

N

E

T

W

O

R

K



CONTENTS

- Network Definition
- Network Types
- Network Topologies
- OSI Model
- TCP/IP Model
- Encapsulation & De-encapsulation
- Mac Address & IPs
- Ports&Protocols



Network Definition

What is a network?

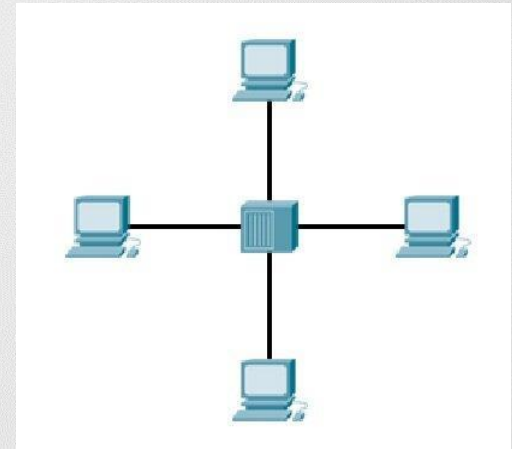
A computer network is a system of interconnected devices that can communicate using protocols. These devices communicate to exchange resources (e.g. files and printers) and services.

The two computers are directly **connected** using a **cable**. This small network can be used to exchange data between just these two computers.



What if we want to expand our network?

we can use a **network device** to connect more than two computers together



Importance of Networks

- Data sharing
- Sharing of expensive devices and network resources
- Modern Technologies (VOIP, BYOD, Video Conferencing, IOTetc)

Network components

End devices (servers and hosts)

- ex: PC-laptop-smart phone-network printer-server..etc

Network Devices

- Devices that interconnect different computers together

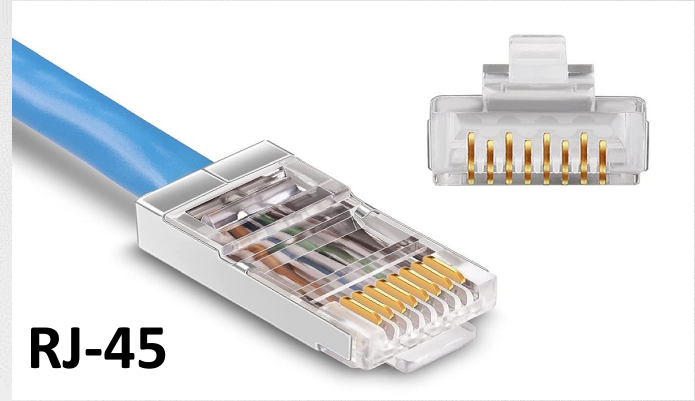
- ex: hub, switch, router, firewalls..etc

Media

- wires-wireless



NIC



RJ-45



Router



Switch

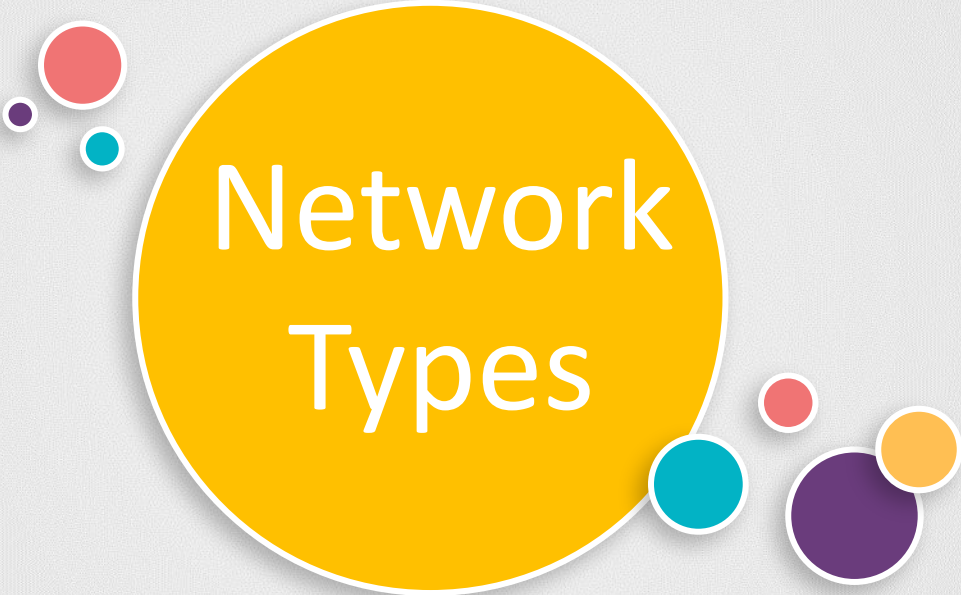
Network vs Internet

The **network** consists of computers that are physically connected and can be used as a personal computer as well as to share information with each other.

The internet is a technology which links these small and large networks with each other and builds a more extensive network.

The internet called network of networks.

Note: In Internet, all of these devices are called hosts or end systems.

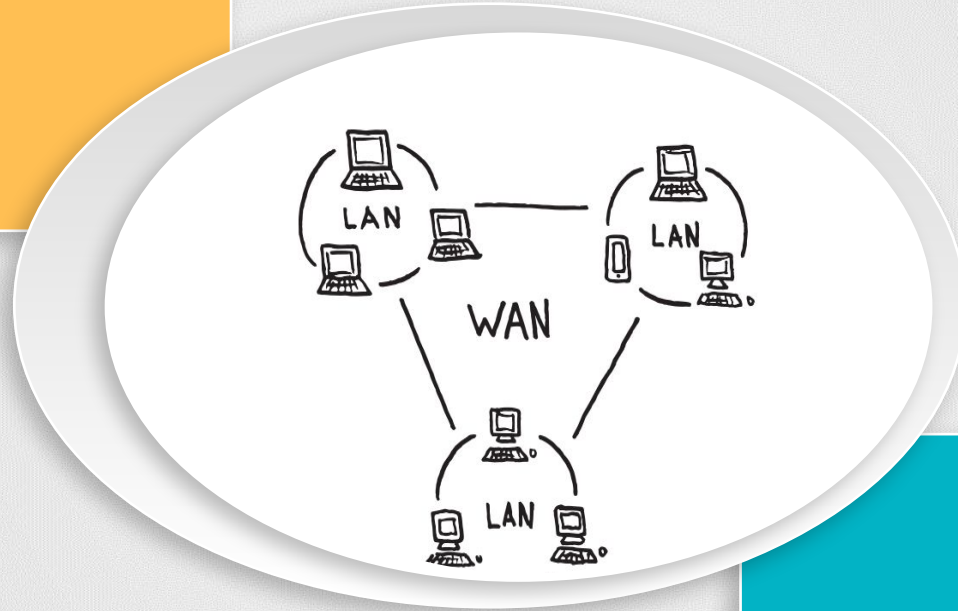


Network Types

Computer Network Types

LAN

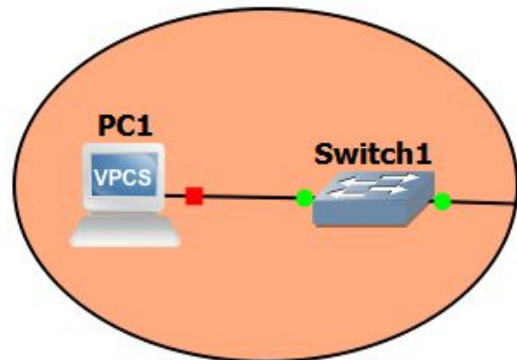
Local Area Network



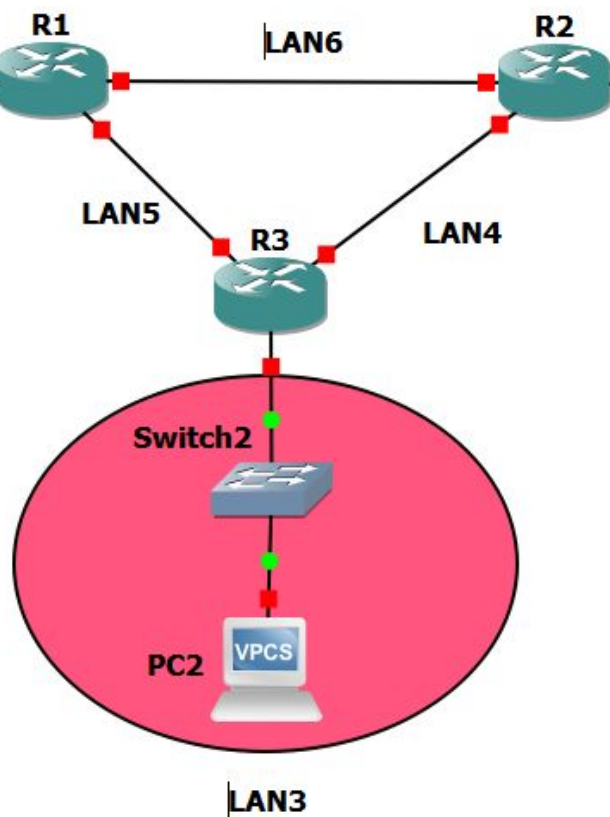
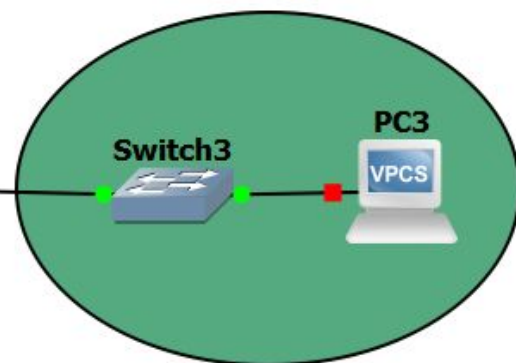
WAN

Wide Area Network

LAN1



LAN2





Network Topologies

Topology

A topology describes how devices are connected and interact with each other using communication links.

Types of Topology

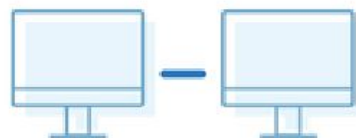
Physical Topology : physical layout of nodes and cables

Logical Topology : describe the way data flow from one computer to another. (how devices communicate internally)

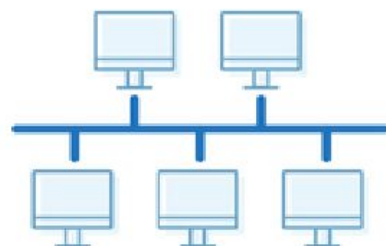
A network can have one physical topology and multiple logical topologies at the same time

Network Topology Types

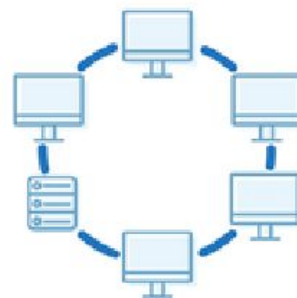
1 Point to point



2 Bus



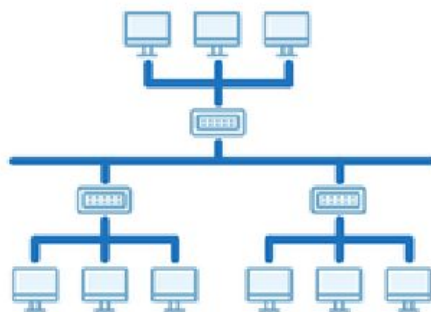
3 Ring



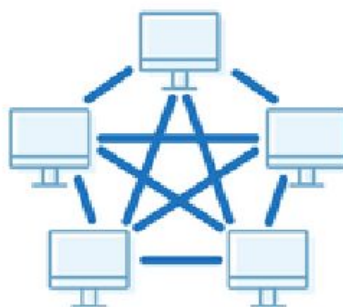
4 Star



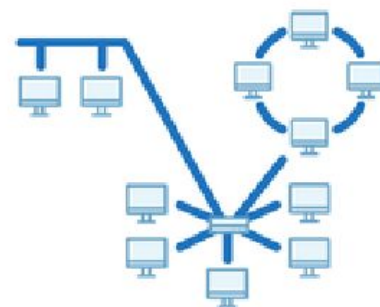
5 Tree



6 Mesh



7 Hybrid



A large orange circle with a white border contains the text "OSI Model" in white. To its left are three small circles: a red one, a purple one, and a teal one. To its right are four small circles: a red one, a teal one, a purple one, and a yellow one.

OSI Model

OSI Model

- Open Systems Interconnection
- It provides a standard for different computer systems to be able to communicate with each other.
- The OSI model has seven layers, with each layer describing a different function of data traveling through a network.

7. Application

6. Presentation

5. Session

4. Transport

3. Network

2. Data Link

1. Physical

Send

7.Application



6. Presentation



5.Session



4.Transport



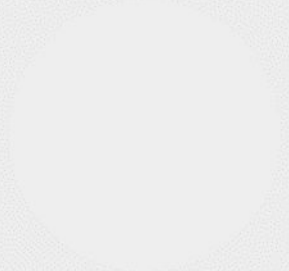
3. Network



2.Data-link



1.Physical



7.Application



6. Presentation



5.Session



4.Transport



3. Network



2.Data-link



1.Physical

receive



Layer 7 – Application Layer (Desktop Layer)

It's implemented by the network applications. These applications produce the data, which has to be transferred over the network. E.g, Web browsers, Skype Messenger.

Layer 6 – Presentation Layer (syntax layer)

- Encoding/Decoding (Translation): ASCII ↔ 0,1 Machine Language
- Defines data formats. Examples: ASCII, doc,JPG,PDF,...etc
- Compression /decompression
- Encryption/ Decryption:

Layer 5 – Session Layer

- Defines how to establish and terminate a session between the two systems.

Layer 4 – Transport Layer

- Segmentation and reassembly
- Flow Control
- Error Control

7.Application



6. Presentation



5.Session



4.Transport

Layer 3 – Network Layer

- Defines device(logical) addressing such as IP addresses
- Routing (choose the best path to destination.)

Layer 2 – Data-link Layer

The data link layer has two sublayers:

1. **Logical Link Control** – used for flow control and error detection.
2. **Media Access Control** – used for hardware addressing and for controlling the access method.

Layer 1 – Physical Layer

Physical – defines how to move bits from one device to another. It details how cables, connectors and network interface cards are supposed to work and how to send and receive bits.

4.Transport



3. Network

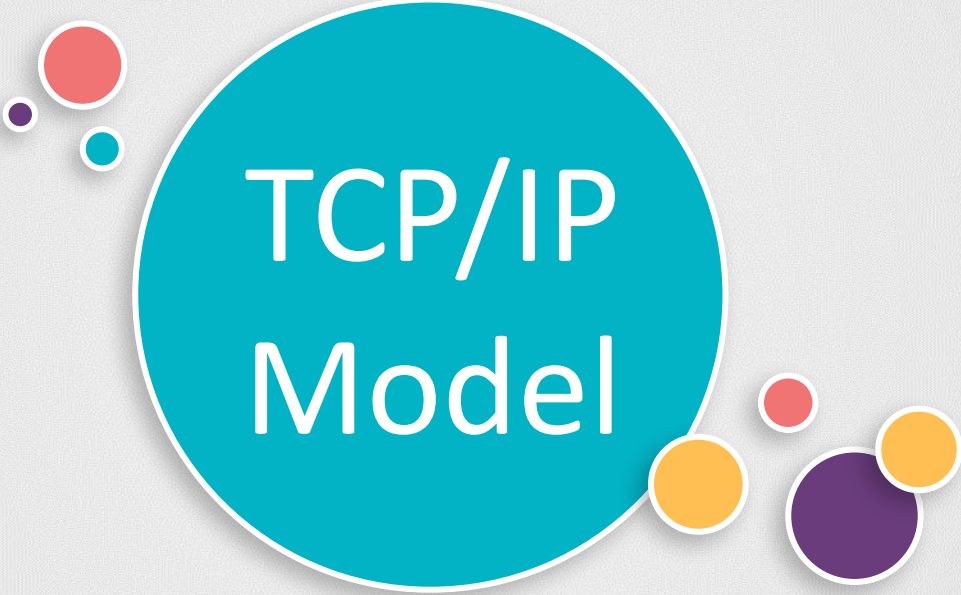


2.Data-link



1.Physical

It is a common practice to reference a protocol by the layer number or layer name. For example, HTTPS is referred to as an application (or Layer 7) protocol.

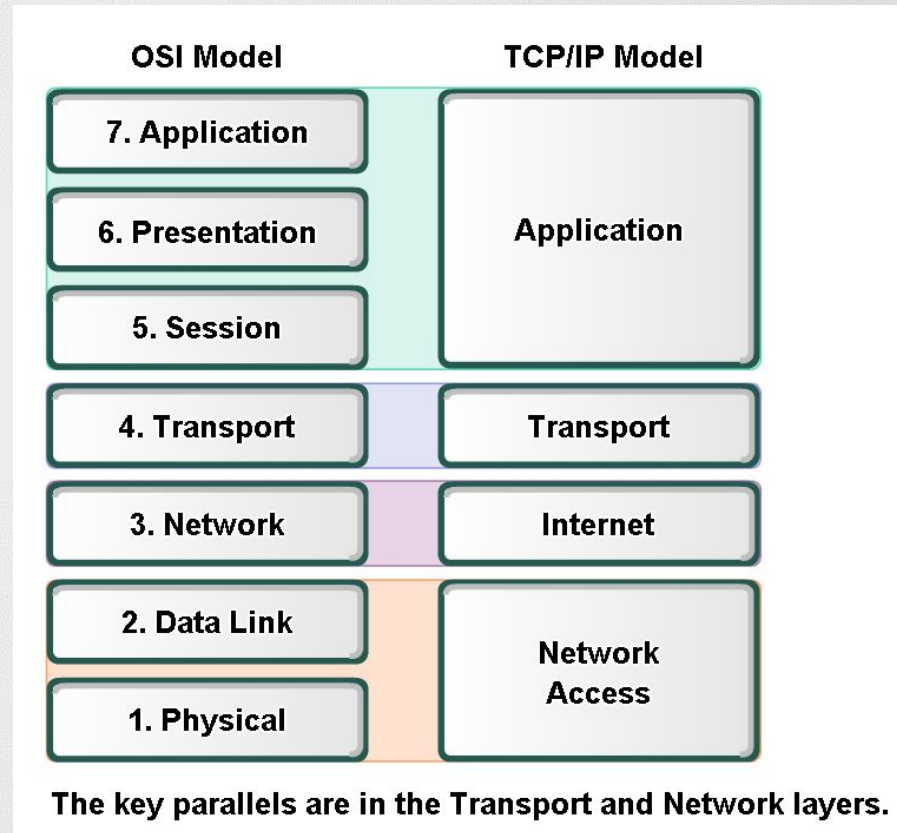


TCP/IP Model

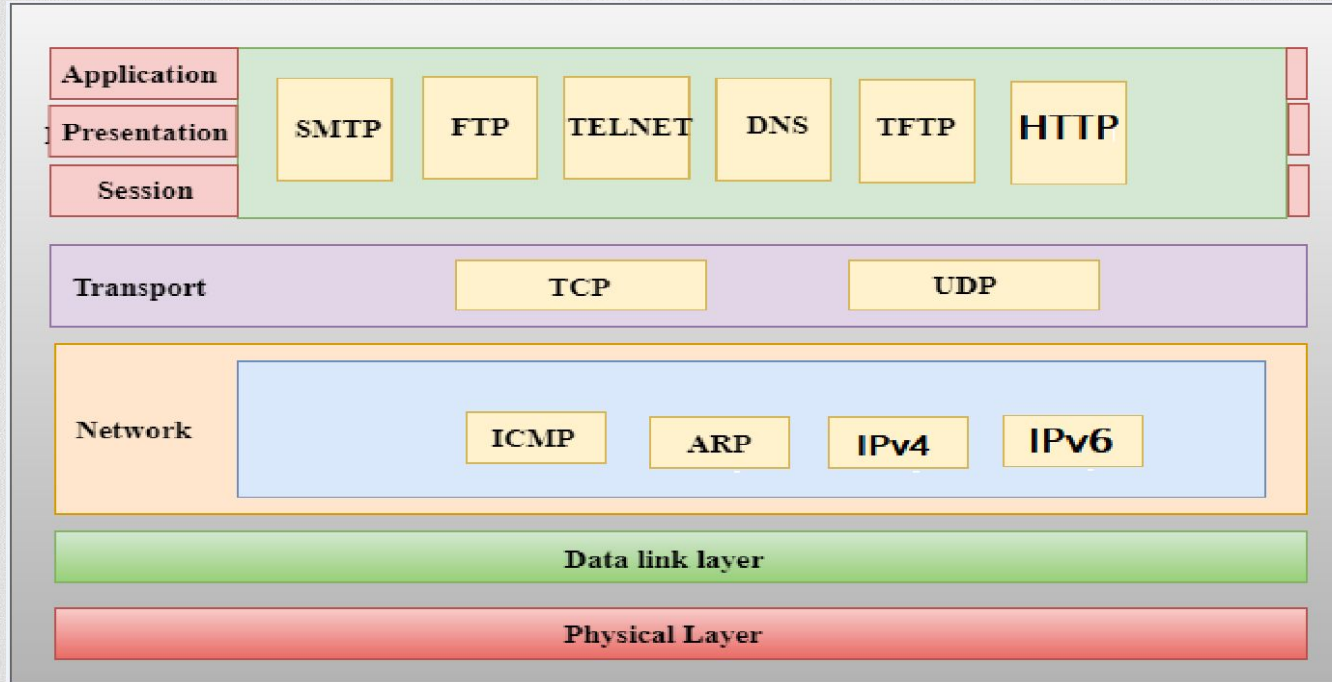
Layers with TCP/IP and OSI Model

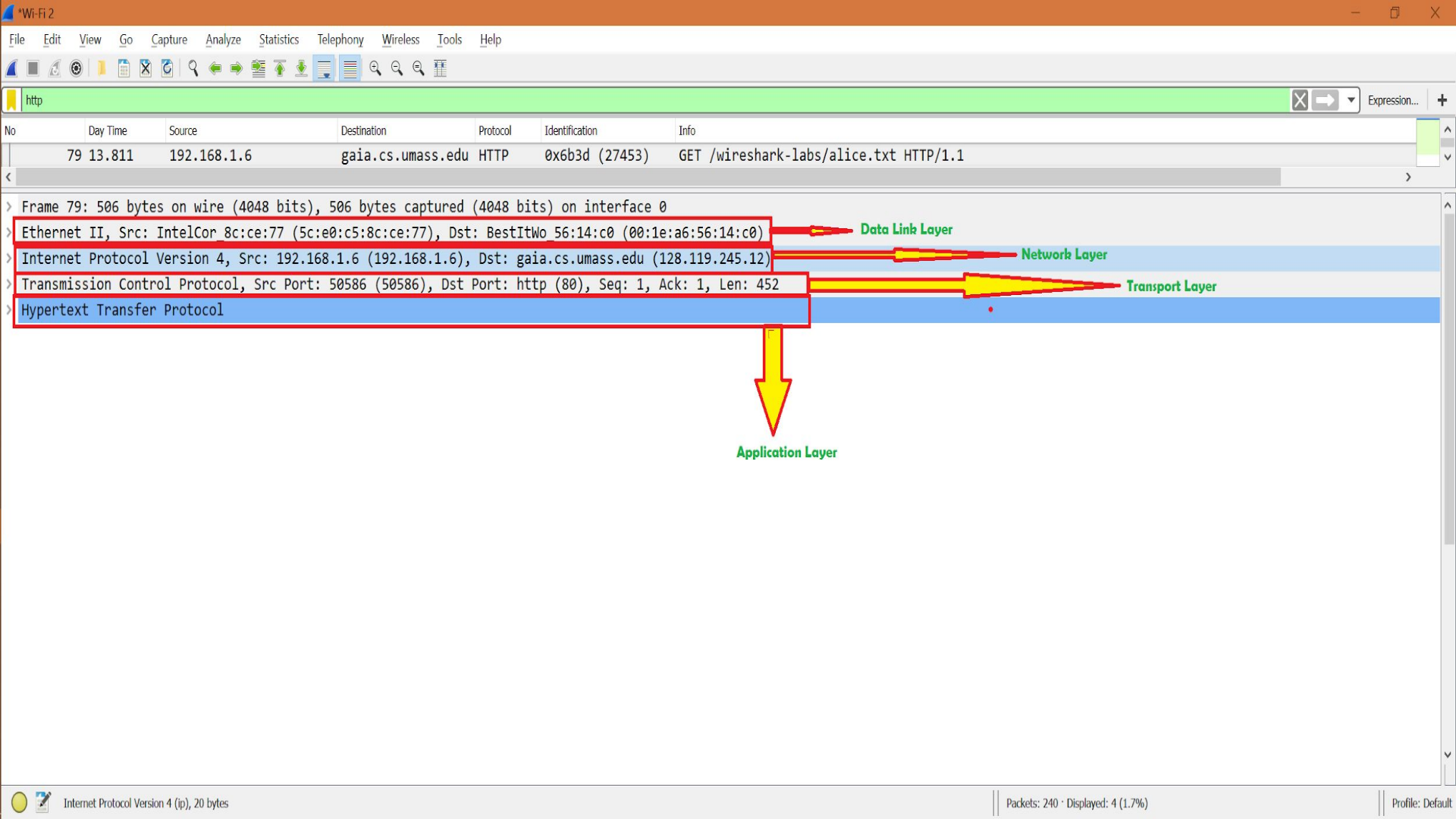
The Application, Presentation, and Session layers of the OSI model are merged into a single layer in the TCP/IP model.

Also, Physical and Data Link layers are called Network Access layer in the TCP/IP model.



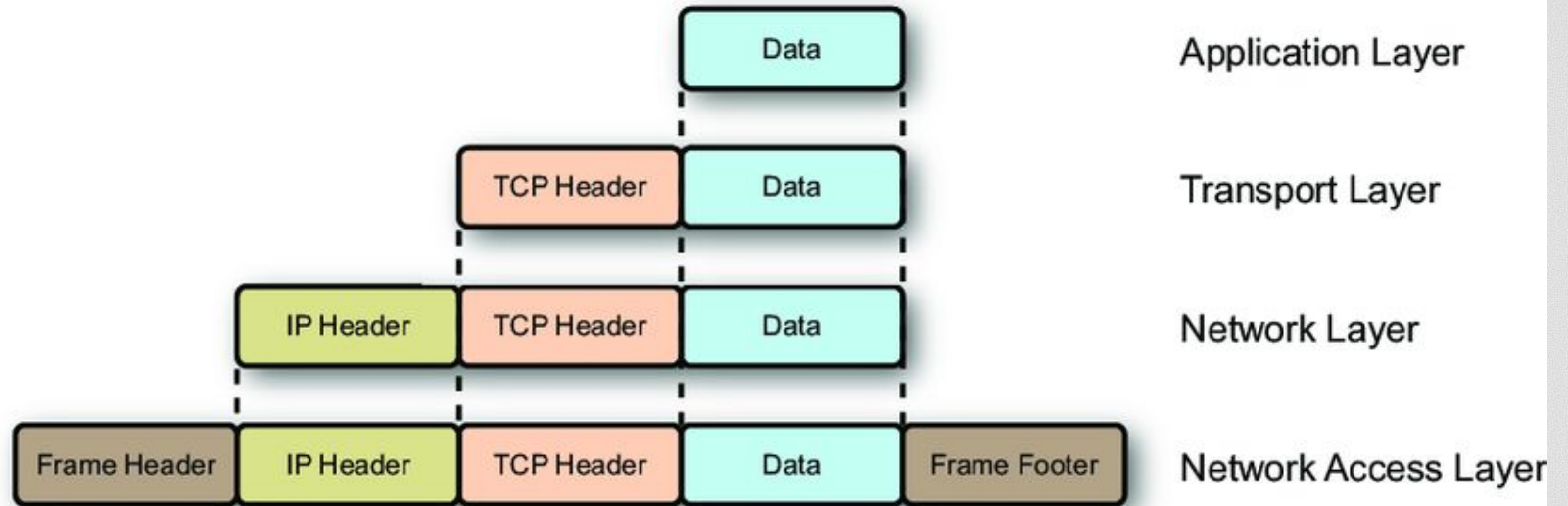
The following table shows which protocols reside on which layer of the TCP/IP model:







Encapsulation & De-encapsulation



Data Encapsulation

is the process in which some extra information is added to the data item to add some features to it.

Data encapsulation adds the protocol information to the data so that data transmission can take place in a proper way. This information can either be added in the header or the footer of the data.

Data De-encapsulation

Data De-encapsulation is the reverse process of data encapsulation.

The encapsulated information is removed from the received data to obtain the original data.

This process takes place at the receiver's end.

The data is de-encapsulated at the same layer at the receiver's end to the encapsulated layer at the sender's end.

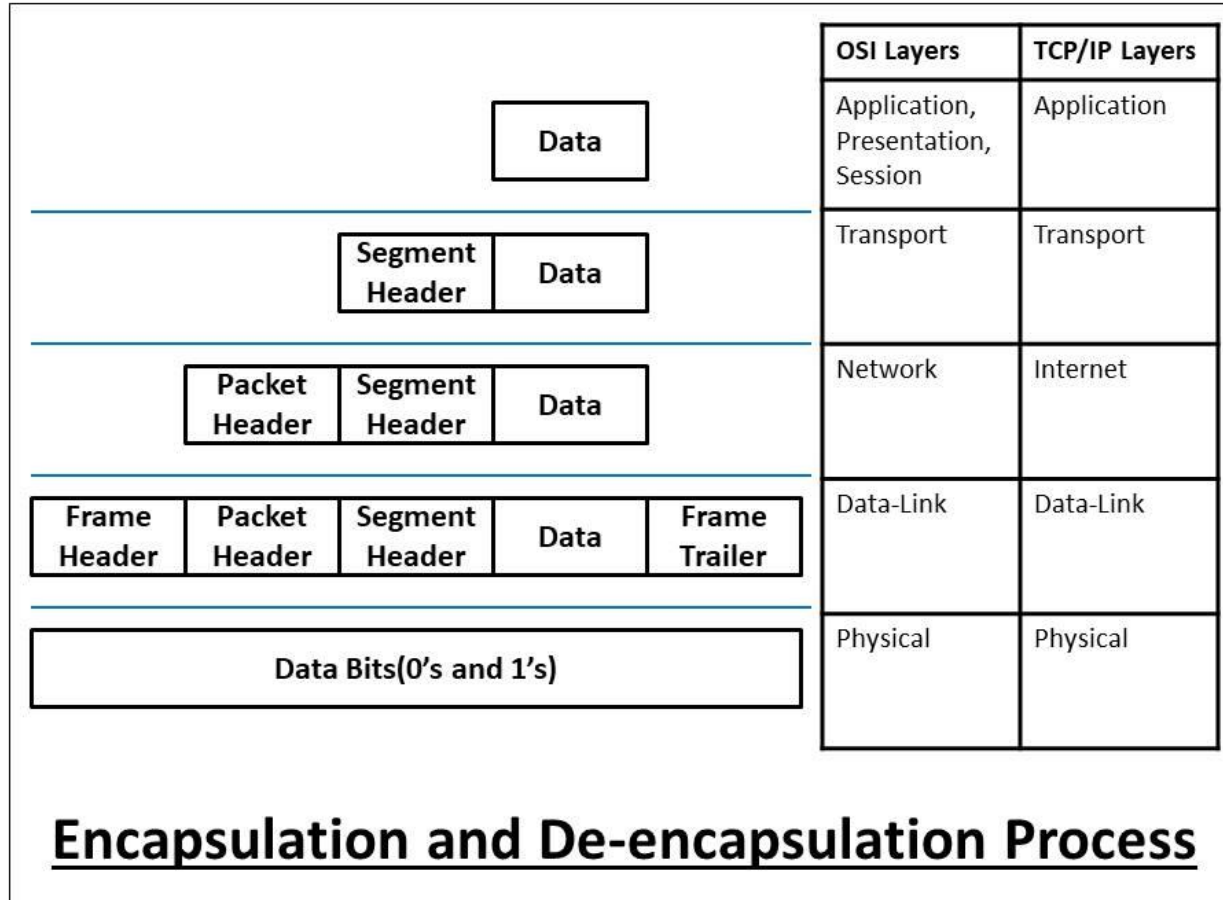
The added header and trailer information are removed from the data in this process.

we use different terms for the encapsulated form of the data that is described in the below-mentioned diagram.

| OSI Layers | TCP/IP Layers | Encapsulated Term |
|--------------|---------------|-------------------|
| Application | Application | Data |
| Presentation | | Data |
| Session | | Data |
| Transport | Transport | Segment |
| Network | Internet | Packet |
| Data-Link | Data-Link | Frame |
| Physical | Physical | Bits |

Encapsulated Data Term(OSI & TCP/IP Model)

the whole process of encapsulation and de-encapsulation in the OSI and TCP/IP model

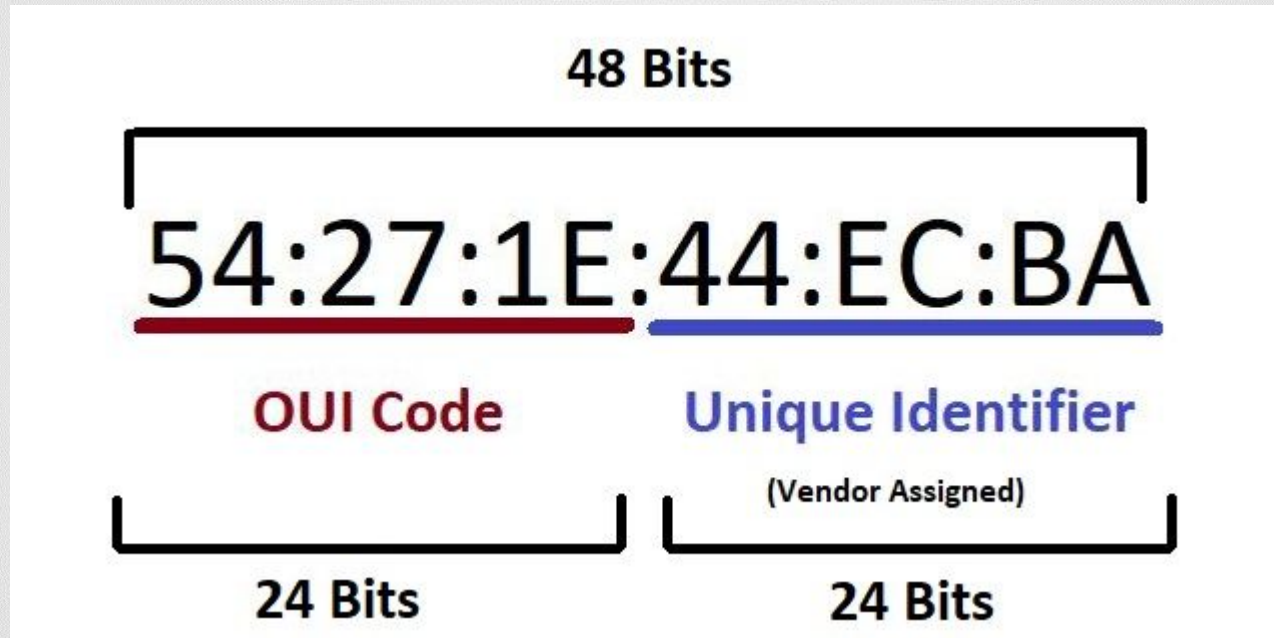


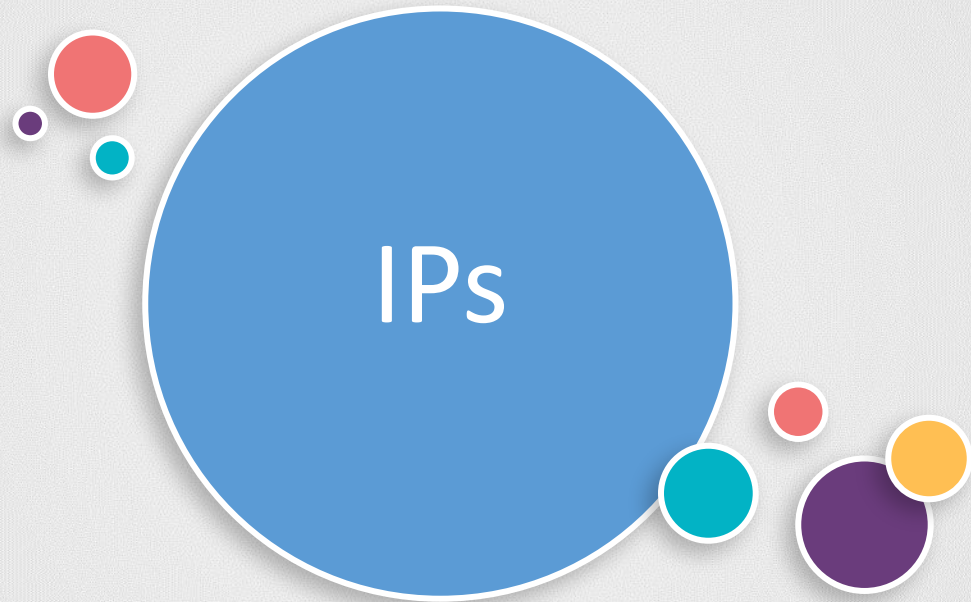


MAC
Address

A MAC address is a unique hardware identification number, but you can usually change the address in software.

Each network interface connected to your network — whether it's your router, wireless device, or network card in your computer — has a unique MAC address.

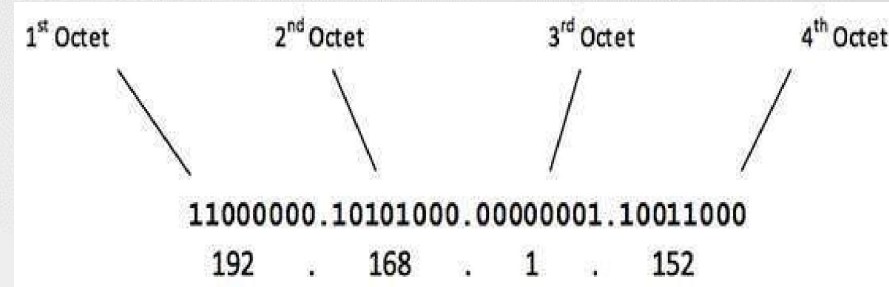




IPv4

IP stands for Internet Protocol. This address is used to identify a device on the internet or even a local network. It also helps you to develop a virtual connection between a destination and a source.

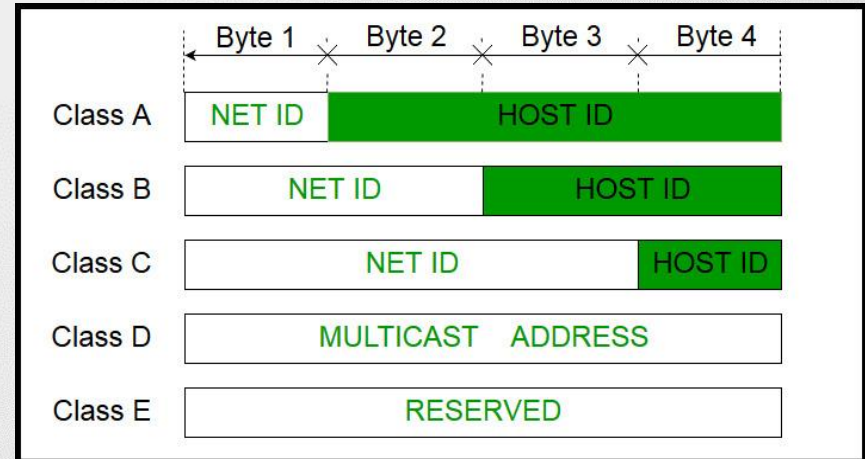
Each IP address in IPv4 are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses.



IP Address is divided into two parts:

Prefix (Network Address): identifies the physical network to which the computer is attached.

Suffix (Host Address): identifies the individual computer on the network.

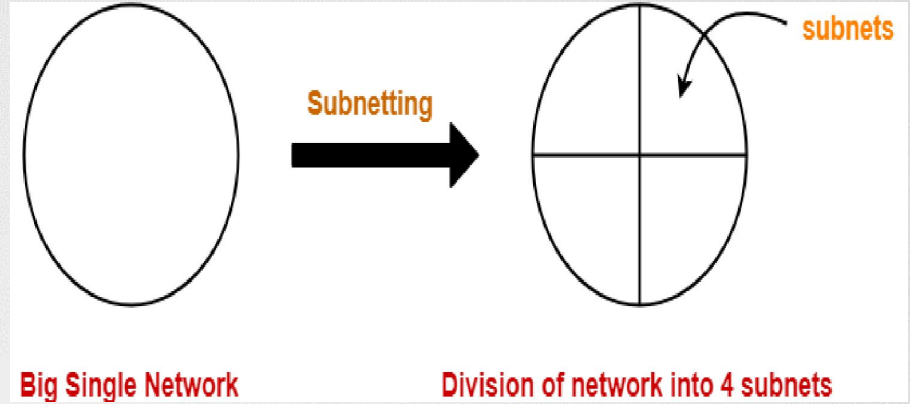


The table below shows the network classes:

| IP ADDRESS CLASS | IP RANGE START | IP RANGE END |
|------------------|----------------|-----------------|
| A | 0.0.0.0 | 127.255.255.255 |
| B | 128.0.0.0 | 191.255.255.255 |
| C | 192.0.0.0 | 223.255.255.255 |
| D | 224.0.0.0 | 239.255.255.255 |
| E | 240.0.0.0 | 255.255.255.255 |

Subnetting

It is the technique for logically partitioning a single physical network into multiple smaller sub-networks or subnets.



Subnet Mask

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address.

[illegible]

Slash Notation

| Network Mask | Slash Equivalent |
|-----------------|------------------|
| 255.0.0.0 | /8 |
| 255.255.0.0 | /16 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |
| 255.255.255.254 | /31 |
| 255.255.255.255 | /32 |

IPv6

IPv6 address is made of 128 bits divided into eight 16-bits groups.

128-Bits

1st group 2nd group 3rd group 4th group 5th group 6th group 7th group 8th group

2001:4860:4860:0000:0000:0000:0000:8844

16-bits

8 Groups

Types of IP addresses

1- Static IP Address

A static IP address is simply an address that doesn't change. Once your device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes.

2- Dynamic IP Address

Dynamic IP addresses are subject to change. Dynamic addresses are assigned by DHCP servers.

DHCP (Dynamic Host Configuration Protocol)

It's a network management protocol used on Internet Protocol networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client–server architecture.

DHCP Client vs DHCP Server

DHCP client is anything needing an IP address that is not configured as a static. So a phone, computer, Smart TV, etc., all need IP addresses.

DHCP server is the one responsible for handing out these IPs to the clients. The server tracks how many addresses it has available in its pool and who it has handed these out to via MAC so that it doesn't hand out duplicates.

Example: Your home router is a DHCP server and a client. That is because it has two network interfaces: The WAN interface and the LAN interface. On the LAN interface it acts as the server handing out IPs to clients on your LAN. But on its WAN interface it acts as a client and requests an IP from your ISP.

Public IP Address vs Private IP Address

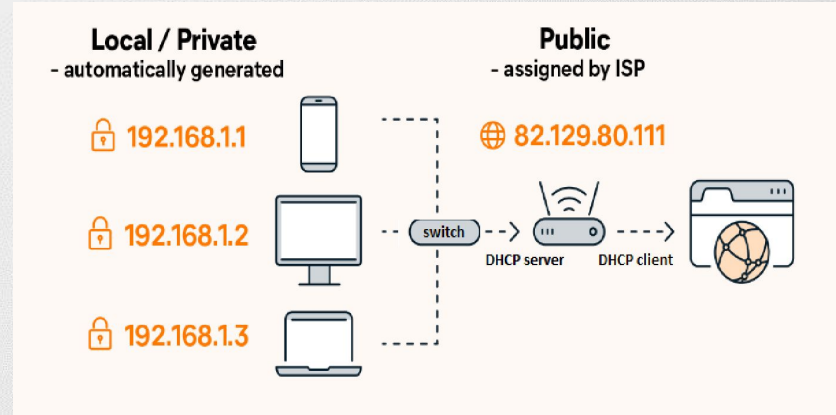
A private IP address is used within a private network to connect securely to other devices within that same network.

A public IP address identifies you to the wider internet so that all the information you're searching for can find you.

Public IP Range: Any number not included in the reserved private IP address range. E.g, 8.8.8.8.

| Class | Range | Subnet Mask |
|-------|-------------------------------|------------------|
| A | 10.0.0.0 — 10.255.255.255 | 255.0.0.0 (8) |
| B | 172.16.0.0 — 172.31.255.255 | 255.240.0.0 (12) |
| C | 192.168.0.0 — 192.168.255.255 | 255.255.0.0 (16) |

Reserved private IP address range





Ports & Protocols

What is a port?

A port is a virtual point where network connections start and end.

Each port is associated with a specific process or service.

Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

Are ports part of the network layer?

Ports are a transport layer (layer 4) concept.

Only a transport protocol such as the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) can indicate which port a packet should go to.

There are 65,535 possible port numbers, although not all are in common use.

What Is a Network Protocol, and How Does It Work



A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols.

Some of the protocols :

ARP (Address Resolution Protocol) – used to associate an IP address with a MAC address.

IP (Internet Protocol) – used to deliver packets from the source host to the destination host based on the IP addresses.

ICMP (Internet Control Message Protocol) – used to detect and report network error conditions. Used in ping.

TCP (Transmission Control Protocol) – a connection-oriented protocol that enables reliable data transfer between two computers.

UDP (User Datagram Protocol) – a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.

Telnet (Telecommunications Network) – used to connect and issue commands on a remote computer.

Some of the most commonly used ports, along with their associated networking protocol, are:

Ports **20** and **21**: File Transfer Protocol (FTP). **FTP** is for transferring files between a client and a server.

Port **22**: Secure Shell (SSH). **SSH** is one of many tunneling protocols that create secure network connections.

Port **25**: Simple Mail Transfer Protocol (SMTP). **SMTP** is used for email.

Port 53: Domain Name System (DNS). **DNS** helps Internet users and network devices discover websites using human-readable hostnames, instead of numeric IP addresses.

Port 80: Hypertext Transfer Protocol (HTTP). **HTTP** used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Port 443: HTTP Secure (HTTPS). **HTTPS** is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port.

THANK YOU

