Networks

Faruk Avcı

April 16, 2024

Contents

1 Introduction to Networking

1.1 Definition and Basics

Networking, in the context of computer science and information technology, refers to the practice of connecting various computing devices together to facilitate communication and data exchange among them. The primary objective of networking is to enable the sharing of resources and information, ensuring that data can be transmitted efficiently and accurately between devices.

To achieve seamless communication, it is crucial that both the transmitting and receiving devices adhere to a common set of rules or protocols. These protocols define the language and methods through which devices communicate, ensuring that the sender's message is accurately interpreted by the receiver. Without such standardized protocols, the interconnected devices would be unable to understand each other, leading to ineffective communication and data transfer.

Figure 1: Devices and Networks

1.2 Common Types of Networks

1.2.1 Local Area Network (LAN)

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is typically limited to a geographic area such as a writing lab, school, or building. Key characteristics of a LAN include:

- High data transfer rates.
- Geographical limitation to a small area like a building or campus.
- Often used for connecting computers in a single organization.

Computers connected to a LAN are broadly categorized based on their roles and the services they provide. as servers or workstations. Servers are generally not used by humans directly, but rather run continuously to provide "services" to the other computers (and their human users) on the network. Services provided can include printing and faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control (security) for the network's resources, and many others.

Workstations are called such because they typically do have a human user which interacts with the network through them. Servers tend to be more powerful than workstations, although configurations are guided by needs. For example, a group of servers might be located in a secure area, away from humans, and only accessed through the network. In such cases, it would be common for the servers to operate without a dedicated display or keyboard. However, the size and speed of the server's processor(s), hard drive, and main memory might add dramatically to the cost of the system. On the other hand, a workstation might not need as much storage or working memory, but might require an expensive display to accommodate the needs of its user. Every computer on a network should be appropriately configured for its use.

On a single LAN, computers and servers may be connected by cables or wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPs). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less.

1.2.2 Wide Area Network (WAN)

Wide Area Networks (WANs) connect networks in larger geographic areas, such as Florida, the United States, or the world. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of global network.

Using a WAN, schools in Florida can communicate with places like Tokyo in a matter of seconds, without paying enormous phone bills. Two users a half-world apart with workstations equipped with microphones and a webcams might teleconference in real time. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the Internet. To users, however, a WAN will not appear to be much different than a LAN.

1.3 Networking Devices Overview

In the realm of network design, various devices play pivotal roles. Here, we delve into the functionalities and unique attributes of these devices.

1.3.1 Repeater

A repeater serves a fundamental purpose in network communication. It regenerates weak or degraded signals, ensuring that data transmission remains robust over longer distances.

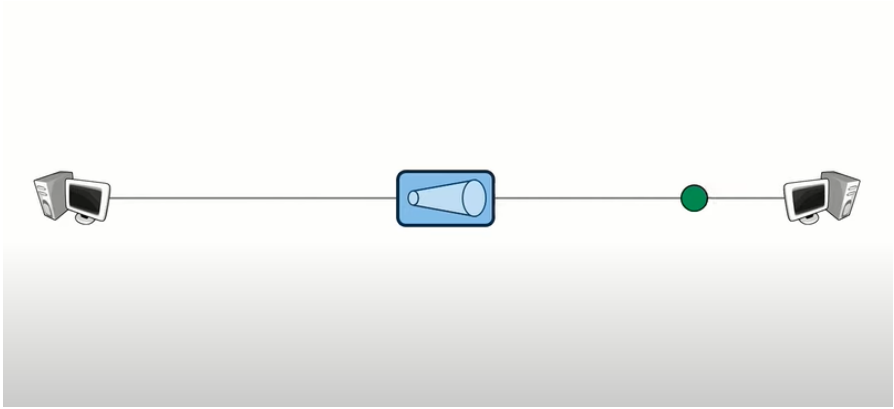

Figure 2: Illustration of a Repeater enhancing signal strength

Functionality: Consider a scenario where two hosts are connected over a significant distance. The signal, while traversing, loses strength due to attenuation. The repeater, positioned at an optimal midpoint, regenerates the signal's integrity, facilitating uninterrupted communication between the endpoints.

Application: Repeaters are pivotal in extensive network infrastructures, like campus networks or large office buildings, where signal strength can diminish due to distance and obstructions.

1.3.2 Hub

The hub serves as a central connection point in a network. It is a simple device that connects multiple computers, printers, and other network devices together. Unlike more advanced networking devices like switches or routers, a hub does not filter data or know where the data is supposed to be sent. It simply retransmits the incoming data packets to all connected devices, except the one it originated from.

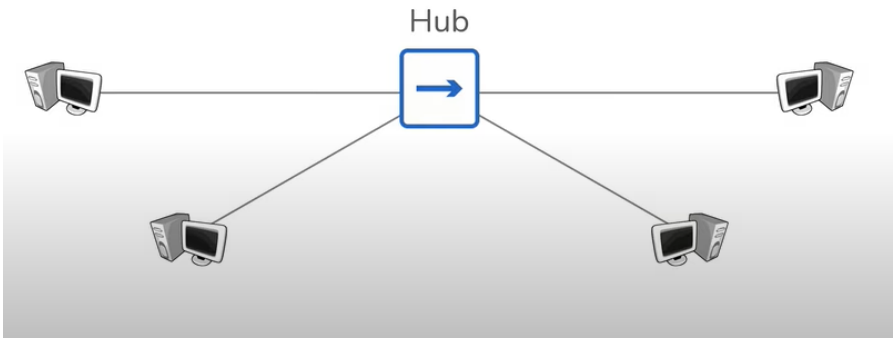

Figure 3: Illustration of a Hub distributing data packets to all connected devices

Functionality: When a data packet arrives at one port, the hub broadcasts it out to all other ports, regardless of which device the packet is intended for. This can lead to an inefficient use of bandwidth, especially in networks with a lot of devices, as each device needs to process and reject packets not intended for it.

Application: Hubs are typically used in small or less complex network setups where the network traffic is minimal and a simple connectivity solution is sufficient.

1.3.3 Bridge

A bridge is a device that connects two separate network segments, allowing them to communicate as if they were part of the same network. It helps manage the flow of data and reduces unnecessary traffic by deciding whether to forward or block data packets based on their destination.

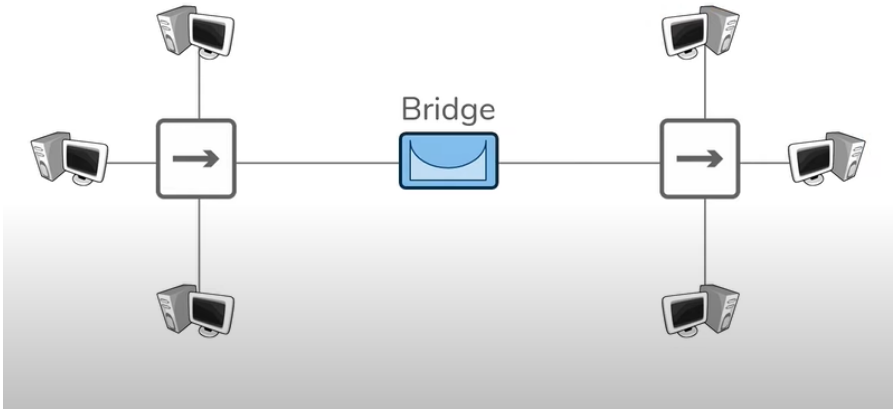

Figure 4: Illustration of a Bridge connecting two network segments

Functionality: Think of a bridge as a kind of gatekeeper. It looks at the incoming data and decides if it should stay on one side or go to the other. This decision is based on where the data needs to go, making sure that only necessary information crosses over.

Application: Bridges are useful in large networks that need to be split into smaller, more manageable sections. They help in reducing traffic, as they prevent data that doesn't need to cross over from doing so.

1.3.4 Switch

A switch is a high-tech device in a network that connects multiple devices together, such as computers, printers, and servers. Its main job is to receive data (like emails or videos) and send it specifically to the device it's meant for, not just everywhere like a hub would. Switches are combination of Hubs and Bridges. Note that switches facilitate communication **within a network**.

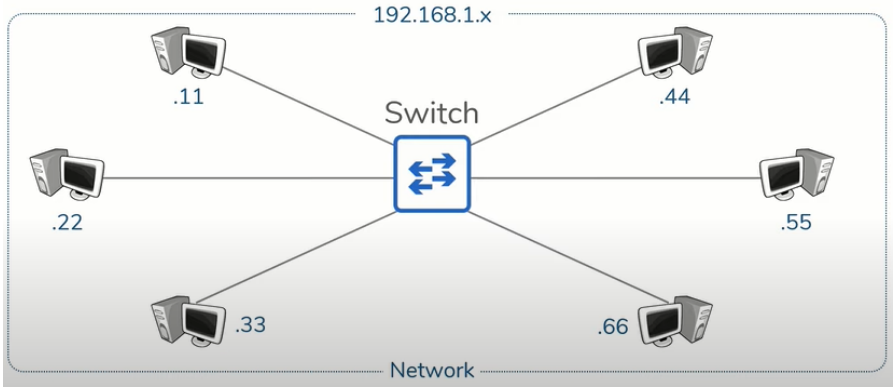

Figure 5: Illustration of a Switch directing data to specific devices

Functionality: Imagine a switch as a smart postman. When it receives a letter (data packet), it knows exactly which house (device) to deliver it to. It looks at the address (device's network information) and sends it directly to the right recipient. This way, only the intended device receives the data, making the network more efficient and secure.

Application: Switches are essential in almost every modern network, especially where there are many devices. They help in making sure that the network is not congested with unnecessary data, speeding up the communication and ensuring that information is securely delivered.

1.3.5 Router

A router is an advanced device in the realm of networking, pivotal for directing data packets between different networks. It acts as an intelligent intermediary, not just passing data along, but making decisions about the best pathways for the data to travel efficiently and securely.

Functionality: A router examines the data packets that arrive and uses information within the packet, such as IP addresses, to decide where to send them next. This process, known as routing, is essential for ensuring that data reaches its correct destination across interconnected networks. Routers use routing tables and protocols to determine the most efficient path for each packet.

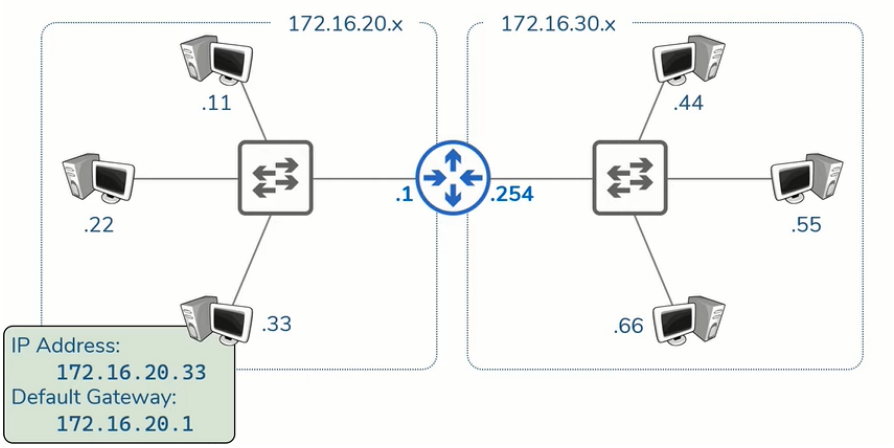

Figure 6: Illustration of a Router directing data between networks

Diverse Roles: Beyond directing traffic, routers play several critical roles. They connect different network architectures, such as Ethernet and Wi-Fi, serve as a firewall to protect networks from external threats, and can also prioritize traffic to optimize performance for critical applications.

Application: In home environments, routers connect the household to the internet, allowing multiple devices to share a single internet connection. In businesses, routers facilitate internal network communication and provide a gateway to the external internet, supporting data exchange, cloud services, and remote applications.

1.3.6 Network Topology

The network topology diagram represents ACME, Inc.'s internal network structure, which spans across two major offices located in New York and Tokyo. Each office has distinct subnetworks dedicated to different departments: Sales, Engineering, and Marketing, which are identified by unique IP subnets within the private IP address range of 10.x.x.x, specifically segmented into 10.20.x.x for New York and 10.40.x.x for Tokyo. The subnets are further tailored for each department, as denoted by the third octet (e.g., .55, .66, .77). Connectivity between these subnetworks and the global internet is facilitated through routers, symbolizing the company's robust international network infrastructure and its commitment to seamless interdepartmental and global communications.

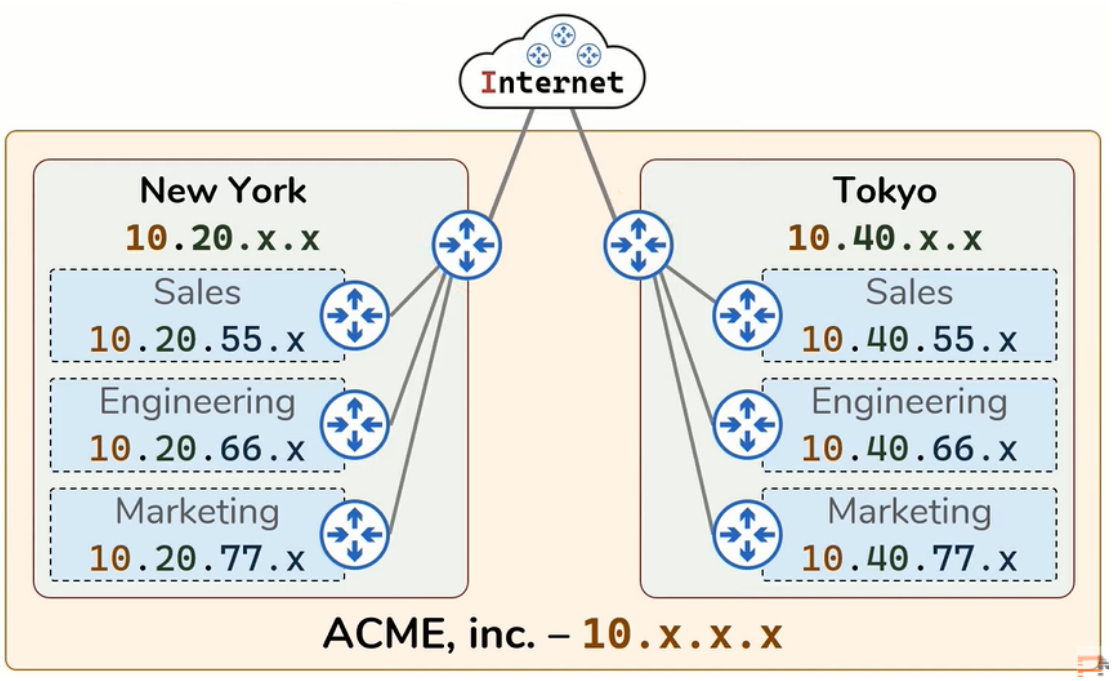

Figure 7: Network topology diagram showcasing ACME, Inc.'s New York and Tokyo office networks and their connections to the Internet.

2 Cabling

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Basically, there are three types of cables are used in networking:

2.1 Unshielded Twisted Pair Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks. A magnetic field and a copper cable can create electricity. The problem is that a pair of wires running parallel create a small electromagnetic field. The field from one pair of wires can affect the signal on another pair of wires. This is called crosstalk.

	Copper Cable	Fiber Optic Cable
Material	Made of copper. Conducts electrical current.	Made of glass or plastic fibers. Transmits light.
Advantages	• Widely used and well understood • Less expensive per meter • Easier to connect and install	• Higher bandwidth capacity • Less signal loss over long distances • Immune to electromagnetic interference
Disadvantages	• Susceptible to electromagnetic interference • Lower bandwidth than fiber • Signal loss over long distances	• More expensive • Fragile, can be difficult to splice • Requires specialized knowledge to install

Table 1: Comparison of Copper Cable and Fiber Optic Cable

Untwistes Pair Cable: UTP eliminates most crosstalk by twisting the pairs of wires together. The quality of UTP may vary from telephone-grade wire to extremely high-

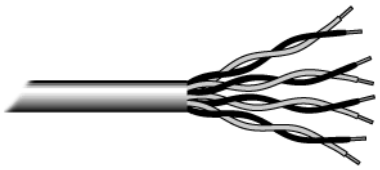

Figure 8: UTP Cable

speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.

UTP Connector: Connectors used with twisted pair cabling are modular connectors, which are small and rectangular. The RJ45 connector is the most common type of modular connector used with UTP cable. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Figure 9: Categories of UTP Cable

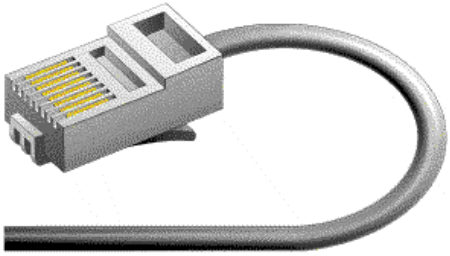

Figure 10: RJ45 Connector

2.2 Shielded Twisted Pair Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables. Shielded twisted pair cable is available in three different configurations:

- Each pair of wires is individually shielded with foil.
- All pairs of wires are encased in a foil shield.
- The entire cable is shielded.

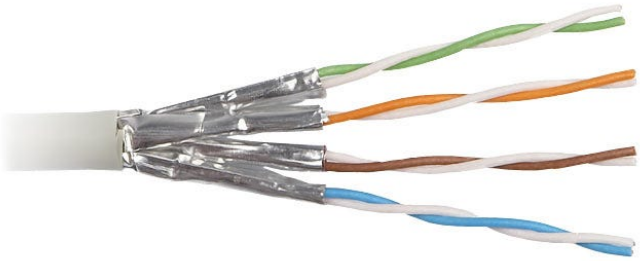

Figure 11: Shielded Twisted Pair Cable

2.3 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers. Although coaxial cabling is difficult to install, it is highly resistant to signal interference.

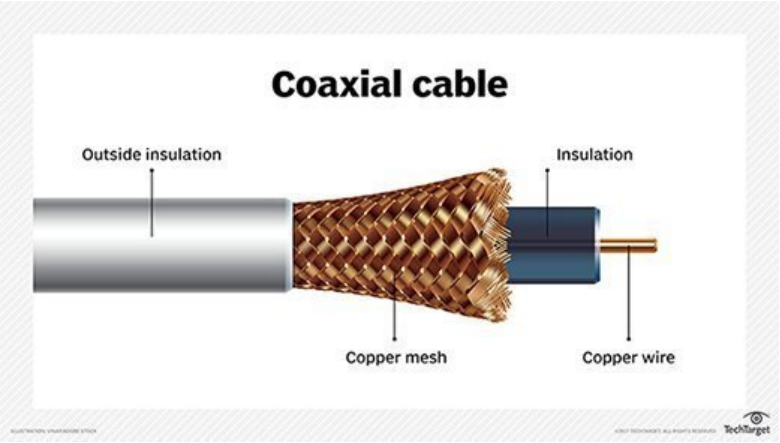

Figure 12: Coaxial Cable

In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice for running longer lengths in a linear bus network.

Coaxial Cables are used in:

1. **Television Antenna Connections:** Coaxial cables are commonly used in antenna or cable TV connections due to their ability to transmit high-quality video signals over long distances without significant interference.

2. **Internet and Network Connections:** Some types of coaxial cables are employed in broadband internet connections and in local area networks (LAN) for data transmission. They offer a reliable medium for high-speed data exchange.

3. **RF (Radio Frequency) Transmission:** Coaxial cables are preferred for radio frequency transmission, especially for low-frequency signals. They are designed to carry radio signals with minimal loss and interference.

4. **CCTV (Closed-Circuit Television) Systems:** The use of coaxial cables is prevalent in connecting CCTV cameras. Their robust design ensures the reliable transmission of video signals, making them a staple in security systems.

Coaxial Cable Connectors: Coaxial cables use different types of connectors to establish connections with devices. The most common connectors include BNC (Bayonet Neill-Concelman) and F-type connectors. These connectors are designed to ensure a secure and reliable connection between the cable and the device, minimizing signal loss and interference.

Figure 13: BNC Connector

Figure 14: F Connector

2.4 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals, eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Full Duplex: Fiber optic cable supports full-duplex transmission. This means that signals can be sent and received simultaneously, allowing for faster data transfer rates.

Half Duplex: In half-duplex transmission, data can only flow in one direction at a time. This can lead to slower data transfer rates compared to full-duplex transmission.

Single Mode Fiber SMF: Single-mode fiber is designed for long-distance communication and is used in applications that require high bandwidth and low attenuation. It has a small core size of 9 microns and is ideal for transmitting data over long distances. Laser light is used to transmit data over single-mode fiber, allowing for high-speed data transmission over long distances.

Multi-Mode Fiber MMF: Multi-mode fiber is used for shorter distances and is suitable for applications that require high bandwidth over short distances. It has a larger core size of 50 or 62.5 microns and is commonly used in LANs, data centers, and other short-distance applications. LED light sources are typically used to transmit data over multi-mode fiber.

Connectors: Fiber optic cables use different types of connectors to establish connections with devices. The most common connectors include LC, SC, and ST connectors. These connectors are designed to ensure a secure and reliable connection between the cable and the device, minimizing signal loss and interference.+

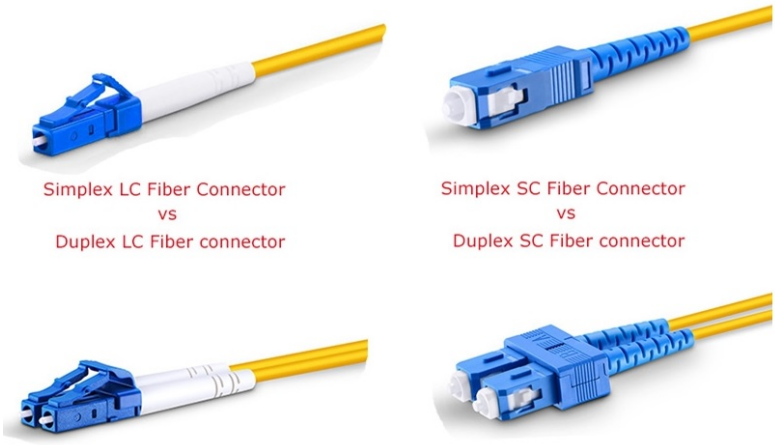

Figure 15: Fiber Optic Cable Connectors

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Figure 16: Ethernet Cabling

2.5 Wireless

More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Figure 17: Wireless Network

3 OSI Model

A protocol is a set of rules that governs the communications between computers on a network. In order for two computers to talk to each other, they must be speaking the same language. Many different types of network protocols and standards are required to ensure that your computer (no matter which operating system, network card, or application you are using) can communicate with another computer located on the next desk or half-way around the world. The OSI (Open Systems Interconnection) Reference Model defines seven layers of networking protocols.

Layer Name	**Protocol**	**Data Unit**	**Adressing**
Application	HTTP, SMTP	Messages	-
Transport	TCP, UDP	Segment	Port
Network	IP	Packet	IP Adress
Data LInk	Ethernet, WiFi	Frame	Mac Adress
Physical	-	Bits	-

Table 2: OSI Model Layers

3.1 Physical Layer (*TransportingBits*)

This layer conveys the bit stream electrical impulse, light, or radio signal through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects.

Technologies: Ethernet(UTP), WiFi, Bluetooth, Fiber Optic, Coaxial Cable, Repeaters

3.2 Data Link Layer (*TransportingFrames*)

The Data Link Layer, also known as Layer 2 of the OSI model, is primarily concerned with the reliable transmission of data across the physical network medium. One of its key functionalities is addressing frames so that they can be delivered to the appropriate destination. This is where MAC (Media Access Control) addresses come into play.
MAC Address: A MAC address is a unique identifier assigned to a network interface controller (NIC) by the manufacturer. It serves as a hardware address that distinguishes one device from another on a network. MAC addresses are assigned at the Data Link Layer and are typically represented as a sequence of hexadecimal digits, such as 00:1A:2B:3C:4D:5E.
Technologies: Network Interface Cards (NIC), WiFi Access Cards, Switches

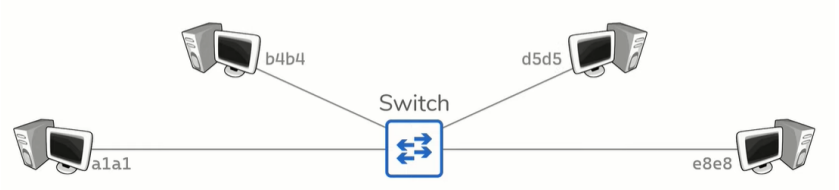

Figure 18: Data Link Layer

3.3 Network Layer (*TransportingPackets*)

The Network Layer, or Layer 3 of the OSI model, is responsible for routing data packets from the source to the destination across multiple networks. It uses logical addressing, such as IP addresses, to identify devices on the network and determine the best path for data transmission.
IP Address: An IP address is a numerical label assigned to each device connected to a network that uses the Internet Protocol for communication. It serves as a unique identifier for devices on a network and enables data packets to be routed to the correct destination.
Technologies: Routers, Hosts

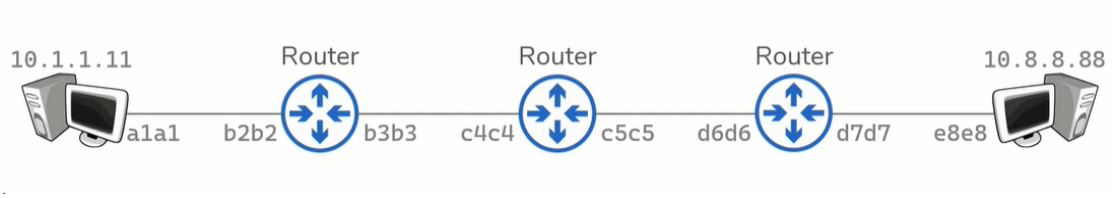

Figure 19: Network Layer

Difference Between MAC and IP adresses
The function that MAC addresses and IP addresses both perform is to designate a specific device within a network. The MAC address designates the physical location of a device within a local network, whereas the IP address signifies the device's global or internet-accessible identity. The manufacturer of the NIC card provides the MAC Address, whereas the Internet Service Provider supplies the IP Address.

3.4 Transport Layer (*TransportingSegments*)

The Transport Layer, at OSI Layer 4, ensures efficient and reliable transmission of data packets across networks. It breaks data into packets, assigning them sequence numbers for proper reassembly. Ports and TCP are vital components:
Ports: Virtual endpoints in networking software, facilitating simultaneous communication between multiple services or applications.
TCP (Transmission Control Protocol): A connection-oriented protocol ensuring reliable data transfer. It uses port numbers to establish connections between devices and guarantees data integrity by acknowledging packet receipt and retransmitting lost or corrupted packets.

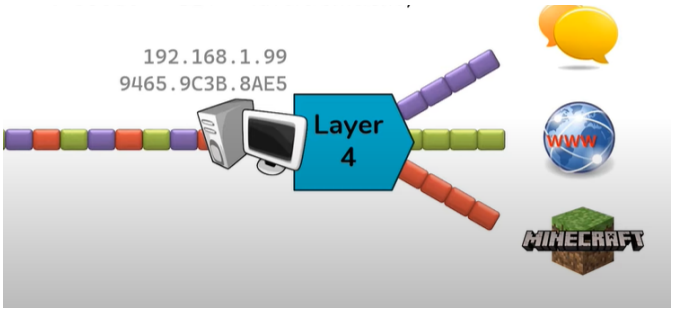

Figure 20: Transport Layer

3.5 Application Layer

The Application Layer, residing at the top of the OSI model (Layer 7), enables end-user applications to interact with the network. It facilitates communication between software applications and network services, providing a platform for user-level functionalities. Key components include:
Protocols: There protocols listed below are a few of the more well-known:

- DNS - Domain Name System - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa
- DHCP - Dynamic Host Configuration Protocol - can automatically assign Internet addresses to computers and users
- FTP - File Transfer Protocol - a protocol that is used to transfer and manipulate files on the Internet
- HTTP - HyperText Transfer Protocol - An Internet-based protocol for sending and receiving webpages
- IMAP - Internet Message Access Protocol - A protocol for e-mail messages on the Internet
- IRC - Internet Relay Chat - a protocol used for Internet chat and other communications
- SMTP - Simple Mail Transfer Protocol - A protocol for e-mail messages on the Internet

Data Representation: Handles data formatting and conversion for interoperability between different systems and platforms.
User Interface: Provides interfaces for users to interact with network services, such as web browsers for HTTP-based services.

4 IPv4

4.1 Introduction to IPv4

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks. IPv4 was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6. Each IP address is a 32-bit number that uniquely identifies a device on a network. An IPv4 address consists of four numbers separated by periods. Each number can range from 0 to 255, making the total number of possible IPv4 addresses approximately 4.3 billion. However, due to the rapid growth of the internet, the number of available IPv4 addresses has been exhausted, leading to the adoption of IPv6.

IPv6 (Internet Protocol version 6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

Each of the four numbers in an IPv4 address is called an octet because it is 8 bits long. The numbers are written in decimal form, separated by periods. Each octet can represent a number from 0 to 255, which is the range of values that can be stored in an 8-bit binary number.

sample IPv4 address: 192.168.1.34
sample bit representation: 11000000.10101000.00000001.00100010

4.2 Components of an IPv4 Address

IP adresses are two adress in one.

- **Network Adress:** Identifies the network to which the device is connected. First 2 octets.
- **Host Adress:** Identifies a specific device on a network. Last 2 octets.

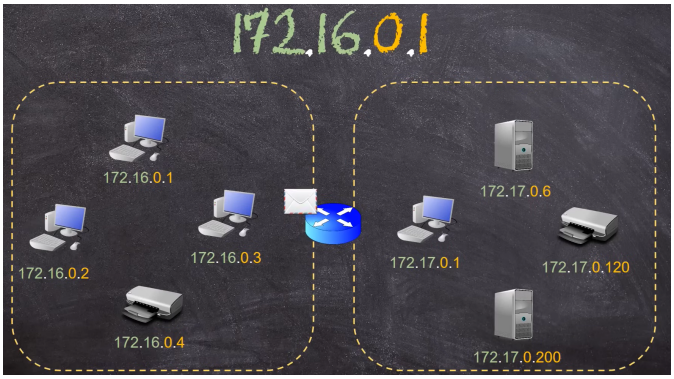

Figure 21: Components of an IPv4 Address

4.3 IPv4 Classes

4.3.1 Class A

When the internet first created first octet is used for network and the last 3 octets are used for host. The first bit of the first octet is always set to 0. The range of the first octet is 1-126.

Range of Network Adress:

- 00000001 - 01111110
- 1 - 126
- 126 networks
- Range: 1.0.0.0 - 126.0.0.0

Range of Host Adress:

- 00000000 - 11111111
- 0 - 255
- 255*255*255 = 16,777,216

Networks that starts with 0 and 127 are reserved.

4.3.2 Class B

As the internet grew, the first 2 octets are used for network and the last 2 octets are used for host. The first 2 bits of the first octet are always set to 10. The range of the first octet is 128-191.

Range of Network Adress:

- 10000000 - 10111111
- 128 - 191
- 255*(191-128) = 16,384 networks
- Range: 128.0.0.0 - 191.255.0.0

Range of Host Adress:

- 00000000 - 11111111
- 0 - 255
- 255*255 = 65,536

4.3.3 Class C

As the internet grew, the first 3 octets are used for network and the last octet is used for host. The first 3 bits of the first octet are always set to 110. The range of the first octet is 192-223.

Range of Network Adress:

- 11000000 - 11011111
- 192 - 223
- 255*255*(223-192) = 2,097,152 networks
- Range: 192.0.0.0 - 223.255.255.0

Range of Host Adress:

- 00000000 - 11111111
- 0 - 255
- 255

4.3.4 Class D and Class E

- **Class D:** Reserved for multicast groups.
- **Class E:** Reserved for future use.

Examples: Identify the class of each IP address and determine which part represents the host address.

- 9.4.3.47
- 203.42.62.1
- 103.88.77.22

4.4 Subnet Mask

Subnet Mask: A subnet mask is a numerical value used to separate the network and host portions of an IP address. It determines which part of an IP address is the network ID and which part is the host ID. For instance, consider the IP address 192.168.1.0 with a subnet mask of 255.255.255.0. In this example, the first three octets (192.168.1) represent the network ID, while the last octet (0) represents the host ID.

Here are a few more examples to illustrate:

- IP Address: 10.0.0.1

Subnet Mask: 255.0.0.0
Network ID: 10
Host ID: 0.0.1

- IP Address: 172.16.10.5

Subnet Mask: 255.255.0.0
Network ID: 172.16
Host ID: 10.5

Subnet masks are used at a bit-level to determine the network and host portions of an IP address. They are typically expressed in decimal format (like the examples above) or using CIDR notation (such as /24).

Subnetting: Let's say you have a network with the IP address 172.16.0.0 and a subnet mask of 255.255.0.0 , and that means 65k hosts. But you only need 100 hosts. You can subnet the network into smaller subnets to meet your requirements.

4.5 VLSM (Variable Length Subnet Masking)

VLSM is a technique that allows network administrators to divide an IP address space into subnets of different sizes, thereby optimizing the use of IP addresses. This method enables more efficient allocation of IP addresses by creating subnets with varying numbers of hosts based on the specific requirements of each network segment.

Follow the link for more information: VLSM and Subnetting

4.6 Default Gateway

It's known that router helps to connect different networks. The question is "How do devices find the router?". The answer is the default gateway. The default gateway is the IP address of the router that connects a device to other networks. When a device wants to communicate with a device on another network, it sends the data to the default gateway, which then forwards it to the appropriate destination.

Broadcasting: When a device wants to communicate with all devices on the network, it sends a broadcast message. The broadcast address is the highest address in the network.

If router recieves a broadcast message, it will not forward it to other networks because it is not efficient to send broadcast messages to other networks. It never forwards broadcast messages. But what if we need to announce something to all networks? The answer may be sending messages to all devices individually (called UNICAST) which is not efficient. Broadcasting may be the answer but what is a printer going to do with a message that is intended for a computer like a video? Also other networks will not be able to see the message since routers do not forward broadcast messages.

The solution is multicasting. Multicasting is a method of sending messages to a group of devices that are interested in receiving the message. It is more efficient than broadcasting because it targets only the devices that need the information. Multicasting is used for streaming video, audio, and other content to multiple recipients simultaneously. Also it refers to Class D IP addresses. Range of Class D IP addresses is: 224.0.0.0 to 239.255.255.255

4.7 Public & Private IP Addresses

How do we make sure that our IP adress are unique? The answer is the Internet Assigned Numbers Authority (IANA). IANA is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. IANA allocates IP addresses to Regional Internet Registries (RIRs), which in turn allocate IP addresses to Internet Service Providers (ISPs) and other organizations. Then the ISPs assign IP addresses to its customers.
RFC 1918: RFC 1918 defines three ranges of IP addresses that are reserved for private networks. These addresses are not routable on the public internet, meaning they are only used within private networks and are not globally unique. The three ranges are:

- 10.0.0.0 /8
- 172.16.0.0 /12
- 192.168.0.0 /16

Private IP Addresses: They are reserved for internal use and are not globally unique. Private IP addresses can be reused in different networks without conflict. They are commonly used in homes, businesses, and other private environments to create local networks (Eduroam). But private IPs are not allowed on the public internet. If a device with a private IP address needs to communicate with the internet, it must use Network Address Translation (NAT) to translate its private IP address to a public IP address. This process is handled by the router.(This topic will be covered in the future)

4.8 Adress Assignment

- **Static IP Address:** A static IP address is manually assigned to a device and remains constant. It is typically used for servers, network devices, and other devices that require a fixed address. Static IP addresses are less flexible than dynamic IP addresses but provide greater control over network resources.
- **Dynamic IP Address:** A dynamic IP address is automatically assigned to a device by a DHCP server. DHCP server has a pool that contains available IP adresses. When a device starts up, it broadcasts message around the local network to find the DHCP server then server gives appropriate IP adress to that device. It is temporary and may change each time the device connects to the network. Dynamic IP addresses are commonly used for personal computers, smartphones, and other devices that do not require a fixed address.

5 TCP & UDP

5.1 Introduction to TCP and UDP

TCP and UDP are two of the most common transport layer protocols used in networking. They are responsible for ensuring that data is transmitted reliably and efficiently between devices on a network. While both protocols serve similar functions, they have distinct characteristics that make them suitable for different types of applications.

In the header source port and destination port are used to identify the application that is sending or receiving the data. A port is a communication endpoint that allows multiple applications to share a single network connection. Ports are identified by a 16-bit number ranging from 0 to 65535. The source port is used to identify the application on the sending device, while the destination port identifies the application on the receiving device.

Value of source port is choosen randomly by the sending device. But the destination port is fixed. For example, the port number 80 is commonly used for HTTP traffic, while port 443 is used for HTTPS traffic.

TCP header contains the following fields:

Local IP	Remote IP	Local Port	Remote Port	Protocol
172.16.0.1	10.0.0.1	80	34761	TCP

Figure 22: TCP Header

Ports that are being used currently can be seen by using the command:

```
netstat -ano
```

Difference Between TCP and UDP:

- TCP has additional features while UDP is lightweight and faster.
- TCP is connection-oriented, ensuring reliable data delivery, while UDP is connectionless and does not guarantee delivery.
- TCP has built-in error checking and retransmission mechanisms, while UDP does not.
- TCP is used for applications that require reliable data transmission, such as web browsing and email, while UDP is used for real-time applications like video streaming and online gaming.
- TCP has windowing which is a flow control mechanism that allows the sender to adjust the rate of data transmission based on the receiver's capacity, while UDP does not have this feature.
- TCP has ordered data delivery, meaning that data packets are delivered in the order they were sent, while UDP does not guarantee the order of delivery.

5.2 TCP Connection Establishment

It is mentioned that TCP is a connection-oriented protocol. This means that a connection must be established between the sender and receiver before data can be transmitted.

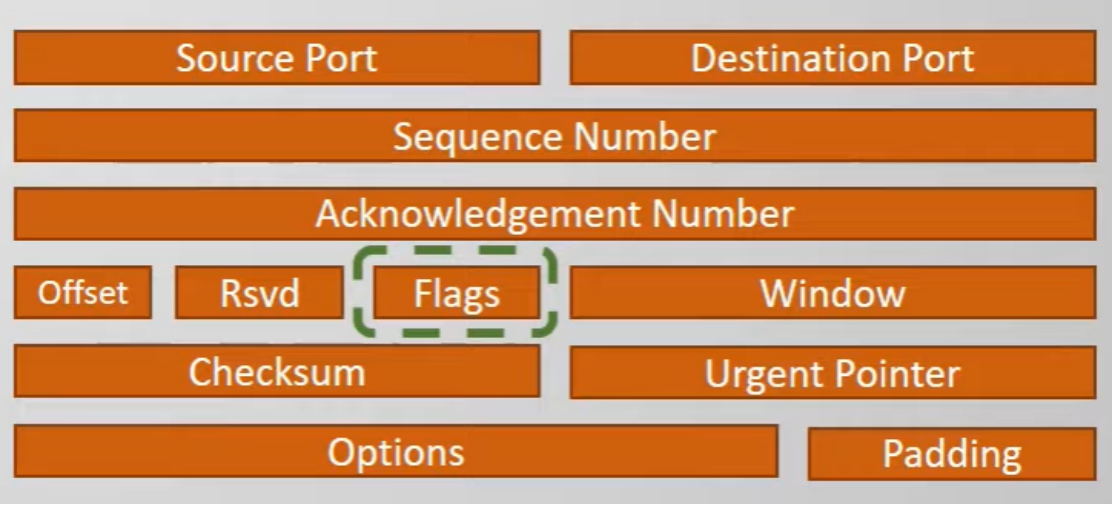

Figure 23: TCP Header

The process of establishing a connection is known as the **TCP three-way handshake**. Flags are used in the TCP header to indicate the status of the connection. The flags are:

- SYN (Synchronize): Used to initiate a connection.
- ACK (Acknowledgment): Used to acknowledge the receipt of a packet.
- FIN (Finish): Used to terminate a connection.
- RST (Reset): Used to reset a connection.
- URG (Urgent): Used to indicate that the data is urgent.
- PSH (Push): Used to push data to the application layer.

The client sends a SYN packet to the server to initiate the connection. Some details are included in the packet such as source and destination ports, windowsize ,and sequence number(randomly generated by the client and important for security).

If client and server are agreed on the connection, server sends a SYN-ACK packet to client where port numbers are swapped and sequence number is increased by 1.

After clients receives the SYN-ACK packet, it sends an ACK packet to the server to acknowledge the receipt of the SYN-ACK packet. The connection is now established and data can be transmitted between the client and server, and the sequence number is increased by 1.

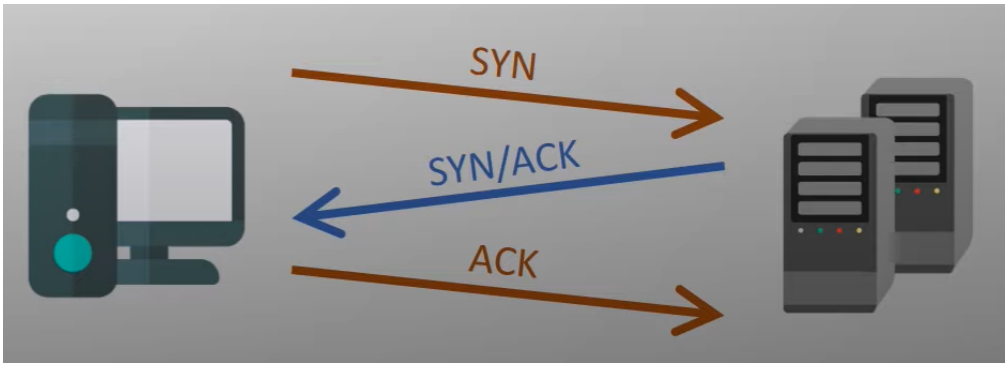

Figure 24: TCP Three-Way Handshake

After a time period, the connection will be terminated because maybe the client does not need the connection anymore or an error occured. There are two ways to terminate the connection. First way:

- Server sends FIN and ACK packet to client to indicate that it is ready to terminate the connection.
- Client sends an ACK packet to server to acknowledge the receipt of the FIN-ACK packet.
- Client sends a FIN and ACK packet to server to indicate that it is ready to terminate the connection.
- Server sends an ACK packet to client to acknowledge the receipt of the FIN-ACK packet.

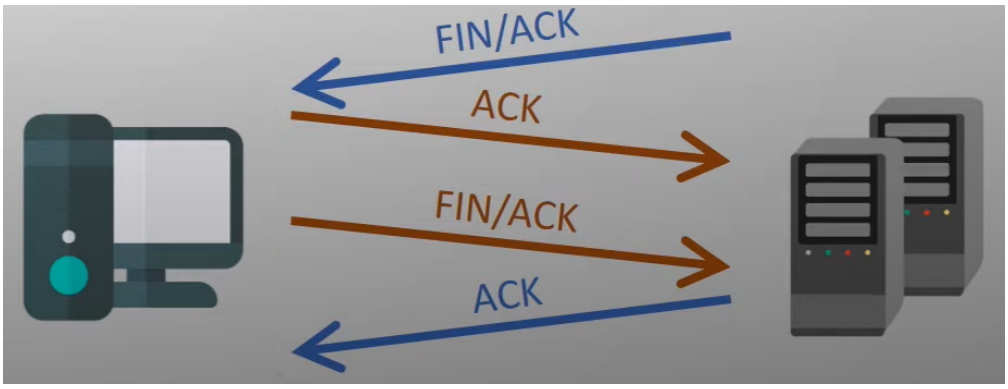

Figure 25: TCP Connection Termination

FİRst pair of messages to start the process and the second pair of messages to end the process.

Second way:

- Server sends RST packet to client to indicate that it is ready to terminate the connection.
- And the connection is terminated.

This type of termination are occured in case of errors. For example, if the port is not open, the server will send a RST packet to the client to indicate that the connection cannot be established. This happens before the three-way handshake is completed. This type of termination helps with troubleshooting network issues.