Module 5: Wireless Network Communication

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Wireless Network Communication

Module Objective: Troubleshoot a wireless network.

Topic Title	Topic Objective
Wireless Communications	Explain how wireless devices enable network communication.
WLAN Threats	Describe threats to WLANs.
Secure WLANs	Troubleshoot a wireless connection.

5.1 Wireless Communications

Video - WLAN Operation

This video will cover the following:

- Infrastructure Mode
- Ad hoc mode
- Tethering
- Basic Service Set (BSS)
- Extended Service Set (ESS)
- 802.11 Frame Structure
- Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)
- Wireless Client and AP Association
- Passive and Active Discovery Mode

Wireless versus Wired LANs

The table summarizes the differences between wireless and wired LANs.

Characteristic	802.11 Wireless LAN	802.3 Wired Ethernet LANs
Physical Layer	radio frequency (RF)	physical cables
Media Access	collision avoidance	collision detection
Availability	anyone with a wireless NIC in range of an access point	physical cable connection required
Signal Interference	yes	minimal
Regulation	different regulations by country	IEEE standard dictates

802.11 Frame Structure

All Layer 2 frames consist of a header, payload, and Frame Check Sequence (FCS) section. The 802.11 frame format is like the Ethernet frame format, except that it contains more fields.

- Frame Control – It identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
- Duration - It is typically used to indicate the remaining duration needed to receive the next frame transmission.
- Address1 - It usually contains the MAC address of the receiving wireless device or AP.
- Address2 - It usually contains the MAC address of the transmitting wireless device or AP.
- Address3 – It sometimes contains the destination MAC address, such as the default gateway to which the AP is attached.
- Sequence Control - It contains information to control sequencing and fragmented frames.
- Address4 - It is usually missing because it is used only in ad hoc mode.
- Payload – It contains the data for transmission.
- FCS - It is used for Layer 2 error control.

CSMA/CA

WLANs are half-duplex, shared media configurations. 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 CSMA/CA as the method to determine how and when to send data on the network. A wireless client does the following:

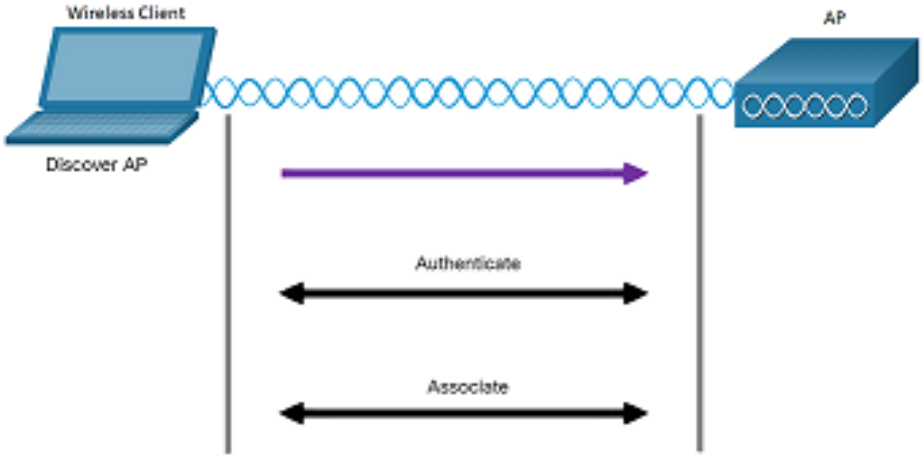
1. Listens to the channel (carrier) to see if it senses no other traffic on the channel (idle).
2. Sends a ready to send (RTS) message to the AP to request dedicated access to the network.
3. Receives a clear to send (CTS) message from the AP granting access to send.
4. If the wireless client does not receive a CTS message, it waits a random amount of time to restart 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.

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:

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



Wireless Client and AP Association (Cont.)

A wireless client and an AP must agree on specific parameters that must be configured on the AP and subsequently on the client to enable the negotiation of a successful association.

- SSID – It appears in the list of available wireless networks on a client.
- Password - It is required from the wireless client to authenticate to the AP.
- Network mode - It refers to the 802.11a/b/g/n/ac/ad WLAN standards.
- Security mode – It refers to the security parameter settings, such as WEP, WPA, or WPA2.
- Channel settings – It refers to the frequency bands used to transmit wireless data.

Passive and Active Discover Mode

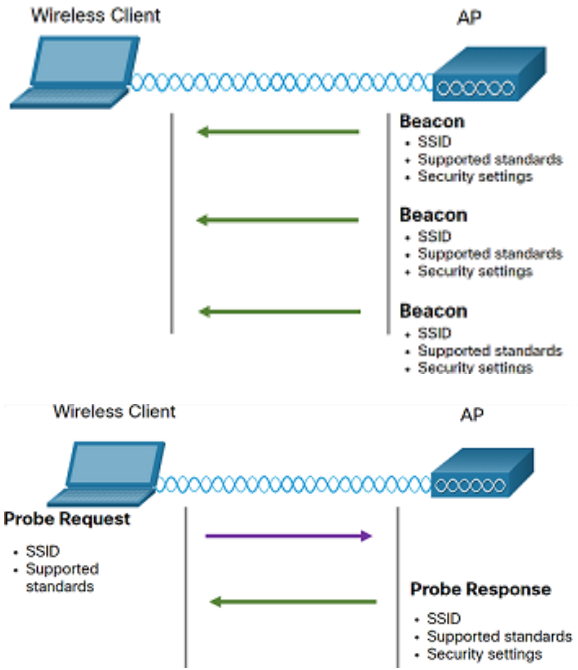
Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process. This process can be passive or active.

Passive mode

- The AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.

Active mode

- Wireless clients must know the name of the SSID and initiate the process by broadcasting a probe request frame on multiple channels.
- APs configured with the SSID will send a probe response that includes the SSID, supported standards, and security settings.



Wireless Devices - AP, LWAP, and WLC

- Home and small business wireless routers integrate the functions of a router, switch, and access point into one device.
- All the control and management functions of the APs on a network can be centralized into a Wireless LAN Controller (WLC).
- When using a WLC, the APs no longer act autonomously, but instead act as lightweight APs (LWAPs).
- LWAPs only forward data between the wireless LAN and the WLC.
- A Major benefit of centralizing the AP management functions in the WLC is simplified configuration and monitoring of numerous access points.

5.2 WLAN Threats

Video - WLAN Threats

This video will cover the following:

- Interception of Data
- Wireless Intruders
- Denial of Service (DoS) Attacks
- Rogue APs

Wireless Security Overview

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.

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.
- Rogue APs - Unauthorized APs installed by a well-intentioned user or for malicious purposes can be detected using management software.

DoS Attacks

Wireless DoS attacks can be the result of:

- Improperly configured devices - Configuration errors can disable the 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 (microwave ovens, cordless phones, baby monitors). The 2.4 GHz band is more prone to interference than the 5 GHz band.

To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

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 an inexpensive wireless router that can potentially allow access to a secure network resource.

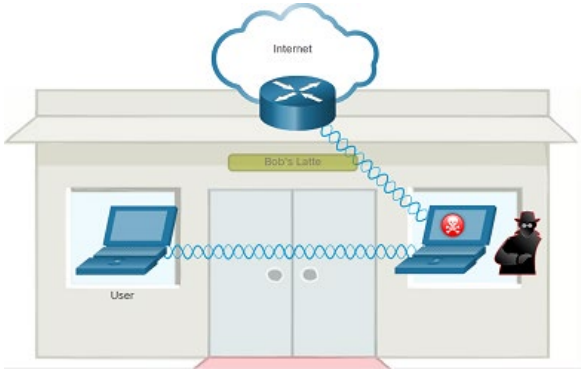
The connected rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.

A personal network hotspot could also be used as a rogue AP.

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

Man-in-the-Middle Attack

- The hacker is positioned in between two legitimate entities to read or modify the data that passes between the two parties.
- "Evil twin AP" attack: an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.
- Wireless clients attempting to connect to a WLAN see two APs 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 that captures the data and forwards it to the legitimate AP.
- Return traffic from the legitimate AP is sent to the rogue AP, captured, and forwarded to the unsuspecting user.



5.3 Secure WLANs

Video - Secure WLANs

This video will cover the following:

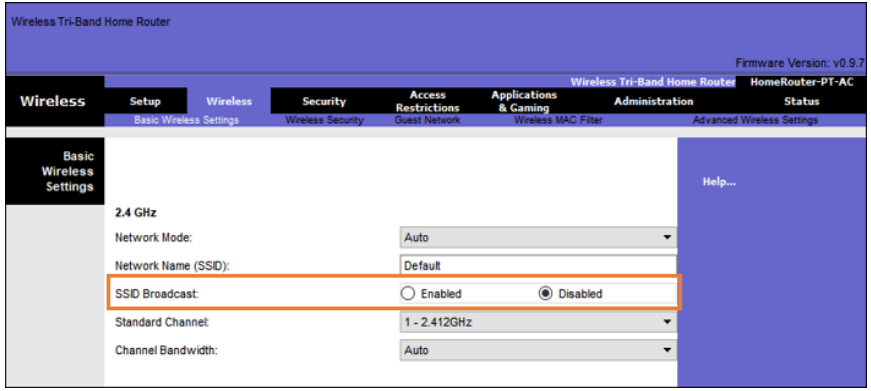
- SSID Cloaking
- MAC Address Filtering
- Authentication and Encryption Systems (Open Authentication and Shared Key Authentication)

SSID Cloaking and MAC Address Filtering

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

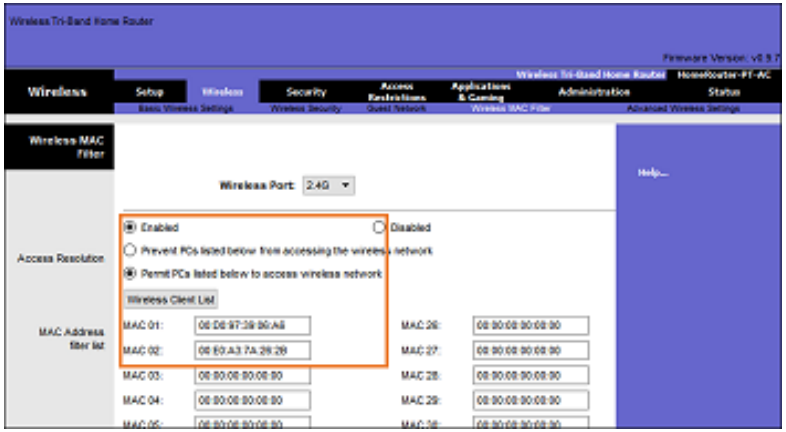
- APs and some wireless routers allow the SSID beacon frame to be disabled.
- Wireless clients must manually configure the SSID to connect to the network.



SSID Cloaking and MAC Address Filtering (Cont.)

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.



802.11 Original Authentication Methods

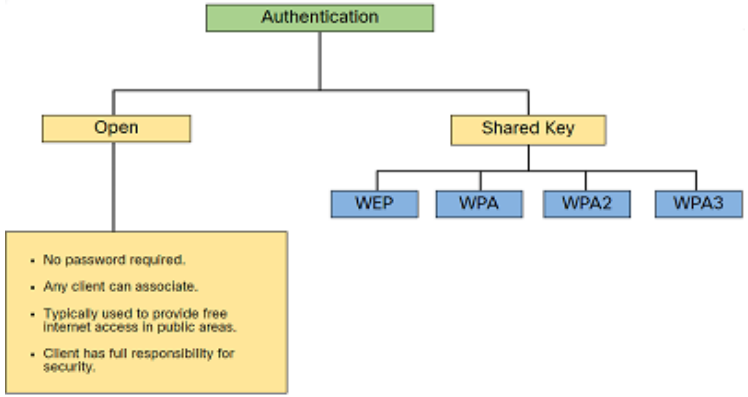
SSIDs are easily discovered even if APs do not broadcast them, and MAC addresses can be spoofed.

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 can easily connect and should only be used when security is of no concern.

- Shared key authentication - Provides mechanisms (WEP, WPA, WPA2, and WPA3) to authenticate and encrypt data between a wireless client and AP.



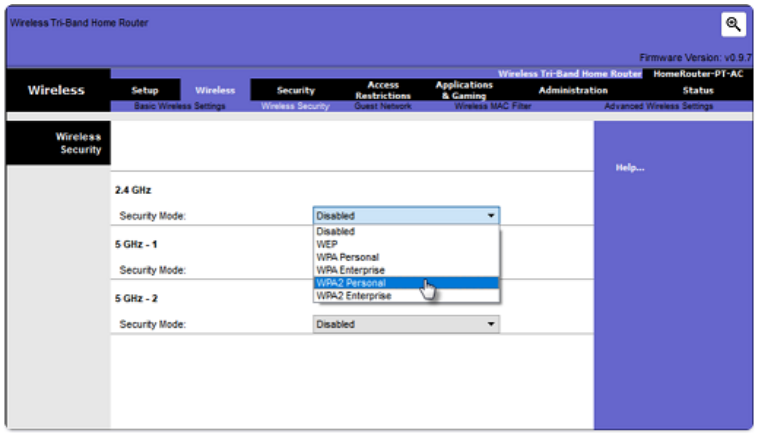
Shared Key Authentication Methods

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

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, 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.

Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2 (stronger). Two WPA2 authentication methods are:



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.

Enterprise

- Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server.

- The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard Extensible Authentication Protocol (EAP).

Encryption Methods

The WPA and WPA2 standards use the following encryption protocols:

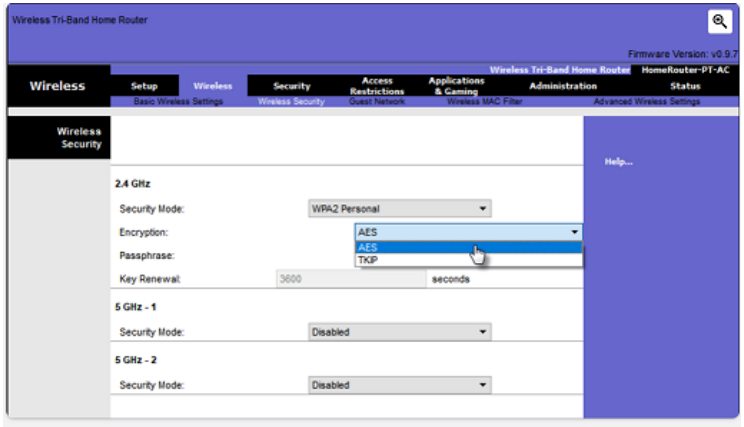
Temporal Key Integrity Protocol (TKIP)

- It is used by WPA and provides support for legacy WLAN equipment by addressing the original flaws associated with WEP encryption.

Advanced Encryption Standard (AES)

- It is used by WPA2 and the preferred method because it is a far stronger method of encryption.

- It uses 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.

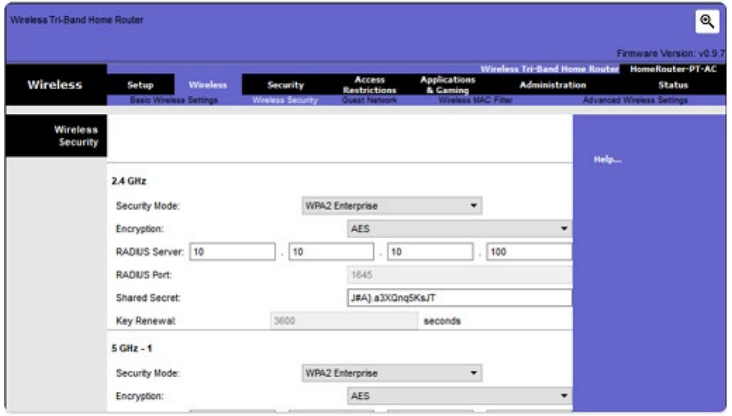


Authentication in the Enterprise

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: 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.
- Shared key - Used to authenticate the AP with the RADIUS server.



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

Packet Tracer - Configure Basic Wireless Security

In this Packet Tracer, you will do the following:

Configure Basic Wireless Security using WPA2 Personal.

- Verify connectivity.
- Configure basic wireless security.
- Update the wireless settings on Laptop.
- Verify connectivity.

Packet Tracer - Troubleshoot a Wireless Connection

In this Packet Tracer, you will do the following:

- Troubleshoot a wireless connection.
- Identify faults in a wireless network.
- Correct misconfigured devices in a wireless network.

5.4 Wireless Network Communication Summary

What Did I Learn in this Module?

- Wireless networking devices connect to an AP or wireless router using the 802.11 frame format that is like the Ethernet frame format but with additional fields.
- WLAN devices use the CSMA/CA method to determine how and when to send data on the network.
- APs can be configured autonomously (individually) or by using a WLC to simplify the configuration and monitoring of numerous access points.
- Wireless networks are susceptible to threats, including data interception, wireless intruders, DoS attacks, and rogue APs.
- A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization.
- In an MiTM attack, the threat actor is positioned between two legitimate entities to read or modify the data that passes between the two parties.
- There are four shared key authentication techniques available: WEP, WPA, WPA2, and WPA3.
- Home routers typically have two choices for authentication: WPA and WPA2 (stronger).