WEEK 9
TCP/IP, PHYSICAL AND DATA LINK LAYERS

PHYSICAL LAYER

Physical (hardware) layer: lowest level layer of the Internet Model.

- Contains the actual network hardware – cables, antennas, network interfaces
- Standardises so that devices from different manufacturers can interoperate
- Devices directly connected by a cable or radio link exchange messages at the physical layer

How is a message sent from client to server?

1. In the client, the message is represented digitally as a sequence of bits.

2. the message is passed to the data-link layer software, containing the address of the sender and receiver.

*The data-link layer controls the Network Interface Card (NIC), which is the hardware that establishes connection to the network and instructs the hardware to send the message.

3. The physical layer hardware translates the bits of the mesage into signals, which are then transmitted through a medium to the switch.

4. In the switch, the physical layer hardware receives the signal and decodes it back into bits.

5. The data link layer software interprets the bits – checks destination address.

6. The data-link layer software forwards the message to the destination by sending it through the physical port that the server is connected to.

7. The physical layer converts the bits into a signal, which is transmitted through a medium to the server.

8. In the server, the physical layer (in the NIC) receives the signals and translates them to bits

9. The data link layer reconstructs the message, checks it is received correctly and passes it on to the higher-level layers

NETWORK HARDWARE

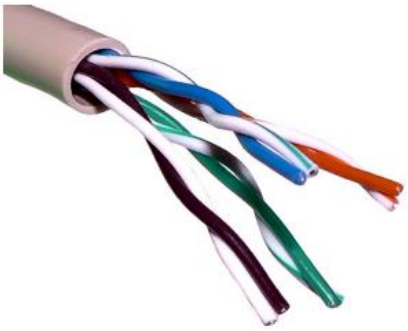
Network Interface Cards (NIC): hardware that connect devices to the network.

- For wired networks, the NIC is in the form of a socket, where you can plug in a cable
- For wireless networks, the NIC is connected to an antenna
- In the early days of networking, they were physical “cards” that you would slot into your PC in order to connect to a network
- Today, most computers have multiple NICs. Eg. a smartphone has at least three NIC – one to connect to 3G/4G network, WiFi network and other devices via Bluetooth

Network cables can be distinguished by its material. There are 4 types of cables:

1. Unshielded Twisted Pair (UTP)
2. Shielded Twisted Pair (STP)
3. Coaxial Cables
4. Optical Fibre

Unshielded Twisted Pair (UTP): contains several pairs of copper cable, twisted together



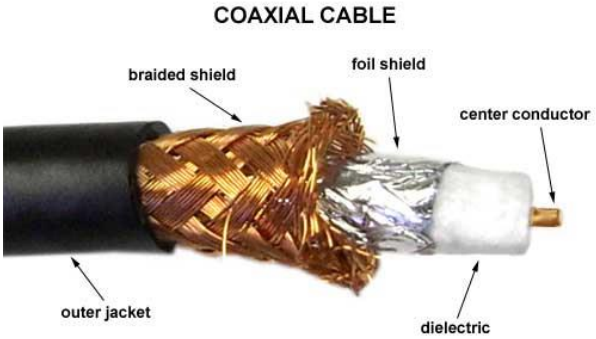
- Each copper cable is wrapped in a plastic insulation layer
- The cables are twisted in pairs
- All the pairs are wrapped together in another plastic insulation layer
- Cables are twisted to reduce interference
- It is the most common type of LAN cable
- There are different categories of UTP cables – the higher the number (eg. UTP-5), the better the quality of the cable, and the higher the transmission rate.

Shielded Twisted Pair (STP): similar to UTP, but adds metal shielding to provide better protection from electromagnetic interference

- Required for very high speed Ethernet (> 10GB/s)
- Required for environments with strong electromagnetic interference

Coaxial cables: an inner wire surrounded by an insulation layer and a wire mesh

- No longer common in network installations



Optical fibre cable: cable that contains optical fibres, which are used to carry light

- Used for networks that transmits light signals
- Laser lights are sent through the fibre, which conducts the light with very little loss
- Achieves higher data transfer rates than copper cables
- Not affected by electromagnetic interference
- <u>Common uses:</u>
    - Submarine cables to maximise data transfer between continents
    - Backbone networks to provide high-speed connections between switches

SIGNALS

Messages are transferred using physical signals

Signal: energy that travels through a medium

- Analogy – hearing a car alarm
    - The alarm is an "audio signal"
    - Physically, audio signals are sound waves which travels through the air
    - The wave is the energy, the air is the medium
- In computer networks…
    - Electrical signals (energy) travels through copper cables (medium)
    - Radio waves (energy) travels through space (medium)
    - Light waves (energy) travels through optical fibres (medium)

There are 2 types of signals:

1. **Digital:** waveform with a limited number of discrete states
2. **Analog:** a continuous wave, typically varying over time

Digital signals: a sequence of 0s and 1s that are sent through a wire

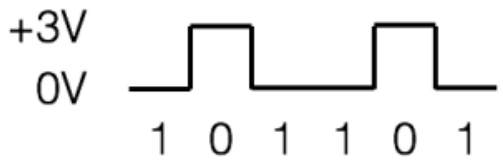
- Digital signals encode 0s and 1s into different voltage levels on a copper cable
- **Square wave:** used to represent digital signals graphically because the wave form rises and falls sharply.

There are 3 ways to encode bits into voltage levels:

1. Unipolar encoding
2. Bipolar encoding (Non-Return to Zero)
3. Manchester encoding

Unipolar encoding: only one polarity is used to encode the data (positive voltage)

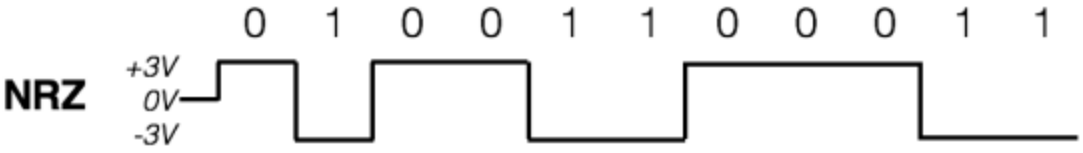
- Eg. 0V encodes a 0, some positive voltage encodes a 1. This could also be reversed



- In this example, 1 is 0V and 0 is +3V
- The horizontal axis represents time
- Over time, the sender switches the voltage from 0V to +3V, which the receiver detects
- <u>Disadvantage:</u> it can be difficult for the sender to distinguish between 0V and a small positive voltage, if there is noise in the signal.

Bipolar encoding: Non-Return to Zero (NRZ) is the simplest form of bipolar encoding, and it's where two polarities are used to encode the data (positive and negative)

- Eg. 0 is represented by a positive voltage, and 1 is represented by a negative voltage



How does the receiver detect two 1s in a row?

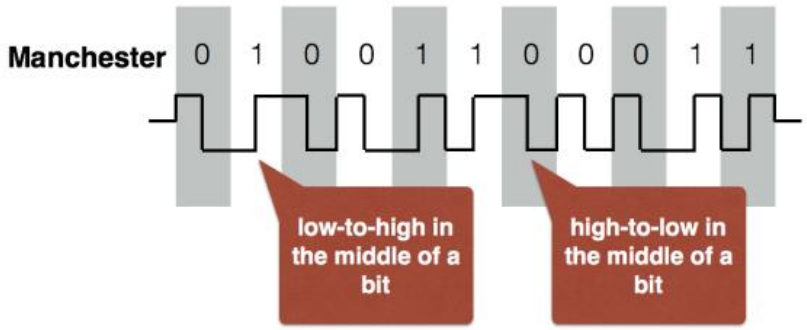
- **Time window:** a fixed time span that is defined, for each bit that's being transmitted
- Eg. For 1000 bits per second, the defined time window is 1 millisecond. The sender would send -3V for 2 milliseconds to send two 1s.
- This requires the receiver to synchronise with the sender, to find out how long the transmission of each bit is supposed to take

The easiest way to synchronise with the sender: send a sequence of 0s and 1s, so that the signal switches between the two states regularly.

- Disadvantage: if the receiver is a little bit faster of slower than the sender, it will cause the synchronisation to drift, which introduces errors

Manchester encoding: synchronisation signal is embedded into the data signal, so that the receiver can always re-synchronise itself. The data is transmitted in the middle of the time window.

- Eg. 0 is represented as a transition from positive to negative voltage, and 1 is represented as a transition from negative to positive voltage.



- In order to transmit two 1s or two 0s, the signal has to be "reset" in between the two bits

How does Manchester encoding fix the synchronisation problem?

- Since each bit is represented by a *transition*, rather than a *state*, we are guaranteed to have at least one change of voltage in each time unit
- The receiver can extract the timing from this information and continuously re-synchronise itself with the sender

Analog signals: data transmitted as analogy signals are transmitted as sine waves.

- **Sine wave:** used to represent analog signals graphically as the states change gradually from high to low.
- Digital signals only encode information into one aspect of the square wave. Analog signals can contain much richer information.

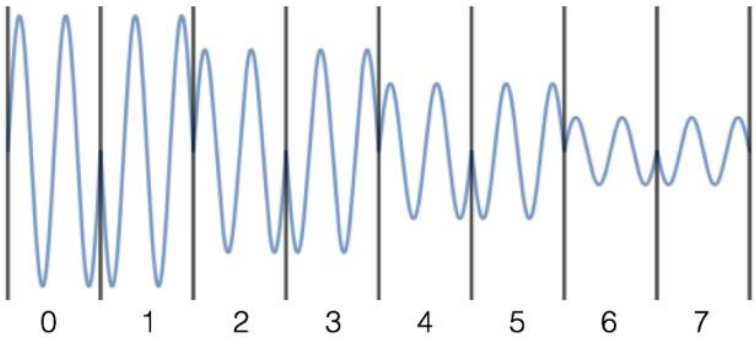
Analog signals can be describe using 3 parameters:

1. **Amplitude:** height of the wave
2. **Frequency/wavelength:** how many oscillations per second
3. **Phase:** the direction the wave is going at a particular time point

To transmit data, the parameters can be modified to represent a 0 or 1:

- **Frequency modulation (FM):** a high frequency could be 1 and low frequency could be 0
- **Amplitude modulation (AM):** a high amplitude could be 1 and a low amplitude could be 0
- **Phase modulation (PM) / phase-shift keying (PSK):** the wave starting in a downward direction could be 1, and the wave in an upward direction could be 0

Combining modulation techniques results in richer information:



- The image combines amplitude and phase modulation
- Eg. 3 is represented by the second-highest amplitude and the downward phase
- This results is a higher transmission rate, because four times the amount of data can be transmitted in a single time unit

Attenuation: the weakening of the signal with increasing distance from the transmitter
- The closer to the transmitter we are, the stronger the signal
- A wooden door, or light wall can cut the signal strength of WiFi in half

MODEM

Modulation: turning digital data into analog signals
Demodulation: turning analog signals into digital signals

Modem: a device that does both modulation and demodulation.
- **Early modems:** used a speaker to turn digital signals into acoustic signals (sound waves), which were transmitted through a telephone. A microphone records the sound and turns them into analog signals.
- **Second generation modems:** directly connected to a telephone line, avoiding the conversion to sound and back.
- Both modems are limited to the bandwidth of audio signals (frequencies that the telephone lines were designed to carry)

Asymmetric Digital Subscriber Line (ADSL): today's modem also uses a connection through telephone lines, however the receiving modem is only a few kilometres away
- Can use a much broader range of frequencies, don't have to be carried through the legacy phone network
- Achieves much higher data transmission rates

DATA-LINK LAYER

Data-link layer: responsible for controlling the hardware and for error detection

MEDIA ACCESS CONTROL

Media access control (MAC): the main function of the data-link layer, where it controls when a device is allowed to transmit

Only one device is allowed to transmit

There are 2 approaches to MAC:

1. **Controlled access:** only one device has permission to send at any point in time
    a. There are 2 ways for controlled access:
        i. There is a central authority, assigning permission to send
        ii. Permission gets passed from device to device
2. **Contention-based access:** access is provided on a first-come-first-served basis
    a. Usually, devices would avoid a transmission if they can "sense" another transmission
    b. **Collide:** when two devices start transmitted at the same time
    c. Contention-based MAC needs a mechanism for detecting when a collision occurs
    d. Advantage: no "central authority" is required, making it a natural choice for Ethernet

ETHERNET

Ethernet: a system for setting up a LAN, which has protocols that control the passing of information between devices to avoid simultaneous transmissions.

The original Ethernet used a single coaxial cable that was shared by all devices on the same LAN

- A new device could be connected by "tapping" the cable – dripping a tap wire through the insulation into the copper core
- Could deliver 10 Ambits/s

Nowadays, Ethernet mostly uses UTP cables connected to switches.

- Typical speeds are 1 Gbit/s in local networks
- And 10 Gbit/s in backbone networks

MAC in Ethernet is based on the **CSMA/CD method:**

- **CS – Carrier Sense:** a device "listens" to the network, and only starts a transmission when no other device is transmitting
- **MA – Multiple Access:** multiple devices share the same medium
- **CD – Collision Detection:** while a device is sending, it monitors the network
    - When it detects a collision, it immediately stops the transmission of the frame and transmits a **jam signal** instead.
    - **Jam signal:** makes it clear to all other devices that a collision has happened

Disadvantage of Collision Detection:

- If two devices detect a collision, two jam signals are sent, then both devices would re-transmit at the same time, leading to another collision
- Solution: the devices waits for a random, short amount of time before re-transmitting.

Each device only sends a single frame at a time, so other devices can jump in before it starts transmitting the next frame

There are 2 types of Ethernet topology:

1. Shared bus / multi-point topology
2. Star topology

Shared bus / multi-point topology: all devices are connected to a single long cable.

- Advantage: it is cheap.

There are 3 disadvantages of the Shared Bus topology:

1. All devices receive all messages that are sent into the network, even ones that are not meant for them.
    a. Solution: each message has a destination address, so each device checks whether the address matches their own. Only the intended recipient will process the message
        i. **MAC address:** each device in an Ethernet LAN has a unique address.
            - Each Ethernet NIC sold has a unique address hard-wired into it, so it can simply be plugged into an existing network without first configuring its address
            - Consists of 6 bytes (6 hexadecimal numbers separated by colons), eg. Ac:87:a3:14:9e:59
2. Maintenance is difficult.
    a. The entire network is affected if…
        i. Any physical connection wasn't done properly
        ii. Attached devices wasn't behaving as it should
    b. Solution: use a star topology.
3. The reliance on collision detection limits the size of the network

Star topology: devices are connected to a central hub.

- **Hub:** the central component. It is a small device with a number of sockets, so each computer could be connected to the hub using a cable
- Although physical topology is different, logical topology is the same as the bus – messages transmitted are sent to all devices. In hubs, this causes frames to be damaged in collisions.

Switched Ethernet: the hubs in a star topology is replaced with a switch. This changes the logical topology from bus to star.

- The circuit is no longer shared – messages are sent directly from one device to another
- **Switch:** a device, which forwards data packets to an appropriate part of the network, enabling logical start topology
    1. Reads an incoming frame, checks it destination MAC address, sends the frame to the correct port that is connected to the device with that address

How do switches work?

Let's assume A wants to send a message to B through a switch

1. The switch receives the message, but does now know which port B is connected to
2. The message is broadcasted to all ports (behaves like a bus topology)
3. Now, the switch knows which port A belongs to (port 0). This information is stored into a **forwarding table**.

Now, B sends a message back to A through the switch

4. The switch receives a frame addressed to A.
5. It looks up A's port in the forwarding table and sends the message directly to A
6. Now, the switch knows which port B belongs to (port 1).

Buffer memory: switches can include a buffer memory to make the transmissions more efficient

- A and B wants to send a message to D at the same time. The switch stores one frame in its buffer memory, and forwards the other one, eliminating collision.

WIRELESS LOCAL AREA NETWORKS (WLAN)

Wireless networks: standard way of connecting to the Internet

- 4G networking on mobile phone
- WLAN (WiFi) for laptop computers

There are 3 advantages of wireless networks:

1. Don't need cables
2. Access is more flexible, don't need to be close to a socket
3. Enables people to be mobile

IEEE 802.11: family of standards, known as WLAN or WiFi

- Each new version of the standard brings faster transmission rates (802.11a, 802.11b etc.)
- Other wireless technologies:
    1. **IEEE 802.16:** WiMax, a successor to WiFi and 3G
    2. **IEEE 802.15:** Bluetooth / Wireless Personal Area Network (WPAN), used to create small networks of personal devices

WLAN frequencies:

- WLAN uses radio waves to communicate
- The range of frequencies different devices can use is strictly regulated
- WLAN doesn't require permission to install a new wireless network, because it uses part of the spectrum that has been allocated to be used freely.

There are 2 main bands that WLAN devices can use:

1. Frequency of 2.4 Ghz
2. Frequency of 5 Ghz

Higher frequency means higher transmission rates

- Disadvantage: high frequencies have strong attenuation, meaning they become weaker with more distance

Channels: the IEEE standard defines a number of channels (frequency ranges) that WLAN devices are allowed to use. Allows for different wireless networks, which don't interfere with each other.

- There are 13 channels, each is about 22 Mhz wide.
- Most channels overlap, except channels 1, 6 and 11.

There are 2 scenarios, where WLAN networks are not set-up on different channels:

1. Neighbouring networks are set on channels 1 and 3: channel-1-network transmits, channel-3-network hears a lot of noise, where the frequencies overlap. This can lead to frames being received with errors, decreasing transmission rates.
2. Two neighbouring networks are set on channel 1: both networks can hear each other, which doesn't change the error rate, due to carrier sensing. However, both networks share the same frequencies, resulting in half the transmission rate.

There are 2 types of WLAN topologies:

1. Ad-hoc network / independent network / independent Basic Service Set (Independent BSS)
2. Infrastructure BSS

Independent BSS: a number of devices that can talk to each other.

- Behaves like Ethernet Bus topology, where a device sends a frame into the network, and all the other devices determines whether the process the frame or not

Infrastructure BSS: WLAN that uses a central Access Point (AP)

- **Access Point (AP):** connects the WLAN to the rest of the network using a cable-based Ethernet.
    1. At home, the AP may be integrated into the ADSL modem
    2. In organisations, multiple APs are around the building (Monash – attached to ceiling)
- All communication goes through the AP, behaves like a hub – all devices can still hear all messages, but only reacts to messages from the AP

Extended Service Set (ESS): Multiple APs connected to the same network are installed so that the area they cover overlap.

- All APs transmits the same identifier of the network, such as "eduroam"
- Allows mobile devices to **roam** between different BSSs.
- A device in an area covered by > 1 AP, connects by measuring their respective signal strengths.
- Roaming is done purely at the data-link level, meaning you can switch between APs, without it interrupting your other activities.

MAC in WLAN: similar to MAC in shared Ethernet, but instead of cables, transmissions are through radio waves.

- If two devices are close enough, they can detect when either device sends a frame to the AP
- **Hidden node problem:** if two devices are too far away from each other, they may not be able to detect the other device sending a frame to the AP as the signal becomes too weak.

WLANs uses CSMA/CA:

- **CA – Collision Avoidance:** this has 2 mechanisms…
    1. **Automatic Repeat Request (ARQ):** After sending a frame to the AP, a device will wait for *acknowledgement* from the AP that it was received correctly. If no acknowledgement is received, something is wrong, and the device waits a random time before re-transmitting
    2. **Controlled access:** the device sends a short "Request to Send (RTS)" message to AP. The device only transmits if it receives a "Clear to Send (CTS)" message from the AP. Not used in all wireless networks, only required where there are many WLAN devices.