CCNA 2 v7.0 Curriculum: Module 12 – WLAN Concepts

itexamanswers.net/ccna-2-v7-0-curriculum-module-12-wlan-concepts.html

June 9, 2020

Contents

12.0 Introduction

12.0.1 Why should I take this module?

Welcome to WLAN Concepts!

Do you use a wireless connection at home, work or school? Ever wonder how it works?

There are many ways to connect wirelessly. Like everything else involving networks, these connection types are best used in particular situations. They require specific devices and are also prone to certain types of attacks. And of course, there are solutions to mitigate these attacks. Want to learn more? The WLAN Concepts module gives you the foundational knowledge you need to understand what Wireless LANs are, what they can do, and how to protect them.

If you are curious, don't wait, get started today!

12.0.2 What will I learn in this module?

Module Title: WLAN Concepts

Module Objective: Explain how WLANs enable network connectivity.

Topic Title	Topic Objective
Introduction to Wireless	Describe WLAN technology and standards.
Components of WLANs	Describe the components of a WLAN infrastructure.
WLAN Operation	Explain how wireless technology enables WLAN operation.
CAPWAP Operation	Explain how a WLC uses CAPWAP to manage multiple APs.
Channel Management	Describe channel management in a WLAN.
WLAN Threats	Describe threats to WLANs.
Secure WLANs	Describe WLAN security mechanisms.

12.1 Introduction to Wireless

12.1.1 Benefits of Wireless

A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments. Networks must support people who are on the move. People connect using computers, laptops, tablets, and smart phones. There are many different network infrastructures that provide network access, such as wired LANs, service provider networks, and cell phone networks. But it's the WLAN that makes mobility possible within the home and business environments.

In businesses with a wireless infrastructure in place, there can be a cost savings any time equipment changes, or when relocating an employee within a building, reorganizing equipment or a lab, or moving to temporary locations or project sites. A wireless infrastructure can adapt to rapidly changing needs and technologies.

12.1.2 Types of Wireless Networks

Wireless networks are based on the Institute of Electrical and Electronics Engineers (IEEE) standards and can be classified broadly into four main types: WPAN, WLAN, WMAN, and WWAN.

Click each wireless network type for more information.

- WPAN
- WLAN
- WMAN
- WWANs

Wireless Personal-Area Networks (WPAN) - Uses low powered transmitters for a short-range network, usually 20 to 30 ft. (6 to 9 meters). Bluetooth and ZigBee based devices are commonly used in WPANs. WPANs are based on the 802.15 standard and a 2.4-GHz radio frequency.

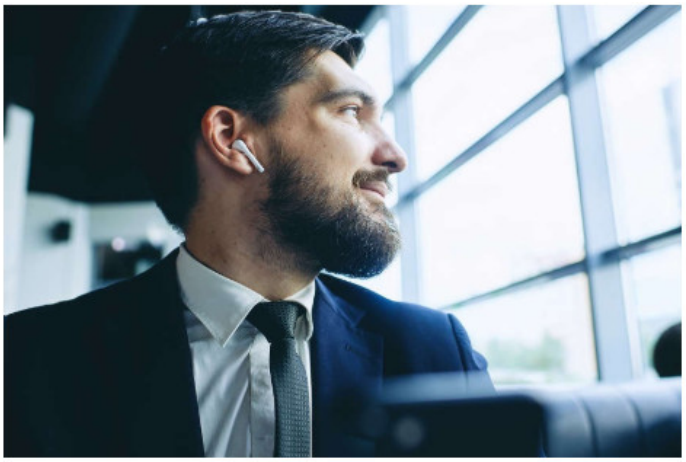
12.1.3 Wireless Technologies

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device they are using.

Click each wireless technology for more information.

Bluetooth - An IEEE 802.15 WPAN standard that uses a device-pairing process to communicate over distances up to 300 ft. (100m). It can be found in smart home devices, audio connections, automobiles, and other devices that require a short distance connection. There are two types of Bluetooth radios:

- **Bluetooth Low Energy (BLE)** - This supports multiple network technologies including mesh topology to large scale network devices.
- **Bluetooth Basic Rate/Enhanced Rate (BR/EDR)** - This supports point to point topologies and is optimized for audio streaming.



12.1.4. 802.11 Standards

The world of wireless communications is vast. However, for particular job-related skills, we want to focus on specific aspects of Wi Fi. The best place to start is with the IEEE 802.11 WLAN standards. These standards define how radio frequencies are used for wireless links. Most of the standards specify that wireless devices have one antenna to transmit and receive wireless signals on the specified radio frequency (2.4 GHz or 5 GHz). Some of the newer standards that transmit and receive at higher speeds require access points (APs) and wireless clients to have multiple antennas using the multiple-input and multiple-output (MIMO) technology. MIMO uses multiple antennas as both the transmitter and receiver to improve communication performance. Up to four antennas can be supported.

Various implementations of the IEEE 802.11 standard have been developed over the years. The table highlights these standards.

IEEE WLAN Standard	Radio Frequency	Description
802.11	2.4 GHz	speeds of up to 2 Mbps
802.11a	5 GHz	• speeds of up to 54 Mbps • small coverage area • less effective at penetrating building structures • not interoperable with the 802.11b and 802.11g
802.11b	2.4 GHz	• speeds of up to 11 Mbps • longer range than 802.11a • better able to penetrate building structures

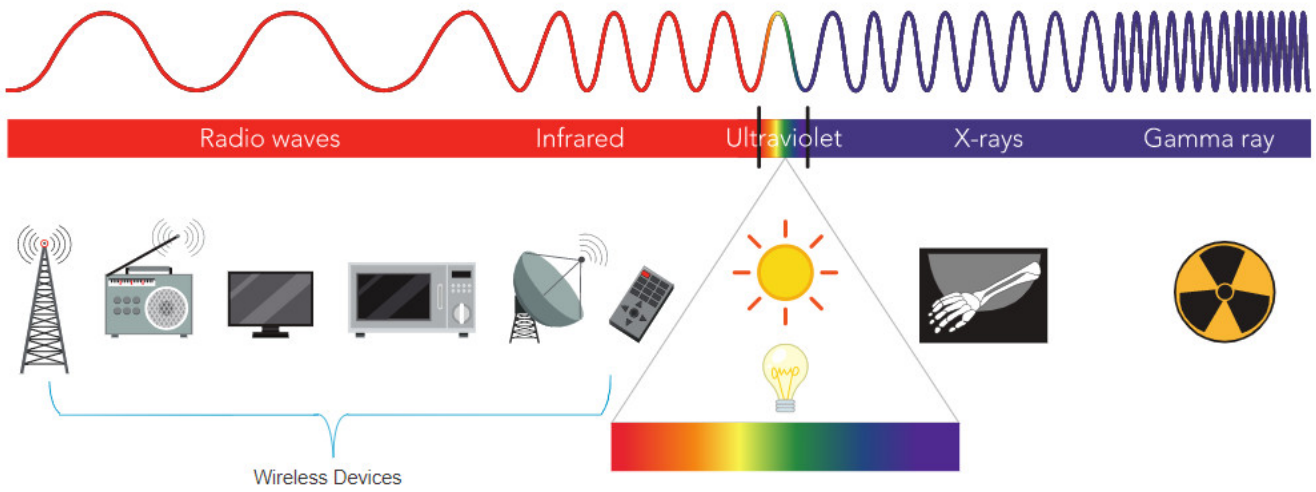
IEEE WLAN Standard	Radio Frequency	Description
802.11g	2.4 GHz	• speeds of up to 54 Mbps • backward compatible with 802.11b with reduced bandwidth capacity
802.11n	2.4 GHz 5 GHz	• data rates range from 150 Mbps to 600 Mbps with a distance range of up to 70 m (230 feet) • APs and wireless clients require multiple antennas using MIMO technology • backward compatible with 802.11a/b/g devices with limiting data rates
802.11ac	5 GHz	• provides data rates ranging from 450 Mbps to 1.3 Gbps (1300 Mbps) using MIMO technology • Up to eight antennas can be supported • backwards compatible with 802.11a/n devices with limiting data rates
802.11ax	2.4 GHz 5 GHz	• released in 2019 – latest standard • also known as High-Efficiency Wireless (HEW) • higher data rates • increased capacity • handles many connected devices • improved power efficiency • 1 GHz and 7 GHz capable when those frequencies become available • Search the internet for Wi-Fi Generation 6 for more information

12.1.5 Radio Frequencies

All wireless devices operate in the radio waves range of the electromagnetic spectrum. WLAN networks operate in the 2.4 GHz frequency band and the 5 GHz band. Wireless LAN devices have transmitters and receivers tuned to specific frequencies of the radio waves range, as shown in the figure. Specifically, the following frequency bands are allocated to 802.11 wireless LANs:

- 2.4 GHz (UHF) – 802.11b/g/n/ax
- 5 GHz (SHF) – 802.11a/n/ac/ax

The Electromagnetic Spectrum



12.1.6 Wireless Standards Organizations

Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards are the ITU-R, the IEEE, and the Wi-Fi Alliance.

Click each button for more information about the standards organization.

- ITU
- IEEE
- Wi-Fi Alliance

ITU

The International Telecommunication Union (ITU) regulates the allocation of the radio frequency spectrum and satellite orbits through the ITU-R. ITU-R stands for the ITU Radiocommunication Sector.

12.2 WLAN Components

12.2.1 Video – WLAN Components

In the previous topic you learned about the benefits of wireless, types of wireless networks, 802.11 standards, and radio frequencies. Here we will learn about WLAN components.

Click Play to view a video about WLAN components.

12.2.2 Wireless NICs

Wireless deployments require a minimum of two devices that have a radio transmitter and a radio receiver tuned to the same radio frequencies:

- End devices with wireless NICs
- A network device, such as a wireless router or wireless AP

To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver. However, if a device does not have an integrated wireless NIC, then a USB wireless adapter can be used, as shown in the figure.

Note: Many wireless devices you are familiar with do not have visible antennas. They are embedded inside smartphones, laptops, and wireless home routers.

USB Wireless Adapter

12.2.3 Wireless Home Router

The type of infrastructure device that an end device associates and authenticates with varies based on the size and requirement of the WLAN.

For example, a home user typically interconnects wireless devices using a small, wireless router, as shown in the figure. The wireless router serves as an:

- **Access point** – This provides 802.11a/b/g/n/ac wireless access.
- **Switch** – This provides a four-port, full-duplex, 10/100/1000 Ethernet switch to interconnect wired devices.

- **Router** – This provides a default gateway for connecting to other network infrastructures, such as the internet.

A wireless router is commonly implemented as a small business or residential wireless access device. The wireless router advertises its wireless services by sending beacons containing its shared service set identifier (SSID). Devices wirelessly discover the SSID and attempt to associate and authenticate with it to access the local network and internet.

Most wireless routers also provide advanced features, such as high-speed access, support for video streaming, IPv6 addressing, quality of service (QoS), configuration utilities, and USB ports to connect printers or portable drives.

Additionally, home users who want to extend their network services can implement Wi-Fi range extenders. A device can connect wirelessly to the extender, which boosts its communications to be repeated to the wireless router.

12.2.4 Wireless Access Points

While range extenders are easy to set up and configure, the best solution would be to install another wireless access point to provide dedicated wireless access to the user devices. Wireless clients use their wireless NIC to discover nearby APs advertising their SSID. Clients then attempt to associate and authenticate with an AP. After being authenticated, wireless users have access to network resources. The Cisco Meraki Go APs are shown in the figure.

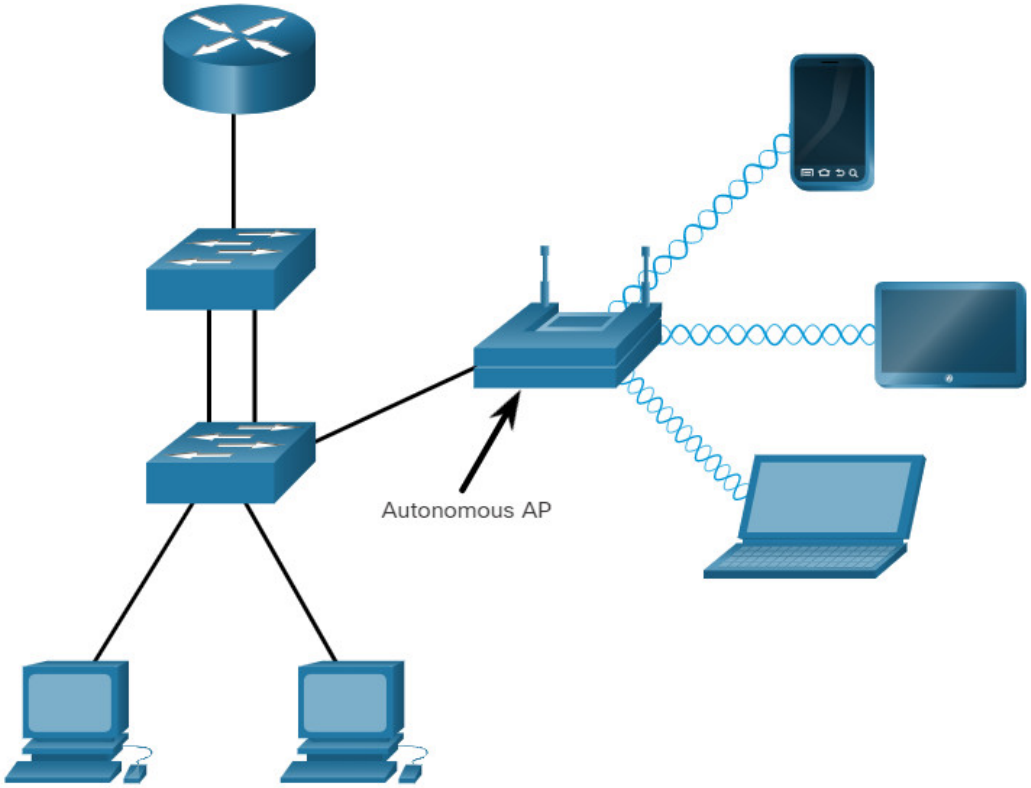
12.2.5 AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

Click each button for a topology and explanation of each type.

- Autonomous APs
- Controller-based APs

Autonomous APs
These are standalone devices configured using a command line interface or a GUI, as shown in the figure. Autonomous APs are useful in situations where only a couple of APs are required in the organization. A home router is an example of an autonomous AP because the entire AP configuration resides on the device. If the wireless demands increase, more APs would be required. Each AP would operate independent of other APs and each AP would require manual configuration and management. This would become overwhelming if many APs were needed.



12.2.6 Wireless Antennas

Most business class APs require external antennas to make them fully functioning units.

Click each antenna for more information.

Omnidirectional Antennas
Omnidirectional antennas such as the one shown in the figure provide 360-degree coverage and are ideal in houses, open office areas, conference rooms, and outside areas.

12.3 WLAN Operation

12.3.1 Video – WLAN Operation

The previous topic covered WLAN components. This topic will cover WLAN operation.

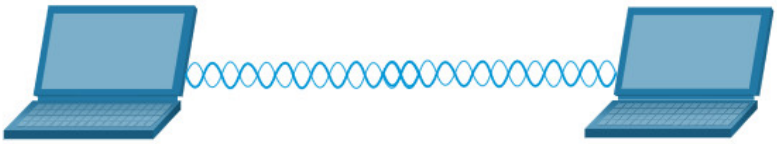
Click Play to view a video about WLAN operation.

12.3.2. 802.11 Wireless Topology Modes

Wireless LANs can accommodate various network topologies. The 802.11 standard identifies two main wireless topology modes: Ad hoc mode and Infrastructure mode. Tethering is also a mode sometimes used to provide quick wireless access.

Click each wireless topology mode for more information.

Ad hoc mode - This is when two devices connect wirelessly in a peer-to-peer (P2P) manner without using APs or wireless routers. Examples include wireless clients connecting directly to each other using Bluetooth or Wi-Fi Direct. The IEEE 802.11 standard refers to an ad hoc network as an independent basic service set (IBSS).



12.3.3 BSS and ESS

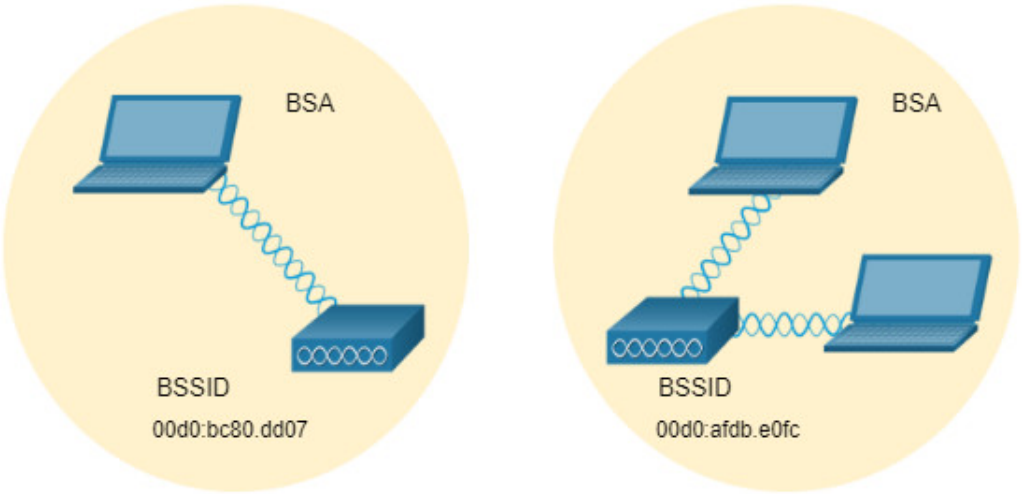
Infrastructure mode defines two topology building blocks: A Basic Service Set (BSS) and an Extended Service Set (ESS).

Click BSS and ESS for more information.

- BSS
- ESS

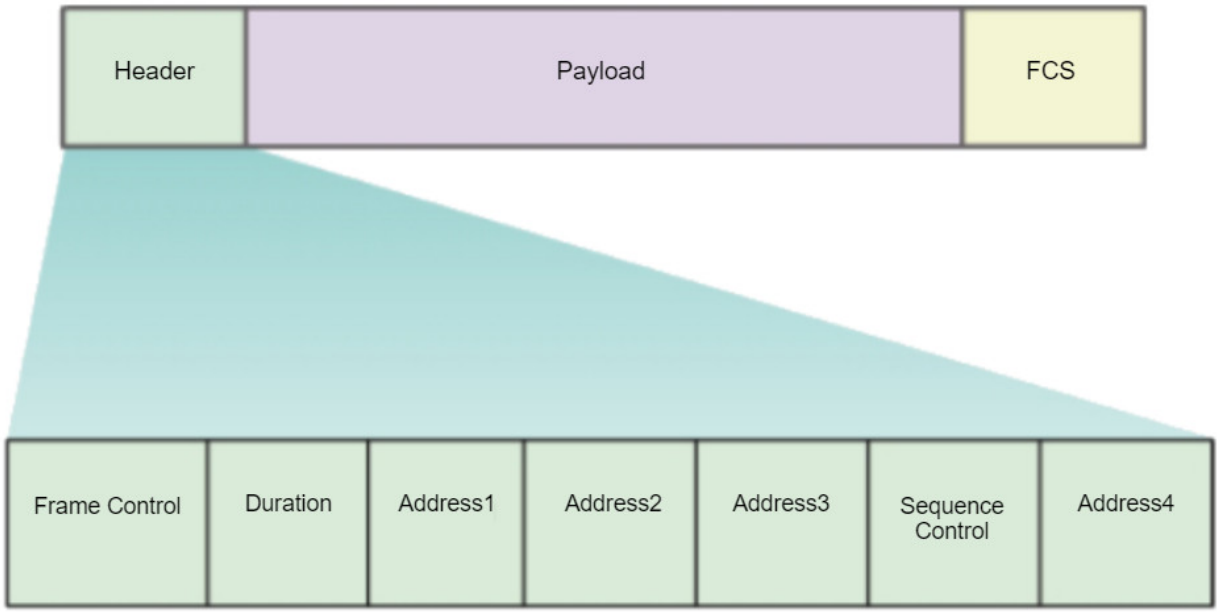
Basic Service Set
A BSS consists of a single AP interconnecting all associated wireless clients. Two BSSs are shown in the figure. The circles depict the coverage area for the BSS, which is called the Basic Service Area (BSA). If a wireless client moves out of its BSA, it can no longer directly communicate with other wireless clients within the BSA.

The Layer 2 MAC address of the AP is used to uniquely identify each BSS, which is called the Basic Service Set Identifier (BSSID). Therefore, the BSSID is the formal name of the BSS and is always associated with only one AP.



12.3.4. 802.11 Frame Structure

Recall that all Layer 2 frames consist of a header, payload, and Frame Check Sequence (FCS) section. The 802.11 frame format is similar to the Ethernet frame format, except that it contains more fields, as shown in the figure.



All 802.11 wireless frames contain the following fields:

- **Frame Control** – This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
- **Duration** – This is typically used to indicate the remaining duration needed to receive the next frame transmission.
- **Address1** – This usually contains the MAC address of the receiving wireless device or AP.
- **Address2** – This usually contains the MAC address of the transmitting wireless device or AP.

- **Address3** – This sometimes contains the MAC address of the destination, such as the router interface (default gateway) to which the AP is attached.
- **Sequence Control** – This contains information to control sequencing and fragmented frames.
- **Address4** – This usually missing because it is used only in ad hoc mode.
- **Payload** – This contains the data for transmission.
- **FCS** – This is used for Layer 2 error control.

12.3.5 CSMA/CA

WLANs are half-duplex, shared media configurations. Half-duplex means that only one client can transmit or receive at any given moment. Shared media means that wireless clients can all transmit and receive on the same radio channel. This creates a problem because a wireless client cannot hear while it is sending, which makes it impossible to detect a collision.

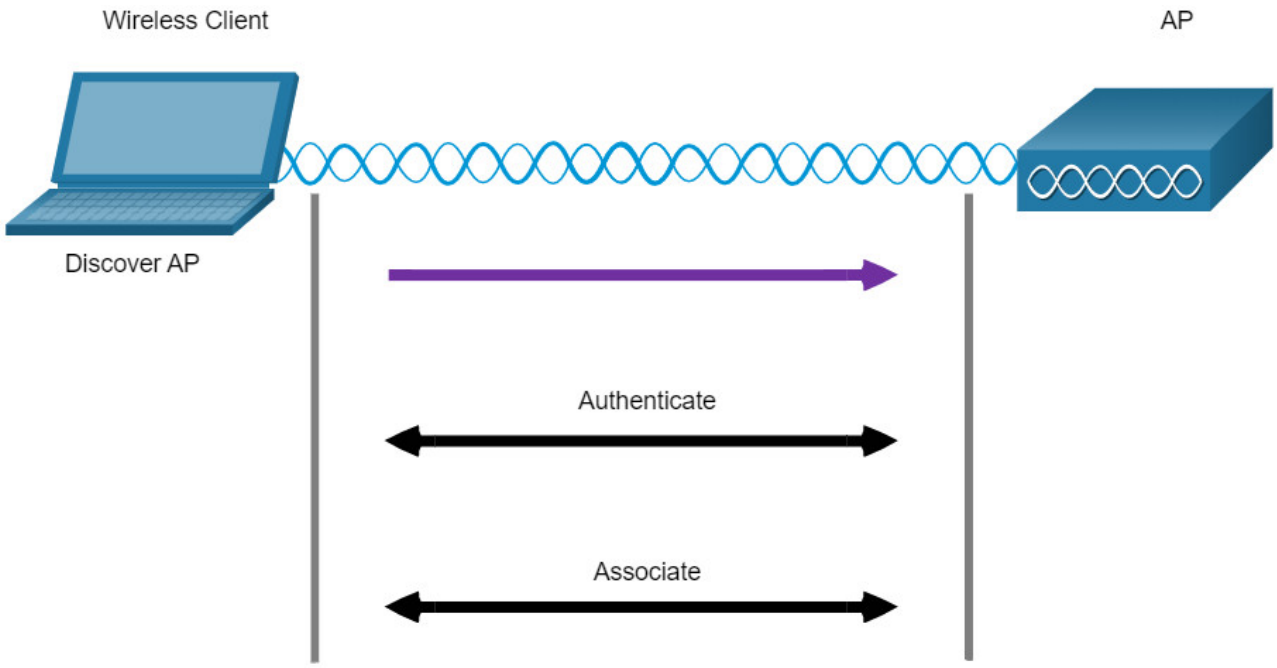
To resolve this problem, WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) as the method to determine how and when to send data on the network. A wireless client does the following:

1. Listens to the channel to see if it is idle, which means that is senses no other traffic is currently on the channel. The channel is also called the carrier.
2. Sends a ready to send (RTS) message to the AP to request dedicated access to the network.
3. Receives a clear to send (CTS) message from the AP granting access to send.
4. If the wireless client does not receive a CTS message, it waits a random amount of time before restarting the process.
5. After it receives the CTS, it transmits the data.
6. All transmissions are acknowledged. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process.

12.3.6 Wireless Client and AP Association

For wireless devices to communicate over a network, they must first associate with an AP or wireless router. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. Wireless devices complete the following three stage process, as shown in the figure:

- Discover a wireless AP
- Authenticate with AP
- Associate with AP



In order to have a successful association, a wireless client and an AP must agree on specific parameters. Parameters must then be configured on the AP and subsequently on the client to enable the negotiation of a successful association.

- **SSID** -The SSID name appears in the list of available wireless networks on a client. In larger organizations that use multiple VLANs to segment traffic, each SSID is mapped to one VLAN. Depending on the network configuration, several APs on a network can share a common SSID.
- **Password** – This is required from the wireless client to authenticate to the AP.
- **Network mode** – This refers to the 802.11a/b/g/n/ac/ad WLAN standards. APs and wireless routers can operate in a Mixed mode meaning that they can simultaneously support clients connecting via multiple standards.
- **Security mode** – This refers to the security parameter settings, such as WEP, WPA, or WPA2. Always enable the highest security level supported.
- **Channel settings** – This refers to the frequency bands used to transmit wireless data. Wireless routers and APs can scan the radio frequency channels and automatically select an appropriate channel setting. The channel can also be set manually if there is interference with another AP or wireless device.

12.3.7 Passive and Active Discover Mode

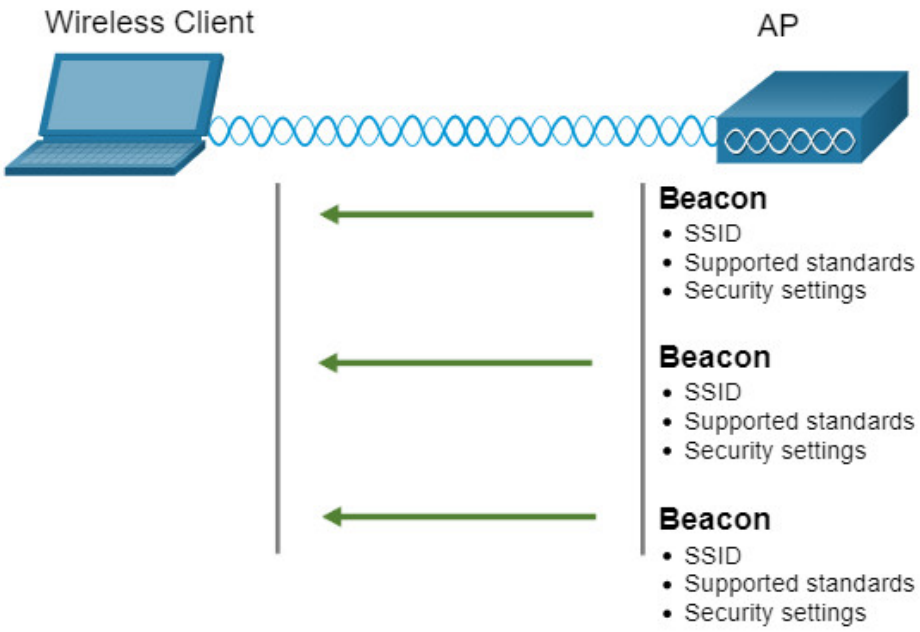
Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process. This process can be passive or active.

Click each mode for more information.

- Passive mode

- Active mode

Passive mode
In passive mode, the AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings. The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area. This allows the wireless clients to choose which network and AP to use.



12.4 CAPWAP Operation

12.4.1 Video – CAPWAP

In the previous topic you learned about WLAN operation. Now you will learn about Control and Provisioning of Wireless Access Points (CAPWAP).

Click Play to view a video about Control and Provisioning of Wireless Access Points (CAPWAP) protocol.

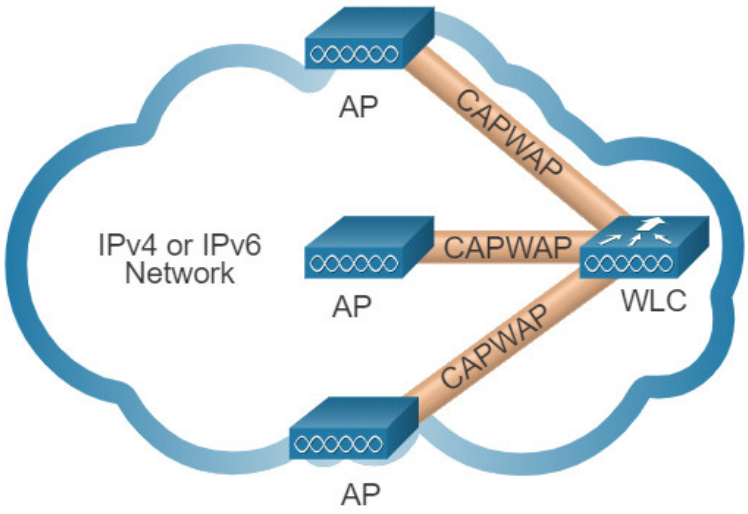
12.4.2 Introduction to CAPWAP

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

CAPWAP is based on LWAPP but adds additional security with Datagram Transport Layer Security (DTLS). CAPWAP establishes tunnels on User Datagram Protocol (UDP) ports. CAPWAP can operate either over IPv4 or IPv6, as shown in the figure, but uses IPv4 by

default.

IPv4 and IPv6 can use UDP ports 5246 and 5247. However, CAPWAP tunnels use different IP protocols in the frame header. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.



12.4.3 Split MAC Architecture

A key component of CAPWAP is the concept of a split media access control (MAC). The CAPWAP split MAC concept does all of the functions normally performed by individual APs and distributes them between two functional components:

- AP MAC Functions
- WLC MAC Functions

The table shows some of the MAC functions performed by each.

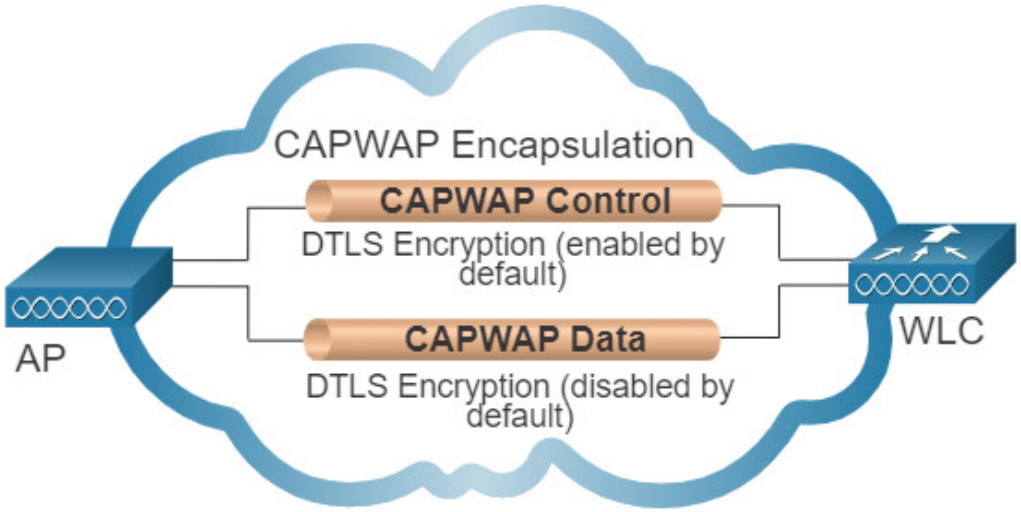
AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgements and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

12.4.4 DTLS Encryption

DTLS is a protocol which provides security between the AP and the WLC. It allows them to communicate using encryption and prevents eavesdropping or tampering.

DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel, as shown in the figure. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MITM) attacks.

CAPWAP data encryption is optional and is enabled per AP. Data encryption requires a DTLS license to be installed on the WLC prior to being enabled on an AP. When enabled, all WLAN client traffic is encrypted at the AP before being forwarded to the WLC and vice versa.

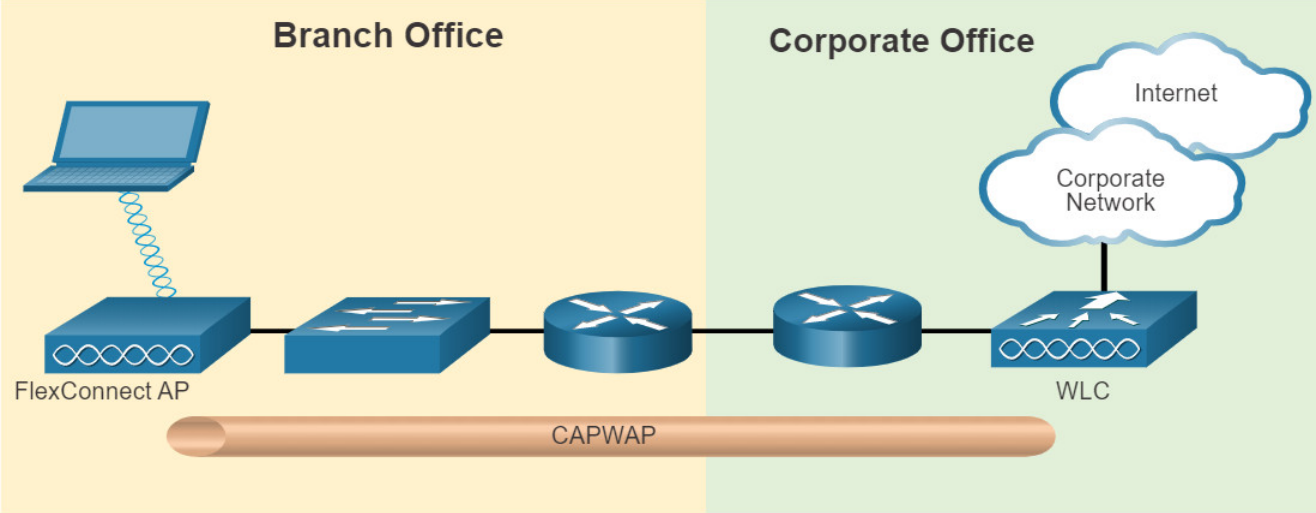


12.4.5 FlexConnect APs

FlexConnect is a wireless solution for branch office and remote office deployments. It lets you configure and control access points in a branch office from the corporate office through a WAN link, without deploying a controller in each office.

There are two modes of operation for the FlexConnect AP.

- **Connected mode** – The WLC is reachable. In this mode the FlexConnect AP has CAPWAP connectivity with its WLC and can send traffic through the CAPWAP tunnel, as shown in the figure. The WLC performs all its CAPWAP functions.
- **Standalone mode** – The WLC is unreachable. The FlexConnect has lost or failed to establish CAPWAP connectivity with its WLC. In this mode, a FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.



12.5 Channel Management

12.5.1 Frequency Channel Saturation

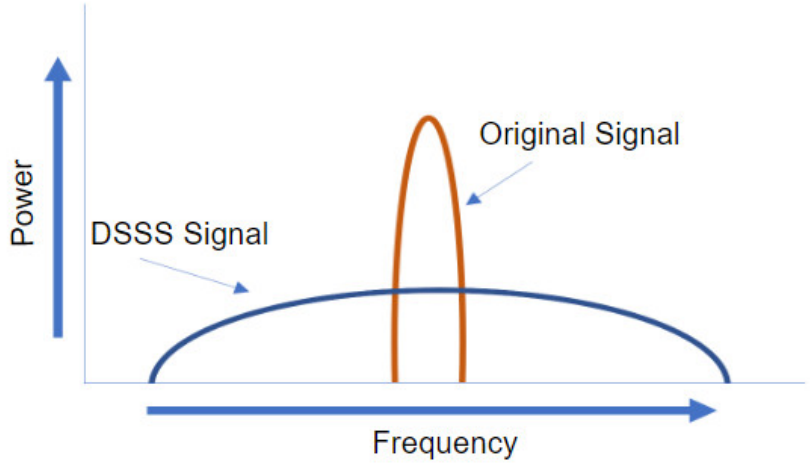
Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate. A common practice is for frequencies to be allocated as ranges. Such ranges are then split into smaller ranges called channels.

If the demand for a specific channel is too high, that channel is likely to become oversaturated. The saturation of the wireless medium degrades the quality of the communication. Over the years, a number of techniques have been created to improve wireless communication and alleviate saturation. These techniques mitigate channel saturation by using the channels in a more efficient way.

Click each frequency channel saturation technique for more information.

- DSSS
- FHSS
- OFDM

Direct-Sequence Spread Spectrum (DSSS) - This is a modulation technique designed to spread a signal over a larger frequency band. Spread spectrum techniques were developed during war time to make it more difficult for enemies to intercept or jam a communication signal. It does this by spreading the signal over a wider frequency which effectively hides the discernable peak of the signal, as shown in the figure. A properly configured receiver can reverse the DSSS modulation and re-construct the original signal. DSSS is used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.

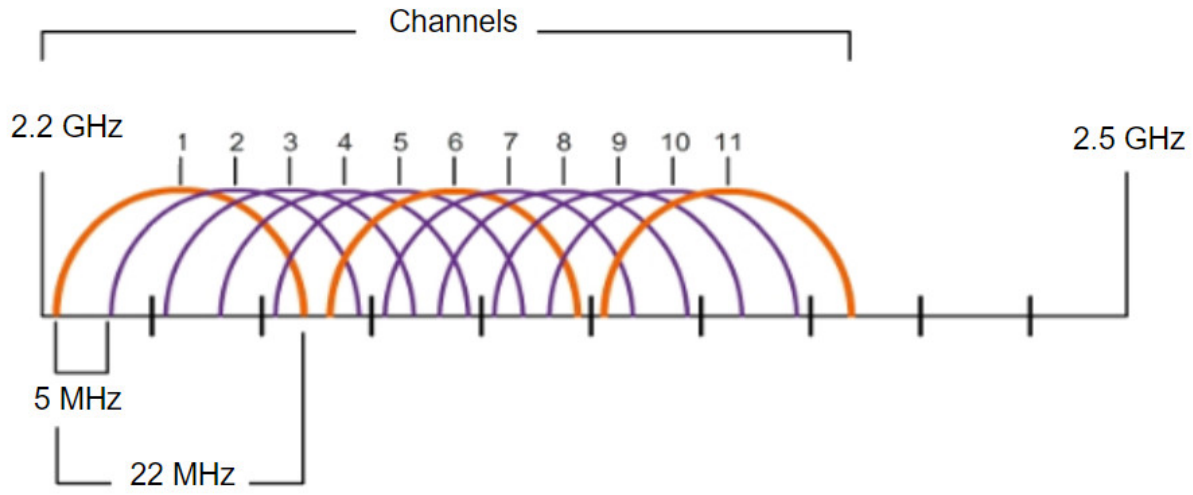


12.5.2 Channel Selection

A best practice for WLANs requiring multiple APs is to use non-overlapping channels. For example, the 802.11b/g/n standards operate in the 2.4 GHz to 2.5GHz spectrum. The 2.4 GHz band is subdivided into multiple channels. Each channel is allotted 22 MHz bandwidth and is separated from the next channel by 5 MHz. The 802.11b standard identifies 11 channels for North America, as shown in the figure (13 in Europe and 14 in Japan).

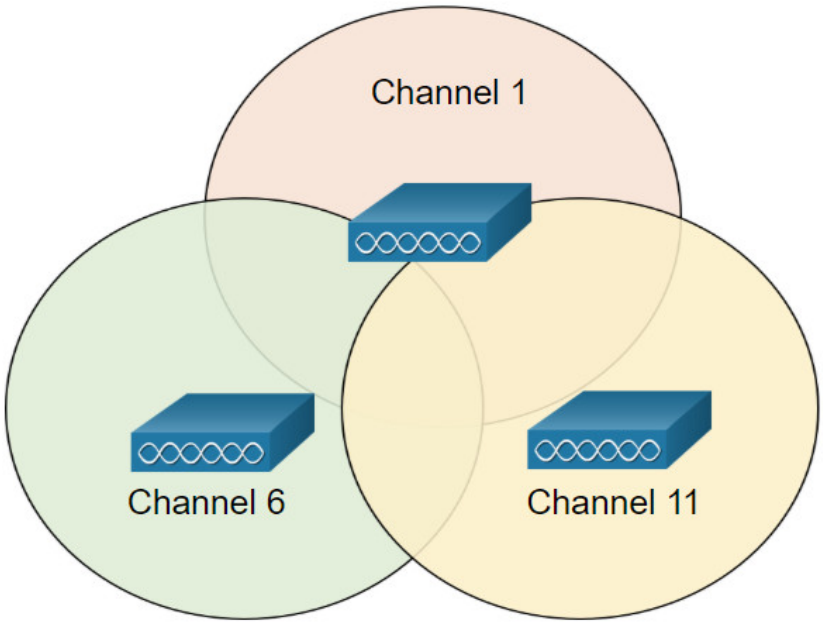
Note: Search the internet for 2.4 GHz channels to learn more about the variations for different countries.

2.4GHz Overlapping Channels in North America



Interference occurs when one signal overlaps a channel reserved for another signal, causing possible distortion. The best practice for 2.4GHz WLANs that require multiple APs is to use non-overlapping channels, although most modern APs will do this automatically. If there are three adjacent APs, use channels 1, 6, and 11, as shown in the figure.

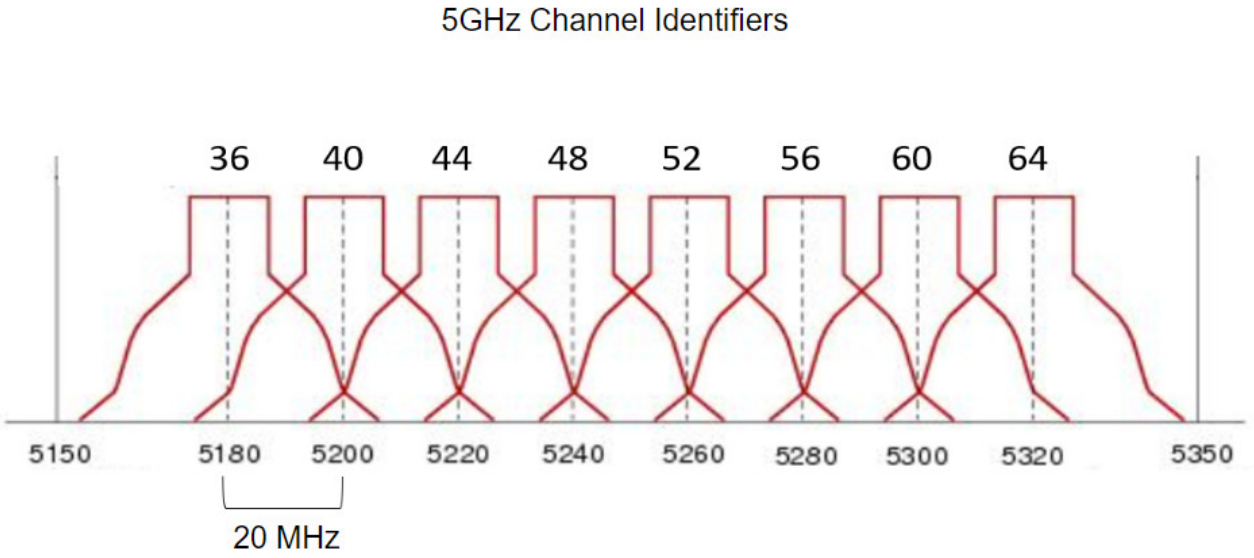
2.4GHz Non-Overlapping Channels for 802.11b/g/n



For the 5GHz standards 802.11a/n/ac, there are 24 channels. The 5GHz band is divided into three sections. Each channel is separated from the next channel by 20 MHz. The figure shows the first section of eight channels for the 5GHz band. Although there is a slight overlap, the channels do not interfere with one another. 5GHz wireless can provide faster data transmission for wireless clients in heavily populated wireless networks because of the large amount of non-overlapping wireless channels.

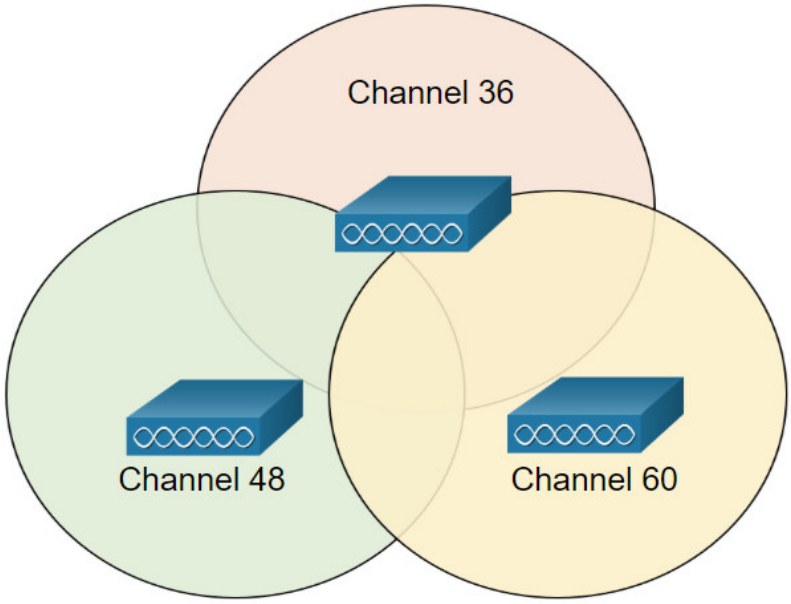
Note: Search the internet for 5GHz channels to learn more about the other 16 channels available and to learn more about the variations for different countries.

5GHz First Eight Non-Interfering Channels



As with 2.4GHz WLANs, choose non-interfering channels when configuring multiple 5GHz APs that are adjacent to each other, as shown in the figure.

5GHz Non-Interfering Channels for 802.11a/n/ac



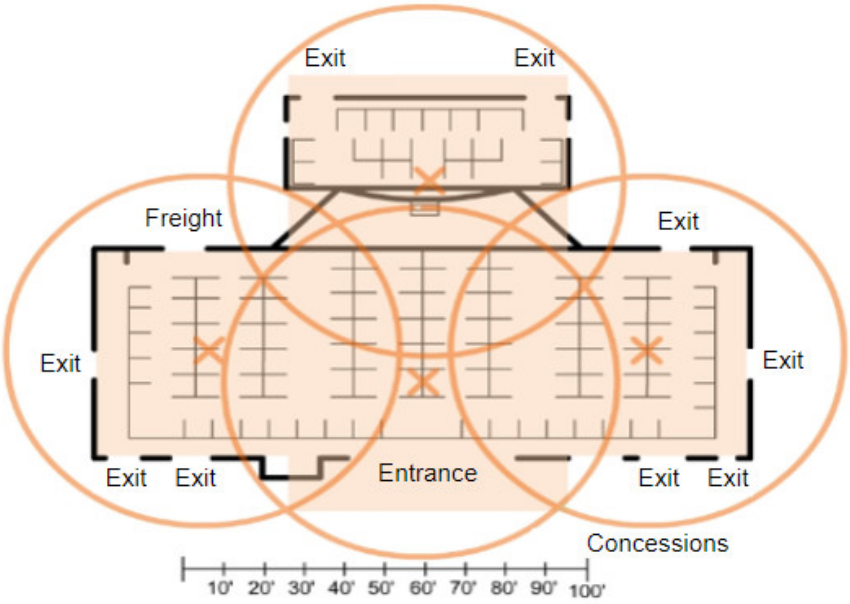
12.5.3 Plan a WLAN Deployment

The number of users supported by a WLAN depends on the geographical layout of the facility, including the number of bodies and devices that can fit in a space, the data rates users expect, the use of non-overlapping channels by multiple APs in an ESS, and transmit power settings.

When planning the location of APs, the approximate circular coverage area is important (as shown in the figure), but there are some additional recommendations:

- If APs are to use existing wiring or if there are locations where APs cannot be placed, note these locations on the map.
- Note all potential sources of interference which can include microwave ovens, wireless video cameras, fluorescent lights, motion detectors, or any other device that uses the 2.4 GHz range.
- Position APs above obstructions.
- Position APs vertically near the ceiling in the center of each coverage area, if possible.
- Position APs in locations where users are expected to be. For example, conference rooms are typically a better location for APs than a hallway.
- If an IEEE 802.11 network has been configured for mixed mode, the wireless clients may experience slower than normal speeds in order to support the older wireless standards.

When estimating the expected coverage area of an AP, realize that this value varies depending on the WLAN standard or mix of standards that are deployed, the nature of the facility, and the transmit power that the AP is configured for. Always consult the specifications for the AP when planning for coverage areas.



12.6 WLAN Threats

12.6.1 Video – WLAN Threats

The previous topics covered the WLAN components and configuration. Here you will learn about WLAN threats.

Click Play to view a video about threats to WLANs.

12.6.2 Wireless Security Overview

A WLAN is open to anyone within range of an AP and the appropriate credentials to associate to it. With a wireless NIC and knowledge of cracking techniques, an attacker may not have to physically enter the workplace to gain access to a WLAN.

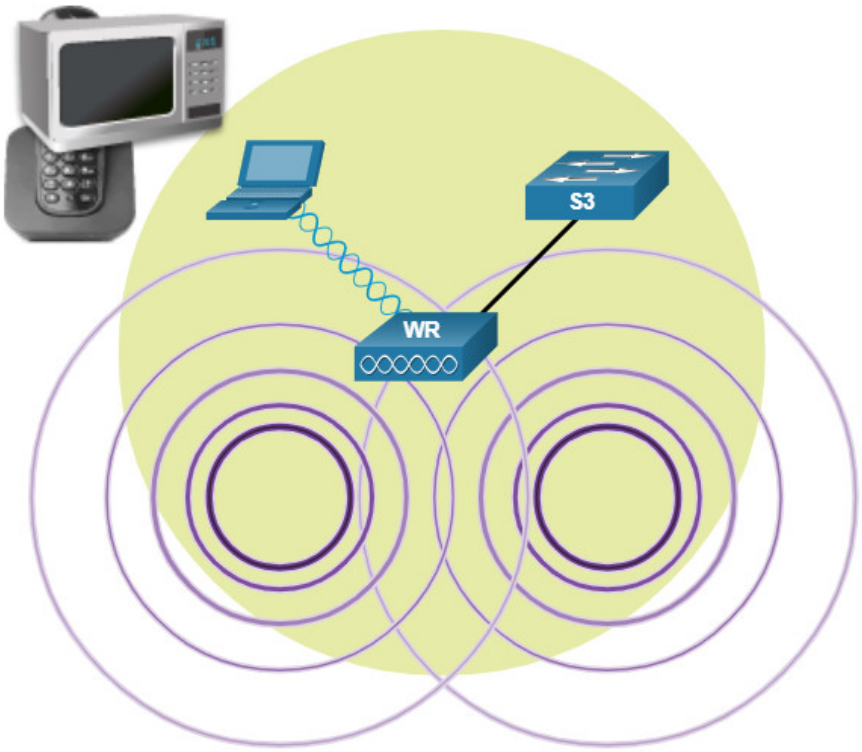
Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including:

- **Interception of data** – Wireless data should be encrypted to prevent it from being read by eavesdroppers.
- **Wireless intruders** – Unauthorized users attempting to access network resources can be deterred through effective authentication techniques.
- **Denial of Service (DoS) Attacks** – Access to WLAN services can be compromised either accidentally or maliciously. Various solutions exist depending on the source of the DoS attack.
- **Rogue APs** – Unauthorized APs installed by a well-intentioned user or for malicious purposes can be detected using management software.

12.6.3 DoS Attacks

Wireless DoS attacks can be the result of:

- **Improperly configured devices** – Configuration errors can disable the WLAN. For instance, an administrator could accidently alter a configuration and disable the network, or an intruder with administrator privileges could intentionally disable a WLAN.
- **A malicious user intentionally interfering with the wireless communication** – Their goal is to disable the wireless network completely or to the point where no legitimate device can access the medium.
- **Accidental interference** – WLANs are prone to interference from other wireless devices including microwave ovens, cordless phones, baby monitors, and more, as shown in the figure. The 2.4 GHz band is more prone to interference than the 5 GHz band.



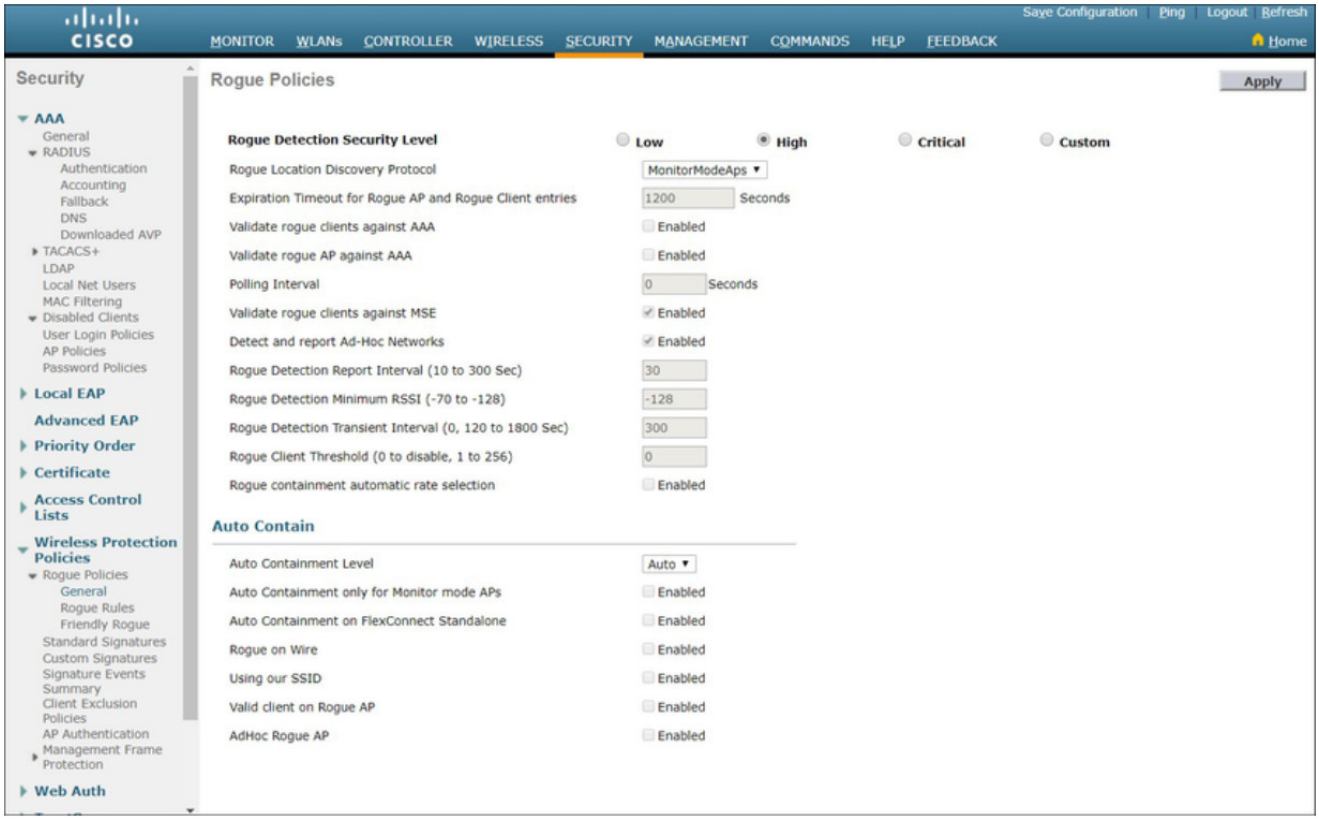
12.6.4 Rogue Access Points

A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy. Anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network resource.

Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.

A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP. Doing so circumvents the security measures and other unauthorized devices can now access network resources as a shared device.

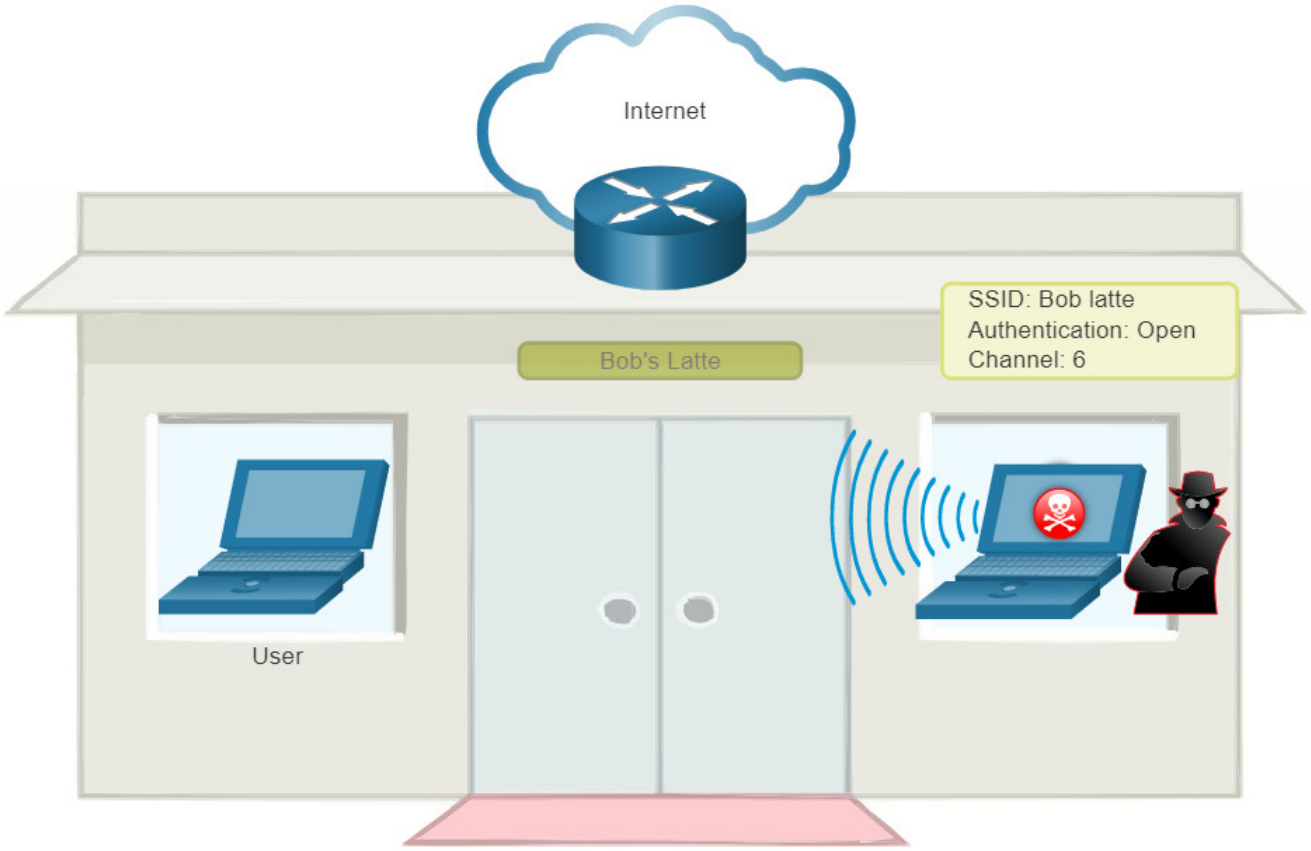
To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies, as shown in the figure, and use monitoring software to actively monitor the radio spectrum for unauthorized APs.



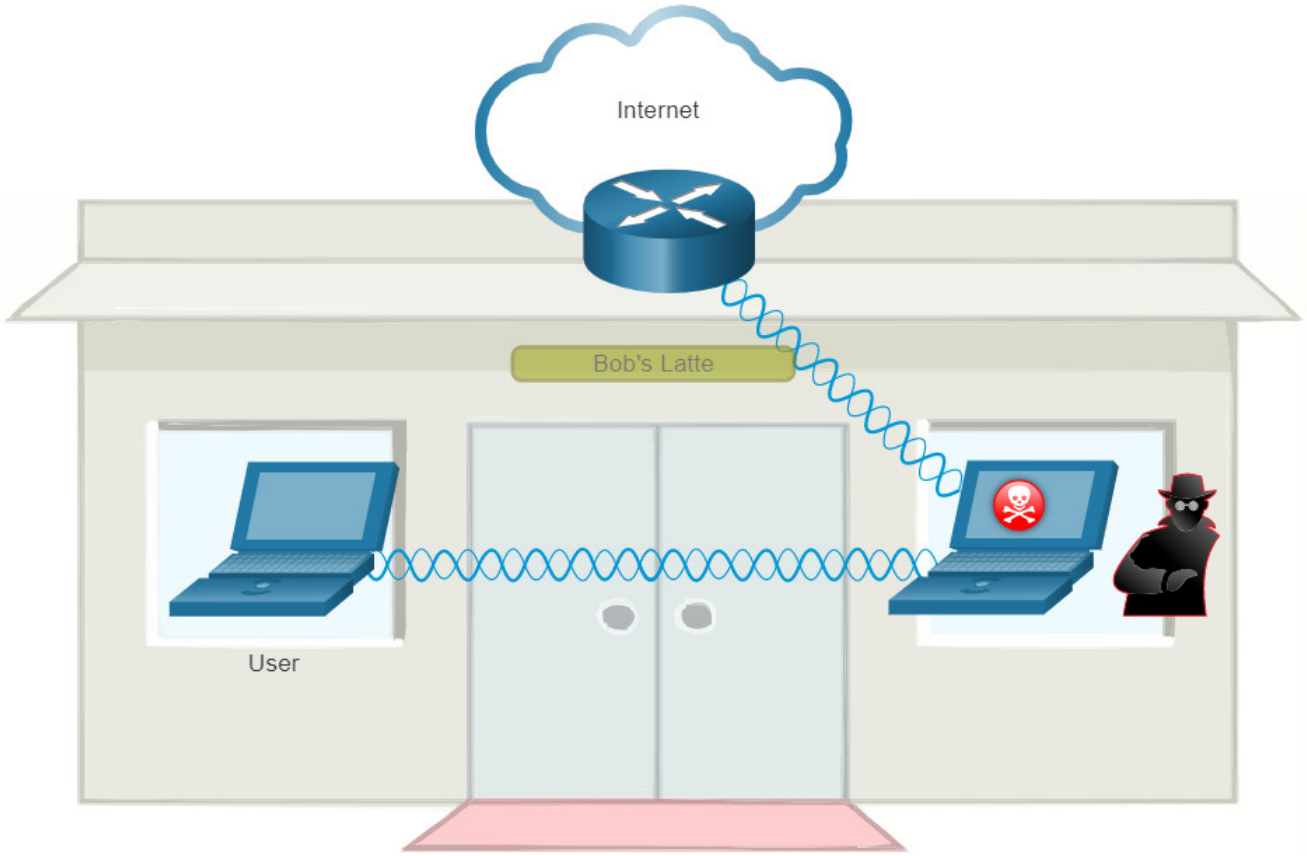
12.6.5 Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. There are many ways in which to create a MITM attack.

A popular wireless MITM attack is called the “evil twin AP” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP, as shown in the figure. Locations offering free Wi-Fi, such as airports, cafes, and restaurants, are particularly popular spots for this type of attack due to the open authentication.



Wireless clients attempting to connect to a WLAN would see two APs with the same SSID offering wireless access. Those near the rogue AP find the stronger signal and most likely associate with it. User traffic is now sent to the rogue AP, which in turn captures the data and forwards it to the legitimate AP, as shown in the figure. Return traffic from the legitimate AP is sent to the rogue AP, captured, and then forwarded to the unsuspecting user. The attacker can steal the user's passwords, personal information, gain access to their device, and compromise the system.



Defeating an attack like an MITM attack depends on the sophistication of the WLAN infrastructure and the vigilance in monitoring activity on the network. The process begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

12.7 Secure WLANs

12.7.1 Video – Secure WLANs

The previous topic explained the WLAN threats. What can you do to secure the WLAN?

Click Play to view a video about techniques for securing WLANs.

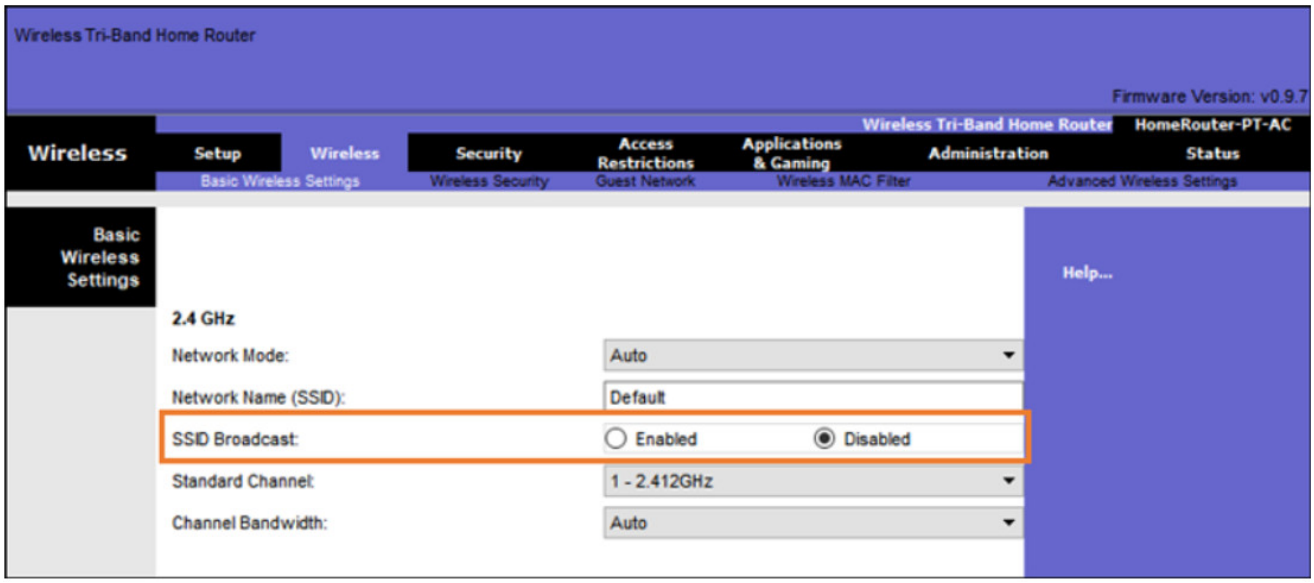
12.7.2 SSID Cloaking and MAC Address Filtering

Wireless signals can travel through solid matter, such as ceilings, floors, walls, outside of the home, or office space. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, even outside.

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs: SSID cloaking and MAC address filtering.

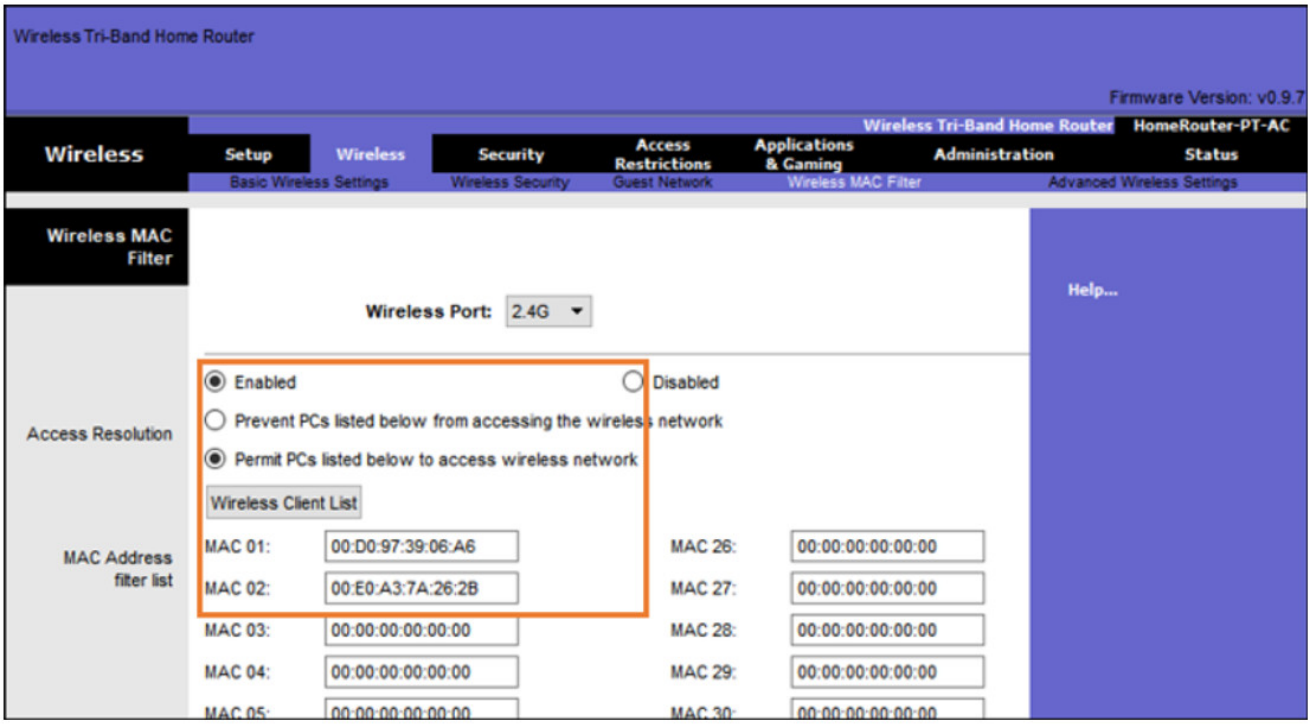
SSID Cloaking

APs and some wireless routers allow the SSID beacon frame to be disabled, as shown in the figure. Wireless clients must manually configure the SSID to connect to the network.



MAC Addresses Filtering

An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.



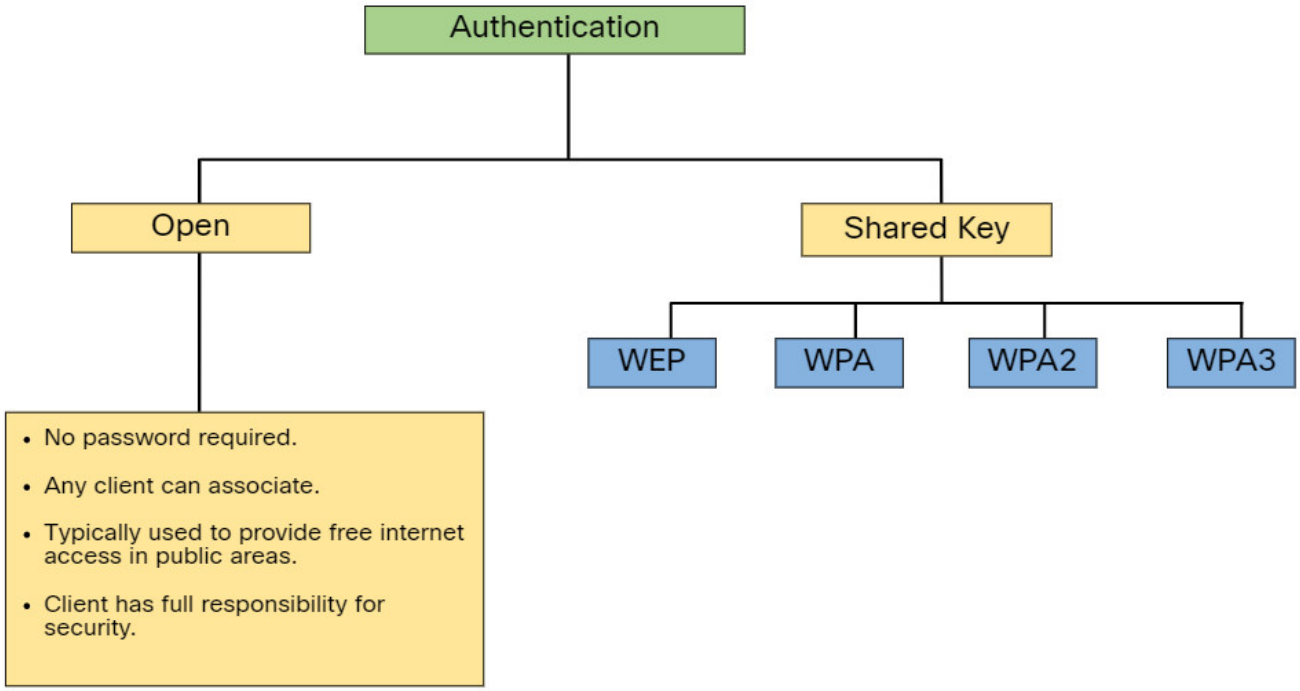
12.7.3. 802.11 Original Authentication Methods

Although these two features would deter most users, the reality is that neither SSID cloaking nor MAC address filtering would deter a crafty intruder. SSIDs are easily discovered even if APs do not broadcast them and MAC addresses can be spoofed. The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

- **Open system authentication** – Any wireless client should easily be able to connect and should only be used in situations where security is of no concern, such as those providing free internet access like cafes, hotels, and in remote areas. The wireless client is responsible for providing security such as using a virtual private network (VPN) to connect securely. VPNs provide authentication and encryption services. VPNs are beyond the scope of this topic.
- **Shared key authentication** – Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

The following chart summarizes these authentication methods.



12.7.4 Shared Key Authentication Methods

There are four shared key authentication techniques available, as described in the table. Until the availability of WPA3 devices becomes ubiquitous, wireless networks should use the WPA2 standard.

Authentication Method	Description

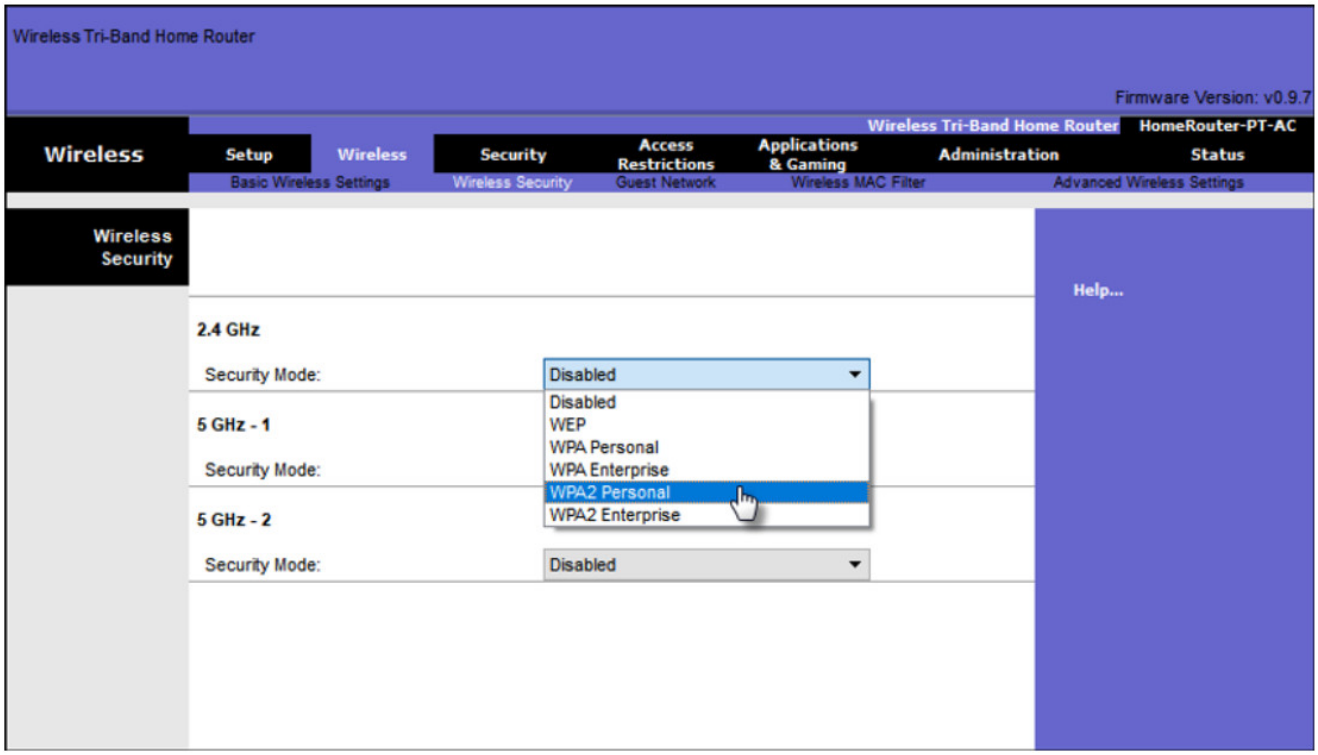
Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. However, the key never changes when exchanging packets. This makes it easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP, but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	WPA2 is the current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

12.7.5 Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. The figure shows the option to select one of two WPA2 authentication methods:

- **Personal** – Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise** – Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

In the figure, the administrator is configuring the wireless router with WPA2 Personal authentication on the 2.4 GHz band.



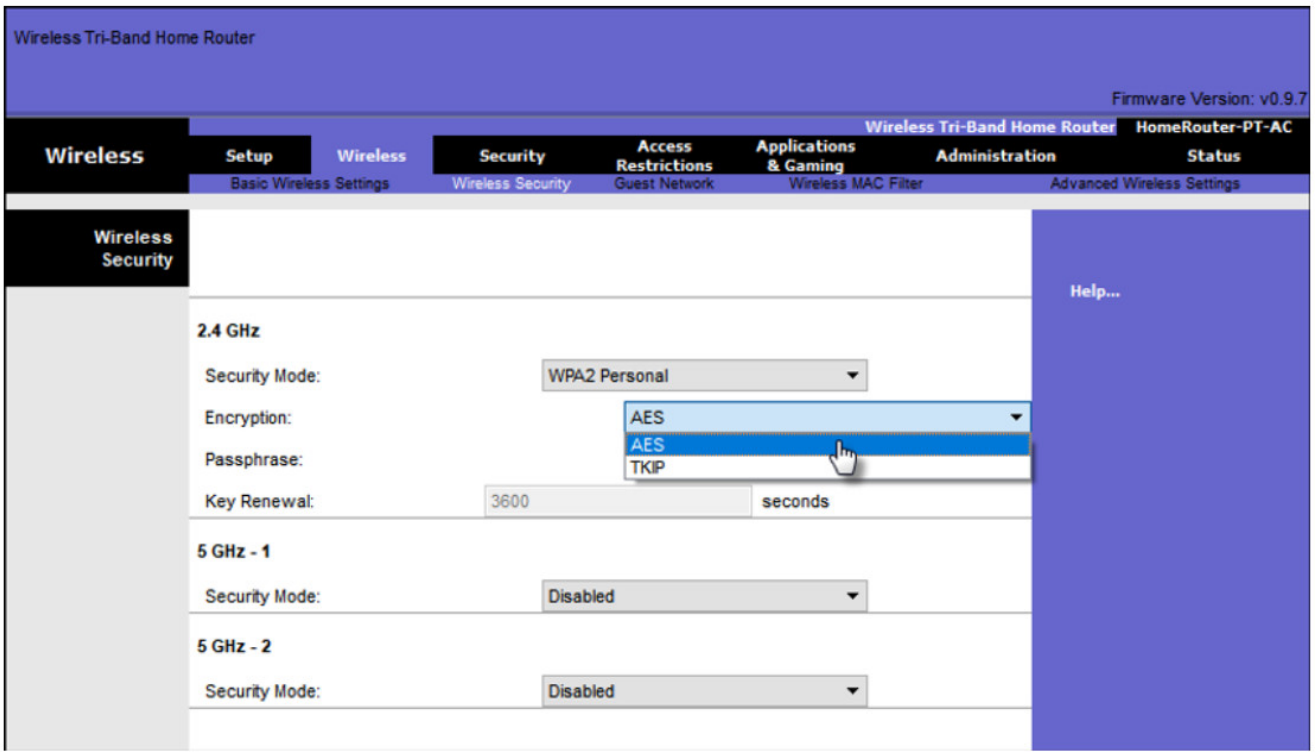
12.7.6 Encryption Methods

Encryption is used to protect data. If an intruder has captured encrypted data, they would not be able to decipher it in any reasonable amount of time.

The WPA and WPA2 standards use the following encryption protocols:

- **Temporal Key Integrity Protocol (TKIP)** – TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Message Integrity Check (MIC) in the encrypted packet to ensure the message has not been altered.
- **Advanced Encryption Standard (AES)** – AES is the encryption method used by WPA2. It is the preferred method because it is a far stronger method of encryption. It uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

In the figure, the administrator is configuring the wireless router to use WPA2 with AES encryption on the 2.4 GHz band.

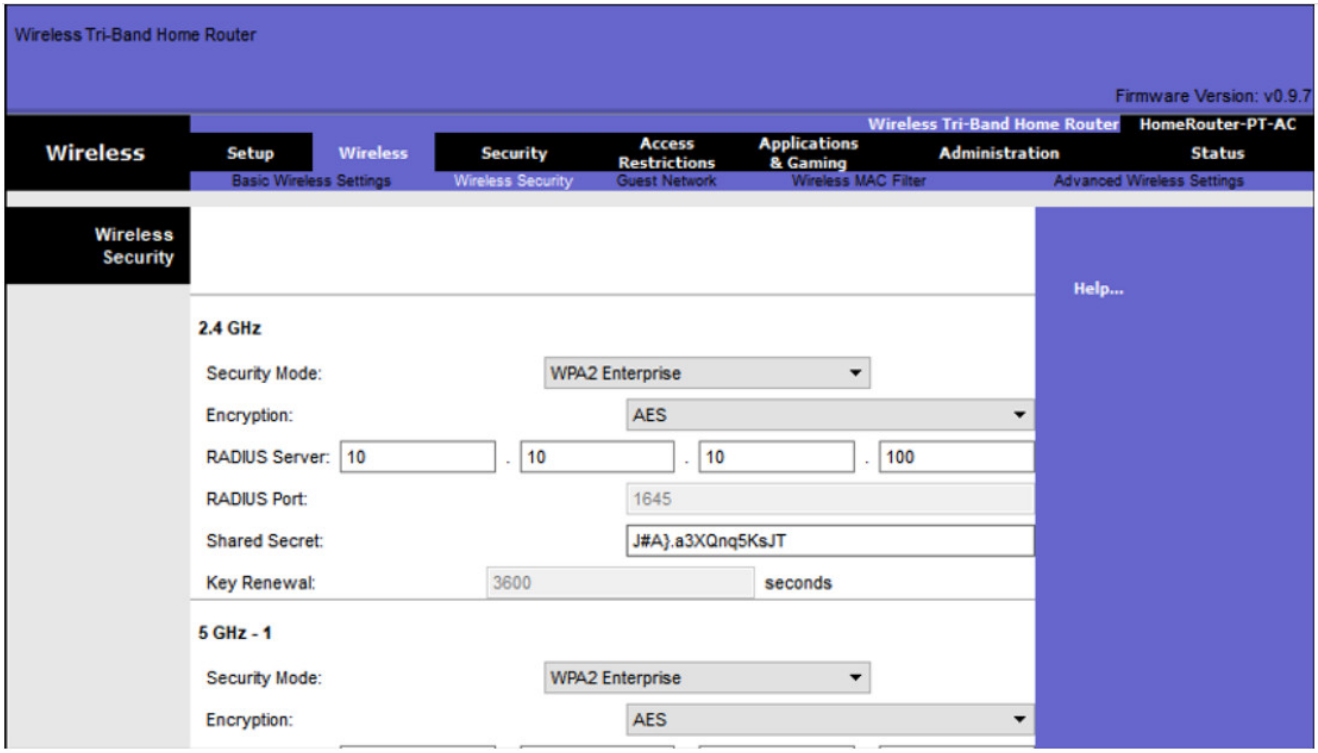


12.7.7 Authentication in the Enterprise

In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients such access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

- **RADIUS Server IP address** – This is the reachable address of the RADIUS server.
- **UDP port numbers** – Officially assigned UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646, as shown in the figure.
- **Shared key** – Used to authenticate the AP with the RADIUS server.

In the figure, the administrator is configuring the wireless router with WPA2 Enterprise authentication using AES encryption. The RADIUS server IPv4 address is configured as well with a strong password to be used between the wireless router and the RADIUS server.



The shared key is not a parameter that must be configured on a wireless client. It is only required on the AP to authenticate with the RADIUS server. User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

The 802.1X login process uses EAP to communicate with the AP and RADIUS server. EAP is a framework for authenticating network access. It can provide a secure authentication mechanism and negotiate a secure private key which can then be used for a wireless encryption session using TKIP or AES encryption.

12.7.8 WPA3

At the time of this writing, devices that support WPA3 authentication were not readily available. However, WPA2 is no longer considered secure. WPA3, if available, is the recommended 802.11 authentication method. WPA3 includes four features:

- WPA3-Personal
- WPA3-Enterprise
- Open Networks
- Internet of Things (IoT) Onboarding

WPA3-Personal

In WPA2-Personal, threat actors can listen in on the “handshake” between a wireless client and the AP and use a brute force attack to try and guess the PSK. WPA3-Personal thwarts this attack by using Simultaneous Authentication of Equals (SAE), a feature specified in the

IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.

WPA3-Enterprise

WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) Suite which is commonly used in high security Wi-Fi networks.

Open Networks

Open networks in WPA2 send user traffic in unauthenticated, clear text. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

IoT Onboarding

Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices without configuring them first, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration, and needed any easy way to get connected to the wireless network. The Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hardcoded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although not strictly part of the WPA3 standard, DPP will replace WPS over time.

12.8 Module Practice and Quiz

12.8.1 What did I learn in this module?

A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments. Wireless networks are based on IEEE standards and can be classified into four main types: WPAN, WLAN, WMAN, and WWAN. Wireless LAN technologies uses the unlicensed radio spectrum to send and receive data. Examples of this technology are Bluetooth, WiMAX, Cellular Broadband, and Satellite Broadband. The IEEE 802.11 WLAN standards define how radio frequencies are used for wireless links. WLAN networks operate in the 2.4 GHz frequency band and the 5 GHz band. Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards are the ITU-R, the IEEE, and the Wi-Fi Alliance.

To communicate wirelessly, most devices include integrated wireless NICs that incorporate a radio transmitter/receiver. The wireless router serves as an access point, a switch, and a router. Wireless clients use their wireless NIC to discover nearby APs advertising their SSID. Clients then attempt to associate and authenticate with an AP. After being authenticated, wireless users have access to network resources. APs can be categorized as either autonomous APs or controller-based APs. There are three types of antennas for business class APs: omnidirectional, directional, and MIMO.

The 802.11 standard identifies two main wireless topology modes: Ad hoc mode and Infrastructure mode. Tethering is used to provide quick wireless access. Infrastructure mode defines two topology building blocks: A Basic Service Set (BSS) and an Extended Service Set (ESS). All 802.11 wireless frames contain the following fields: frame control, duration, address 1, address 2, address 3, sequence control, address 4, payload, and FCS. WLANs use CSMA/CA as the method to determine how and when to send data on the network. Part of the 802.11 process is discovering a WLAN and subsequently connecting to it. Wireless devices discover a wireless AP, authenticate with it, and then associate with it. Wireless clients connect to the AP using a scanning process which may be passive or active.

CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. The CAPWAP split MAC concept does all of the functions normally performed by individual APs and distributes them between two functional components: AP MAC functions and WLC MAC functions. DTLS is a protocol which provides security between the AP and the WLC. FlexConnect is a wireless solution for branch office and remote office deployments. You configure and control access points in a branch office from the corporate office through a WAN link, without deploying a controller in each office. There are two modes of operation for the FlexConnect AP: connected and standalone.

Wireless LAN devices have transmitters and receivers tuned to specific frequencies of radio waves to communicate. Frequencies are allocated as ranges. Ranges are then split into smaller ranges called channels: DSSS, FHSS, and OFDM. The 802.11b/g/n standards operate in the 2.4 GHz to 2.5GHz spectrum. The 2.4 GHz band is subdivided into multiple channels. Each channel is allotted 22 MHz bandwidth and is separated from the next channel by 5 MHz. When planning the location of APs, the approximate circular coverage area is important.

Wireless networks are susceptible to threats, including: data interception, wireless intruders, DoS attacks, and rogue APs. Wireless DoS attacks can be the result of: improperly configured devices, a malicious user intentionally interfering with the wireless communication, and accidental interference. A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization. When connected, a threat actor can use the rogue AP to capture MAC addresses, capture data packets, gain access to network resources, or launch a MITM attack. In a MITM attack, the threat actor is positioned in between two legitimate entities to read or modify the data that passes between the two parties. A popular

wireless MITM attack is called the “evil twin AP” attack, where a threat actor introduces a rogue AP and configures it with the same SSID as a legitimate AP. To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies.

To keep wireless intruders out and protect data, two early security features are still available on most routers and APs: SSID cloaking and MAC address filtering. There are four shared key authentication techniques available: WEP, WPA, WPA2, and WPA3 (Devices with WPA3 are not yet readily available). Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. Encryption is used to protect data. The WPA and WPA2 standards use the following encryption protocols: TKIP and AES. In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

12.8.2 Module Quiz – WLAN Concepts

Download Slide Powerpoint (PPT)

CCNA 2 v7.0 Curriculum: Module 12 - WLAN Concepts.pptx

1 file(s) 4.53 MB

Download

Tags:ccna 2 v7 modules