Security+ SY0-601

Module 9: Wireless.

Table of Contents.

1. 802.11 wireless standards.
2. Wireless security settings.
3. Authentication protocols.
4. Authentication methods.
5. Network installation considerations.
6. Wireless vulnerabilities and attacks.

Learning objectives.

Upon completion of this module, you should be able to:

- List the five common wireless standards and their respective attributes. Explain which standards are current and which are in disuse.
- Describe the various security settings cryptographic algorithms that can be set on a WAP.
- List the protocols and tools for authentication and encryption in the wireless environment.
- Describes the authentication modes that can be configured in a wireless network.
- Compare and contrast infrastructure and Ad-hoc/Wi-Fi direct topologies. Describe the components of the various structures and types of SSIDs.
- List and describe common wireless attacks.

802.11 wireless standards.

802.11 WIRELESS STANDARDS.

Key concepts.

In this section, we will cover the following key concepts:

- 802.11 throughput.
- 802.11 standards.
- WiFi2 802.11a 5.0 GHz.
- WiFi1 802.11b 2.4 GHz.
- WiFi3 802.11g 2.4 GHz.
- WiFi4 802.11n 2.4 and 5 GHz.
- WiFi5 802.11ac 5 GHz (2.4 GHz).
- WiFi6 802.11ax 2.4, 5 GHz, and 6GHz.

802.11 WIRELESS STANDARDS.

802.11 throughput.

Wireless Standards Throughput.

802.11a	54 Mbps (5.0Ghz)
802.11b	11 Mbps (2.4Ghz)
802.11g	54 Mbps (2.4Ghz)
802.11n	288/600 Mbps (2.4Ghz, 5.0Ghz) (MIMO)
802.11ac	450 Mbps (2.4Ghz) 1300 Mbps (5.0Ghz) (MU-MIMO)
802.11ax	10 Gbps. (2.4Ghz, 5.0Ghz, 6Ghz) (MU-MIMO)

802.11 WIRELESS STANDARDS.

802.11 standards.

- The 802.11 standards specify the characteristics of wireless LAN Ethernet networks.

- IEEE 802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum of around 5 GHz; this higher frequency shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions. This standard is also known as Wi-Fi 2.

802.11 WIRELESS STANDARDS.

IEEE 802.11b.

IEEE 802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standards. Vendors often prefer using these frequencies to lower their production costs.

- Because 802.11b is unregulated, gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. 802.11b supports a theoretical speed of up to 11 Mbps.

- IEEE 802.11b was released as a standard in 1999; IEEE 802.11b used the same 2.4 GHz frequency as the original 802.11 standard — DSSS. It supported a maximum theoretical rate of 11 Mbps and ranged up to 150 feet.

802.11 WIRELESS STANDARDS.

IEEE 802.11g.

- IEEE 802.11g attempts to combine the best of 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps and uses the 2.4 GHz frequency for a greater range. 802.11g is backward compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

- This standard is also known as **Wi-Fi 3**.

802.11 WIRELESS STANDARDS.

IEEE 802.11n.

IEEE 802.11n was designed to improve 802.11g in the amount of bandwidth it supports by using several wireless signals and antennas, called MIMO (Multiple Input Multiple Output), instead of one.

MIMO (Multiple Input Multiple Output) used multiple transmitters/receivers that could operate simultaneously at one or both ends of the link to a single device; this provided a significant increase in data without needing a higher bandwidth or transmit power. 802.11n operated in *both* the 2.4 GHz and 5 GHz bands.

802.11 WIRELESS STANDARDS.

IEEE 802.11ac.

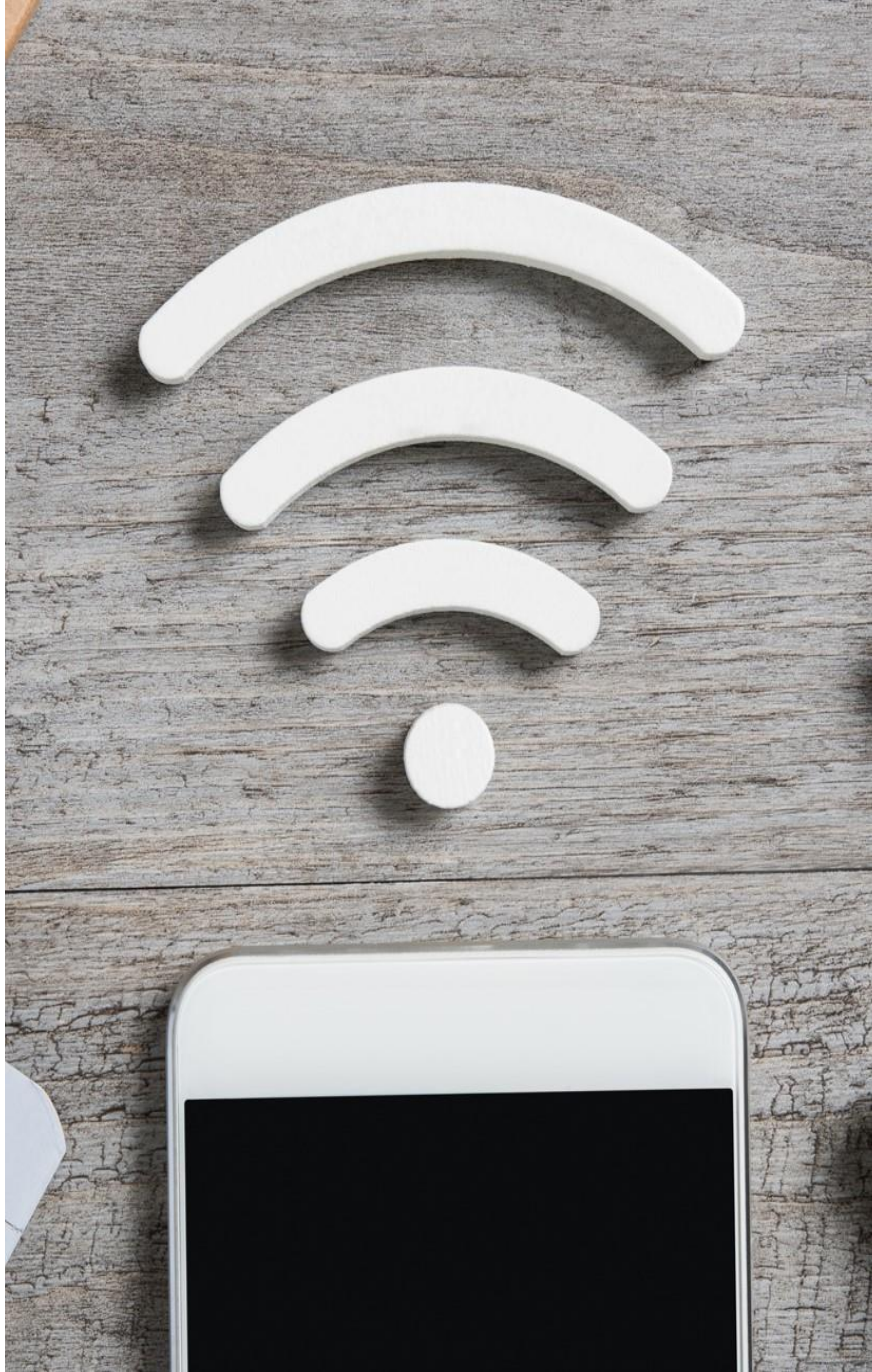
- IEEE 802.11ac is the generation of Wi-Fi that first signaled popular use. 802.11ac uses dual-band wireless technology, supporting simultaneous connections on 2.4 GHz and 5 GHz Wi-Fi devices.
- Wi-Fi 5 Exclusively in the 5 GHz band.
- Supports up to eight spatial streams (compared with 802.11n’s four streams).
- MU-MIMO.

802.11 WIRELESS STANDARDS.

IEEE 802.11ax.

The IEEE 802.11ax standard went live in 2019 and will replace 802.11ac as the de facto wireless standard. Wi-Fi 6 maxes out at 10 Gbps, uses less power, is more reliable in congested environments, and supports better security.

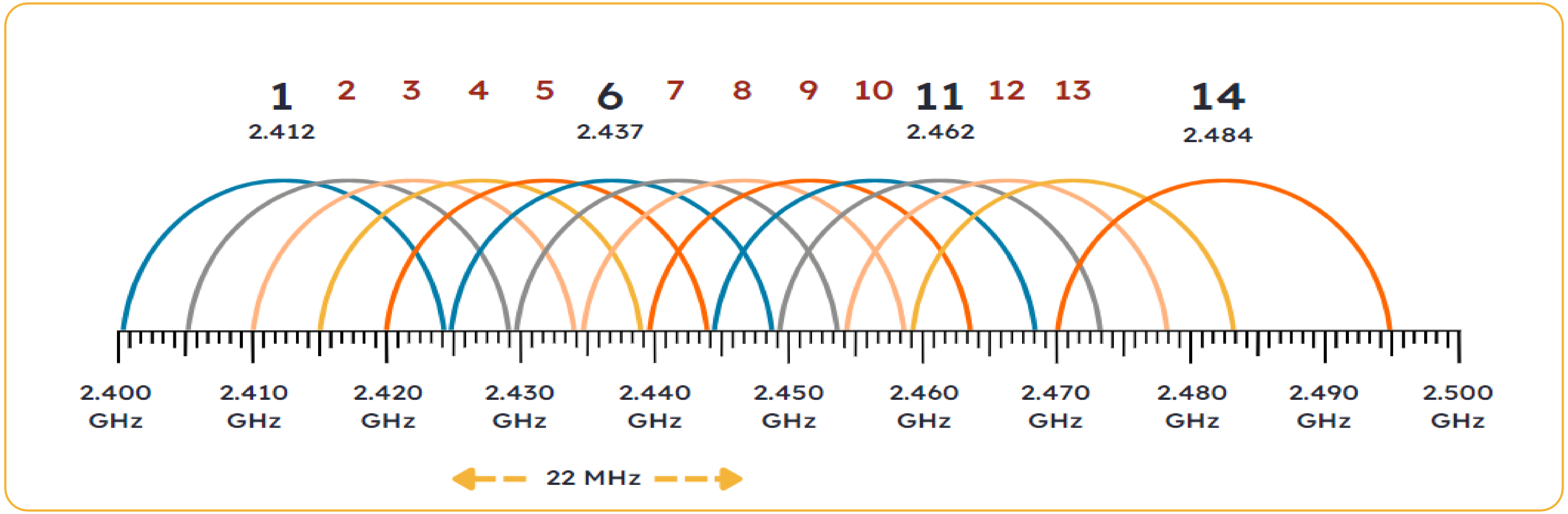
- Up to to 9.6 Gbps
- 2.4 GHz and 5 Ghz frequency
- MU-MIMO
- Wi-FI6 (also. Used 6GHz)
- APs and Clients must support 802.11ax



802.11 WIRELESS STANDARDS.

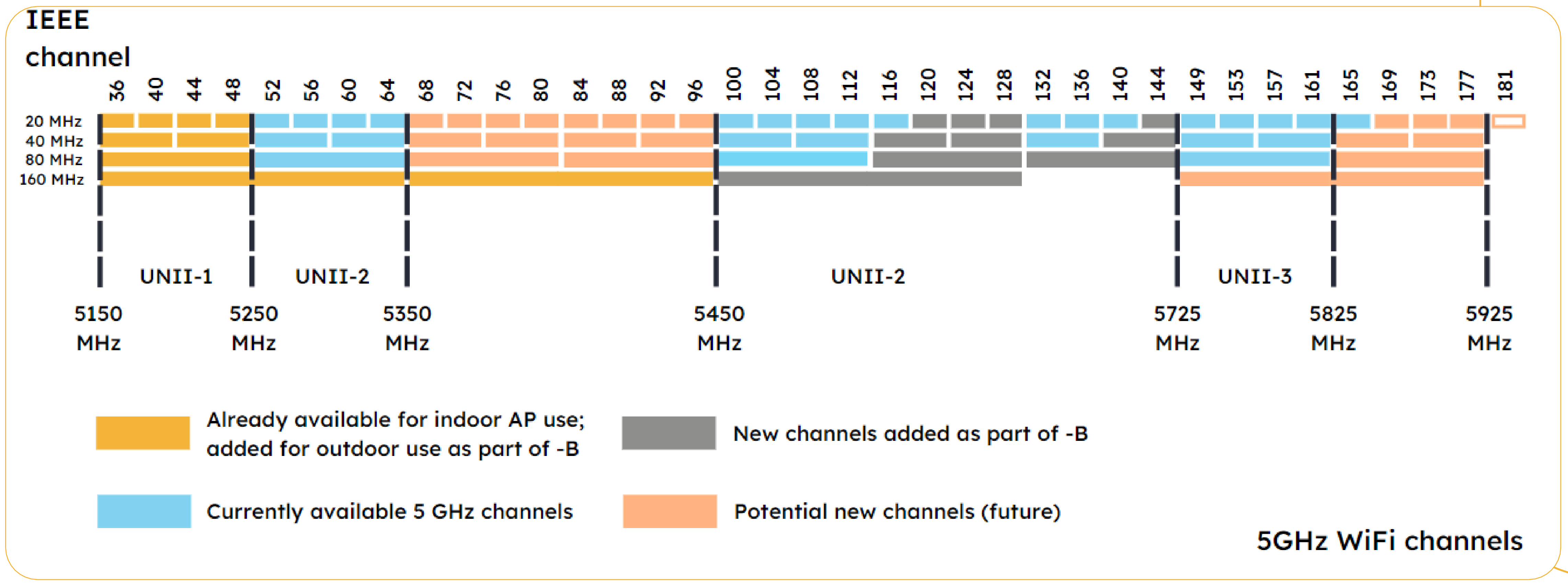
2.4 GHz.

2.4 GHz is one of the main frequency ranges used by Wi-Fi; the lower frequency provides further range but transmits data at slower speeds. This frequency is very congested as it contends with many IoT devices, including microwave transmissions, TV remotes, baby monitors, and co-channel interference.



802.11 WIRELESS STANDARDS.

5 GHz.



5GHz WiFi channels

5 GHz is one of two main frequency ranges used by Wi-Fi. It is the higher frequency that provides a shorter range but transmits data at higher speeds.

The 5 GHz allows for higher speeds and greater throughput; however, the shorter wavelength, as opposed to the 2.4.GHz means it is more difficult to get around obstructions such as walls. There are 23 non-overlapping channels to choose from.

802.11 WIRELESS STANDARDS.

Knowledge check.

Let’s apply what we have covered:

- Which wireless standards broadcast in the 2.4 GHz range by default?
- Which ones are considered 5.0 GHz by default?
- What is MIMO, and within which standard do we find it?

Wireless security settings.

WIRELESS SECURITY SETTINGS.

Key concepts.

In this section, we will cover the following key concepts:

- WEP.
- RC4 and IV.
- WPA.
- WPA2.
- AES.
- WPA3.
- SAE.
- CCMP and GCMP.

WIRELESS SECURITY SETTINGS.

Wired Equivalent Privacy (WEP).

- Wired Equivalent Privacy (WEP) is an old, obsolete, and insecure encryption method using RC4; it was first used in wireless with 802.11b. You will see WEP as an option on older or backward-compatible WAP — do not use this unless you have no other choice.
- WEP is considered a deprecated standard; the issue is with the initialization vector (IV). Encryption keys could be discovered using AIRCRACK and AIRSNORT.
- The IV is a randomly generated 24-bit value that is sent in the header of the packet; this reduces a 64-bit encryption key to 40-bits and a 128-bit encryption key to 104-bit encryption actual size.

WIRELESS SECURITY SETTINGS.

RC4.

Rivest Cipher 4 (RC4) is a stream cipher created in 1987. A stream cipher is a type of cipher that operates on data a byte at a time to encrypt it. RC4 was once one of the most used stream ciphers, having been used in Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols, the IEEE 802.11 wireless LAN standard, and the Wi-Fi Security Protocol WEP. It generates weak initialization vectors (IVs), which attackers can easily exploit.

WIRELESS SECURITY SETTINGS.

Initialization Vector (IV).

- An initialization vector (IV) is a binary value used to initialize a cryptographic algorithm.
- In cryptography, an initialization vector (IV) is a block of bits that is required to allow a stream cipher or a block cipher to be executed in any of several modes of operation in order to produce a unique stream independent from other streams produced by the same encryption key, without having to go through a (usually lengthy) re-keying process.

WIRELESS SECURITY SETTINGS.

Wi-Fi Protected Access.

In 2003, as WEP gradually performed its weakness, Wi-Fi Protected Access (WPA) was adopted by the Wi-Fi Alliance as an alternative for WEP as the draft IEEE 802.11i standard. Temporal Key Integrity Protocol (TKIP) was added to the RC4 encryption to increase security. The increase in encryption key size to 256-bit was introduced with WPA, with an actual size of 232-bits, subtracting the initialization vector size.

In addition to TKIP and an increase in encryption size, WPA also included a modified integrity-checking mechanism – CRC32-MIC. This is often referred to as the Michael Algorithm.

WPA operates in two modes: Personal and Enterprise. Personal uses a pre-shared key for authentication. Enterprise provides the security needed for wireless networks in business environments where a RADIUS server is deployed.

WIRELESS SECURITY SETTINGS.

WPA2.

Wi-Fi Protected Access II (WPA2) is the finalized 802.11i encryption standard used in many devices today; it replaced RC4/TKIP with AES-CCMP.

CCMP is used with AES, and CBC-MAC provides data integrity.

WPA2 uses the same authentication modes as WPA:

- Personal using a pre-shared key.
- Enterprise using IEEE 802.1X with EAP and a RADIUS server.

WPA2 uses an imperfect 4-way handshake to enable wireless connections, which is the source of the KRACK vulnerability and why WPA3 was implemented.

WIRELESS SECURITY SETTINGS.

Advanced Encryption Standard (AES).

Advanced Encryption Standard (AES) is the default encryption symmetric encryption algorithm.

- AES is a block cipher with three lengths of AES encryption keys: 128, 192, and 256-bit. Even though the key length of this encryption method varies, its block size — 128 bits (or 16 bytes) — stays fixed.
- AES-128 goes through 10 rounds of encryption, which means that the attack was not a threat in real life. In theory, cracking a 128-bit AES encryption key can take up to 36 quadrillion years.
- In addition, AES requires less memory than many other types of encryption (like DES).

WIRELESS SECURITY SETTINGS.

WPA3.

Wi-Fi Protected Access III (WPA3) is the newest encryption method used in newer wireless technologies. The Wi-Fi Alliance introduced WPA3 in June 2018; It replaced AES-CCMP with AES-GCMP (Galois/Counter Mode Protocol). WPA3 provides the most robust encryption security for wireless communication.

Data Integrity is accomplished with a 256-bit Broadcast/Multicast Integrity Protocol Cipher-Based Message Authentication Code (BIP-GMAC-256).

While the two authentication modes are still called Personal and Enterprise, the methods used in each have changed. WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations.

This capability is enabled through the simultaneous authentication of equals (SAE). The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction. Perfect forward secrecy (PFS) is achieved by replacing WPA2's 4-way handshake with the Dragonfly Handshake.

WIRELESS SECURITY SETTINGS.

Simultaneous Authentication of Equals of (SAE).

Simultaneous Authentication of Equals (SAE) is used with WPA3 and replaces the PSK 4-way handshake that is used in WPA2 and was found to have security issues. SAE utilizes Diffie-Hellman over elliptic curves key agreement and a hash value that is a combination of the password and the device's MAC address. This key exchange is referred to as the Dragonfly Handshake.

WIRELESS SECURITY SETTINGS.

CCMP and GCMP.

Counter Mode CBC-MAC Protocol (CCMP) is a Cipher Block Chaining Message Authentication Code Protocol used with symmetric block ciphers to strengthen the cipher. The CCM mode combines Counter Mode (CTR) for confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) for authentication and integrity. The enhanced privacy and security of CCMP compared with TKIP requires additional processing power, often necessitating new or upgraded hardware.

Galois Counter Message Authentication Code Protocol (GCMP) is used with WPA3 for better performance and is more efficient; it was first supported with 802.11ac.

WPA3-Enterprise uses 256-bit Galois/Counter Mode Protocol (GCMP-256) to provide authenticated encryption.

CONTINUED ON NEXT SLIDE >

WIRELESS SECURITY SETTINGS.

CCMP and GCMP.

GCMP can take full advantage of parallel processing and efficiently use an instruction pipeline or a hardware pipeline. By contrast, the cipher block chaining (CBC) mode of operation incurs pipeline stalls that hamper its efficiency and performance. This efficiency improvement is best seen when both authentication and encryption need to be performed on a message by overlapping the execution of those operations.

WIRELESS SECURITY SETTINGS.

Knowledge check.

Let’s apply what we have covered:

- Describe the difference between the personal modes of WPA2 and WPA3.
- Describe how the initialization vector affects the key size of WEP and WPA.

Authentication protocols.

AUTHENTICATION PROTOCOLS.

Key concepts.

In this section, we will cover the following key concepts:

- WPS.
- EAP.
- EAP-TLS.
- EAP-TTLS.
- PEAP.
- EAP-FAST.

AUTHENTICATION PROTOCOLS.

Wi-Fi Protected Setup (WPS).

- Wi-Fi Protected Setup (WPS) is the easiest but least secure authentication method for WLAN; it uses a push-button that associates the devices using a PIN. If a device does not have a push button, the PIN must be manually entered.
- WPS is highly vulnerable to brute-force attacks. PINs are eight digits; however, one digit is a checksum, and the remaining seven are further split into two groups of four and three digits, respectively.
- Easy Connect is a brand name for Device Provisioning Protocol (DPP), which uses public/private keys. QR codes or NFC tags communicate each device’s public key. Easy Connect was released with WPA3.

AUTHENTICATION PROTOCOLS.

Extensible Authentication Protocol (EAP).

Extensible Authentication Protocol (EAP) is an XML-based framework for communicating what authentication protocol will be used.

EAP is an authentication framework, not a specific authentication mechanism, and is frequently used in wireless networks and point-to-point connections.

AUTHENTICATION PROTOCOLS.

EAP-TLS.

EAP-TLS (EAP-Transport Layer Security) is one of the strongest authentication types; it is widely supported. Both the supplicant and the server are configured with certificates that provide mutual authentication.

The digital certificate must be signed by a certificate authority (CA) that both the client and the server trust; this gives better security to the EAP-TLS method, as intruders would still be required to hack the client-side certificate even if the password is somehow compromised. However, this could be a cumbersome task for a large WLAN installation.

AUTHENTICATION PROTOCOLS.

EAP-TTLS.

EAP-TTLS is an EAP (Extensible Authentication Protocol) method that encapsulates a TLS (Transport Layer Security) session, consisting of a handshake phase and a data phase.

EAP-TTLS is different from EAP-TLS because it does away with the EAP-TLS requirement of a supplicant-side certificate. Only the authentication server component requires a digital certificate. The authentication server is authenticated using its digital certificate.

CONTINUED ON NEXT SLIDE >

AUTHENTICATION PROTOCOLS.

EAP-TTLS.

An encrypted tunnel is then established between the supplicant and the authentication server. The supplicant's authentication credentials, such as a digital certificate or password, are passed to the authentication server over the established tunnel.

The supplicant can use other authentication methods, such as Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Microsoft CHAP (MS-CHAP) v2.

Having to manage certificates only on the server side makes EAP-TTLS much easier to manage.

AUTHENTICATION PROTOCOLS.

Protected Extensible Authentication Protocol (PEAP).

PEAP (Protected Extensible Authentication Protocol), also known as Protected EAP, is an authentication protocol that encapsulates EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

AUTHENTICATION PROTOCOLS.

EAP-FAST.

- EAP with Flexible Authentication via Secure Tunneling (FAST) is a protocol proposed by Cisco Systems to replace the previously proposed Lightweight Extensible Authentication Protocol (LEAP). EAP-FAST was designed to address the weaknesses of LEAP while preserving its “lightweight” implementation. EAP-FAST uses a pre-shared key called a protected access credential (PAC) to establish a TLS tunnel in which client credentials are verified.

- You will often see EAP-FAST (EAP-Flexible Authentication via Secure Tunneling [FAST]) with Enterprise authentication to a WAP.

AUTHENTICATION PROTOCOLS.

Knowledge check.

Let’s apply what we have covered:

- At its most basic level, what is EAP all about? (Hint: Extensible Authentication Protocol.)
- EAP-TLS – What makes it special? (Hint: Think about why this version is considered best at lessening the chances of MiTM attacks.)

Authentication methods.

AUTHENTICATION METHODS.

Key concepts.

In this section, we will cover the following key concepts:

- PSK.
- Enterprise authentication.
- Open authentication.
- Captive portals/splash page.

AUTHENTICATION METHODS.

Pre-shared key (PSK).

- Pre-shared key (PSK) authentication uses a passphrase to generate the key used to encrypt communications; it is also used for group communications because many users share the same secret. PSK is a client authentication method that uses a string of 64 hexadecimal digits, or a passphrase of 8 to 63 printable ASCII characters, to generate unique encryption keys for each wireless client.

- PSK is often mistakenly called the Wi-Fi password.

AUTHENTICATION METHODS.

Enterprise authentication.

Enterprise authentication is one of the main ways to set up a WAP to authenticate users before connecting them to the WLAN. An 802.1X network differs from home networks in one major way: it has an authentication server, which is most commonly a RADIUS server.

RADIUS checks a user's credentials to see if they are an active member of the organization and, depending on the network policies grants users varying levels of access to the network. This allows unique credentials or certificates to be used per user, eliminating the reliance on a single network password that can be easily stolen.

RADIUS or TACACS+ servers are the most popular AAA servers.

AUTHENTICATION METHODS.

Open authentication.

- Open authentication is another way to set up a connection to a WAP. No authentication of users takes place – you are setting up a hotspot – a public WAP. Also, be aware that any data transferred over an open connection will be unencrypted.

- Open authentication encryption can be controlled by the browser or by the end user implementing a VPN solution to ensure that the data is encrypted.

AUTHENTICATION METHODS.

Captive portals/splash page.

- When you log onto a network that is set up with open authentication, you may find yourself redirected to a captive portal or splash page. This will allow the provider to accept payment for using the network, such as paying for Wi-Fi on an airplane.

  There may also be a splash page that describes the terms and conditions you agree to while using the network.

- If you are not connecting using HTTPS or a VPN, then any data transferred over that connection will be unencrypted. Initiate your VPN after you sign onto the hotspot.

AUTHENTICATION METHODS.

Knowledge check.

Let’s apply what we have covered:

- If you select WAP2-Enterprise, that implies that you have a certain type of server to facilitate a corporate LAN connection. What type of server are we speaking about here?

Network installation considerations.

NETWORK INSTALLATION CONSIDERATIONS.

Key concepts.

In this section, we will cover the following key concepts:

- Ad hoc wireless.
- Peer-to-peer.
- Wi-Fi direct.
- WAP.
- SSID.
- BSS/BSSID.
- ESS/ESSID.
- AP modes.
- STA.

NETWORK INSTALLATION CONSIDERATIONS.

Ad hoc wireless.

An ad hoc wireless network is one in which wireless devices connect without using a wireless access point (WAP). Ad hoc connections are not permanent — in fact, these can be created without an administrator. This is not the only concern, however. Ad hoc connections will cause the user devices to have degraded performance issues, and any host-based intrusion system will fail; given this, they can become a vector for data loss.

The ad hoc connection becomes a bridge into the corporate network, providing one more vector for an attacker. Administrators can stop an ad hoc network by restricting user access to Control Panel, especially the Network settings. An example of an ad hoc network would be a laptop directly connecting wirelessly to another laptop to transfer data.

NETWORK INSTALLATION CONSIDERATIONS.

Peer-to-peer.

Once two devices have located each other, they enter negotiations about which device will act as the P2P Group Owner (P2P GO). The P2P GO closely resembles the AP in a traditional network, allowing the other device to connect to it. Printers, Smart TVs, and similar Internet of Things (IoT) devices are often designed to act by default P2P GOs.

They emit beacon frames so that other devices can find them and determine if they are suitable to connect to. Unfortunately, Kismet and Aircrack-ng suite can discover P2P devices in the Group Owner (GO) mode.

This allows anyone to establish a Wi-Fi connection to the printer without any authentication or notification. The attacker then has full access to the printer — potentially including its print memory and history — and an entry point to the wider Wi-Fi network that the printer is connected to.

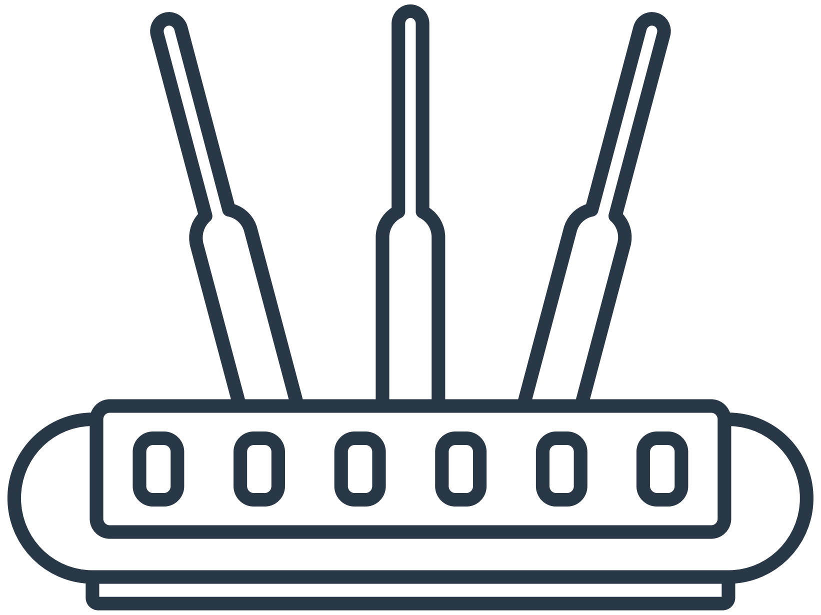
NETWORK INSTALLATION CONSIDERATIONS.

Wi-Fi Direct.

- Wi-Fi Direct is a peer-to-peer (P2P) wireless network connection between two or more devices; one of the devices acts as an access point and allows connections using WPS, WPA, or WPA2.
- Wi-Fi Direct is a lot like Bluetooth except with speeds up to 250Mbps (ten times the speed offered by Bluetooth 4.0). It allows two devices to set up a peer-to-peer (P2P) Wi-Fi network without a wireless router.
- The Wi-Fi Direct standard mandates that once a connection is requested, the devices then use the WPS connection protocol to establish the connection. The WPS pin is a numerical eight-digit code, which is easily subjected to brute force attack. HP's implementation of the WPS protocol is to automatically allow Wi-Fi Direct connections using the default WPS password of '12345678'.

NETWORK INSTALLATION CONSIDERATIONS.

Wireless Access Point (WAP).



A Wireless Access Point (WAP) is a networking device that enables connected wireless devices to pass data to and from another network; this is generally a wired network but could also be a cellular network.

Wireless access points (WAPs) are becoming one of the main entry points for devices into a network.

This network is generally connected to the internet through a default gateway. Default settings on most WAPs have little to no security features enabled; administrators must properly configure these.

NETWORK INSTALLATION CONSIDERATIONS.

Service Set Identifier (SSID).

A Service Set Identifier (SSID) is the unique name of a wireless local area network (WLAN); most people refer to it as the name of your wireless connection.

The service set identifier (SSID) is the name that has been given to a WLAN. Most WAPs come with a default SSID containing the WAP manufacturer's name and random digits.

CONTINUED ON NEXT SLIDE >

NETWORK INSTALLATION CONSIDERATIONS.

Service Set Identifier (SSID).

The default SSID should be changed, as it provides fingerprinting information about your WAP device. Administrators should also not use any personal information when changing the SSID. SSIDs can be up to 32 characters, normally comprised of ASCII letters and digits.

Administrators should also disable the broadcast of the SSID, which is called SSID cloaking.

Basic Service Set (BSS).

- A Basic Service Set (BSS) is the network that wireless devices use to communicate. This network may be ad hoc or use a wireless access point (WAP). A BSS is the most basic wireless local area network; it is the logical topology of all the devices or stations (STAs) connected to a single WAP. A WAP in infrastructure mode will be at the center of a BSS.
- BSS networks are in most homes and smaller businesses as the preferred methods to connect to the WLAN and, thereby, the internet

CONTINUED ON NEXT SLIDE >

NETWORK INSTALLATION CONSIDERATIONS.

BSSID.

- A BSSID is the MAC address of the WAP, which resides in layer 2 of the OSI model.
- Tools such as Aircrack-ng can easily identify the BSSID of a WAP, as the BSSID is part of the information sent in an AP broadcast. Other tools, such as bettercap, can be used to configure a Wi-Fi Pineapple rogue WAP with the same BSSID. Used in conjunction with the same SSID as a target WAP, you have created an evil twin. If a user "auto-joins" a previously known network, they could connect to the evil twin.

Extended Service Set (ESS).

- An Extended Service Set (ESS) is a wireless network of numerous BSSs, each having the same SSID; this allows a wireless device to "roam" and connect from one WAP to another as they move through a building.
- The ESS allows stations (STAs) to roam from one WAP to another without re-authenticating. The wireless controller or fat client WAPs are normally connected to the wired network. You will see extended service sets (ESSs) in medium to large business networks where multiple WAPs are employed together with the same SSID (called an ESSID since it is joining ESSs) to enable roaming connections to the WLAN.
- ESSID is the same as an SSID for a BSS. The SSID on each WAP in an ESS must be the same.

CONTINUED ON NEXT SLIDE >

AP modes.

Wireless routers/access points have several modes that define their use.

The normal setup is AP mode or infrastructure mode; other modes include client, client bridged, ad-hoc, and repeater.

- Access point (AP) mode connects to wireless clients (wireless adapter cards) such as laptops, desktops, and PDAs. Wireless clients can only communicate to APs in access point mode.
- AP client or wireless client mode allows the access point to become a wireless client to another AP. In essence, the AP has now become a wireless adapter card. You would use this mode to allow an AP to communicate with another AP.

CONTINUED ON NEXT SLIDE >

NETWORK INSTALLATION CONSIDERATIONS.

AP modes.

Point-to-point/wireless bridge mode allows the access point to communicate with another access point capable of point-to-point bridging; however, be aware that most manufacturers use proprietary settings when enabling bridging mode in the access point. A typical scenario for this selection is connecting two buildings through a wireless connection.

CONTINUED ON NEXT SLIDE >

NETWORK INSTALLATION CONSIDERATIONS.

AP modes.

The Wireless Distribution System (WDS) mode is like the bridge mode. In WDS mode, you can get your access points to communicate with each other wirelessly.

The access points will not communicate with wireless clients in this mode. The WDS with AP mode allows your access points to communicate with each other wirelessly and, at the same time, allows wireless clients to connect to the network.

NETWORK INSTALLATION CONSIDERATIONS.

Station (STA).

Stations are devices that can use wireless protocols; they are abbreviated as STA.

A wireless device connected to a WAP is considered a station (STA). Some texts refer to the STA as the wireless network interface card. Administrators need to be able to track/monitor the stations connected to their WAPs just as they would track/monitor endpoints connected to the wired network. It should be noted that some devices can operate in either STA or AP mode.

Any wireless device that can connect to an ad hoc or wireless infrastructure network is a station — laptop, smartphone, iPad, etc.

NETWORK INSTALLATION CONSIDERATIONS.

Knowledge check.

Let's apply what we have covered:

- What is the difference between an ESS and a BSS?
- When I ask for the PSK for your SSID, what am I trying to get, and what am I trying to do?

Wireless vulnerabilities and attacks.

WIRELESS VULNERABILITIES AND ATTACKS.

Key concepts.

In this section, we will cover the following key concepts:

- Evil twin.
- Rogue Access Point.
- Disassociation.
- Jamming.
- Bluetooth attacks.
- Near Field Communication (NFC).
- Radio Frequency Identifier (RFID).
- Initialization vector.
- Weak encryption.

WIRELESS VULNERABILITIES AND ATTACKS.

Evil twin.

- An evil twin is a WAP that has been set up for malicious purposes. Often, the SSID is either the same or similar to a legitimate access point.

- Threat actors will often set these up with high power to “drown out” the legitimate WAP in hopes of luring someone to connect.

Rogue AP.

- A rogue AP is an access point that has been installed on a network without authorization; it could be malicious or not.

- Rogue APs represent a serious security breach as they are unauthorized and generally not set up securely.

- Administrators should periodically check that all devices connected to the wired network are authorized. Administrators should also use a spectrum analyzer to ensure that only authorized Wi-Fi transmissions are made.

WIRELESS VULNERABILITIES AND ATTACKS.

Disassociation attack.

- Connecting to a WAP is called associating with it. A disassociation attack forces clients to attempt to re-associate with the WAP. A bad actor will also bring up their rogue WAP, or evil twin, at this point, hoping the affected users will view this new (rogue) WAP as a better option and select the new WAP.

  The hacker's end game is to capture the unsuspecting user's login credentials.

- Disassociation attacks could also be implemented as a DoS attack by repeatably kicking users off their connection.

WIRELESS VULNERABILITIES AND ATTACKS.

Jamming.

Jamming is an attack used by attackers to prevent your cell phone from making or receiving calls, text messages, and emails, prevent your Wi-Fi-enabled device from connecting to the internet, prevent your GPS unit from receiving correct positioning signals, or prevent a first responder from locating you in an emergency.

WIRELESS VULNERABILITIES AND ATTACKS.

Bluetooth attacks.

- BlueBorne, in general, is any attack that can happen over Bluetooth.
- Blue Snarfing is the theft of data from a wireless device through Bluetooth connections.
- Blue Jacking is the sending of unsolicited messages from one Bluetooth device to another Bluetooth device.
- Bluebugging allows the attacker to take over the victim’s Bluetooth devices and spy on phone calls, transmit messages, and connect to the internet without the victim’s knowledge.

WIRELESS VULNERABILITIES AND ATTACKS.

Near Field Communication (NFC).

Near Field Communication (NFC) is used to communicate with other NFC devices within very close range, typically about 4 inches.

NFC is susceptible to the following attacks:

- Eavesdropping.
- Data Modification.
- Data Corruption.
- Replay Attack.
- Data Insertion.
- MiTM.

WIRELESS VULNERABILITIES AND ATTACKS.

Radio Frequency Identifier (RFID).

Radio Frequency Identifier (RFID) is a one-way communication method that allows for longer-range communication when compared to NFC – the higher range for RFID is around 100 meters. It utilizes radio frequencies to track, tag, or locate items. This can be facilitated with passive or active RFID.

Passive RFID has no internal power source and gets its power from the receiving device. Active RFID has an internal power source, typically in the form of a battery.

These radio tags help facilitate tracking but can themselves be tracked.

CONTINUED ON NEXT SLIDE >

WIRELESS VULNERABILITIES AND ATTACKS.

Radio Frequency Identifier (RFID).

RFID cloning allows the attacker to access confidential information by copying data from a valid RFID to the cloned RFID.

RFID spoofing allows an attacker to control data transmission after spoofing the RFID signals and transmitting the attacker's data along with the original ID of the RFID tag to appear to be legitimate.

Initialization Vector (IV).

An Initialization Vector (IV) is a binary value used to initialize a cryptographic algorithm.

- In cryptography, an initialization vector (IV) is a block of bits that is required to allow a stream cipher or a block cipher to be executed in any of several modes of operation in order to produce a unique stream independent from other streams produced by the same encryption key, without having to go through a (usually lengthy) re-keying process.
- One of the issues with Wired Equivalent Privacy (WEP) is that this initial IV was a short key, 24 bits, and sent in clear text; this led to bad actors having the ability to find the value for this IV and crack WEP relatively easily.

Weak encryption.

Weak encryption involves using an older or not mathematically-secure encryption protocol on a network. WPS, WEP, and WPA are considered weak in today's computing world. You will see weak encryption in one of three ways:

1. Older equipment still being used may not be able to use strong encryption.
2. Many IoT devices are limited by weak encryption. They can or cannot use any encryption due to power consumption requirements.
3. Downgrade attacks target systems with strong encryption but are willing to use weak encryption to communicate. You can and should enforce no downgrading in your systems.

CONTINUED ON NEXT SLIDE >

WIRELESS VULNERABILITIES AND ATTACKS.

Knowledge check.

Let's apply what we have covered:

- Describe the Bluetooth attacks.
- How would you explain the differences between an evil twin and a rogue access point?

End of Module.

For additional practice, please complete all associated self-study activities and labs.