6.1 Wireless communications

Radio frequency (RF)

Wireless technology can be used to send data between two devices using radio waves. A ***radio wave*** is an artificially generated energy that radiates electrical current into open space.

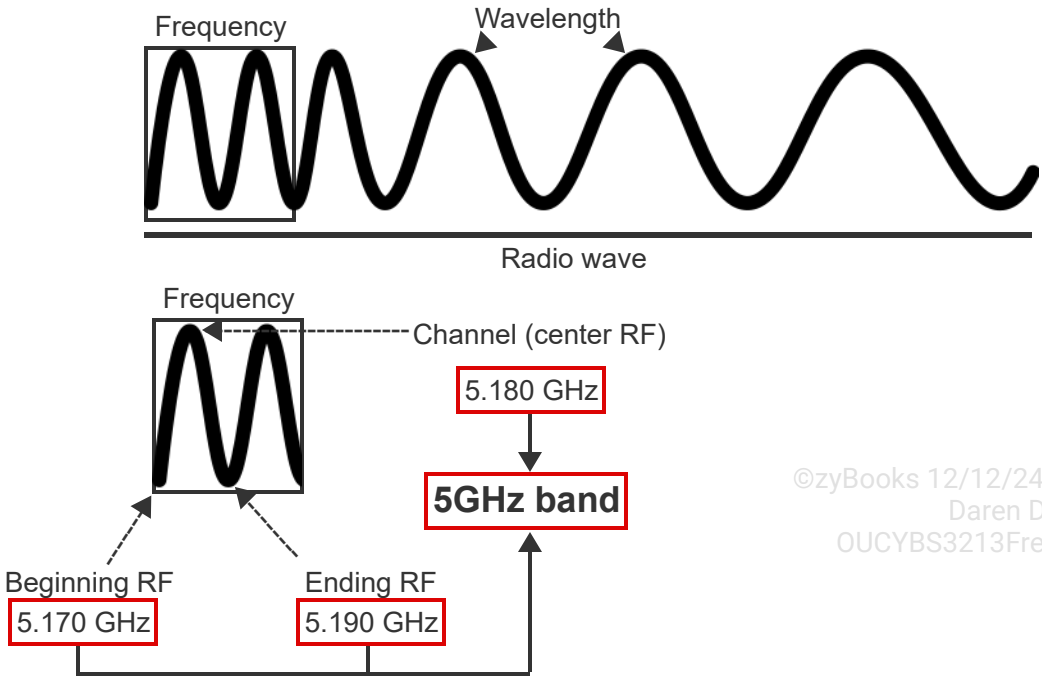
Characteristics of a radio wave:

- ***Frequency*** is a radio wave's occurrence, measured as events per second.
- ***Wavelength*** is a radio wave's traveled distance, measured in meters or feet.

Radio frequency (RF) is a numeric identifier for a radio wave's frequency measured in one billion events per second known as ***gigahertz (GHz)***. A ***band*** is a range of radio frequencies. Ex: Wi-Fi uses 2.4 GHz and 5 GHz bands. A radio wave has a beginning RF, a center RF, and an ending RF. A ***channel*** is a radio wave's center RF.

Most wireless technologies use radio waves with frequencies between 10 MHz and 6 GHz.

PARTICIPATION ACTIVITY 6.1.1: Radio frequency (RF).



Animation content:

Static image: A radio wave with a box labeled "Frequency" around the first two full radio waves. A label "Wavelength" has arrows pointing to two adjacent peaks. A copy of the wave within the Frequency box is below the radio wave. An arrow labeled "Channel (center RF), 5.180 GHz" points to the first peak of the wave. An arrow labeled "Beginning RF, 5.170 GHz" points to the first minimum of the wave. An arrow labeled "Ending RF, 5.190 GHz" points to the second minimum of the wave. The beginning RF, ending RF, and Channel (center RF) have arrows pointing to a box labeled "5GHz band".

Animation captions:

1. A radio wave chart identifies the wave's frequency and wavelength. A radio wave's wavelength begins at one RF and ends at another RF.
2. A channel is a radio wave's center RF. Channel numbers are used in device configurations.
3. A radio wave's RF value is a whole number and three fractional positions, measured in GHz. A band is either a whole number or a whole number and one fractional position. Ex: 2.4 and 5 GHz band.

PARTICIPATION ACTIVITY 6.1.2: RF.

1) What type of energy is useable for data transmissions?
   - Frequency
   - Radio wave
   - RF

2) What numerically identifies a radio wave?
   - Wavelength
   - GHz
   - RF

3) What is a range of radio frequencies called?
   - Infrared
   - Gamma rays
   - Band

4) What identifies a radio wave's center RF?
   - Channel

- Band
- MHz

Signals

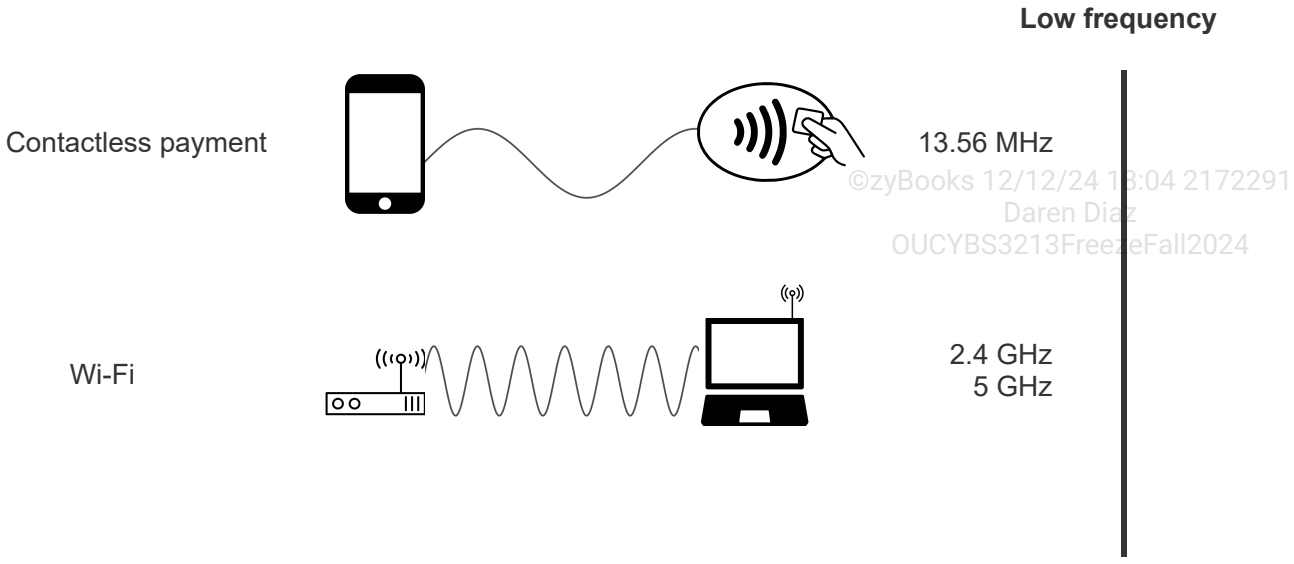
Wireless signals are electromagnetic waves traveling through the air. Signals are formed when electric energy travels through a piece of metal, like an antenna, producing waves. These waves can travel some distance depending on the signal power and environment. Ex: Concrete, wood, or metal walls, or lakes between the sending and receiving devices.

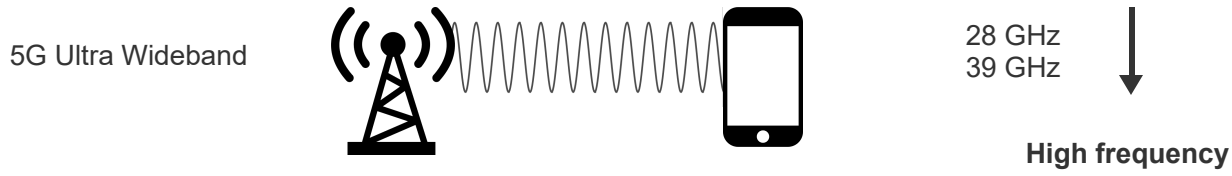
Wireless devices use signals in the transmission of data. The signal frequency determines the type of transmission used.

Types of wireless signals:

- A ***narrowband signal*** occupies a narrow frequency range or has a small bandwidth.
- A ***wideband signal*** has a large bandwidth.
- ***Broadband*** is wide bandwidth data transmission, generating an analog carrier frequency, which carries multiple digital signals or multiple channels. Broadband can be used for transmitting cable TV. In the context of internet access, broadband is any dedicated internet access with higher access speed than dial-up.
- ***Baseband*** is the frequency range occupied by a signal before modulation. A ***baseband radio processor (BP)***, also known as ***baseband processor***, is a network interface controller chip managing the radio functions. A synthesized tune or a microphone audio signal output uses a baseband signal.

PARTICIPATION ACTIVITY 6.1.3: Wireless technology.





Animation content:

Static image: Three examples of wireless technologies arranged from low frequency to high frequency. The first is "Contactless payment" and shows a smartphone with a low-frequency wave connecting to an NFC icon. Contactless payment is labeled as 13.56 MHz. The second is "Wi-Fi" and shows a router with a mid-frequency wave connecting to a laptop. Wi-Fi is labeled as 2.4 GHz and 5 GHz. The third is "5G Ultra Wideband" and shows a cell tower with a high-frequency wave connecting to a smartphone. 5G Ultra Wideband is labeled as 28 GHz and 39 GHz.

Animation captions:

1. Different frequencies are used to wirelessly send data. Contactless payment operates on the 13.56 MHz band to send data.
2. Wi-Fi operates on the 2.4 GHz and 5 GHz bands to send data. The 5 GHz band is faster, but the 2.4 GHz band can travel farther.
3. 5G Ultra Wideband operates on the 28 GHz and 39 GHz bands to send data. The higher frequency bands support faster speeds for many users in the same area.

PARTICIPATION ACTIVITY 6.1.4: Wireless technology.

1) Which signal has the smaller frequency range?
   - Wideband
   - Narrowband
   - Baseband

2) Frequency measures a wave's _____.
   - speed
   - height
   - length

3) Which frequency band has the highest frequency?
   - 2.4 GHz
   - 13.56 MHz

- 550 kHz

Common wireless technologies

Given an application, an appropriate wireless technology should be chosen based on the application's bandwidth, range, and reliability needs.

Commonly used wireless technologies include:

- ***Infrared (IR)*** sends data over a high frequency infrared connection. An IR wave cannot go through an obstacle, so an IR connection requires a line of sight between the two connected devices.
- ***Bluetooth*** is a low power, short range wireless technology that pairs two devices. Bluetooth is often used to connect a device to peripherals. Ex: A computer connects to a wireless keyboard via Bluetooth.
- ***Wi-Fi*** uses a router to connect devices to each other and the Internet. Wi-Fi is the most common wireless technology used for home and office networks.
- ***Cellular*** uses cell towers to send data to mobile devices like smartphones and tablets. A cellular network is provided by a carrier, like AT&T or Verizon. All data sent using cellular technology travels through a network that is managed by an outside organization.

Table 6.1.1: Common wireless technologies.

Wireless technology	Range	Frequency bands	Bandwidth	Examples
IR	3 - 30 feet	315 - 344 GHz	Up to 16 Mbit/s	TV remote control
Bluetooth	30 feet	2.4 GHz	Up to 2.1 Mbit/s	Wireless headphones Fitness tracker
Wi-Fi	150 feet	2.4 GHz 5 GHz	Up to 9.6 Gbit/s	Laptop Smart TV
Cellular	10 miles	800 MHz - 40 GHz	Up to 10 Gbit/s	5G cellular data Mobile hotspot

PARTICIPATION ACTIVITY 6.1.5: Common wireless technologies.

Choose the most appropriate wireless technology for each application.

How to use this tool

Bluetooth **IR** **Wi-Fi** **Cellular**

	Connecting to the Internet in an office building
	Connecting a wireless speaker to a smartphone
	Controlling an LED light strip
	Connecting to the Internet in a public area

Reset

Other wireless technologies

Other less used wireless technologies exist that have a specific function or lower bandwidth capabilities:

- ***Radio frequency identification (RFID)*** uses a tag and a reader to identify and track objects. A physical tag is attached to or embedded in an object. When a reader is within range, the reader receives data from the tag.
- ***Near-field communication (NFC)*** instantly connects two devices in close proximity. NFC is based on RFID. However, NFC allows each device to act as a tag or a reader, so data can be sent in either direction.
- ***Global Positioning System (GPS)*** is a system of satellites that are used for mapping and navigation. A GPS receiver uses signals from multiple satellites to calculate the device's position.
- ***ZigBee*** is a low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks. Ex: Home automation. Zigbee consumes less power than Wi-Fi, but Wi-Fi uses higher bandwidth.

Table 6.1.2: Common wireless technologies.

Wireless technology	Range	Frequency bands	Bandwidth	Examples
RFID	3 - 300 feet	125 kHz 13.56 MHz 860 - 960 MHz	Up to 848 Kbit/s	Hotel room key Pet microchip
NFC	4 inches	13.56 MHz	Up to 424 Kbit/s	Contactless payment Digital business card
GPS	13,000 miles	1575.42 MHz 1227.6 MHz	50 bit/s	Google Maps Geofencing
ZigBee	10-333 feet (Best under 40 feet)	2.4 GHz (Global), 868Mhz (Europe) and 915MHz (America)	Up to 250 Kbit/s	Wireless network sensors Light bulb and switch

PARTICIPATION ACTIVITY 6.1.6: Common wireless technologies.

Choose the most appropriate wireless technology for each application.

How to use this tool

ZigBee **RFID** **GPS** **NFC**

	Granting building access with a contactless card
	Connecting a smartphone to a Wi-Fi network
	Navigating a delivery route

	Low-cost, low-power wireless machine-to-machine (M2M).

Reset

6.2 Common wireless connectivity

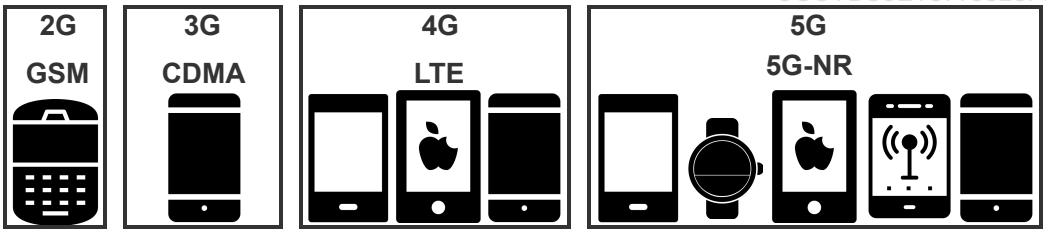
Cellular connectivity

A ***cellular network*** is a wireless network composed of small geographical areas called "cells", central towers for communications, and wireless devices. A ***subscriber identity module (SIM)*** card is a smart card storing identification information connecting a cellular phone to a specific cellular network. Some mobile devices are replacing SIM cards with an eSIM. An ***eSIM*** is embedded in a mobile device connecting the smart device to the cellular network. A mobile carrier can lock a device to only work with the carrier's network. Carrier unlocking allows the device to work with any carrier cell network.

A site survey identifies what cellular network standard meets the needs for BYOD and mobility. Four cellular network technologies exist:

- ***Global system for mobile communications (GSM)*** is a European-developed protocol suite used by the second generation (2G) of wireless mobile communication.
- ***Code division multiple access (CDMA)*** is the underlying channel access method used by the third generation (3G) of wireless mobile communication.
- ***Long term evolution (LTE)*** is the wireless broadband communication standard used by the fourth generation (4G) of wireless mobile communication.
- ***Fifth generation (5G)*** is the latest wireless broadband communication standard used by cellular networks.

PARTICIPATION ACTIVITY 6.2.1: Cellular standards.



Animation content:

Wireless broadband communication standard generations. GSM and 2G replaced the first generation (1G) analog standard. 2G offered digitally encrypted voice conversations and mobile data services. CDMA and 3G introduced mobile internet access, provided faster data rates, and improved security. Most cellular providers ended 3G support in 2022. LTE and 4G increased mobile data rates to 100 Mbps. 4G is expected to be a valid cellular option for several years to come. 5G is the latest wireless broadband communication standard. 5G frequencies are known as 5G new radio (5G NR), but most vendors just use the 5G name.

Animation captions:

1. GSM and 2G replaced the first generation (1G) analog standard. 2G offered digitally encrypted voice conversations and mobile data services.
2. CDMA and 3G introduced mobile internet access, provided faster data rates, and improved security. Most cellular providers ended 3G support in 2022.
3. LTE and 4G increased mobile data rates to 100 Mbps. 4G is expected to be a valid cellular option for several years to come.
4. 5G is the latest wireless broadband communication standard. 5G frequencies are known as 5G new radio (5G NR), but most vendors just use the 5G name.

PARTICIPATION ACTIVITY 6.2.2: Cellular network design.

1) Which wireless communication generation marked the transition from analog services to digital services?
   - 1G
   - 2G
   - 3G

2) Which wireless communication generation used CDMA as the underlying channel access method?
   - 2G
   - 3G
   - 4G

3) Which wireless broadband communication standard is used in 4G?

- GSM
- CDMA
- LTE

4) What is the latest wireless broadband communication standard available to users?

- 4G
- 5G
- 6G

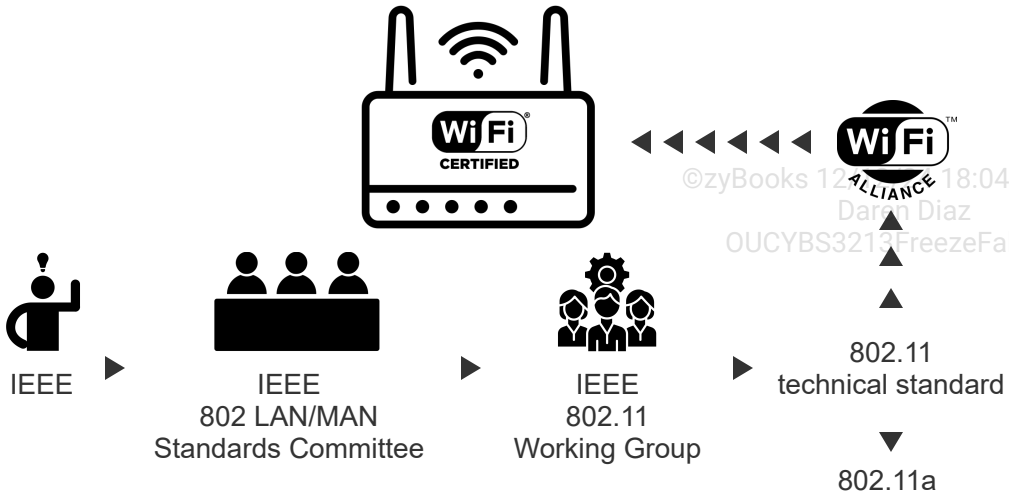
Wi-Fi connectivity

A technical standard defines one or more aspects of a technology. A vendor produces a networked device based on a technical standard. A third-party certifies a networked product to ensure proper implementation of a technical standard. A WLAN requires a combination of technical standards, networked devices, and product certifications to ensure device interoperability.

Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that advances technology through technical standard development and other efforts. The IEEE 802 LAN/MAN Standards Committee defines many aspects of WLAN technology in the IEEE Standard 802.11.

Wi-Fi Alliance is a network of companies responsible for certifying the proper implementation of an IEEE technical standard. ***Wi-Fi*** is Wi-Fi Alliance's certification indicating a WLAN product meets an IEEE technical standard. "Wi-Fi certified" means the Wi-Fi Alliance certifies a networking device properly implements an IEEE technical standard.

PARTICIPATION ACTIVITY 6.2.3: WLAN standards development.



802.11b
802.11g

etc.

Animation content:

A hardware advancement enables a WAP to achieve faster speeds. IEEE recognizes a need to standardize a concept or idea. The appropriate IEEE Standards Committee commissions a Working Group to draft a new technical standard. The new WAP is usually produced while the technical standard is being ratified. Once the technical standard is ratified, Wi-Fi Alliance begins the certification process. If the WAP meets the IEEE technical standard, the WAP receives the Wi-Fi CERTIFIED logo. Over time, new amendments go through the same development process and become part of the original technical standard.

Animation captions:

1. A hardware advancement enables a WAP to achieve faster speeds. IEEE recognizes a need to standardize a concept or idea.
2. The appropriate IEEE Standards Committee commissions a Working Group to draft a new technical standard.
3. The new WAP is usually produced while the technical standard is being ratified. Once the technical standard is ratified, Wi-Fi Alliance begins the certification process.
4. If the WAP meets the IEEE technical standard, the WAP receives the Wi-Fi CERTIFIED logo.
5. Over time, new amendments go through the same development process and become part of the original technical standard.

PARTICIPATION ACTIVITY 6.2.4: WLAN Standards Organizations.

1) Which organization develops technical standards for WLANs?
   - IEEE
   - Wi-Fi Alliance
   - FCC

2) Which organization certifies a WLAN product properly implements a technical standard?
   - IEEE
   - Wi-Fi Alliance

- ITU

3) Which IEEE entity is directly responsible for drafting the 802.11 technical standard?

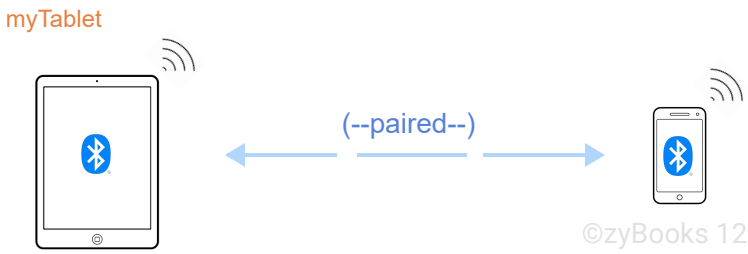
- IEEE 802 LAN/MAN Standards Committee
- IEEE 802.11 working group
- Wi-Fi Alliance

Bluetooth connectivity

Bluetooth is a short-range wireless technology that enables the connection of nearby devices. Bluetooth connects a main device with one or more peripheral devices. Bluetooth operates in the unlicensed 2.4 GHz band. Non-Bluetooth technologies which operate in the unlicensed 2.4 GHz band may cause interference with Bluetooth devices. Ex: Some wireless keyboards and mice, as well as Wi-Fi, operate in the same frequency band as Bluetooth devices.

Bluetooth communications typically take place between paired devices. ***Pairing*** is the process of establishing a trusted connection between two Bluetooth devices. Paired devices use encrypted communication to exchange data. Unpaired, unencrypted communications are also possible. Ex: Sending a contact over a Bluetooth connection is done using one-time, unpaired, unencrypted communication.

PARTICIPATION ACTIVITY 6.2.5: Bluetooth pairing process.



Paired Bluetooth devices can exchange data using encrypted communication.

Animation content:

Static image: A tablet labeled "myTablet" with a Bluetooth symbol on the screen. A smartphone with a Bluetooth symbol on the screen. A two-way arrow between the tablet and the smartphone labeled "paired".
Step 1: Two devices seeking to communicate via Bluetooth must be paired.
A tablet and a smartphone appear with a Bluetooth symbol on each screen.
Step 2: Pairing begins when one device becomes discoverable. The device lets any device within range know of the device's existence. Here, the tablet is discoverable.
The text "myTablet" appears above the tablet.
Step 3: Another device can then initiate pairing with a discovered device by sending a pairing request. The smartphone sends a pairing request to the tablet.
A blue arrow labeled "PAIR" appears and moves from the smartphone to the tablet. The arrow disappears.
Step 4: In response, the tablet challenges the smartphone to present the Bluetooth Personal Identification Number (PIN).
A blue arrow labeled "PIN?" appears and moves from the tablet to the smartphone. The arrow disappears.
Step 5: If the smartphone responds with the correct PIN, the devices are paired. Data can now be exchanged using encrypted communication.
A blue arrow labeled "5291" appears and moves from the smartphone to the tablet. "Correct!" appears and then disappears. A two-way arrow labeled "paired" appears between the tablet and the smartphone.

Animation captions:

1. Two devices seeking to communicate via Bluetooth must be paired.
2. Pairing begins when one device becomes discoverable. The device lets any device within range know of the device's existence. Here, the tablet is discoverable.
3. Another device can then initiate pairing with a discovered device by sending a pairing request. The smartphone sends a pairing request to the tablet.
4. In response, the tablet challenges the smartphone to present the Bluetooth Personal Identification Number (PIN).
5. If the smartphone responds with the correct PIN, the devices are paired. Data can now be exchanged using encrypted communication.

PARTICIPATION ACTIVITY 6.2.6: Bluetooth basics.

1) Bluetooth operates in the 2.4 GHz band. Which wireless technologies also operate in the 2.4 GHz band?

   - NFC
   - Cellular

- Wi-Fi

2) What type of authentication information is required for pairing two Bluetooth devices?

- Password
- PIN
- Certificate

3) Which process establishes a trusted connection between two Bluetooth devices?

- pairing
- syncing
- association

Sharing devices

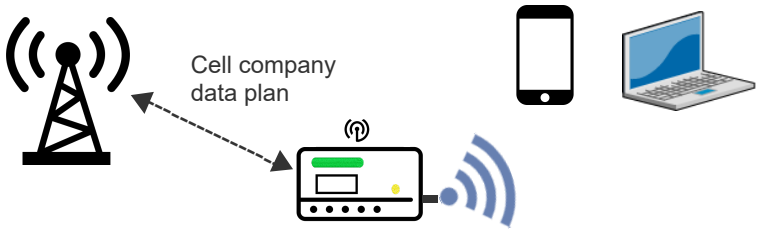
Mobile devices can share resources by tethering, hotspots, or USB On-The-Go.

A ***mobile hotspot*** is a service offered by various telecom providers that provide localized Wi-Fi to users for internet access.

A ***tethering*** strategy involves connecting one device without Wi-Fi to another device that has Wi-Fi connectivity. Ex: A user could tether a laptop to a smartphone through cabling or a wireless connection. Some phones can share a Wi-Fi connection by tethering to a phone that has a hotspot configured. Smartphones can share mobile data by Wi-Fi, Bluetooth, or USB.

USB On-The-Go (USB OTG or OTG) is a specification allowing USB devices, to be a host, allowing other USB devices to attach. Ex: USB flash drives or external media, digital cameras, mouse or keyboards. USB OTG allows devices to switch between the roles of host and device. Ex: A mobile phone may read from removable media as the host device, but be used as a USB mass storage device when connected to a host computer.

PARTICIPATION ACTIVITY 6.2.7: Mobile hotspots.



Hotspot

Animation content:

Static image: A cell tower, a mobile hotspot, two smartphones, and a laptop. A two-way arrow labeled "Cell company data plan" is between the cell tower and the mobile hotspot. The mobile hotspot has a Wi-Fi signal pointing toward the smartphones and the laptop.

Animation captions:

1. Mobile hotspots are self-contained units receiving a cellular data signal to provide internet connection to mobile devices.
2. A hotspot sends and receives a signal to a cellular tower.
3. Hotspots are typically designed for a specific cellular carrier, and require a suitable cellular data-only plan to operate.
4. Mobile hotspots only provide internet access for mobile devices.

PARTICIPATION ACTIVITY 6.2.8: Sharing devices.

1) What type of connection do mobile hotspots provide to mobile devices?
   - Cellular
   - Internet
   - Tethering

2) Which is a strategy that involves connecting a device without Wi-Fi to a smartphone that has Wi-Fi connectivity?
   - Hotspot
   - USB On-The-Go
   - Tethering

3) What does a hotspot require from a cell company to provide internet access to mobile devices?
   - Data plan
   - Tethering
   - USB support

6.3 WLAN standards

2.4 GHz band channels

The ***2.4 GHz band*** is a lower frequency, longer wavelength band used in a WLAN. The IEEE 802.11 technical standard recommends a WLAN communicates using the 2.4 GHz band's 14 channels. ***Channel width***, measured in megahertz (MHz), is the distance between a channel's starting RF and ending RF. One megahertz is one million events per second. The channel width of each 2.4 GHz channel is 22 MHz.

Table 6.3.1: 2.4 GHz band channels.

Channel	Starting RF (MHz)	Center RF (MHz)	Ending RF (MHz)
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483

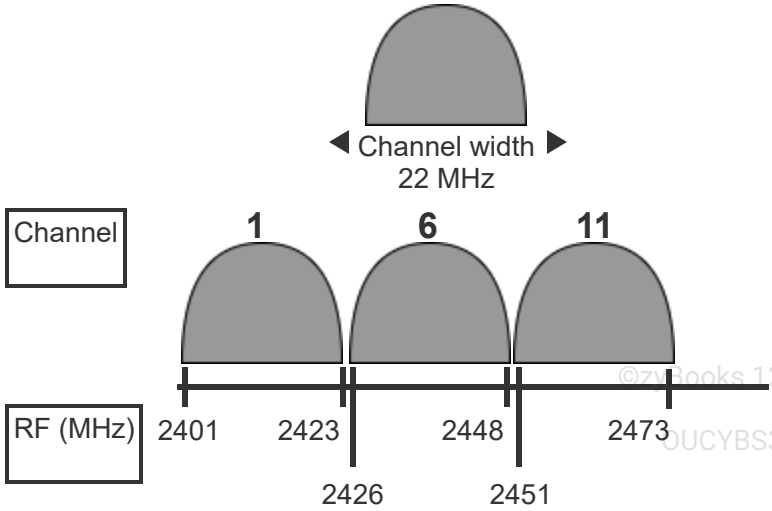
14	2473	2484	2495

The starting RF and ending RF causes channel overlap among adjacent channels. ***Channel overlap*** is an interference type caused by nearby wireless access points using the same channel or an overlapping channel. Ex: Channel 3's frequency range of 2411-2433 MHz overlaps with channel 1's frequency range of 2401-2423 MHz. Only three universally authorized 2.4 GHz channels do not overlap. Certain IEEE 802.11 technical standards allow for bonded channels. A ***bonded channel*** is the aggregation of at least two adjacent channels.

2.4 GHz channel authorization

Channels 1, 6, 11, and 14 do not overlap. However, not every channel is universally authorized for WLANs. The United States only authorizes channels 1 through 11 for WLANs. The European Union only authorizes channels 1 through 13 for WLANs. Japan authorizes all 14 channels for WLANs.

PARTICIPATION ACTIVITY 6.3.1: 2.4 GHz band channels.



2.4 GHz band channels.

Animation content:

Static image: Four semicircles showing 2.4 GHz band channels. One semicircle is in the top row with a two-way arrow labeled "Channel width, 22 MHz" spanning the semicircle's width. The bottom row has three semicircles above a number line labeled "RF (MHz)". The first semicircle is labeled as channel 1 and goes from 2401 MHz to 2423 MHz. The second semicircle is labeled as channel 6 and goes from 2426 MHz to 2448 MHz. The third semicircle is labeled as channel 11 and goes from 2451 MHz to 2473 MHz.
Step 1: The 2.4 GHz band ranges from 2.400 GHz to 2.499 GHz. The IEEE 802.11 technical standard specifies fourteen 22 MHz-wide channels.

A semicircle appears. A two-way arrow labeled "Channel width, 22 MHz" appears and spans the width of the semicircle.
Step 2: At least ten channels overlap with one or more adjacent channels. Ex: channels 1-5 overlap.
A number line appears, labeled "RF (MHz)". The number line starts at 2401 MHz. A gray semicircle labeled as channel 1 appears starting at 2401 MHz. White semicircles labeled channel 2, 3, and 4, and 5 appear overlapping to the right. The channel 5 semicircle starts just before 2423 MHz, and the channel 1 semicircle ends at 2423 MHz.
Step 3: At least three channels do not overlap with an adjacent channel. Ex: channels 1 and 6 do not overlap.
A gray semicircle labeled as channel 6 appears starting at 2426 MHz and ending at 2448 MHz.

_____

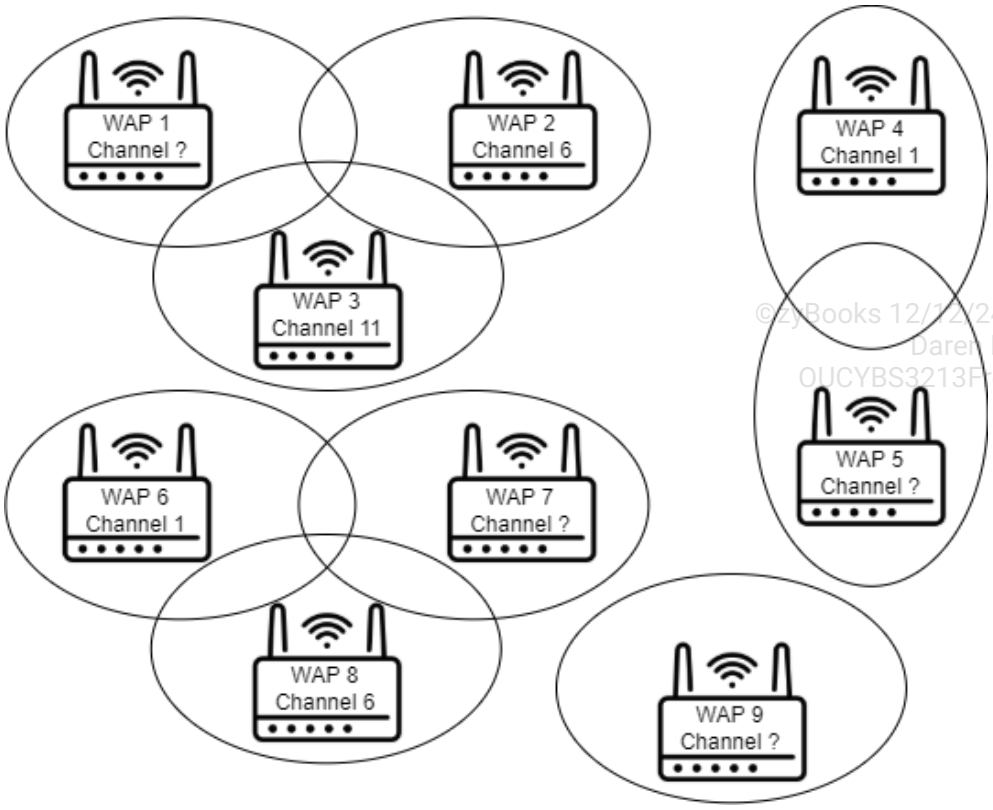
Step 4: The three non-overlapping channels in the 2.4 GHz band are 1, 6, and 11.
White semicircles appear for channels 7 through 10 and 11 through 14. A gray semicircle appears for channel 11 starting at 2451 MHz and ending at 2473 MHz. Channel 14 ends at 2495 MHz.
Step 5: Nearby WAPs use different combinations of the three non-overlapping channels to provide roaming and avoid interference.
The white semicircles representing the overlapping channels disappear.

Animation captions:

1. The 2.4 GHz band ranges from 2.400 GHz to 2.499 GHz. The IEEE 802.11 technical standard specifies fourteen 22 MHz-wide channels.
2. At least ten channels overlap with one or more adjacent channels. Ex: channels 1-5 overlap.
3. At least three channels do not overlap with an adjacent channel. Ex: channels 1 and 6 do not overlap.
4. The three non-overlapping channels in the 2.4 GHz band are 1, 6, and 11.
5. Nearby WAPs use different combinations of the three non-overlapping channels to provide roaming and avoid interference.

PARTICIPATION ACTIVITY 6.3.2: 2.4 GHz channel selection.

Refer to the below image for each question. The image depicts a WLAN with several WAPs and each WAP's coverage area. Select the appropriate channel in each scenario.



1) What channel should WAP 1 use to avoid channel overlap with WAPs 2 and 3?

- 1
- 6
- 11

2) What channel could WAP 5 be configured with?

- 1 or 6
- 6 or 11
- 1 or 11

3) What channel should WAP 7 use to avoid channel overlap?

- 2
- 7
- 11

4) What channel should WAP 9 use to avoid channel overlap?

- 1, 6, or 11

- 36, 40, or 44
- 100, 104, or 108

5 GHz band channels

The ***5 GHz band*** is a higher frequency, shorter wavelength band used in a WLAN. The 5 GHz band consists of 25 channels. Each 5 GHz channel is 20 MHz wide, and all 25 channels are non-overlapping channels. The 5 GHz channels are organized in various unlicensed national information infrastructure bands. An ***unlicensed national information infrastructure (U-NII)*** band is a band defined by the United States (US) Federal Communications Commission (FCC) for WLAN and wireless ISP use. Four U-NII bands are used in WLANs:

- ***U-NII 1*** is the U-NII band including 5 GHz channels 36, 40, 44, and 48.
- ***U-NII 2*** or U-NII 2A is the U-NII band including 5 GHz channels 52, 56, 60, and 64.
- ***U-NII 2 extended*** or U-NII 2C is the U-NII band including 5 GHz channels 100 to 144.
- ***U-NII 3*** is the U-NII band including 5 GHz channels 149 to 165.

Several 5 GHz band channels can be bonded in widths of 40 MHz, 80 MHz, and 160 MHz. A WAP using a bonded 5 GHz channel uses an intermediate channel number based on channel width used. Some 5 GHz channels cannot be bonded because the bonded channel interferes with a non-WLAN channel or band. Ex: channel 165 is near the end of the U-NII 3 band and channel 169 is in the U-NII 4 band.

Table 6.3.2: 5 GHz band channels.

U-NII band	Center RF (MHz)	Channel	40 MHz channel	80 MHz channel	160 MHz channel
1	5180	36	38	42	50
	5200	40			
	5220	44	46		
	5240	48			
2A	5260	52	54	58	
	5280	56			
	5300	60	62		

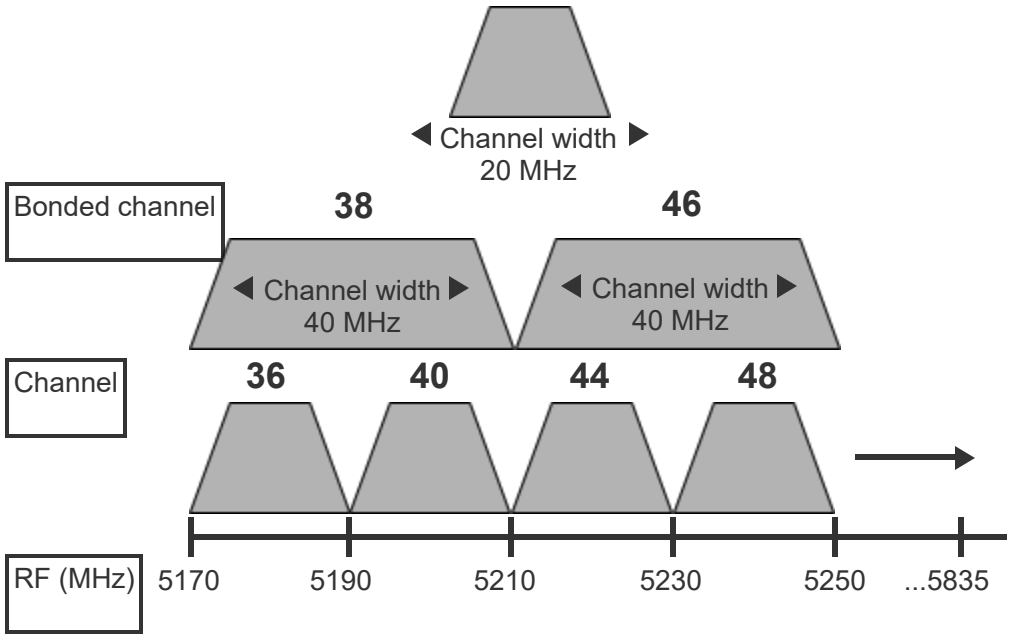
	5320	64			
2C	5500	100	102	106	114
	5520	104			
	5540	108	110		
	5560	112			
	5580	116	118	122	
	5600	120			
	5620	124	126		
	5640	128			
	5660	132	134	138	None
	5680	136			
	5700	140	142		
	5720	144			
3	5745	149	151	155	None
	5765	153			
	5785	157	159		
	5805	161			
	5825	165	None	None	

5 GHz band channel numbering

Channel 36 is the first 5 GHz channel because the U-NII band channels start at 5.180 GHz. The 2.4 GHz band starts at channel 1 because the RF authorized for WLANs starts at 2.401 GHz, and the 2.4 GHz band is not part of U-NII. Each 5 GHz channel is spaced four numbers apart because only every fourth channel is defined for WLAN use. Each 5

*GHz channel also spans 20 MHz, or 4 * 5 MHz. Ex: channel 36 is 5180 MHz and channel 40 is 5200 MHz.*

PARTICIPATION ACTIVITY 6.3.3: 5 GHz band channels.



5 GHz band channels.

Animation content:

Static image: Several trapezoids showing 5 GHz band channels. One trapezoid is in the top row with a two-way arrow labeled "Channel width, 20 MHz" spanning the trapezoid's width. The middle row has two wider trapezoids labeled as bonded channel 38 and bonded channel 46. Both trapezoids have a channel width of 40 MHz. The bottom row has four trapezoids above a number line labeled "RF (MHz)". The first trapezoid is labeled as channel 36 and goes from 5170 MHz to 5190 MHz. The second trapezoid is labeled as channel 40 and goes from 5190 MHz to 5210 MHz. The third trapezoid is labeled as channel 44 and goes from 5210 MHz to 5250 MHz. The fourth trapezoid is labeled as channel 48 and goes from 5230 MHz to 5250 MHz. An arrow extends to the right, and the last mark on the number line is 5835 MHz.

Step 1: The 5 GHz band ranges from 5.170 GHz to 5.835 GHz. The IEEE 802.11 technical standard specifies 25 channels with a 20 MHz channel width.

A trapezoid appears. A two-way arrow labeled "Channel width, 20 MHz" appears and spans the width of the trapezoid.

Step 2: 5 GHz channels do not overlap. However, nearby WAPs using the same channel will experience interference. Ex: two WAPs using channel 36.
A number line appears, labeled "RF (MHz)". The number line starts at 5170 MHz. A trapezoid labeled as channel 36 appears and goes from 5170 MHz to 5190 MHz. A trapezoid labeled as channel 40 appears and goes from 5190 MHz to 5210 MHz. A trapezoid labeled as channel 44 appears and goes from 5210 MHz to 5250 MHz. A trapezoid labeled as channel 48 appears and goes from 5230 MHz to 5250 MHz. An arrow extends to the right, and the last mark on the number line is 5835 MHz.
Step 3: A bonded 5 GHz channel uses an intermediate channel number based on the channel width used. Ex: channel 38 bonds channels 36 and 40.
Above the previous trapezoids, two wider trapezoids labeled as bonded channel 38 and bonded channel 46 appear. Both trapezoids have a channel width of 40 MHz.

Animation captions:

1. The 5 GHz band ranges from 5.170 GHz to 5.835 GHz. The IEEE 802.11 technical standard specifies 25 channels with a 20 MHz channel width.
2. 5 GHz channels do not overlap. However, nearby WAPs using the same channel will experience interference. Ex: two WAPs using channel 36.
3. A bonded 5 GHz channel uses an intermediate channel number based on the channel width used. Ex: channel 38 bonds channels 36 and 40.

PARTICIPATION ACTIVITY 6.3.4: 5 GHz band channels.

1) Which higher frequency, shorter wavelength WLAN band has exactly 25 non-overlapping channels?
   - 2.4 GHz
   - 5 GHz
   - 6 GHz

2) Which channel is in the U-NII 1 band?
   - 36
   - 52
   - 100

3) If channels 52 and 56 are bonded with a 40 MHz channel width, what bonded channel number is used?
   - 38
   - 54

- 62

4) Which U-NII band does channel 157 belong to?

- 2
- 3
- 4

Legacy WLAN technical standards

The IEEE 802.11 technical standards are updated whenever a technological advancement is made. Legacy technical standards are "rolled-up" to maintain interoperability with legacy devices still in use.

Table 6.3.3: 802.11 technical standard roll-ups.

Standard	Contents
802.11-1997	Original IEEE 802.11 technical standard
802.11-2007	Roll-up of 1997-2003 amendments
802.11-2012	Roll-up of 1997-2007 amendments
802.11-2016	Roll-up of 1997-2012 amendments
802.11-2020	Roll-up of 1997-2018 amendments

Vendors refer to three legacy IEEE 802.11 standards in their documentation and interfaces:

- ***802.11a*** is a legacy IEEE 802.11 standard with 54 Mbps bandwidth on the 5 GHz band.
- ***802.11b*** is a legacy IEEE 802.11 standard with 11 Mbps bandwidth on the 2.4 GHz band.
- ***802.11g*** is a legacy IEEE 802.11 standard with 54 Mbps bandwidth on the 2.4 GHz band and backward compatibility with IEEE 802.11b.

PARTICIPATION ACTIVITY

6.3.5: 802.11 legacy standards.

802.11b	802.11a	802.11g
Band: 2.4 GHz	Band: 5 GHz	Band: 2.4 GHz
Bandwidth: 11 Mbps	Bandwidth: 54 Mbps	Bandwidth: 54 Mbps
Distance: 150 feet	Distance: 95 feet	Distance: 95 feet

Animation content:

Static image: Three columns. The first column shows 802.11b had a 2.4 GHz band, 11 Mbps bandwidth, and a distance of 150 feet. The second column shows 802.11a had a 5 GHz band, 54 Mbps bandwidth, and a distance of 95 feet. The third column shows 802.11g had a 2.4 GHz band, 54 Mbps bandwidth, and a distance of 95 feet.

Animation captions:

1. 802.11b devices were available before 802.11a devices. The 2.4 GHz band provided a larger coverage area at a slower bandwidth.
2. 802.11a devices became available in the early 2000s. The 5 GHz band provided a higher bandwidth with a smaller coverage area.
3. 802.11g devices provided 5 GHz bandwidth with 2.4 GHz coverage. 802.11g provided backward compatibility for 802.11b devices.

PARTICIPATION ACTIVITY | 6.3.6: Legacy WLAN standards.

How to use this tool

802.11g **802.11b** **802.11a**

	Legacy IEEE 802.11 standard with 11 Mbps bandwidth on the 2.4 GHz band.
	Legacy IEEE 802.11 standard with 54 Mbps bandwidth on the 5 GHz band.

	Legacy IEEE 802.11 standard with 54 Mbps bandwidth on the 2.4 GHz band and backward compatibility with IEEE 802.11b.

Reset

Modern WLAN technical standards

Modern IEEE 802.11 standards focus on narrowing the bandwidth gap between wired LANs and WLANs. Three modern IEEE 802.11 standards exist:

- ***802.11n*** is a modern IEEE 802.11 standard providing 600 Mbps bandwidth on both the 2.4 GHz and 5 GHz bands.
- ***802.11ac*** is a modern IEEE 802.11 standard providing ~7 Gbps bandwidth on the 5 GHz band.
- ***802.11ax*** is a modern IEEE 802.11 standard providing 11 Gbps bandwidth on the 2.4 and 5 GHz bands.

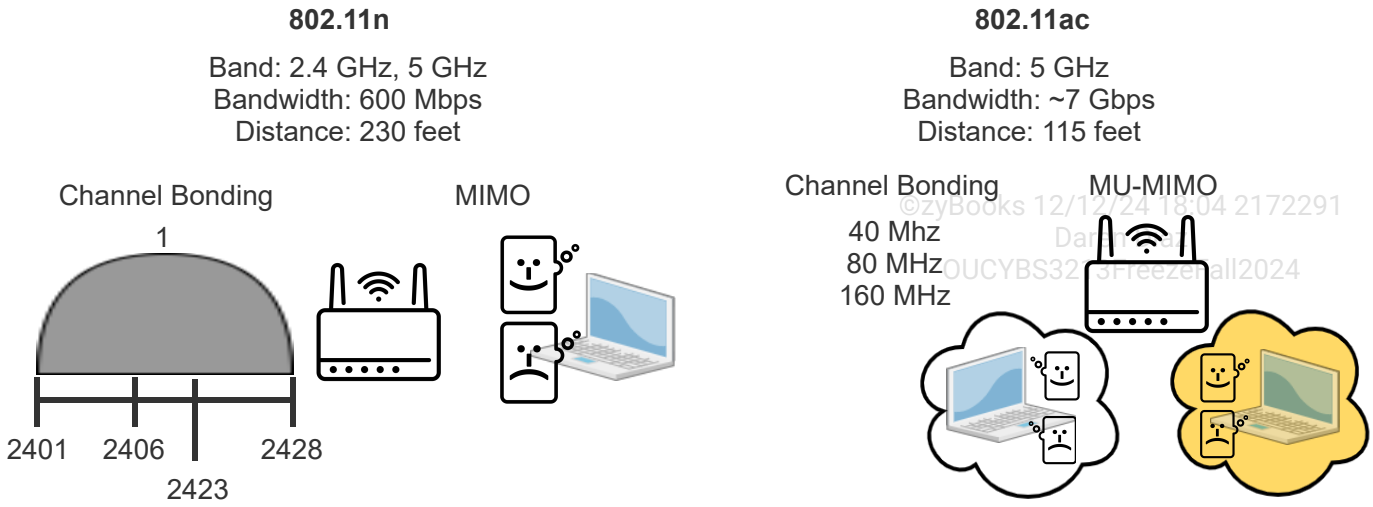
Table 6.3.4: Wi-Fi Alliance's consumer-friendly generation names.

IEEE standard	Wi-Fi Alliance name
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6, Wi-Fi 6E

Modern WLAN technical standards introduced three new specifications:

- Channel bonding is the aggregating of at least two adjacent WLAN channels. Channel bonding can be used to increase throughput between devices in a wireless network.
- ***Multiple Input Multiple Output (MIMO)*** is the leveraging of at least 2 receiving antennas and 1 transmitting antenna per band to improve RF signal quality and bandwidth.
- ***Multi-User MIMO (MU-MIMO)*** is an enhanced version of MIMO intended to improve RF signal quality and bandwidth on a device-by-device basis.

PARTICIPATION ACTIVITY 6.3.7: 802.11n and 802.11ac.



Animation content:

Static image: The left side shows 802.11n has 2.4 GHz and 5 GHz bands, 600 Mbps bandwidth, and a distance of 230 feet. A gray semicircle labeled "Channel Bonding, 1" shows on a number line going from 2401 to 2428. A router, a laptop, a message with a happy face, and a message with a sad face are below the label "MIMO". The right side shows 802.11ac has a 5 GHz band, about 7 Gbps bandwidth, and a distance of 115 feet. A list labeled "Channel Bonding" includes 40 MHz, 80 MHz, and 160 MHz. A router is below the label "MU-MIMO". Two clouds are below the router. Each cloud contains a laptop, a message with a happy face, and a message with a sad face. The right cloud has a yellow background.

Step 1: 802.11n devices became available in 2009. Two significant specifications were included: channel bonding and MIMO.

The left side shows 802.11n has 2.4 GHz and 5 GHz bands, 600 Mbps bandwidth, and a distance of 230 feet. THe labels "Channel Bonding" and "MIMO" appear.

Step 2: Channel bonding allowed the aggregation of two adjacent channels in either band. A wider channel allows higher throughput for a single transmission. Ex: Bonding 2.4 GHz band channels 1 and 2.

Under "Channel Bonding", a number line going from 2401 to 2428 appears. Two semicircles labeled channel 1 and channel 2 appear overlapping above the number line. Channel 1 goes from 2401 to 2423. Channel 2 goes from 2406 to 2428. Channel 2 disappears and channel 1 stretches from 2401 to 2428.

Step 3: MIMO utilized feedback from client devices to improve RF quality. However, the feedback format was never standardized among vendors, and MIMO did not always meet expectations.

Under "MIMO", a router and a laptop appear. A wireless signal travels from the router to the laptop. A message with a sad face goes from the laptop to the router. Another wireless signal travels from the router to the laptop. A message with a happy face goes from the laptop to the router.

Step 4: 802.11ac devices became available in 2014 in two waves. Wave 1 devices supported channel bonding up to 80 MHz, and wave 2 devices supported channel bonding up to 160 Mhz.

The right side shows 802.11ac has a 5 GHz band, about 7 Gbps bandwidth, and a distance of 115 feet. A list labeled "Channel Bonding" appears and includes 40 MHz, 80 MHz, and 160 MHz.
Step 5: 802.11ac standardized the client feedback format, leading to MU-MIMO. MU-MIMO used the feedback to generate a tailored RF signal for each client device.
A router appears under the label "MU-MIMO". Two laptops appear below the router. Each laptop has a message with a happy face and a message with a sad face. A white cloud appears and moves from the router to the outside of the left laptop. A yellow cloud appears and moves from the router to the outside of the right laptop.

Animation captions:

1. 802.11n devices became available in 2009. Two significant specifications were included: channel bonding and MIMO.
2. Channel bonding allowed the aggregation of two adjacent channels in either band. A wider channel allows higher throughput for a single transmission. Ex: Bonding 2.4 GHz band channels 1 and 2.
3. MIMO utilized feedback from client devices to improve RF quality. However, the feedback format was never standardized among vendors, and MIMO did not always meet expectations.
4. 802.11ac devices became available in 2014 in two waves. Wave 1 devices supported channel bonding up to 80 MHz, and wave 2 devices supported channel bonding up to 160 Mhz.
5. 802.11ac standardized the client feedback format, leading to MU-MIMO. MU-MIMO used the feedback to generate a tailored RF signal for each client device.

PARTICIPATION ACTIVITY 6.3.8: Modern WLAN standards.

1) Which modern IEEE standard offers 600 Mbps bandwidth on both the 2.4 GHz and 5 GHz bands?
   - ○ 802.11n
   - ○ 802.11ac
   - ○ 802.11ax

2) Which modern IEEE 802.11 standard offers ~7 Gbps bandwidth on the 5 GHz band?
   - ○ 802.11n
   - ○ 802.11ac
   - ○ 802.11ax

3) Which modern IEEE 802.11 standard offers 11 Gbps bandwidth on the 2.4

GHz and 5 GHz bands?

- 802.11n
- 802.11ac
- 802.11ax

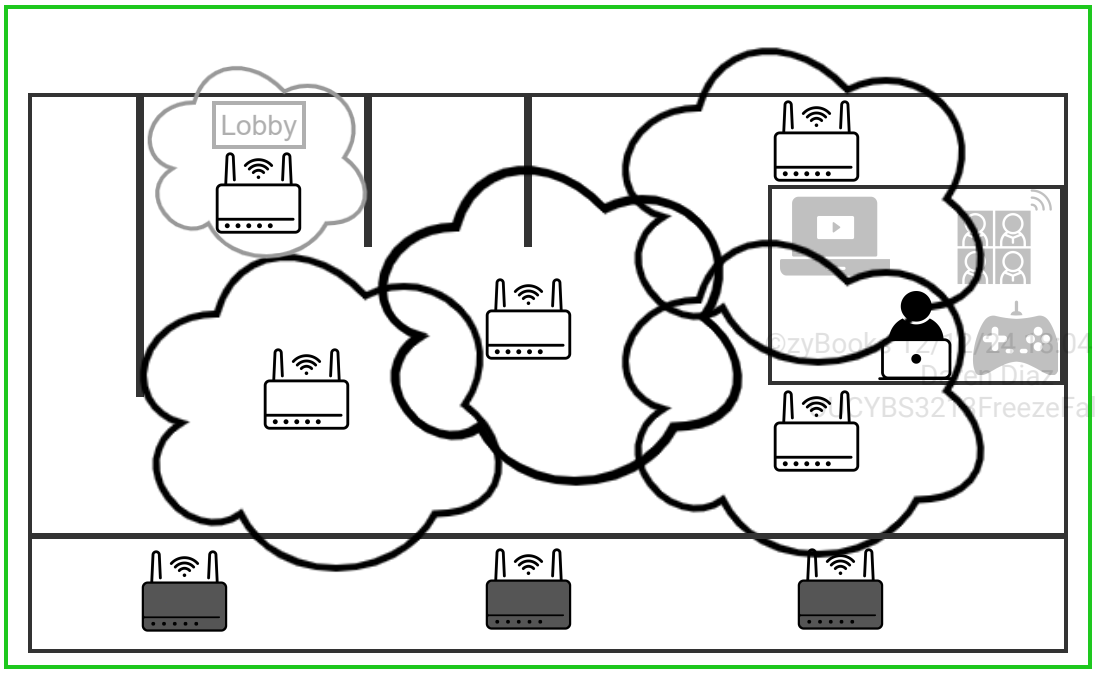
6.4 WLAN design

Site surveys

A ***site survey*** is the process of evaluating RF behavior to achieve roaming, simplify association, and satisfy security requirements. ***Roaming*** is a wireless device's ability to seamlessly maintain association. ***Association*** is a wireless device's ability to discover and connect to a WLAN.

Site surveys are used before, during, and after deploying wireless equipment. Site surveys rely on a combination of hardware, software, and established procedures to ensure a WLAN performs as expected. A ***WiFi analyzer*** is a software-based tool used during a site survey to evaluate RF behavior. A WiFi analyzer can be in an independent tool or part of a site survey application suite. A ***heat map***, or ***heatmap***, is included with most WiFi analyzers to visually represent a WLAN's coverage area.

PARTICIPATION ACTIVITY 6.4.1: Site survey.



Animation content:

Static figure: A floor of an office building with individual rooms. Step 1: A person with a laptop appears in one room and an AP appears in the middle of the office floor. The person walks the entire floor into each room to complete a site survey. Roaming provides seamless WLAN connectivity in desired areas. Association issues occur when a site survey is not completed.A site survey satisfies WLAN roaming and security requirements. Step 2: More devices appear in one room and cloud coverage appears with more access points to cover most areas of the floor. A site survey factors in application resource requirements, or WLAN performance will suffer. Many applications are sensitive to network performance issues. Step 3: Another AP appears in a cloud to cover the lobby area, not covered in step 2. A site survey addresses WLAN physical security through WAP placement, antenna polarization, power level adjustment, wireless client isolation, and guest network isolation. Step 4: Three dark AP's appear in an adjacent area.. A site survey also identifies neighboring WLANs and wireless devices. All noise and interference sources must be identified to mitigate WLAN performance issues.

Animation captions:

1. Roaming provides seamless WLAN connectivity in desired areas. Association issues occur when a site survey is not completed.
2. A site survey factors in application resource requirements, or WLAN performance will suffer. Many applications are sensitive to network performance issues.
3. A site survey addresses WLAN physical security through WAP placement, antenna polarization, power level adjustment, wireless client isolation, and guest network isolation.
4. A site survey also identifies neighboring WLANs and wireless devices. All noise and interference sources must be identified to mitigate WLAN performance issues.

PARTICIPATION ACTIVITY 6.4.2: Site surveys.

1) What software tool is used before, during, and after deploying wireless equipment to ensure a WLAN performs as expected?
   - ○ WiFi analyzer
   - ○ Heat map
   - ○ Site survey

2) What software tool is specifically used to visually represent a WLAN's coverage area?

- WiFi analyzer
- Heat map
- Site survey

3) What term describes a wireless device's ability to maintain connectivity to a WLAN?
   - Association
   - Roaming
   - Isolation

4) What term describes a wireless device's ability to discover and connect to a WLAN?
   - Authentication
   - Authorization
   - Association

WLAN Controller

A ***Wireless LAN (WLAN) controller*** is a network device for controlling Wi-Fi access points in an enterprise network. Advanced WLAN controllers can provide additional security capabilities like intrusion prevention. Smaller networks may not use a WLAN controller.

Two WLAN controller deployment types exist:

- A ***centralized deployment*** consolidates the wireless network which allows for easier upgrading and advanced wireless functionality. Controllers are based on-site and installed in a centralized location. A centralized deployment is used when buildings and networks are close together.
- A ***distributed deployment*** converges wired and wireless on an access switch, and performs both switch and wireless controller roles. Wi-Fi access points provide independent distributed intelligence but work together to provide control mechanisms.

Table 6.4.1: Wi-Fi access point and WLAN controller configuration.

Before deployment, each Wi-Fi access point and the WLAN controller should be configured for security:

Step	Task	Explanation

1	Ensure default settings and passwords are disabled.	Attackers can exploit standard preconfigured passwords and weak protocols to gain device access.
2	Update the firmware and install software patches if available.	Vulnerabilities detected since the device was packaged may have been fixed in a firmware update or software patch.
3	Set up an isolated virtual LAN (VLAN) for remote management.	Isolation is necessary to prevent unauthorized access to management functions, providing an additional layer of security.

PARTICIPATION ACTIVITY 6.4.3: Wi-Fi network installation.

In each scenario, identify which step of the network security configuration process was likely overlooked.

1) A Wi-Fi access point was breached. Investigation revealed that 2 months before the attack the Wi-Fi access point manufacturer had identified a vulnerability and provided a fix.
   - Ensure default settings and passwords are disabled
   - Update the firmware and install software patches if available
   - Set up an isolated virtual LAN (VLAN) for remote management

2) Several weeks after a Wi-Fi network was deployed, an attacker used a password found on a website to gain access to the Wi-Fi access point.
   - Ensure default settings and passwords are disabled
   - Update the firmware and install software patches if available
   - Set up an isolated virtual LAN (VLAN) for remote management

3) An employee was no longer in a wireless administration role, but continued to have access to a Wi-Fi access point.

- Ensure default settings and passwords are disabled
- Update the firmware and install software patches if available
- Set up an isolated virtual LAN (VLAN) for remote management

WLAN Design

A site survey identifies the infrastructure required for a service set and the infrastructure's configurations. A ***service set*** is a group of wireless devices. Three service set types exist:

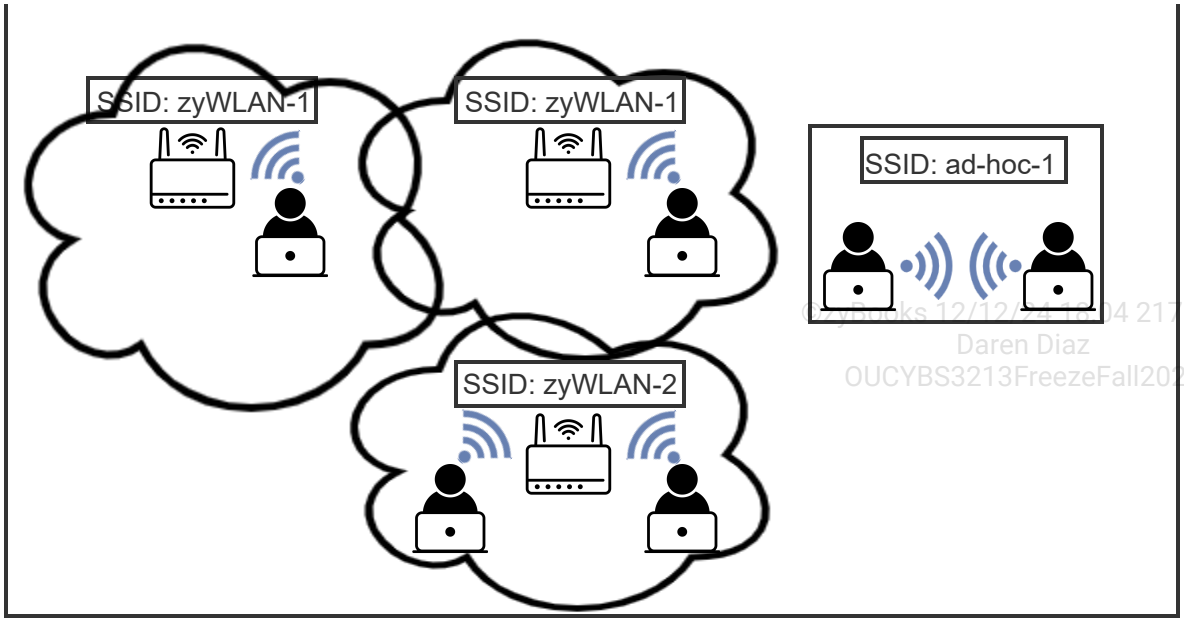
- An ***independent basic service set (IBSS)***, or ad-hoc, is a service set without a WAP.
- A ***basic service set (BSS)*** is a service set with at least one WAP configured with a single SSID.
- An ***extended service set (ESS)*** is a service set with at least two WAPs configured with the same SSID.

A service set identifier (SSID) exists for each service set. A ***service set identifier (SSID)*** is a logical identifier, or name, for a service set. An SSID is a name applied to a BSS or IBSS to help connections.

Other service set identifiers:

- A ***basic service set identifier (BSSID)*** is the WAPs MAC address uniquely identifying the WAP. The SSID keeps the packets within the WLAN, where the BSSID is used in user association. When moving a laptop from one room to another the BSSID will change to the new associated AP, but the SSID remains the same.
- An ***independent service set identifier (IBSSID)*** is the SSID for an IBSS, connecting wireless devices without an AP. IBSS is used when two or more wireless devices want to share or transfer files without connecting to a wireless network provided by an AP.
- An ***extended service set identifier (ESSID)*** is the unique name assigned to all the BSSs in the network. An ESSID is used for a wireless network with multiple WAPs.

PARTICIPATION ACTIVITY 6.4.4: WLAN design.



Animation content:

Static image: A box labeled "SSID: ad-hoc-1" containing two users on laptops. Three clouds. The first cloud is labeled "SSID: zyWLAN-1" and has a WAP and one user on a laptop. The second cloud is labeled "SSID: zyWLAN-1" and has a WAP and one user on a laptop. The third cloud is labeled "SSID: zyWLAN-2" and has a WAP and two users on laptops.
Step 1: An IBSS is formed when a service set device defines an SSID, and other devices associate with the IBSSID. Ad-hoc networks lack the features of other service sets.
A box labeled "SSID: ad-hoc-1" appears containing 2 users on laptops.
Step 2: The SSID is used to connect to the WLAN and the BSSID identifies the individual WAP. The default WAP BSSID is the WAP's NIC MAC address.
A cloud labeled "SSID: zyWLAN-1" appears with 2 users on laptops and a WAP.
Step 3: Many WLANs require multiple WAPs. Each WAP maintains a BSS and BSSID. If WAPs do not share the same SSID, roaming is not possible and an ESS does not exist.
A cloud labeled "SSID: zyWLAN-2" appears with 2 users on laptops and a WAP.
Step 4: An ESS is formed when multiple WAPs share the same SSID. Each device is associated with only one BSS, but can roam among the WAPs with the same SSID.
Another cloud labeled "SSID: zyWLAN-1" appears with a WAP. A user from the other zyWLAN-1 cloud moves to the new cloud.

Animation captions:

1. An IBSS is formed when a service set device defines an SSID, and other devices associate with the IBSSID. Ad-hoc networks lack the features of other service sets.
2. The SSID is used to connect to the WLAN and the BSSID identifies the individual WAP. The default WAP BSSID is the WAP's NIC MAC address.
3. Many WLANs require multiple WAPs. Each WAP maintains a BSS and BSSID. If WAPs do not share the same SSID, roaming is not possible and an ESS does not exist.

4. An ESS is formed when multiple WAPs share the same SSID. Each device is associated with only one BSS, but can roam among the WAPs with the same SSID.

PARTICIPATION ACTIVITY 6.4.5: WLAN design.

1) What is the name for a service set?
   - WLAN
   - SSID
   - MAC

2) What type of service set functions without a WAP?
   - IBSS
   - BSS
   - ESS

3) What type of service set is formed when multiple WAPs are configured with different SSIDs?
   - IBSS
   - BSS
   - ESS

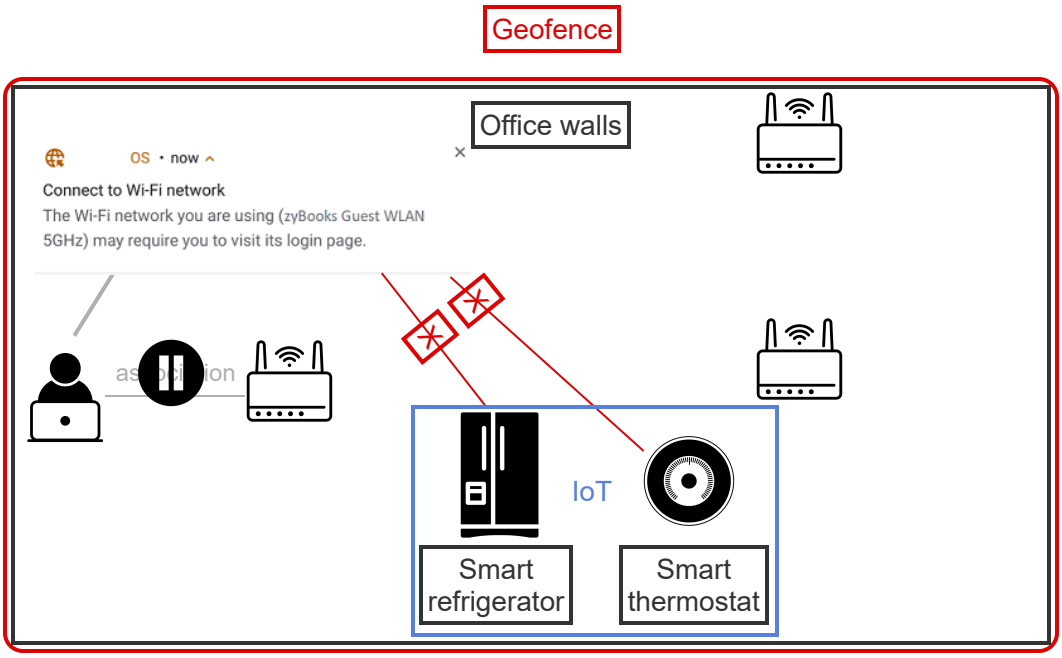
4) What type of service set is formed when multiple WAPs share the same SSID?
   - IBSSID
   - BSSID
   - ESS

WLAN guest access

During a site survey, WLAN guest access requirements are identified so the appropriate security configurations can be made during deployment. A user or device is considered a guest when temporary WLAN access is required, but the user or device must be isolated from the rest of the WLAN infrastructure. Most WLANs are advertised as "open". However, an "open" WLAN may have additional association requirements.

WLAN guest access can be controlled based on the physical characteristics of a user's device, like a device's global positioning system (GPS) coordinates. ***Geofencing*** is the practice of using GPS or radio frequency identification (RFID) to define a virtual perimeter for a geographic boundary. Logical characteristics can also control WLAN guest access. A ***captive portal*** is a basic website a user must open before association with a WLAN is granted. A captive portal website may require users to open a website, agree to an acceptable use policy, and enter user credentials.

PARTICIPATION ACTIVITY 6.4.6: WLAN guest access.



Animation content:

Static image: A large box is labeled "Geofence". Within the Geofence box, a smaller box is labeled "Office walls". The Office walls box contains three WAPs, a user on a laptop, a smart refrigerator, a smart thermostat, and a dialog box that says "Connect to Wi-Fi network. The Wi-Fi network you are using (zyBooks Guest WLAN 5GHz) may require you to visit its login page." The smart refrigerator and the smart thermostat are within a box labeled "IoT" and have red lines with X's connected to the dialog box. The user on a laptop has a connection with a pause symbol connected to one of the WAPs. The user on a laptop has another connection to the dialog box.

Step 1: A geofence enhances a WLAN's security by only allowing access to certain devices from certain physical locations.

A box labeled "Office walls" appears with three WAPs and a user on a laptop. A box labeled "Geofence" appears outside of the Office walls box.

Step 2: A captive portal can function alone or be combined with a geofence to require users to open a website, agree to an acceptable usage policy, and enter user credentials.

A connection labeled "association" appears between the user and one of the WAPs. A pause button

appears over the connection. A dialog box appears that says "Connect to Wi-Fi network. The Wi-Fi network you are using (zyBooks Guest WLAN 5GHz) may require you to visit its login page." A connection appears between the user and the dialog box.
Step 3: A separate configuration is required for a device without a web browser because the device cannot access the captive portal.
A smart refrigerator and a smart thermostat appear. Red connections with X's appear between the smart devices and the dialog box.
Step 4: IoT devices also require special consideration. Many IoT devices lack basic security features and should be isolated from the rest of the WLAN infrastructure.
A box labeled "IoT" appears around the smart refrigerator and the smart thermostat.

Animation captions:

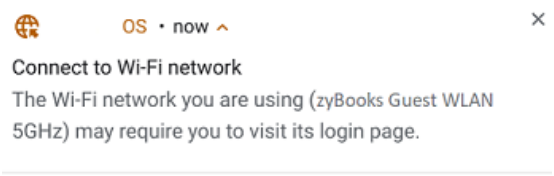
1. A geofence enhances a WLAN's security by only allowing access to certain devices from certain physical locations.
2. A captive portal can function alone or be combined with a geofence to require users to open a website, agree to an acceptable usage policy, and enter user credentials.
3. A separate configuration is required for a device without a web browser because the device cannot access the captive portal.
4. IoT devices also require special consideration. Many IoT devices lack basic security features and should be isolated from the rest of the WLAN infrastructure.

PARTICIPATION ACTIVITY 6.4.7: WLAN guest access.

1) Which WLAN security mechanism enhances physical security by defining a virtual perimeter for a geographic boundary?
   - Geolocation
   - Geotagging
   - Geofencing

2) Which WLAN security mechanism requires a user to visit a specific website prior to gaining access to a WLAN?
   - RADIUS
   - TACACS+
   - Captive portal

3) Refer to the below image. Which security mechanism is the WLAN using?



- Geofencing
- RFID
- Captive portal

4) Which class of device requires special WLAN access considerations because the devices lack basic security features?

- 802.11 devices
- Bluetooth devices
- IoT devices

CHALLENGE ACTIVITY 6.4.1: WLAN design.

581480.4344582.qx3zqy7

Start

What is the service set described in each scenario?

A WAP defines an SSID of "zyWLAN", and a smartphone and a laptop associate with the zyW

Pick

Two laptops associated without a WAP.

Pick

Multiple WAPs with a shared SSID.

Pick

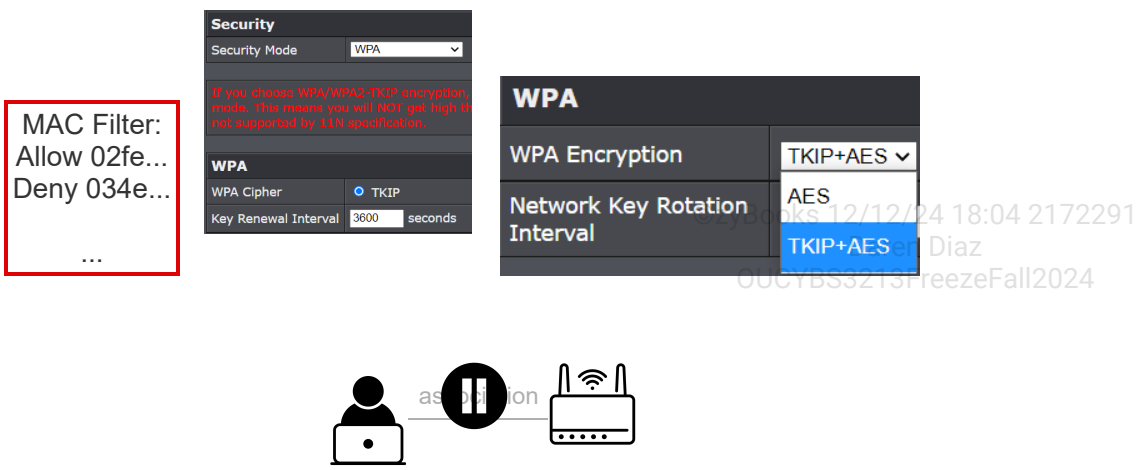
6.5 WLAN security standards

Legacy WLAN security standards

Legacy WLAN security standards exist for backwards compatibility with legacy wireless devices. Many legacy standards are better than the alternative of having no security whatsoever. However, a WLAN deployment should rely on modern security standards when possible.

MAC filtering is a WLAN access control method controlling device access based on MAC address. ***Temporal Key Integrity Protocol (TKIP)*** was an IEEE 802.11 and Wi-Fi Alliance encryption protocol standard that used a unique 128-bit encryption key. ***Wi-Fi Protected Access (WPA)*** is a Wi-Fi Alliance security certification combining PSK with either TKIP or advanced encryption standard (AES).

PARTICIPATION ACTIVITY 6.5.1: Legacy WLAN security standards.



Animation content:

Static image: A box with the text "MAC Filter: Allow 02fe..., Deny 034e..." A Security dialog box showing Security mode WPA and WPA Cipher TKIP. A WPA dialog box showing WPA Encryption TKIP+AES. A user on a laptop with a connection to a WAP. A pause icon is over the connection.
Step 1: A WAP is configured with a MAC filter list of allowed MAC addresses, denied MAC addresses, or both. A spoofed MAC address can easily defeat a MAC filter.
A user on a laptop and a WAP appear. A connection labeled "association" appears between the user and the WAP. A pause symbol appears over the connection and a box with the text "MAC Filter: Allow 02fe..., Deny 034e..." appears over the connection and moves up and to the left.
Step 2: TKIP existed as a standalone placeholder encryption standard until WPA was finalized. TKIP was rolled into WPA, but was deprecated in the 802.11-2012 standard.
A security dialog appears with a box around "WPA Cipher: TKIP".
Step 3: WPA used PSK for device authentication and either TKIP or AES for encryption. WPA was offered in two modes: WPA-personal and WPA-enterprise.
The box moves up to outline "Security Mode: WPA".
Step 4: WPA-personal used PSK and was intended for smaller WLANs. WPA-enterprise used 802.1X/EAP and was intended for larger WLANs.
A WPA dialog box appears showing WPA Encryption TKIP+AES.

Animation captions:

1. A WAP is configured with a MAC filter list of allowed MAC addresses, denied MAC addresses, or both. A spoofed MAC address can easily defeat a MAC filter.
2. TKIP existed as a standalone placeholder encryption standard until WPA was finalized. TKIP was rolled into WPA, but was deprecated in the 802.11-2012 standard.
3. WPA used PSK for device authentication and either TKIP or AES for encryption. WPA was offered in two modes: WPA-personal and WPA-enterprise.
4. WPA-personal used PSK and was intended for smaller WLANs. WPA-enterprise used 802.1X/EAP and was intended for larger WLANs.

PARTICIPATION ACTIVITY 6.5.2: Legacy WLAN security standards.

1) Which WLAN security standard is easily defeated by MAC spoofing?
   - MAC filtering
   - WEP
   - TKIP

2) Which WLAN security standard combines PSK with either TKIP or AES?
   - WEP
   - WPS

- WPA

3) Which WPA mode is intended for small or home-based WLANs?
   - WPA-TKIP
   - WPA-enterprise
   - WPA-personal

4) Which encryption standard is considered the most secure?
   - RC4
   - TKIP
   - AES

Modern WLAN security standards

Modern WLAN security standards should be used when possible to avoid the weaknesses of legacy WLAN security standards. Newer WPA versions enhanced the protections introduced by the original versions by leveraging more advanced encryption standards. ***WPA2 (Wi-Fi protected access 2)*** is the second version of the Wi-Fi Alliance's security certification combining PSK or 802.1X/EAP with AES. ***Advanced Encryption Standard (AES)*** is a block cipher encryption algorithm with a key length of 128 bits, 192 bits, or 256 bits. ***Counter Mode CBC-MAC Protocol (CCMP)***, also known as ***AES CCMP***, is the encryption mechanism used with WPA2 wireless networks. CCMP has replaced TKIP.

WPA3 improves on WPA2 in the following ways:

- Uses 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Uses 384-bit Hashed Message Authentication Mode for transferring encryption keys.
- Uses Wi-Fi Device Provisioning Protocol (DPP) to transmit access to the system without transmitting the password.

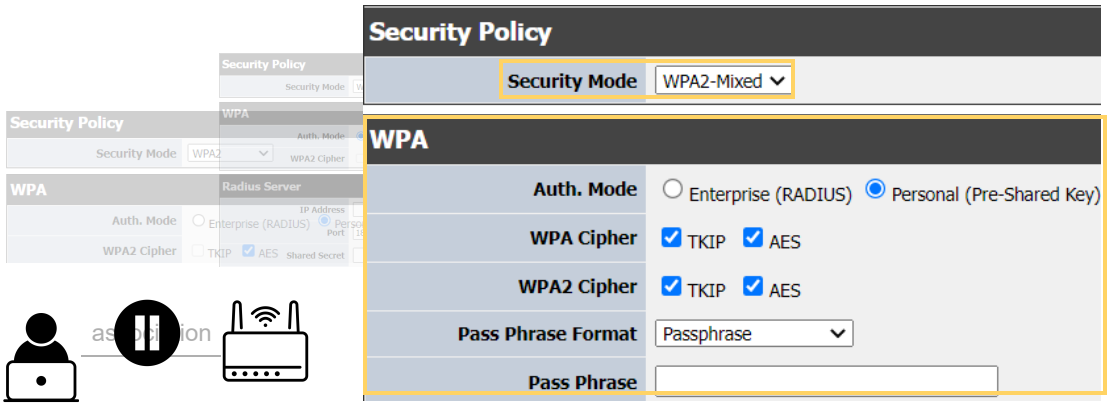
Forms of WPA3:

- Wi-Fi enhanced open
- WPA3-Personal
- WPA3-Enterprise

Wi-Fi enhanced open provides encryption using opportunistic wireless encryption. ***Opportunistic wireless encryption (OWE)*** is a Wi-Fi standard ensuring protected communication between each pair of endpoints by adding encryption. OWE allows for network access without a password.

WPA3 Personal uses passphrase-based authentication and offers a familiar user experience but a superior level of protection against brute force cracking using SAE. ***Simultaneous Authentication of Equals (SAE)*** is a secure key exchange protocol. WPA3 SAE replaces the Pre-Shared Key (PSK) authentication method used in previous versions of WPA to generate a key that's completely unique to each authentication.

PARTICIPATION ACTIVITY 6.5.3: WPA2.



Animation content:

Static image: A user on a laptop connected to a WAP. The connection has a pause symbol over it. A Security Policy dialog box with an outline around "Security Mode: WPA2-Mixed". A WPA dialog box that shows "Auth. Mode: Personal (Pre-Shared Key)", "WPA Cipher: TKIP, AES", "WPA2 Cipher: WKIP, AES" and "Pass Phrase Format: Passphrase".

Step 1: WPA used either TKIP or AES, while WPA2 only uses the more secure AES standard. WPA2-personal is intended for smaller WLAN deployments.

A user on a laptop and a WAP. A connection labeled "association" appears between the laptop and the WAP. A pause symbol appears on the connection. A Security Policy dialog box appears with "Security Mode: WPA2" outlined. A WPA dialog box appears with "Auth. Mode: Personal (Pre-Shared Key)" and "WPA2 Cipher: AES" outlined.

Step 2: Since enterprise WLANs are larger and have stricter security requirements, WPA2-enterprise uses 802.1X/EAP for authentication and AES for encryption.

The previous dialog boxes fade and new dialog boxes appear. The new Security Policy dialog box outlines "Security Mode: WPA2". The new WPA dialog box outlines "Auth. Mode: Enterprise (RADIUS)". A new Radius Server dialog box appears.

Step 3: WPA2-mixed allows both WPA and WPA2 clients to use a common PSK. WPA2-mixed is not an official term used by the IEEE or Wi-Fi Alliance.
Previous dialog boxes fade. The new Security Policy dialog box outlines "Security Mode: WPA2-Mixed". The new WPA dialog box shows "Auth. Mode: Personal (Pre-Shared Key)", "WPA Cipher: TKIP, AES", "WPA2 Cipher: WKIP, AES" and "Pass Phrase Format: Passphrase".

Animation captions:

1. WPA used either TKIP or AES, while WPA2 only uses the more secure AES standard. WPA2-personal is intended for smaller WLAN deployments.
2. Since enterprise WLANs are larger and have stricter security requirements, WPA2-enterprise uses 802.1X/EAP for authentication and AES for encryption.
3. WPA2-mixed allows both WPA and WPA2 clients to use a common PSK. WPA2-mixed is not an official term used by the IEEE or Wi-Fi Alliance.

PARTICIPATION ACTIVITY 6.5.4: Modern WLAN Security Standards.

Which WPA2 usage mode is the most appropriate for the following WLANs?

1) A school WLAN intended for student use.
   - Open
   - WPA2-personal
   - WPA2-enterprise

2) A members-only WLAN for a gym.
   - Open
   - WPA2-personal
   - WPA2-enterprise

3) An airport WLAN for passengers waiting for flights.
   - Open
   - WPA2-personal
   - WPA2-enterprise

4) A WLAN located in someone's home.
   - Open
   - WPA2-personal
   - WPA2-enterprise

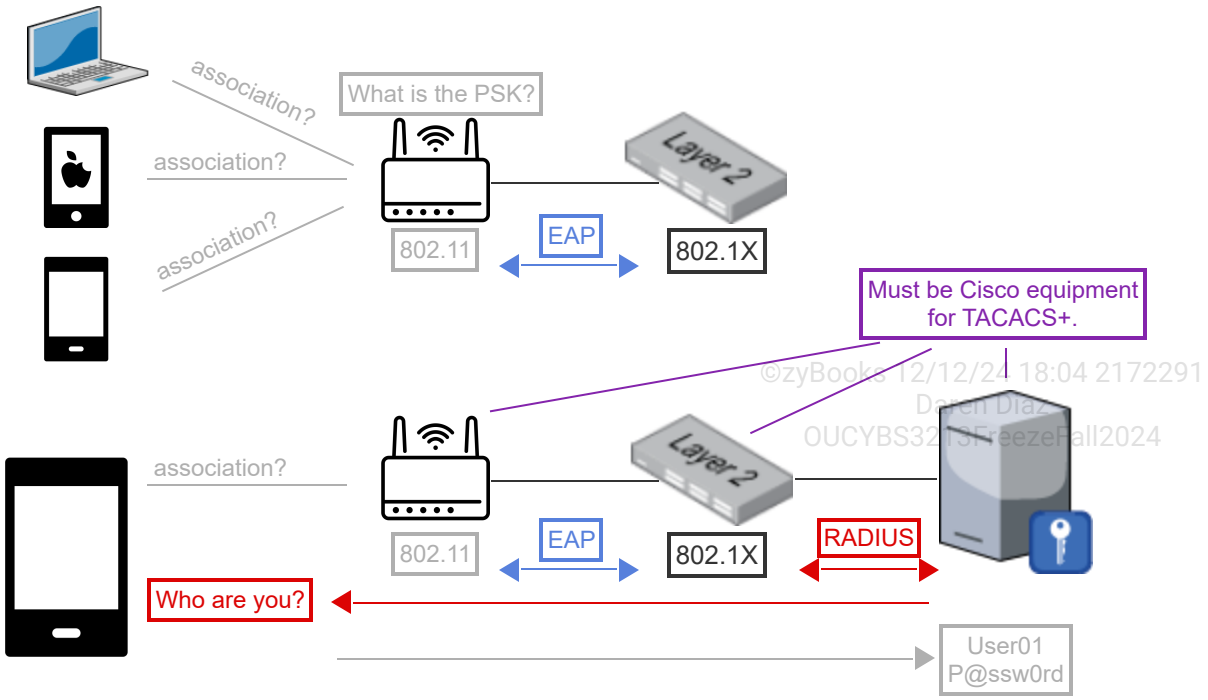
6.6 WLAN authentication and attacks

WLAN authentication

WLAN authentication can verify the identity of a user, a device, or both prior to allowing association with a WLAN. WLAN authentication can occur locally on a WAP or a WAP can forward a user's claim to a centralized server. Five primary authentication options exist for a WLAN:

- ***Pre-shared key (PSK)*** is a shared credential used for device authentication.
- ***Extensible Authentication Protocol (EAP)*** is an authentication framework for transporting different types of authentication protocols.
- ***IEEE 802.1X*** is an IEEE standard for port-based access control.
- ***Remote Authentication Dial-In User Service (RADIUS)*** is a networking protocol for centralized authentication, authorization, and accounting (AAA) services.
- ***Terminal Access Controller Access-Control System Plus (TACACS+)*** is a proprietary networking protocol developed by Cisco for centralized authentication, authorization, accounting, and auditing (AAAA) services.

PARTICIPATION ACTIVITY 6.6.1: WLAN authentication options.



Animation content:

Static image: Two groups of device connections. The first group shows a laptop, a smartphone, and a tablet connected to a WAP. The connections are labeled "association?" The WAP is labeled "What is the PSK?" and "802.11". The WAP connects to a switch labeled "Layer 2" and "802.1X". A two-way arrow labeled "EAP" spans the length of the connection between the WAP and the switch. The second group of devices shows a tablet connected to a WAP. The connection is labeled "association?" The WAP is labeled "802.11". The WAP is connected to a switch labeled "Layer 2" and "802.1X". A two-way arrow labeled "EAP" spans the length of the connection between the WAP and the switch. The switch is connected to a RADIUS server. A two-way arrow labeled "RADIUS" spans the length of the connection between the switch and the RADIUS server. The label "Must be Cisco equipment for TACACS+" points to the WAP, switch, and RADIUS server. An arrow labeled "Who are you?" points from the RADIUS server to the tablet. An arrow labeled "User01, P@ssw0rd" points from the tablet to the RADIUS server.

Step 1: PSK is a viable option for a small office and home WLANs. A weakness of PSK is the shared credential is no longer secret once a party knows what the credential is.

A WAP appears connected to a server labeled "Layer 2". A laptop, a smartphone, and a tablet appear. Connections appear between the devices and the WAP. The connections are labeled "association?" "What is the PSK?" appears above the WAP.

Step 2: 802.1X provides port-based access control, but lacks a method for wireless clients to submit credentials. EAP is combined with 802.1X to extend 802.1X to a WLAN.

"802.11" appears under the WAP. "802.1X" appears below the switch. A two-way arrow labeled "EAP" appears between the "802.11" and "802.1X" labels.

Step 3: EAP requires a RADIUS device. Some WAPs function as both a WAP and a RADIUS device; but, most WLANs make use of a dedicated RADIUS server.

A copy of the WAP, layer 2 switch, "802.11", "802.1X", and "EAP" arrows appears. Another tablet appears. A RADIUS server appears connected to the layer 2 switch. A two-way arrow labeled "RADIUS" appears between the layer 2 switch and the RADIUS device. The message "Who are you?" moves from the RADIUS server to the tablet. The message "User01, P@ssw0rd" moves from the tablet to the RADIUS server.

Step 4: RADIUS is an open version of TACACS+; but, TACACS+ is considered a more robust security option. Cisco wireless equipment is required for TACACS+.

"Must be Cisco equipment for TACACS+" appears and points to the RADIUS server, the layer 2 switch, and the WAP.

Animation captions:

1. PSK is a viable option for a small office and home WLANs. A weakness of PSK is the shared credential is no longer secret once a party knows what the credential is.
2. 802.1X provides port-based access control, but lacks a method for wireless clients to submit credentials. EAP is combined with 802.1X to extend 802.1X to a WLAN.
3. EAP requires a RADIUS device. Some WAPs function as both a WAP and a RADIUS device; but, most WLANs make use of a dedicated RADIUS server.

4. RADIUS is an open version of TACACS+; but, TACACS+ is considered a more robust security option. Cisco wireless equipment is required for TACACS+.

PARTICIPATION ACTIVITY 6.6.2: WLAN Authentication.

1) Which WLAN authentication option is suitable for a small office or home WLAN?
   - PSK
   - RADIUS
   - TACACS+

2) Which WLAN authentication option is an open standard designed to centralize AAA services?
   - PSK
   - RADIUS
   - TACACS+

3) Which WLAN authentication option is considered the most robust?
   - PSK
   - RADIUS
   - TACACS+

4) Which standard is required to extend RADIUS or TACACS+ authentication to a WLAN?
   - PSK
   - 802.1X
   - EAP

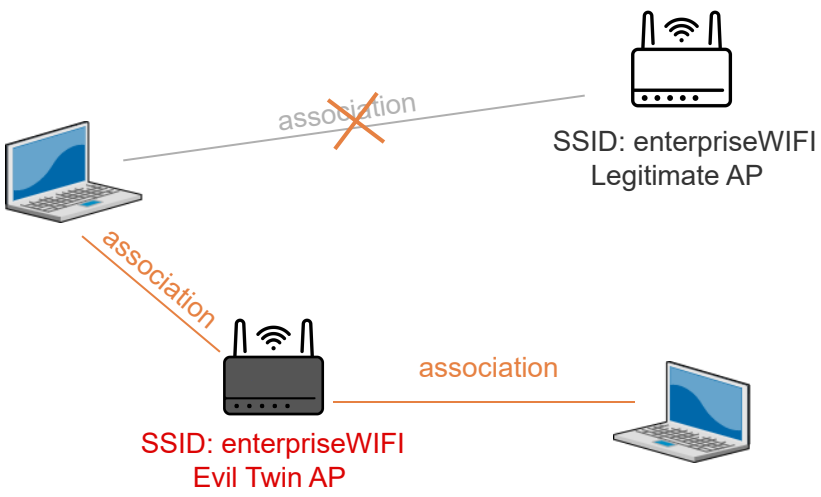
Spoofing

Both a rogue AP and an evil twin can be considered spoofing. ***Spoofing*** is the act of a user or device impersonating another user or device to gain access to systems, steal data, steal money, or spread malware. A ***rogue AP*** is a WAP that is in range of a WLAN, but does not belong to the entity controlling the WLAN. A rogue AP is not inherently malicious. However, the term usually refers to a WAP engaged

in malicious activity. An ***evil twin attack*** is when an attacker presents a fake WAP, also known as an evil twin AP, and tricks a user's device into associating with the evil twin's AP.

Many vendors offer a wireless intrusion prevention system to help mitigate spoofing. A ***wireless intrusion prevention system (WIPS)*** is a WLAN monitoring device or service able to detect and prevent intrusions. Ex: A WIPS can detect an evil twin, quarantine the evil twin, and prevent devices from associating with the evil twin.

PARTICIPATION ACTIVITY 6.6.3: Rogue AP and evil twin attack.



Rogue AP and evil twin attack.

Animation content:

Static image: A laptop is connected to a WAP labeled "SSID: enterpriseWIFI, Legitimate AP". The connection is crossed out, and the laptop is connected to a second WAP labeled "SSID: enterpriseWIFI, Evil Twin AP". A second laptop is also connected to the Evil Twin AP.

Animation captions:

1. A laptop is associated with a WAP with the SSID "enterpriseWIFI".
2. In an evil twin attack, an attacker introduces a WAP with the same SSID as a legitimate WAP. The attacker's WAP is also considered a rogue AP.
3. Once the attacker configures their WAP with the same SSID as a legitimate WAP, the attacker's fake WAP is considered an evil twin AP instead of a rogue AP.
4. The attacker's goal is to disassociate the laptop from the legitimate WAP or simply wait for an unaware user to associate with the evil twin AP.
5. Wireless devices usually connect to an SSID with the best signal quality. An attacker may boost an evil twin's AP power to make the signal quality more enticing.

PARTICIPATION ACTIVITY 6.6.4: Spoofing.

1) Which type of attack has a user or device impersonate another user or device?
   - Poisoning
   - Hacking
   - Spoofing

2) Which spoofing type involves an external WAP with or without malicious intent?
   - Rogue AP
   - Evil twin
   - Deauthentication

3) Which attack type involves an illegitimate WAP impersonating a legitimate WAP?
   - Rogue AP
   - Evil twin
   - DNS spoofing attack

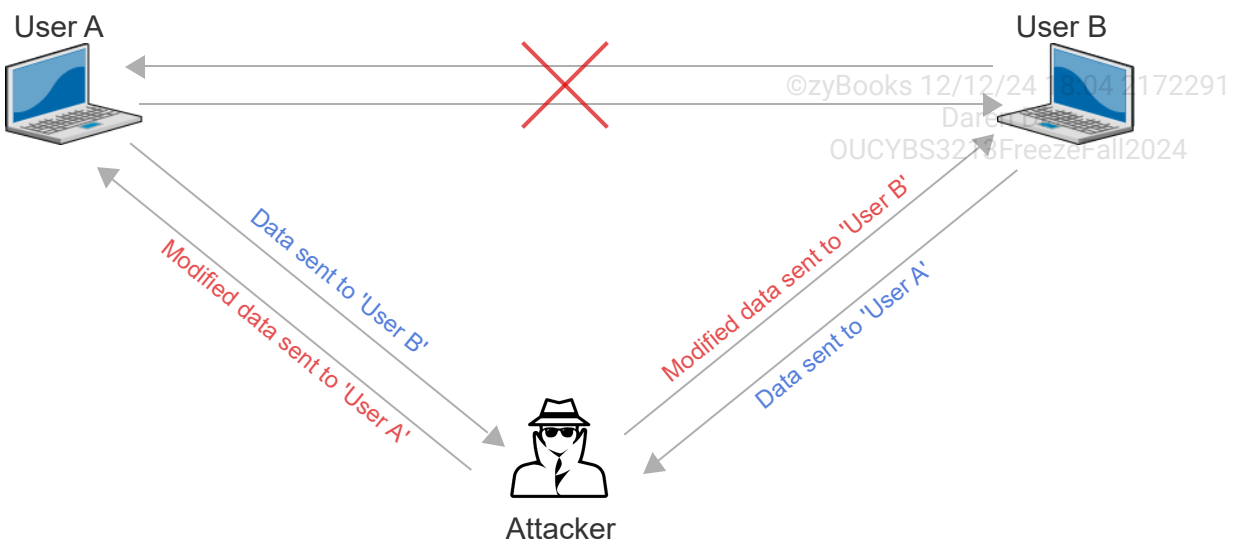
4) What is used to mitigate wireless spoofing?
   - WPA
   - WEP
   - WIPS

On-path attacks

An ***on-path attack*** is an attack where an attacker eavesdrops or modifies the communications between two parties. In an on-path attack, both parties are unknowingly in communication with an attacker. An on-path attack can be used as a vector for other attack types. Ex: An on-path attack intercepts and modifies a user's DNS query as part of a DNS poisoning attack. ***DNS poisoning*** is an attack used to redirect a user to a malicious website by modifying the user's DNS query.

An on-path attack can be mitigated by use of a secure channel. A ***secure channel*** is a communication channel that guarantees data authenticity and data confidentiality.

PARTICIPATION ACTIVITY | 6.6.5: On-path attack.



Animation content:

Static image: A computer labeled "User A", a computer labeled "User B", and an icon labeled "Attacker". An arrow points from User A to User B. An arrow points from User B to User A. A red "X" is on both arrows. An arrow labeled "Data sent to User B" points from User A to the Attacker. An arrow labeled "Modified data sent to User B" points from the Attacker to User B. An arrow labeled "Data sent to User A" points from User B to the Attacker. An arrow labeled "Modified data sent to User A" points from the Attacker to User A.

Animation captions:

1. An attacker intercepts communication between two parties and creates a separate connection to each party.
2. The attacker intercepts the data sent from 'User A' to 'User B', modifies the data, and sends the modified data to 'User B'.
3. The attacker intercepts the data sent from 'User B' to 'User A', modifies the data, and sends the modified data to 'User A'.

PARTICIPATION ACTIVITY | 6.6.6: On-path attacks.

1) A(n) _____ attack is an attack in which an attacker eavesdrops or modifies communications between two parties.

- rogue AP
- on-path
- secure channel

2) What is used to mitigate an on-path attack?

- DNS poisoning
- Rogue AP
- Secure channel

3) Which attack type uses an on-path attack as a vector?

- Evil twin
- Rogue AP
- DNS poisoning

4) What attack type eavesdrops the communications between two parties?

- ARP poisoning
- On-path attack
- Evil twin

Deauthentication attack

A WLAN user typically undergoes authentication prior to associating with a WLAN. ***Authentication*** is the act of verifying or proving a user's claim to an identity. Authentication may require a user to provide a shared password or a unique login credential. An authenticated user is fully associated with a WLAN and can access protected network resources. An attacker can deauthenticate a WLAN user to hijack a user's authenticated session or deny service to the WLAN. ***Deauthentication*** is an attack where a user's authentication is invalidated.

PARTICIPATION ACTIVITY 6.6.7: Deauthentication (detauth) attack.

Animation content:

Static image: A laptop labeled "MAC: A0-CA-C8-13-C1-35" connects to a WAP. A red X is on the connection. An attacker has an arrow labeled "deauth: (MAC: A0-CA-C8-13-C1-35)" pointing to the WAP.

.

Animation captions:

1. A laptop is associated with a WAP using the laptop's MAC address. The WAP prevents multiple devices from using the same MAC address.
2. An attacker sends a deauthentication message to the WAP with a spoofed version of the laptop's MAC address, forcing the WAP to deauthenticate the laptop.
3. The attacker now has an opening to launch an evil twin attack, a DoS attack, or another attack type.

PARTICIPATION ACTIVITY | 6.6.8: Deauthentication attack.

1) What is typically the first requirement for WLAN client association?
   - Authorization
   - Authentication
   - Accounting

2) Which attack type invalidates a user's authentication?
   - Deauthentication
   - Evil twin
   - Rogue AP

3) What identifying characteristic is used in a deauthentication attack?
   - IP address

- MAC address
- URL

4) Which activity verifies a user's claim to an identity?

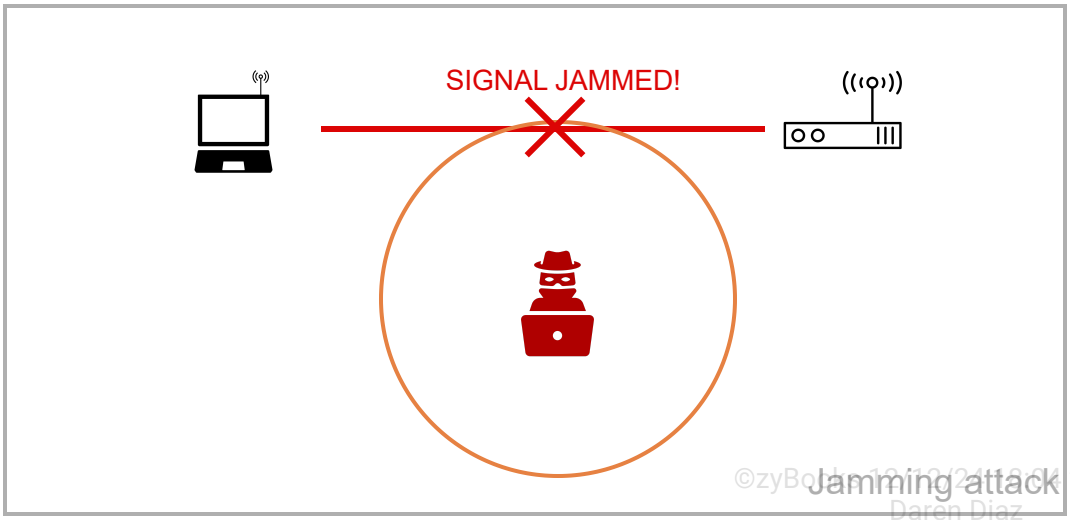
- Authorization
- Auditing
- Authentication

Jamming

Jamming is an attack in which a high power "loud" signal is used to drown out or jam the legitimate communication signal. Jamming is not difficult or expensive to accomplish.

Jamming is a type of Denial of Service (DoS) attack which interferes with the transmission channels by continuously sending useless packets to interrupt the communication between legitimate nodes. Jamming could lead to ways of mounting a channel-based on-path attack against WPA's Temporal Key Integrity Protocol (TKIP).

PARTICIPATION ACTIVITY 6.6.9: Wi-Fi attacks: Deauthing and jamming.



Animation content:

Static image: A laptop connects to a WAP. An attacker is surrounded by a circle that overlaps the connection between the laptop and the WAP. A red X labeled "SIGNAL JAMMED!" is on the connection between the laptop and the WAP.

Animation captions:

1. In a jamming attack, an attacker tries to disrupt communication between a laptop and an AP with a "loud" signal.
2. To jam a signal, an attacker introduces a high powered signal between a laptop and an AP.

PARTICIPATION ACTIVITY | 6.6.10: Wi-Fi attacks.

How to use this tool

Evil twin attack **Deauth attack** **Jamming attack**

	An attacker fools a user into associating with the attacker's access point.
	An attacker uses a high power signal to disrupt Wi-Fi communications.
	An attacker falsifies a deauth message with a device's MAC address resulting in the device getting disassociated from an access point.

Reset

PARTICIPATION ACTIVITY | 6.6.11: Wi-Fi attacks.

1) The SSID is used in a deauthentication (deauth) attack.
   - ○ True
   - ○ False

2) An evil twin attack works because a user device, like a laptop, is fooled by an attacker's access point having the same SSID as the legitimate network.
   - ○ True

- False

3) A jamming attack is possible in Wi-Fi networks and not other wireless networks.

- True
- False

CHALLENGE ACTIVITY 6.6.1: WLAN authentication and attacks.

581480.4344582.qx3zqy7

Start

Which authentication option is described in each scenario?

Pick 1) Provides an open standard WLAN authentication option designed to centralize AAA services

Pick 2) Provides a WLAN authentication option suitable for a small office or home WLAN

Pick 3) Provides the most robust WLAN authentication option

1 2 3

Check Next

6.7 Bluetooth security

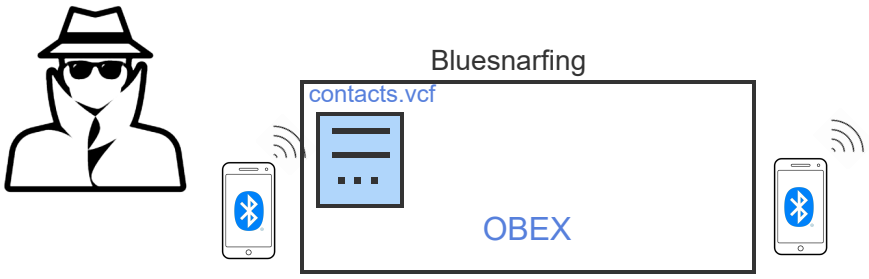
Bluetooth attacks

Bluejacking is an attack where an attacker sends an unsolicited prank message to a nearby Bluetooth enabled device.

Bluesnarfing is an attack where an attacker connects to a Bluetooth device and downloads files without a user's knowledge. In some bluesnarfing attacks, an attacker may be able to change files as well. A bluesnarfing attack is carried out by using Bluetooth's Object Exchange (OBEX) protocol. The ***Object Exchange protocol (OBEX)*** is a protocol for transferring information, like pictures and contacts, over a Bluetooth connection.

Bluebugging is an attack where an attacker takes control of a target device to eavesdrop or forward calls to the attacker's device. Bluebugging is so called because of the eavesdropping or bugging capability.

PARTICIPATION ACTIVITY 6.7.1: Bluesnarfing.



In a bluesnarfing attack an attacker gains unauthorized access to a nearby device's data using Bluetooth. This data may include contacts, pictures, and other files.

Animation content:

Static image: An attacker, two smartphones with Bluetooth symbols, and a box labeled "Bluesnarfing". A box labeled "contacts.vcf" and the text "OBEX" are in the Bluesnarfing box.
Step 1: In a bluesnarfing or bluejacking attack, an attacker uses a Bluetooth capable device, usually

a smartphone.
An attacker and a smartphone with a Bluetooth symbol appear.
Step 2: In bluejacking, the attacker creates a new contact, but does not add contact details. Instead, the attacker adds a prank message.
The text "New contact" appears below the smartphone. A box with the text "You have been hacked!" appears below "New contact".
Step 3: Bluejacking scans for nearby Bluetooth devices, and sends the new contact to the scanned Bluetooth device.
A second smartphone with a Bluetooth symbol appears. A wireless signal moves outward from the attacker's smartphone toward the new smartphone. The text "contact" moves from the attacker's smartphone to the new smartphone. The text "Received contact" and a box with the text "You have been hacked!" appear below the new smartphone.
Step 4: If the attacker finds a Bluetooth device that is in "discoverable" mode within range the attacker can launch a bluesnarfing attack.
The new message and received messages disappear. The wireless signal reappears moving outwardly from the attacker's smartphone to the second smartphone.
Step 5: A bluesnarfing attack uses the OBEX protocol to attack a discovered device. An OBEX GET message is sent with a filename request. Ex: Get "contacts.vcf"
The wireless signal disappears. A box labeled "Bluesnarfing" appears between the two smartphones. An arrow labeled "GET contacts.vcf" moves within the Bluesnarfing box from the attacker's smartphone to the second smartphone. The text "OBEX" appears in the Bluesnarfing box. A box labeled "contacts.vcf" moves within the Bluesnarfing box from the second smartphone to the attacker's smartphone.

Animation captions:

1. In a bluesnarfing or bluejacking attack, an attacker uses a Bluetooth capable device, usually a smartphone.
2. In bluejacking, the attacker creates a new contact, but does not add contact details. Instead, the attacker adds a prank message.
3. Bluejacking scans for nearby Bluetooth devices, and sends the new contact to the scanned Bluetooth device.
4. If the attacker finds a Bluetooth device that is in "discoverable" mode within range the attacker can launch a bluesnarfing attack.
5. A bluesnarfing attack uses the OBEX protocol to attack a discovered device. An OBEX GET message is sent with a filename request. Ex: Get "contacts.vcf"

PARTICIPATION ACTIVITY 6.7.2: Bluetooth security.

How to use this tool

Bluebugging | Bluejacking | Bluesnarfing

	An attack type in which an attacker can listen to a target's calls.
	An attack type in which an attacker sends an unexpected message in the form of a contact to a target device.
	An attack type in which an attacker steals files from a target user device utilizing Bluetooth.

Reset

Preventing Bluetooth attacks

Bluetooth attacks, like bluejacking and bluesnarfing, can be easily prevented. Bluetooth attacks often make use of Bluetooth's discoverable mode. When a device is discoverable, the device sends a Bluetooth broadcast message to nearby devices containing the device's MAC address and name.

PARTICIPATION ACTIVITY 6.7.3: Preventing Bluetooth attacks.

Steps towards preventing Bluetooth attacks.

Animation content:

Static image: A smartphone with a green Bluetooth symbol.
Step 1: Bluetooth should be turned off when not in use. Bluetooth attacks are not possible if Bluetooth is disabled.
A smartphone with a blue Bluetooth symbol appears. The blue Bluetooth symbol changes from blue to gray.
Step 2: Devices should only be discoverable during pairing and not otherwise. Most attacks are launched by an attacker finding a device that is discoverable.

The Bluetooth symbol disappears. The text "myDevice" appears above the smartphone. A red X appears over the text.
Step 3: The preset default PIN should be changed. Default PINs for most manufacturers are well-known by attackers.
The text "PIN: 1234" appears on the smartphone's screen. The "1234" is changed to "5937".
Step 4: Bluejacking and bluesnarfing are no longer possible with Bluetooth version 5 or patched older Bluetooth versions.
The text disappears from the smartphone's screen. The text "Check for updates?" appears on the screen. The text is changed to "Update now?" The text disappears, and a green Bluetooth symbol appears on the screen.

Animation captions:

1. Bluetooth should be turned off when not in use. Bluetooth attacks are not possible if Bluetooth is disabled.
2. Devices should only be discoverable during pairing and not otherwise. Most attacks are launched by an attacker finding a device that is discoverable.
3. The preset default PIN should be changed. Default PINs for most manufacturers are well-known by attackers.
4. Bluejacking and bluesnarfing are no longer possible with Bluetooth version 5 or patched older Bluetooth versions.

PARTICIPATION ACTIVITY 6.7.4: Preventing Bluetooth attacks.

1) To prevent Bluetooth attacks, what should be done when a device is not actively using Bluetooth?

   - Device should be turned off
   - Bluetooth should be turned off
   - No action is necessary

2) What action should be taken to prevent a Bluesnarfing attack?

   - Device should be turned off

- Bluetooth should be turned off
- Make the Bluetooth device non-discoverable

3) In addition to turning off Bluetooth when not in use and setting a device to be non-discoverable, how can a Bluetooth device's security be maintained?
   - Update Bluetooth software and drivers
   - Use Wi-Fi instead of Bluetooth
   - Replace the device with a new device

6.8 Embedded systems

Embedded systems

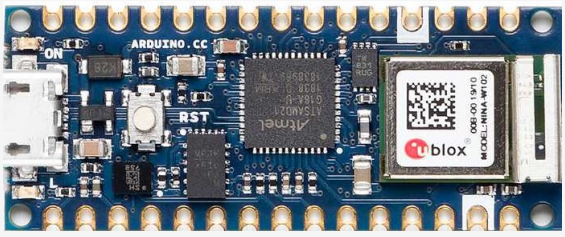
An ***embedded system*** is a specialized computer system built into a larger system and used to control certain functions of the larger system. An embedded system has hardware and software to accomplish a specific task.

Custom firmware, also known as ***aftermarket firmware***, is an unofficial new or modified version of firmware created by third parties for devices to provide new features or to unlock hidden functionality. Ex: Video game consoles use custom firmware. ***Over-the-air (OTA) firmware*** is the wireless delivery of new software or firmware to mobile or embedded devices. OTA has the ability to add new software features to a product after a device has been deployed in the field to improve functionality over time and rapidly respond to bugs and security vulnerabilities.

Many embedded system application's operations have time constraints. A ***real-time operating system (RTOS)*** is an operating system that prioritizes data processing so a system can respond to changes within a limited time frame. RTOS performs repeated tasks within a tight time boundary. A ***baseband processor (BP)*** is a network interface controller chip that manages all of an antenna's radio functions. Baseband processors run a RTOS as firmware. Ex: iPhones

The table below lists some common embedded systems.

Table 6.8.1: Common embedded systems.

System	Capabilities	Security Considerations
Raspberry Pi - Single-board computer  Image source: https://www.unsplash.com/photos/jvHymbpto1E	• Performs typical PC functions with a less powerful microprocessor • Runs Linux	• Networking vulnerability • The OS, can be easily modified, if an attacker gets physical access • The Linux distributed OS can be *hardened*
Arduino - Microcontroller  Image source: https://www.arduino.cc/	• Limited capabilities. Arduino runs a single program at a time from onboard storage • Standard I/O includes USB • Networking can be added	• USB interface can be exploited • The attack surface is increased if networking capabilities are added • Limited capabilities mean limited damage in case of an attack

©zyBooks 12/12/24 18:04 2172291
Daren Diaz
OUCYBS3213FreezeFall2024

Field Programmable Gate Array (FPGA) - Reconfigurable computing device  Image source: Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons)	• Pre-programmable integrated circuit that is customized to perform a specialized function • An FPGA can be reprogrammed	• An attacker could reprogram a FPGA • Threat is limited by the capabilities of FPGAs

PARTICIPATION ACTIVITY 6.8.1: Embedded systems security constraints.

1) Why can't advanced security software be installed on most embedded systems?

   - An embedded system may not have network capability.
   - An embedded system may not support the programming environment needed to run advanced security software.
   - An embedded system has limited computational power, memory, and storage.

2) What are the security implications for an embedded system with limited network connectivity?

   - Delivering patches and software updates is difficult.
   - No network access means no attacks.
   - Impossible to manage and update an embedded system.

3) When replacing a compromised embedded system, which embedded

system characteristic can cause a problem?

- Embedded systems low-cost
- Embedded systems are often built into a larger system
- Embedded systems is a simple computational device that performs limited functions

Internet of Things

The ***Internet of Things (IoT)*** refers to Internet-connected devices and systems that are used in a variety of sensing and automation applications. Ex: Smart home devices like Google Nest and Ring Video Doorbell are IoT devices. Embedded systems make up a majority of IoT devices in use today.

Facility automation refers to devices and systems that enable automation of routine tasks at a facility. Facility automation systems use IoT devices such as sensors as part of the system. Ex: Security camera.

Common IoT devices include:

- A ***sensor*** is a device measuring a physical property. Ex: Temperature or humidity. A sensor is an IoT device when using the internet to report measurements back to some central location
- A ***smart device*** is an internet-connected device capable of data processing and is user customizable through the installation of apps and other software. Ex: Smartphone.
- A ***wearable*** is a device that is worn by an individual. A wearable may also offer smart device capabilities. Ex: Smartwatch.

Table 6.8.2: IoT device security concerns.

Sensors	Smart device	Wearable
Sensor measurements are vulnerable to attacks Some HVAC sensors communicate with insecure building protocols.	Dangerous if lost or stolen Bluetooth exposure attacks Exposure reduced by traffic separation	Network data exposure must be reviewed and mitigated Data exposure to third parties Banned by US military because of GPS capability

PARTICIPATION ACTIVITY 6.8.2: IoT devices.

How to use this tool

Smart device **Wearable** **Facility automation** **Sensor**

	An IoT device used to measure a physical property.
	An IoT device worn by an individual.
	An IoT device that is internet connected, capable of data processing, and is user-customizable through apps.
	An IoT device used to monitor or control the operation of a facility.

Reset

IoT security considerations

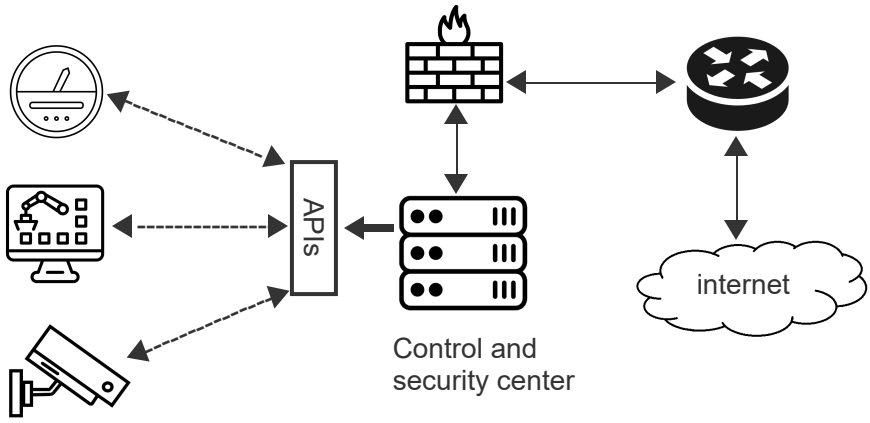
In traditional computing devices such as a PC or server, the hardware and software can be carefully controlled by a security professional at an organization. An IoT device such as a wearable or smart

device may be brought into a workplace by an employee or visitor, and is not under the organization's control.

The following security considerations exist:

- Data handling and storage: An IoT device may send data to the cloud for storage and processing in some applications. Proper vendor data handling and storage is critical.
- Networking: Data in transit is vulnerable. The limited capabilities of some IoT devices can present challenges such as limitations on data encryption.
- Limited hardware and software capabilities: Since IoT devices are simpler than PCs, security capabilities are limited.
- Weak defaults: Vendor provided devices can have security vulnerabilities like default passwords and backdoors.
- Lack of support and software upgrades: Vendors may not provide consistent software patches. Lack of vendor support when problems occur can be a persistent problem.
- Proprietary hardware and software: Hardware and software on PCs and other standard IT equipment can be managed by an organization to have robust security. Vendor devices may have proprietary hardware and software that cannot be managed easily.

PARTICIPATION ACTIVITY 6.8.3: IoT security.



Animation content:

Static image: Three IoT devices with two-way arrows between the IoT devices and a rectangle labeled "APIs". A server labeled "Control and security center" has an arrow pointing to the APIs rectangle and a two-way arrow between the server and a firewall. The firewall has a second two-way arrow between the firewall and a router. The router has another two-way arrow between the router and a cloud labeled "Internet".

Animation captions:

1. A company has multiple IoT devices to control and secure.
2. Control and security center is responsible for software maintenance, configurations, firmware updates, patches, and authentication of tasks.
3. Firewall rules can help with security from outside users and hackers.

PARTICIPATION ACTIVITY 6.8.4: IoT security consideration.

1) How can data in transit be protected?
   - Authentication
   - Encryption
   - Authorization

2) Which of the following components in an IoT application has the most security issues?
   - Network infrastructure
   - Cloud server
   - IoT device

3) Which security issue describes the scenario when an IoT device has the manufacturer preset administrative account password?
   - Limited hardware and software capabilities
   - Proprietary hardware and software
   - Weak defaults

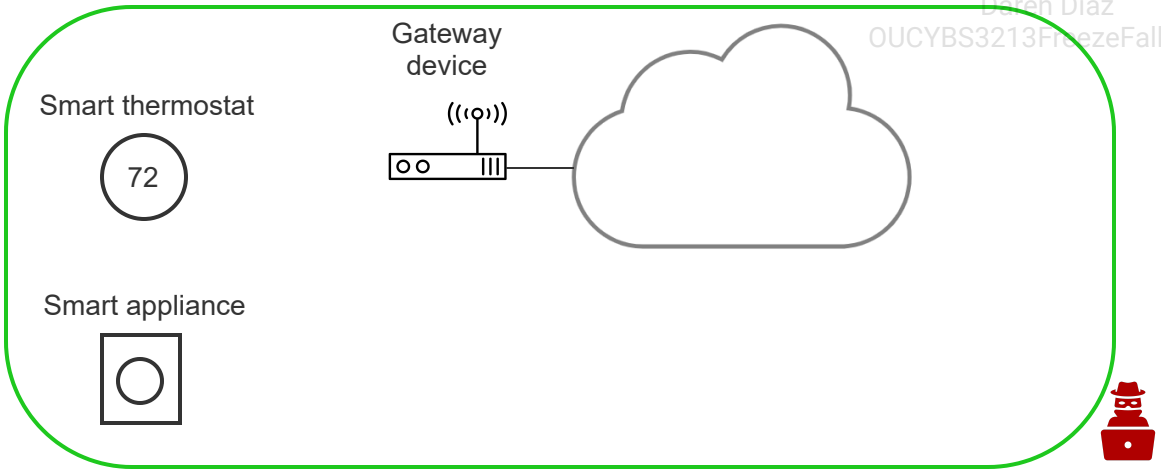
IoT security threats and vulnerabilities

The most common types of attacks on IoT devices are the following:

- A ***Man-In-The-Middle***, or ***MitM*** attack, is an attack in which an attacker eavesdrops or modifies the communications between two parties.
- An ***eavesdropping*** attack is an attack in which data in transit is intercepted by an attacker.
- A ***firmware hijacking*** is a type of attack in which an attacker takes advantage of outdated firmware to take over a device.

- A ***botnet***, short for "robot network", refers to a network of devices that are under the control of an attacker. The attacker can then use the botnet to launch other attacks, such as a DDoS attack.

PARTICIPATION ACTIVITY | 6.8.5: IoT security threats and vulnerabilities.



Animation content:

Static image: A box containing a smart thermostat, a smart appliance, and a device gateway connected to a cloud. An attacker is outside of the box.
Step 1: An IoT device sends data to a gateway. A gateway collects data from one or more IoT devices and sends the data to a cloud server for processing.
A smart thermostat, a smart appliance, and a device gateway connected to a cloud. Green arrows representing data move from the smart devices to the device gateway. A green arrow moves from the device gateway to the cloud.
Step 2: An attacker may have direct physical access to an IoT device.
An attacker appears and moves next to the smart appliance.
Step 3: An attacker may take over a gateway or edge device, opening a range of attacks such as eavesdropping, man-in-the-middle, etc.
The attacker moves next to the gateway device. The gateway device changes from white to red.
Step 4: An attacker can take over multiple IoT devices and gateways to set up a botnet. A botnet can be used to launch DDoS and other attacks.
Two red smart thermostats and two red smart appliances appear around the attacker.
Step 5: The cloud server is a vulnerability, especially if the server is vendor hosted. Poor security at the vendor end can mean an opening for an attacker.
The additional red smart devices disappear. The device gateway changes back to white. The

attacker moves next to the cloud.
Step 6: Robust IoT security requires an end-to-end focus on protecting against each of the vulnerabilities and thereby protecting against an attacker.
The smart devices, device gateway, and cloud are enclosed in a box and the attacker moves outside the box.

Animation captions:

1. An IoT device sends data to a gateway. A gateway collects data from one or more IoT devices and sends the data to a cloud server for processing.
2. An attacker may have direct physical access to an IoT device.
3. An attacker may take over a gateway or edge device, opening a range of attacks such as eavesdropping, man-in-the-middle, etc.
4. An attacker can take over multiple IoT devices and gateways to set up a botnet. A botnet can be used to launch DDoS and other attacks.
5. The cloud server is a vulnerability, especially if the server is vendor hosted. Poor security at the vendor end can mean an opening for an attacker.
6. Robust IoT security requires an end-to-end focus on protecting against each of the vulnerabilities and thereby protecting against an attacker.

PARTICIPATION ACTIVITY 6.8.6: IoT security threats and vulnerabilities.

1) Which is a specific type of attack conducted by taking over multiple IoT devices?
   - Eavesdropping
   - Botnets
   - Firmware hijacking

2) Which is a major security threat for IoT devices that is hard or even impossible to mitigate?
   - Network connectivity
   - Default passwords
   - Limited computational capabilities

3) Which is not a concern for IoT security?
   - Two factor authentication
   - Encryption

- Patching and software updates

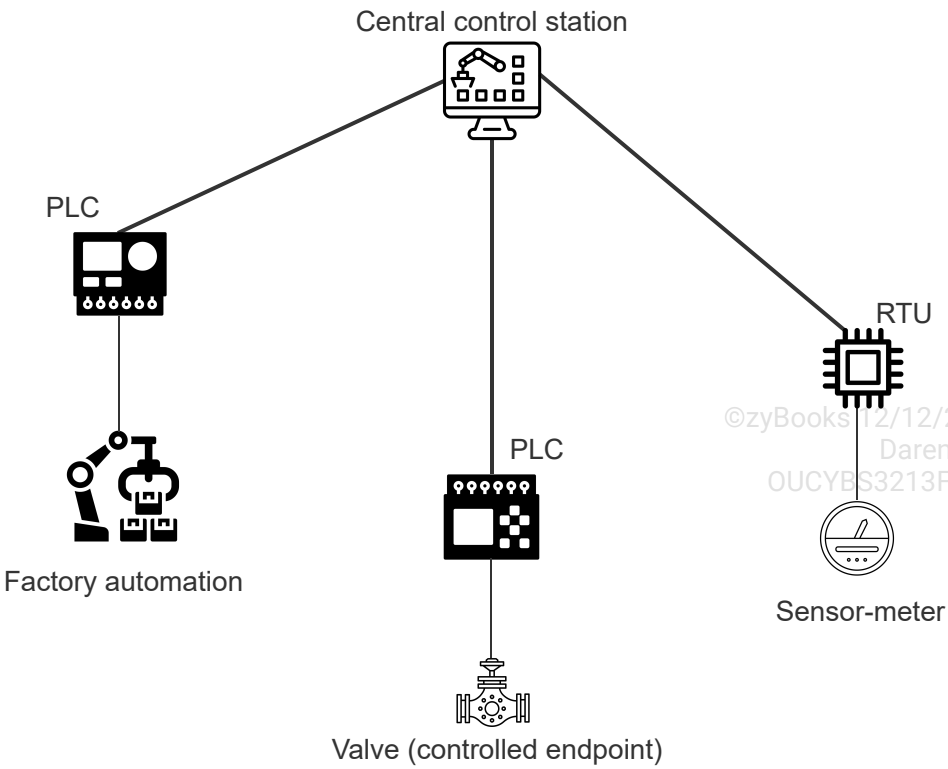
SCADA and ICS

Supervisory Control and Data Acquisition (SCADA) is a type of ***Industrial Control System (ICS)*** used to control and monitor distributed industrial systems. Ex: A SCADA system is used to control the operation of an urban water supply system and collect relevant data such as consumer usage and overall system performance. A SCADA system may use a combination of embedded systems, sensors, controllers, actuators, control terminals, and networked computers. As technology evolves, IoT devices may become part of SCADA systems.

SCADA systems consist of two component types:

- A ***Remote Telemetry Unit (RTU)***, also known as ***Remote Terminal Unit*** or ***Remote Telecontrol Unit***, is a SCADA component used to collect data from sensors in an industrial facility or distributed across a large-scale geographic area. Ex: A water meter at a consumer's residence in a water distribution system is an RTU.
- A ***Programmable Logic Controller (PLC)*** is a SCADA component that is used in a variety of industrial control and monitoring applications that uses sensor input to drive outputs based on programmed parameters. Ex: PLCs are used to control valves in the water distribution system based on flow rate.

PARTICIPATION ACTIVITY 6.8.7: SCADA.



A SCADA system remotely controls and monitors industrial equipment and sensors.

Animation content:

Static image: A desktop labeled "Central control station" connects to three devices. The first device is labeled "PLC". That PLC connects to a machine icon labeled "Factory automation". The second device connected to the Central control station is also labeled "PLC". That PLC connects to a valve icon labeled "Valve (controlled endpoint)". The third device connected to the Central control station is labeled "RTU". The RTU is connected to a meter icon labeled "Sensor-meter".

Animation captions:

1. A SCADA system has a central control station. The control station controls and monitors Programmable Logic Controllers (PLCs) and Remote Telemetry Units (RTUs).
2. PLCs are used to control automation devices such as in factories and water management. RTUs are used to monitor sensors and meters.
3. Network traffic between PLCs, RTUs, and the control station is susceptible to attack.
4. PLCs, RTUs, and end devices can also be a vulnerability if an attacker gains access. Securing endpoints is critical.

PARTICIPATION ACTIVITY 6.8.8: SCADA systems.

1) Which applications is unlikely to have a SCADA system?

   - Facility automation
   - Logistics management
   - Home HVAC system

2) A SCADA system is used to control and monitor the operation of an electricity distribution system in a city. What type of component would be needed to collect information on the electricity consumption of each residence?

   - PLC
   - RTU
   - Sensor

3) A SCADA system is used in a manufacturing plant. An operation in an assembly line requires the use of a robotic arm to remove a component if a fault is detected. Which type of component is suitable for this task?

- PLC
- RTU
- Sensor

4) Which are two security concerns for a SCADA system?

- Control station and remote devices
- Control station and network traffic
- Network traffic and remote devices

5) Why is a control station more secure than the remote devices and network traffic?

- The control station can be physically secured and robust network security tools can be installed to defend against network attacks.
- The control station can be physically secured and network based attacks are not possible
- Installing a strong set of network security tools eliminates anything else to worry about.

6.9 Mobile devices

Mobile device deployment models

Mobile devices present challenges for organizations today. Organizations need to decide which employee devices are allowed to connect to the organization's network. Also, organizations need to identify methods to manage and enforce device security and monitor device activity. Different mobile device deployment models exist:

Bring your own device (BYOD) is an organizational policy allowing employees to use personally owned devices for work-related activities. Applying enterprise security to employee mobile devices is more challenging than applying to organizational devices, since the organization does not own the employee devices and must consider the end-user's privacy for personal information stored on the device. BYOD increases employee satisfaction and productivity and makes the mobile workforce more affordable by eliminating the need to buy additional hardware.

Corporate-owned, personally-enabled devices (COPE) are devices provided to an individual by the organization and used primarily for organizational purposes, but the individual is also allowed to use the device in a personal capacity. Ex: A company provides an iPhone to an employee. The employee can use the iPhone for work and personal use, saving the employee the cost of purchasing a device.

Corporate-owned, business-only devices (COBO) are devices provided to an individual by the organization and used solely for organizational purposes. COBO is the same as COPE, except COBO prohibits personal use of the device. Ex: COBO devices often come in the form of kiosk tablets that are used by a business at large, rather than by individuals.

Choosing your own device (CYOD) is an organizational policy allowing employees to choose from a list of devices specified by the organization, giving employees more freedom and flexibility to choose a device(s), while staying under the umbrella of device management that IT has already established. Ex: A company provides a list of Android phones for employees to choose for use. An employee can use the device for work and usually personal use, saving the employee the cost of purchasing a device. Still under the management of the organization, employee personal information can be monitored by the organization.

PARTICIPATION ACTIVITY 6.9.1: Personal and corporate devices.

Difference between each type of device

	BYOD	COPE	COBO	CYOD
Who owns device?	E	O	O	O
Who owns the device's data?	E O	E O	O	E O
Who maintains the device?	E O	O	O	O
Who pays monthly ongoing costs?	E	O	O	O
What capacity can device be used?	**P** W	**P** W	W	**P** W

E = Employee | O = Organization | **Personal** | Work

Animation content:

Static image: A table titled "Difference between each type of device" with columns "BYOD", "COPE", "COBO", and "CYOD". The rows are labeled "Who owns device?", "Who owns the device's data?", "Who maintains the device?", "Who pays monthly ongoing costs?", and "What capacity can device be used?" The BYOD column indicates that the employee owns the device, the employee and the organization own the device's data, the employee and the organization maintain the device, the employee pays monthly ongoing fees, and the device can be used for personal and work purposes. The COPE column indicates that the organization owns the device, the employee and the organization own the device's data, the organization maintains the device, the organization pays monthly ongoing costs, and the device can be used for personal and work purposes. The COBO column indicates that the organization owns the device, the organization owns the device's data, the organization maintains the device, the organization pays monthly ongoing costs, and the device can only be used for work purposes. The CYOD column indicates that the organization owns the device, the employee and the organization own the device's data, the organization maintains the device, the organization pays monthly ongoing costs, and the device can be used for personal and work purposes.

Animation captions:

1. In BYOD, the employee owns and and pays the monthly associated costs, but both the employee and the organization maintains the device and owns the device's data.
2. In COPE, the organization owns and maintains the device, and pays the monthly associated costs, but both the employee and the organization owns the device's data.
3. In COBO, the organization owns the device and the device's data, maintains, and pays associated monthly device costs. The employee has no personal device obligations.
4. In CYOD, the organization owns and maintains the device and pays the monthly associated costs, but both the employee and the organization owns the device's data.
5. In BYOD, COPE, and CYOD the device can be used for personal and work duties, but in a COBO environment the device can be used for only work duties.

PARTICIPATION ACTIVITY 6.9.2: Mobile device policies.

How to use this tool

BYOD | COPE | CYOD | COBO

An organizational policy allowing employees to use personally owned

	devices for work-related activities.
	A device provided to an individual by the organization and used primarily for organizational purposes, but the individual is also allowed to use the device in a personal capacity.
	A device provided to an individual by the organization and used only for organizational purposes.
	A device an employee chooses from a list specified by the organization giving employees more freedom and flexibility to choose a device(s), while staying under the umbrella of device management that IT has already established.

Reset

Managing mobile devices

Employees use laptops and smartphones to access information at different locations and at any time, causing potential security problems for organizations. Initial solutions focused solely on devices and lacked application and content management. Mobile device management methods evolved to replace device-based solutions.

Mobile device management (MDM) is a cloud-based or on-premise model, allowing an organization to view endpoints and monitor user behaviors and business-critical data on the endpoints. An organization should be able to access the organization's devices, integrations, reports, apps and secure documents easily.

Mobile device management software features:

- Reduce IT administration - Ex: MDM software performs repetitive tasks, like configuring and testing each new mobile device
- Improve end-user productivity - Ex: MDM helps end users get set up on corporate networks much faster.
- Reduce IT risk - Ex: Cybersecurity requirements can be applied systematically instead of relying upon users to manage updates manually.

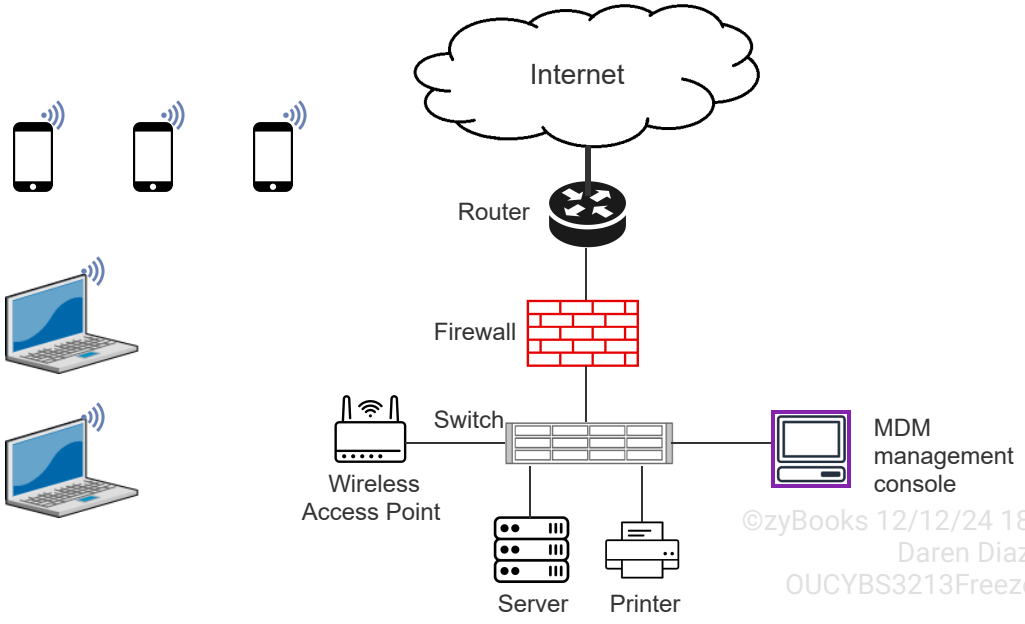
- Enable enterprise growth - Ex: MDM can manage thousands of users allowing for enterprise growth.
- Optimize mobile device spending - Ex: MDM helps identify unused or missing devices helping limit the number of device purchases.

Enterprise mobility management (EMM) is the distribution, organization, and control of mobile devices used in enterprise mobility. Ex: Cell phones, smartphones, tablets, and laptops. EMM encompasses application and endpoint management and BYOD. EMM solutions are highly scalable, and contain new security features powered by AI analytics.

Unified endpoint management (UEM) is a solution to secure, manage, and identify computers, mobile devices, and other endpoints. UEM solutions help enterprises secure and control the entire IT environment and endpoints. Ex: Secure users' personal data, apps, content and enterprise data. UEM provides the ability to push updates or enterprise applications, and apply security policies to devices, and remove all applications and data from a lost or stolen device.

Mobile application management (MAM) is an organizational practice and technology allowing control of an organization's mobile maximum compliance across all devices. MAM secures the applications on the devices used to access organizational data. Ex: Outlook, SharePoint, and OneDrive.

PARTICIPATION ACTIVITY 6.9.3: Mobile device management.



Animation content:

Static image: Three smartphones and two laptops. A cloud labeled "Internet" is connected to a router. The router is connected to a firewall. The firewall is connected to a switch. The switch is

connected to a wireless access point, a server, a printer, and an MDM management console.
Step 1: Reporting and inventory tools consolidate all enrolled devices and associated information into reports. Daily updates are generated automatically.
A cloud labeled "Internet" is connected to a router. The router is connected to a firewall. The firewall is connected to a switch. A printer and an MDM management console appear connected to the switch.
Step 2: Platform is automatically updated with new features at a company's disposal.
A wireless access point and a server appear connected to the switch.
Step 3: The ability to search for anything and everything gives an organization easy access to devices, integrations, reports, apps and secure documents.
Three smartphones and two laptops appear to the left.

Animation captions:

1. Reporting and inventory tools consolidate all enrolled devices and associated information into reports. Daily updates are generated automatically.
2. Platform is automatically updated with new features at a company's disposal.
3. The ability to search for anything and everything gives an organization easy access to devices, integrations, reports, apps and secure documents.

PARTICIPATION ACTIVITY 6.9.4: Mobile device management.

How to use this tool

EMM **MAM** **UEM** **MDM**

	A cloud-based or on-premise model, allowing an organization to view endpoints, users, and items in between.
	The distribution, organization, and control of mobile devices used in enterprise mobility.
	A solution to secure, manage, and identify computers, mobile devices, and other endpoints.
	An organizational practice and technology allowing control of the

	organizations mobile apps, maintaining maximum compliance across all devices.

Reset

VM solutions for mobile devices

Employees are resistant to organizations monitoring, managing and loading applications on employee-owned devices. Also, organizations are concerned about vulnerable data stored on employee-owned devices.

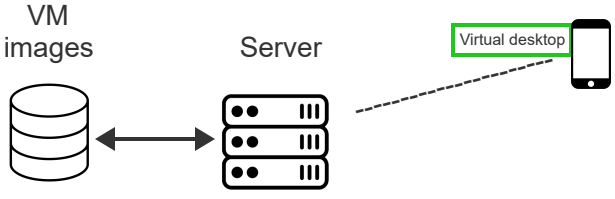
Virtual Desktop Infrastructure (VDI) is a technology using VMs to provide and manage virtual desktops. A VDI allows the user to choose whatever desktop OS preferred and allows the IT team to provide the updated current version. Each end-user connects to the virtual server through a broker that redirects the end-user to the virtual desktop environment. The IT department saves time by only having to update the image and not each individual end-user device. Data is stored on the organization's servers and not the end-user device, eliminating a data breach possibility for a lost or stolen device.

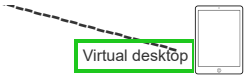
Two VDI types exist:

- A ***client-based mobile VDI*** installs a mobile VDI client application on each mobile device. The VDI session allows the mobile device to access various applications and data through a virtualized interface.
- A ***browser-based mobile VDI*** is an architecture using a web browser to access a web-based mobile VDI client. A browser-based mobile VDI does not require a mobile VDI client application on the mobile device.

Virtual Mobile Infrastructure (VMI) is a mobile-centric technology that runs mobile apps on a mobile operating system (OS)/virtual machine that is located on a remote server. VMI is referred to as a Mobile VDI because a VMI applies the same principles that allows VDI to run desktop applications on desktops and mobile.

PARTICIPATION ACTIVITY 6.9.5: VDI.





Animation content:

Static image: A database icon labeled "VM images" next to a server. A two-way arrow is between the VM images database and the server. A smartphone is connected to the server with a dashed line. A label next to the smartphone says "Virtual desktop". A tablet is connected to the server with a dashed line. A label next to the tablet says "Virtual desktop".
Step 1: Virtual desktop can be used to supply the same desktop environment across user devices. A database icon labeled "VM images" next to a server. A two-way arrow is between the VM images database and the server. A smartphone is connected to the server with a dashed line. A tablet is connected to the server with a dashed line.
Step 2: Mobile devices send a login request to a server. The user's login is configured for VDI. The server retrieves desktop image from the database.
Login requests move from the smartphone and tablet to the server. Virtual desktops move from the VM images database to the server.
Step 3: The server sends the virtual desktop image to the mobile device.
The virtual desktops move from the server to the smartphone and tablet.

Animation captions:

1. Virtual desktop can be used to supply the same desktop environment across user devices.
2. Mobile devices send a login request to a server. The user's login is configured for VDI. The server retrieves desktop image from the database.
3. The server sends the virtual desktop image to the mobile device.

PARTICIPATION ACTIVITY 6.9.6: Mobile device deployment.

1) The two types of mobile VDI are client and browser based VDI.

   - ○ True
   - ○ False

2) VMI runs mobile apps on a mobile operating system (OS)/virtual machine that is located on a remote server.

   - ○ True
   - ○ False

Mobile device security

Mobile device security enables an IT department to remotely manage users and the user's devices, providing security and management for all mobile devices connected to a network.

MicroSD HSM is a hardware security module loaded on a microSD card. A MicroSD HSM provides security services using hardware-based crypto engines, including encryption, key generation and key life cycle management, digital signature, and authentication.

Other mobile device security types:

- EMM platform - Enables IT to gather real-time insights to stop potential threats.
- Email security - Enable advanced email security that detects, blocks, and addresses threats quickly, while providing data end-to-end encryption.
- Endpoint protection - Ensures mobile devices follow security standards by quickly alerting security teams of detected threats.
- VPN - Allows remote users and branch offices to securely access corporate applications and resources.
- PKI - Enables a technology for authenticating users. Mobile PKI provides trusted encryption and identity.

Table 6.9.1: Mobile device security threats.

Security threat	Example
Data leakage	Riskware apps are a problem if users grant broad permissions. Only give apps the permissions needed to properly function.
Unsecured WiFi	Free Wi-Fi networks are usually unsecured. Never use Free Wi-Fi to access confidential or personal services, like banking or credit card information.
Network spoofing	Access points advertise common SSIDs to get users to connect. Hackers obtain information if user supplies the same password combination for login.
Phishing attacks	Mobile device users are also more susceptible because email apps display less information to accommodate for smaller screen sizes.
Spyware	Spyware monitors and records information about the user's actions, without the user's knowledge or permission. A Stalkerware app tracks a device location.

Broken cryptography	Broken cryptography happens when app developers use weak encryption algorithms, fail to implement strong encryption, or leave "back doors" open.

PARTICIPATION ACTIVITY 6.9.7: Mobile device security.

1) Chris granted broad permissions to all organizational mobile devices, posing which possible security threat?
   - Broken cryptography
   - Data leakage
   - Spyware

2) Which platform allows Kai, an IT specialist to stop a potential threat using real-time information?
   - Enterprise mobility management
   - MicroSD HSM
   - VPN

3) Chris received an email on a mobile phone with a link to login to a website and pay a fraudulent invoice is an example of which security threat?
   - Unsecured Wi-Fi
   - Network spoofing
   - Phishing

Mobile device applications and installation

Geotagging is the process of appending geographic coordinates to media based on the location of a mobile device. Geotags can be applied to photos, videos, websites, text messages, and QR codes. Geotags reveal where individuals are when engaging with a website, or movement throughout the day. Geotagging analyzes this information, allowing organizations to provide specialized offers and messaging.

SMS is a texting technology to send messages over a cellular network. SMS does not require mobile data or Wi-Fi to send and receive SMS messages, which is convenient when having limited internet connectivity. ***MMS*** is a texting technology to send messages and multimedia content over a cellular network. MMS technology supports text messages sending pictures, audio files, and contact cards. A phone's built-in messaging app can send MMS.

RCS is Android's built-in messaging application and converts native texting apps into a live chat platform. RCS requires an internet connection to transmit messages. RCS supports many content formats. Ex: Pictures, videos, location, Emojis, and payment alerts.

iMessage is Apple's instant messaging service and is supported by iOS devices like iPhones, iPads, and MacBooks. iMessage requires cellular data or Wi-Fi to send and receive messages and takes less time to send large media files than MMS. iMessage supports similar content formats as RCS.

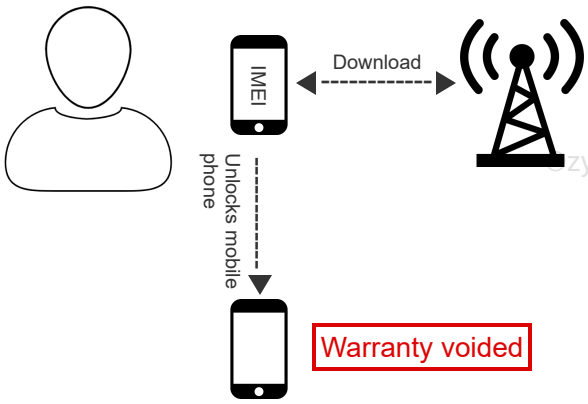
Sideloading is the process of adding an application that has not been approved by the device's operating systems developer. Google's default configuration does not allow sideloaded apps, but settings can be changed to allow apps from third-party sources.

Jailbreaking is a method of circumventing a device's security features by increasing user permissions on the device. Jailbreaking allows the installation of applications from third-party sources. Apple maintains a high level of device security by restricting all devices to only allow apps downloaded from the official App Store. Jailbreaking is an option to install third-party apps on an Apple device.

Rooting modifies the device software to provide root access to the device, allowing superuser privileges. Rooting is often confused with the Android version of jailbreaking. While rooting is similar to jailbreaking, rooting provides a great deal more freedom to Android users.

The Apple App Store for iOS and the Google Play Store for Android are the two largest distribution channels for mobile apps, but over 300 third-party app stores exist worldwide.

PARTICIPATION ACTIVITY 6.9.8: Rooting process.



Static image: A user next to a smartphone with "IMEI" on the screen. A cell tower is next to the smartphone. A two-way arrow labeled "Download" is between the smartphone and the cell tower. The smartphone has an arrow labeled "Unlocks mobile phone" pointing toward a second smartphone. The text "Warranty voided" is next to the second smartphone.

Animation captions:

1. On an Android smartphone, administrator rights can be legitimately obtained.
2. Users type the smartphone's unique number (IMEI) and download the modified OS software.
3. It will unlock the smartphone's bootloader and enable the upload of a modified operating system that will grant a user's full rights.
4. Manufacturers void warranties on such unlocked smartphones and gives the smartphone the status of "developer device".

PARTICIPATION ACTIVITY | 6.9.9: Cellular applications.

How to use this tool

Geotagging **Rooting** **RCS** **Jailbreaking** **Sideloading** **iMessage**

	The process of appending geographic coordinates to media based on the location of a mobile device.
	Android's built-in messaging application and converts native texting apps into a live chat platform.
	Apple's instant messaging service and is supported by iOS devices like iPhones, iPads, and MacBooks.
	The process of adding an application that has not been approved by the device's developer.
	A method of circumventing security by increasing user permissions on the device.

	Provides root access to the device, allowing superuser privileges.

Reset

6.10 LAB: RADIUS server (Walkthrough)

IT-Labs are not printable at this time.

6.11 LAB: Wireless attacks (Walkthrough)

IT-Labs are not printable at this time.