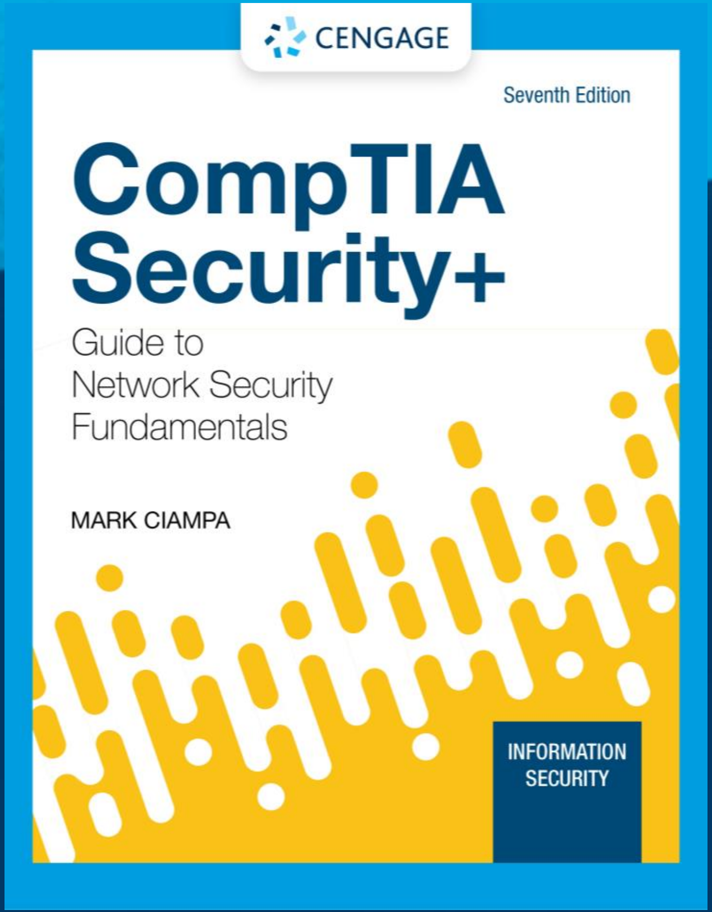

CENGAGE

Seventh Edition

CompTIA Security+

Guide to Network Security Fundamentals

MARK CIAMPA

INFORMATION SECURITY

CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 11: Wireless Network Security

CENGAGE

Module Objectives

By the end of this module, you should be able to:

1. Describe the different types of wireless network attacks
2. List the vulnerabilities of WLAN security
3. Explain the solutions for securing a wireless network

Wireless Attacks

- Several attacks can be directed against wireless data system including:
  - Bluetooth attacks
  - Near Field Communication (NFC) attacks
  - Radio frequency identification systems
  - Wireless local area network attacks

Bluetooth Attacks (1 of 3)

- **Bluetooth** is a wireless technology that uses short-range radio frequency (RF) transmissions
    - It provides rapid device pairings
- Bluetooth is a *personal area network* (*PAN*) technology designed for data 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 Attacks (2 of 3)

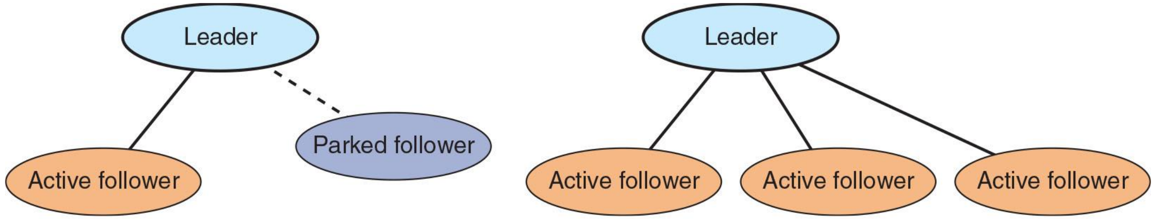


Figure 11-1 Bluetooth piconets

Figure 11-1 Bluetooth piconets

Bluetooth Attacks (3 of 3)

- **Bluejacking** is an attack that sends unsolicited messages to Bluetooth-enabled devices
  - Usually involves 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, or other data by connecting to the Bluetooth device without owner’s knowledge

Near Field Communication (NFC) Attacks (1 of 2)

- **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

Near Field Communication (NFC) Attacks (2 of 2)

- Examples of NFC uses:
  - *Automobile*
  - *Entertainment*
  - *Office*
  - *Retail stores*
  - *Transportation*
- NFC devices are used in *contactless payment systems*
  - A consumer can pay for a purchase by simply tapping a store’s payment terminal with their smartphone

Radio Frequency Identification (RFID) 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
    - 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 different attacks (see Table 11-3 in the text)

Wireless Local Area Network Attacks (1 of 10)

- A *wired local area network* (*WLAN*) is designed to replace or supplement a wired LAN
- It is important to know about the:
  - History and specifications of IEEE WLANs
  - Hardware necessary for a wireless network
  - Different types of WLAN attacks directed at enterprise and home users

Wireless Local Area Network Attacks (2 of 10)

- WLAN Versions
  - Institute of Electrical and Electronics Engineers (IEEE) is the most influential organization for computer networking and wireless communications
  - In 1997, the IEEE released the final draft for a WLAN standard called IEEE 802.11
  - Amendments to this standard include:
    - IEEE 802.11a
    - IEEE 802.11b
    - IEEE 802.11g
    - IEEE 802.11n
    - IEEE 802.11ac
    - IEEE 802.11ax
  - To reduce confusion, the Wi-Fi Alliance adopted “consumer-friendly” version numbers (see Table 11-4)

Wireless Local Area Network Attacks (3 of 10)

IEEE name	Wi-Fi Alliance version	Ratification date	Frequency used	Maximum data rate
802.11	None	1997	2.4 GHz	2 Mbps
802.11b	Wi-Fi 1	1999	2.4 GHz	11 Mbps
802.11a	Wi-Fi 2	1999	5 GHz	54 Mbps
802.11g	Wi-Fi 3	2003	2.4 GHz	54 Mbps
802.11n	Wi-Fi 4	2009	2.4 GHz & 5 GHz	600 Mbps
802.11ac	Wi-Fi 5	2014	5 GHz	7.2 Gbps
802.11ax	Wi-Fi 6	2019	2.4 GHz & 5 GHz & 1-6 GHz	9.6 Gbps

Wireless Local Area Network Attacks (4 of 10)

- WLAN Hardware
  - A wireless client network interface card adapter performs same functions as wired adapter
    - Antenna sends and receives signals through airwaves
  - *Access point* (*AP*) is a centrally located WLAN connection device that can send and receive wireless signals
    - Primarily consists of an antenna and a radio transmitter/receiver
    - Access point (AP) functions
      - Acts as “base station” for wireless network
      - Acts as a bridge between wireless and wired networks because it can connect to a wired network by a cable

Wireless Local Area Network Attacks (5 of 10)

- WLAN Hardware (continued)
  - A WLAN using an AP is operating in *infrastructure mode*
  - Networks that are not using an AP operate in *ad hoc mode*
    - Devices can only communicate between themselves and cannot connect to another network
    - The Wi-Fi Alliance has created a similar technical specification called **Wi-Fi Direct**
  - A *residential WLAN gateway* is used by small offices or home users to connect to the Internet
  - Types of APs include fat vs. thin APs, controller vs. standalone, and captive portal APs

Wireless Local Area Network Attacks (6 of 10)

- WLAN Enterprise Attacks
  - In a network, a well-defined boundary protects data and resources
    - This boundary is known as a “hard edge”
  - There are two types of hard edges:
    - A network hard edge
    - The 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
  - Those attacks will be covered on the following slides

Wireless Local Area Network Attacks (7 of 10)

- **Rogue access** point is an unauthorized access point that allows an attacker to bypass network security configurations
  - Usually set up by an insider (employee)
  - May be set up behind a firewall, opening the network to attacks
- **Evil twin** is an AP set up by an attacker
  - Attempts to mimic an authorized AP
  - Attackers capture transmissions from users to evil twin AP

Wireless Local Area Network Attacks (8 of 10)

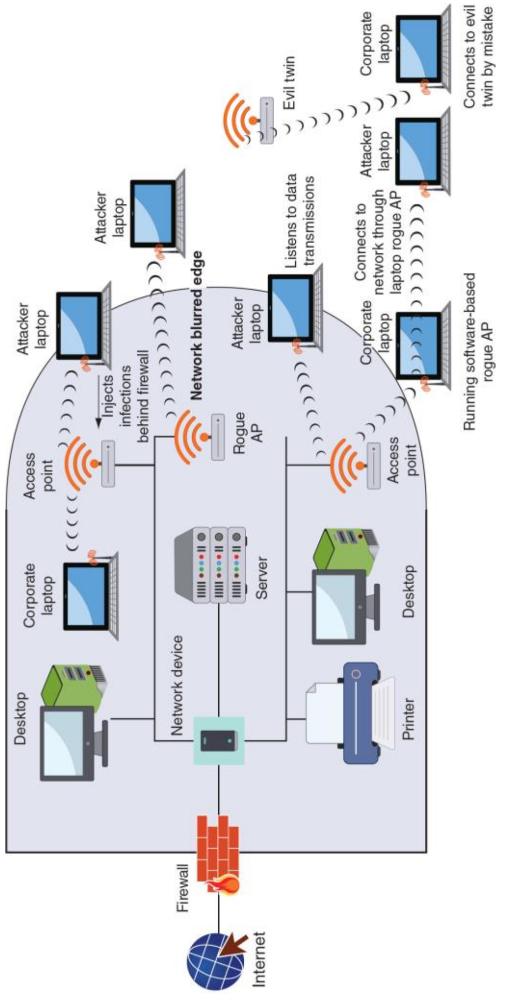


Figure 11-9 Rogue access point and evil twin attacks

Figure 11-9 Rogue access point and evil twin attacks

Wireless Local Area Network Attacks (9 of 10)

- Intercepting Wireless Data
  - An attacker can pick up the RF signal from an open or misconfigured AP
  - Using a WLAN to read this data could yield significant information to an attacker regarding the wired enterprise network
- Wireless Denial of Service Attack
  - **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
  - *Spoofing* occurs when attackers craft a fictitious frame that pretends to come from a trusted client when it actually comes from the attacker
  - Manipulating duration field values occurs when attackers send a frame with the duration field set to a high value, preventing other devices from transmitting for that period of time

Wireless Local Area Network Attacks (10 of 10)

- 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*

Knowledge Check Activity 1

Which wireless technology establishes two-way communication when two devices are brought within 4 cm of each other or tapped together and is often used in contactless payment systems?

a. Bluetooth

b. NFC

c. RFID

d. 802.11ad

Knowledge Check Activity 1: Answer

Which wireless technology establishes two-way communication when two devices are brought within 4 cm of each other or tapped together and is often used in contactless payment systems?

Answer: b. NFC

Near field communication (NFC) is a set of standards used to establish communication between devices in very close proximity (about 4cm). RFID is similar but can work in distances from 10 mm to 6 m. NFC is often used in contactless payment systems.

Vulnerabilities of WLAN Security

- The original IEEE 802.11 committee recognized wireless transmissions could be vulnerable
  - They implemented several wireless security protections in the standard while leaving others to the WLAN vendor’s discretion
  - Several of these protections were vulnerable and led to multiple attacks

Wired Equivalent Privacy

- *Wired Equivalent Privacy* (*WEP*) is an IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmissions
    - Encrypts the transmission
- A secret key is shared between wireless client device and AP
- WEP vulnerabilities include the following:
    - WEP can only use 64-bit or 128-bit number to encrypt
        - *Initialization vector (IV)* is only 24 of those bits
        - Short length makes it easier to break
    - WEP violates the cardinal rule of cryptography: avoid a detectable pattern
        - Attackers can see duplication when IVs start repeating

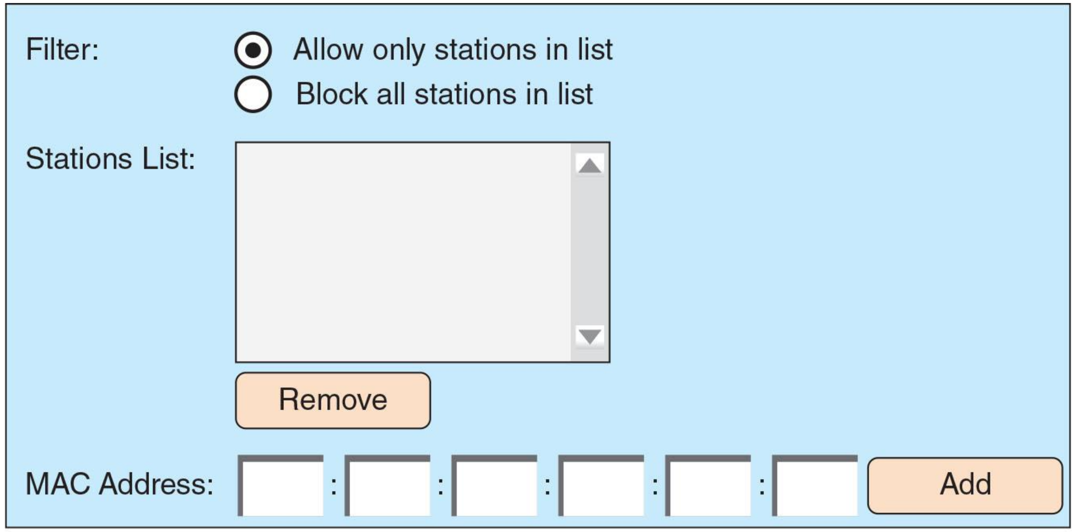
Wi-Fi Protected Setup

- **Wi-Fi Protected Setup** (**WPS**) is an optional means of configuring security on WLANS
- Two common WPS methods include the following:
  - PIN method - utilizes a PIN printed on a sticker of the wireless router or displayed through a software wizard
    - User enters Pin and security configuration automatically occurs
  - Push-button method - user pushes buttons and 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
  - The wireless router reports the validity of the first and second halves of the PIN separately

MAC Address Filtering (1 of 2)

- Wireless access control is intended to limit a user’s admission to the AP
- **Media Access Control (MAC)** address filtering is the most common type of wireless access control
  - It is used by nearly all wireless AP vendors
  - 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 address of approved device and substitute it on his own device
  - Managing a large number of addresses is challenging

MAC Address Filtering (2 of 2)



Filter: ● Allow only stations in list ○ Block all stations in list

Stations List:

MAC Address: : : : : :

Figure 11-10 MAC address filtering

Figure 11-10 MAC address filtering

Wi-Fi Protected Access (WPA)

- *Wi-Fi Protected Access* (*WPA*) was introduced by the Wi-Fi Alliance to fit into the exiting 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
- 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

Knowledge Check Activity 2

What does the WPA Personal protocol use to establish authentication?

a. Digital certificate

b. MAC address

c. PIN

d. Preshared key

Knowledge Check Activity 2: Answer

What does the WPA Personal protocol use to establish authentication?

Answer: d. Preshared key

WPA Personal accomplishes authentication using a preshared key (PSK) which is a value that has been previously shared using a secure communication channel between two parties.

Wireless Security Solutions

- Modern wireless security solutions are much more secure
- Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3) form the foundation of today's wireless security solutions

Wi-Fi Protected Access 2 (WPA2) (1 of 4)

- **Wi-Fi Protected Access 2 (WPA2)** is based on final IEEE 802.11i standard
- There 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) (2 of 4)

- AES-CCMP Encryption
  - 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
- IEEE 802.1x Authentication
  - Authentication for the WPA2 Enterprise model (called the **enterprise method**) uses the IEEE 802.1x standard
  - This standard provides greater degree of security by implementing port-based authentication
  - IEEE 802.1x blocks all traffic on a port-by-port basis until client is authenticated

Wi-Fi Protected Access 2 (WPA2) (3 of 4)

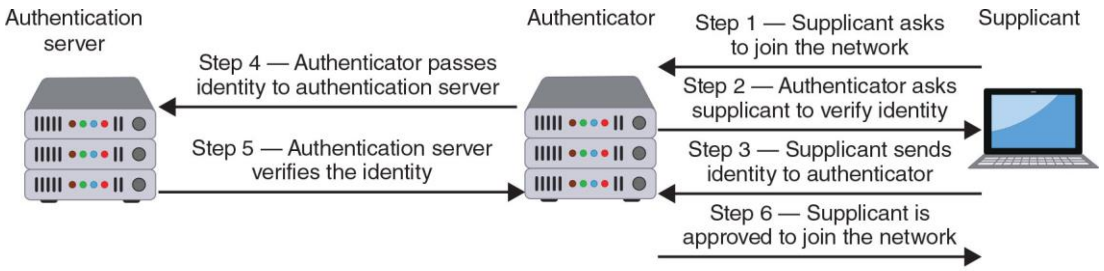

Authentication server
Authenticator
Supplicant
Step 1 — Supplicant asks to join the network
Step 2 — Authenticator asks supplicant to verify identity
Step 3 — Supplicant sends identity to authenticator
Step 4 — Authenticator passes identity to authentication server
Step 5 — Authentication server verifies the identity
Step 6 — Supplicant is approved to join the network

Figure 11-11 IEEE 802.1x process

Figure 11-11 IEEE 802.1x process

Wi-Fi Protected Access 2 (WPA2) (4 of 4)

- **Extensible Authentication Protocol** (**EAP**) is a framework for transporting authentication protocols
  - EAP defines message format
  - EAP uses four types of packets
    - Request
    - Response
    - Success
    - 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 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
  - WPA3 supports a longer 192-bit encryption
  - When using open or public Wi-Fi networks, WPA3 applies individual data encryption
  - WPA3 has improved interaction capabilities with Internet of Things (IoT) devices

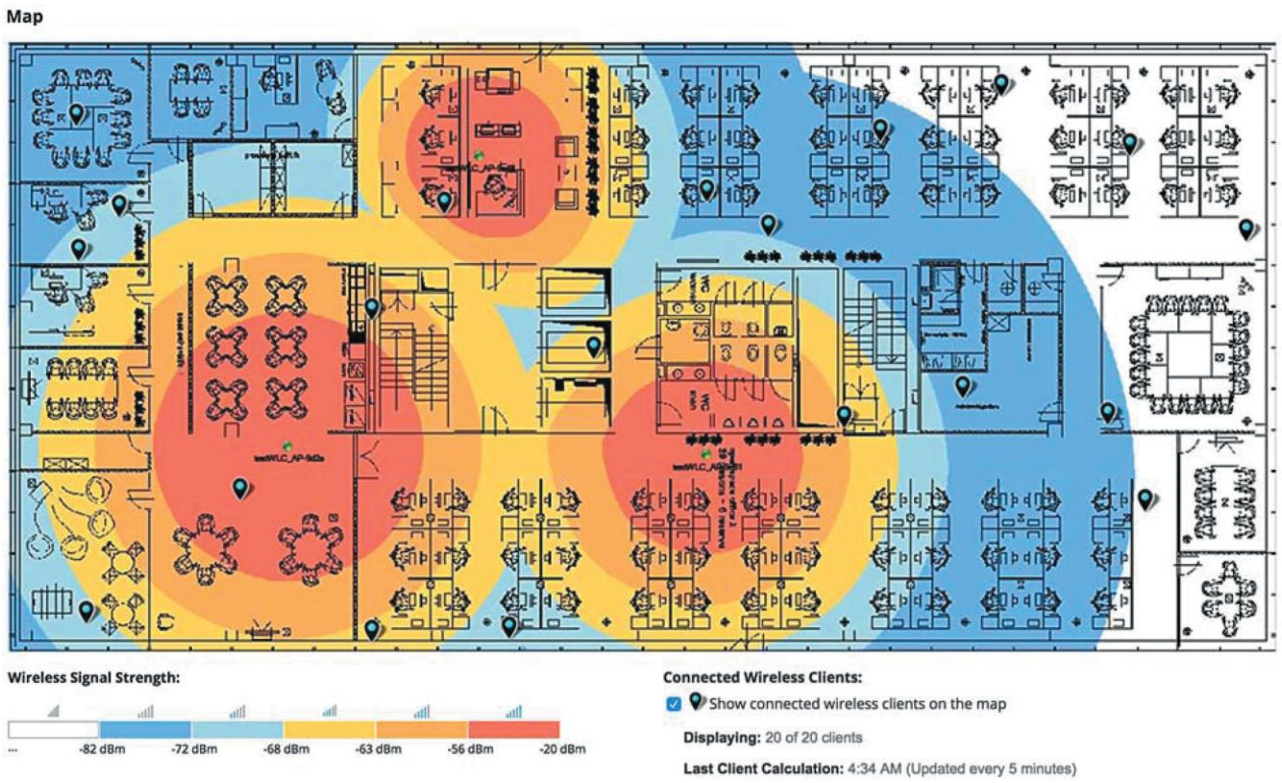
Additional Wireless Security Protections

- Other security steps can be taken to protect a wireless network such as:
  - Installation and configuration
  - Specialized systems communications
  - Rogue AP system detection

Installation (1 of 2)

- 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 is an in-depth examination and analysis of a wireless LAN site
- Several tools can be used in a site survey for installation:
  - Heat maps
  - Wi-Fi analyzers
  - Channel overlays

Installation (2 of 2)



Connected Wireless Clients:

☑ Show connected wireless clients on the map

Displaying: 20 of 20 clients

Last Client Calculation: 4:34 AM (Updated every 5 minutes)

Source: solarwinds.com

Figure 11-12 Wi-Fi heat map

Figure 11-12 Wi-Fi heat map

Configuration (1 of 2)

- 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
  - Reducing power allows less signal to reach outsiders
- Spectrum Selection
  - Some APs provide the ability to adjust frequency spectrum settings, including:
    - *Frequency band*
    - *Channel selection*
    - *Channel width*

Configuration (2 of 2)

- 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 deter 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

Specialized Systems Communications

- Several wireless technologies relate to communications for specialized and embedded systems:
  - *Zigbee*
  - *5G*
  - *Narrowband IoT*
  - *Cellular IoT baseband*
  - *Subscriber identity module (SIM) card*

Rogue AP System Detection

- Identifying rogue APs is known as *rogue AP system detection*
  - Detection requires a special sensor called a wireless probe
- There are 4 types of wireless probes can monitor airwaves for traffic:
  - *Wireless device probe*
  - *Desktop probe*
  - *Access point probe*
  - *Dedicated probe*
- Once a suspicious signal is detect 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
  - Any device not on the list is considered a rogue AP

Knowledge Check Activity 3

Which of the following is NOT a packet type used with Extensible Authentication Protocol (EAP)?

a. Acknowledgement

b. Request

c. Success

d. Response

Knowledge Check Activity 3: Answer

Which of the following is NOT a packet type used with Extensible Authentication Protocol (EAP)?

Answer: a. Acknowledgement

EAP uses four types of packets: request, response, success, and failure.

Self-Assessment

Consider the wireless technologies discussed in this module. Now think about your own experiences using wireless technologies. List the technologies you think you have used (Bluetooth, NFC, RFID, Wi-Fi) and try to recall how and if they were being used securely. What are some of the common security mistakes naïve wireless users might make that can make them vulnerable to attacks?

Summary (1 of 2)

- Bluetooth is a wireless technology using short-range RF transmissions
- Near field communication (NFC) is a set of standards primarily for smartphones and smartcards used to communicate with devices in close proximity
- A wireless technology similar to NFC is radio frequency identification (RFID)
- A wireless local area network (WLAN) is designed to replace or supplement a wired LAN
  - The IEEE has developed standards for WLANs
- WLANs are frequently the target of attackers
- A rouge AP is an unauthorized AP that allows an attacker to bypass network security and open the network and its users to attacks

Summary (2 of 2)

- IEEE 802.11 committee implemented several wireless security protections in the 802.11 standard
  - WEP and WPS, however, have significant design and implementation flaws
- Controlling access to the WLAN can be accomplished using MAC filtering on the AP
- Wi-Fi Protected Access (WPA) and WPA2 have become the foundations of wireless security today
- Other steps to protect a wireless network include:
  - Detecting rogue access points, choosing the best type of AP to match the needs of the network, managing APs through a wireless LAN controller (WLC), using a captive portal AP, access point power level adjustment, antenna positioning