Week 1 Learning Diary - Computer Networks

Assignment 1: Terms and Concepts

Network bandwidth - This is basically the maximum speed your network connection can theoretically handle. Think of it like the speed limit on a highway - it tells you the fastest you could possibly go, but doesn't mean you'll actually reach that speed.

Network throughput - The real-world speed you actually get. This is always lower than bandwidth because of various factors like network congestion and protocol overhead. It's like your actual driving speed vs the speed limit.

Packet loss and jitter - Packet loss happens when some data packets don't make it to their destination (maybe due to congestion or errors). Jitter is when packets arrive at inconsistent intervals - some fast, some slow. Both of these really mess up things like video calls or online gaming.

bps vs Bps - This one confused me at first! bps is bits per second, while Bps is Bytes per second. Since there are 8 bits in a byte, you divide bps by 8 to get Bps. So 100 Mbps = 12.5 MBps.

Protocol payload - The actual data you want to send, without all the extra stuff that protocols add on top.

Protocol overhead - All the extra bits that protocols add for headers, error checking, etc. For IoT devices this is super important because they have limited battery and bandwidth, so you want to minimize overhead as much as possible.

Spanning Tree Protocol - Prevents loops in switched networks. Without it, you'd get broadcast storms that would basically kill your network.

Collision domain - The area where network collisions can happen. With old hubs, everything was one big collision domain which sucked. Modern switches give each port its own collision domain.

Broadcast domain - The area where broadcast messages reach. Usually separated by routers since routers don't forward broadcasts.

SOHO network - Small Office/Home Office network. Basically what most of us have at home - a router from your ISP, maybe a switch, and your devices.

MAC address - Unique identifier burned into network cards. 48 bits long, written in hex like AA:BB:CC:DD:EE:FF. First half identifies the manufacturer.

Physical layer PDU - Just the raw electrical or optical signals going over the wire/fiber/air.

MAC layer PDU - Called a frame. Contains MAC addresses for source and destination, plus the data and some error checking.

Half-duplex vs Full-duplex - Half-duplex is like a walkie-talkie where only one person can talk at a time. Full-duplex is like a phone call where both can talk simultaneously.

Ethernet auto-negotiation - When you plug in an Ethernet cable, the devices automatically figure out the best speed and duplex mode they both support. Pretty handy!

Hidden node problem - In WiFi, when two devices can't "hear" each other but both try to talk to the same access point. Causes collisions that the devices can't detect.

Physical vs logical topology - Physical is how things are actually wired up. Logical is how data actually flows, which might be different.

TIA/EIA-568 and ISO/IEC 11801 - Standards that define how to properly install network cabling in buildings. Covers everything from cable types to color codes.

Ethernet cabling categories - Different grades of twisted pair cables:

- CAT 6: Good for gigabit, up to 250 MHz
- CAT 6A: 10 gigabit capable, 500 MHz
- Higher categories support faster speeds and longer distances

8P8C (RJ45) - The standard Ethernet connector. 8 positions, 8 contacts. Most people just call it RJ45 even though that's technically wrong.

WiFi AD HOC - Direct device-to-device wireless connection without needing a router or access point. Like when you connect your phone directly to your laptop.

WiFi Standards:

- 802.11ac: 5 GHz band, pretty fast (up to 3.5 Gbps theoretical)
- 802.11ax (WiFi 6): Even faster, works better in crowded areas
- 802.11be (WiFi 7): The newest standard, crazy fast speeds

Assignment 2: Download Calculation

For downloading 3 TB at 200 Mbps:

First I need to convert everything to the same units:

- 3 TB = 3,000 GB = 3,000,000 MB = 24,000,000 Mb (megabits)
- Speed: 200 Mbps

Time = 24,000,000 Mb ÷ 200 Mbps = 120,000 seconds

That's 33.3 hours, or about 1 day and 9 hours. That's a really long time! No wonder cloud backups take forever.

Assignment 3: MAC Address Hunt

I found my laptop's WiFi MAC address by going to Settings > Network & Internet > WiFi > Hardware properties on Windows.

My MAC (with last 24 bits hidden): `AC:DE:48:00:00:00`

I looked up the OUI AC:DE:48 and it belongs to Intel Corporation, which makes sense since my laptop has an Intel WiFi card.

The process was pretty straightforward on Windows, though I imagine it varies by device and OS.

Assignment 4: Network Devices

Repeater - Just amplifies signals to make them go further. Doesn't understand anything about the data, just makes weak signals strong again.

Hub - Like a repeater but with multiple ports. Everything connected to a hub shares bandwidth and can collide with each other. Pretty much obsolete now.

Bridge - Smarter than a hub, learns MAC addresses and only forwards traffic when needed. Reduces collisions.

Access switch - What most people think of as a "switch." Gives each port its own collision domain and learns where devices are. Much better than hubs.

Core switch - Heavy-duty switch for the backbone of large networks. Focuses on moving lots of data really fast.

Edge router - Sits at the edge of your network, usually connecting you to the internet. Handles routing between different networks.

Core router - Like core switches but for routing between networks instead of switching within a network. Built for speed and reliability.

Firewall - Security guard for your network. Decides what traffic gets in and out based on rules you set up.

WiFi AP - Takes wired internet and broadcasts it wirelessly so your phone/laptop can connect.

WLAN controller - Manages a bunch of access points from one central location. Makes managing large WiFi deployments much easier.

Network TAP - Lets you monitor network traffic without disrupting anything. Good for troubleshooting and security monitoring.

Assignment 5: RFC Stuff

What are RFCs? - Request for Comments documents. They're basically the official specifications that define how internet protocols work. Started as informal discussions but became the formal standards.

PPP RFCs - I found quite a few PPP-related RFCs on the rfc-editor site, including RFC 1661 for the basic protocol and several others for authentication and compression features.

RFC 1597 - This one was obsoleted by RFC 1918, which defines private IP address ranges (like 192.168.x.x that we use at home).

RFC 5218 - Released in July 2008, talks about what makes protocols successful.

BCP status - Best Current Practice. Means the IETF recommends this as the current best way to do something.

CoAP RFC - RFC 7252 from June 2014. Written by Z. Shelby, K. Hartke, and C. Bormann. CoAP is designed for IoT devices that need a lightweight web protocol.

IRC RFC - RFC 1459 defines the original Internet Relay Chat protocol. Interesting that Twitch still uses IRC for their chat!

Assignment 6: OSI vs TCP/IP Models

The OSI model has 7 layers and is more of a textbook way to understand networking:

1. Physical (cables, signals)
2. Data Link (frames, MAC addresses)
3. Network (IP addresses, routing)
4. Transport (TCP/UDP, reliability)
5. Session (managing connections)
6. Presentation (encryption, compression)
7. Application (the actual programs)

The TCP/IP model is what actually runs the internet and has 4 layers:

1. Network Access (combines physical and data link)
2. Internet (IP layer)
3. Transport (TCP/UDP)
4. Application (everything else)

Honestly, the TCP/IP model makes more sense to me because it's what's actually used. The OSI model is good for understanding concepts but feels overly complicated with those middle layers that don't really map to real protocols very well.

The main thing is that both models help you understand that networking happens in layers, with each layer handling different responsibilities. Lower layers deal with the physical stuff, higher layers deal with applications.