Wireless Networking

- Introduction
- The IEEE 802.11 Wireless LAN Standard
- Wireless Networking
- Bluetooth, WiMAX, RFID, and Mobile Communications
- Wireless LAN Security

DRAFT

Introduction

- So far, we have been looking at OSI Layers **#1** and **#2** -- the physical link and data link (MAC) layers
- We have already examined two types of wired links
  - Ethernet over twisted-pair
  - Fiber-optic networking
- For sheer bandwidth and speed, nothing can really beat a wired connection.
- However, wired connections also have some downsides…

Introduction

- Those include:
  - The necessity of having a cable and being near a wall plate
    - This, of course, limits the user's mobility, even if the device itself is mobile!
  - Costs of installing cable and wall plates
  - Practical limits on the number of physical connections to the network
- Furthermore, if you ever want to upgrade the network – speed, hardware, etc. – it will be a lot of work!

Introduction

- When users do not need the full speed possible with a wired connection, you can have a trade-off and gain greater mobility and flexibility by connecting to the network wirelessly.
- Over this part of the course, we will examine wireless technologies, along with issues related to setup, maintenance, and security.

The IEEE 802.11 Wireless LAN Standard

- Just as the IEEE 802.3 standard defines the physical and datalink aspects of wired Ethernet, the **802.11** standard defines the same aspects of a wireless LAN (WLAN).
- Wireless networking offers a number of advantages, most notably:
  - Making networking easier and less costly in areas that would be challenging or impossible to wire
  - Increasing user mobility

The IEEE 802.11 Wireless LAN Standard

- At the same time, the network administrator must be prepared for the unique issues and challenges posed by WLAN setup and maintenance -- understanding the technologies involved.
- 802.11 defines three main areas of wireless networking
  - The Physical layer, which concerns the lower-level data transmission technologies. This usually uses either of two EMR types: **Radio** (usually) or **Infrared** (rarely)
  - The MAC (media access control) layer, which handles data reliability, access, and security
  - The actual protocols and services for managing the previous

Wireless Network Topology

- We can identify two primary WLAN topologies:
  - Basic Service Set (BSS)
  - Extended Service Set (ESS)
- In **BSS**, all clients communicate directly, having recognized and linked wirelessly with one another (*Figure 4-1*)
  - This is also known as **ad hoc networking**
  - A BSS topology can be improved upon by adding an access point
    - An access point is a transceiver (transmitter/receiver) that connects a WLAN to a wired LAN (*Figure 4-2*)
    - Here, communication between a wireless client and any other client will pass through the **access point**

Wireless Network Topology

- An **ESS** topology enhances user mobility by incorporating multiple access points (*Figure 4-3*)
  - When a user passes from one access point's range into another, we call this a hand-off
  - Assuming the access points are arranged such that their signals overlap sufficiently, the roaming user's hand-offs will appear relatively seamless.
- In the 802.11 standard, network access is handled using **carrier sense multiple access/collision avoidance** (*CSMA/CA*).
  - When the channel (i.e., the frequency) is quiet, a client may transmit.
  - Otherwise, any other clients must wait.

Physical Layer Technologies

- We can begin discussion with some relevant terms…
- **Frequency**: How many wave cycles occur within a given amount of time.
  - Frequency is usually measured in hertz (Hz), such that 1 Hz equals 1 cycle per second.
  - Many of the terms that follow are defined in terms of frequencies.
- As mentioned earlier, most wireless data transmission takes place over the **radio frequency** (*RF*) portion of the electromagnetic spectrum.

Physical Layer Technologies

- The RF spectrum is divided into **bands**, with definite beginning and ending points.
  - These may be very *wide* ranges, even in the hundreds or thousands of MHz!
  - A wireless communications system will be said to "operate within" one or more bands.
  - Frequency bands are often designated or *reserved* for specific purposes. For example...
    - FM radio uses a band ranging roughly from 88 to 108 MHz
    - The AM radio band ranges from 535 to 1605 kHz

Source: `http://hyperphysics.phy-astr.gsu.edu/hbase/audio/radio.html`

Physical Layer Technologies

- These are some bands defined by the International Telecommunications Union, a body of the United Nations that deals with issues related to communication and information technologies

→→→→

Band number	Abbreviations (key below)	Frequency ranges (lower exclusive, upper inclusive)
3	ULF	300-3000 Hz
4	VLF	3-30 kHz
5	LF	30-300 kHz
6	MF	300-3000 kHz
7	HF	3-30 MHz
8	VHF	30-300 MHz
9	UHF	300-3000 MHz
10	SHF	3-30 GHz
11	EHF	30-300 GHz

Key:

F = "frequency"

L = "low", M = "medium", H = "high"

V = "very", U = "ultra", S = "super", E = "extremely"

Source: https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.431-8-201508-I!!PDF-E.pdf

Physical Layer Technologies

- There is a group of bands called the "ISM" bands -- short for "industrial, scientific, and medical". Wi-Fi technology uses two of those bands:
  - **2.4 GHz** (2.4-2.5 GHz)
  - **5 GHz** (~5.15-5.815 GHz)
- Not all frequencies in those bands are necessarily available for wireless networking, though
- There are various *regulatory bodies and agencies* that make these determinations.

Physical Layer Technologies

- In terms of networking, a **channel** can be generally defined as a conduit for signal transmission.
  - For a wired networks, the channels would be tangible objects -- i.e., the cables.
  - On WLANs, however, EMR is the transmission medium, so "channels" are defined in terms of frequency ranges.
  - Specifically, a frequency band is divided into channels.
  - If a channel has many devices trying to broadcast at once, there can be issues of co-channel congestion -- where everyone has to "wait their turn".

Physical Layer Technologies

- **Example:** The **FM radio band** -- ranging *88 to 108 MHz* -- has 100 channels
  - Each channel is a **200 kHz** (*0.2 MHz*) range within the whole:
  - The first channel starts at the beginning of the band, and the last channel ends at the end of the band.
  - A channel is identified by its center frequency -- a.k.a., ***carrier frequency*** -- so…
    - The first FM channel is **88.1** (*88.0-88.2*) MHz
    - The following frequencies proceed by increments of 0.2: 88.3, 88.5, …
    - …until the last FM channel, which is **107.9** (*107.8-108.0*) MHz

Physical Layer Technologies

- The bandwidth surrounding the carrier frequency is used for modulation, as well as providing a buffer before the next channel.
  - What is modulation?
  - For example, how do AM and FM radio differ?
- Another variable of importance is signal power or received signal strength of a transmission
  - This is typically measured in units of *decibel-milliwatts* (***dBm***).
  - You need not understand the mathematics behind this unit.

Physical Layer Technologies

- The received signal strength value will usually be between <u>-10</u> and <u>-100</u> dBm
  - The closer the value is to zero, the better your signal. For example, a signal of **-20 dBm** is much better than **-95 dBm**
  - Many factors -- both hardware-related and environmental -- can affect the value.
  - As a general rule, the value will worsen with increasing distance from the signal origin.
- **Source:** **https://www.accuware.com/support/knowledge-base/what-is-the-signal-strength-rss/**

Physical Layer Technologies

- If you recall, the original IEEE 802.11 standard was released in 1997.
- Since then, there have been new standards, in the form of regular amendments.
    - These amendments are usually indicated by appending alphabetical suffixes ("a", "b", "ac", etc.) to the more general "802.11" designation -- leading to names like "802.11b" and "802.11ac".
    - Collectively, we may call them the **802.11*x* standards**.

Physical Layer Technologies

- Here are some of the more relevant ones:

Suffix	Data Rates	Range	Frequencies
a	Up to 54 Mbps	Up to 75 ft.	5 GHz
b	Up to 11 Mbps	100-150 ft.	2.4 GHz
g	Up to 54 Mbps	Up to 150 ft.	2.4 GHz
n	200+ Mbps	Up to 150 ft.	2.4 GHz or 5 GHz
ac	Up to 1 Gbps	115 ft.*	5 GHz

*** http://litepoint.com/whitepaper/80211ac_Whitepaper.pdf**

- An organization known as the Wi-Fi Alliance certifies wireless equipment based on these standards.

Physical Layer Technologies

- Within the 802.11x standards, wireless networking makes use of four primary physical layer signalling technologies:
    1. Infrared (IR)
    2. Frequency Hopping Spread Spectrum (FHSS)
    3. Direct Sequence Spread Spectrum (DSSS)
    4. Orthogonal Frequency Division Multiplexing (OFDM)
- **IR** signaling was part of the original 802.11 standard, but it never really caught on, and it is even described as "obsolete" within the standard itself.

Physical Layer Technologies

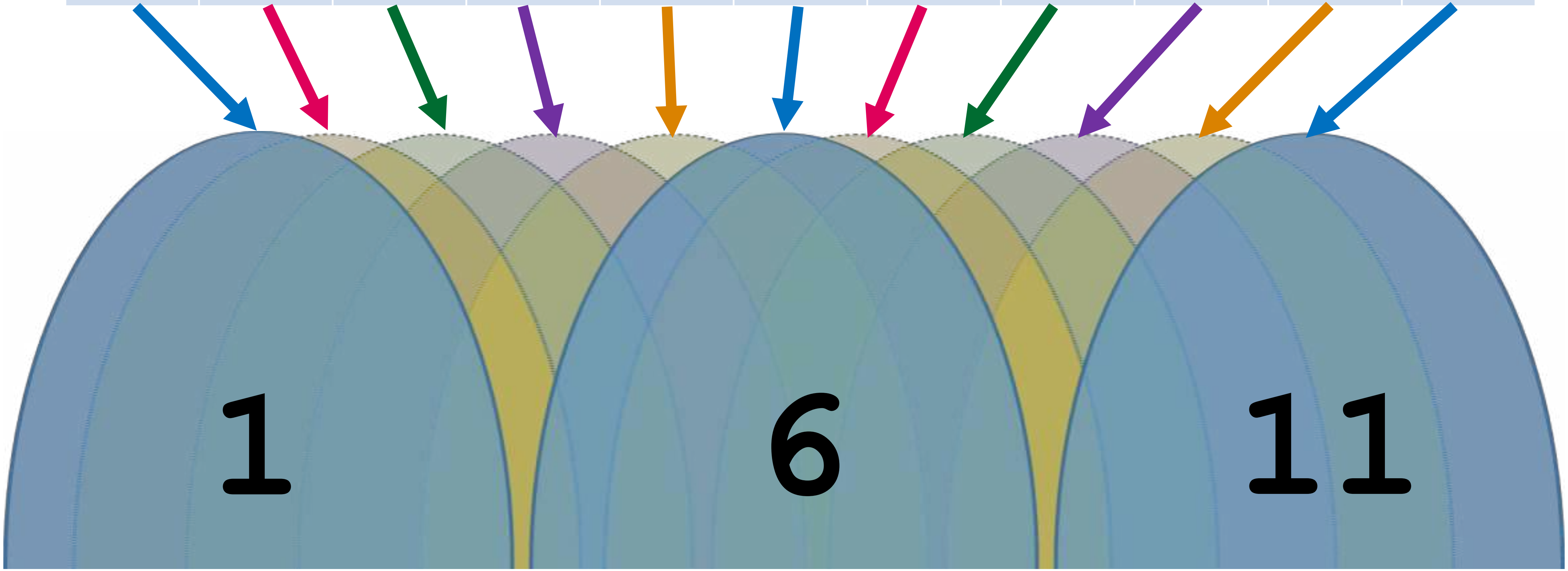
- **FHSS** (*frequency hopping spread spectrum*) uses 79 channels, each 1 MHz wide, within the 2.4 GHz ISM band.
  - FHSS will repeatedly change the transmission frequency in a sequence, in a **pseudorandom**.
  - In other words, there is actually repetition.
  - The resulting order is called the **hopping sequence**.
  - Similar to IR, FHSS is not commonly used.

Physical Layer Technologies

- **DSSS** (*direct sequence spread spectrum*) uses fourteen 22-MHz-wide channels within the 2.4 GHz band.
- Mathematically, DSSS involves adding "noise" (technically, pseudorandom noise) topic the transmitted signal
  - That process which is then reversed upon reception.
  - In North America, we only use ***11*** of those 14 channels
  - The carrier frequencies for those 11 channels *start* at 2.412 GHz and *end* at 2.462, incrementing by 5 MHz each time.

2.4 GHz Channels 1-11

1	2	3	4	5	6	7	8	9	10	11
2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462



Physical Layer Technologies

- Because the channel widths exceed the distance between two adjacent carrier frequencies, some of the channels overlap.
  - This can create an issue called ***adjacent channel interference***, which is analogous to crosstalk in wired channels.
  - This can actually be *more* problematic than co-channel interference.
  - One way to avoid this is for devices restrict themselves to non-overlapping channels: **1**, **6**, and **11**

Physical Layer Technologies

- Finally, **OFDM** (*orthogonal frequency division multiplexing*) divides a channel into sub-channels.
  - Data can be sent over those sub-channels in parallel.
  - Although the sub-channels may be overlapping, they will not interfere with one another – which is what the term "orthogonal" indicates.
  - This allows for potentially *higher data rates*.
  - At the same time, it *consumes more power*.

Physical Layer Technologies

- Different 802.11x standards use different signal modulation technologies
  - **802.11a** uses OFDM technology, in the 5-GHz band
  - **802.11b**, operating in the 2.4-GHz band, uses DSSS.
  - **802.11g** uses both DSSS and OFDM.
    - Because g operates in the same frequency band as b, devices for both standards are mutually interoperable.
    - This simplifies upgrading a 802.11**b** network to **g**

Physical Layer Technologies

- **802.11n** also uses both DSSS and OFDM, while operating in both wireless bands: 2.4 GHz and 5 GHz
  - It incorporates a technique called **MIMO** (multiple input, multiple output), which splits data streams into multiple parts .
  - This increases the data rate, but it also consumes more power.
- **802.11ac** uses OFDM, operating in the 5GHz band. It features a number of improvements over predecessors and allows for higher data rates:
  - **MUMIMO** (multiuser MIMO) -- a variation on MIMO that splits the data stream 8 ways and has wider (80 MHz!) channels
  - **Beamforming** -- The ability to direct signal to a specific device

Physical Layer Technologies

- There are two other amendments of note:
  - **802.11i:** *Improved data encryption* on 802.11a/b/g
  - **802.11r:** *Speedier hand-offs* -- crucial in the event voice traffic becomes more common.

Wireless (WiFi) Networking

- A wireless-capable device will have a wireless adapter that allows it to connect to an RF channel.
  - An example is the wireless NIC in your laptop or smartphone
  - This adapter will provide three services:
    - Data delivery
    - Authentication -- ensuring you are a valid and allowed user
    - Privacy
- It will make this connection via an **access point**.

Wireless (WiFi) Networking

- Access points are devices that provide for:
  - Connection of a device to a wireless LAN (WLAN)
  - Connection (i.e., bridging) between the WLAN and the wired network
- See *Figure 4-6*
- A client device will use a service set identifier (**SSID**) in order to gain access to the WLAN

Wireless (WiFi) Networking

- SSIDs are also usually a network name:
  - This is often a *human-readable* name, such as "UMB-Student"
  - The access point, then, will use the SSID to determine if the client can connect
  - When a connection is made, we call that an ***association***
    - The client will have the access point's MAC address (*Figure 4-7*)
    - User will receive a notification if association is lost (*Figure 4-8*)
- The access point builds a table of MAC addresses (for clients) to forward data packets

Wireless (WiFi) Networking

- You can form wireless connections between buildings.
  - This will place over wireless bridges:
    - Point-to-point (*Figure 4-9a*)
    - Point-to-multipoint (*Figure 4-9b*)
  - It can be accomplished using rooftop antennas (*Figure 4-10*)
  - This can be problematic because the signal can suffer attenuation on account of *obstacles* and *distance*
- Another option is to place wireless access points throughout a building, which requires you to perform a site survey…

Site Surveys

- A **site survey** is the process of evaluating a site and finding the best positions for access points, so as to allow for maximum RF availability for wireless clients.
- (What you are doing in Lab 6 is a variation on this -- in other words, evaluating the current placement of access points.)
- A site survey -- which can address both indoor and outdoor environments -- will seek pertinent information

Site Surveys

- Data sought may include….
  - Power sources
  - Connections to other networks, such as the wired LAN
  - Locations of transmission devices, such as:
    - Access points (indoor)
    - Antennas (outdoor)
  - Signal coverage
  - Bandwidth supported
  - Possible sources of signal interference

Site Surveys

- For example, ***Figure 4-11*** depicts:
  - Several wireless access points
  - Their coverage areas
  - A possible path through the site, for a device user
- As we can see in the figure, *at no point* is the user outside of some access point's range
- In contrast, ***Figure 4-12*** shows us:
  - The floor plan
  - Available wired connections
  - Points (***A-D***) at which signal measurements were taken

Site Surveys

- With just one access point at position #1, signal quality worsened from A to D (***Figures 4.14-17***).
- This lead the designers to add a second access point at *position #2*.
- In the aforementioned figures, you can also see the ***Wifi Analyzer*** app measuring signal strength.
- As you may remember, all the signal strength values are negative, but the greater values are considered stronger/better.

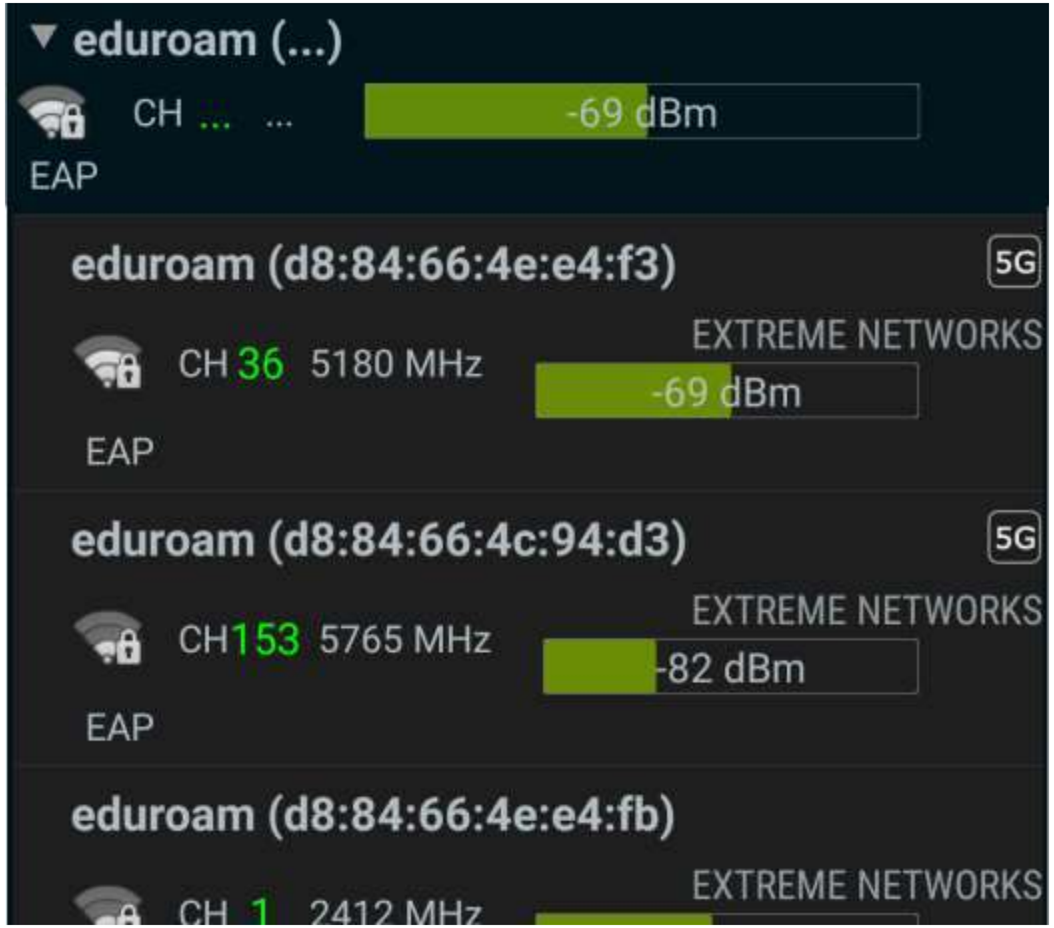
Site Surveys - Examining signals

- When you are in a building, you may be able to use signal strength to locate access points. You will be looking for things like…
  - SSID -- the network name
  - Access points
  - Signals
- You may get multiple signals for one SSID, especially more common ones like **UMB-Student** and **eduroam**.

Site Surveys - Examining signals

If you look at the signals closely, you will see data like the following:

- Channel number
- Frequency
- BSSID (Basic service set identifier)



Site Surveys - Examining signals

- Let's look at a snapshot of the *eduroam* signals:
  - On the third floor of the Science building
  - Near the elevators
- As you see, the BSSIDs look like *MAC addresses*.
- In particular, the first three pairs are the same, indicating that **`d8:84:66`** is the OUI for the access point's manufacturer: *Extreme Networks*.

Site Surveys - Examining signals

- Beyond this, you will also notice some other things:
  - After the OUI, you see another pair of digits, which is either **`4c`** or **`4e`**
  - You see both *2.4G* and *5G* signals on both.
  - **`4c`** is followed by **`94`**, while **`4e`** is followed by **`e4`** and **`f9`**
  - You may also see other patterns following those…

Other Wireless Technologies

- In addition to Wi-Fi, there are some technologies worth knowing about:
  - Bluetooth
  - WiMAX
  - RFID
  - Mobile
- We will look at the first three…

Bluetooth

- **Bluetooth** (henceforth, BT) is a technology with which you are probably familiar, if you have ever connected two more electronic devices -- of your own -- wirelessly.
- Examples?
- Some include…
    - Headpiece
    - Headphones
    - Mobile Phone to Personal Computer

Bluetooth

- BT -- set up by the *IEEE 802.15* standard -- allows us to replace a wired device connection (e.g., USB) with a wireless connection.
- It uses the 2.4 GHz ISM band, which is also used by what 802.11x standards?
    - **b** , **g** , and **n**
- Up to 8 devices can be set up in an ad hoc network called a **piconet**, where one device is the "master"

Bluetooth

- A BT connection is set up as follows:
  1. Enable BT on a device
  2. The device will perform an inquiry procedure to find other available BT devices. Also called discovery. The other devices will need to:
     a. Have BT enabled
     b. Be "discoverable" by other BT devices
  3. If a device is found, a connection is established and synchronized using a paging procedure.
- Setting up two devices to be connected is called pairing. For security's sake, there may be a Passkey to restrict pairing.

WiMAX

- **WiMAX** stands for Worldwide Interoperability for Microwave Access, and its corresponding standard is *IEEE 802.16e*
  - Another standard -- 802.20 -- is under development
- It can provide fixed and mobile stations with **broadband wireless access** (BWA).
  - *Fixed*: Up to 30 miles
  - *Mobile*: 3-10 miles

WiMAX

- It can also allow for last mile broadband access over a wireless medium.
  - **Last mile** refers to the final linkage between access provider and client.
- Many aspects of WiMAX are not restrictive:
  - Not a single protocol design.
  - Serves many different types of topologies.
  - Many different frequencies
  - Flexible channel sizes (3.5 MHz, 5 MHz, etc.)
  - Many different power levels
- Its signaling format is ***OFDM***, which has non-line-of-sight advantages and minimizes certain kinds of interference

RFID

- **Radio frequency identification** allows for tracking people and things using radio waves
- The idea is that:
    - The object to be tracked will have an RFID tag -- also called a transponder.
    - A reader (transceiver) will send radio waves that strike the tag.
- The radio waves (sent by the reader) will cause the tag to activate and transmit data back to the sender (i.e. the reader/transceiver). This "reflecting back" is called **backscatter**.

RFID

- RFID has substantial uses in many areas:
  - Shipping, for tracking cargo
  - Retail, for inventory
  - Timing races, such as marathons
  - Conferences, for traffic management
- **Source:**

  http://blog.atlasrfidstore.com/what-is-rfid-used-for-in-applications

RFID

- An RFID system can be characterized by three features:
  - ***How the tag is powered***
    - *Passive* - using the RF energy from the reader
    - *Semi-active* - a combination of a battery (for tag electronics) and backscatter (for transmitting back to the reader)
    - *Active* - using a batter for everything
  - ***Operating frequency***
    - *LF* (low frequency) - 125/134 kHz
    - *HF* (high frequency) - 13.56 MHz
    - *UHF* (ultra high frequency) - 860-960 MHz and 2.4GHz

RFID

- ***Communications protocol***
  - This is also called the Air Interface protocol.
  - RFID uses the **Slotted Aloha** protocol, which is similar to Ethernet in terms of avoiding collisions

WLAN Security

- With wired connections, you have some knowledge and control regarding who is connecting to the LAN
- However, with wireless connections, you have radio frequencies transmitting in the air, and you can never be completely certain….
  - how far the signal reaches
  - or who might be picking it up
    - What is ***war driving***?
    - What is ***packet sniffing***?

WLAN Security

- Fortunately, we have many means of securing a wireless network…
  - Change default SSID and password
    - Those are given by the manufacturer itself
    - They will, generally, be very well-known -- for example, by potential hackers
  - Continue to change SSIDs and passwords frequently
  - Turn off SSID broadcasting, so that this information is not being shared with everyone
  - Use MAC filtering
  - Use RADIUS
  - Use third party encryption software

WLAN Security

- Two aspects of security are particularly important
  - ***Authenticating*** clients on the network -- establishing their identities and authorization to use the network.
  - ***Encryption*** of data packets sent over the connection
- There are two main types of authentication:
  - ***Open***: This is essentially ensuring that the SSID of the client matches that of the network. Needless to say, it is not very secure.
  - ***Shared-key***: The access point sends a data packet to the client, who uses a shared key to encrypt the data, which is then returned to the access point, who decrypts it.
    - The cryptographic key comes from **WEP** (wired equivalent privacy).
    - Verification of key is the basis for establishing that the client is allowed on the network

WLAN Security

- Shared-key encryption is particularly vulnerable to malicious cracking attempts, but it is better than no security at all.
  - WEP was retired by the 802.11 standard
  - However, it is still widely in use
- A better option is *Wi-Fi Protected Access* (WPA):
  - **WPA** (c. 2003) made substantial improvements over WEP in terms of encryption and authentication.
  - **WPA2** (c. 2004) improved upon this with more sophisticated encryption methods.
- There are many options for wireless security, requiring substantial decision-making by the network admin.