Chapter 10 Wireless Network Attacks and Defenses

Wireless Attacks

- The most common wireless technologies include the following:
  - Cellular
  - Bluetooth
  - Near Field Communication (NFC)
  - Radio frequency identification
  - Wireless local area networks

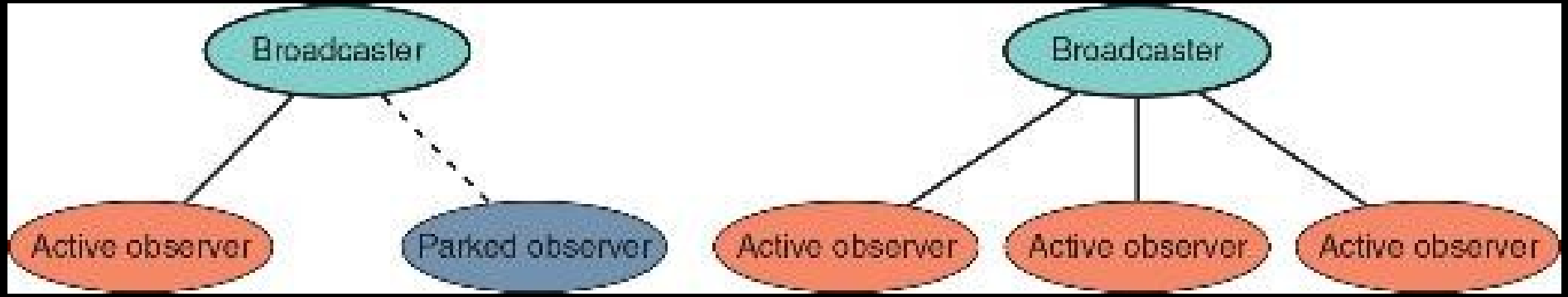
Cellular Networks

- **Cellular networks** are operated by telecommunication service providers and are the most widespread wireless networks
- Faster 5G cellular service has allowed service providers to offer fixed wireless service for Internet connectivity
- Telecommunication service providers own, maintain, and manage their own network equipment and facilities
  - End users are not responsible for configuring or securing these cellular networks

Bluetooth Attacks

- **Bluetooth** is a wireless technology that uses short-range radio frequency (RF) transmissions for communications over short distances
- The primary type of Bluetooth network topology is a piconet
  - It is established when two Bluetooth devices come within range of each other
  - One device (leader) controls all wireless traffic
  - The other device (follower) takes commands
    - Active followers are sending transmissions
    - Parked followers are connected but not actively participating

Bluetooth Piconets



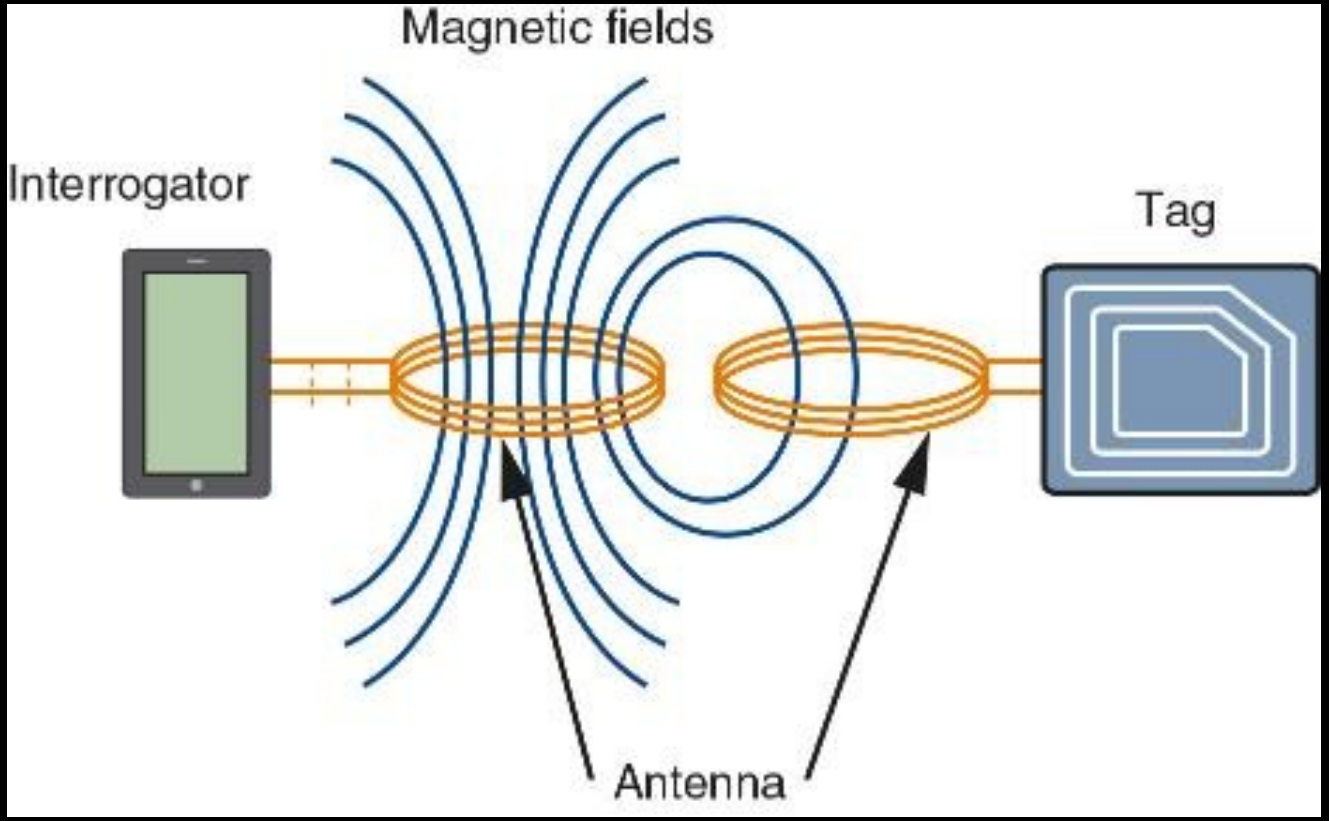
Bluetooth Attacks

- **Bluejacking** is an attack that sends unsolicited messages to Bluetooth-enabled devices
  - Usually involves sending text messages, images, or sounds
- Bluejacking is considered more annoying than harmful because no data is stolen
- **Bluesnarfing** is an attack that accesses unauthorized information from a wireless device through a Bluetooth connection
  - The attacker copies e-mails, contacts, pictures, or other data by connecting to the Bluetooth device without owner's knowledge

Near Field Communication Attacks

- **Near field communication** (**NFC**) is a set of standards used to establish communication between devices in close proximity
  - Once devices are brought within 4 cm of each other or tapped together, two-way communication is established
- Devices using NFC can be active or passive
  - A passive NFC device contains information that other devices can read but does not read or receive any information (example, NFC tag)
  - An active NFC device can read information as well as transmit data

NFC Magnetic Induction



Near Field Communication Attacks

Vulnerability	Explanation	Defense
Eavesdropping	Unencrypted NFC communication between the device and terminal can be intercepted and viewed.	Because an attacker must be extremely close to pick up the signal, users should remain aware of their surroundings while making a payment.
Data theft	Attackers can “bump” a portable reader to a user’s smartphone in a crowd to make an NFC connection and steal payment information stored on the phone.	This can be prevented by turning off NFC while in a large crowd.
Man-in-the-middle attack	An attacker can intercept the NFC communications between devices and forge a fictitious response.	Devices can be configured in pairing so one device can only send while the other can only receive.
Device theft	The theft of a smartphone could allow an attacker to use that phone for purchases.	Smartphones should be protected with passwords or strong PINs.

Radio Frequency Identification Attacks

- **Radio frequency identification** (**RFID**) is commonly used to transmit information between employee identification badges, inventory tags, book labels, and other paper-based tags that can be detected by a proximity reader
- Most RFID tags are passive because they do not have their own power supply
  - Because they do not require a power supply, they can be very small
- RFID tags are susceptible to attacks such as unauthorized tag access, fake tags, eavesdropping, and RFID cloning

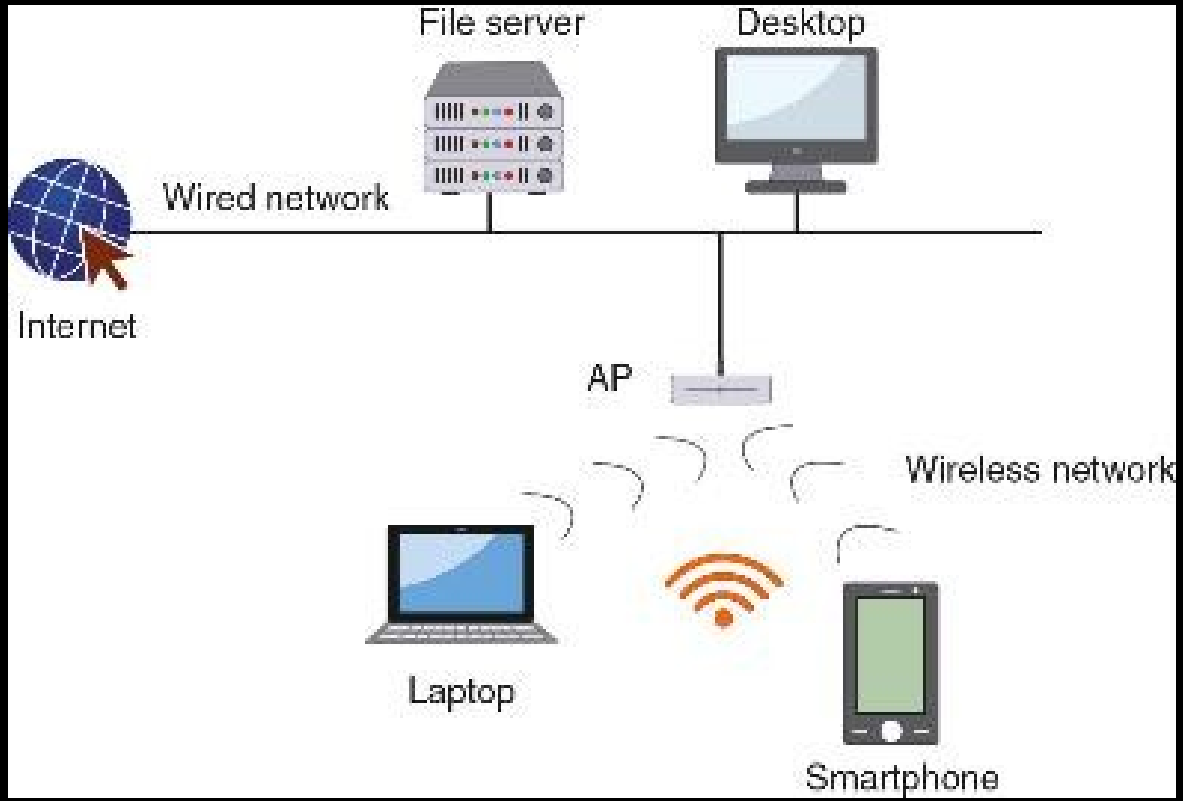
Wireless Local Area Network Attacks

- A wireless local area network (WLAN) is designed to replace or supplement a wired local area network
- It is important to know the following:
  - The different versions of Wi-Fi
  - The hardware necessary for a wireless network
  - The different types of WLAN attacks directed at both the enterprise and consumers

Wireless Local Area Network Attacks

- A wireless client network interface card (**wireless adapter**) performs the same functions as a wired adapter
  - An antenna sends and receives signals through airwaves
- An **access point** (**AP**) is a centrally located WLAN connection device that can send and receive wireless signals
  - It acts as “base station” for the wireless network
  - An AP acts as a bridge between wireless and wired networks because it can connect to a wired network by a cable

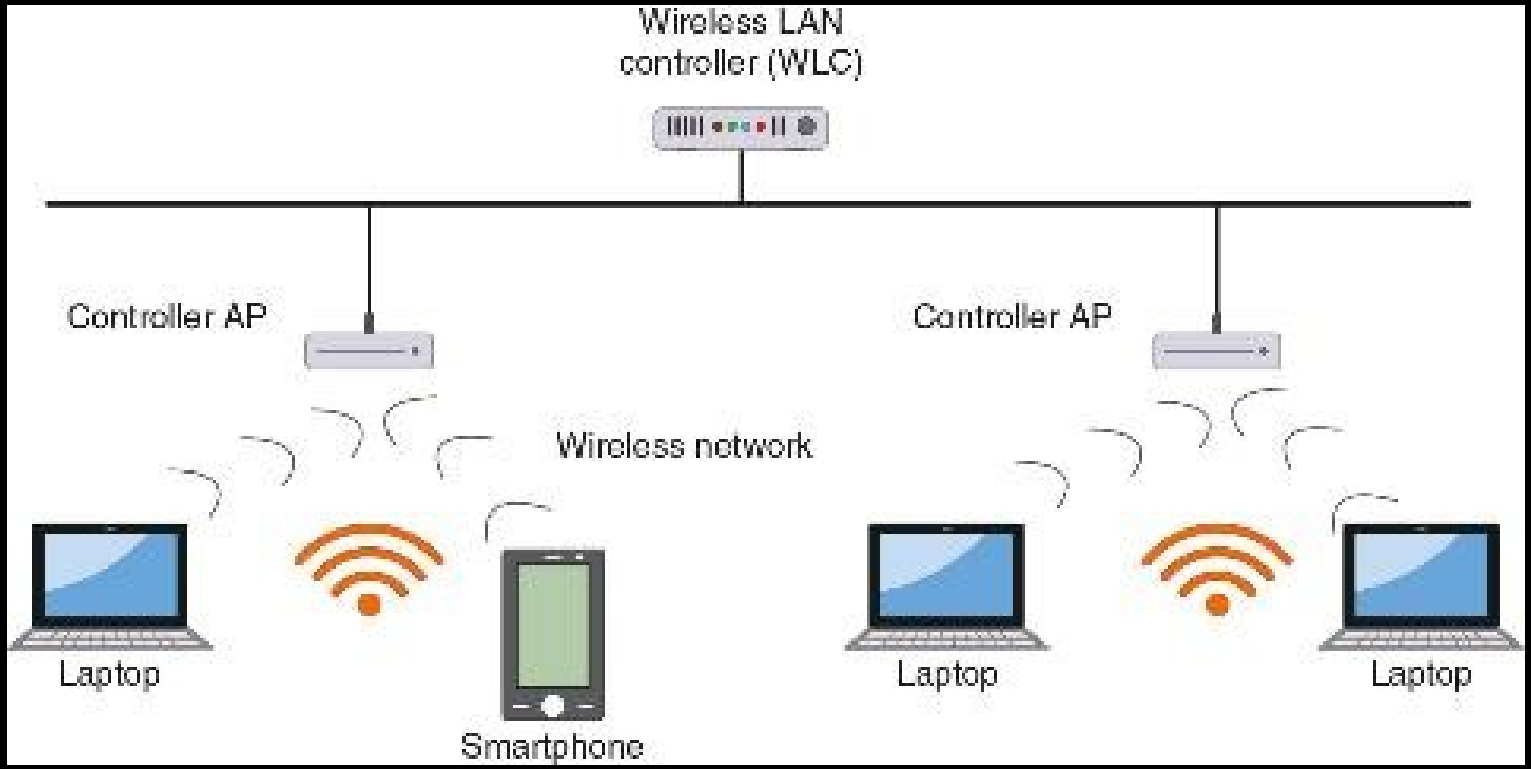
WLAN Setup


File server
Desktop
Wired network
Internet
AP
Wireless network
Laptop
Smartphone

Wireless Local Area Network Attacks

- Autonomous APs can manage wireless authentication, encryption, and other functions for wireless client devices
  - These APs are sometimes called “fat APs”
- APs that do not contain management and configuration functions are called “thin APs”
- **Controller APs** can be managed through a dedicated wireless LAN controller (WLC)
- A **captive portal AP** uses a standard web browser to provide information and allows the user to agree to a policy or present valid login credentials

Controller APs with WLC



WLAN Enterprise Attacks

- In a network, a well-defined boundary or “hard edge” protects data and resources
  - There are two types of hard edges: a network hard edge and a second is made up of the walls and buildings that house the enterprise
- The introduction of WLANs in enterprises has changed hard edges to “blurred edges”
- There are several types of wireless attacks that can be directed at the enterprise

WLAN Enterprise Attacks

- A **rogue AP** is an unauthorized access point that allows an attacker to bypass network security configurations
  - It is usually set up by an insider (employee)
  - It may be set up behind a firewall, opening the network to attacks
- An **evil twin** is an AP set up by an attacker
  - It attempts to mimic an authorized AP
  - Attackers capture transmissions from users to the evil twin AP

WLAN Enterprise Attacks

- Intercepting Wireless Data
  - An attacker can pick up the RF signal from an open or misconfigured AP
- Wireless Denial Attacks
  - **RF jamming** occurs when attackers use intentional RF interference to flood the RF spectrum with enough interference to prevent a device from communicating with the AP
  - An attacker can create false deauthentication or disassociation management frames that appear to come from another device, causing the client to disconnect from the AP (called a **disassociation attack**)

WLAN Enterprise Attacks

- Wireless Consumer Attacks
  - Most home users fail to configure any security on their home networks
  - Attackers can:
    - Steal data
    - Read wireless transmissions
    - Inject malware
    - Download harmful content

Question

- Jenny is investigating a security incident in which the smartphone of the CEO was compromised and confidential data was stolen. She suspects that it was an attack that used Bluetooth. Which attack would this be?

Answer

- Jenny is investigating a security incident in which the smartphone of the CEO was compromised and confidential data was stolen. She suspects that it was an attack that used Bluetooth. Which attack would this be?
- Bluesnarfing is an attack that accesses unauthorized information from a wireless device through a Bluetooth connection. In a bluesnarfing attack, the attacker copies emails, calendars, contact lists, cell phone pictures, or videos by connecting to the Bluetooth device without the owner’s knowledge or permission.

Wired Equivalent Privacy (WEP)

- **Wired Equivalent Privacy** (**WEP**) is an IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmissions
  - WEP encrypts the transmission
- A secret key is shared between the wireless client device and AP
- WEP vulnerabilities include the following:
  - WEP can use only a 64-bit or 128-bit number to encrypt
  - WEP violates the cardinal rule of cryptography: avoid a detectable pattern

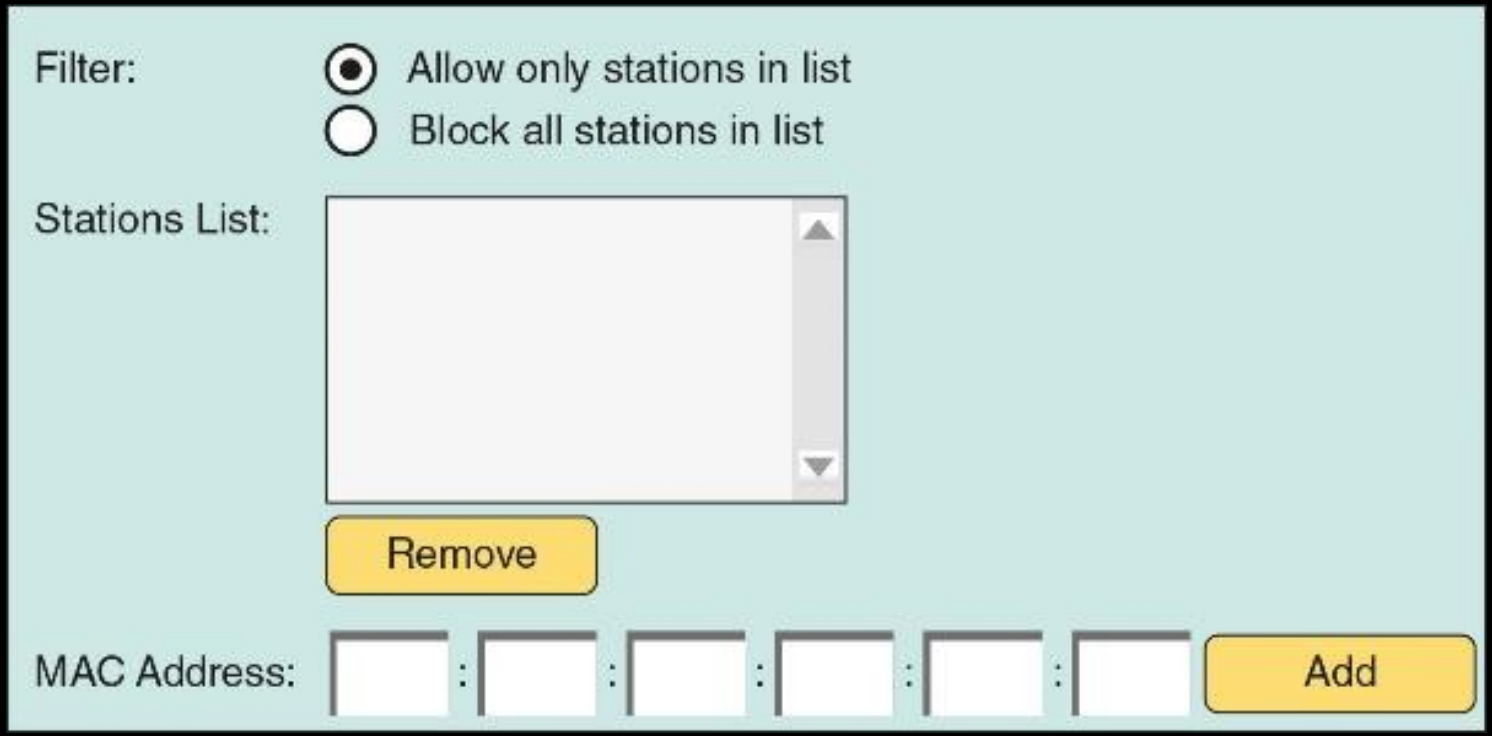
Wi-Fi Protected Setup (WPS)

- **Wi-Fi Protected Setup** (**WPS**) **–** two common methods include the following:
  - The PIN method utilizes a PIN printed on a sticker of the wireless router or displayed through a software wizard
  - The push-button method is where a user pushes buttons and the security configuration takes place
- Design and implementation flaws include the following:
  - There is no lockout limit for entering PINs, the last PIN character is only a checksum, and the wireless router reports the validity of the first and second halves of the PIN separately

MAC Address Filtering

- **Media Access Control (MAC)** address filtering is the most common type of wireless access control
  - It permits or blocks device based on MAC address
- Vulnerabilities of MAC address filtering include the following:
  - MAC addresses are initially exchanged in an unencrypted format
    - Attackers can see addresses of approved devices and substitute it on their own device
  - Managing a large number of addresses is challenging

MAC Address Filtering



Wi-Fi Protected Access (WPA)

- **Wi-Fi Protected Access** (**WPA**) was introduced by the Wi-Fi Alliance to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements
- There are two modes of WPA:
  - WPA Personal
  - WPA Enterprise
- WPA addresses both encryption and authentication

Wi-Fi Protected Access (WPA)

- Authentication for WPA Personal is accomplished using a preshared key (PSK)
  - In a WLAN, a PSK is a secret value that is manually entered on both the AP and each wireless device
  - Devices that have the secret key are automatically authenticated by the AP

Question

- What is a vulnerability of MAC address filtering in a WLAN environment?

Answer

- What is a vulnerability of MAC address filtering in a WLAN environment?
- Filtering by MAC address has several vulnerabilities. MAC addresses are initially exchanged between wireless devices and the AP in an unencrypted format. An attacker monitoring the airwaves could easily see the MAC address of an approved device and then substitute it on their own device.

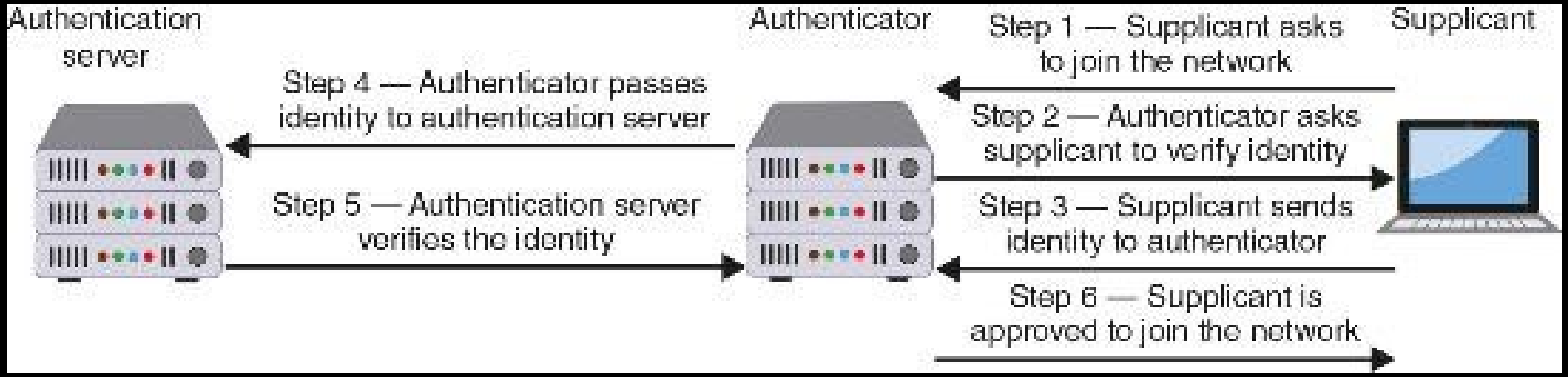
Wi-Fi Protected Access 2 (WPA2)

- **Wi-Fi Protected Access 2** (**WPA2**) is based on final IEEE 802.11i standard
- The following are two modes of WPA2:
  - WPA2-Personal
  - WPA2-Enterprise
- WPA2 addresses two major security areas of WLANs:
  - Encryption
  - Authentication

Wi-Fi Protected Access 2 (WPA2)

- The encryption protocol used for WPA2 is the **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)**
  - It specifies the use of CCM with AES
- The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication
- Authentication for the WPA2-Enterprise model uses the IEEE 802.1x standard
- This standard provides greater degree of security by implementing port-based authentication

IEEE 802.1x Process



Wi-Fi Protected Access 2 (WPA2)

- **Extensible Authentication Protocol** (**EAP**) is a framework for transporting authentication protocols
- EAP defines message format and uses four types of packets
  - Request, Response, Success, and Failure
- A common EAP protocol is **Protected EAP** (**PEAP**)
  - PEAP simplifies deployment of 802.1x by using Microsoft Windows logins and passwords
  - It creates encrypted channel between client and authentication server

Wi-Fi Protected Access 2 (WPA2)

EAP name	Description
EAP-TLS	Uses digital certificates for authentication
EAP-TTLS	Security tunnels client password authentication within Transport Layer Security (TLS) records
EAP-FAST	Securely tunnels any credential form for authentication (such as a password or a token) using TLS

Wi-Fi Protected Access 3 (WPA3)

- The next generation of Wi-Fi Protected Access (WPA) is known as **WPA3**
- Security improvements of WPA3 include the following:
  - WPA3 includes **Simultaneous Authentication of Equals (SAE)** which is designed to increase security at the time of the handshake when keys are being exchanged
  - When using open or public Wi-Fi networks, WPA3 applies individual data encryption
  - WPA3 has improved interaction capabilities with Internet of Things (IoT) devices

Additional Wireless Protections

- Important considerations must be taken into account when installing a new WLAN for an organization:
  - All areas of a building should have adequate wireless coverage
  - All employees must have a reasonable amount of bandwidth
  - A minimum amount of wireless signal should “bleed” outside the walls of the building
- A **site survey**, which is an in-depth examination and analysis of a wireless LAN site, should be considered

Additional Wireless Protections

- Some AP configuration settings are designed to limit the spread of the wireless RF signal so that a minimum amount of signal extends past the physical boundaries of the enterprise to be accessible to outsiders
- Signal Strength Settings
  - Some APs allow adjustment of the power level at which the LAN transmits
- Spectrum Selection
  - Some APs provide the ability to adjust frequency spectrum settings, including: frequency band, channel selection, and channel width

Additional Wireless Protections

- Antenna Placement and Type
  - APs should be located near the center of coverage area
  - APs can be secured high on a wall to reduce signal obstructions and theft
  - If possible, the AP and antenna should be positioned so that a minimal amount of signal reaches beyond the security perimeter of the building
    - Another option is to use a type of antenna that focuses its signal in a concentrated direction toward authorized users instead of broadcasting it over a wide area

Rouge AP System Detection

- Identifying rogue APs is known as rogue AP system detection
- There are 4 types of wireless probes that can monitor airwaves for traffic:
  - Wireless device probe
  - Desktop probe
  - Access point probe
  - Dedicated probe
- Once a suspicious signal is detected by a wireless probe:
  - The information is sent to a centralized database where WLAN management system software compares it to a list of approved APs