi and data collection scanning typically do not require a lot of bandwidth
 - Other applications that require file transfers or database access are often more bandwidth intensive
 - High definition video streaming is also bandwidth intensive
- Number of Clients Remember that the WLAN is a shared medium
- All throughput is aggregate, and all available bandwidth is shared

Weather

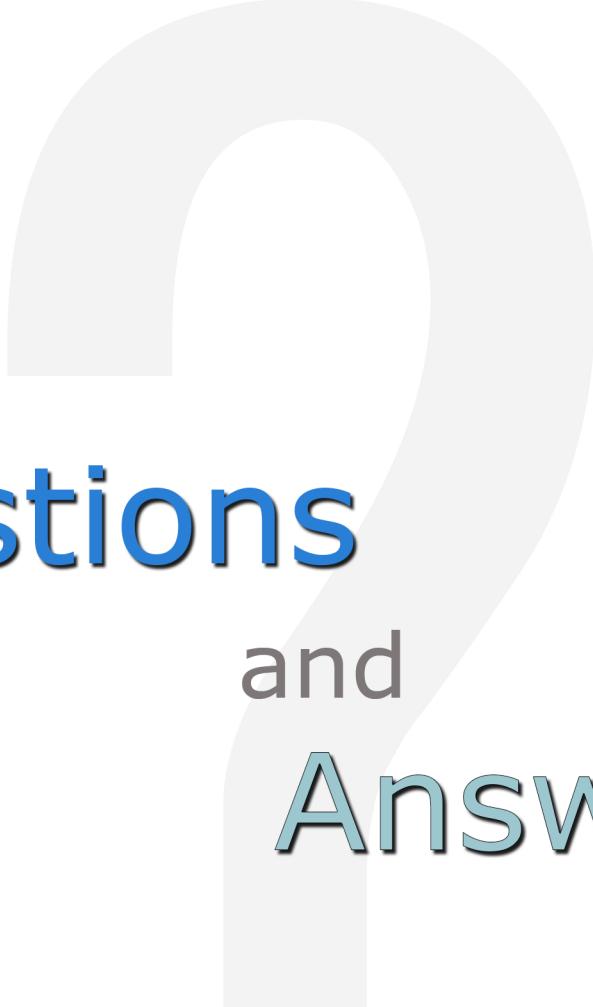
- When deploying a wireless mesh network outdoors or perhaps an outdoor bridge link, a WLAN administrator must take into account the adverse affect of weather conditions
- The following weather conditions must be considered:
 - Lightning Direct and indirect lightning strikes can damage WLAN equipment
 - Lightning arrestors should be used for protection against transient currents
 - Solutions such as lightning rods or copper/fiber transceivers may offer protection against lightning strikes
 - Because of the long distances and narrow beam widths, 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

Weather (Cont.)

- ❑ Conditions such as rain, snow, and fog present two unique challenges
 - ❑ First, all outdoor equipment must be protected from damage caused by exposure to water
 - ❑ Water damage is often a serious problem with cabling and connectors
 - ❑ Connectors should be protected with drip loops and coax seals to prevent water damage
 - ❑ Precipitation can also cause an RF signal to attenuate
 - ❑ A torrential downpour can attenuate a signal as much as 0.08 dB per mile (0.05 dB per kilometer) in both the 2.4 GHz and 5 GHz frequency ranges

Module Review

- Layer 2 retransmissions
 - 802.11 coverage considerations
 - Voice vs. data
 - Performance
 - Weather
 - Upper layer troubleshooting



Questions and Answers

Review Questions:

1. True or False: 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.
 - A. True
 - B. False
2. True or False: A narrowband RF signal occupies a larger frequency space and will cause a denial of service (DoS) for an entire band, such as the 2.4 GHz ISM band.
 - A. True
 - B. False
3. True or False: The term all-band interference is typically associated with frequency hopping spread spectrum (FHSS) communications that usually disrupt the 802.11 communications at 2.4 GHz.
 - A. True
 - B. False
4. True or False: Roaming problems and interference issues will often be mitigated in advance if proper WLAN design techniques are performed and a thorough site survey is conducted.
 - A. True
 - B. False
5. True or False: Proper network design now entails providing necessary speed while trying to maximize the number of devices connected to any single access point at the same time.
 - A. True
 - B. False

Answer Key:

1. A
True. 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.
2. B
False. A narrowband RF signal occupies a smaller and finite frequency space and will not cause a denial of service (DoS) for an entire band, such as the 2.4 GHz ISM band.
3. A
True. The term all-band interference is typically associated with frequency hopping spread spectrum (FHSS) communications that usually disrupt the 802.11 communications at 2.4 GHz.
4. A
True. Roaming problems and interference issues will often be mitigated in advance if proper WLAN design techniques are performed and a thorough site survey is conducted.
5. B
False. 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.

Certified Wireless Network Administrator
Module 13 - Security

WORKBOOK

Module Introduction

- 802.11 security basics
- Legacy 802.11 security
- Robust security
- Traffic segmentation
- Infrastructure security
- VPN wireless security

802.11 Security Basics

- Five major security components are required:
 - Data privacy and integrity
 - Authentication, authorization, and accounting (AAA)
 - Segmentation
 - Monitoring
 - Policy

802.11 Security Basics (Cont.)

- The wireless portal must be protected, and therefore an authentication solution is needed to ensure that only authorized devices and users can pass through the portal via a wireless access point (AP)
 - After users have been authorized to pass through the wireless portal, VLANs and identity-based mechanisms are needed to further restrict access to network resources

802.11 Security Basics (Cont.)

- 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
 - Using cipher encryption technologies to obscure information is mandatory to provide proper data privacy
 - A cipher is an algorithm used to perform encryption
 - The RC4 algorithm is a streaming cipher used in technologies that are often used to protect Internet traffic, such as Secure Sockets Layer (SSL)
 - The AES algorithm, originally named the Rijndael algorithm, is a block cipher that offers much stronger protection than the RC4 streaming cipher

802.11 Security Basics (Cont.)

- ❑ Authentication, authorization, and accounting (AAA) is a key computer security concept that defines the protection of network resources:
 - ❑ Authentication is the verification of identity and credentials
 - Users or devices must identify themselves and present credentials, such as usernames and passwords or digital certificates
 - More secure authentication systems use multifactor authentication, which requires at least two sets of different types of credentials to be presented
 - ❑ Authorization determines if the device or user is authorized to have access to network resources
 - This can include identifying whether you can have access based upon the type of device you are using (laptop, tablet, or phone), time of day restrictions, or location
 - Before authorization can be determined, proper authentication must occur
 - ❑ Accounting is tracking the use of network resources by users and devices
 - It is an important aspect of network security, used to keep a historical trail of who used what resource, when, and where
 - A record is kept of user identity, which resource was accessed, and at what time
 - Keeping an accounting trail is often a requirement of many industry regulations, such as the payment card industry (PCI)

802.11 Security Basics (Cont.)

- An equally important aspect of wireless security is segmentation
 - Segmentation is the chosen method of separating user traffic within a network
 - A full-time monitoring solution is also needed to protect against possible attacks that target the WLAN
 - Numerous layer 1 and layer 2 attacks are possible

802.11 Security Basics (Cont.)

- Every network card has a physical address known as a MAC address
 - This address is a 12-digit hexadecimal number
 - Every 802.11 radio has a unique MAC address
 - Most vendors provide MAC filtering capabilities on their access points
 - MAC filters can be configured to either allow or deny traffic from specific client MAC addresses to associate and connect to an AP

Robust Security

- The 802.11-2012 standard defines an enterprise authentication method as well as a method of authentication for home use
 - The current standard defines the use of an 802.1X/EAP authentication and also the use of a preshared key (PSK) or a passphrase
 - Prior to the ratification of the 802.11i amendment, the Wi-Fi Alliance introduced the Wi-Fi Protected Access (WPA) certification as a snapshot of the not-yet-released 802.11i amendment, supporting only TKIP/RC4 dynamic encryption-key generation
 - 802.1X/EAP authentication was intended for the enterprise, and passphrase authentication was suggested

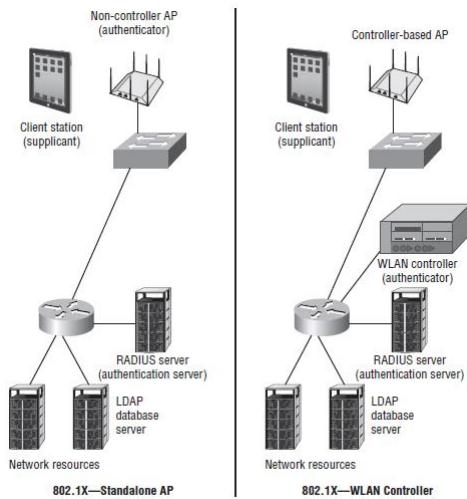
Robust Security (Cont.)

- The 802.11-2012 standard defines what are known as a robust security network (RSN) and robust security network associations (RSNAs)
 - Two 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

Robust Security (Cont.)

- The IEEE 802.1X standard is not specifically a wireless standard and is often mistaken
- The 802.1X framework consists of three main components:
 - Supplicant
 - A host with software that requests authentication and access to network resources is known as a supplicant
 - Each supplicant has unique authentication credentials that are verified by the authentication server
 - 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 two virtual ports
 - Uncontrolled: allows EAP authentication traffic to pass through
 - Controlled: blocks all other traffic until the supplicant has been authenticated
 - 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

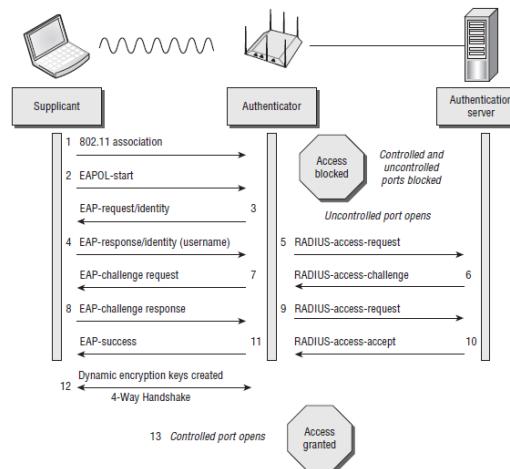
Robust Security (Cont.)



Robust Security (Cont.)

- Extensible Authentication Protocol
 - The key word in EAP is Extensible
 - EAP is a layer 2 protocol that is very flexible
 - Many different flavors of EAP exist
 - Cisco's Lightweight Extensible Authentication Protocol (LEAP) is proprietary
 - Protected Extensible Authentication Protocol (PEAP) is considered standards based

Robust Security (Cont.)

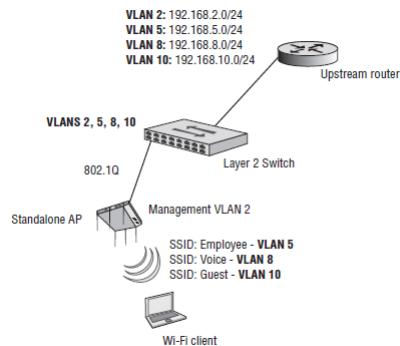


Robust Security (Cont.)

- As discussed earlier, segmentation is a key part of a network design
 - Once authorized onto network resources, user traffic can be further restricted as to what resources may be accessed and where user traffic is destined
 - Segmentation can be achieved through a variety of means
 - Firewalls
 - Routers
 - VPNs
 - VLANs

Robust Security (Cont.)

- Virtual Local Area Networks (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



Robust Security (Cont.)

- ❑ Role-based Access Control (RBAC) is another approach to restricting system access to authorized users
 - ❑ Many of the WLAN vendors provide RBAC capabilities
 - ❑ The three main components:
 - Users
 - Roles
 - Permissions
 - ❑ Separate roles can be created, such as a sales role or a marketing role
 - Individuals or groups of users are assigned to one of these roles
 - ❑ Permissions can be defined as layer 2 permissions (VLANs or MAC filters)

Robust Security (Cont.)

- Access points and other WLAN hardware can be quite expensive
 - Enterprise access points can cost as much as \$2,000 USD
 - 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
 - Access points locked inside the enclosure units are safeguarded against theft

Robust Security (Cont.)

- All wireless infrastructure devices must be able to be accessed by administrators through a management interface
 - Enterprise equipment usually can be configured through:
 - Command-line interface
 - Web interface
 - Simple Network Management Protocol (SNMP)

Robust Security (Cont.)

- Although the 802.11-2012 standard clearly defines layer 2 security solutions, 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
 - Although not usually a recommended practice, VPNs were often used for WLAN security because the VPN solution was already in place inside the wired infrastructure

Robust Security (Cont.)

- 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 first packet is encapsulated inside the second or outer packet

Robust Security (Cont.)

- 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

Robust Security (Cont.)

- Most businesses like to provide Wi-Fi guest access as a convenience to visitors
 - Guest wireless networks allow Internet access to visitors, such as contractors, students, or salespeople
 - Many organizations understand the need for their visitors to be able to access the Internet, especially to access email
 - Organizations provide WLAN guest access with a unique SSID and guest VLAN

Robust Security (Cont.)

- ❑ VLAN guest user traffic should be segmented into a unique VLAN tied to an IP subnet that does not mix with the employee user VLANs
 - ❑ Guest traffic is often also routed to a demilitarized zone (DMZ)
 - ❑ Guest WLAN firewall policies tend to be very restrictive
 - ❑ Guest firewall policies typically allow for DHCP and DNS but restrict access to private networks
 - ❑ 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16
 - ❑ Guest users are not allowed on these private networks because corporate network servers and resources usually reside on the private IP space
 - ❑ The guest firewall policy normally routes all user traffic straight to an Internet gateway and away from corporate network infrastructure

Robust Security (Cont.)

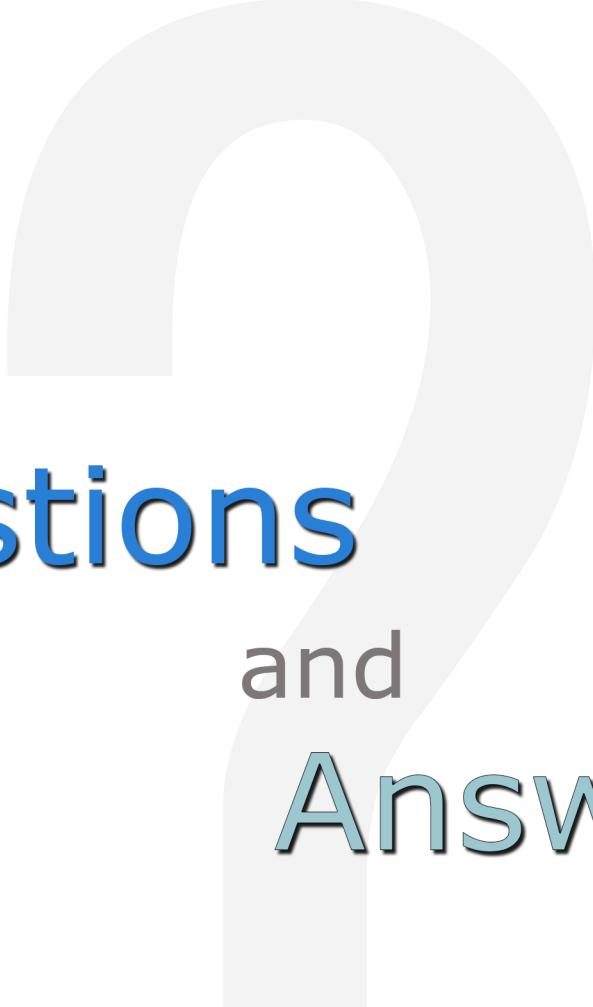
- ❑ Captive Web Portal guest users must normally log in through a captive web portal page before they can proceed to the Internet
 - ❑ One of the most important aspects of the captive web portal page is the legal disclaimer
 - ❑ Most guest WLANS require a guest user to authenticate with credentials via a captive web portal
 - Therefore, a database of user credentials must be created
 - ❑ Unlike a preexisting Active Directory database, a guest user database is created on the fly

Robust Security (Cont.)



Module Review

- 802.11 security basics
 - Legacy 802.11 security
 - Robust security
 - Traffic segmentation
 - Infrastructure security
 - VPN wireless security



Questions and Answers

Review Questions:

1. True or False: The wireless portal must be protected, and therefore an authentication solution is needed to ensure that only authorized devices and users can pass through the portal via a wireless access point (AP).
 - A. True
 - B. False

2. True or False: After users have been authorized to pass through the wireless portal, VLANs and identity-based mechanisms are needed to further restrict access to network resources.
 - A. True
 - B. False

3. True or False: Protecting data privacy in a wired network is more difficult because physical access to the wired medium is more restricted, whereas access to wireless transmissions is available to anyone in listening range.
 - A. True
 - B. False

4. True or False: Segmentation is the chosen method of separating user traffic within a network.
 - A. True
 - B. False

5. True or False: Virtual Local Area Networks (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.
 - A. True
 - B. False

Answer Key:

1. A
True. The wireless portal must be protected, and therefore an authentication solution is needed to ensure that only authorized devices and users can pass through the portal via a wireless access point (AP).
2. A
True. After users have been authorized to pass through the wireless portal, VLANs and identity-based mechanisms are needed to further restrict access to network resources.
3. B
False. 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.
4. A
True. Segmentation is the chosen method of separating user traffic within a network.
5. A
True. Virtual Local Area Networks (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.

Certified Wireless Network Administrator

Module 14 – Types of Wireless Attacks

WORKBOOK

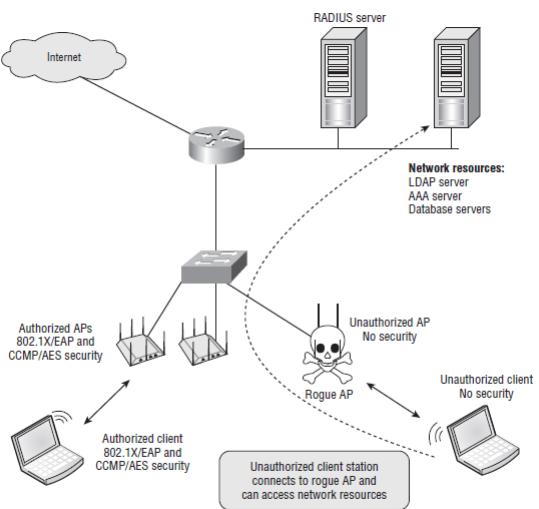
Module Introduction

- Wireless attacks
 - Intrusion monitoring
 - Wireless security policy

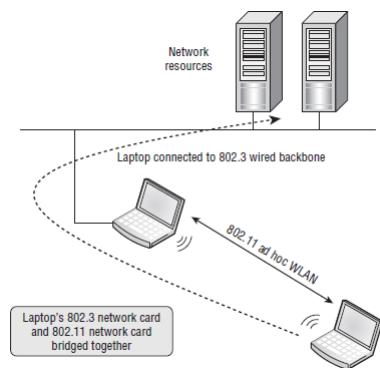
Wireless Attacks

- The portal must be protected with strong authentication methods so that only legitimate users and devices with the proper credentials will be authorized to have access to network resources
 - If the portal is not properly protected, unauthorized users can gain access to these resources
 - The big buzz-phrase in Wi-Fi security has always been the rogue access point
 - A potential open and unsecured gateway straight into the wired infrastructure that the company wants to protect
 - A rogue access point is any unauthorized Wi-Fi device that is not under the management of the proper network administrators

Wireless Attacks (Cont.)



Wireless Attacks (Cont.)



Wireless Attacks (Cont.)

- 802.11 wireless networks operate in license free frequency bands
- 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
 - Malicious eavesdropping

Wireless Attacks (Cont.)

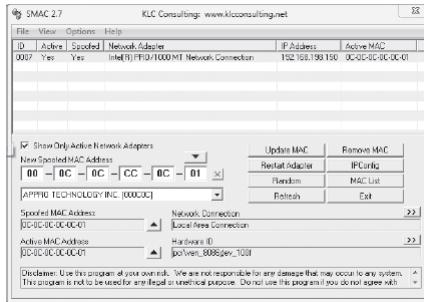
- WLAN discovery is typically considered harmless and in the past was referred to as wardriving
 - Wardriving was strictly the act of looking for wireless networks, usually while in a moving vehicle
 - The term wardriving was derived from wardialing from the 1983 film War Games
 - Wardialing is illegal in the US, but not wardriving

Wireless Attacks (Cont.)

- ❑ Authorization to network resources can be achieved by either an 802.1X/EAP authentication solution or the use of PSK authentication
 - ❑ 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
 - ❑ Some types of EAP authentication are more secure than others
 - 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

Wireless Attacks (Cont.)

- All 802.11 radios have a physical address known as a MAC address
 - This address is a 12-digit hexadecimal number that is seen in clear text in the layer 2 header of 802.11 frames
 - Wi-Fi vendors often provide MAC filtering capabilities on their APs
 - Usually, MAC filters are configured to apply restrictions that will allow traffic only from a specific client stations to pass through

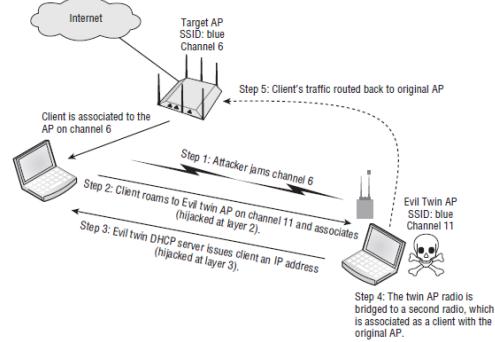


Wireless Attacks (Cont.)

- Wireless infrastructure hardware, such as autonomous APs and WLAN controllers, can be managed by administrators via a variety of interfaces, much like managing wired infrastructure hardware
- Devices can typically be accessed via:
 - Web interface
 - Command line interface
 - Serial port
 - Console connection
 - Simple Network Management Protocol (SNMP)

Wireless Attacks (Cont.)

- An attack that often generates a lot of press is 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
 - Some small Wi-Fi USB devices also have the ability to operate as an AP



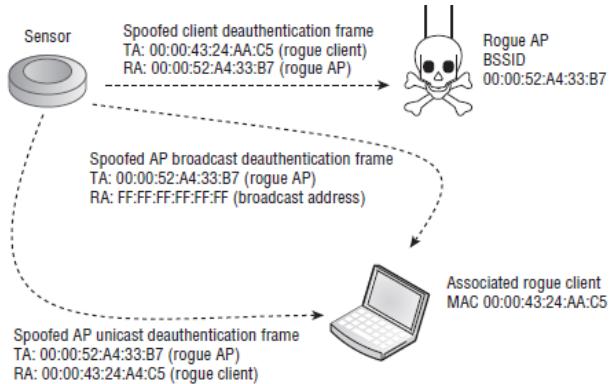
Wireless Attacks (Cont.)

- 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
 - Intentional jamming attacks occur when an attacker uses some type of signal generator to cause interference in the unlicensed frequency space
 - Both narrowband and wideband jammers exist that will interfere with 802.11 transmissions, 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 is more common and not malicious
 - Unintentional interference from microwave ovens, cordless phones, and other devices can also cause Denial of Service
 - Though it is not necessarily an attack, it can cause as much harm as an intentional jamming attack

Intrusion Monitoring

- In today's world, a Wireless Intrusion Detection System (WIDS) might be necessary even if there is no authorized 802.11 Wi-Fi network on site
 - Wireless can be an intrusive technology, and if wired data ports at a business are not controlled, any individual (including employees) can install a rogue access point
 - Most WIDS vendors prefer to call their product a wireless intrusion prevention system (WIPS)
 - 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

Intrusion Monitoring (Cont.)



Wireless Security Policy

□ General Security Policy

- When establishing a wireless security policy, you must first define a general policy
- A general wireless security policy establishes why a wireless security policy is needed for an organization

Wireless Security Policy (Cont.)

- ❑ A functional policy is also needed to define the technical aspects of wireless security
 - ❑ Establishes how to secure the wireless network in terms of what solutions and actions are needed
 - ❑ The following items will be defined:
 - Policy Essentials: basic security procedures, such as password policies, training, and proper usage of the wireless network
 - Baseline Practices: minimum wireless security practices, such as configuration checklists, staging and testing procedures
 - Design and Implementation: the actual authentication, encryption, and segmentation solutions that are to be put in place
 - Monitoring and Response: all wireless intrusion detection procedures and the appropriate response to alarms

Highly Recommended Wireless Security Policies

- 1. BYOD Policy**
 - ❑ Employees bring personal Wi-Fi devices (smartphone, tablet) to the workplace
 - ❑ Employees expect to use these Wi-Fi devices on the secure corporate WLAN
 - ❑ Define a Bring Your Own Device policy that clearly states how personal devices will be onboarded and used while connected to the company WLAN and which corporate network resources are accessible
 - 2. Remote Access WLAN Policy**
 - ❑ End users take their devices off site and away from company grounds
 - ❑ Most users likely use wireless networks at home and at wireless hotspots
 - ❑ Many of these remote wireless networks have absolutely no security in place, so a Remote Access WLAN policy must be strictly enforced
 - 3. Rogue AP Policy**
 - ❑ No end users should ever be permitted to install their own devices on the corporate network
 - ❑ This includes APs, wireless routers, wireless hardware USB clients, and WLAN NICs
 - ❑ Could open unsecured portals into the main infrastructure network

Highly Recommended Wireless Security Policies (Cont.)

4. Ad Hoc Policy

- ❑ End users should not be permitted to set up ad hoc or peer-to-peer networks
- ❑ Peer-to-peer networks are susceptible to peer attacks, and can serve as unsecured portals to the infrastructure network if the computer's Ethernet port is also in use

5. Wireless LAN Proper Use Policy

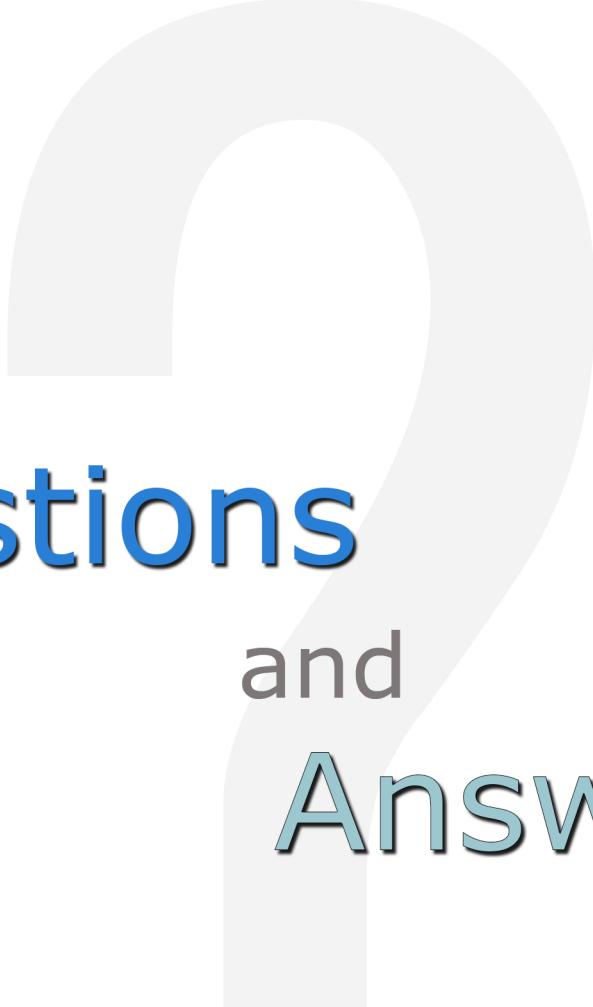
- ❑ Should outline the proper use and implementation of the main corporate wireless network
- ❑ Should include installation procedures, security implementations, allowed app use on the WLAN

6. IDS Policy

- ❑ Defines how to properly respond to alerts generated by the Wireless Intrusion Detection System
- ❑ Example: how to deal with the discovery of rogue APs and all necessary actions that should follow

Module Review

- Wireless attacks
 - Intrusion monitoring
 - Wireless security policy



Questions and Answers

Review Questions:

1. True or False: The portal must be protected with strong authentication methods so that only legitimate users and devices with the proper credentials will be authorized to have access to network resources.
 - A. True
 - B. False

2. True or False: A rogue access point is an authorized Wi-Fi device that is not under the management of the proper network administrators.
 - A. True
 - B. False

3. True or False: Access to wireless transmissions is available to anyone within listening range, and therefore strong encryption is mandatory.
 - A. True
 - B. False

4. True or False: WLAN discovery is typically considered harmless and in the past was referred to as wirewalking.
 - A. True
 - B. False

5. True or False: An attack that often generates a lot of press is wireless hijacking, also known as the evil twin attack.
 - A. True
 - B. False

Answer Key:

1. A
True. The portal must be protected with strong authentication methods so that only legitimate users and devices with the proper credentials will be authorized to have access to network resources.
2. B
False. A rogue access point is any unauthorized Wi-Fi device that is not under the management of the proper network administrators.
3. A
True. Access to wireless transmissions is available to anyone within listening range, and therefore strong encryption is mandatory.
4. B
False. WLAN discovery is typically considered harmless and in the past was referred to as wardriving.
5. A
True. An attack that often generates a lot of press is wireless hijacking, also known as the evil twin attack.

Certified Wireless Network Administrator
Module 15 – Fundamentals of Site Surveys

WORKBOOK

Module Introduction

- WLAN site survey interview
 - Documentation and reports
 - Vertical market considerations

WLAN Site Survey Interview

- Is a site survey even needed?
 - The answer to that question is almost always a resounding yes
 - If an owner of a small retail shop desires a wireless network, the site survey that is conducted may be as simple as placing a small office, home office (SOHO) Wi-Fi router in the middle of the shop, turning the transmit power to a lower setting, and making sure you have connectivity

WLAN Site Survey Interview (Cont.)

- Even though 802.11 technologies have been around since 1997, much misunderstanding and misinformation about wireless networking still exists
- Because many businesses and individuals are familiar with Ethernet networks, a “just plug it in and turn it on” mentality is prevalent

WLAN Site Survey Interview (Cont.)

- The first question that should be:
 - 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
 - Always ask about the business needs
 - 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

WLAN Site Survey Interview (Cont.)

- Next step is to begin asking all the necessary questions for planning the site survey and designing the wireless network
- Although the final design of a WLAN is completed after the site survey is conducted, some preliminary design based on the capacity and coverage needs of the customer is recommended
- You will need to sit down with a copy of the building's floor plan and ask the customer where they want RF coverage

WLAN Site Survey Interview (Cont.)

□ User and Device Density

- ❑ Three important questions need to be asked:
 1. How many users currently need wireless access and how many Wi-Fi devices will they be using?
 2. 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
 3. Most significant: Where are the users?
 - ❑ Peak On/Off Use
 - Be sure to ask what the peak times are—that is, when access to the WLAN is heaviest

WLAN Site Survey Interview (Cont.)

- Existing Transmitters
 - Does not refer just to previously installed 802.11 networks
 - Refers to interfering devices such as microwaves, cordless headsets, cordless phones, wireless machinery
 - Portability vs. Mobility
 - There are two types of mobility
 1. Related to being portable
 2. True mobility

WLAN Site Survey Interview (Cont.)

- 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
 - ▣ Professional site survey companies have reported that as much as 40 percent of their business is troubleshooting existing WLANs, which often requires conducting a second site survey or discovering that one was never conducted to begin with

WLAN Site Survey Interview (Cont.)

- ❑ You have already learned that the usual purposes of a WLAN are to provide client mobility and to provide access via an AP into a preexisting wired network infrastructure
 - ❑ Part of the interview process includes asking the correct questions so that the WLAN will integrate properly into the existing wired architecture
 - ❑ Roaming
 - ❑ Is roaming required?
 - In most cases, the answer will be yes, because mobility is a key advantage of wireless networking
 - Any devices that run connection-oriented applications will need seamless roaming

WLAN Site Survey Interview (Cont.)

- PoE
 - How will the access points be powered?
 - APs are often mounted in the ceiling
 - Power over Ethernet (PoE)
 - 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

WLAN Site Survey Interview (Cont.)

- Because of the widespread acceptance of Wi-Fi in business environments, most companies offer some sort of wireless guest access to the Internet
 - Guest users access the WLAN via the same access points

Documents and Reports

- Proper documentation about the facility and network must be obtained
 - Blueprints
 - You need a floor plan layout in order to discuss coverage and capacity needs with network administration personnel



Documents and Reports (Cont.)

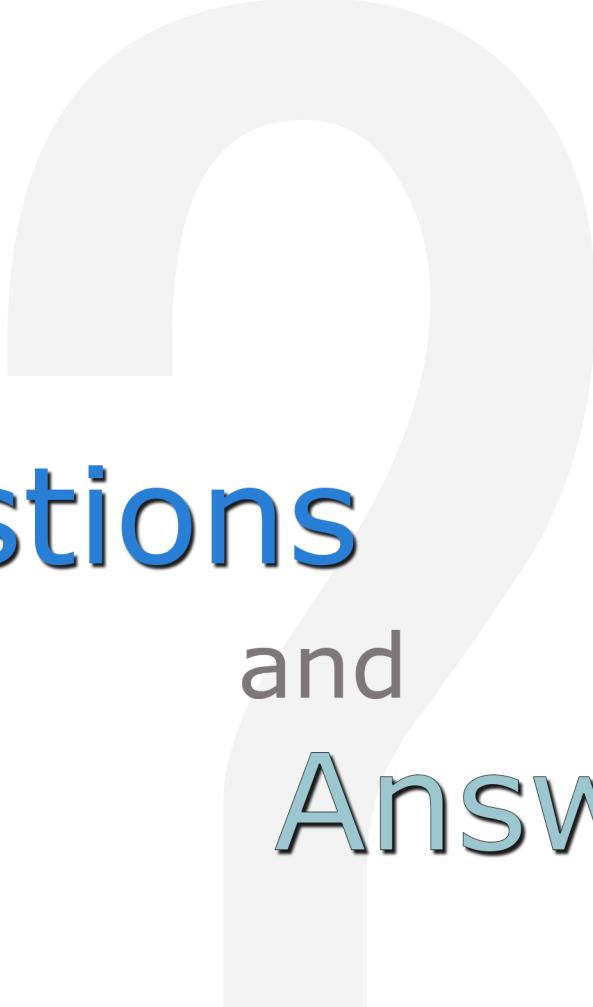
- Spectrum Analysis
 - Be sure to identify potential sources of interference
 - RF Coverage Analysis define RF cell boundaries
 - Hardware Placement and Configuration recommend AP placement, antenna orientation, channel reuse pattern, power settings, and any other AP-specific information such as installation techniques and cable routing
 - Capacity and Performance Analysis includes results from application throughput testing, which is sometimes an optional analysis report included with the final survey report

Documents and Reports (Cont.)

- Some of the CWNA exam is focused on outdoor site surveys for establishing bridge links
 - Calculations necessary for outdoor bridging surveys are numerous, including:
 - The Fresnel zone
 - Earth bulge
 - Free space path loss
 - Link budget
 - Fade margin

Module Review

- WLAN site survey interview
 - Documentation and reports
 - Vertical market considerations



Questions and Answers

Review Questions:

1. True or False: Even though 802.11 technologies have been around since 1997, much misunderstanding and misinformation about wireless networking still exists.
 - A. True
 - B. False

2. True or False: When doing a WLAN site survey, existing transmitters refers to previously installed 802.11 networks.
 - A. True
 - B. False

3. True or False: Because of the widespread acceptance of Wi-Fi in business environments, most companies offer some sort of wireless guest access to the Internet.
 - A. True
 - B. False

4. True or False: 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.
 - A. True
 - B. False

5. True or False: Capacity and performance analysis includes results from application throughput testing, which is sometimes an optional analysis report included with the final survey report.
 - A. True
 - B. False

Answer Key:

1. A
True. Even though 802.11 technologies have been around since 1997, much misunderstanding and misinformation about wireless networking still exists.
2. B
False. When doing a WLAN site survey, existing transmitters refer to interfering devices such as microwaves, cordless headsets, cordless phones, wireless machinery.
3. A
True. Because of the widespread acceptance of Wi-Fi in business environments, most companies offer some sort of wireless guest access to the Internet.
4. A
True. 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.
5. A
True. Capacity and performance analysis includes results from application throughput testing, which is sometimes an optional analysis report included with the final survey report.

Certified Wireless Network Administrator
Module 16 – Site Survey Tools

WORKBOOK

Module Introduction

- Site survey defined
 - Site survey tools
 - Coverage analysis

Protocol and Spectrum Analysis

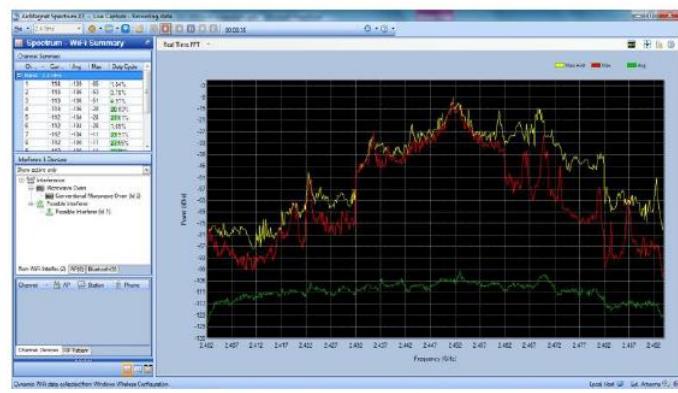
- Ten years ago, if you wanted to plan and design a wireless network, the likelihood of interference from other networks or wireless devices was much less than it is now
 - Wi-Fi-based protocol analyzers can examine 802.11 frames and identify SSID and BSSID information along with packet and security information
 - Signal strength measurements along with channel information can be monitored and documented, provide an overview, and at times, provide an RF map of the existing 802.11 environment
 - 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

Spectrum Analysis

- ❑ Before conducting the coverage analysis survey, locating sources of potential interference is a must
 - ❑ Some companies and consultants still ignore spectrum analysis because of the cost generally associated with purchasing the necessary spectrum analyzer hardware
 - ❑ However, with the prices of PC-based analyzers decreasing over recent years, spectrum analysis has become more of the norm with site surveys



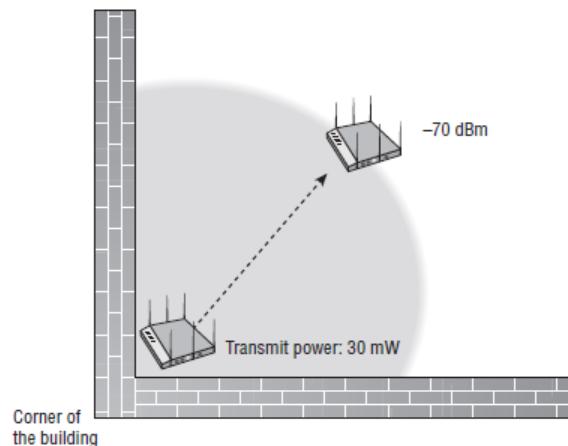
Spectrum Analysis (Cont.)



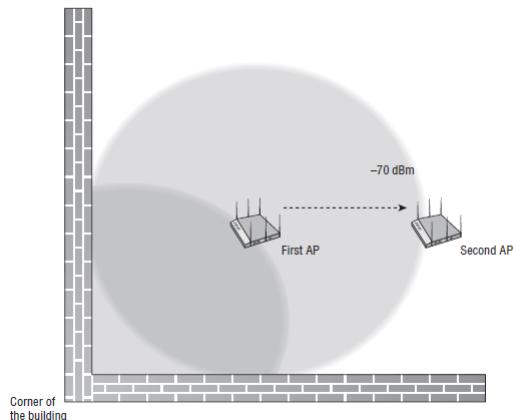
Spectrum Analysis (Cont.)

- After you conduct a spectrum analysis site survey, your next step is the all-important determination of proper 802.11 RF coverage inside your facility
- After all the capacity and coverage needs have been determined, 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

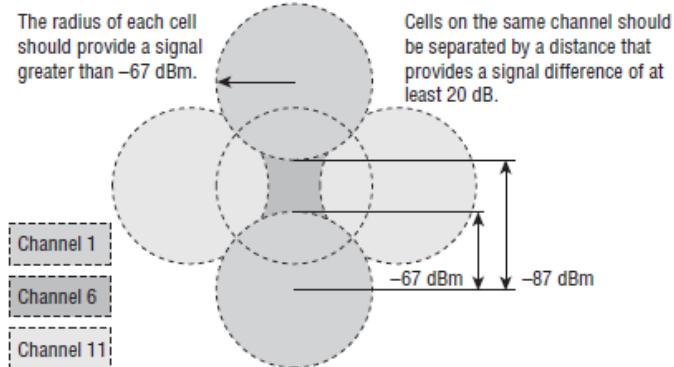
Site Survey



Site Survey (Cont.)



Site Survey (Cont.)



AP Placement and Configuration

- 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
 - Another often overlooked component in WLAN design during coverage analysis is the use of semidirectional antennas
 - Many deployments of WLANs use only the manufacturer's default low-gain omnidirectional antenna, which typically has about 2.14 dBi of gain

Application Analysis

- Whereas spectrum analysis and coverage analysis are considered mandatory during 802.11 wireless site surveys, application analysis has not always been
 - 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

Indoor Site Survey Tools

- As stated earlier, a spectrum analyzer will be needed for locating potential sources of interference
 - Your main weapon in your coverage analysis arsenal will be a received signal strength measurement tool

Outdoor Site Survey Tools

- Outdoor site surveys are conducted using either outdoor access points or mesh routers, which are the devices typically used to provide access for client stations in an outdoor environment
- These outdoor Wi-Fi surveys will use most of the same tools as an indoor site survey but may also use a Global Positioning System (GPS) device to record latitude and longitude coordinates

Outdoor Site Survey Tools (Cont.)

- Topographic Map Instead of a building floor plan, a topographic 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
 - The bridge link analysis software is a predictive modeling tool
 - 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)

Coverage

- ❑ Manual coverage analysis involves the techniques described earlier, which are used to find the cell boundaries
 - ❑ There are two major types of manual coverage analysis surveys:
 - ❑ Passive
 - During a passive manual survey, 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
 - During an active manual survey, 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
 - However, upper-layer information such as packet loss and layer 2 retransmission percentages can be measured because the client card is associated to a single access point

Coverage (Cont.)

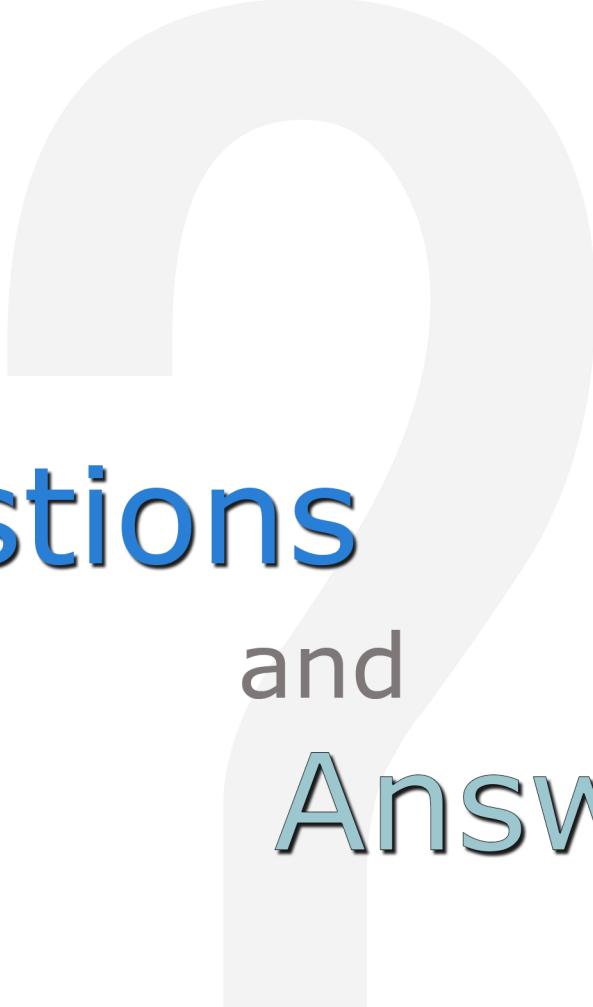
- The last method of RF coverage analysis uses applications that provide RF simulations and modeling design capabilities
 - Predictive coverage analysis is accomplished using an application that creates visual models of RF coverage cells, bypassing the need for actually capturing RF measurements

Confirmation

- 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
 - Hopefully, these numbers meet or exceed your expectations

Module Review

- Site survey defined
 - Site survey tools
 - Coverage analysis



Questions and Answers

Review Questions:

1. True or False: Ten years ago, if you wanted to plan and design a wireless network, the likelihood of interference from other networks or wireless devices was much greater than it is now.
 - A. True
 - B. False

2. True or False: Wi-Fi-based protocol analyzers can examine 802.11 frames and identify SSID and BSSID information along with packet and security information.
 - A. True
 - B. False

3. True or False: Some companies and consultants still ignore spectrum analysis because of the cost generally associated with purchasing the necessary spectrum analyzer hardware.
 - A. True
 - B. False

4. True or False: Whereas spectrum analysis and coverage analysis are considered optional during 802.11 wireless site surveys, application analysis has not always been.
 - A. True
 - B. False

5. True or False: Predictive coverage analysis is accomplished using an application that creates visual models of RF coverage cells, bypassing the need for actually capturing RF measurements.
 - A. True
 - B. False

Answer Key:

1. B
False. Ten years ago, if you wanted to plan and design a wireless network, the likelihood of interference from other networks or wireless devices was much less than it is now.
2. A
True. Wi-Fi-based protocol analyzers can examine 802.11 frames and identify SSID and BSSID information along with packet and security information.
3. A
True. Some companies and consultants still ignore spectrum analysis because of the cost generally associated with purchasing the necessary spectrum analyzer hardware.
4. B
False. Whereas spectrum analysis and coverage analysis are considered mandatory during 802.11 wireless site surveys, application analysis has not always been.
5. A
True. Predictive coverage analysis is accomplished using an application that creates visual models of RF coverage cells, bypassing the need for actually capturing RF measurements.

Certified Wireless Network Administrator
Module 17 - PoE

WORKBOOK

Module Introduction

- History of PoE
 - PoE devices (overview)
 - Planning and deploying PoE

Non-Standard

- As with most new technologies, 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
- In the meantime, vendor-proprietary PoE continued to proliferate

802.3af

- The IEEE 802.3af Power over Ethernet committee created the PoE amendment to the 802.3 standard
 - It was officially referred to as IEEE 802.3 “Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface”
 - This amendment to the IEEE 802.3 standard was approved on June 12, 2003, and defined how to provide PoE to 10BaseT (Ethernet), 100BaseT (Fast Ethernet), and 1000BaseT (Gigabit Ethernet) devices

Powered Device

- The powered device (PD) either requests or draws power from the power-sourcing equipment
- PDs must be capable of accepting up to 57 volts from either the data lines or the unused pairs of the Ethernet cable

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

Discovery

- In the past, some vendors used proprietary layer 2 discovery protocols to perform classification
 - Although these techniques are good from the power-management and consumption perspective, they are proprietary and will not work with other manufacturers' products
 - Link Layer Discovery Protocol (LLDP) is a standards-based layer 2 neighbor discovery protocol that can also be used for more detailed power classification

Discovery (Cont.)

- The power-sourcing equipment (PSE) provides power to the PD
- The power supplied is at a nominal 48 volts (44 volts to 57 volts)
 - The PSE 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
 - If a device does not respond to the detection signature, the PSE will withhold power
 - This prevents noncompliant PD equipment from becoming damaged

Endpoint

- An endpoint PSE provides power and Ethernet data signals from the same device
 - Endpoint devices are typically PoE-enabled Ethernet switches



Midspan

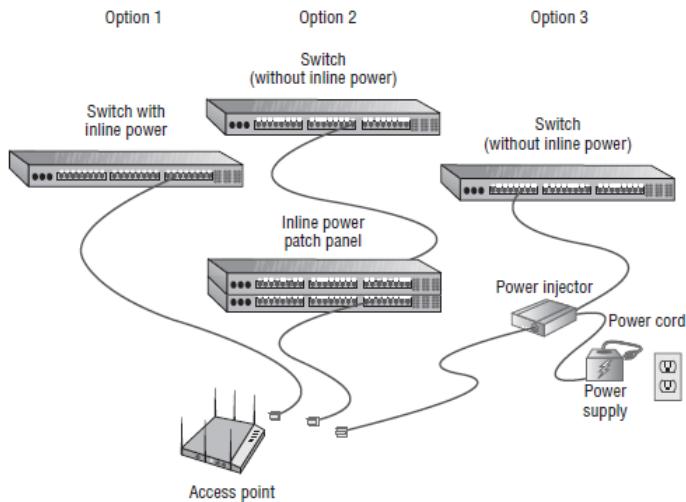
- A midspan PSE acts as a pass-through device, adding power to an Ethernet segment
 - Midspan equipment enables you to provide PoE to existing networks without having to replace the existing Ethernet switches
 - A midspan PSE is placed between an Ethernet source (such as an Ethernet switch) and a PD

MDI

- The Power-Sourcing Equipment (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
 - Keep in mind that the Ethernet maximum distance limitations of 100 meters (328 feet) still apply when PoE mechanisms are utilized



PoE



PoE (Cont.)

- ❑ Instead of the power being distributed for hundreds or thousands of devices, the power for these devices is now being sourced from either a single or a limited number of locations
 - ❑ 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+
 - ❑ Assuming that your PDs do not require PoE+, this means that a typical PoE-enabled 24-port Ethernet switch must be able to provide about 370 watts of power to provide PoE to all 24 ports ($15.4 \text{ watts} \times 24 \text{ ports} = 369.6 \text{ watts}$)

PoE (Cont.)

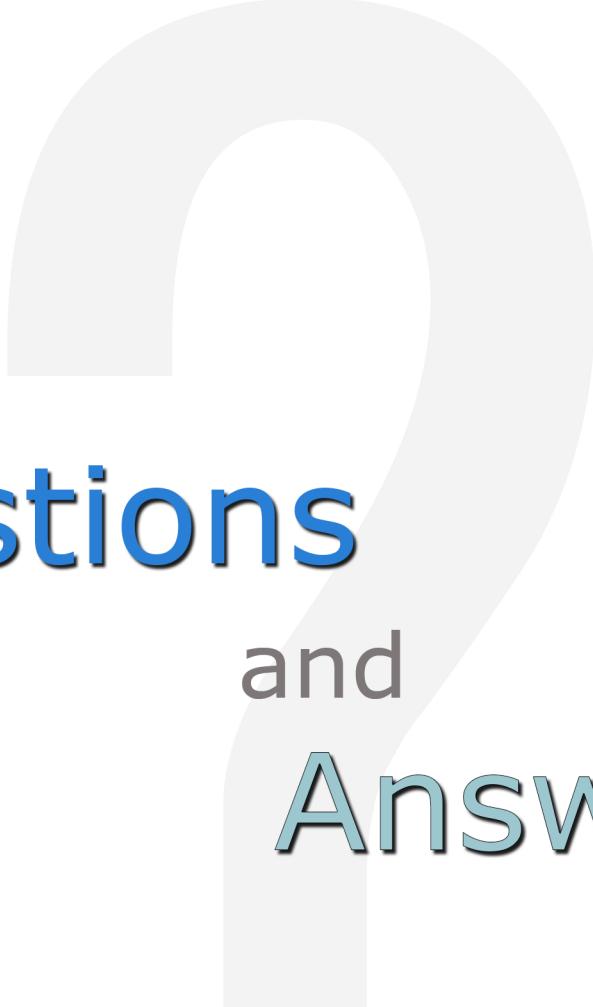
System at a Glance		PoE Port Status											
		1	3	5	7	9	11	13	15	17	19	21	23
USB													
	2	4	6	8	10	12	14	16	18	20	22	24	
PSE Details													
Port	Status	Power			Powered Device Type			Powered Device Class					
eth1/1	Delivering	5.5 Watts			802.3af			Class 0					
eth1/2	Searching	0.0 Watts			None			Class not defined					
eth1/3	Searching	0.0 Watts			None			Class not defined					
eth1/4	Searching	0.0 Watts			None			Class not defined					
Total Power for PoE Devices: 194.3 Watts				Total Power Used: 5.5 Watts				Remaining Power: 188.8 Watts					

PoE (Cont.)

- As children, we knew that 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 VoWi-Fi 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

Module Review

- History of PoE
 - PoE devices (overview)
 - Planning and deploying PoE



Questions and Answers

Review Questions:

1. True or False: Endpoint devices are typically PoE-enabled Ethernet switches.
 - A. True
 - B. False

2. PDs must be capable of accepting up to _____ volts from either the data lines or the unused pairs of the Ethernet cable.
 - A. 160
 - B. 45
 - C. 57
 - D. 1468

3. True or False: Link Layer Discovery Protocol (LLDP) is a standards-based layer 2 neighbor discovery protocol that can also be used for more detailed power classification.
 - A. True
 - B. False

4. The IEEE process to create a PoE standard began in?
 - A. 1999
 - B. 2002
 - C. 1998
 - D. 2000

5. At maximum power for a PD, the PSE must be capable of providing _____ or _____ of power to each PoE device, depending on whether your devices require PoE+.
 - A. 15w and 29.9w
 - B. 15.4w and 30w
 - C. 15.3w and 31w
 - D. 15.5w and 30w

Answer Key:

1. A
True. Endpoint devices are typically PoE-enabled Ethernet switches.
2. C
PDs must be capable of accepting up to 57 volts from either the data lines or the unused pairs of the Ethernet cable.
3. A
True. Link Layer Discovery Protocol (LLDP) is a standards-based layer 2 neighbor discovery protocol that can also be used for more detailed power classification.
4. A
The IEEE process to create a PoE standard began in 1999.
5. B
At maximum power for a PD, the PSE must be capable of providing 15.4W or 30W of power to each PoE device, depending on whether your devices require PoE+.

Certified Wireless Network Administrator
Module 18 – High Throughput (HT)

WORKBOOK

Module Introduction

- 802.11n-2009 amendment
- Wi-Fi Alliance certification
- MIMO
- HT channels
- HT MAC

802.11n-2009 Amendment

- The 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
 - The benefits of using MIMO are increased throughput and even greater range

Wi-Fi Alliance Certification

Feature	Explanation	Type
Support for two spatial streams	Access points are required to transmit and receive at least two spatial streams. Client stations are required to transmit and receive at least one spatial stream.	Mandatory
Support for three spatial streams	Access points and client stations capable of transmitting and receiving three spatial streams.	Optional (tested if implemented)

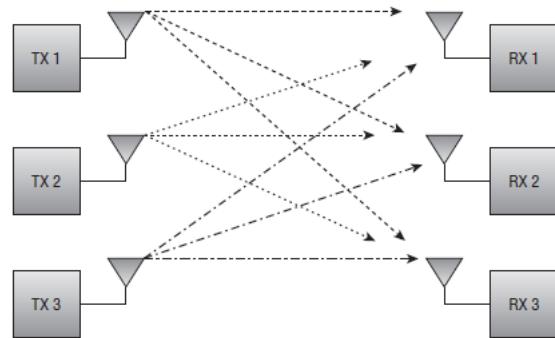
Wi-Fi Alliance Certification (Cont.)

Feature	Explanation	Type
Support for A-MPDU and A-MSDU in receive mode.	Required for all devices. Reduces MAC layer overhead.	Mandatory
Support for A-MPDU in transmit mode.		
Support for Block ACK	Required for all devices. Sends a single Block ACK frame to acknowledge multiple received frames.	Mandatory
2.4 GHz operation	Devices can be 2.4 GHz only, 5 GHz only, or dual-band. For this reason, both frequency bands are listed as optional.	Optional (tested if implemented)
5 GHz operation	Devices can be 2.4 GHz only, 5 GHz only, or dual-band. For this reason, both frequency bands are listed as optional.	Optional (tested if implemented)
Concurrent operation in 2.4 GHz and 5 GHz bands	This mode is tested for APs only. APs capable of operating in both bands are certified as "concurrent dual-band."	Optional (tested if implemented)
40MHz channels in the 5 GHz band	Bonding of two adjacent 20 MHz channels to create a single 40 MHz channel. Provides twice the frequency bandwidth.	Optional (tested if implemented)
20/40 MHz coexistence mechanisms in the 2.4 GHz band	If an AP supports 40 MHz channels in the 2.4 GHz band, coexistence mechanisms are required. Default 2.4 GHz channel size is 20 GHz.	Optional (tested if implemented)
Greenfield preamble	Greenfield preamble cannot be interpreted by legacy stations. The Greenfield preamble improves efficiency of the 802.11n networks with no legacy devices.	Optional (tested if implemented)
Short guard interval (short GI, 20 and 40 MHz)	Short GI is 400 nanoseconds; the traditional GI is 800 nanoseconds. Improves data rates by 10%.	Optional (tested if implemented)
Space-time block coding (STBC)	Improves reception by encoding data streams in blocks across multiple antennas. Access points can be certified after STBC.	Optional (tested if implemented)
HT Duplicate mode	Allows an AP to send the same data simultaneously on each 20 MHz channel within a bonded 40 MHz channel.	Optional (tested if implemented)

MIMO

- ❑ The heart and soul of the 802.11n amendment exists at the Physical (PHY) layer with the use of a technology known as multiple-input, multiple-output (MIMO)
 - ❑ MIMO requires the use of multiple radios and antennas, called radio chains
 - ❑ 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
 - ❑ MIMO systems can also use multiple antennas to provide for better transmit and receive diversity, which can increase range and reliability
 - ❑ There are various transmit and receive diversity techniques
 - ❑ Space-time block coding (STBC) and cyclic shift diversity (CSD) are transmit diversity techniques where the same transmit data is sent out of multiple antennas

MIMO (Cont.)

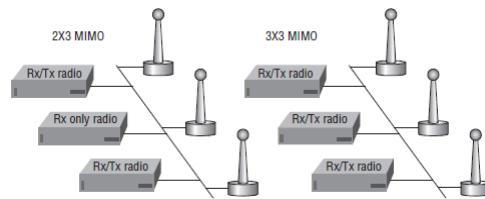


MIMO (Cont.)

- ❑ 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 analog/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

MIMO (Cont.)

- The use of multiple transmitters in a MIMO system provides for the transmission of more data via spatial multiplexing
 - The use of multiple receivers increases signal-to-noise ratio (SNR) because of advanced MIMO antenna diversity



Spatial Multiplexing (SM)

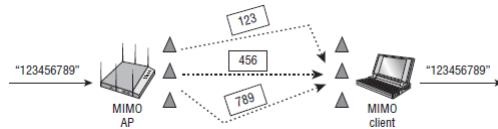
- You have already learned that MIMO radios will transmit multiple signals
- A MIMO radio also has the ability to send independent unique data streams
 - Each independent data stream is known as a spatial stream
 - Each unique stream can contain data that is different from the other streams transmitted by one or more of the other radio chains

Spatial Multiplexing (SM) (Cont.)

- The benefit of sending multiple unique data streams is that throughput is drastically increased
 - If a MIMO access point sends two unique data streams to a MIMO client station that receives both streams, the throughput is effectively doubled
 - If a MIMO access point sends three unique data streams to a MIMO client station that receives all three streams, the throughput is effectively tripled

Spatial Multiplexing (SM) (Cont.)

- Do not confuse the independent unique streams of data with the number of transmitters
 - In fact, when referring to MIMO radios it is important to also reference how many unique streams of data are sent and received by MIMO radios



MIMO Diversity

- If you cover one of your ears with your hand, will you hear better or worse with a single ear?
 - Obviously, you will hear better with two ears
- Do you think you would be able to hear more clearly if you had three or four ears instead of just two?
- Do you think you would be able to hear sounds from greater distances if you had three or four ears instead of just two?
 - Yes, a human being would hear more clearly and with greater range if equipped with more than two ears.
- MIMO systems employ advanced antenna diversity capabilities that are analogous to having multiple ears

MIMO Diversity (Cont.)

- ❑ Antenna diversity often is mistaken for the spatial multiplexing capabilities that are utilized by MIMO
 - ❑ Antenna diversity (both receive and transmit) is a method of using multiple antennas to survive the negative effects of multipath
 - ❑ As you just learned, MIMO takes advantage of multipath with spatial multiplexing to increase data capacity
 - ❑ Simple antenna diversity is a method of compensating for multipath as opposed to utilizing multipath
 - ❑ Multipath produces multiple copies of the same signal that arrive at the receiver with different amplitudes

Space-Time Block Coding (STBC)

- 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
 - STBC can be used when the number of radio chains exceeds the number of spatial streams
 - By sending copies of the same information on multiple antennas, the actual rate of the data transmitted does not increase as transmit antennas are added

Cyclic Shift Diversity (CSD)

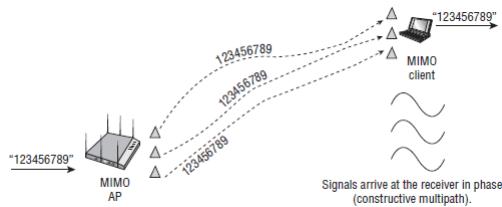
- ❑ Cyclic shift diversity (CSD) is another transmit diversity technique specified in the 802.11n standard
 - ❑ Unlike STBC, a signal from a transmitter that uses CSD can be received by legacy 802.11g and 802.11a devices
 - ❑ For mixed mode deployments, where 802.11n coexists with 802.11g and 802.11a devices, there is a need to have a way of transmitting the symbols in the legacy OFDM preamble over multiple transmit antennas

Transmit Beamforming (TxBF)

- The 802.11n amendment also proposes an optional PHY capability called transmit beamforming (TxBF), which uses phase adjustments
 - Can be used when there are more transmitting antennas than there are spatial data streams
 - Allows a MIMO transmitter using multiple antennas to adjust the phase and amplitude of the outgoing transmissions in a coordinated method
 - Results in constructive multipath communication, the result is a higher signal-to-noise ratio and greater received amplitude
 - Therefore, transmit beamforming will result in greater range for individual clients communicating with an access point

Transmit Beamforming (TxBF) (Cont.)

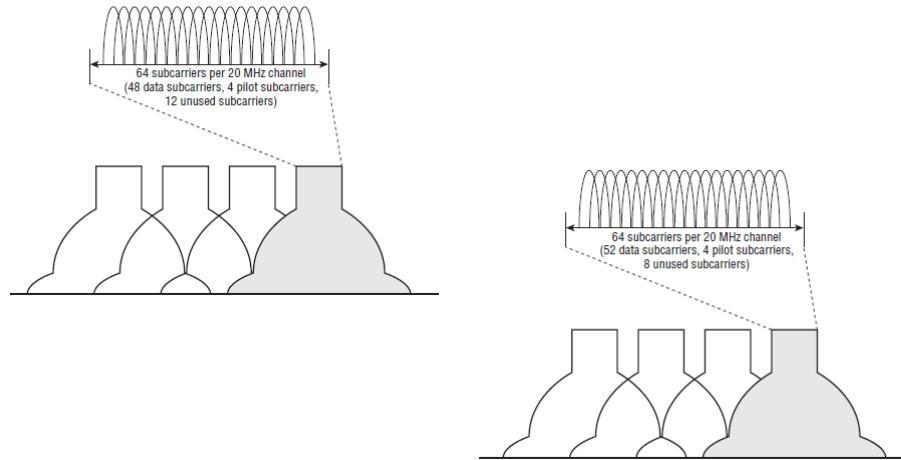
- Transmit beamforming relies on implicit feedback or explicit feedback from both the transmitter and receiver.
 - Any frame can be used as a sounding frame
 - Null function data frames can be used if another frame is not used
 - When using implicit feedback, the beamformer sends a sounding frame and then receives long training symbols transmitted by the beamformee, which allows the MIMO channel between the beamformee and beamformer to be estimated by the beamformer



20 MHz Non-HT and HT Channels

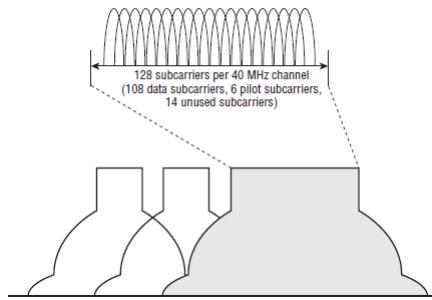
- ❑ 802.11a and 802.11g radios use 20 MHz OFDM channels
 - ❑ Each channel consists of 64 subcarriers
 - Forty-eight of the subcarriers transmit data
 - Four of the subcarriers are used as pilot tones for dynamic calibration between the transmitter and receiver
 - The remaining subcarriers are not used
 - ❑ OFDM technology also employs the use of convolutional coding and forward error correction
 - ❑ 802.11n (HT) radios also use the same OFDM technology and have the capability of using either 20 MHz channels or 40 MHz channels
 - The 20 MHz channels used by HT radios have four extra subcarriers and can carry a little more data than a non-HT OFDM channel
 - ❑ As a result, the HT 20 MHz channel with a single spatial stream can provide greater aggregate throughput for the same frequency space

20 MHz Non-HT and HT Channels (Cont.)



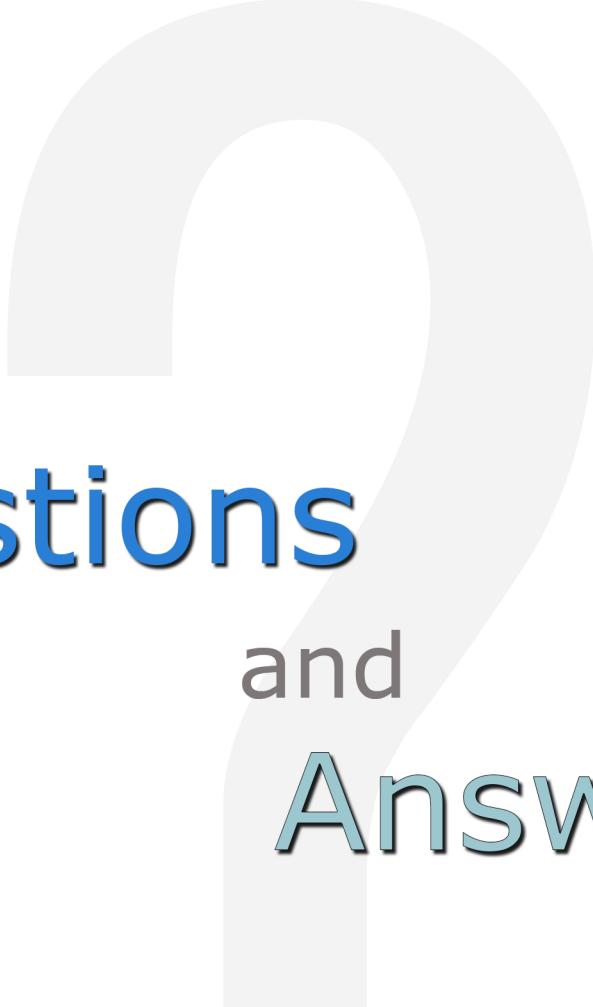
40 MHz Channels

- ❑ 802.11n (HT) radios also have the capability of using 40 MHz OFDM channels
 - ❑ The 40 MHz channels used by HT radios are essentially two 20 MHz OFDM channels that are bonded together
 - ❑ Each 40 MHz channel consists of a primary and secondary 20 MHz channel
 - ❑ The primary and secondary 20 MHz channels must be adjacent 20 MHz channels in the frequency in which they operate



Module Review

- 802.11n-2009 amendment
- Wi-Fi Alliance certification
- MIMO
- HT channels
- HT MAC



Questions and Answers

Review Questions:

1. True or False: SISO systems use a double radio chain.
 - A. True
 - B. False

2. True or False: Space-time block coding (STBC) is a method where the same information is transmitted on two or more antennas.
 - A. True
 - B. False

3. True or False: A MIMO radio has the ability to send dependent unique data streams.
 - A. True
 - B. False

4. True or False: Antenna diversity often is mistaken for the spatial multiplexing capabilities that are utilized by MIMO.
 - A. True
 - B. False

5. True or False: 802.11n (HT) radios have the capability of using 40 MHz OFDM channels.
 - A. True
 - B. False

Answer Key:

1. B
False. SISO systems use a single radio chain.
2. A
True. Space-time block coding (STBC) is a method where the same information is transmitted on two or more antennas.
3. B
False. A MIMO radio has the ability to send independent unique data streams.
4. A
True. Antenna diversity often is mistaken for the spatial multiplexing capabilities that are utilized by MIMO.
5. A
True. 802.11n (HT) radios do have the capability of using 40 MHz OFDM channels.

Certified Wireless Network Administrator
Module 19 – Very High Throughput (VHT)

WORKBOOK

Module Introduction

- 802.11ac-2013 amendment
- 5 GHz only
- 20, 40, 80, and 160 MHz channels
- 256-QAM modulation
- Modulation and coding schemes
- Single-user MIMO
- 802.11ac data rates

802.11ac

Technology	802.11n	802.11ac
Frequency	2.4 GHz and 5 GHz	5 GHz only
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Channel widths	20 MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz, 160 MHz
Spatial streams	Up to four	Up to eight on APs, up to four on clients
Short Guard Interval Support	Yes	Yes
Beamforming	Multiple types, both implicit and explicit, not typically implemented	Explicit beamforming with null data packets (NDPs)
Number of modulation and coding schemes (MCSs)	77	10
Support for A-MSDU and A-MPDU	Yes	Yes, all frames transmitted as A-MPDU
MIMO support	Single-user MIMO	Single-user MIMO and multiuser MIMO (MU-MIMO)
Maximum # of simultaneous user transmissions	One	Four
Maximum data rate	600 Mbps	6.933 Gbps

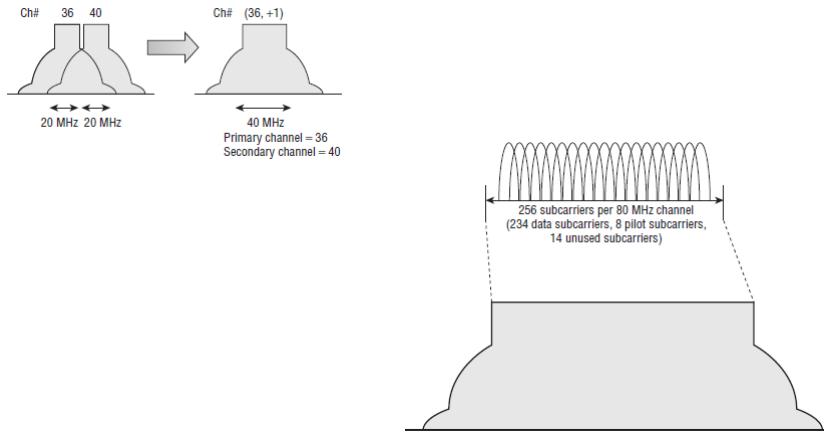
802.11ac (Cont.)

- With the introduction of 40 MHz channels in 802.11n and the limit of 3 non-overlapping channels in the 2.4 GHz band, enterprises cannot effectively implement 40 MHz channels with their 2.4 GHz radios
- In order to benefit from the faster data rates of 802.11n, companies have migrated to 5 GHz radios

802.11ac (Cont.)

- 802.11ac channels are a further evolution of the enhancements that were introduced with the 802.11n amendment
 - When Orthogonal Frequency Division Multiplexing (OFDM) was introduced with 802.11a, the channels were 20 MHz wide
 - When two 20 MHz HT channels are bonded together, some of the formerly unused subcarriers at the bottom of the higher channel and at the top end of the lower channel are able to be used to transmit data

802.11ac (Cont.)

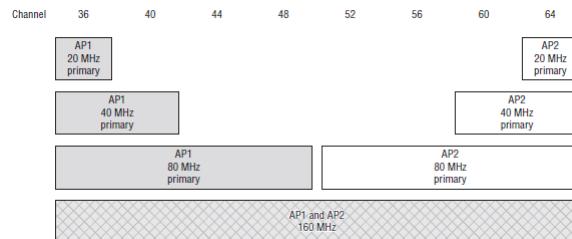


802.11ac (Cont.)

- The second channel width that was introduced with 802.11ac is a 160 MHz channel
- As you might deduce, the 160 MHz channel is made up of two 80 MHz channels
- 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

802.11ac (Cont.)

- Choosing four channel groupings for an AP may not seem that difficult, but it becomes much more difficult and important when choosing channels for multiple APs



802.11ac (Cont.)

- ❑ 256-QAM is an evolutionary upgrade that was introduced with 802.11ac
 - ❑ The 802.11a amendment introduced 64-QAM modulation
 - 64-QAM identifies 64 unique values
 - Essentially performs a phase shift that can differentiate eight different levels and also performs an amplitude shift, which can also differentiate eight different levels
 - ❑ Combine the two of them and the system has the ability to identify the 64 unique values
 - ❑ Having 64 distinct values provide the ability for each value to represent 6 bits ($2^6 = 64$)

802.11ac (Cont.)

- 256-QAM is used for the highest modulation coding sets
 - To achieve these higher data rates, higher signal-to-noise ratios are needed
 - This also means that the clients need to be close to the AP in order to achieve these data rates
 - Since a 256-QAM signal can transmit 8 bits per subcarrier compared with the 6 bits that were transmitted with 64-QAM, a speed increase of 33 percent is achieved solely by deploying this feature

802.11ac (Cont.)

- Although the amendment specifies a maximum of eight spatial streams, it is unlikely that APs that support eight streams will be manufactured any time soon
 - The second wave of 802.11ac access point chipsets that are expected to support MU-MIMO will most likely be 4x4:4 radios
 - It is also likely that 4x4:4 radios will emerge in laptop radios
 - 802.11ac radios in tablets and smartphones will most likely remain 1x1:1 or 2x2:2 due to battery life and the increased power required to implement multiple-spatial-stream radios

802.11ac (Cont.)

- With single-user MIMO, beamforming is used to focus a signal to a client
 - This focused transmission should increase the level of the signal that the client receives—and hopefully allow the AP and client to communicate using a higher data rate than would be possible without 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

802.11ac (Cont.)

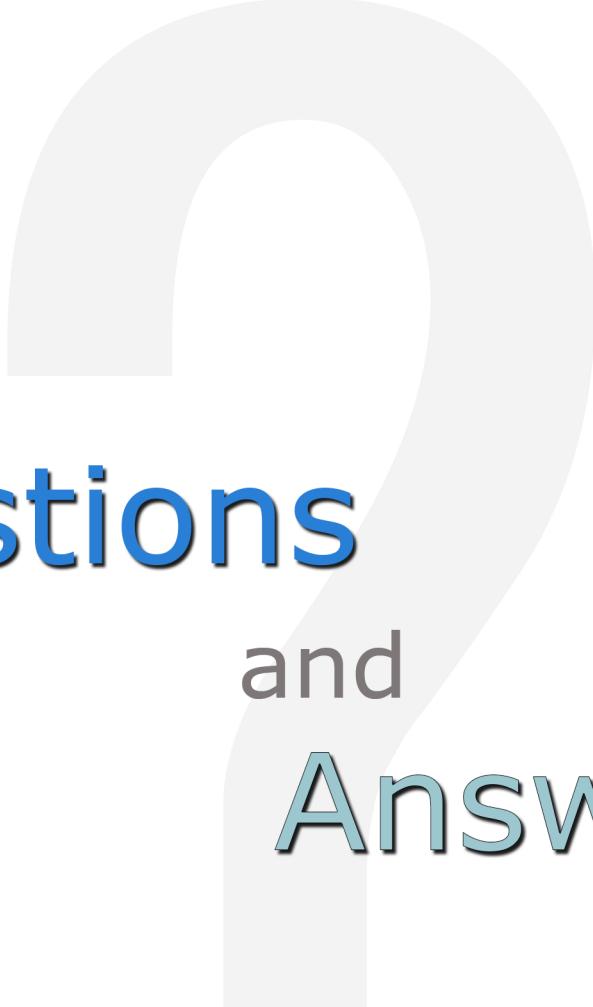
- The second phase of 802.11ac may require faster uplink technology than Gigabit Ethernet
 - The second phase of 802.11ac is expected to support channel widths of up to 160 MHz and four spatial streams
 - Since the AP will support four spatial streams, the 2.4 GHz 802.11n maximum transmission speed will increase from 450 Mbps to 600 Mbps

802.11ac (Cont.)

Feature	Mandatory	Optional
Channel width	20, 40, 80 MHz	80+80, 160 MHz
Modulation and coding	MCS 0–7	MCS 8,9
Spatial streams	One for clients, two for APs	Two to eight
Guard Interval	Long (800 nanoseconds)	Short (400 nanoseconds)
Beamforming feedback		Respond to beamforming sounding
Space-time block coding (STBC)		Transmit and receive STBC
Low-density parity check (LDPC)		Transmit and receive LDPC
Multiuser MIMO		Up to four spatial streams per client, using the same MCS

Module Review

- 802.11ac-2013 amendment
- 5 GHz only
- 20, 40, 80, and 160 MHz channels
- 256-QAM modulation
- Modulation and coding schemes
- Single-user MIMO
- 802.11ac data rates



Questions and Answers

Review Questions:

1. True or False: With the introduction of 40 MHz channels in 802.11n and the limit of 3 non-overlapping channels in the 2.4 GHz band, enterprises cannot effectively implement 40 MHz channels with their 2.4 GHz radios.
 - A. True
 - B. False
2. When Orthogonal Frequency Division Multiplexing (OFDM) was introduced with 802.11a, the channels were _____ MHz wide.
 - A. 40
 - B. 30
 - C. 20
 - D. 10
3. True or False: 128-QAM is an evolutionary upgrade that was introduced with 802.11ac.
 - A. True
 - B. False
4. The second channel width that was introduced with 802.11ac is a _____ MHz channel.
 - A. 80
 - B. 40
 - C. 160
 - D. 360
5. True or False: In 802.11ac, the two 80 MHz channels have to be adjacent.
 - A. True
 - B. False

Answer Key:

1. A
True. With the introduction of 40 MHz channels in 802.11n and the limit of 3 non-overlapping channels in the 2.4 GHz band, enterprises cannot effectively implement 40 MHz channels with their 2.4 GHz radios.
2. C
When Orthogonal Frequency Division Multiplexing (OFDM) was introduced with 802.11a, the channels were 20 MHz wide.
3. B
False. 256-QAM is an evolutionary upgrade that was introduced with 802.11ac.
4. C
The second channel width that was introduced with 802.11ac is a 160 MHz channel.
5. B
False. The two 80 MHz channels do not have to be adjacent.

Certified Wireless Network Administrator
Module 20 - BYOD

WORKBOOK

Module Introduction

- Mobile Device Management
- Guest WLAN access

Mobile Device Management

- Consumerization of IT is a phrase used to describe a shift in information technology (IT) that begins in the consumer market and moves into business and government facilities
 - It has become common for employees to introduce consumer market devices into the workplace after already embracing new technology at home
 - Personal mobile Wi-Fi devices, such as smartphones and tablets, have been around for quite a few years
 - The Apple iPhone was first introduced in June 2007, and the first iPad debuted in April 2010

Mobile Device Management (Cont.)

- Because of the proliferation of personal mobile devices, a BYOD policy is needed to define how employees' personal devices may access the corporate WLAN
- A Mobile Device Management (MDM) solution might be needed for onboarding personal mobile devices as well as Company-Issued Devices (CIDs)

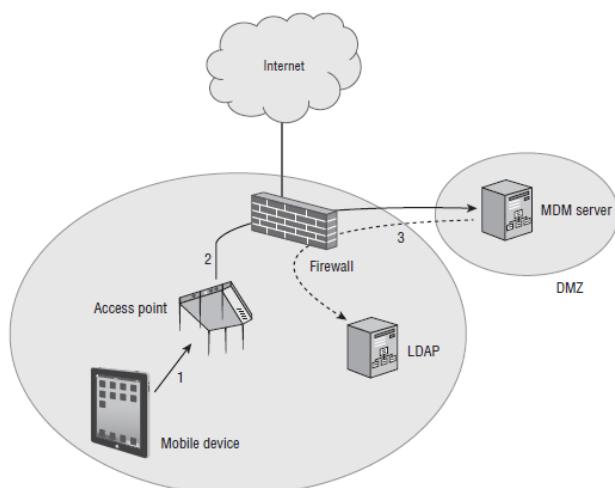
Company-Issued Devices vs. Personal Devices

- An MDM solution can be used to manage both company-issued devices and personal devices
 - The management of CID and BYOD is quite different
 - A company-issued device was purchased by the company with the intent of enhancing employee performance
 - A tablet or smartphone might be issued to an individual employee or shared by employees on different shifts
 - 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

Company-Issued Devices vs. Personal Devices (Cont.)

- The basic architecture of any MDM solution consists of four main components:
 - Mobile Device
 - Requires access to the corporate WLAN
 - Can be either a company-owned or employee-owned device
 - AP/WLAN Controller
 - All 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
 - Responsible for enrolling client devices
 - Provisions the mobile devices with MDM profiles that define client device restrictions as well as configuration settings
 - Push Notification Servers
 - The MDM server communicates with push notification servers for over-the-air management of mobile Wi-Fi devices
 - Apple Push Notification service (APNs)
 - Google Cloud Messaging (GCM)

Company-Issued Devices vs. Personal Devices (Cont.)



MDM Profiles

- We have already learned that MDM profiles are used for mobile device restrictions
 - The MDM profiles can also be used to globally configure various components of a mobile device
 - MDM profiles are essentially configuration settings for a mobile device

MDM Agent Software

- The operating systems of some mobile devices require MDM agent application software
 - Android devices require an MDM agent application
 - The OS is an open-source operating system that can be customized by the various mobile device manufacturers
 - While this provides much more flexibility, managing and administering Android devices in the enterprise can be very challenging due to the sheer number of hardware manufacturers
 - Steps
 - An employee downloads the MDM agent from a public website or company website and installs it on their Android device
 - The MDM agent contacts the MDM server over the WLAN and is typically required to authenticate to the server
 - The MDM agent must give the MDM server permission to make changes to the device and function as the administrator of the device

Over the Air Management

- Once a device has been provisioned and enrolled with an MDM server, a permanent management relationship exists between the MDM server and the mobile device
 - The MDM server can monitor device information
 - Device name
 - Serial number
 - Capacity
 - Battery life
 - Applications installed
 - Some information cannot be seen/monitored
 - SMS messages
 - Personal emails
 - Calendars
 - Browser history
- The mobile device can still be managed remotely, even if the mobile device is no longer connected to the corporate WLAN
- The MDM server can still manage the device as long as the device is connected to the Internet from any location

Over the Air Management (Cont.)

- 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

Guest WLAN

- Although the primary purpose for enterprise WLANs has always been to provide employees wireless mobility
 - WLAN access for company guests can be just as important
 - Customers, consultants, vendors, and contractors often need access to the Internet to accomplish job-related duties
 - When they are more productive, employees will also be more productive
 - Guest access can also be a value-added service and often breeds customer loyalty

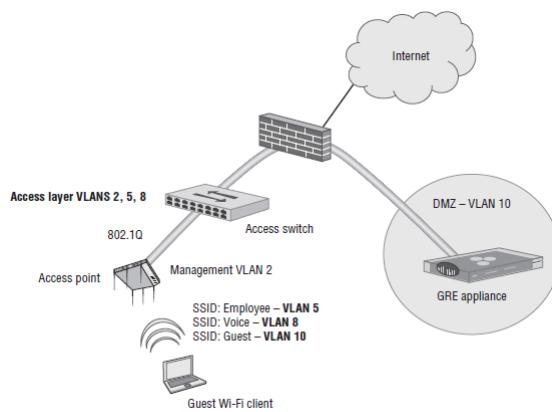
Guest WLAN (Cont.)

- Today, the more common method is to place all employees on the same SSID and leverage Remote Authentication Dial-In User Service (RADIUS) attributes to assign different groups of users to different VLANs
- What has not changed over time is the recommendation that all guest user traffic be segmented onto a separate SSID

Guest WLAN (Cont.)

- Guest user traffic should be segmented into a unique VLAN tied to an IP subnet that does not mix with the employee VLANs
 - Segmenting your guest users into a unique VLAN is a security and management best practice
 - The main debate about the guest VLAN is whether or not the guest VLAN should be supported at the edge of the network
 - 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

Guest WLAN (Cont.)



Guest Isolation

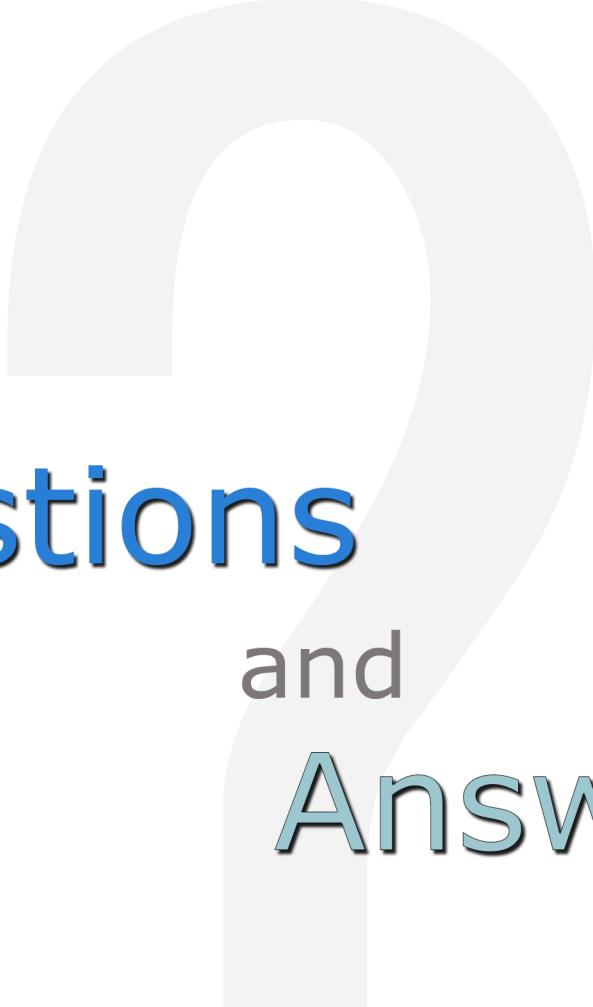
- When guest users are connected to the guest SSID, they are all in the same VLAN and the same IP subnet
 - Because they reside in the same VLAN, the guests can perform peer-to-peer attacks against each other
 - Client isolation is a feature that can be enabled on WLAN access points or controllers to block wireless clients from communicating directly with other wireless clients on the same wireless VLAN
 - Client isolation (or the various other terms used to describe this feature) usually means that packets arriving at the AP's wireless interface are not allowed to be forwarded back out of the wireless interface to other clients

Guest Registration

- Guest management solutions have always relied on a company receptionist or lobby ambassador to register the guest users
 - 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
 - Commonly referred to as self-registration

Module Review

- Mobile Device Management
- Guest WLAN access



Questions and Answers

Review Questions:

1. True or False: Consumerization of IT is a phrase used to describe a shift in information technology (IT) that begins in the consumer market and moves into business and government facilities.
 - A. True
 - B. False
2. The basic architecture of any MDM solution consists of:
 - A. Mobile Device
 - B. AP and WLAN Controller
 - C. MDM Server
 - D. All of the above
3. True or False: MDM profiles can be used to globally configure various components of a mobile device.
 - A. True
 - B. False
4. Do Android devices require an MDM agent application?
 - A. Yes
 - B. No
5. True or False: 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.
 - A. True
 - B. False

Answer Key:

1. A
True. Consumerization of IT is a phrase used to describe a shift in information technology (IT) that begins in the consumer market and moves into business and government facilities.
2. D
The basic architecture of any MDM solution consists of mobile devices, AP and WLAN controller and MDM server.
3. A
True. MDM profiles can be used to globally configure various components of a mobile device.
4. A
Yes. Android devices do require an MDM agent application.
5. A
True. 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.