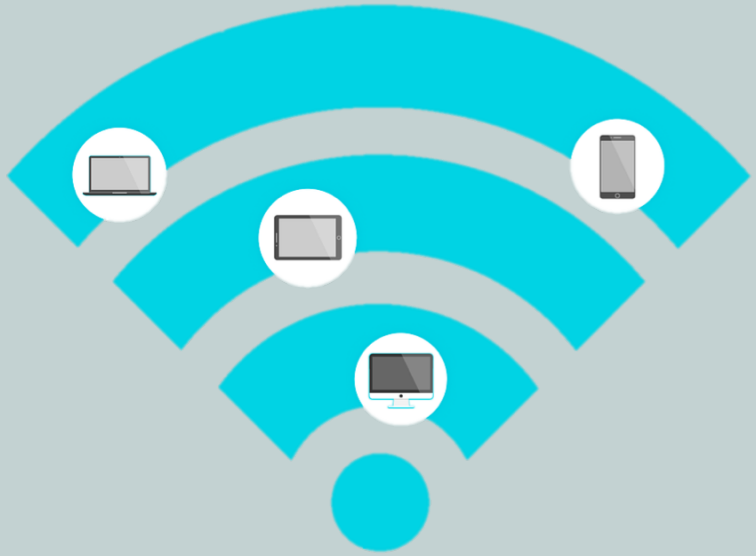
Wireless Networking (WLAN)

CompTIA Network+ (N10-007)

Wireless Networks (WLANs)

- Allows users to roam within a coverage area
- Popularity has increased exponentially
- Convenient to use and expand network access throughout a room, floor, or building



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wireless Networks (WLANs)

- IEEE 802.11 is the most common type

- Other wireless options exist (used for PAN)
  - Bluetooth
  - Infrared (IR)
  - Near-Field Communications (NFC)
  - Ant+
  - Z-Wave

Ad Hoc

- Wireless devices communicate directly with each other without the need for a centralized access point

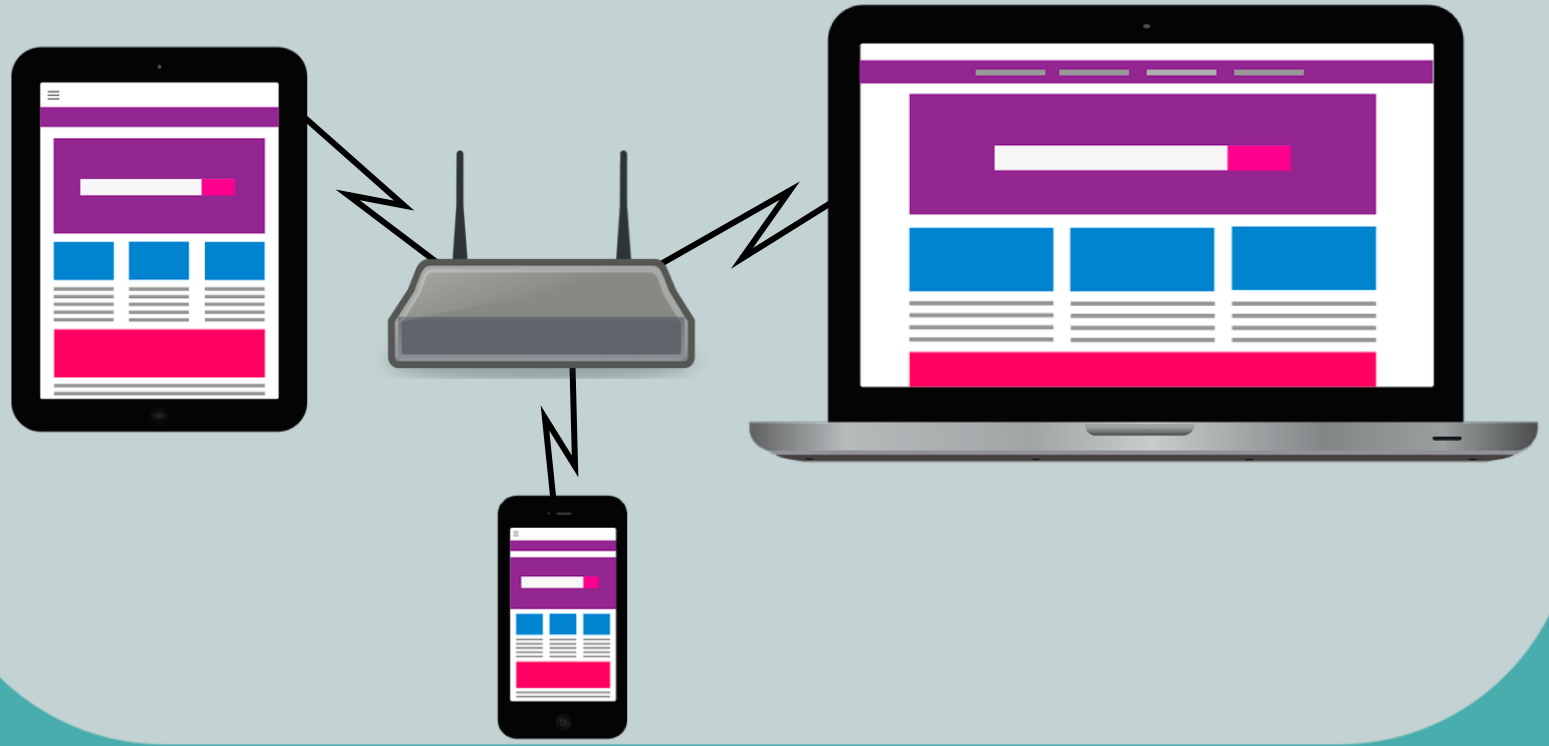
- Peer-to-Peer connections

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

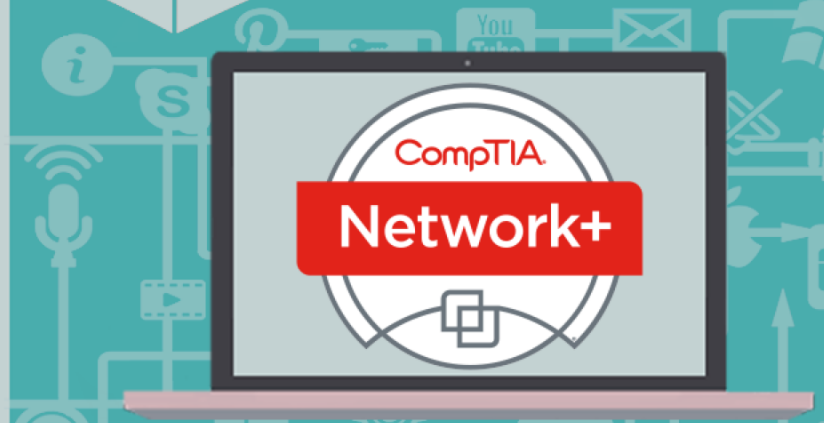
Infrastructure

- Wireless devices communicate with other wireless or wired devices through a wireless router or access point

- Traditional WiFi in Home and Office networks



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



Wireless Access Point (AP or WAP)

- Expands wired LAN into the wireless domain
  - Does not interconnect two networks (not a router)
  - Functions as a hub
- Connects wired LAN and wireless devices into the same subnet
- All clients on an access point are on a single collision domain

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wireless Router

- Gateway device and base station for wireless devices to communicate with each other and connect to the Internet

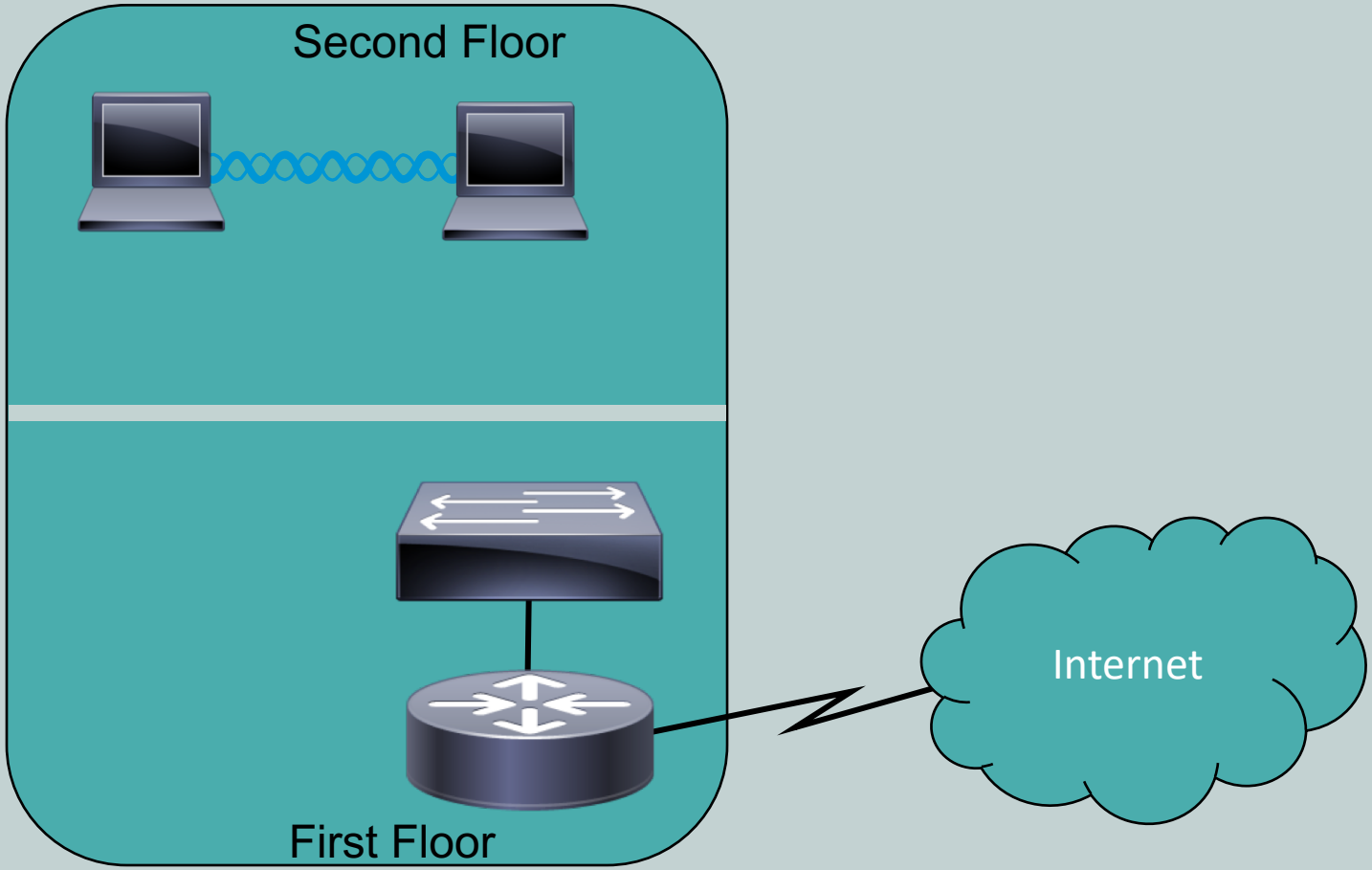
- Often combines many features into one device:
  - Wireless Access Point (WAP or AP)
  - Router
  - Switch
  - Firewall
  - Fiber, Cable, or DSL modem

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

WLAN Service Sets

CompTIA Network+ (N10-007)

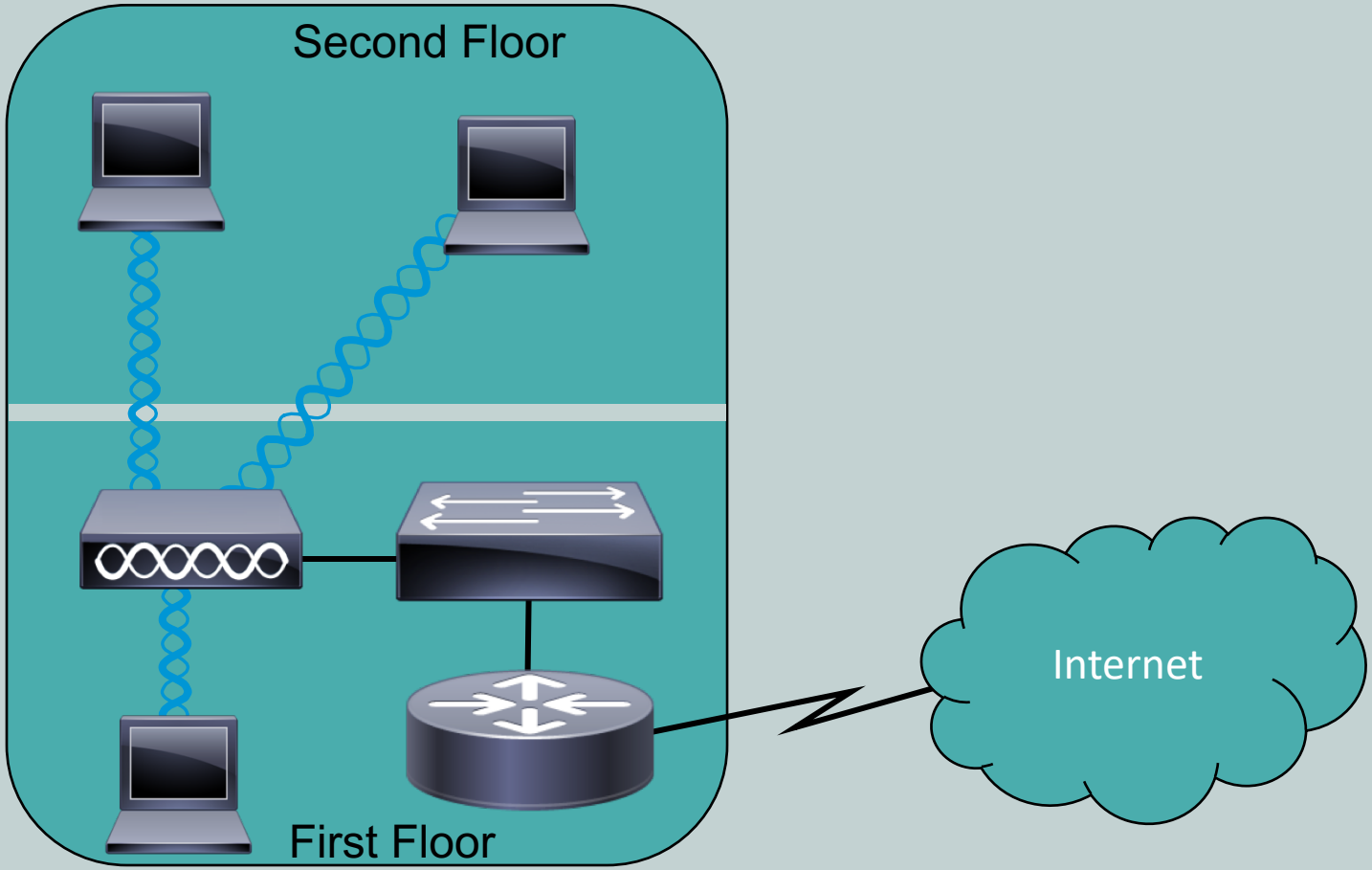
Independent Basic Service Set (IBSS)



Contains only devices/clients with no APs
(AD-HOC WLAN)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

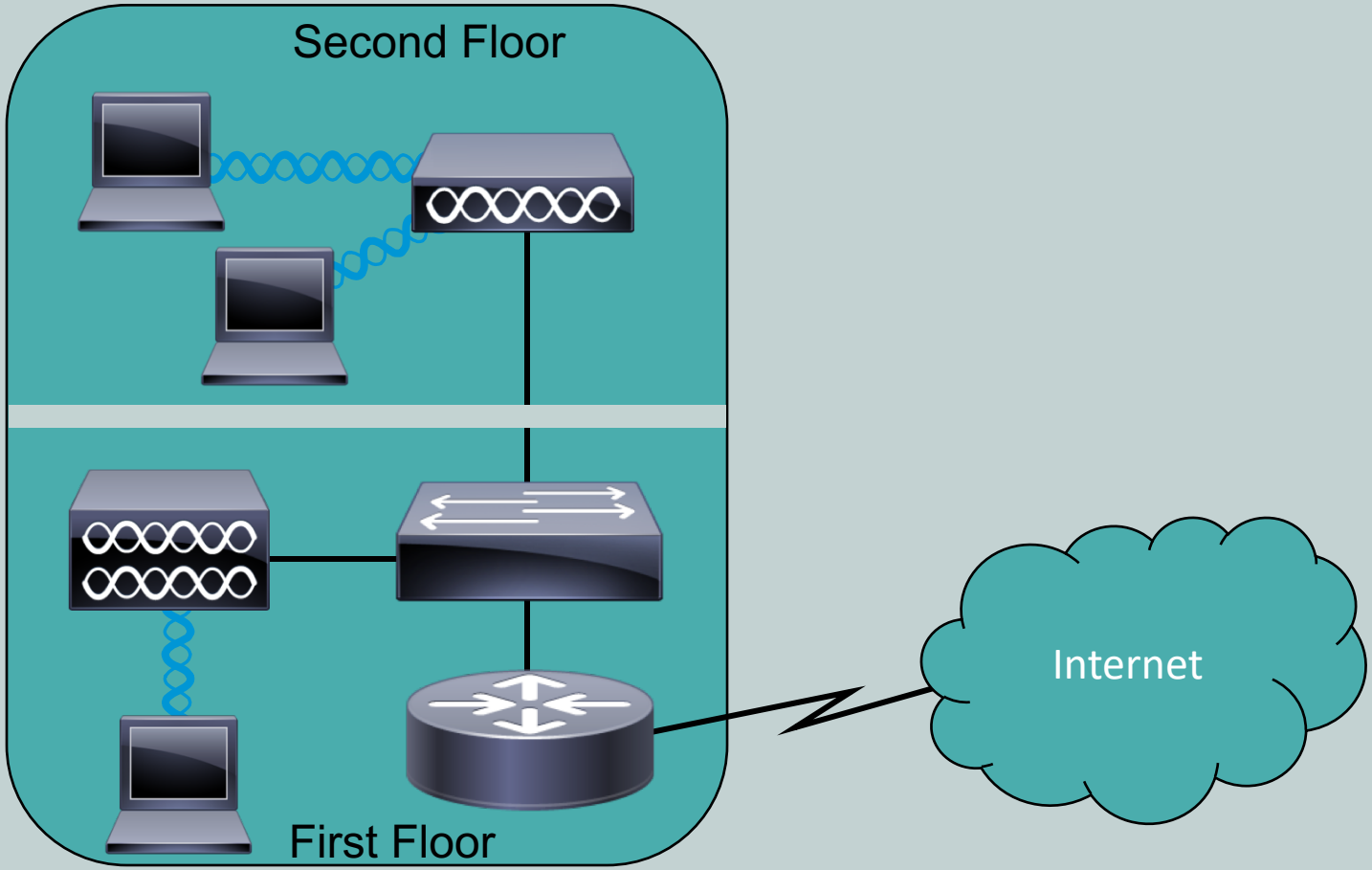
Basic Service Set (BSS)



Only one AP connected to the network
(Example: SOHO network)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Extended Service Set (ESS)

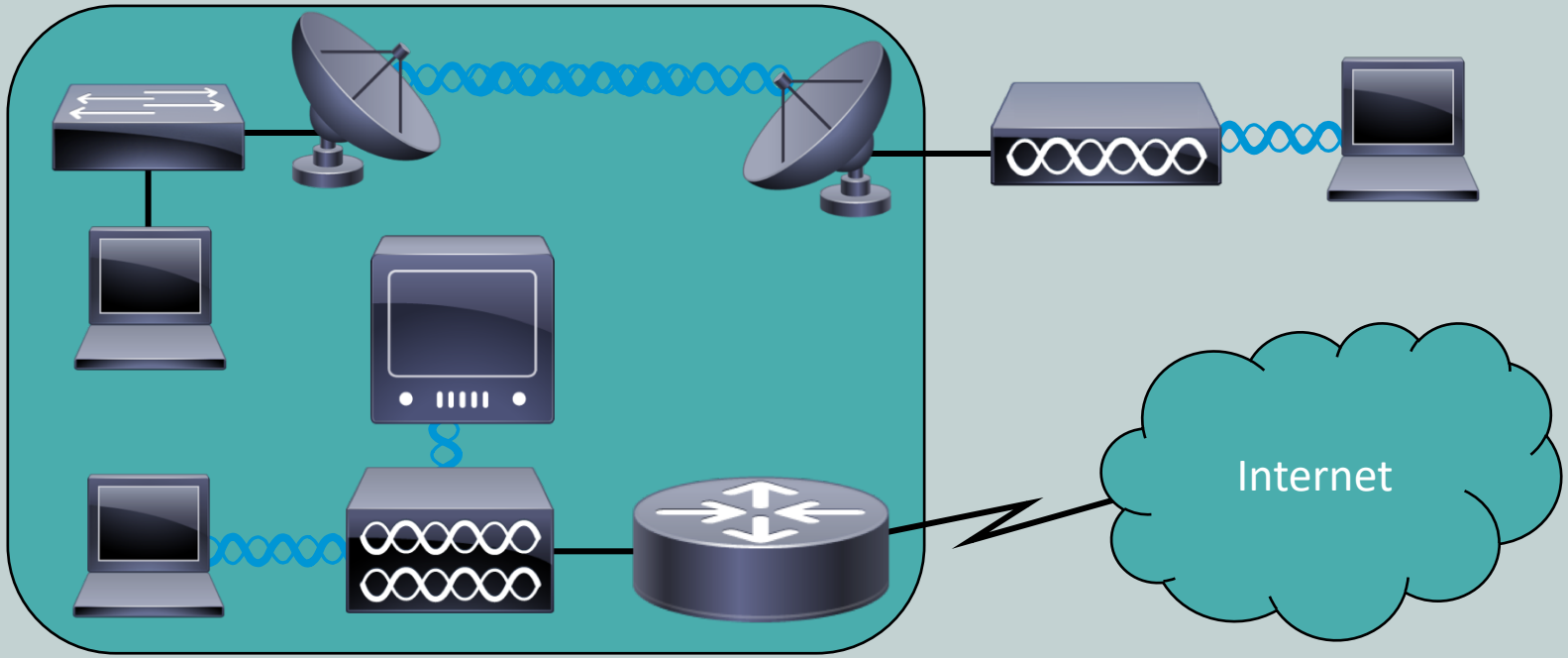


Contains multiple APs to provide coverage
(Example: College Campus)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Mesh Topology

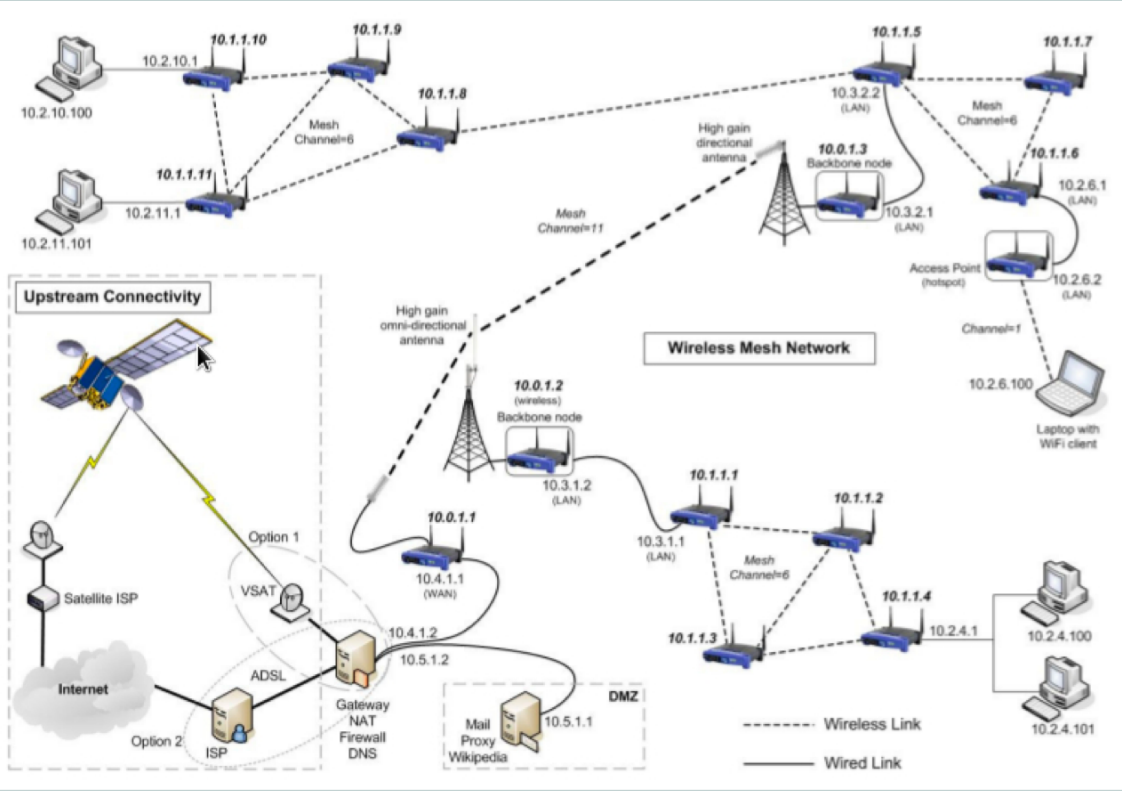
- May not use a centralized control
- Range of combined wireless defines network
- Uses WiFi, Microwave, Cellular, and more



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Mesh Topology

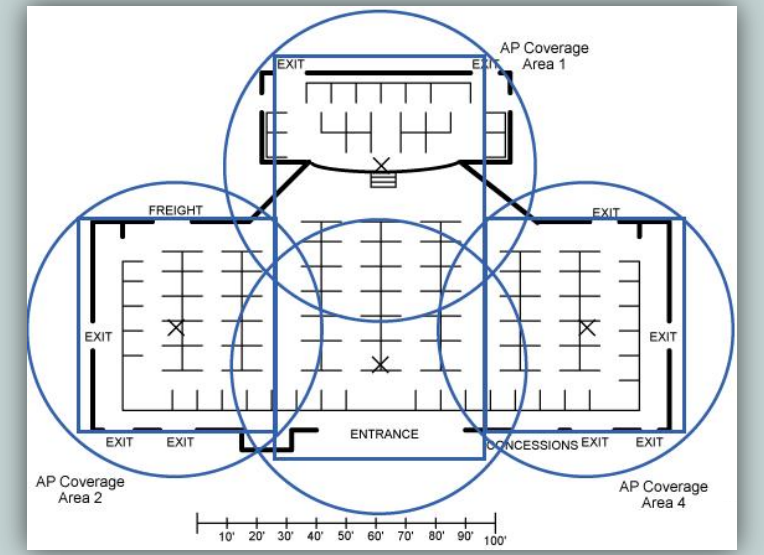
- May not use a centralized control
- Range of combined wireless defines network
- Combines WiFi, Microwave, Cellular, & more



AP Placement

- Careful planning is required to prevent the APs from interfering with one another and still maintaining the desired coverage area in ESS

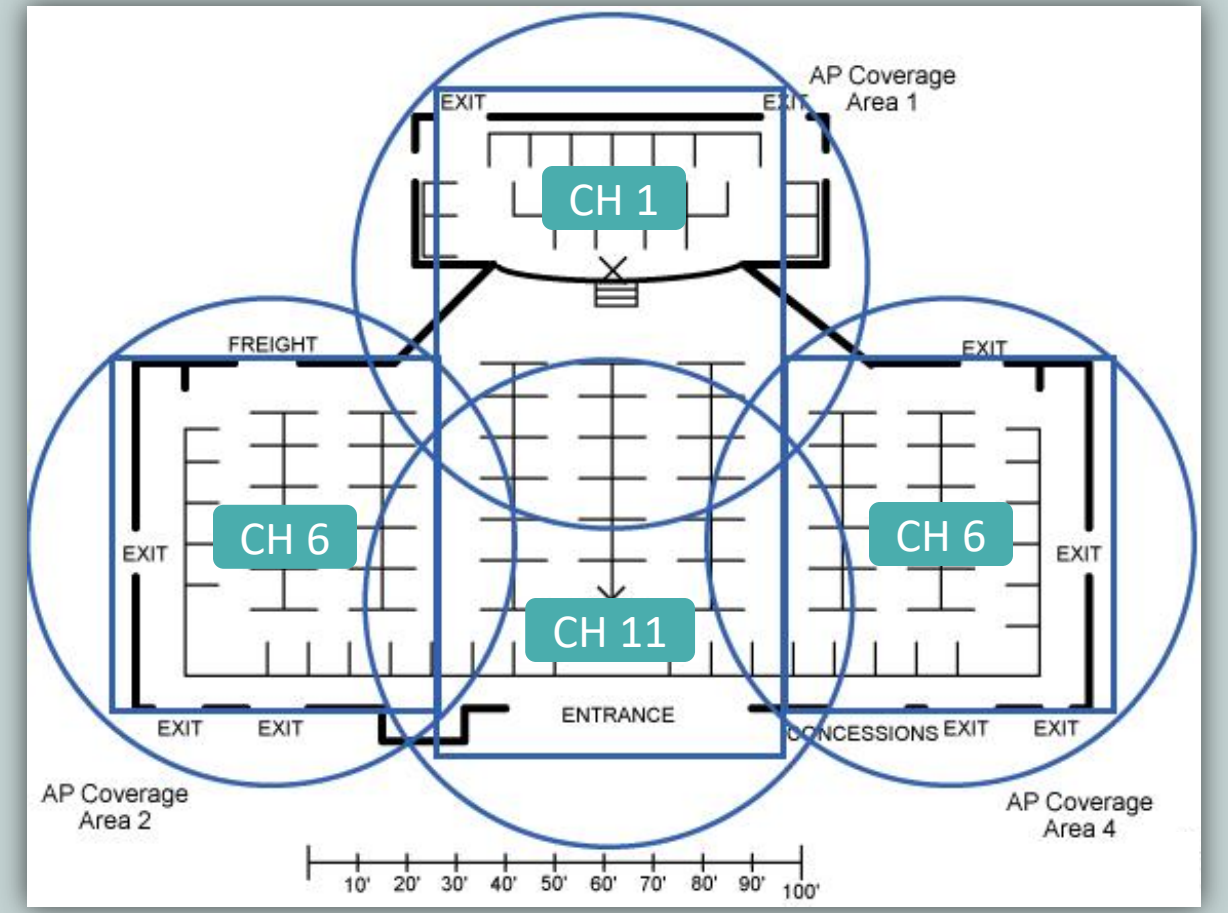
- Coverage should overlap between APs to allow uninterrupted roaming from one cell to another but can't use overlapping frequencies



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA Network+

AP Placement (2.4 Ghz)

- Non-overlapping coverage cells for 2.4 GHz band should have 10% to 15% coverage overlap in coverage area

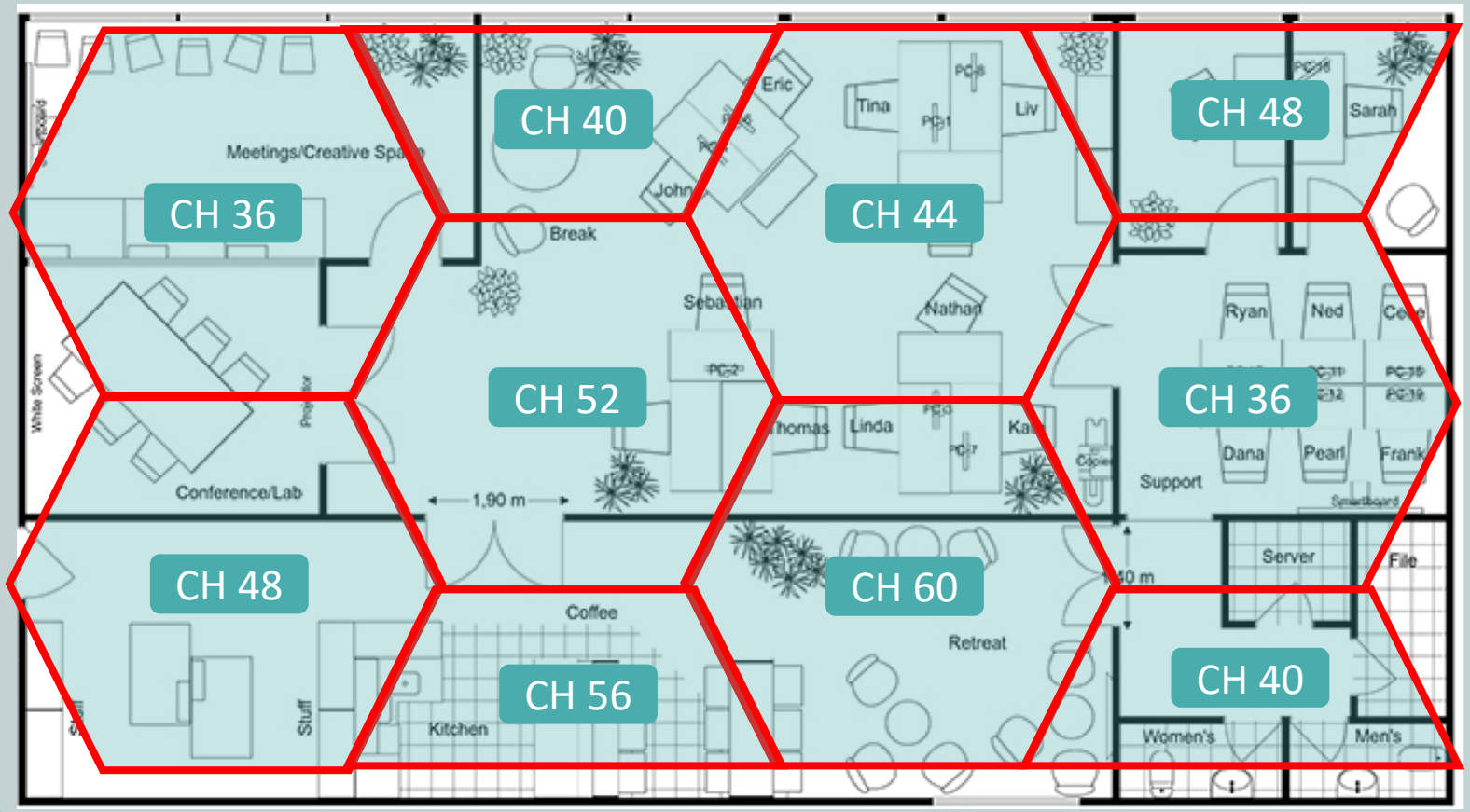


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

AP Placement (5 Ghz)

- Identical channels should be separated by at least two cells instead of one

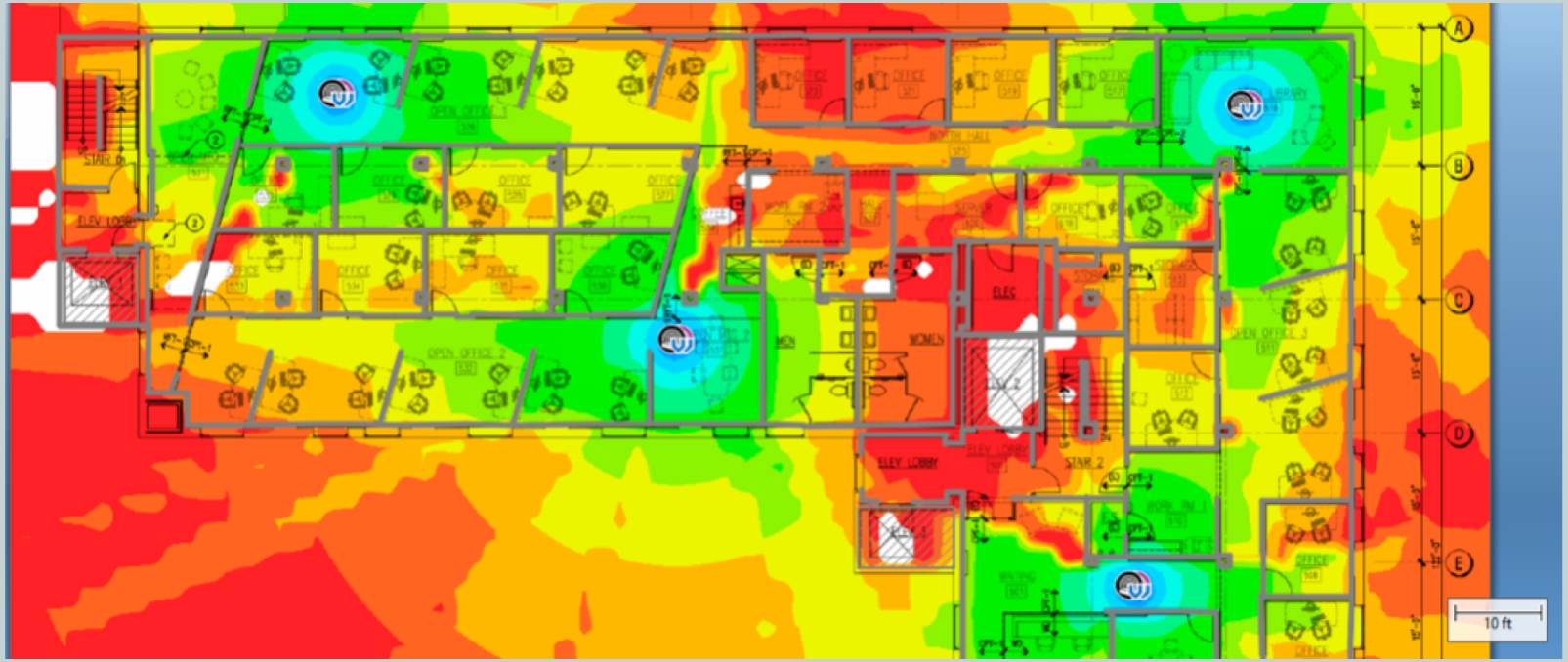


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Site Surveys

- Wireless survey to determine coverage areas
- Produces a *heat map* with coverage



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wireless Range Extenders

- Specialized device that overcomes distance limitations of wireless networks
- Amplifies the signal and extends reachability or a wireless cell
- Wireless repeater receives signal on one antenna and repeats it on other

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wireless Antennas

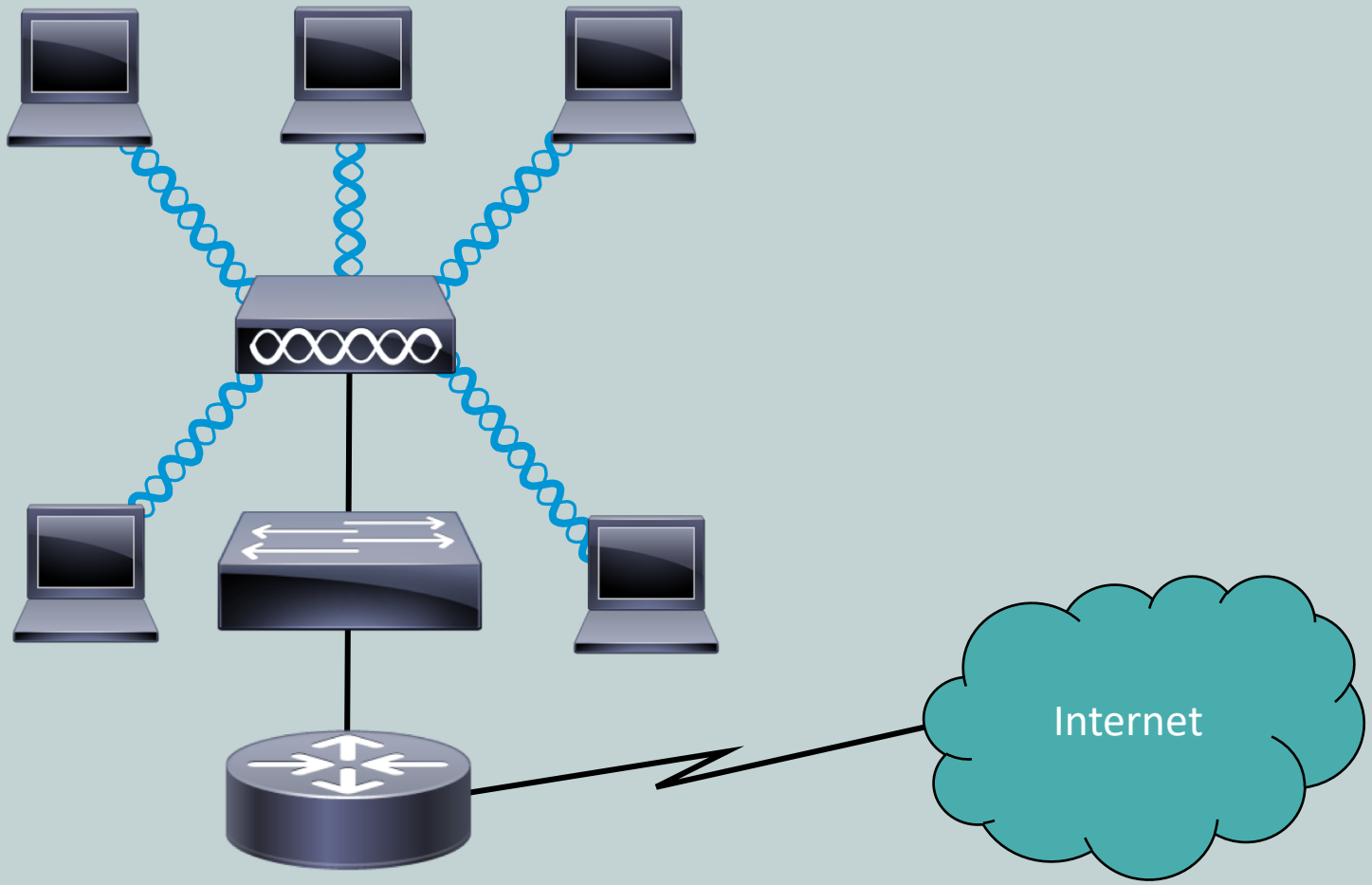
CompTIA Network+ (N10-007)

Antennas

- Coverage areas vary based on the type used
- Most SOHO wireless APs have fixed antennas
- Enterprise-class APs support different types
- Factors in antenna effectiveness
  - Distance
  - Pattern of Wireless Coverage
  - Environment (indoor/outdoor)
  - Avoiding Interference with other APs

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

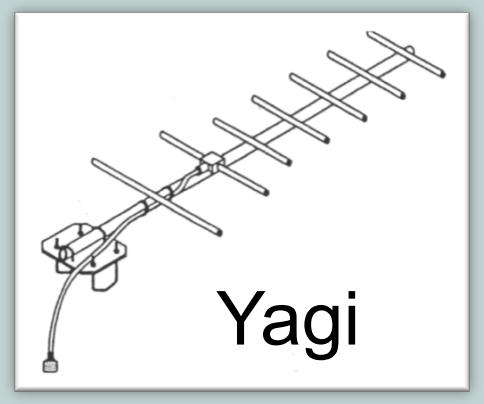
Omnidirectional Antenna

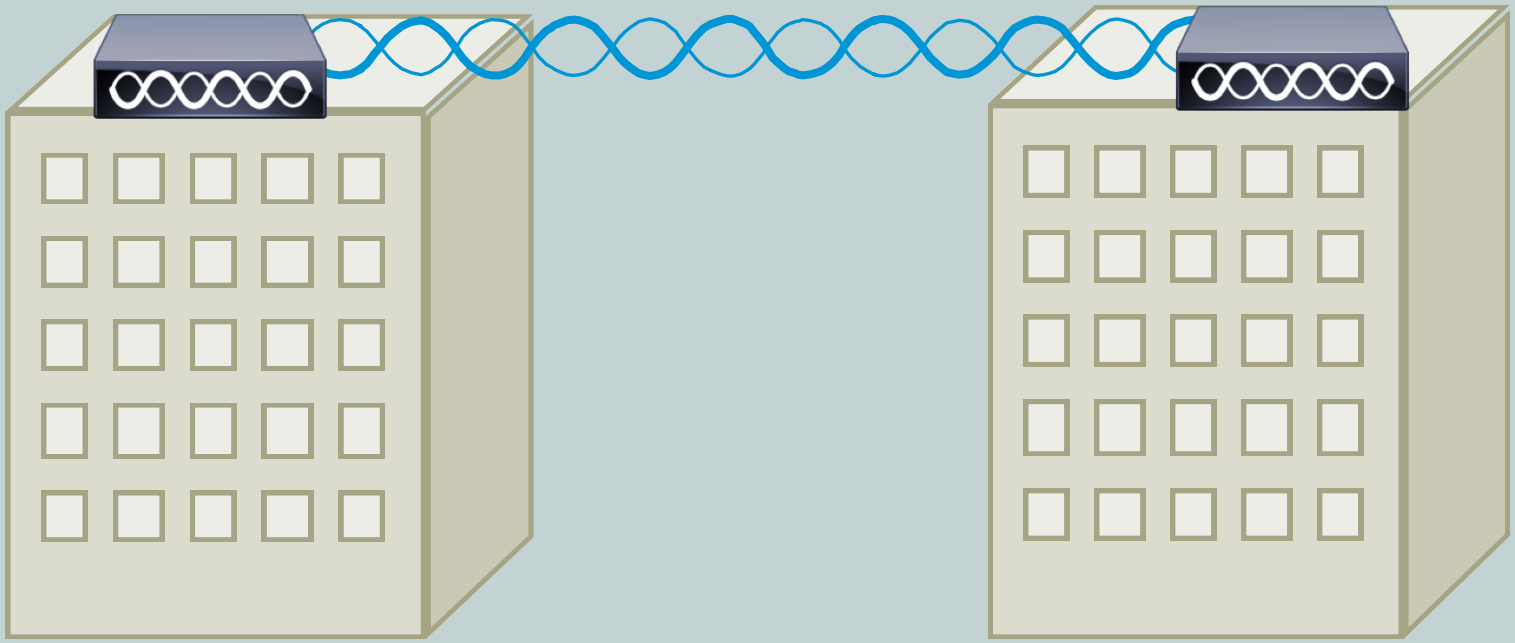


Radiates power equally in all directions

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Unidirectional Antenna





Focuses power in one direction
for covering greater distances

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

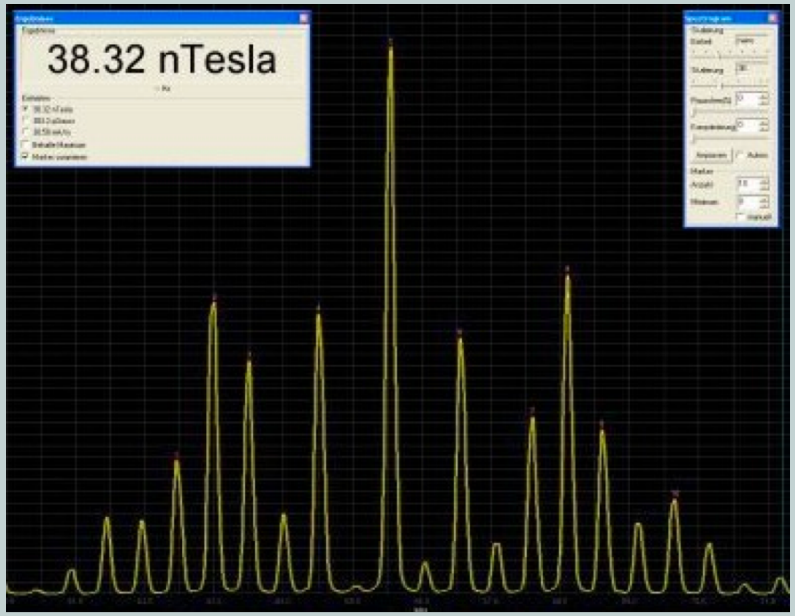
Wireless Frequencies

CompTIA Network+ (N10-007)

Spread Spectrum Wireless Transmissions

- Direct-Sequence Spread Spectrum (DSSS)
- Frequency-Hopping Spread Spectrum (FHSS)
- Orthogonal Frequency-Division Multiplexing (OFDM)

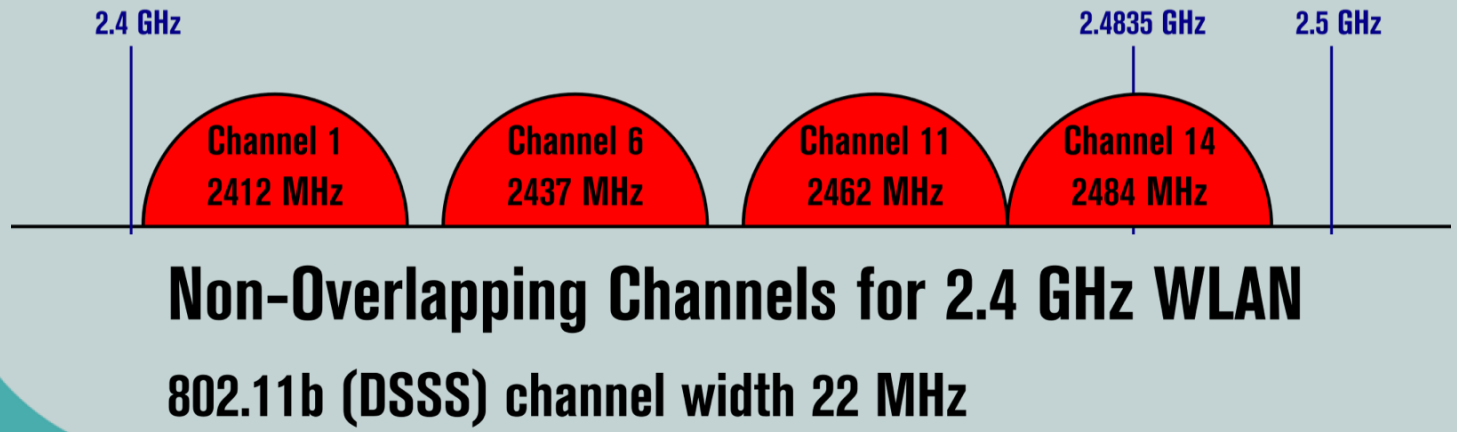
Only DSS and OFDM are commonly utilized in today's WLANs



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Direct-Sequence Spread Spectrum (DSSS)

- Modulates data over an entire range of frequencies using a series of signals known as *chips*
- More susceptible to environmental interference
- Uses entire frequency spectrum to transmit



Non-Overlapping Channels for 2.4 GHz WLAN

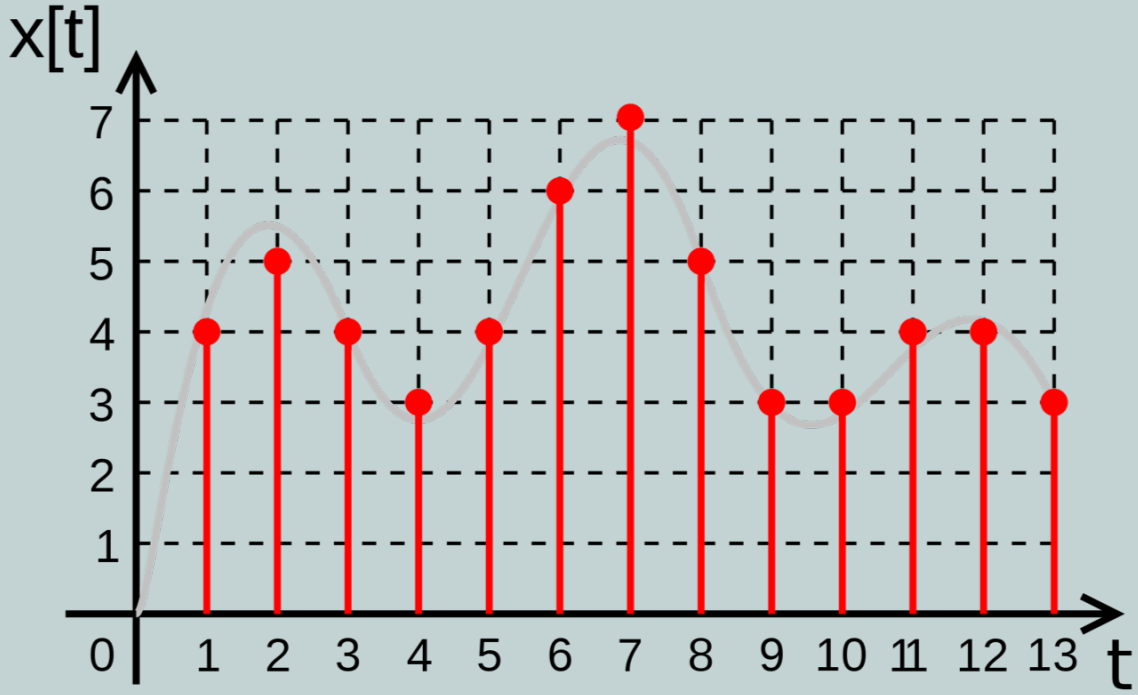
802.11b (DSSS) channel width 22 MHz

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Frequency-Hopping Spread Spectrum (FHSS)

- Devices hop between predetermined frequencies

- Increases security as hops occur based on a common timer

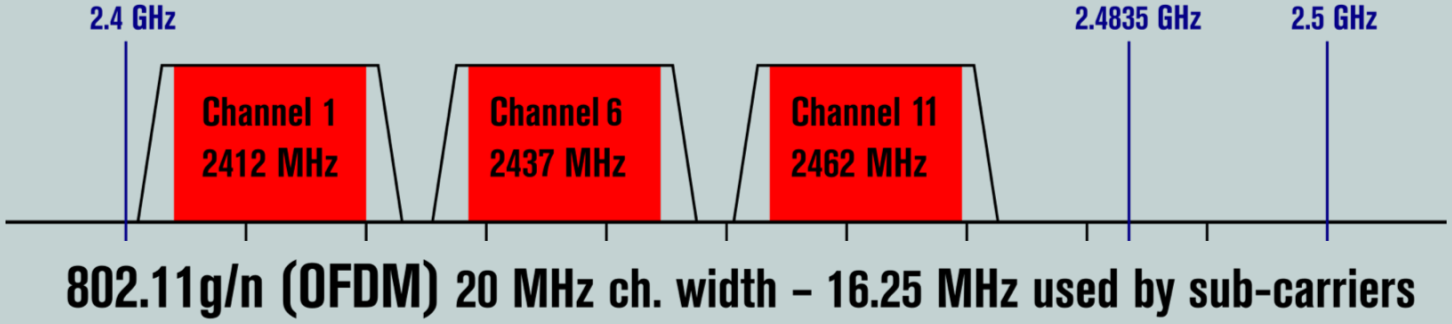


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

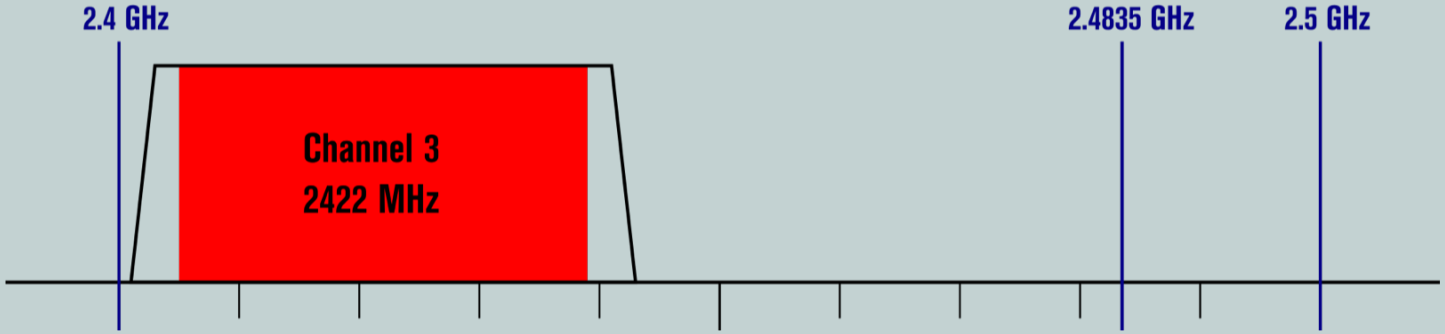
Orthogonal Frequency Division Multiplexing (OFDM)

- Uses slow modulation rate with simultaneous transmission of data over 52 data streams

- Allows for higher data rates while resisting interference between data streams



802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Frequencies and Channels

- IEEE 802.11 standards are differentiated by their characteristics, such as frequency range used:
  - 2.4 GHz band
    - *2.4 GHz to 2.5 GHz range*
  - 5 GHz band
    - *5.75 GHz to 5.875 GHz range*

- Each band has specific frequencies (or channels) to avoid overlapping other signals

- Channels 1, 6, and 11 will avoid overlapping frequencies in 2.4 GHz band

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

802.11 Wireless Standards

Standard	Band (GHz)	Maximum Bandwidth	Transmission Method	Maximum Range
802.11	2.4	1 Mbps or 2 Mbps	DSSS or FHSS	20m indoors 100m outdoors
802.11a	5	54 Mbps	OFDM	35m indoors 120m outdoors
802.11b	2.4	11 Mbps	DSSS	32m indoors 140m outdoors
802.11g	2.4	54 Mbps	OFDM or DSSS	32m indoors 140m outdoors
802.11n	2.4, 5, Both	> 300 Mbps (channel bonding)	OFDM	70m indoors 250m outdoors
802.11ac	5	> 3 Gps (with MU-MIMO)	OFDM	70m indoors 250m outdoors

Radio Frequency Interference (RFI)

- Caused by using similar frequencies to WLAN

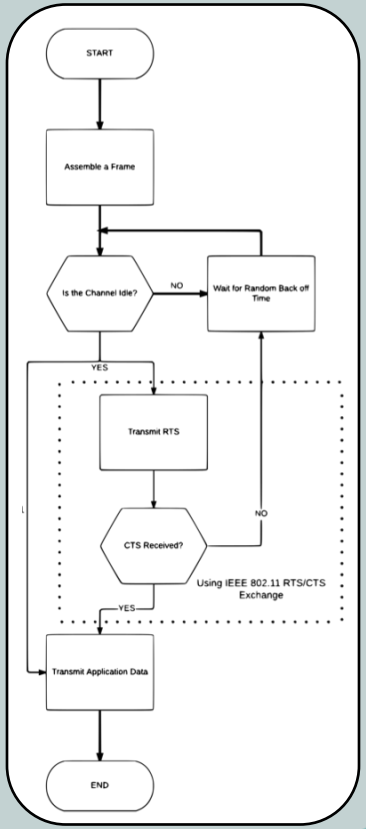
- Common sources of interference:
  - Other wifi devices (overlapping channels)
  - Cordless phones and baby monitors (2.4 GHz)
  - Microwave ovens (2.4 Ghz)
  - Wireless security systems (2.4 GHz)
  - Physical obstacles (Walls, appliances, cabinets)
  - Signal strength (Configurable on some devices)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA Network+

Carrier Sense Multiple Access/Collision Avoidance

- WLAN uses CSMA/CA to control access to medium, where wires Ethernet uses CSMA/CD

- Listens for transmission to determine if safe to transmit
  - If channel is clear, transmits Request to Send (RTS)
  - Device waits for acknowledgment
  - If received a RTS, responds with Clear to Send (CTS)
  - If not received, device starts random back off timer



Wireless Security

CompTIA Network+ (N10-007)

Wireless Security

- Wireless networks offer convenience, but also many security risks

- Encryption of data transferred is paramount to increasing security

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Pre-Shared Key

- Both AP and client uses same encryption key

- Problems:
  - Scalability is difficult if key is compromised
  - All clients must know the same password

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wired Equivalent Privacy

- Original 802.11 wireless security standard
  - Claimed to be as secure as wired networks
- Static 40-bit pre-shared encryption key
  - Upgraded to 64-bit and 128-bit key over time
- Uses 24-bit Initialization Vector (IV)
  - Sent in clear text
- Brute Force Attack within minutes using AirCrack-ng and other tools

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Wi-Fi Protected Access (WPA)

- Replaced WEP and its weaknesses
- Temporal Key Integrity Protocol (TKIP)
  - 48-bit Initialization Vector (IV) instead of 24-bit IV
  - Rivest Cipher 4 (RC4) used for encryption
- Uses Message Integrity Check (MIC)
  - Confirms data was not modified in transit
- Enterprise Mode WPA
  - Users can be required to authenticate before exchanging keys
  - Keys between client and AP are temporary

Wi-Fi Protected Access 2 (WPA2)

- Created as part of IEEE 802.11i standard
  - Requires stronger encryption and integrity checks
  - Integrity checking through CCMP
    - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- Uses Advanced Encryption Standard (AES)
  - 128-bit key or above
- Supports two modes
  - Personal mode with pre-shared keys
  - Enterprise mode with centralized authentication

WiFi Exam Tips

If you are asked about…	Look for the answer with…
Open	No security or protection
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

WEP and WPA/WPA2 Security Cracking

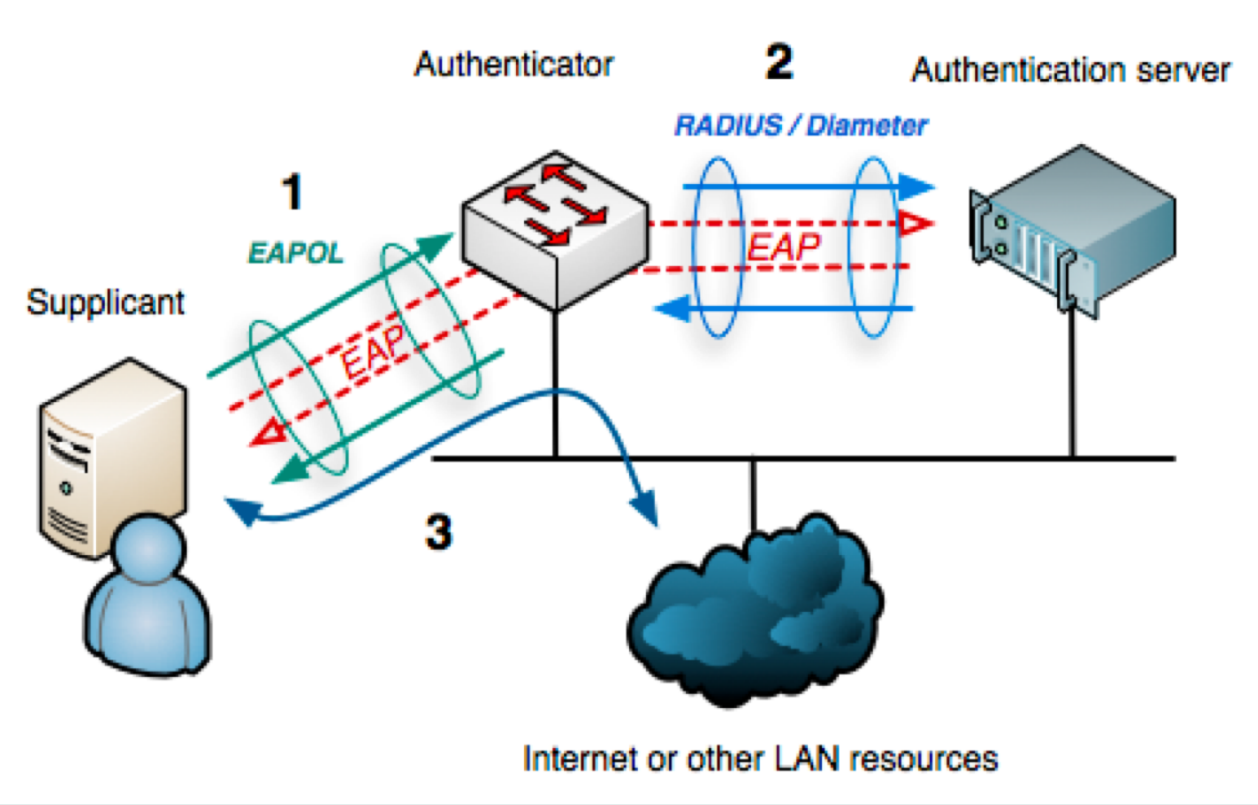
- Utilities can capture wireless packets and run mathematical algorithms to determine the pre-shared key

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA Network+

Network Authentication 802.1x

- Each wireless user authenticates with their own credentials

- Used also in wired networks

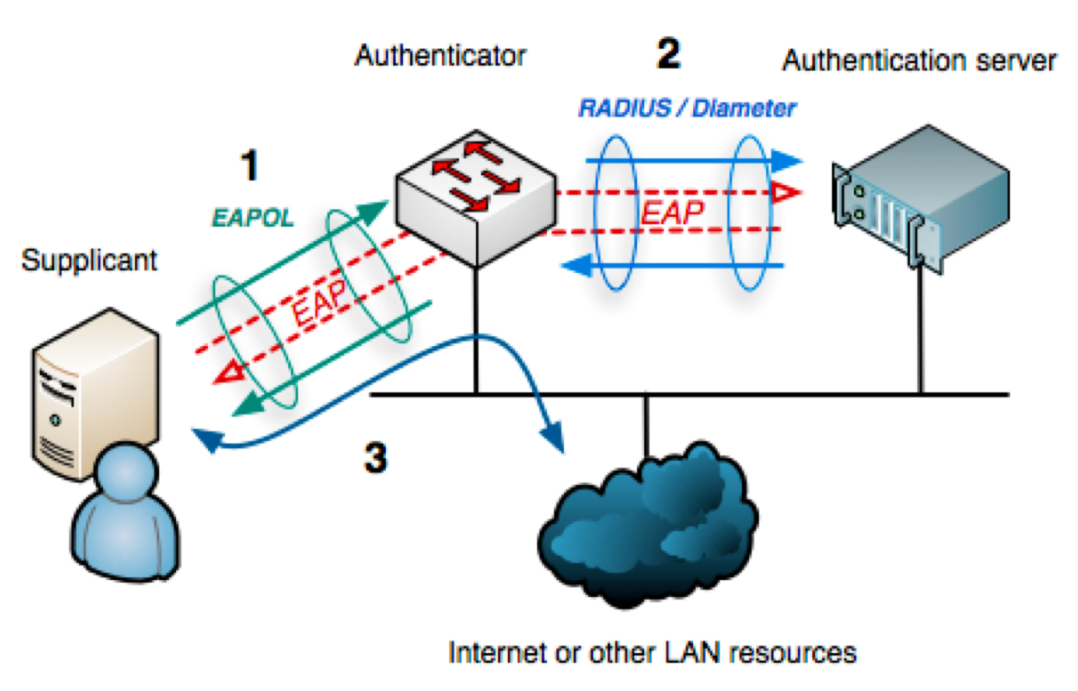


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Extensible Authentication Protocol (EAP)

- Authentication performed using 802.1x

- EAP-FAST
  - Flexible Authentication via Secure Tunneling
- EAP-MD5
- EAP-TLS



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

MAC Address Filtering

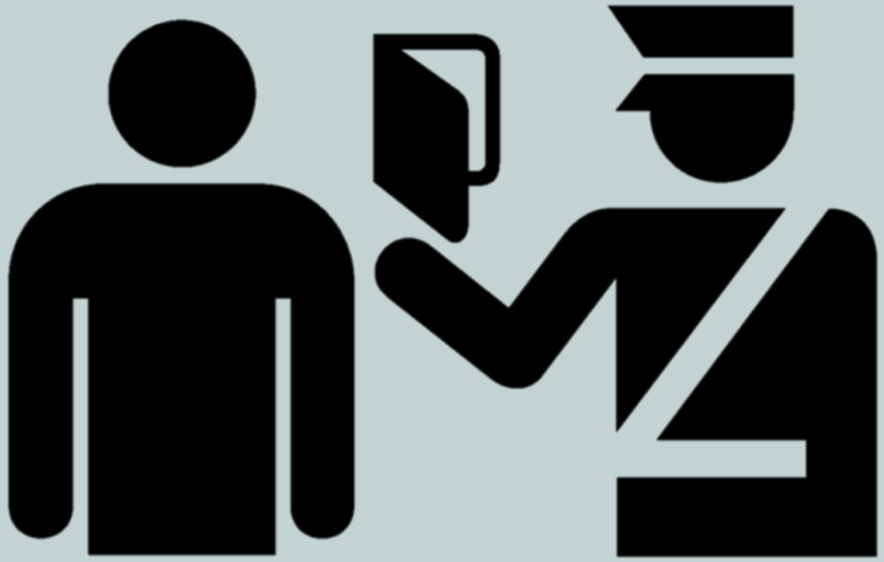
- Configures an AP with a listing of permitted MAC addresses (like an ACL)

- Problems:
  - Knowledgeable users can falsify their MAC easily using freely available tools
  - Examples:
    - MAC Address Changer (Windows)
    - MacDaddyX (OSX)
    - Macchanger (Linux)

Network Admission Control (NAC)

- Permits or denies access to the network based on characteristics of the device instead of checking user credentials

- Conducts a posture assessment of client
  - Checks the OS and antivirus version of client



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Captive Portals

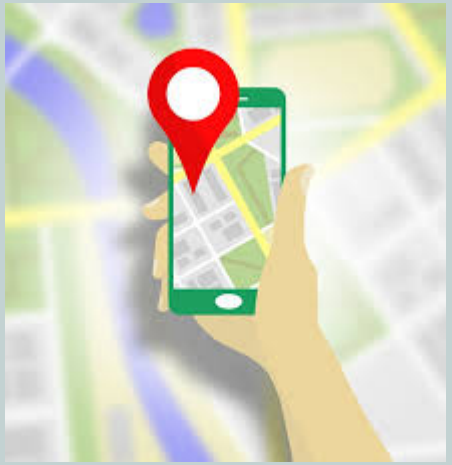
- Web page that appears before the user is able to access the network resources

- Webpage accepts the credentials of the user and presents them to the authentication server

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Geofencing

- GPS or RFID defines real-world boundaries
- Barriers can be active or passive
- Device can send alerts if it leaves area
- Network authentication can use it to determine access

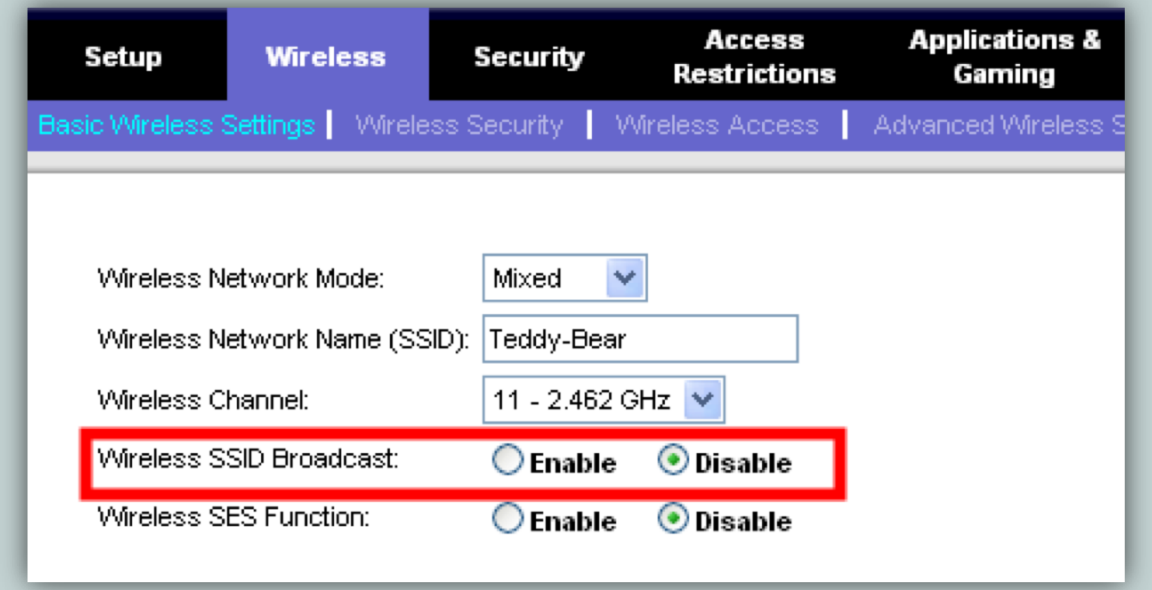


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Disable SSID Broadcast

- Configures an AP to not broadcast the name of the wireless LAN

- Problem:
  - Knowledgeable users can still easily find the SSID using wireless sniffing tools



Rogue Access Point

- Malicious users set up an AP to lure legitimate users to connect to the AP
- Malicious users can then capture all the packets (data) going through the rogue access point

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE
CompTIA
Network+

Unsecured Wireless Networks

- War Driving
  - Occurs when users perform reconnaissance looking for unsecured wireless networks
- War Chalking
  - Occurs when users write symbols on a wall to notify others of AP characteristics