# Section 15:Wireless Networking

** 116. Introduction to 802.11**
Basics:

The wireless standard is 802.11.

802.11 uses radio waves.

WAP - Wireless access point (Bridging device)

SSID - Service set Identifier

Two ways to do 802.11:

1. Infastructure mode - Means that you are using a wireless access point
2. Ad hoc mode - creating a local network with your computer

- BSSID (Basic Service Set Identifier) - A single WAP with a single SSID
- ESSID (Extended Service Set Identifier)Lots of wireless access points with a switch on the same broadcast domain with the same SSID

802.11 have been designed to run in the ISM (Industrial Service and Medical) bands. There are a number of bands but the two we use for 802.11 are the 2.4GHz band and the 5.0GHz band.

A band is a range of frequencies or "Channels"

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

Transmission of the data comes in two forms:

1. Direct-sequence spread-spectrum (DSSS) - Sub frequencies in a channel. A signal gets spread between those frequencies and if one gets stopped then another one would get through. (Old way)
2. OFDM (Orthogonal frequency-division multiplexing) (Modern way) - Using a type of spread spectrum but the channels, especially in the 5GHz frequency, can be very wide.

Review:

- A WAP is a bridging device that connects into an Ethernet network and communicates via radio waves to wireless clients
- A WAP has an SSID (Service Set Identifier), a word or phase used to connect wireless devices to the WAP device.
- CSMA/CA (Carrier sense mulitple access with collision avoidance) is the method used to prevent wireless collisions.

---

**117. 802.11 Standards**

These will be on the net plus

** 802.11b **

- ran at 11Mbps
- ran on the 2.4GHz Band (14 Channels, 11 in the US) -The problem with these channels is that they overlap. So really we only have three channels 1, 6 or 7, and 11 without overlapping
- DSSS (Direct-sequence spread-spectrum)

**802.11a**

- runs on 5GHz range
- has channels (but we dont discuss them in 5GHz range)
- 54Mbps
- OFDM (Orthoganal frequency-division multiplexing)

**802.11g**

- Changed the game
- runs on 2.4GHz band
- runs at 54Mbps
- OFDM (Orthoganal frequency-division multiplexing)
- backward compatible with 802.11b

**802.11n**

- was a way to increase the speed beyond 54Mbps
- was a way to move into the 5GHz range
- runs at both 2.4GHz and 5GHz band
- Can run at 108-300Mbps
- MIMO - muliple channels to talk to different devices.
- OFDM
- Invented a different kind of packet so to be backward compatible you had to enter legacy modes
- Greenfield mode = all n devices on network
- Lots of antennas

**802.11ac**

- Runs in the 5GHz band
- can also run in the 2.4GHz band but not for 802.11ac
- Has backward compatibility but only *by making an better access point*, NOT because 802.11ac is different.
- 1GBps +++
- It builds on the 802.11 MIMO concept and uses MU-MIMO (Multi User -MIMO)

Review:

*Early wireles standards were 802.11b (2.4GHz) and 802.11a(5.0GHz)
*First widely used standard was 802.11g (2.4GHz)
*Current fastest standards are 802.11n and 802.11ac

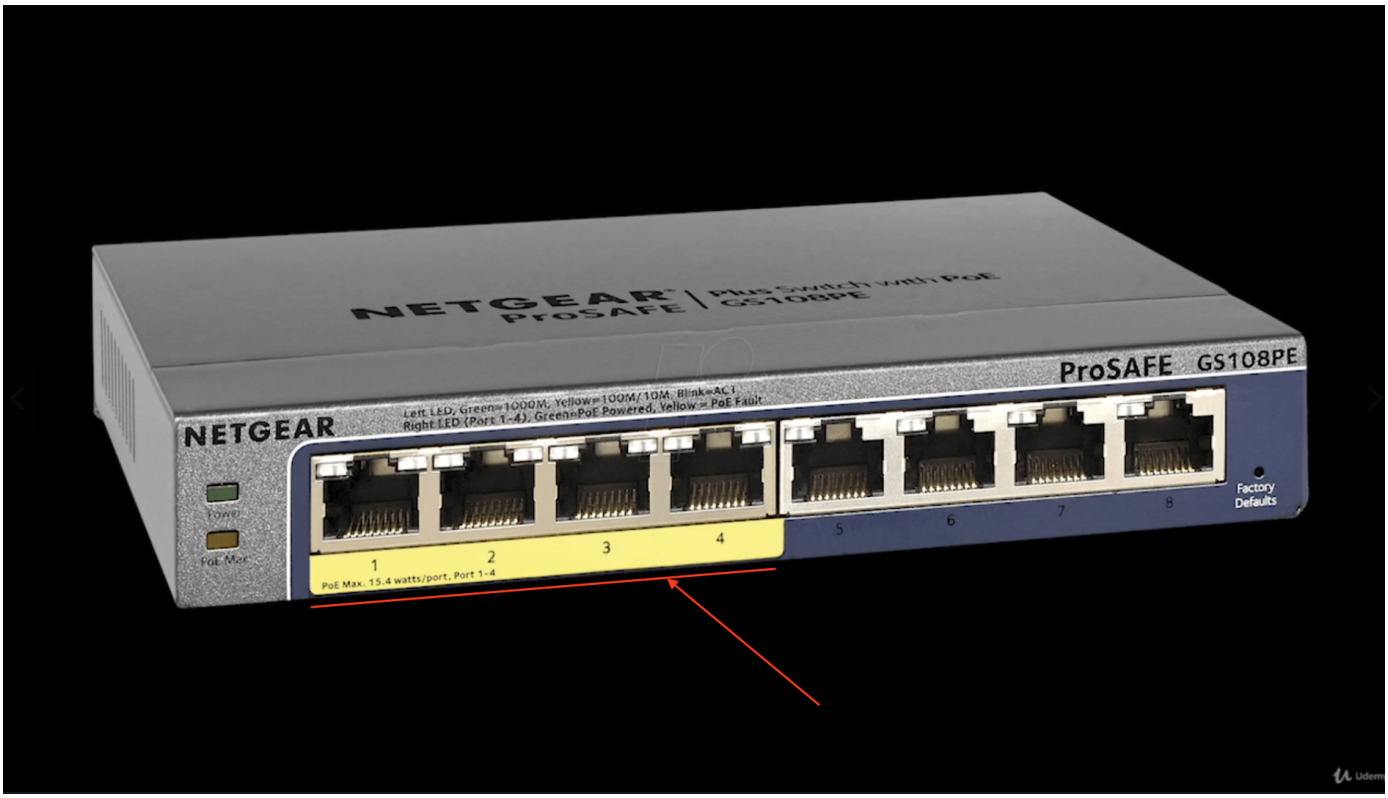
---

**118. Power over Ethernet**

802.3 standard - Power over Ethernet - Common with wireless access points

Need a PoE wireless adapter and a PoE capable Switch

PoE Switch:




If you don't have a PoE switch you can used a PoE injector (Has to have power):

**The original PoE standard was PoE 802.3af (15.4 watts)**
**The max wattage was a problem. It was not enough. So a new version came out called**

**PoE+ 802.3at, 30watts**

Review:

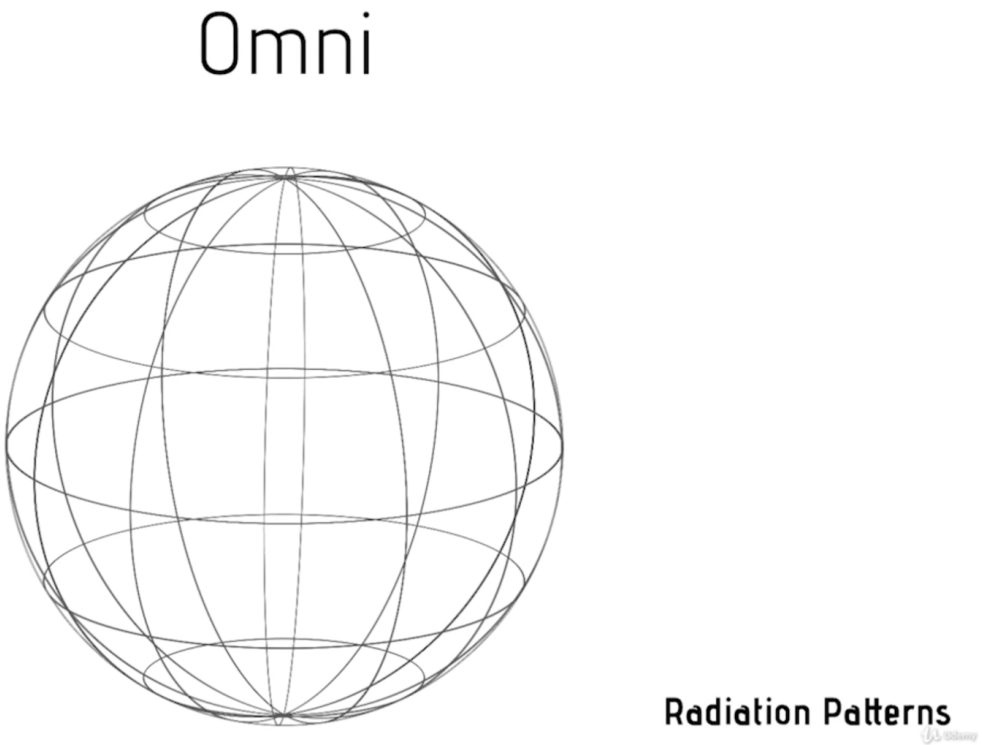
*A PoE WAP needs to use a PoE switch or a PoE injector but does not need a direct connected 110 plug.
*PoE uses 802.3af orignally, but has been replaced with PoE+ using 802.3at standard that supports the newer WAPs supporting to 30 watts

---

**119. Antennas**

802.11 is radio waves so lets talk about antennas

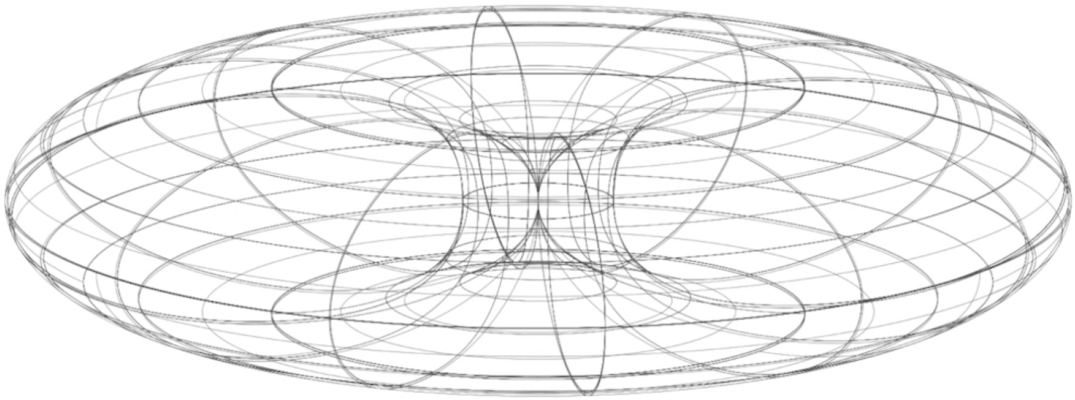
Omni antenna - a single metal antenna that comes to a point (compTIA uses the terms omni antenna)




---

Dipole antenna - two antennas that are equal to each other, connected at a point, and pointing in opposite directions. (common in 802.11)

# Dipole

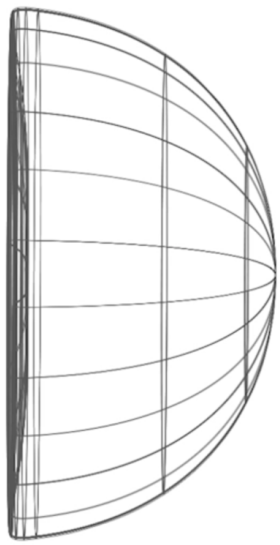


Radiation Patterns

---

Patch antenna: (Extremely common in enterprise environments)

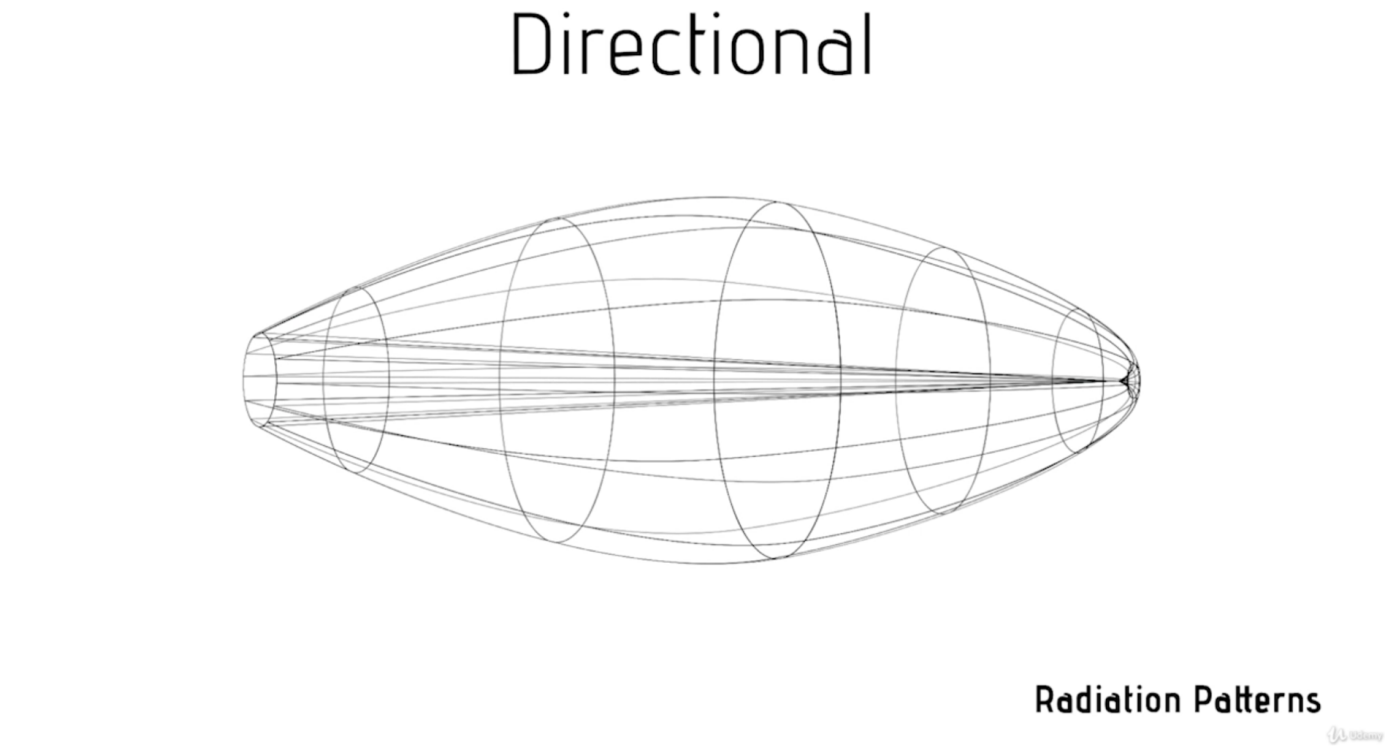
# Patch



Radiation Patterns

---

Directional/Yagi antenna - Extremely directional (popular for connecting two buildings)




---

Directional/Parabolic - stronger than yagi (Looks like a satellite dish)

SMA (SubMiniature version A) Connector:


*We can change the size of the radiation pattern by increasing or decreasing the GAIN on the antenna.
*Gain is measured in dBi (decibles)

Review:
*Exam with ask what kind of antenna to use, what kind of gain you would use and what the coverage will be.

*Different types of antennas have different radiation patterns and can be placed to provide a radiation pattern to meet wireless requirements
*Patch antennas are regularly used on exterior walls
*Antenna placement and the gain should be considered when selecting antenna types, locations, and security boundaries.

---

**120. Wireless Security Standards**

*Original 802.11 used passphrase for authentication

*Open/Shared

*Closed - needed a passphrase

-WEP (wired equivelent privacy)
-Authentication providing a passphrase and then encryption with that passphrase

*WEP was an authentication that got thrown out the door but WEP also had encryption

Original WEP worked great but had a problem:
-Used RC4 protocol (a streaming protocol) and that was an issue

802.11i - was supposed to fix problems including the problems with WEP but it was going to take too much so they came up with WPA.

WPA is an improvement on WEP. Fixed the initilization vector problem with TKIP.

TKIP (Temporal Key Integrity Protocol) - More robust than WEP. Used the same RC4 protocol except it fixed the initialization vector issue from being so predictable.

RC4 was still crackable with TKIP so they came out with AES

WPA2 with AES (A block cipher)- used CCMP AES

CCMP-AES (Counter Mode Cipher Block Chaining Messaging Authentification Code Protocol Counter Mode CBC-
Mac Protocol)

WPA and WPA2 predated 802.11i

On the Exam questions will be asked with TKIP and CCMP so think like this:

WPA = TKIP
WPA2 = AES with CCMP

WPA-PSK: PSK = (Pre shared Key)

Part of the 802.11 standard also included enterprise: You have to use a RADIUS server IP, Port, and password to configure.

For the Exam remember:

WEP 64bit and 128bit key which was really 40bit and 104 bit, WEP is easily crackable

WPA uses TKIP, More robust than WEP, but is still fairly crackable today

WPA2 is the standard today. If using WPA2 use long passords

Review:

*The 802.11 standards are used on both SOHO routers and Enterprise routers
*802.11i was slow to release, so WPA was created using TKIP encryption protocol
*WPA2 uses CCMP-AES as the encryption protocol and is more secure

---

**121.Implementing Wireless Security**

*SSID Broadcast - be aware of for the NET+ but it's not very useful
*MAC ACL - Access Control list based on MAC addresses
*Multiple SSID
*DHCP issue limiting
*Change the default username and password
*Remote Management - Can you access a wireless configuration screen from a wireless network?
*Client Isolation - Single wireless access point that many people are connected to (everyone can see everyone) but with client isolation everyone on the same SSID can not see each other.

Review:

*Disable SSID Broadcast
*Use MAC filtering
*Limit the number of DHCP-issued addresses

---

**122. Threats to your wireless network**

Rogue AP (An unauthorized Access Point) - an access point plugged into a wired network by someone

Evil Twin - An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications.

802.11 jammer are completely illegal in the US
With a jammer you can program to be on a specific channel to jam up the traffic and then create your own hotspot with the same SSID on a different channel

802.11 Jammer:



Instead of using a wireless jammer you can do a "Deauthentication Attack" (Deauth commands)

A Kali machine sends computers on a network a command to get off/log off and then they log on to us and this is a man in the middle attack.

Review:

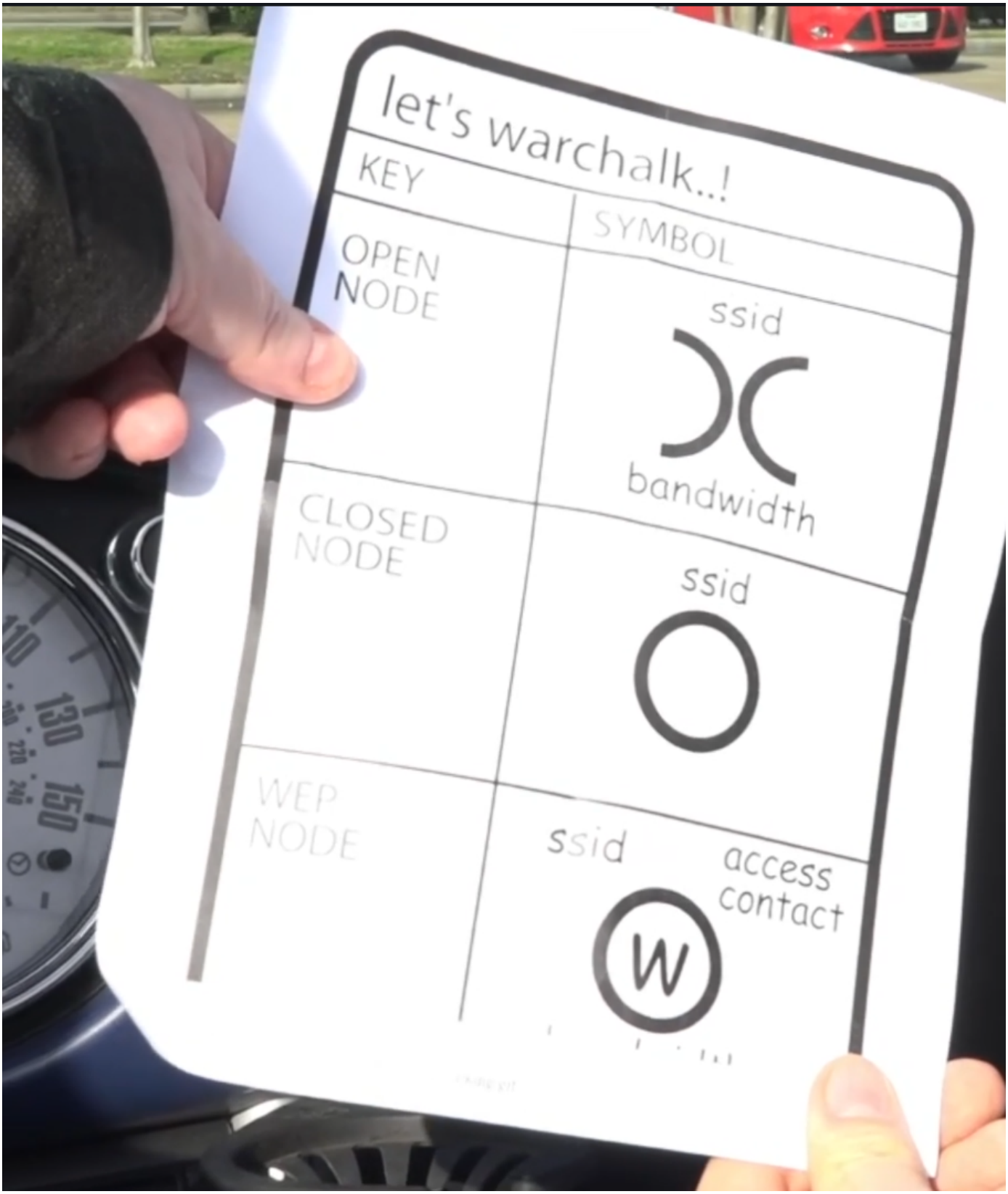
*Rogue access points can be accidental, but evil twins are intentional
*Illegal 802.11 jammers can knock everyone off a network

*Rouge access points and evil twins can cause a lot of headaches

---

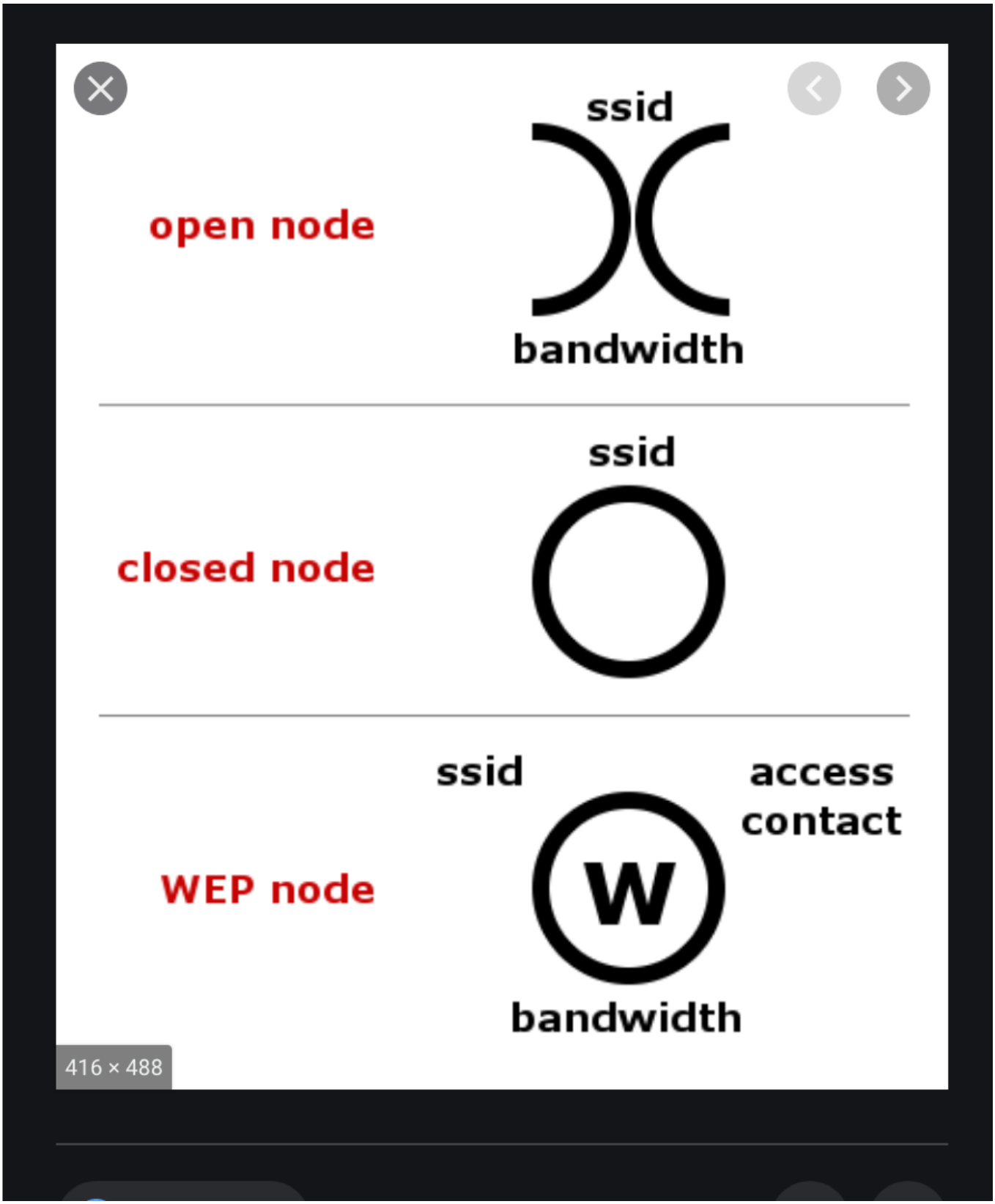
**123. Retro Threats**

War Driving - driving around in a car with an antenna and looking for wireless networks.
War Chalking - Need to know the symbols. (literally finding networks and writing with chalk)




Review:

*War driving is the act of driving around and mapping the location and state of wireless access points
*War chalking is drawing a symbol on the sidewalk indicating the current stat of a present WAP
*Remember the War Chalking symbols for the Net+




**124. Wi-Fi Protected Setup (WPS)**

-the idea was to take your WAP or router and press a button. You now have about 60 seconds to press a button on the other device and they would configure themselves.

The cornerstone of WPS is an 8 Digit code that is being queryed and passed between the devices. The code is broken up into two four digit code.

**WPS is very hackable.

Review:

- WPS enables one-button setup of wireless devices
- All modern wireless devices are WPS-enabled
- WPS can be a security threat

---

**125. Enterprise Wireless**

Wireless Controller - Can be a switch or a piece of software sitting on a server that allows us to control all of our wireless devices simultaneously

Review:

- Enterprise wireless systems have multiple WAPs that can all have the same wireless controller for configuration setup
- The wireless controller can monitor traffic, set up various zones or access areas, and define services' access to specific WAP destinations
- The 802.11 Standards are used on both SOHO routers and enterprise routers

---

**126. Installing a Wireless Network**

1. Need a floor plan.
2. Need to go through a site survey - Walking around in the area and plotting sources
   -Use a wifi analyzer
   -Check channels
   -Generate a heat map
3. Antenna placement (match your 802.11 standard to requirements)
   -Use a patch on the outer walls to shoot signal one direction or
   -Use a dipole that is centralized
   -There is not right or wrong placement until you find dead spots
   -Use of highly directional antennas between buildings
   -Signal to noise ratio is a relative gauge of strength (SNR).
   -Wireless range extender - self standing device that acts as a wireless repeater that allows a signal to come in and make a stronger signal.

Interference could be an issue
Reflection could be an isse be an issue (metal)
Refraction could be an issue (glass)
Absorbtion could be an issue(concrete walls)
Attenuation could be an issue Distance limitations

*Mesh Networks - great for getting rid of dead spots in a wireless network

On the exam:
-Be ready to know placement questions.
-Know antenna signals propogate and I should be good.
-Remember you can use WiFi analyzers to look for dead spots

Review:

- Interference, reflections, and absorbtion are all environmental issues that can affect the wireless signal
- A wi-Fi signal is different on various devices; match raditation patterns and 802.11 specifications to the signal requirment
- Pay attention to the bandwidth and use channels with the least amount of congestion

---

**127. Wireless Scenarios**

Problems you can run into:

1. Interference
   a. Can affect speeds (check your speeds), find the established link speed and see if its slow.
   b. Use Windows utilities to check wireless speeds
2. log into a new network and it says youre connected but you can't get on internet you need to check your IP. If you have a 169.254 (APIPA) address you've probably typed in the wrong WPA password.
3. When you've been working on a network for a long time and suddenly you cannot get on.
   a. Changes to WAP settings will no longer match client profiles.
   b. To fix go to settings and forget the network and log back on to re-establish profile

Review:

- Interference can disrupt or slow wireless connections
- Sources of interference can include other WAPs, wireless mice and keyboards, and even microwaves
- Remove sources of interference or change the WAPs frequency to avoid interference.

---

**128. More Wireless Scenarios**

*The Slow Wireless Network:*

1. Over Capacity - Don't have enough wireless access points on your networks to meet your needs (too many people on the network)
2. Jitter - frames showing up out of order. Only an issue with voice over IPs or videos etc. Manifests as Stops chops, break ups, etc. There is no simple fix. One of the only things you can do is get your capacity up **This will be on the exam** *If you are exposed to Jitter you need to get your capcity up*

*Antenna Problems*

1. Incorrect antenna types
2. Incorrect antenna placement

- For the exam: You may need a certain antenna type for a specific placement
- Antenna with a long cable eats your gain up.

Review:

- Adding or updating access points with more robust 802.11 standard devices should be considered for slow wireless network
- Be aware of gain loss due to length of cable and keep cables short when possible
- Antenna placement is a bit of an art; test and retest to ensure expected coverage

---

**QUIZ**

1. What does ad-hoc mode describe?
   a. Wireless devices connected to a WAP
   b. A bluetooth environment comprised of a mouse and keyboard
   **c. Wireless network comprised only of peer computers**
   d. 802.11 network
2. PoE describes what?
   a. Using power lines to carry Ethernet data
   b. Using wireless access points to provide power to wireless clients
   **c. Using Ethernet cables to carry data and power to network devices**
   d. Using power cables as wireless antennas in Wi-Fi environments
3. Which of the following is not an antenna type typically found in a Wi-Fi environment?
   **a. Tripole**
   b. Dipole
   c. Patch
   d. Yagi
4. Which of the following is not a security task that should be performed on a new WAP?
   **a. Enable backward compatibility**
   b. Change administrator account and password
   c. Enable encryption
   d. Disable SSID broadcast
5. Which term describes the process of scouting for Wi-Fi networks that may be vulnerable?
   **a. War driving**
   b. Snooping
   c. Sniffing
   d. Fox hunting

6. Documenting a "find" after a war driving excursion is known as what?
   a. War marking
   b. Blogging
   **c. War Chalking**
   d. Updating
7. WPS is used for what purpose?
   a. Automatically shares the Wi-Fi password
   b. Automatically sets up a personal area network
   c. Automatically applies protection services to wireless devices
   **d. Automatically configures a wireless device to connect to a WAP**
8. Which choice is not a step in planning and installing wireless networks?
   a. Plan the WAP locations
   b. Perform site survey
   **c. Install patch antenna(s)**
   d. Configure WAP Security
9. Which choice in not a typical Wi-Fi problem?
   a. Interference
   **b. WPS failure**
   c. Wrong WAP password
   d. WAP configuration has changed