Networking basics

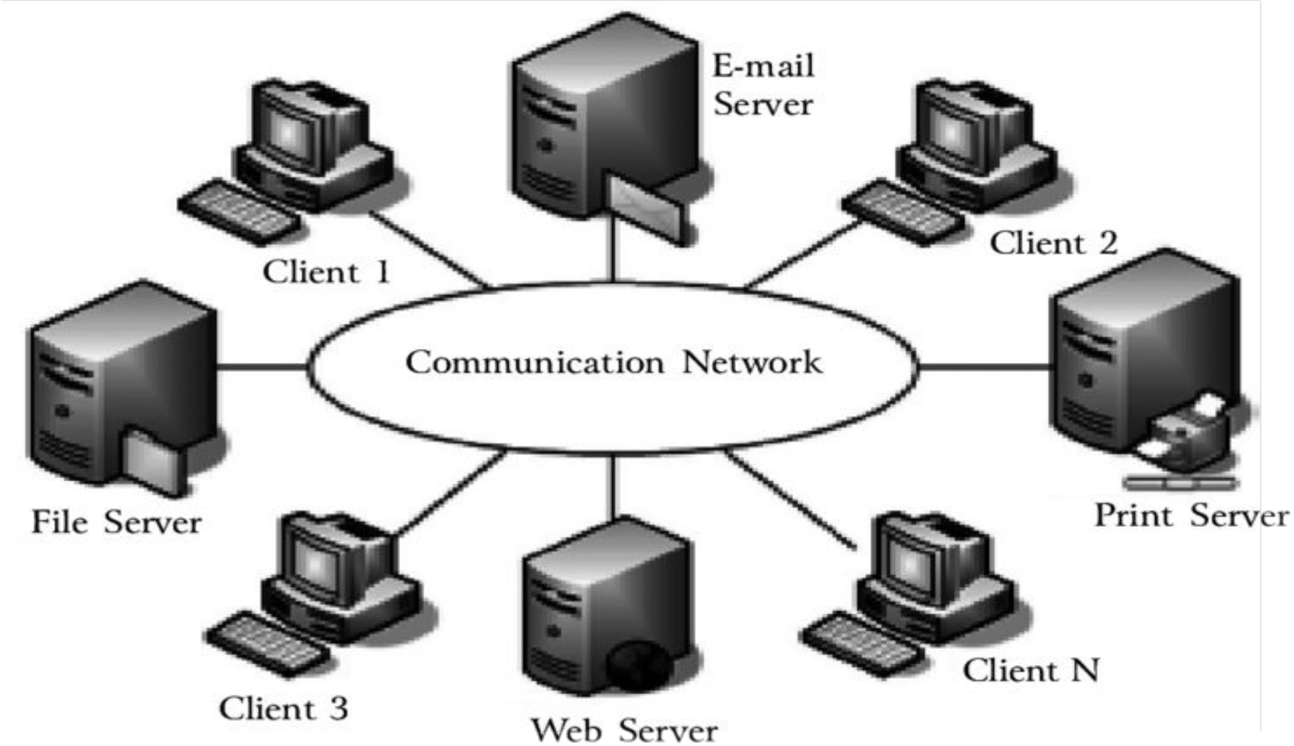
By: Divya Shukla

Session Guidelines and pre-requisites

- Please be ready with your Linux/Ubuntu terminal before the session so that you can try hands-on
- Last 10-15 mins of the session would be dedicated to doubt clearing for the current session and past sessions
- Keep the non-technical questions for the end of the session
- Prefer asking any assignment related question at the end of the session or in the doubt-classes

What is computer networking?

- Computer networking refers to the practice of connecting multiple computing devices together to share resources, exchange information, and communicate with each other.
- These devices can include computers, servers, routers, switches, and various other networking hardware and software components.
- Computer networking is making devices (like computers and phones) talk to each other and share stuff. It's like creating roads and rules for digital communication.

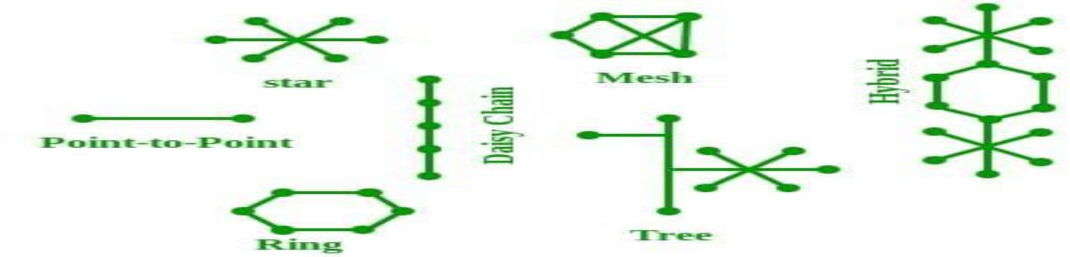

E-mail Server
Client 1
Client 2
Communication Network
File Server
Print Server
Client 3
Web Server
Client N

Why computer networking?

- The primary goal of computer networking is to enable efficient data exchange and communication among these devices, whether they are located in the same geographical area or spread across different locations globally.
- It's like the internet that connects people globally, but for devices. This sharing helps us access websites, send messages, share files, and use various online services smoothly.

Objectives of CN

- **Data Transmission**:Networks allow devices to transmit data(wired/wireless), which can be in the form of text, audio, video, or any other type of information.
- **Resource Sharing**:Networks enable the sharing of resources such as files, printers, and internet connections. This reduces the need for duplicate resources and improves efficiency.
- **Communication:**Networks facilitate communication between devices, whether it's a simple message exchange or a more complex data transfer between servers and clients.
- **Data Security**:Network security is essential to protect sensitive data from unauthorized access, hacking, and other threats. This involves implementing measures like firewalls, encryption, and authentication protocols.
- **Topology**: Network topology refers to the physical or logical layout of devices in a network. Common topologies include star, bus, ring, and mesh, each with its advantages and disadvantages.



Objectives of CN

- **Data Transmission**:Networks allow devices to transmit data(wired/wireless), which can be in the form of text, audio, video, or any other type of information.
- **Resource Sharing**:Networks enable the sharing of resources such as files, printers, and internet connections. This reduces the need for duplicate resources and improves efficiency.
- **Communication:**Networks facilitate communication between devices, whether it's a simple message exchange or a more complex data transfer between servers and clients.
- **Data Security**:Network security is essential to protect sensitive data from unauthorized access, hacking, and other threats. This involves implementing measures like firewalls, encryption, and authentication protocols.
- **Topology**: Network topology refers to the physical or logical layout of devices in a network. Common topologies include star, bus, ring, and mesh, each with its advantages and disadvantages.

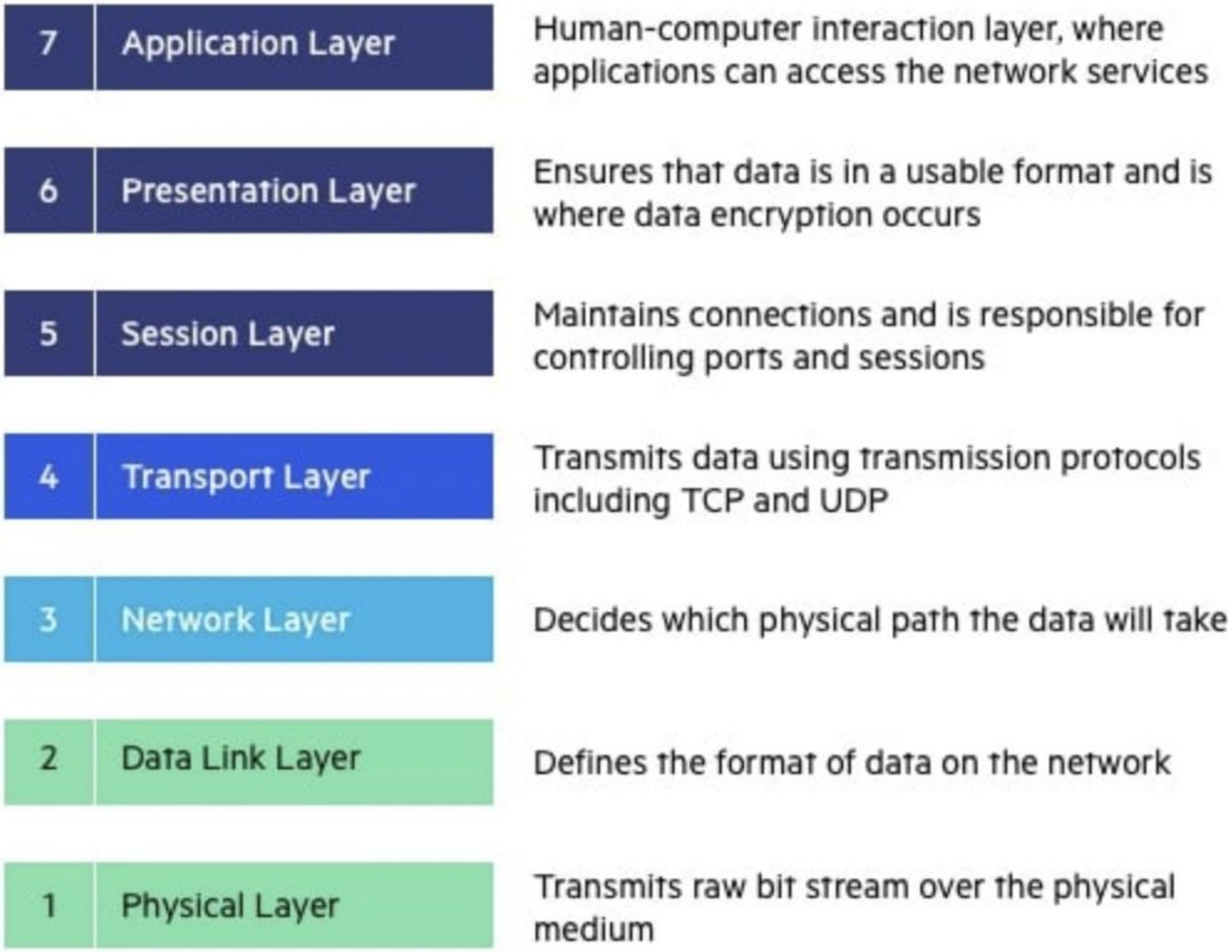
Objectives of CN

- **Data Transmission**:Networks allow devices to transmit data(wired/wireless), which can be in the form of text, audio, video, or any other type of information.
- **Resource Sharing**:Networks enable the sharing of resources such as files, printers, and internet connections. This reduces the need for duplicate resources and improves efficiency.
- **Communication:**Networks facilitate communication between devices, whether it's a simple message exchange or a more complex data transfer between servers and clients.
- **Data Security**:Network security is essential to protect sensitive data from unauthorized access, hacking, and other threats. This involves implementing measures like firewalls, encryption, and authentication protocols.
- **Topology**: Network topology refers to the physical or logical layout of devices in a network. Common topologies include star, bus, ring, and mesh, each with its advantages and disadvantages.

Open Systems Interconnection (OSI)

Think of the OSI model as a way to describe how computers communicate with each other over a network, like the internet. It's like a recipe that helps different devices, like your computer or your smartphone, talk to each other in a organized and understandable way.

It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Open Systems Interconnection (OSI) 7 layers

All = Application Layer

People = Presentation Layer

Seem = Session Layer

To = Transport Layer

Need = Network Layer

Data = Data Link Layer

Processing = Physical Layer

Open Systems Interconnection (OSI) 7 layers

Imagine you want to send a letter to your friend who lives far away. You wouldn't just start writing the letter on a piece of paper and hope it reaches your friend, right? You follow a series of steps:

- **Put It in an Envelope (Presentation Layer)**: Before you send the letter, you might put it in an envelope. This layer helps make sure the letter looks nice and is easy to understand. In the digital world, this layer helps convert the information from your software into a format that can be easily understood by other devices.
- **Address the Envelope (Session Layer):** You put your friend's address on the envelope so the post office knows where to send the letter. In the OSI model, this layer manages the connection between your computer and the one you're sending the message to.

Open Systems Interconnection (OSI) 7 layers

- **Send the Letter (Transport Layer)**:The post office takes care of sending the letter safely to your friend's city. In the OSI model, this layer makes sure that your message gets divided into smaller pieces if needed and that those pieces are sent and received correctly.
- **Route the Letter (Network Layer)**:Now the letter needs to find its way to your friend's house. The post office uses the address to figure out the best route. In the OSI model, this layer helps determine the best path for your message to travel through the network to reach its destination.
- **Get to the Right Street (Data Link Layer)**:The post office sends the letter to your friend's street. In the OSI model, this layer makes sure that the data is properly packaged and addressed for the specific devices on the same network.

Open Systems Interconnection (OSI) 7 layers

- **Deliver to the House (Physical Layer):** The letter is finally delivered to your friend's house. In the OSI model, this layer deals with the actual physical connections, like cables or wireless signals, that allow the data to move between devices.

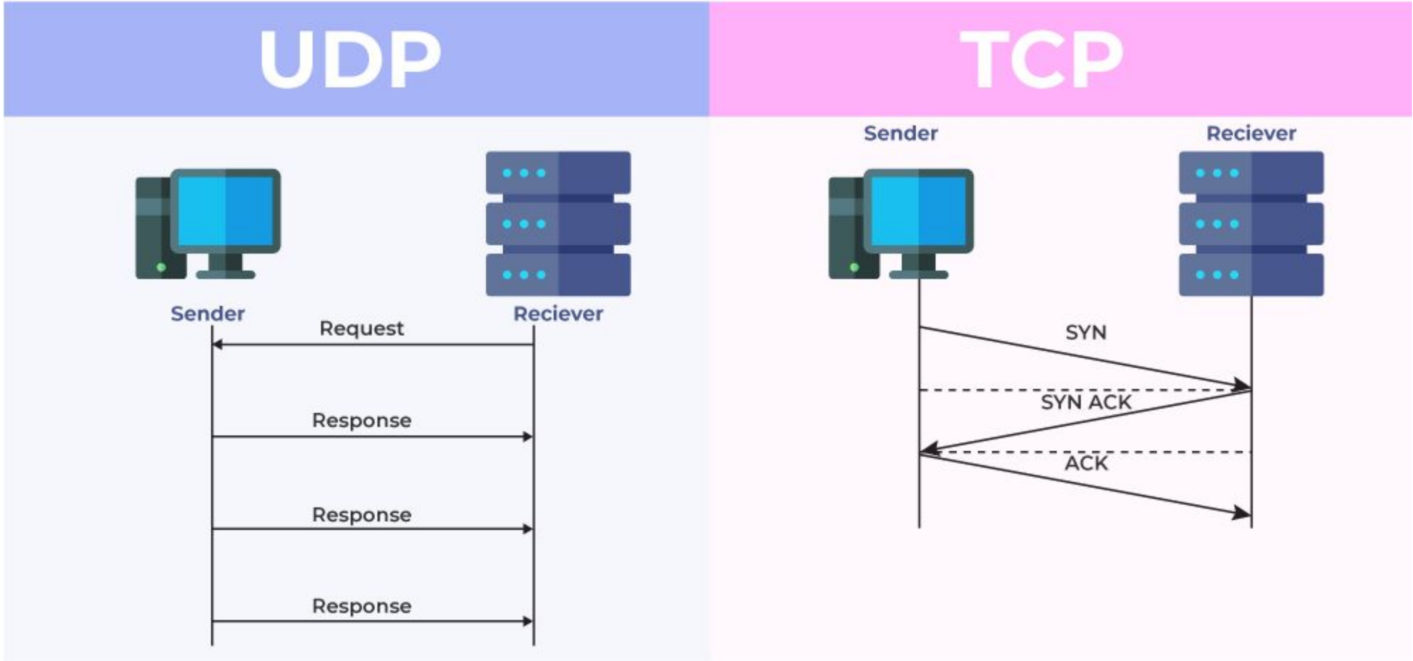
So, the OSI model is like a set of instructions that helps computers break down communication into different steps, making sure everything works smoothly when they talk to each other over the internet or any other network.

TCP & UDP Protocol

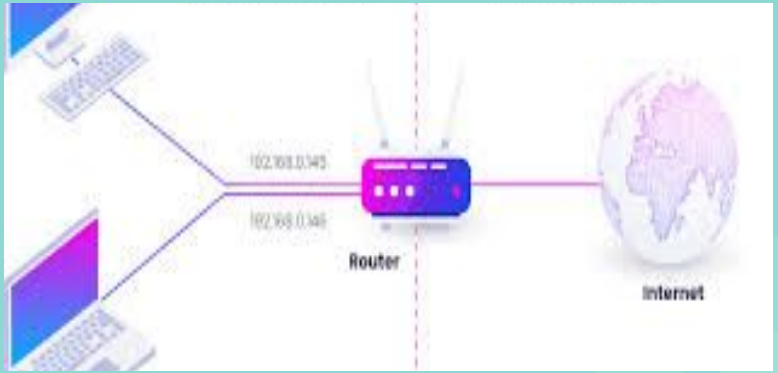
TCP: It is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

UDP: It is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.

TCP & UDP Protocol



Understanding Network and IP



Internet Protocol (IP)

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Imagine you have a house with a unique address that helps the mailman know where to deliver your letters. In the world of computers and networks, an IP address is like a digital address for a device.

Subnets

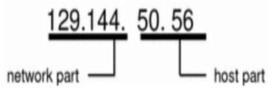
A subnet is a logical subdivision of an IP network. It allows network administrators to divide a single, large network into smaller, more manageable subnetworks. Subnets help in optimizing network performance, security, and organization. Each subnet has its own unique range of IP addresses and can be configured with its own security and routing settings.

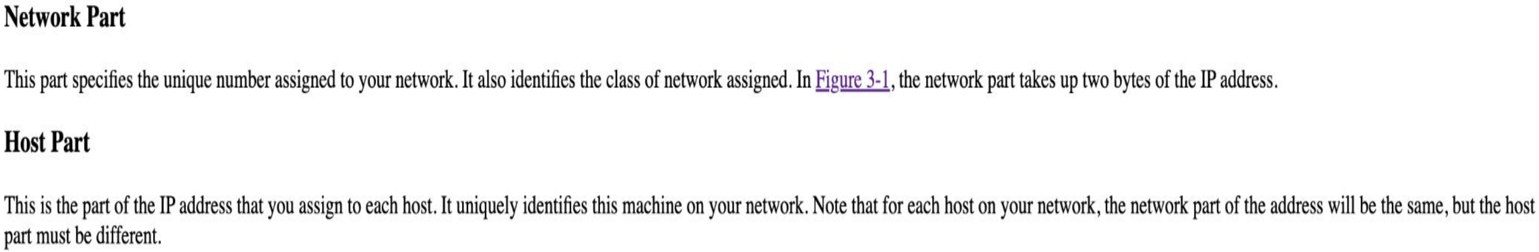
IP Address

IP address is basically divided into two parts: X1. X2. X3. X4

1. [X1. X2. X3] is the Network ID

2. [X4] is the Host ID





Network Part

This part specifies the unique number assigned to your network. It also identifies the class of network assigned. In Figure 3-1, the network part takes up two bytes of the IP address.

Host Part

This is the part of the IP address that you assign to each host. It uniquely identifies this machine on your network. Note that for each host on your network, the network part of the address will be the same, but the host part must be different.

IP Address

Version of IP address:

Currently there are 2 versions of IP addresses are in use i.e IPV4 and IPV6

1. **IPV4 (Internet Protocol Version 4):** It is the first version of Internet Protocol address. The address size of IPV4 is 32 bit number. In this Internet Protocol Security (IPSec) with respect to network security is optional. It is having 4,294,967,296 number of address still we are seeing a shortage in network addresses as the use of network & virtual devices are increasing rapidly.
2. **IPV6 (Internet Protocol Version 6):** It is the recent version of Internet Protocol address. The address size of IPV6 is 128 bit number. In this Internet Protocol Security (IPSec) with respect to network security is mandatory. It allows 3.4 x 10^38 unique IP addresses which seems to be more than sufficient to support trillions of internet devices present now or coming in future.

IP Address

IP addresses are categorized into different classes based on the range of addresses they cover and the number of networks and hosts they can support. However, with the adoption of Classless Inter-Domain Routing (CIDR), these classes are less strictly defined. Traditionally, IP addresses were divided into classes as follows:

Class A: These addresses start with a first octet in the range of 1 to 126. Class A networks are designed for very large organizations, offering a large number of networks but fewer host addresses per network.

Class B: Addresses starting with a first octet in the range of 128 to 191 belong to Class B. They are suitable for medium-sized organizations, providing a balance between networks and hosts.

Class C: Class C addresses begin with a first octet in the range of 192 to 223. These are used for smaller networks and offer more host addresses per network but fewer networks overall.

IP Address

Private vs. Public IP Addresses:

Private IP Addresses: These are reserved for use within a private network and are not routable over the public internet. They're used for local network communication within an organization and are defined by specific ranges:

Class A private addresses range from 10.0.0.0 to 10.255.255.255.

Class B private addresses range from 172.16.0.0 to 172.31.255.255.

Class C private addresses range from 192.168.0.0 to 192.168.255.255.

Public IP Addresses: These are globally unique addresses used on the internet. They're assigned to devices connected directly to the internet and are routable across the internet. Public IPs can be obtained from Internet Service Providers (ISPs) or allocated by internet authorities.

The division between private and public IP addresses is essential for ensuring the scalability and security of the internet. Devices within a private network can use private IPs for communication within that network and rely on routers or other devices to translate between private and public IPs for internet communication.

Type of Internet Protocol (IP)

1. Public IP
2. Private IP

Type of Internet Protocol (IP)

ICMP (Internet Control Message Protocol):
ICMP is a core protocol within the Internet Protocol Suite. It's used for diagnostic and control purposes.
It doesn't serve as a primary data delivery protocol but rather handles error reporting, network congestion, and other control messages between network devices.
ICMP messages are typically generated in response to errors in IP datagrams or for diagnostic or routing purposes.

Type of Internet Protocol (IP)

Examples of ICMP messages include 'ping' requests and responses, which are used to test connectivity between devices, 'destination unreachable' messages indicating a problem reaching a destination, 'time exceeded' messages used for traceroute, and 'redirect' messages for routing optimization.

DGRP (Distance Vector Multicast Routing Protocol):

DGRP stands for Distance Vector Multicast Routing Protocol.

It's a protocol used for routing multicast packets in networks.

Unlike unicast (one-to-one) and broadcast (one-to-all) communication, multicast (one-to-many) enables efficient transmission to multiple recipients interested in specific data.

Type of Internet Protocol (IP)

DGRP calculates the best path for multicast traffic delivery within a network using a distance-vector algorithm, considering factors like path cost and hop count.

Devices running DGRP share information about multicast group membership and forward multicast traffic along the most efficient paths within the network.

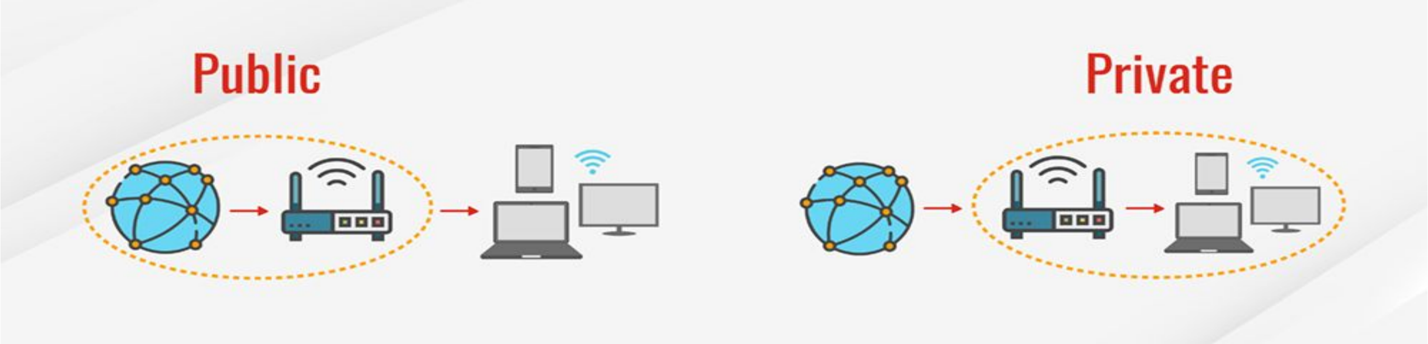
Both protocols, ICMP and DGRP, play crucial roles in network communication, with ICMP handling control messages and DGRP managing efficient multicast packet routing within networks.

IP

Public IP & Private IP

Private IP address of a system is the IP address that is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address that is used to communicate outside the network. A public IP address is basically assigned by the ISP (Internet Service Provider).

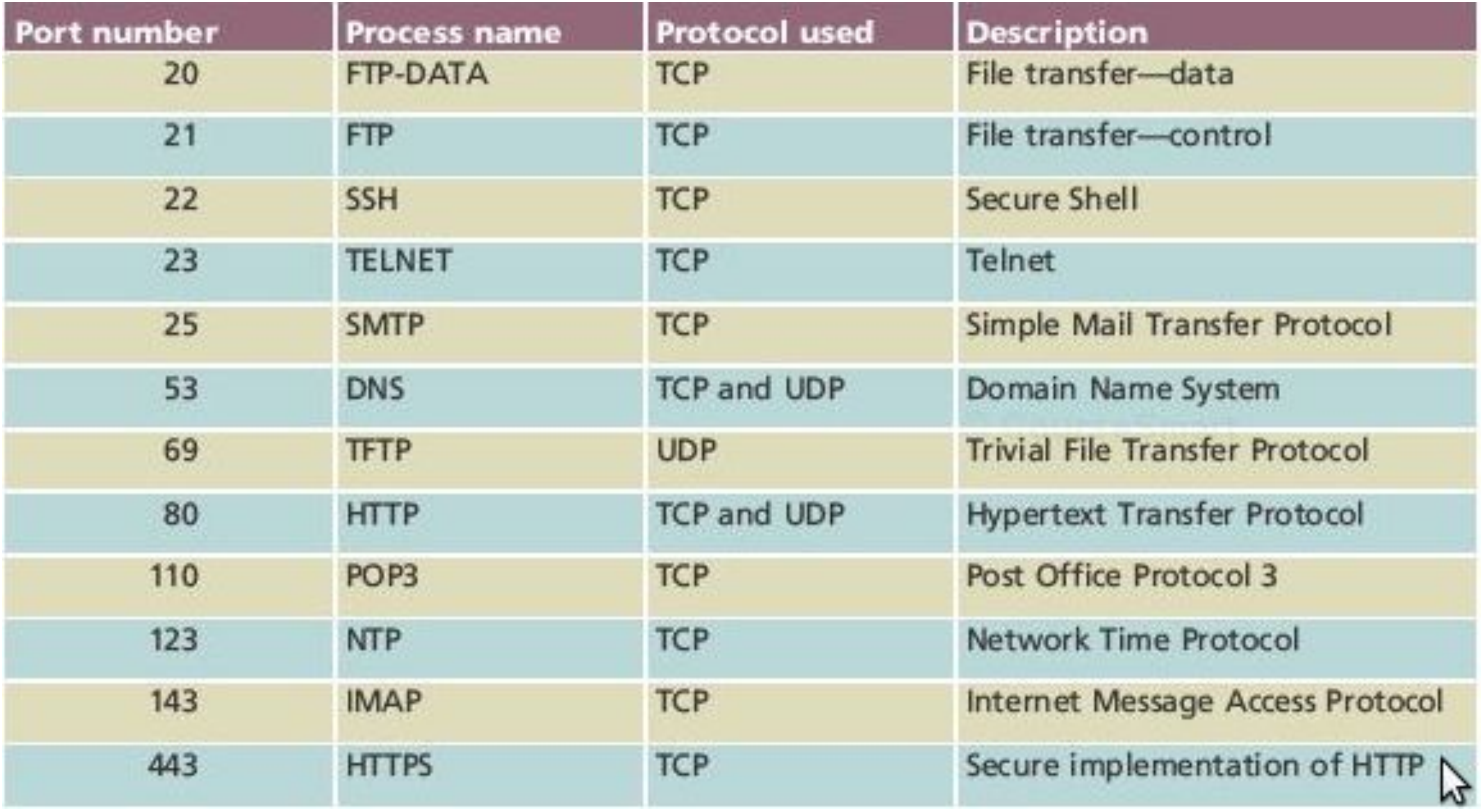


Type of Internet Protocol (IP)

1. Ping
2. Traceroute (Tracert in Windows)
3. ipconfig (Windows) / ifconfig (Linux/macOS)
4. netstat
5. nslookup (Windows) / dig (Linux/macOS)
6. route (Linux/macOS) / route print (Windows)
7. ifup / ifdown (Linux)
8. arp (Windows) / arp -a (Linux/macOS)
9. ssh (Secure Shell)
10. netsh (Windows)

Port

A port is a logical number that identifies specific services or applications on a device. In computer networking, a port is a logical communication endpoint that allows a host to share a single network connection for multiple applications. Ports are identified by a 16-bit number (0-65535) and are associated with specific services or applications, directing incoming and outgoing network traffic. In computer networking, a port is a logical communication endpoint that allows a host to share a single network connection for multiple applications. Ports are identified by a 16-bit number (0-65535) and are associated with specific services or applications, directing incoming and outgoing network traffic



Port number	Process name	Protocol used	Description
20	FTP-DATA	TCP	File transfer—data
21	FTP	TCP	File transfer—control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

Networking Resources

- Ebook: **Computer Networking : Principles, Protocols and Practice**

Let's answer your questions now!

Thanks for attending the lecture :)