NETW2000 - Study Guide

The differences between the topologies

WWAN - Wireless Wide Area Network

- a wireless network that covers a large geographical area
- ex. EDUROAM

WMAN - Wireless Metropolitan Area Network

- a wireless network that covers an area such as a city
- ex. New York City / Edmonton Rec Centers

WPAN - Wireless Personal Area Network

- used for communication between computer devices within proximity of a user
- ex. Bluetooth, peer-to-peer, ad hoc

WLAN - Wireless Local Area Network

- a LAN but wireless
- ex. Home Wi-Fi

WLAN components

BSS - Basic Service Set

- a group of wireless devices served by a single AP

SSID - Service Set Identifier

- serves as the network name for the BSS

BSSID - Basic Service Set Identifier

- MAC (media access control) address of the AP

IBSS - Independent Basic Service Set

- a group of two or more clients that communicate without using an AP (ad hoc or peer-to-peer)

Types of WLAN deployments:

Autonomous

- most common with "**standalone**" AP | aka **autonomous** AP or **fat** AP
- all the configs are in the AP itself
- at **least** two physical interfaces PLUS one for management
  - RF radio, ethernet port, BVI (bridge between the two, for management)
- typically POE and deployed at access layer

Centralized

- requires a **wireless controller** - this allows you to manage and configure APs | **lightweight** APs or **thin** APs
- lightweight APs do not contain the management and configuration functions
- WLC (wireless LAN controller) can be centrally configured, settings auto distributed to all APs | can be placed at core, distribution, or access layer

WLC features:

- AP management
- WLAN Management
- User Management
- Device Monitoring
- VLANs
- Layer 2 security support
- Captive portal - have to sign into a website before data can flow

The differences between the client authentication types

WEP - Wired Equivalent Privacy

- old encryption method, has been cracked for a while. Don't use

WPA Personal

- WPA2 Personal - implements pre-shared key - still weak and susceptible to dictionary attacks

- WPA3 Personal - enhances security through replacing the PSK with simultaneous authentication of equals (SAE)
  - aka a new key is generated with each authentication
  - 128 bit encryption plus forward secrecy (PFS) - prevents compromising session keys

WPA Enterprise

- WPA2 Enterprise - implements RADIUS - based on 802.1x
- WPA3 Enterprise - requires a server certificate validation for confirming the identity of the server to which the device is connecting

How the setup works with RADIUS and Certs

Wi-Fi was setup to use RADIUS authentication for CORP.
To get the internal connection to work we needed to export a certificate from the RADIUS server and install it on each of the clients.

- this is because we configured a secure authentication method with EAP (which requires a valid certificate)

The different types of wireless attacks (review slides)

Rogue Wireless Devices

- potential open and unsecured portal into network infrastructure
- usually installed by employee who didn't realize what they did
- ad hoc wireless can also provide access

Peer-to-Peer attacks

- 802.11 client stations can be configured as infrastructure mode or ad hoc mode (peer to peer)
- people hacking users that are associated to the same access point

Eavesdropping

- casual or malicious
- casual - finding open WLAN networks and discovering layer 2 information about the WLAN
  - this can be through passive scanning - where the client radio listens for AP beacons
  - or through active scanning - where the client radio transmits probe requests
- malicious eavesdropping is using protocol analyzers to capture wireless communications, this is usually considered illegal

- if there is no encryption, plain text communications can be captured
- layer 3-7 can be captured if WPA2 (or better) is not in place
- unencrypted 802.11 frames can be reassembled at the upper layers (VoIP can be turned into a WAV file for example)

Wireless Hijacking (evil twin attack)

- hacker makes a device that pretends to be an AP in a WLAN
- AP uses the same SSID and users connect to it

Social Engineering Attacks

- talking to people and either getting their password from the things they say or from phishing or something

the purpose of performing wireless site surveys and in what instances these might be needed

- help understand how a wireless infrastructure is setup
- analysis can show weak spots in a network
  - this could be no coverage in an area
  - or even too much coverage causing a sever overlap and degraded quality

Review the labs and understand the Internal vs Guest setup for wireless access (no need to memorize configurations)

- AP is setup using VLAN 23 (DHCP)
- created a CORP-WLAN and a GUEST-WLAN
- CORP-WLAN was allowed access to the internal network as well as internet
  - this was setup through RADIUS / AD groups
- GUEST-WLAN was only allowed access to internet (NOT INTERNAL NETWORK)
  - Guest users had to be created (could have been automatically created)
  - and needed to sign into a captive portal - browser tab that opens and has to be accepted before traffic could be routed to internet.