Networking Intro

By Jarrett Lane

You communicate across the world in 3 seconds

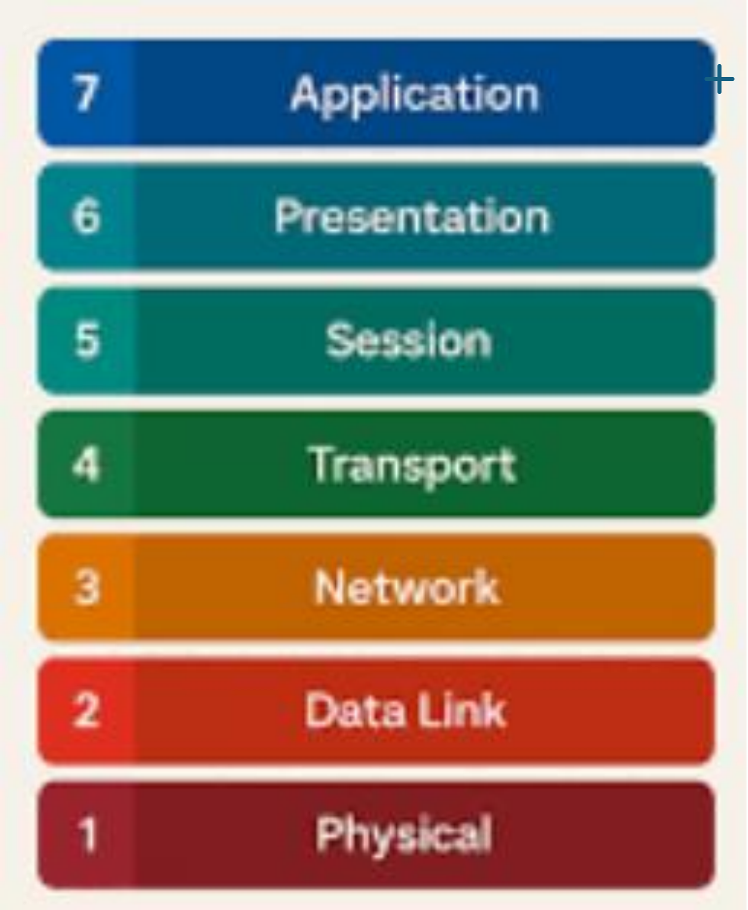
- This is done thanks to networking, the internet is one of the most impactful inventions made by humans, and understanding how it works is important
- It is not only useful but also very interesting to know
- Having a bit of STEM or CS background is good, but anyone can read these slides and learn something

Understanding networking

- Networking is the connection of multiple devices allowing for communication between them
- Networking has many layers and stages, these layers come together to form the internet
- Think about playing a videogame, are you playing a game, launching an app on your computer, or making a ton of 1s and 0s in your hardware act a certain way? All three
- Same concept with networking, understanding the different layers will help you understand how computers communicate across the world

OSI model

- You might be thinking: why tf are we starting with three letter abreviations?
- I dont like them either but this one is good to know, it stands for Open Systems Interconnection and it helps us understand how the internet works
- These layers work together to send various kinds of network traffic to designated destination computers



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

OSI Layer 1: Physical

- To connect things, they need a way to physically send bits to each other, this can be via electric signals via ethernet cables, light signals via fiber optic cables, and radio waves via WiFi, and more.
- We say this is the physical layer, this allows for a connection to even happen in the first place
- Often times, traffic is sent over multiple kinds of physical mediums throughout its journey

OSI Layer 2: Data Link

- In most settings, you have multiple devices connected at once
- Lets say you have 5 packages to send to 5 different people, would you bring them to a post office and address them to those 5 people, or would you personally deliver each package to each person? Unless you are a meth dealer chances are you will use a post office.
- Same with computers, would you rather connect one computer to five others with five different wires, or send traffic to a device that can distinguish the different computers and forward the traffic to the appropriate destination, you will probably choose the device.

OSI Layer 2: Data Link Continued

- The device we use as our "post office" is called a switch
- In networking, a switch is a device that can distinguish multiple computers connected to it and send traffic to the proper destination
- How does a switch know which computer is which? A MAC (Media Access Control) address.

OSI Layer 2: Data Link Continued

- A MAC address is a value that is assigned to a device in a piece of hardware called a NIC (Network interface card)
- We use the NIC to allow devices to connect to other devices, and these NICs have unique MAC addresses that identify the device
- So now you understand that the data link layer allows multiple devices to be connected and communicate with one another in a way that traffic is sent to the correct destination

OSI Layer 3: Network

- Now a group of devices can connect and communicate easily, but what if one device wants to communicate to a device in another group?
- Lets call these groups Networks
- Why have different networks? Well switches can only take so many connections, and we cant really make one big switch for all the devices in this world, thats like having one big post office to deliver all of the mail in the world
- This is why we divide things up to manage the wide scale of all of these devices communicating
- This is what the internet is, a combination of networks

OSI Layer 3: Network Continued

- To continue with the post office example, lets say we have two towns, Alice in town A wants to talk to talk to Bob in town B, if they deliver a letter to the post office addressed to the person in town B something new happens.
- We cant just address to Bob because bob doesnt live in town A so the post office will be like "Who is this?" Thats why on the letter Alice writes "Town B" so when the post office sees the letter, they know "Oh ok he lives in a different town, lets send it to their post office"
- Now Bob will get the letter.

OSI Layer 3: Network Continued

- Notice how when Alice addressed to Bob, she didnt just mention his name, but also his town. This is where the network layer comes in.
- Just like in our example, we have two different addresses for a device: MAC and IP (internet protocol)
- An IP address defines a device in the context of which network it is apart of and where on that network it is located, rather than knowing the physical address, the IP address tells you how to find the device in a more logical way.

OSI Layer 3: Network (the hard part)

- Before going onto layer 4 I want to slightly get into the more confusing parts of layer 3, I will make it easy so dont worry
- One thing that is important to understand is how networks can be split
- Think about an apartment complex, this complex may be one location, but it is made up of multiple buildings and those buildings have multiple housing units.
- Same with networks, one network can be comprised of multiple smaller networks comprised of multiple devices
- We call these smaller networks subnets

OSI Layer 3: Network (the hard part) continued

- To be able to handle this, we split IP addresses into different types: public and private, as well as split the address itself into networks and hosts (devices).
- Without getting into numbers, here is what each split means
- Public VS Private:
    - When we send traffic outside of our network, we send it through a device called the "Gateway" The gateway is the only device that can directly communicate with other networks, so when it is sending traffic across the internet, it has its own public address, this public address basically defines the network. When the gateway talks to our device, it will use its own private address that distinguishes it on our local network. This private address defines the gateway device itself

OSI Layer 3: Network (the hard part) continued

- Network VS Host:
  - If we are using subnets, we can use the IP address to distinguish both which subnet the device is on, and which device on that subnet to communicate with. The network part distinguishes the subnet and the host part distinguishes who on that subnet
- This may be confusing but lets tie it back to the apartment. When you send mail to an apartment, you need to know which apartment complex to send it to (Public), now where in that complex does the letter go (private). Well first check the building number (Network) then the room number (Host)
- I hope this helps, it is a bit tricky at first, ask me questions if you want me to elaborate

OSI Layer 4: Transport

- IRL, we send different kinds of mail, maybe we are sending a letter, maybe we are sending a package. What kind of letter? Bills or birthday card. What kind of package? Amazon delivery or something from your Grandma?
- Also how is this mail being sent, is this mail fragile, does it need to be delivered fast?
- It is important to pay attention to how certain mail is sent, because if you order a TV and it wasnt handled properly, you'll get your TV, but it probably wont be intact

OSI Layer 4: Transport Continued

- This also applies with networking, is the traffic an email or a youtube video, is speed or error handling more important? Here is where the transport layer comes in.
- In the transport layer, we distinguish traffic based on ports and protocols that specify what the traffic is for and how it should be sent

OSI Layer 4: Transport Continued

- Traffic can be sent in two main ways over the internet: Via TCP and UDP protocol
- The TCP protocol sends traffic by establishing a connection with a three way "handshake". This handshake is basically two devices agreeing to monitor their communication to avoid errors and send reliable and accurate traffic
- The UDP protocol doesn't care about establishing a formal connection and just sends data when asked to, which is faster but if error occur they are ignored
- The TCP protocol is used for reliable connections and UDP for quick connections
- You will see TCP used with things like connecting to websites and UDP used with things like video streaming

OSI Layer 4: Transport Continued

- Traffic can vary, maybe the traffic is a web request or maybe its an email.
- We use ports to distinguish this traffic so data is correctly classified. Ports are basically just logical numbers that a computer uses to distinguish different traffic.
- For example, if a computer is sending traffic on port 80, it is talking to a web server via HTTP
- It is important to note that we typically use protocols and ports together, for example if we want to connect to a website via HTTP, we will use a TCP connection on port 80.
- Knowing common ports is good but for now I wont get into it, for now its important to at least understand how ports and protocols shape the transport layer.

Quick Note

- Before getting into layers 5 6 and 7, I want to note that some people consider these three layers as a single layer called the application layer.
- Some people call it App Data, in this case it refers to layer 5 6 and 7 data combined
- Now to layer 5

OSI Layer 5: Session Layer

- If you are talking to someone, you are probably holding some type of conversation. Like imagine you see your friend, they say hi, you say hi, they ask how is your day, you tell them about your day, this is a session, you and your friend respond to each other based on what was last said
- This is called having an attention span, if people didnt have attention spans we would be done for

OSI Layer 5: Session Layer

- In networking we may have connections that are communicating back and forth based on the context of the connection, to be able to maintain this we use the session layer.
- This is especially important when a service requires a user to be logged in, imagine having to re-enter your user/password every time you communicate with a device
- While being able to connect is important, it is equally important to be able to start, maintain, and end a session rather than just response-reply

OSI Layer 6: Presentation Layer

- When receiving raw data, it is important to understand how it is intended to be interpreted. How do you know if all those 1s and 0s you just got make up an image, or maybe text, what kind of text, ASCII or Unicode?
- What if I told you "a" is yq==, 61, 97, and I can keep going
- Maybe the data was encrypted over a secure session, if we dont decrypt the data we will have no idea what was sent in the first place
- This is where the presentation layer comes in, with the millions of ways we might receive data, it is important to make sure we interpret the data as intended

@everyone hop on call
01000000 01100101 01110110 0110010

OSI Layer 7: Application Layer

- When we are sending traffic, we are usually doing it with some type of software. We might be browsing the web with firefox, playing a multiplayer game online, or talking on a call. This layer is responsible for taking data for a specific application and showing the intended result or communication to the user.
- This layer is like the middleman between us and the network itself, handling requests and handling traffic received.

Going back to the video game example

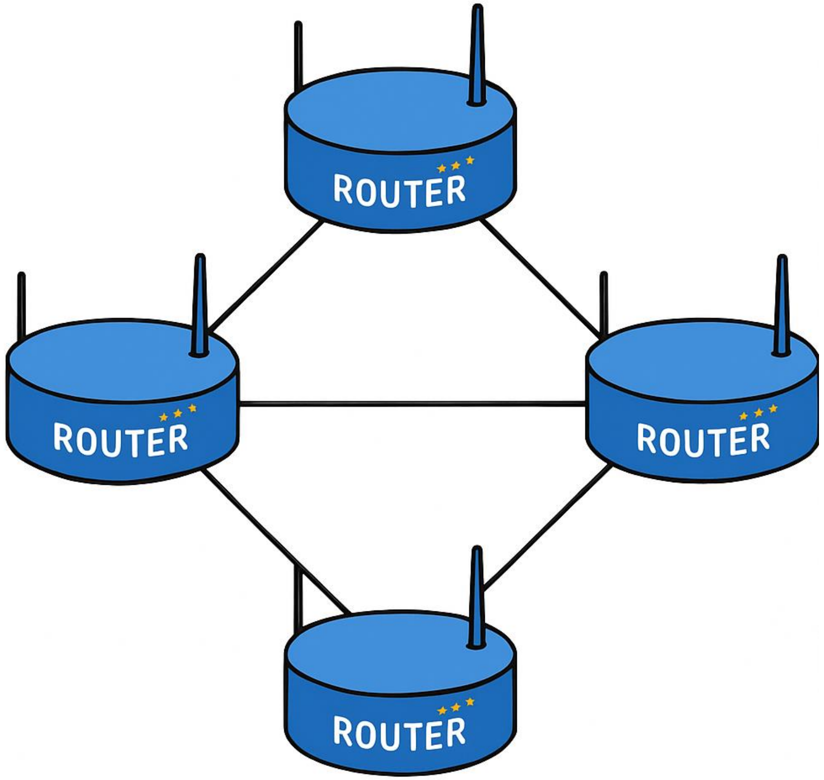
- Remember I said a video game is both an application, and 1s and 0s running on hardware in a certain way
- We can say network traffic is:
  - Bits on a wire
  - Data directed to a certain device
  - Data directed to an address on a network
  - Data for a certian protocol
  - Data that may be part of a session
  - Data that should be decrypted or decoded a certain way
  - Application data for the user to see

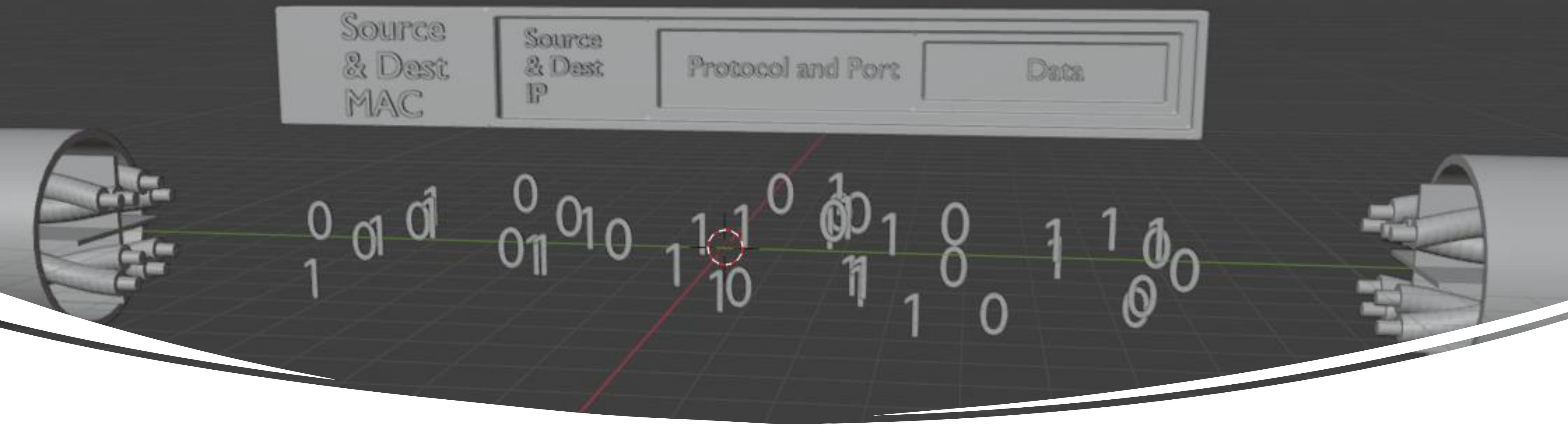
Packets of data

- Think of packets as a single unit of communication between devices
- These packets are composed of data that is relevant to each layer on the OSI model, we surround data of higher layers inside of data from lower layers
- When we want to send data, we first take the actual data we want to send, then add details of which port/protocol to use, then add details of which ip address to talk to, then add details of which MAC to send the data to, then send it over the wire.

Packets traveling the internet

- When sending data our packets hop all over the place, different routers and switches will be used to carry our data, so the packet information will change as it goes.
- For example, when our computer sends data to the internet, the packet first talks to a switch, so the data link part of the packet specifies the switch, when it reaches the switch, the switch sends the packet to the router, so now the data link part points to the router.
- Remember, traffic hops through multiple devices to reach its destination, just like a package may go through multiple post offices to reach its destination





Visualizing a packet

- Here is a quick visual I made for you to see what a packet looks like

Before continuing

These are the fundamentals of networking, keep in mind that much more happens behind the scenes when you use the internet, topics such as routing, protocols, subnets, etc are much deeper

If you want to learn more or get a stringer grasp on everything I said in earlier slides I highly reccomend this channel:

https://www.youtube.com/c/PowerCertAnimatedVideos

This channel is very good and I have used his videos multiple times

Other channels include Professer Messer, Network Chuck, CBT Nuggets, etc.

There are also many websites and resources on the internet in general for learning

Some terms you should know

- ISP (Internet service provider): a company that provides access to the internet
- Routing: the process of selecting paths for data packets to travel from source to destination
- Endpoint: a destination device for traffic
- LAN (local area network): A network covering a limited span of devices or subnets (an organization)
- WAN (wide area network): A network covering a large area connecting multiple LANS (a city or country)
- Cloud: a company that sells resources and services such as software, storage, security solutions, etc. When users use this service, they connect to a data center and access the companies servers. This allows you to run applications, store data, and perform tasks remotely, without needing to own or manage the hardware yourself.

Some tools you should know

- Firewall: block malicious traffic, this can be based on the ip address, which port its directed to, or even the data in the packet (and more)
- Wireshark: capture packets on a network and see the raw data
- VPN: A safe way to connect to a private network, any communication between a trusted device and a private network is encrypted, so this trusted device can communicate with the private network without physically being present
- Certificate: proof that when you communicate with someone, they are who they say they are, this is backed by a Certificate Authority, a trusted 3rd party that vouches for the person who made the certificate, this process uses cryptography

Networking and cybersecurity

- If you want a career in cyber security you need to have a basic understanding of networking.
- Over the years there have been many attacks and defenses in networking, and the landscape is still growing
- Main attack vectors with networking include: capturing unencrypted traffic, breaking weak encryption, spoofing, Denial of service, weak authentication, misconfigured firewalls, etc.
- Main ways of defense are: digital certificates, VLans, Firewalls, UTM, VPNs, authentication servers, etc.
- Learning networking will help you understand these attacks and how to prevent them

Conclusion

- Im just scratching the surface of networking, my main goal of these slides is to get you a basic understanding
- If you want I can go deeper into the cyber security part or I can go deeper in the specifics of networking
- I hope this was helpful if you have any questions ask me or check out that youtube channels i mentioned earlier
- Thank you