Week #1

0.1 Define following terms and concepts shortly:

1. Network bandwidth
2. Network throughput
3. Packet loss and jitter
4. bps vs Bps
5. Protocol payload
6. Protocol overhead (especially for resource-contrained IoT purposes)
7. Spanning Tree Protocol
8. Collision domain
9. Broadcast domain
10. SOHO network
11. MAC (physical) address
12. Physical layer protocol data unit (PDU)
13. MAC layer protocol data unit (PDU)
14. Half-duplex vs Full-duplex
15. Ethernet auto-negotiation
16. Hidden node problem (wireless)
17. Networking physical vs logical topology
18. TIA/EIA-568 and ISO/IEC_11801
19. Ethernet cabling categories. For example, CAT 6
20. 8P8C (RJ45)
21. Wifi AD HOC
22. IEEE 802.11ac, 802.11ax, 802.11be

1. The definition of "**Bandwidth**" in the computing domain refers to the rate of data over time. Data is usually measured in bits, the time unit in seconds, and it's often abbreviated as "bps". This term is also used in lower-layer protocols, like the PHY layer in Wi-Fi, where bandwidth is measured in hertz (Hz), not in bps, but the wider the channel in Hz, the

more bps can be transmitted. In Wi-Fi, it basically represents the channel width. Bandwidth refers to the maximum theoretical capacity of a channel to transmit data, it's a property of the medium or communication channel, not the actual speed.

2. **Throughput**, like bandwidth, also represents a rate of data over time, but unlike bandwidth where bps means the total theoretical capacity of the channel throughput measures the amount of bits delivered from source A to source B. In fact a data transmission can encounter different obstacles on the way, which can lead to packet loss or delays, that is why measuring throughput is critical in networking and signal processing. Data can be measured not only in bits, but also in packets or frames (blocks containing a fixed number of bits).

3. **Packet loss** could be represented by formula: PLR = (1 - (received frames) / (total frames transmitted)) this shows the ratio of lost packets to total sent packets. The higher the result of this formula, the worse the channel quality. Jitter is a complex measurement and it can be calculated in different ways. For example, there are Random Jitter (RJ), Deterministic Jitter (DJ), and Total Jitter (TJ). Basically, jitter shows the variation in the packet delivery time in other words, how much the interval between packet arrivals changes over time the higher is a jitter value the less stable and predictable is a signal.

4. **"bps"** is an abbreviation for bits per second, while "Bps" is bytes per second. 1 byte = 8 bits. "Bps" is used in higher-layer protocols because data sizes are usually measured in bytes rather than bits. "bps" is more useful in lower-layer protocols such as MAC or PHY.

5. **Protocol payload.** Protocol in domain of computing is a set of rules which defines the way how to deliver and extract the message, without which it would be a random bit stream. Payload is an actual message, for which protocol is applied. **Message** is a meaningful expression with well defined bounds (it has finite size) for example: ''`I want to stop writing right now and go take some beer`''. Protocol payload is a message.

6. **Protocol overhead** is the extra cost, which can be represented as time, extra bits, and processing logic needed for delivering data from source to destination. For example, some protocol header bits must be sent with a message (payload) to ensure that the receiver can extract the message. It also could be some logic like a handshake in TCP to establish a connection between RX (receiver) and TX (transmitter). In the end, all of these things are time-consuming, that's why they are called overheads.

7. **Spanning Tree Protocol (STP),** defined in IEEE 802.1D, is used to prevent loops in switched networks. Switches communicate with each other by sending BPDU (Bridge Protocol Data Units) every 2 seconds.

"I Think That I Shall Never See

A Graph More Lovely Than A Tree.

A Tree Whose Crucial Property

Is Loop-free Connectivity.

A Tree That Must Be Sure To Span

So Packets Can Reach Every LAN.

First, The Root Must Be Selected.

By ID, It Is Elected.

Least Cost Paths From Root Are Traced.

In The Tree, These Paths Are Placed.

A Mesh Is Made By Folks Like Me,

Then Bridges Find A Spanning Tree."

At the start, all switches consider themselves as the root bridge and send BPDU messages containing their Bridge ID to neighboring switches. Each switch compares its own Bridge ID with the neighbor's and forwards the smallest one further. After several exchanges, all switches know the Root Bridge, the switch with the lowest Bridge ID. Next, each switch calculates the shortest path to the Root Bridge using the path cost defined in 802.1D. If a switch has multiple paths, the shortest one is kept as the designated port, and the longer path is blocked. As a result, STP creates a loop-free spanning tree, ensuring that packets can reach every LAN segment while avoiding broadcast storms.

8. A **collision domain** is a segment of a network space where a signal is traveling. To communicate, clients sometimes use the same route for example, the same frequency if we talk about Wi-Fi. When two clients try to send data at the same time on the same channel, their signals interfere and collide it will lead to packet loss. After a collision, the data must be retransmitted, which causes delays and reduces network performance.

9. A **broadcast domain** can be described as a segment of a network.If I send a frame on Layer 2 with the destination address FF:FF:FF:FF:FF:FF, it means "send this to all members of my subnet where I am located."If the router is configured to combine several physical subnets into one logical subnet, then all of them become part of the same broadcast domain, even if they are physically separated.However, the actual boundary of such a broadcast domain will always end at the router, which separates this domain from the rest of the internet.

10. **SOHO network** (Small Office / Home Office) is not an official networking term, meaning it is not defined in any standards like IEEE 802.11.SOHO is used to describe a networking scenario, where several clients are connected through the same router or the same physical cable.In most cases,

all clients are members of a single subnet, sharing the same LAN and belonging to the same broadcast domain.However, a SOHO network can also contain multiple broadcast domains — for example, one subnet can be used for guests, another for IoT devices, and another for regular users.This separation is usually done using VLANs configured on the same router.

11. **MAC (physical)** address is a unique number that every device with a network interface has, for example Wi-Fi or Ethernet. It is usually 48 bits and written as hexadecimal pairs, for example AA:BB:CC:DD:EE:FF. MAC addresses are used on the Data Link Layer (Layer 2) so that devices can find each other inside the same network. When one device sends a frame to another, it puts its own MAC as the source and the MAC of the receiver as the destination. Without MAC addresses, sending data would be a lot more complicated, because devices would have to "ask" everyone in the network if the packet is for them.With MAC, it's much easier — switches and Wi-Fi routers know exactly where to deliver the frame.

12. **Physical layer protocol** data unit (PDU) is a bit. Generally, the physical layer does not have any high-level logic except for math and physics, where bits are turned into signals. In Wi-Fi these are radio waves, in Ethernet they are electrical signals, and in optical fiber they are light flashes. The exact instructions on how to modulate the signal come from Layer 2. The physical layer is usually optimized more by mathematicians and physicists than by programmers, but it's best when all three skills are combined in one person.

13. **MAC layer protocol data unit (PDU)** is called a frame. Before sending data to the physical layer, L2 takes the IP packet from L3, adds the source and destination MAC addresses, and then the logic depends on the type of network. In modern Ethernet, which works in full-duplex, there's no need for collision detection, so MAC mostly just adds the addresses and passes the frame down to the PHY layer. In Wi-Fi, the MAC layer is a lot smarter: it has to analyze the channel, choose the right modulation for PHY, run algorithms to avoid collisions (CSMA/CA with random backoff), and only after all of this it sends the frame to L1 for transmission.

14. **Half-duplex vs Full-duplex**. Half-duplex means a device can either transmit or receive, but not at the same time. Full-duplex means sending and receiving simultaneously.In modern Ethernet full-duplex is implemented on the physical level: the cable has separate pairs of wires for transmitting and receiving, so data flows both ways at once without collisions. In Wi-Fi, on the other hand, communication is half-duplex. A station cannot transmit and receive at the same time because its own signal would interfere with the receiver. Wi-Fi uses channel access algorithms and sometimes separates uplink and downlink subcarriers, but simultaneous full-duplex transmission is generally not used in current standards.

15. **Ethernet auto-negotiation** is a synchronization mechanism that allows two devices connected by an Ethernet cable automatically choose the best way to communicate. When devices are connected via cable, both start sending special signals called FLP (Fast Link Pulses), these signals contain information about what technologies each device has, like the supported speeds, duplex modes, and whether they support flow control. After exchanging this information, the devices compare their capabilities and pick the highest performance mode they both support. First, they choose the maximum possible speed, then they check the duplex mode: if both sides support full-duplex, they use it; otherwise, they fall back to half-duplex. Finally, they decide if flow control will be used which is a feature that helps to avoid packet loss when one side is slower than the other by "holding" data transmission. If auto-negotiation is disabled on one device but enabled on the other, the devices may choose different duplex modes, which leads to collisions, retransmissions, and lower performance. That's why in most modern networks, auto-negotiation is enabled on both ends.

16. **Hidden node problem** (wireless) can occur when STAs (clients) are located far from each other but use the same AP (access point) between them. This is a MAC layer problem. In Wi-Fi, all STAs share the same medium. When one STA sends data, it assumes the channel is free, but another STA may do the same, causing collisions and packet loss. To avoid this, the IEEE 802.11 standard includes the RTS/CTS (Request to Send / Clear to Send) mechanism: the device first sends RTS to the AP, and if the AP replies with CTS, other devices stay silent during the transmission. RTS/CTS is not always enabled because it adds overhead and is usually used when many clients are connected to the same AP.

17. **Networking physical vs logical topology. Physical topology** is based on real devices like routers, switches, and bridges (older tech), linked via radio channels or physical cables. A simple example is a PC or several PCs connected to a switch via cables, and the switch connected to a router. Physical topology is a core part of networking, like a skeleton. There are several common types of physical topology, and some of them are outdated today: Star, Mesh, Ring, and Bus.

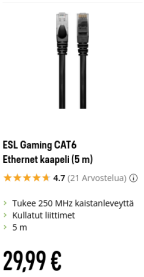
    - Star topology is most common type today. Multiple devices are connected to the same central switch or hub. If one cable fails, the rest of the network keeps working. But if the central device fails, the entire network goes down.
    - Mesh topology is modern and very reliable. Each device connects to several others, so there are multiple paths for data. If one link fails, traffic can be rerouted automatically. Full mesh (each device connected to all others) is rare because it's expensive, so partial mesh is used more often. This idea is also used in Wi-Fi mesh networks to cover a large area without dead zones.

- Ring topology is when devices are connected in a circle, and data goes step by step through each node until it reaches the destination. Today, ring topologies are rare and mostly remain in some industrial or optical systems.
- Bus topology is one of the earliest types, where all devices share a single cable. Simple but depricated, replaced by switches and modern Ethernet.

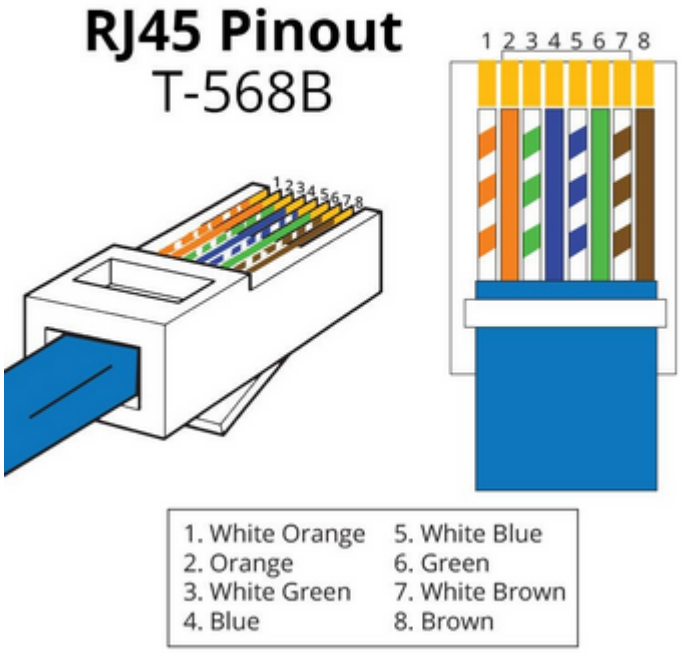
Logical topology describes how data actually flows inside the network, regardless of how devices are physically connected. Even if multiple PCs are connected to the same physical switch (star topology), logically they can belong to different subnets or VLANs, which means they cannot communicate directly.

18. TIA/EIA-568 and ISO/IEC_11801.
    - **TIA/EIA-568** is one of the main branches of the TIA standards, created by the Telecommunications Industry Association (TIA). It focuses on rules for structured cabling systems how to build Ethernet networks so that devices from different vendors work together.The standard defines cable categories like Cat5e, Cat6, Cat6a, and Cat8, each supporting different speeds and frequencies. It also describes how to wire and crimp RJ-45 connectors using two common schemes: T568A and T568B. Patch panels are also defined here, as well as maximum cable lengths and other installation rules. The main goal is to make sure network cables and equipment are compatible, reliable, and follow the same structured approach everywhere.
    - **ISO/IEC 11801** is an international standard for structured cabling systems. It defines how to build universal cabling for offices, campuses, and other customer premises, so that different types of communication like Ethernet, telephony, and building control systems can work over the same infrastructure.This standard covers both twisted-pair copper cables and optical fiber. In many ways, it's similar to TIA/EIA-568, but ISO/IEC 11801 is used globally, while TIA/EIA is mostly American. One important detail is that ISO includes Category 7 and 7a, but these are not recognized by TIA/EIA because there is no widespread hardware support for them.

19. **Ethernet cabling categories.** For example, CAT 6. Cat6 is one of the most common Ethernet cables used today *and backward compatible with the Category 5/5e and Category 3 cable standards* (From wikipedia) . It supports 1 Gbps up to 100 m and can handle 10 Gbps up to around 55 m, with a frequency of 250 MHz. The cable is widely used in offices, homes, small server rooms, IP cameras and VoIP systems, because it's reliable, not too expensive, and still compatible with older equipment. In practice, Cat6 is a good balance between cost and performance, which is why it became the standard choice for most installations.



20. **8P8C (RJ-45)** is the official name of the connector that people usually call RJ-45. The name means 8 Positions, 8 Contacts, which describes the 8 pins inside the plug. This connector is used for Ethernet cables (Cat5e, Cat6, Cat6a, etc.) and lets devices like PCs, switches, and routers connect to each other.The term RJ-45 is technically not correct, because RJ-45 was originally a telephone standard, but in networking the name stuck and everyone uses it. In practice, when you say "RJ-45", people understand it's the standard Ethernet connector.



21. **(IEEE 802.11ac, 802.11ax, 802.11be)** These are different generations of the Wi-Fi standard, each one improving speed, efficiency, and how many devices can work on the same network.

- 802.11ac (Wi-Fi 5) works mostly on 5 GHz, supports channel widths up to 160 MHz, and gives speeds up to several Gbps. Introduced MU-MIMO, which lets multiple devices receive data in parallel instead of waiting one by one.
- 802.11ax (Wi-Fi 6 / 6E) works on 2.4 GHz, 5 GHz, and even 6 GHz (Wi-Fi 6E). Improves MU-MIMO and adds OFDMA, splitting the channel into smaller sub-channels so more devices can transmit at the same time. Better performance in crowded environments and lower latency.
- 802.11be (Wi-Fi 7) the newest generation. Uses channels up to 320 MHz wide and supports Multi-Link Operation (MLO) a device can use multiple frequency bands simultaneously for higher speeds and better stability. It also improves MU-MIMO even further, supporting up to 16 spatial streams and allowing many clients to send and receive data at the same time. Theoretical speeds can go above 40 Gbps.

0.2 Estimate how long does it take to download 3 TB file from cloud based backup service if network download throughput is 200 Mbps for actual payload (i.e. data)?

- Step 1 – Convert 3 TiB to bits (1 TiB = 1024^4 bytes): $3\text{TiB} = 3 \times 1024^4 bytes = 3.295 \times 10^{12}\text{bytes} \times 8\text{byte} = 2.636 \times 10^{13}\text{bits}$
- Step 2 – Divide by the payload throughput (200 Mbps): $T = \frac{2.636 \times 10^{13} bits}{200 \times 10^6 \text{bits/s}} = 1.318 \times 10^5 s$
- Step 3 – Convert seconds to hours: $T_\text{h} = \frac{1.318 \times 10^5 \text{s}}{3600 s/h} \approx 36.6h$

Answer: 36.6 hours

0.3 Locate the MAC address of your mobile phone, laptop wifi interface or some other networked IT device

How did you find it?

List the MAC address in hex format (such as f0:1f:af:cf:d9:1a), but replace last 24 bits with zeros for your privacy

Use OUI MAC address list(s) or lookup tools, and determine the device/chipset vendor of that MAC address. For example, that f0:1f:af:cf:d9:1a is Dell inc.

Device 1: Laptop (Arch Linux)

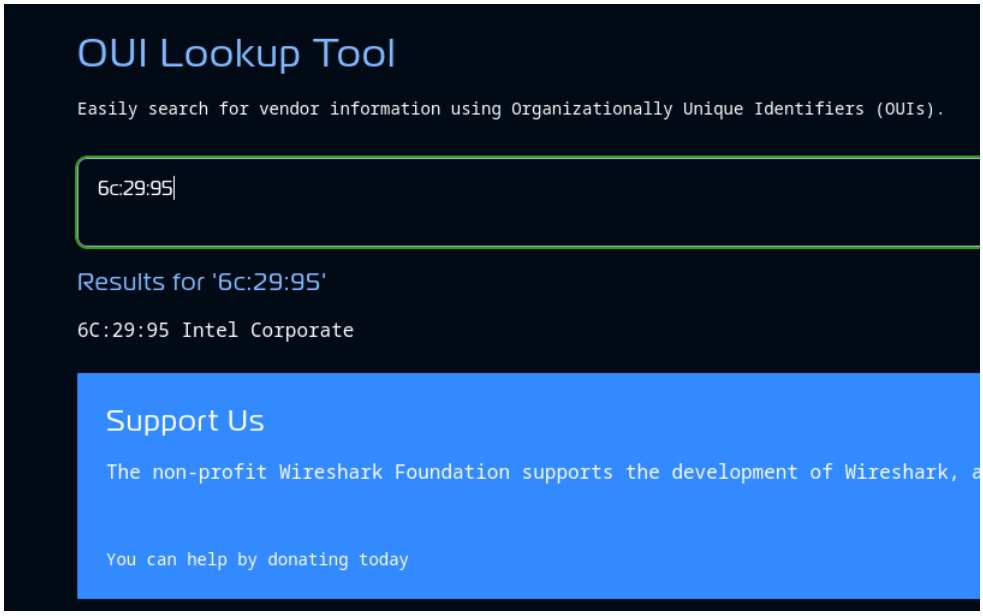
To find the MAC addr I used the ip link command in terminal. Wi-Fi interface is wlan0, its MAC address is shown next to link/ether.

MAC address:

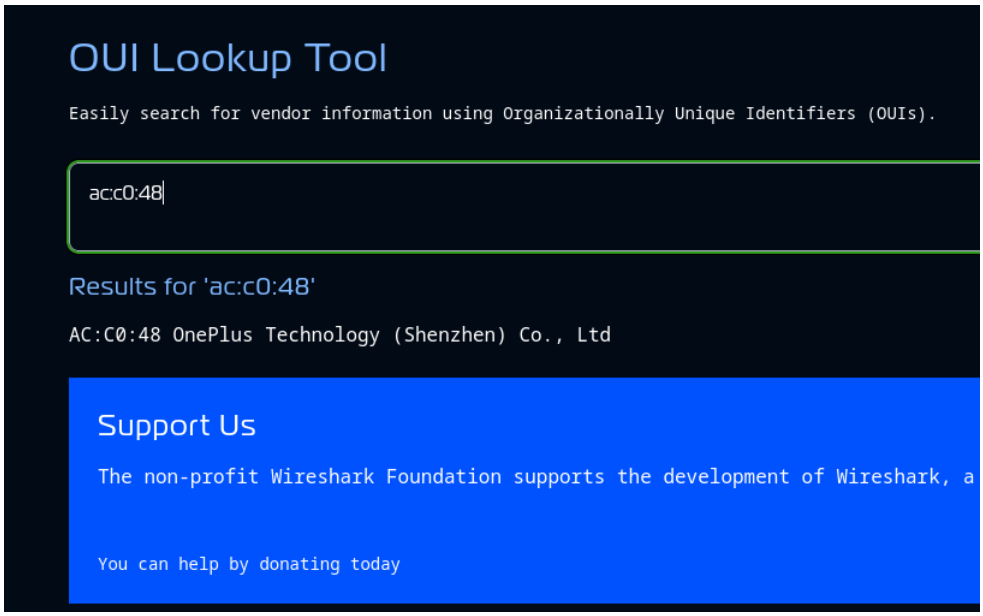
6c:29:95:00:00:00 (last 24 bits zeroed for privacy)

Vendor (OUI lookup):

MAC prefix 6c:29:95 belongs to Intel Corporate



Device 2: Android smartphone
How did you find it?
Went to:
Settings → About phone → Status → Wi-Fi MAC address
MAC address: ac:c0:48:00:00:00 (last 24 bits zeroed for privacy)
Vendor (OUI lookup): AC:C0:48 OnePlus Technology (Shenzhen) Co., Ltd.
(Looked up using the Wireshark OUI Lookup Tool



0.4 Describe shortly what are these network devices, functions, and services

1. Repeater
2. Hub (multiport repeater)
3. Bridge
4. Access switch
5. Core switch
6. Edge router
7. Core router
8. Firewall
9. Wifi AP
10. WLAN AP controller
11. Network TAP

1. **Repeater** is a device used in networks or telecom lines to help signals travel longer distances. When a signal gets weak or noisy, the repeater picks it up, regenerates it, and sends it out again. This way, the signal can reach further without losing quality or becoming unreadable. Repeaters

are used for Ethernet cables, fiber optic links, and even wireless connections. There are different types of repeaters depending on the technology, for example, telephone, optical, or radio repeaters. The main point is that a repeater doesn't just make the signal louder. Repeater actually rebuilds the data and removes most of the noise, so errors don't add up as the signal moves through the network. If the signal is already too weak or too noisy, a repeater might not help, but usually it keeps the data clear over long distances.

2. **Hub**, or multiport repeater, is a simple network device used to connect several computers or other devices in a local network, usually with Ethernet cables. When a device sends data to the hub, the hub copies that data and sends it out to all its ports, so every connected device gets the same message, no matter who it was meant for. This is why hubs work at the physical layer (Layer 1) and don't know anything about addresses or who is supposed to get the data.Because hubs just repeat everything to everyone, they don't help with traffic management if two devices send data at the same time, their signals will collide, which causes errors and forces the devices to resend their data. For this reason, hubs have been replaced by switches in most modern networks, since switches are smarter and only forward data to the right device, reducing collisions and making the network faster.

3. **Bridge** is a network device that splits a network segment into two parts to help filter traffic and cut down on unnecessary data. When data frames arrive, the bridge checks their MAC addresses to see if the sender and receiver are on the same side. If they are, the bridge blocks the traffic from crossing over. If they're on different sides, the bridge lets the data through. This way, bridges help reduce collisions and keep local traffic separate, making the network more efficient. Bridges work at the data link layer (Layer 2). They're especially useful for breaking up a large, busy network into smaller, quieter sections. In modern networks, simple bridges aren't used much anymore because switches can do the same thing (and more), but the main idea is the same: bridges help organize network traffic and stop unnecessary signals from spreading everywhere.

4. **Access switch** is a network switch used to connect end devices, like computers, printers, or phones, to the local network. It's usually placed at the edge of the network, close to users, and has many ports for plugging in devices with Ethernet cables. The main job of an access switch is to forward data only to the specific device it's meant for, using MAC addresses—which means, when one device sends data, the switch checks the destination MAC address and sends that data only to the right port, not to everyone else. This keeps traffic organized and reduces collisions.Access switches work at Layer 2 (the data link layer) and often support extra features, like VLANs for segmenting traffic, or Power over Ethernet (PoE) for powering devices directly through the cable. In most networks, access

switches connect user devices to higher-level switches or routers, forming the first step for devices to access the rest of the network.

5. **ore switch** is a high-performance network switch that is located at the center of a large network and connects multiple access switches together. Its main job is to move large amounts of data between different parts of the network, especially between different buildings or sections of an organization. Core switches usually have very high bandwidth and fast processing to handle lots of simultaneous connections. Unlike access switches, core switches don't connect directly to end devices like computers or printers they mostly connect to other switches and routers. They work at Layer 2 or sometimes Layer 3 (data link), and are designed for speed and reliability, making sure data can always get from one side of the network to the other.

6. **Edge router** is a network device (Layer 3) that sits at the boundary between an internal network (like a company or campus LAN) and an external network, usually the internet or another organization's network. Its main job is to route traffic in and out of the local network, deciding which data goes where based on IP addresses. Edge routers also often handle things like NAT (Network Address Translation), firewall rules, VPNs, and sometimes basic security functions, protecting the internal network from outside threats.In short, the edge router acts as the main gateway between your private network and the outside world.

7. **Core router** is a high-capacity network device (Layer 3) located in the center of large networks, such as service provider backbones or big enterprise networks. Its main job is to quickly route large amounts of data between different parts of the network, connecting multiple edge routers and distribution switches. Core routers are optimized for speed, reliability, and handling high volumes of traffic, but they usually don't connect directly to end devices. In summary, a core router forms the backbone of a big network, moving data efficiently between major segments.

8. **Ffirewall** is a security device or software that controls which data is allowed to enter or leave a network or a single computer based on a set of rules. Its main job is to block unwanted or dangerous traffic. Firewalls can be physical devices placed between networks, or software running on a computer or server. Firewalls check network packets for things like source and destination addresses, ports, and protocols. Based on this information, the firewall decides whether to allow or block the traffic. This helps protect networks from attacks, unauthorized access, and malware. In most modern networks, firewalls are used to separate private internal networks from the public internet, adding an important layer of defense.

9. **WiFi access point (AP)** is a device that allows wireless devices, like laptops and smartphones, to connect to a wired network using Wi-Fi. The AP acts as a bridge between the wireless devices and the wired part of the

network (for example, an Ethernet LAN). When you connect your phone or laptop to Wi-Fi, you're actually connecting to the access point, which then forwards your data to the rest of the network. Wi-Fi APs handle radio communication, manage which devices can connect, and take care of basic security settings like passwords and encryption. In home networks, the AP is often built into the Wi-Fi router, but in bigger networks (like offices or schools), there are usually several standalone APs placed around the building to give good wireless coverage everywhere.In short, a Wi-Fi AP is what lets wireless devices join the local network and get access to the internet or other resources.

10. **Wireless LAN controller (WLC)** is a device or software that centrally manages multiple WiFi access points in large networks, like offices or campuses. Instead of configuring each access point separately, admins use the controller to set WiFi settings (such as passwords, network names, and firewall rules) once, and the changes apply to all APs automatically. The WLC also manages security, firmware updates, and load balancing across access points. Another key function is seamless roaming: as users move through the building, their devices can automatically switch between access points without losing connection, because the controller coordinates the handover process.

11. **Network TAP (Test Access Point)** is a hardware device that's used to monitor and capture network traffic for analysis. It sits between two points in the network and makes an exact copy of all the data passing through, sending it to a monitoring or security tool. Unlike a switch port in mirror mode, a TAP is a dedicated device, so it captures traffic without interfering or slowing down the network.Network TAPs are commonly used for network troubleshooting, security monitoring, or recording traffic for later analysis. They work at Layer 1 (physical layer) and are often used in data centers or anywhere reliable, passive network monitoring is needed.

0.5 RFC assignments

1. What are RFCs?
2. How many PPP related RFC documents can you find from rfc-editor website?
3. What is the current status of RFC1597? What is the number for updated, more recent RFC of same topic?
4. When was RFC5218 released?
5. What is the meaning if RFC status is BCP?
6. List authors of the CoAP RFC (June 2014). What is the RFC number?

7. Twitch.tv provides IRC access to the stream chats. Which RFC defines the original Internet Relay Chat (IRC) Protocol?