Networking Models

- To get into this topic, we will start with an example that is somewhat more familiar to everyone: Using the *telephone*.
- What goes into making a phone call?
  - What do you have to have on hand?
  - What do you have to do?
  - What can go wrong?
- These things – in fact – pertain to many other types of networks, as well. Including *computer* networks.

Networking Models

- In any kind of networking, there will be multiple aspects involved
  - Hardware
  - Rules and standards
  - Connections
  - Software
- To that end, it is helpful to have ***models*** that enable us to understand these things more effectively.
- **What is a *model*?**

Networking Layers

- It is helpful to think of networking as consisting of several layers.
- A lot goes into enabling one computer to talk to another, and you are dealing with multiple factors at once. There are a number of models for networking, but here, we will speak of *five* layers:

  5: Application
  4: Transport
  3: Network
  2: Link
  1: Physical

- Though we will explore each component in depth, in the way of analogy, consider the following animation:

  `https://www.youtube.com/watch?v=VGGmBhARuiY`

Networking Layers

- You are probably the most familiar (if only indirectly) with the ***application*** layer, which is the closest to what the end users typically see.
- You use a piece of software, such as a browser or SSH client – which, in turn, uses a network protocol like *HTTP*, *FTP*, *SSH*, *POP3* and *SMTP*/ *IMAP*
- These protocols constitute the application layer.
- This also entails ***presentation*** , which deals with the form of the data being sent across the network.
- This may be the most obvious in the case of file types: **`txt`**, **`jpg`**, **`png`**, **`mp3`**, **`mov`**, etc.

Networking Layers

- What these are, in fact, are alternative manners of encoding information (which, at the end of the day, is bits and bytes) so that it can be understood by different software programs.
- You can see this by looking at HTTP requests, which will specify certain aspects of presentation
- Presentation can also deal with data encryption and compression
- Where things become a bit murkier is with the ***session*** layer.
- A "session" is an ongoing interchange of data between two nodes of a network, across a connection
- Recall your ***command-line sessions*** ...

Networking Layers

- For a more involved example, if you navigate to a particular web address, you will initiate an HTTP session:
  - Establish a connection with the remote server
  - Send a request (and await the response)
  - The server sends back a response
  - Repeat the previous two steps, as needed
  - Close connection
- Such things can be considered part of an "application" layer
- The layers that follow may seem much more esoteric, but they are *fundamental* for the behavior of computer networking

Networking Layers

- The ***transport*** layer is responsible for ensuring that the data transfer process occurs without error, such that the data integrity is maintained between source and destination
- This can include such aspects as:
  - Establishing connections
  - Separating data into smaller pieces (and numbering them)
  - Acknowledging data receipt – and resending, if necessary
  - Controlling data flow rate
- Port numbers are pertinent to the transport layer.
- Two major transport protocols are TCP and UDP

Networking Layers

- The ***network*** layer, as its name would imply, handles communications between networks.
- Indeed, "internet" is a shortened form of the term "internetwork", a system where networks are connected to one another.
- The network layer has two main responsibilities:
  1. Establishing addresses (i.e., locations) of hosts on networks (What is a "host"?)
  2. Forwarding, or *routing*, data packets along a path from source to destination.
- A router, then, connects devices at the network layer!
- The most common network protocol is Internet Protocol, or IP

Networking Layers

- In contrast, the ***link*** layer handles communications (i.e., data transport) within networks.
- To connect to a network, a device must have a particular piece of hardware called a ***network interface controller*** (NIC). Two examples of NICs:
    - Ethernet card
    - WiFi transceiver
- You can think of the link layer as dealing with communications from one NIC to another NIC.
    - Directly, in a one-to-one connection
    - Indirectly, over a hub or switch

Networking Layers

- Every NIC has a unique identifier called a ***MAC (media access control) address***.
  - An IP address is a *network*-layer identifier, whereas a MAC address identifies the device on the *link*-layer
  - You can think of a MAC address as being more *physical*, whereas an IP address is more *logical*
- Finally, the ***physical*** layer concerns itself with the *hardware* components of a network, such as cables, network interface cards (NICs), and switches/hubs
- In other words, the actual sending of data in its most basic form – as raw bits – across the hardware connections.

Network Administration with Models

- When problems arise on a network, the administrator can look at different layers in order to discern what the problem might be.
- Let's say that a particular remote server cannot be accessed
  - First, the admin would attempt to ping the server (Network Layer). The response will indicate whether the connection is *up* ("reply from") or *down* ("request timed out").
  - In the event of the latter – the connection being down – the admin will consider different possible problems:
    - Cable issues (***Physical Layer***)
    - Switch issues (***Link layer***)
    - Router issues (***Network Layer***)
    - The server itself (***Application layer***)

Ethernet

- You have probably heard this term before, and you are probably most familiar in references to a cable for networking
- However, the term actually refers to a protocol on the *physical* and *link* layers.
- In Ethernet, data are transmitted over the network in well-defined units called *frames*. In networking, you will often hear of "frames" and "packets" because this is how data is ultimately transmitted over a network
- An application (e.g., HTTP) request is broken down into parts:
  - Each part is incorporated into a *transport*-layer **segment**...
  - ...which is wrapped in a *network*-layer **packet**
  - ...which goes into a *link*-layer **frame**

MAC Addresses in a LAN

- On a LAN, every device will have a NIC, the hardware it uses to connect with the network.
- The NIC will have a unique identifier – a MAC address – which is a 48-bit (6-byte) value expressed as 12 hexadecimal digits.
- The MAC address may also be called the **`Ethernet`**, **`physical`**, **`hardware`**, or **`adapter`** address
- Example:

```
00-10-a4-13-6c-6e
```

- The **first three pairs** identify the vendor of the NIC; this sequence, the ***Organizationally Unique Identifier (OUI)***, is assigned by the IEEE

MAC Addresses in a LAN

- MAC example:

```
00-10-a4-13-6c-6e
```

- The vendor assigns the **second three pairs**
- Within a LAN, every device that has a NIC will have a MAC address. Such devices include:
  - Computers
  - Smartphones and tablets with WiFi
  - A router
- Communication within the LAN is from NIC to NIC, using MAC addresses, whereas communication across networks uses IP addresses

Ethernet frame structure

- An Ethernet frame consists of ***eight*** components:

Preamble	**Start Frame Delimiter**	**MAC Address: Destination**	**MAC Address: Source**	**Length or Type**	**Data/ Payload**	**Pad**	**Frame Check Sequence**

- In some cases, adjacent components may be merged and treated as a single component
- Also, some parts of the frame are *data-link* specific, whereas others are added at the *physical* layer
- As we will see, higher layers of networking have their own units (e.g. packets), as well...

Ethernet frame structure

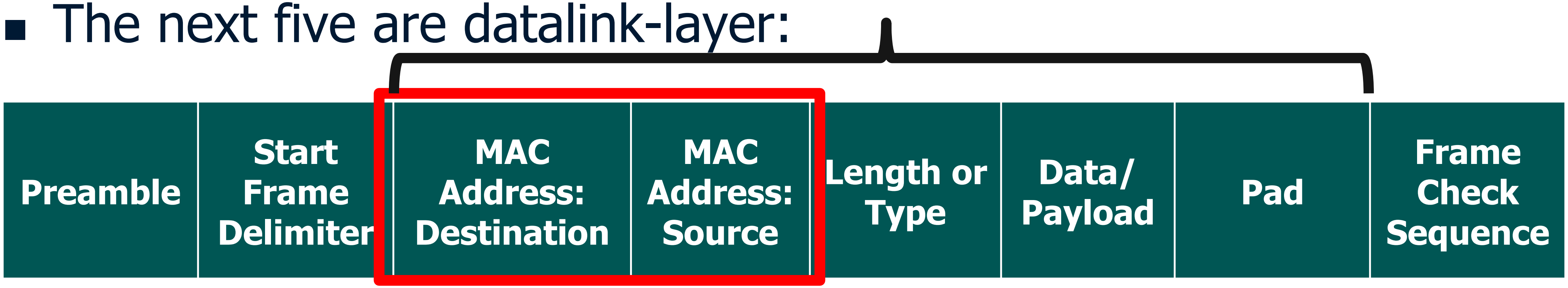
- The first two components are physical-layer:

Preamble	Start Frame Delimiter	MAC Address: Destination	MAC Address: Source	Length or Type	Data/ Payload	Pad	Frame Check Sequence

- The ***preamble*** is a series of 56 alternating bits (1s and 0s) for synchronization, whereas the ***start frame delimiter*** is a series of eight bits: **1 0 1 0 1 0 1 1**.
- Together, they are 64 bits, or 8 bytes
- The last two bits (**1 1**) break the alternating sequence and signal the start of the data-link layer component.

Ethernet frame structure

- The next five are datalink-layer:

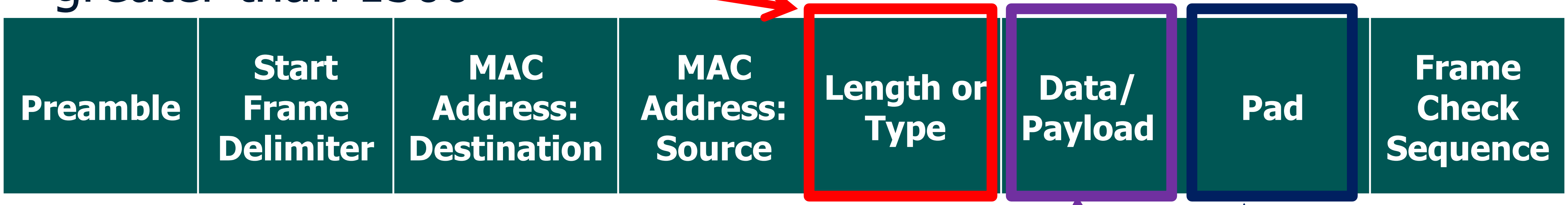


Preamble	Start Frame Delimiter	MAC Address: Destination	MAC Address: Source	Length or Type	Data/ Payload	Pad	Frame Check Sequence

- Each device (computer, router, etc.) on the network will have some type of network adapter, often called a *network interface controller* (NIC), for connecting to a network
- That adapter will have a unique, 6-byte identifier – normally expressed in hex digits – called a ***MAC address***
- What does "MAC" stand for?

Ethernet frame structure

- The fifth component will differ based on data size – ***length*** for data less than 1500 bytes and data format, or ***type***, for data greater than 1500

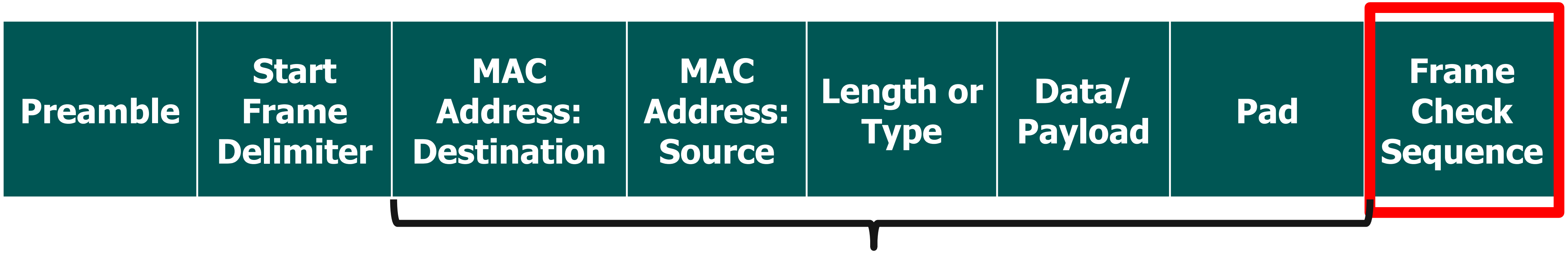


Preamble	Start Frame Delimiter	MAC Address: Destination	MAC Address: Source	Length or Type	Data/ Payload	Pad	Frame Check Sequence

- The ***data***, or "payload", is the packet from Layer 3 – which, in turn, includes data from higher layers.
- If the data component is less than 46 bytes in size, then there will be a ***pad*** to bring it up to 46

Ethernet frame structure

- Finally, the last component – like the first two -- is physical-layer:



Preamble	Start Frame Delimiter	MAC Address: Destination	MAC Address: Source	Length or Type	Data/ Payload	Pad	Frame Check Sequence

- The 4-byte ***frame check sequence*** is calculated based on the bits in the 3rd through 5th components (i.e., the data-link section).
- This is used to detect errors in data transmission, in which case the frame is discarded.

The `ipconfig` command

- The following information is Windows-specific, but there are equivalents for Unix-based operating systems.
- To find configuration information about the network adapter(s) on your computer, you can use the ***`ipconfig`*** command.
  - Open a command line utility, such as ***`Command Prompt`*** or ***`PowerShell`***
  - Type this → ***`ipconfig`***
  - Add any options, as needed
  - Press Enter
- Usually, you will want to use the "all" option, which gives you the most information: ***`ipconfig /all`***

IP Addresses

- A MAC address can identify a host on a LAN, but to identify it outside of the LAN, you will need an alternative identifier
- An IP (Internet Protocol) address consists of four 8-bit values:
  - Each ranging from 0-255
  - Expressed in decimal (base 10)
  - Separated by periods
- An IP address will consist of two parts:
  - A *network* number, identifying the source/destination network
  - A *host* number, identifying the host (i.e., the device)

The *ping* command

- Command name stands for **P**acket **In**ternet **G**roper
- You can use it to test whether or not one device/host is reachable from another
  - Within a LAN
  - Over the Internet
- The most basic use of the command uses one argument – the destination URL or IP address. Example:

```
C:\> ping 10.0.0.148

   Pinging 10.0.0.148 with 32 bytes of data
```

- See textbook for other options (number of packets, time, etc.)

The *ping* command

- A *successful* ping might look like this:

```
Reply from 10.0.0.148: bytes=32 time<1ms TTL=128
Reply from 10.0.0.148: bytes=32 time<1ms TTL=128
Reply from 10.0.0.148: bytes=32 time<1ms TTL=128
Reply from 10.0.0.148: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Versus an *unsuccessful* ping:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.148:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Twisted-Pair Cabling

- In terms of physical connections in computer networks, one of the most common media you will find is **`unshielded twisted-pair`** (UTP) cabling.
- In general, "twisted pair" signifies pairs of insulated copper wires, twisted around one another
- In computer networking, it generally refers to *Ethernet cables*:
  - Category 3 (**`CAT3`**)
  - Category 5 (**`CAT5`**) and 5e (**`CAT5e`**)
  - Category 6 (**`CAT6`**)
  - And more…

Twisted-Pair Cabling

- Twisted-pair cables of Categories 5, 5e, and 6 will consist of *four* **color-coded**, ***twisted*** pairs:
    - **Green and Green/White**
    - **Blue and Blue/White**
    - **Orange and Orange/White**
    - **Brown and Brown/White**
- They will be terminated in an ***RJ-45*** connector, or ***8P8C*** (8 position, 8 contact) – since each wire will have a specific place in the connector.

Understanding Cable: Terms

- To start, consider some measurement terminology…
  - Data units:
    - **`bit`**: Smallest unit of data, with two possible values: **`1`** or **`0`**
    - **`byte`**: A grouping of 8 bits – also called an *octet*. It is the fundamental unit for measuring data.
  - Data transmission:
    - **`hertz`** (***Hz***): A measurement of frequency, where 1 Hz = 1 cycle per second
    - **`bits-per-second`** (***bps***): A measurement of data transmission speed across a connection (Ethernet cable, wireless, etc.)

Understanding Cable: Terms

- Measurement prefixes:
  - **Kilo-** : One thousand (**10^3**) – 1,000
  - **Mega-** : One million (**10^6**) – 1,000,000
  - **Giga-** : One billion (**10^9**) – 1,000,000,000
  - **Tera-** : One trillion (**10^{12}**) – 1,000,000,000,000

- Also, we have terms relating to data transmission *speed*:
  - ***Bandwidth***: Generally refers to a communication channel's (e.g., UTP cable) *capacity* for transmission – usually expressed in ***Mhz***
  - ***Network congestion***: When transmission quality degrades due to data traffic exceeding a channel's capacity.

Understanding Cable: Terms

- ***Bottlenecking***: Another term for network congestion
- Directionality
  - ***Full-duplex***: Channel can send/receive concurrently
  - ***Half-duplex***: Channel can only send or receive, at any specific time
- Other
  - ***Latency***: Time for sending (and/or receiving) a packet
  - ***Signal-to-noise ratio***: Ratio of a *signal strength* (or statistical pattern) to *interference*, or "noise". Measured in decibels (dB)
  - ***Throughput***: A measure of *successful* data transmission, often expressed in ***bps***, with appropriate prefixes

Understanding Cable Types and Speed

- Twisted-pair cables are grouped into different ***categories***, which specify their upper limits with regard to bandwidth and data transmission speed.
- We will look at some now….
  - **CAT3:** Two twisted pairs of copper wire, terminated with an RJ-11; mostly used in landline telephones now, but used for Ethernet in the past. **Bandwidth: 16 Mhz**
  - **CAT5:** Four twisted pairs, color-coded. RJ-45 termination. Commonly used for Ethernet. **Bandwidth: 100 Mhz**
  - **CAT5e:** Same construction as CAT5, but with more stringent testing. Many CAT5 cables may actually meet these requirements….

Understanding Cable Types and Speed

  - **CAT6:** Wires generally thicker than CAT5/5e, along with an internal separator. **`Bandwidth: 250 Mhz`**
  - **CAT6a:** More tightly wound pairs. **`Bandwidth: 500 Mhz`**
  - **CAT7/7a:** Not recognized by TIA/EIA. **`Bandwidths: 600 Mhz/1 Ghz`**
- Different cables will be able/tested to support different…
  - Data rates
  - Duplex modes
  - Directionality
- Some of these cables may also support *higher* data rates than normal, but at *shorter lengths*.

	CAT 3	CAT 5	CAT 5e	CAT 6	CAT 6a	CAT 7/7a
10 Mbps	√	√	√	√	√	√
100 Mbps	🟥	√	√	√	√	√
1000 Mbps	🟥	√	√	√	√	√
10G Mbps	🟥	🟥	🟥	to 55 meters	√	√

- Higher categories have features like shielding and must meet stricter requirements
- 7a (at short distances) can handle 40 Gigabit -- and even 100 Gigabit! -- Ethernet

Fiber-Optic Basics

- Fiber-optic cabling is becoming more common for providing high-speed network cabling – displacing copper, in many places
- In particular, it is useful for supporting faster variants of Ethernet, such as 10 Gigabit and higher.
- Requirements are defined in the TIA/EIA 568-B.3 standards.
- A fiber-optic network features four components (*Figure 3.1*):
  1. ***Fibers*** (within cables) that carry data as (modulated) light beams
  2. A light ***source*** that places data/signal onto the beam
  3. A light ***detector*** that converts the (optical) signal back to electrical
  4. Optical ***connectors*** linking the cable to the source and detector

Fiber-Optic Basics

- As compared to copper, fiber-optic cabling features many substantial advantages:
  - Most notably, the bandwidth is much higher – allowing for speeds well over 10 Gbps, when using laser light sources.
  - Also, fiber-optic cabling reduces or eliminates much of the signal issues of copper – electrical noise, crosstalk, and attenuation.
  - In addition, there are several practical advantages outside of speed and signal:
    - Reduced costs of fiber-optic cabling
    - Elimination of electrical hazards
    - No vulnerability to corrosion
    - Very difficult to tap or intercept

Optical Anatomy

- In some ways, the construction of fiber-optic cables is considerably simpler than that of twisted-pair.
- A basic cable will consist of three layers:
  - **Core:** Carries the light down the cable
  - **Cladding:** Surrounds the core and has a lower refractive index so that the transmitted light will be continuously reflected inside and through the core.
  - **Jacket:** A protective coating of plastic
- Aside from these basics, optic fiber may vary in thickness, material, and modes (of signal propagation).

Optical Anatomy

- One important factor for any kind of fiber is its **numerical aperture**, the ability to accept light and have the signal fully propagate.
  - A cable will have a range of directions – an acceptance cone – from which it can accept light and still experience TIR.
  - The cone will make an angle, and the numerical aperture is calculated based on that cone.
  - Similarly, if you know this value, then you can determine the range of the cone.

Optical Hardware

- To recap, the four main piece of fiber optic hardware are: light sources, light detectors, the intermediate components (i.e., fiber), and connections.
- To begin with, the electrical signals must be converted into light pulses by either of two types of ***sources***:
  1. **Diode Laser (DL)**: Can send data more quickly and put more signal power into a thinner fiber, more efficiently than LED. However, it also more expensive than LED and requires more complex circuitry.

Optical Hardware

2. **Light-Emitting Diode (LED):** These are not as fast or powerful as DL, but they are cheaper and easier to maintain. Their wider wavelengths mean that they are more susceptible to problems like dispersion.

- In addition, there are other forms of lasers used:
  - **Distributed feedback (DFB) lasers**, which are used in in **dense wavelength division multiplex (DWDM)** systems
  - **Vertical cavity surface emitting lasers (VCSELs)**
  - **Tunable lasers**, whose emission wavelength can be altered

Optical Hardware

- The primary form of intermediate hardware (i.e., channels of signal transmission) is the fiber-optic strand, often called…
  - **Fiber**
  - **Light pipe**
  - **Glass**
- Beyond this, there are other – more specialized – forms of intermediate hardware:
  - **Isolators**, which keep the optical power flowing in a single direction
  - **Attenuators**, which reduce signal into a receiver
  - Other devices for splitting or altering signal

Optical Hardware

- For effective signal transmission, fibers must be properly aligned with sources and detectors.
- Various alignment problems (Figure 3-13) may result in signal loss. Much of this can be achieved through effective joining:
  - Splicing is joining two fibers together, by one of two methods:
    1. **Fusion splicing**: A more permanent physical fusing/welding of the two. Video: **https://youtu.be/DIiBVuuRUtM?t=175**
    2. **Mechanical splicing**: Here, the splices leaves an air gap between the two fiber ends, which is filled with an **index-matching gel**

Optical Hardware

- Just as copper twisted-pair cables have (typically) RJ-45 ***connectors***, there are also several for fiber-optic cables.
- Some of the more common ones are SC, ST, FC, LC, and MT-RJ – which you can see in Figure 3-14
- Several concerns factor into connector choice
  - Ease of installation
  - Insertion loss and return loss
  - Repeatability
  - Cost
- Fiber-optic cable termination:

  https://www.youtube.com/watch?v=rKWLCVgkNtM

Optical Networking

- As networking needs increase – so do demands for transmission bandwidth, creating scenarios that fiber-optic networking is well positioned to address:
  - Fiber expense (relative to copper) is diminishing
  - Fiber offers higher bandwidth and security – and over longer distances than copper
- Fiber-optic network types
  - **SONET/SDH**
  - **Optical Ethernet**

Optical Networking

- For many years, the SONET (**s**ynchronous **o**ptical **net**work) and SDH (**s**ynchronous **d**igital **h**ierarchy) were key in long-haul optical networking, offering…
    - Increase in network reliability
    - Network management
    - Defining methods for synchronous multiplexing of digital signals
    - Defining a set of generic operating/equipment standards
    - Flexible architecture

Optical Networking

- SONET/SDH defines a *hierarchy* of data rates:

Signal	Bit Rate	Capacity
OC-1 (STS-1)	51.840Mbps	28DS-Is or 1 DS-3
OC-3 (STS-3)	155.52Mbps	84DS-Is or 3 DS-3s
OC-12 (STS-12)	622.080Mbps	336 DS-1s or 12 DS-3s
OC-48 (STS-48)	2.48832Gbps	1344 DS-1s or 48 DS-3s
OC-192 (STS-192)	9.95328Gbps	5376 DS-Is or 192 DS-3s

- Acronyms:
  - **OC – optical carrier**
  - **STS – synchronous transport signals**
  - **DS – digital signal (**1 → 1.544 Mbps**,** 3 → 44.736 Mbps**)**

Optical Networking

- Optical Ethernet has several numerics, similar to those given for twisted pair
  - In the case of fiber-optic, we assume distances of up to **2 km** (for multimode fiber) or **10 km** (for single mode)
  - Examples include:
    - ***10BASE-F*** : 10 Mbps over fiber (generic specification)
    - ***100BASE-FX*** : 100 Mbps over two strands of fiber
    - ***1000BASE-LX/SX*** : Gigabit with long-/short-wavelength transmitters
    - ***10GBASE-R/W*** : 10 Gigabit for LANs and WANs
- Converters will be required.

Optical Networking

- Distribution in a fiber network will involve a number of considerations:
    - ***Lines:*** At least two fibers, Tx and Rx, for full-duplex operation
    - ***Cross-connects:***
        - Joining fibers, often through mechanical splicing
        - Converters, for moving between optic and electrical signals
    - ***Fiber Maps:***
        - ***Logical:*** A model of the network's structure, with links and levels
        - ***Physical:*** Fiber routes, within the concrete environmental context

Safety

- Working with fiber optic cables may entail some hazards beyond those of twisted-pair, so be careful…
  - One primary danger is getting light in your eyes
    - Even more so because fiber is transmitting wavelengths the eye cannot see
    - Never look into a cable's end!
  - Also be wary of mechanical hazards, such as brittle ends of fiber.
- Safety glasses are a must!

Introduction

- So far, we have been looking at OSI Layers **#1** and **#2** -- the physical layer
- 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.

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

- 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:

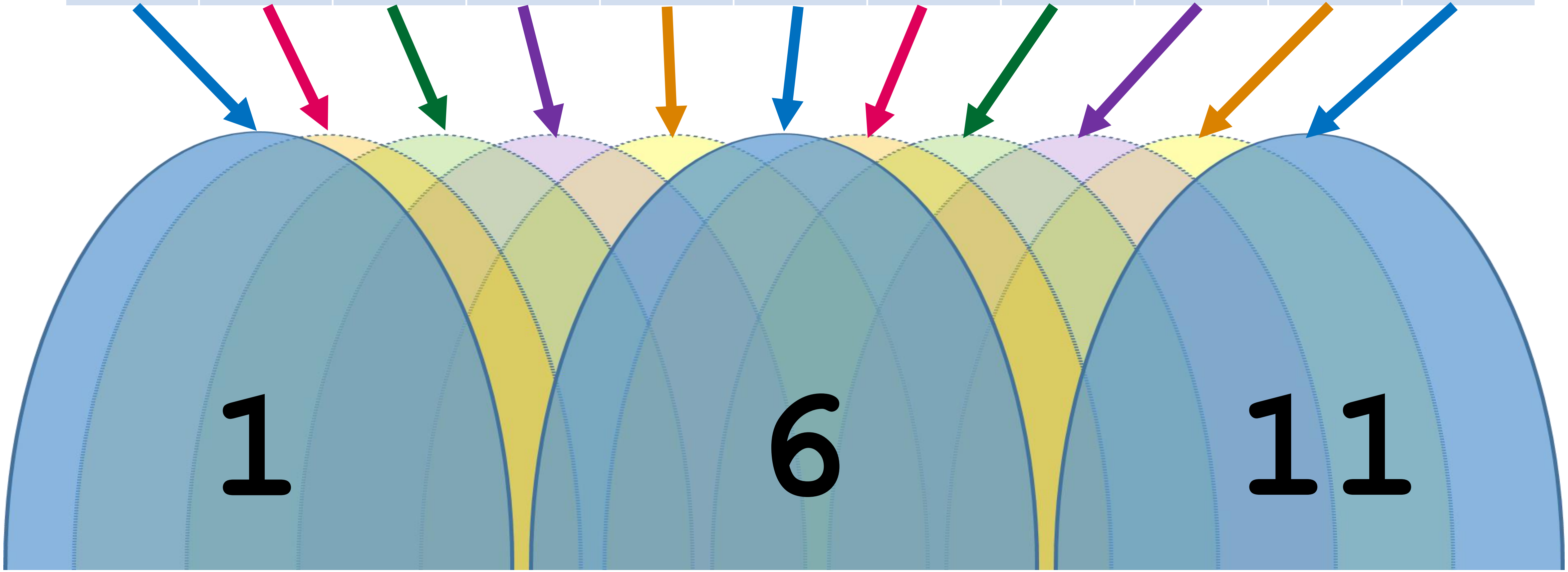
Suffix	Data Rates	Range	Frequencies
a	Up to 54 Mbps	Up to 75 ft.	5 GHz
b	Up to 11 Mbps	100-150 ft.	2.4 GHz
g	Up to 54 Mbps	Up to 150 ft.	2.4 GHz
n	200+ Mbps	Up to 150 ft.	2.4 GHz or 5 GHz
ac	Up to 1 Gbps	115 ft.*	5 GHz

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

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

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**

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.

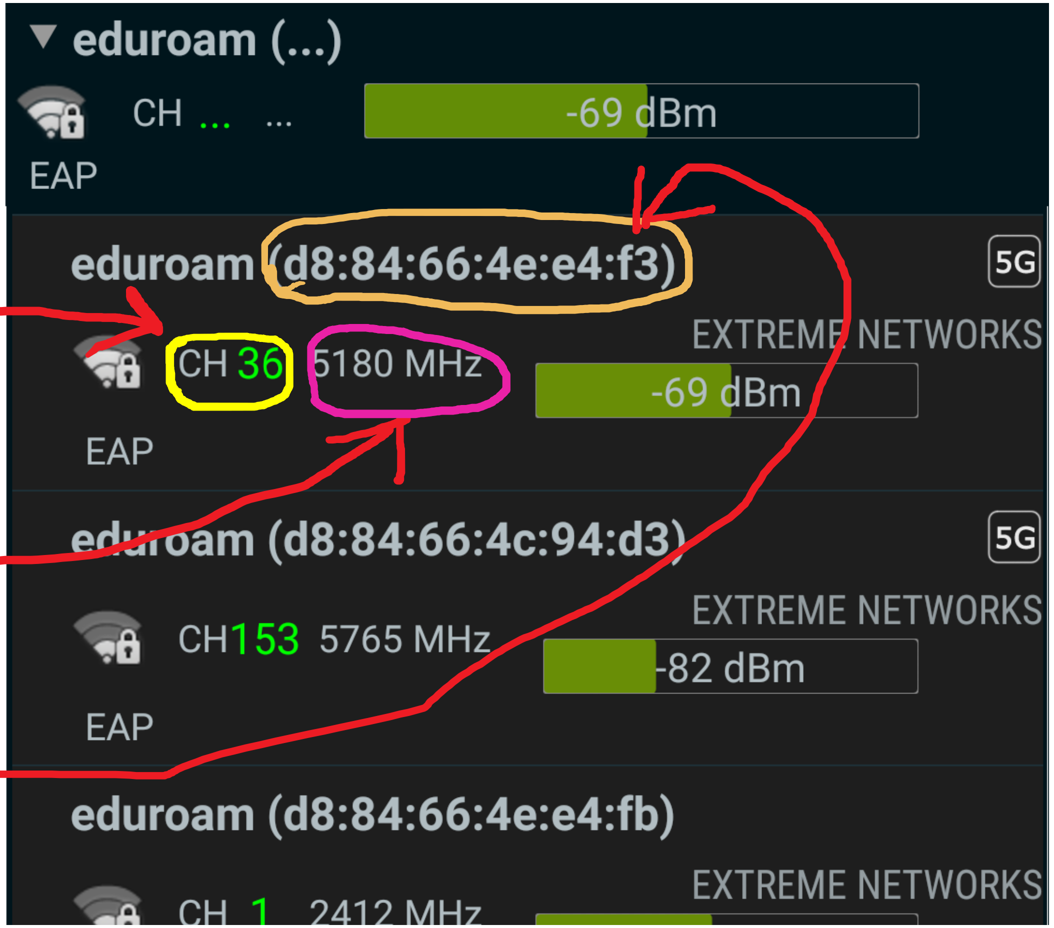
Site Surveys - Examining signals

- 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)



▼ eduroam (...)

CH ... ... -69 dBm

EAP

eduroam (d8:84:66:4e:e4:f3) 5G

EXTREME NETWORKS

CH 36 5180 MHz -69 dBm

EAP

eduroam (d8:84:66:4c:94:d3) 5G

EXTREME NETWORKS

CH153 5765 MHz -82 dBm

EAP

eduroam (d8:84:66:4e:e4:fb)

EXTREME NETWORKS

CH 1 2412 MHz

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…

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.

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.