

---

---

# Networking Fundamentals

Instructor: **Haris Chughtai** ([Linkedin](#))  
[dc.expert123@gmail.com](mailto:dc.expert123@gmail.com)

---

---

*Course developed & delivered by Haris Chughtai ([dc.expert123@gmail.com](mailto:dc.expert123@gmail.com))*

# Networking Fundamental

## Course Content

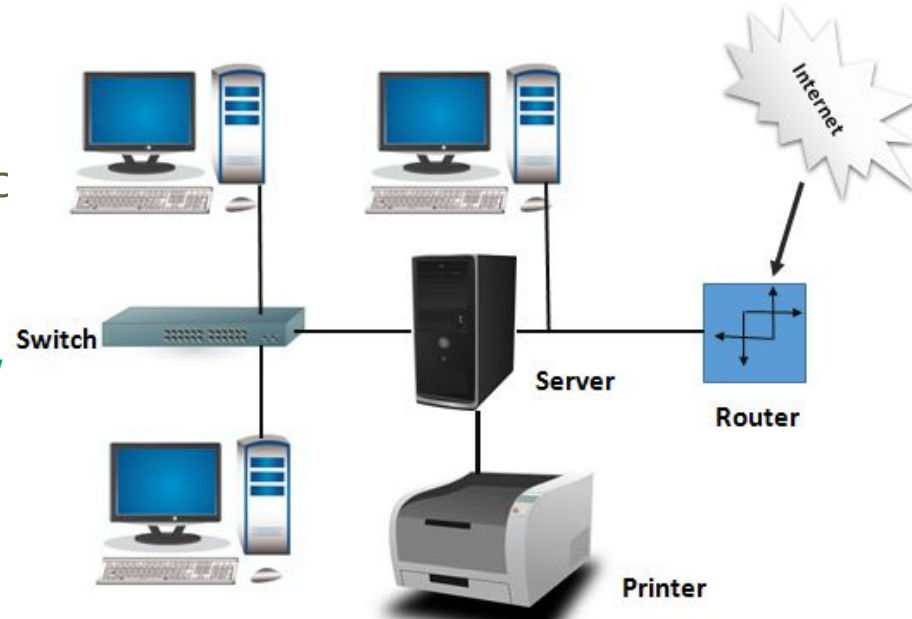
- **Networking Fundamentals**
  - What are computer networks?
  - Layer-2 MAC Addresses
  - Layer-3 IP Addressing & Classes (A, B, C)
  - Types of Networks (LAN, CAN, MAN, WAN)
  - OSI & TCP/IP Reference Models
  - Understanding each layer of TCP/IP Model
  - Typical Network Devices (Switch, Router, AP)
  - Common Network Services (DHCP, DNS, NAT, SNMP, NTP, HTTP, etc)
  - Typical Home Network Design
  - Typical Organization's Network Design
  - What's next - how to move forward to begin your career?

# UNDERSTANDING NETWORKS



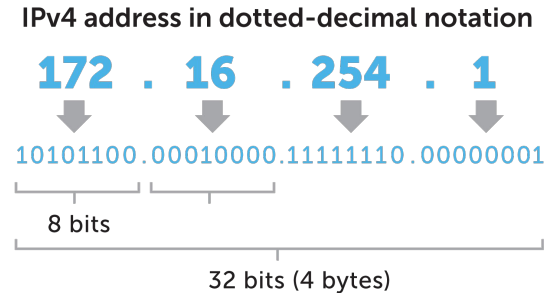
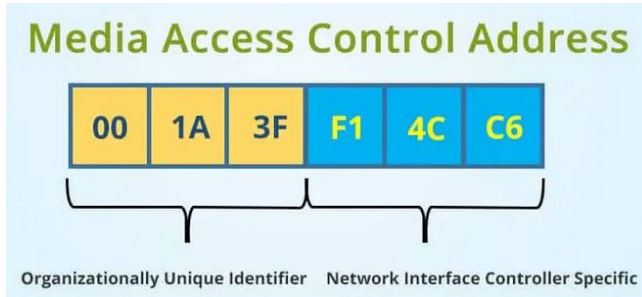
# What are Computer Network (or Communication Networks)

- A computer network is a group of interconnected nodes or computing devices that exchange data and resources with each other.
- <https://www.youtube.com/watch?v=WexBQ1XgaDw>



# MAC & IP Addresses

- The **MAC address - Media Access Control address** is a unique identifier assigned to a NIC (Network interface controller/Card). MAC Address is also known as the Physical Address of a network device. MAC address is a unique identifier assigned to a NIC (Network interface controller/Card). MAC Address is also known as the Physical Address of a network device
- An **IP address** is a unique address that identifies a device on the internet or a local network
- The primary distinction between MAC and IP addresses is that MAC addresses are used to verify the computer's physical address. It uniquely identifies the network's devices. While IP addresses are logical & used to uniquely identify a device's network connection.

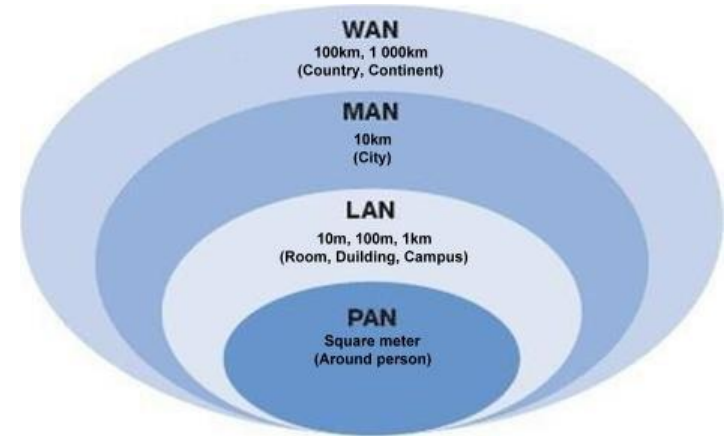
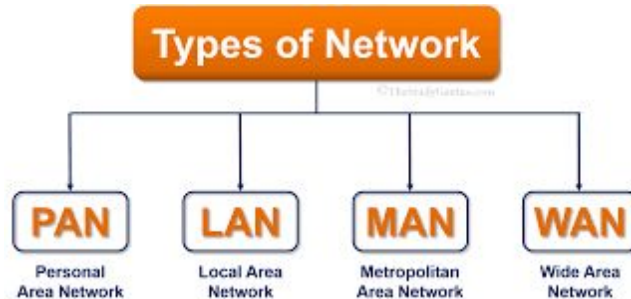


[https://www.youtube.com/watch?v=\\_SxUIR6L-pk](https://www.youtube.com/watch?v=_SxUIR6L-pk)

# NETWORK TYPES & COMPONENTS

# Types of Networks

- Most important aspect of any network is to provide connectivity from point-A to point-B
- Depending on their geographic proximity network can be categorized as PAN, LAN, WAN, and WLAN (Wireless LAN)
- Commonly used terms in the industry are **LAN, WLAN & WAN**
- Common WAN technologies are **MPLS & SDWAN**





[https://www.youtube.com/watch?v=4\\_zSIXb7tLQ](https://www.youtube.com/watch?v=4_zSIXb7tLQ)

*Course developed & delivered by Haris Chughtai (dc.expert123@gmail.com)*

# Networking Components - Wired/Wireless

- Computer networks could be wired or wireless or both type of devices
  - Wired /Cabled - Fiber or Copper
  - Wireless - WiFi, 4G/5G, Satellite
- Typically organization's network consist of mix of Wired (copper & fiber) and Wireless (WiFi) devices

Comparison	 Wired Network	 Wireless Network
Speed	Higher	Lower, but advanced wireless technology makes it possible to achieve a speed equal to wired network
Installation	Complex and requires more time	Easy to install and requires less time
Mobility	Limited, network equipment should be connected to the network system	Not limited, can move freely within wireless network coverage
Bandwidth	Higher	Lower
Common Medium	Copper wires, fiber optic cables	EM waves, radiowaves, infrared waves
Interference	Less	More
Reliability and Security	Reliable and secure with years of development, provide high-performance network	Less Reliable and the failure of router can affect the whole network



# Networking Components - Devices

- Commonly used devices in modern networks are **Wireless APs, Switches, Routers & Firewalls**
- Firewall is mainly a security device to protect network from cyber attacks
- In smaller networks, multiple network device functionalities can be combined into one device e.g. Home Internet modem combines AP, Switch, Router functionalities into one!

<https://www.youtube.com/watch?v=eMamgWlIRFY>

# Common Networking Devices

## ROUTERS

A router is a device that connects two or more networks. E.g. connecting your home network to Internet.

Think of a router as an air traffic controller and data packets as aircraft headed to different airports (or networks).

**Routers function on layer-3  
Network/Internet layer.**



## ACCESS POINTS

An Access Point (AP) or Wireless Access Point (WAP) is a networking device that creates a wireless local area network (WLAN) usually in home, office or large building to allows wireless-capable devices to connect to a wired network. AP connects to a wired router, switch, or hub via an Ethernet cable, and projects a WiFi signal to a designated area.

**APs typically function on layer-2 data  
link/Network Access layer.**



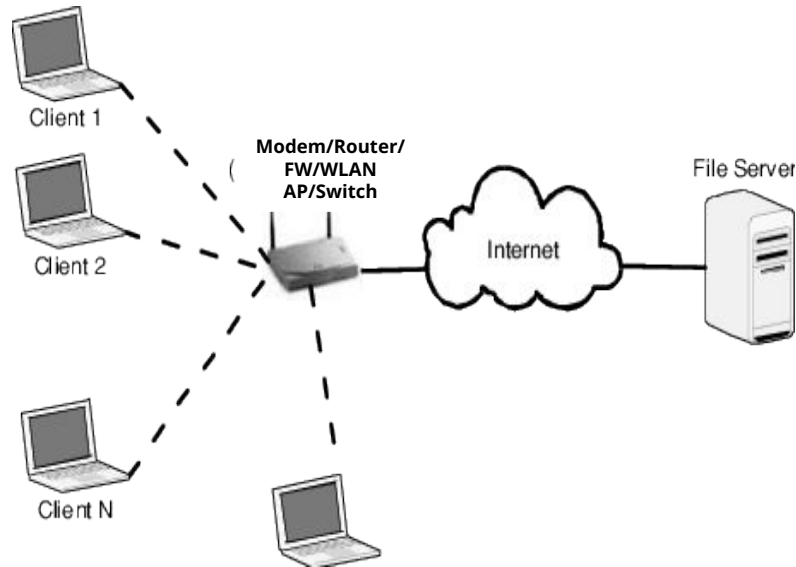
## SWITCHES

A network switch connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.

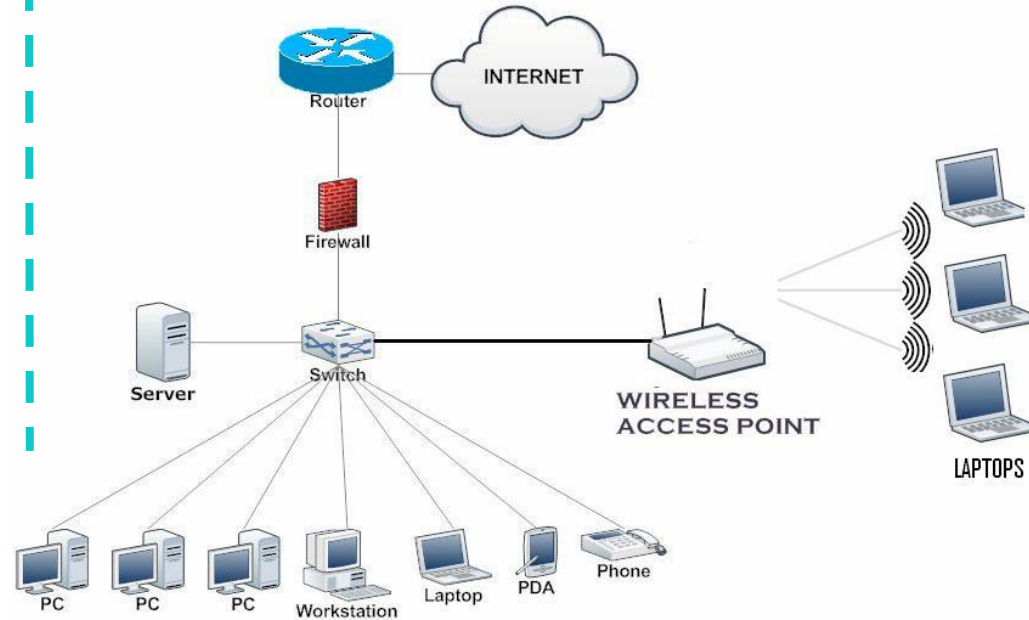
**Switches function on layer-2 data  
link/Network Access layer.**



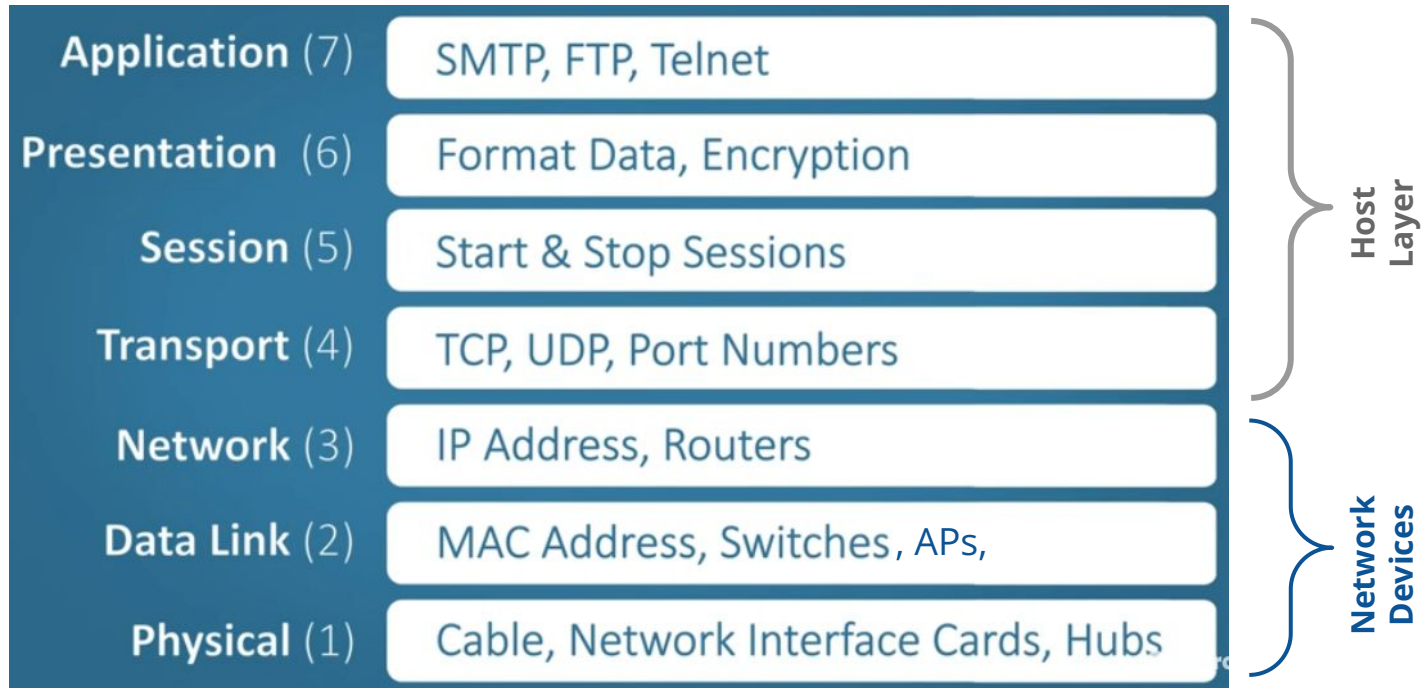
## Typical Home Network



## Typical Organization's Network



# Networking Devices Positioning in OSI Model



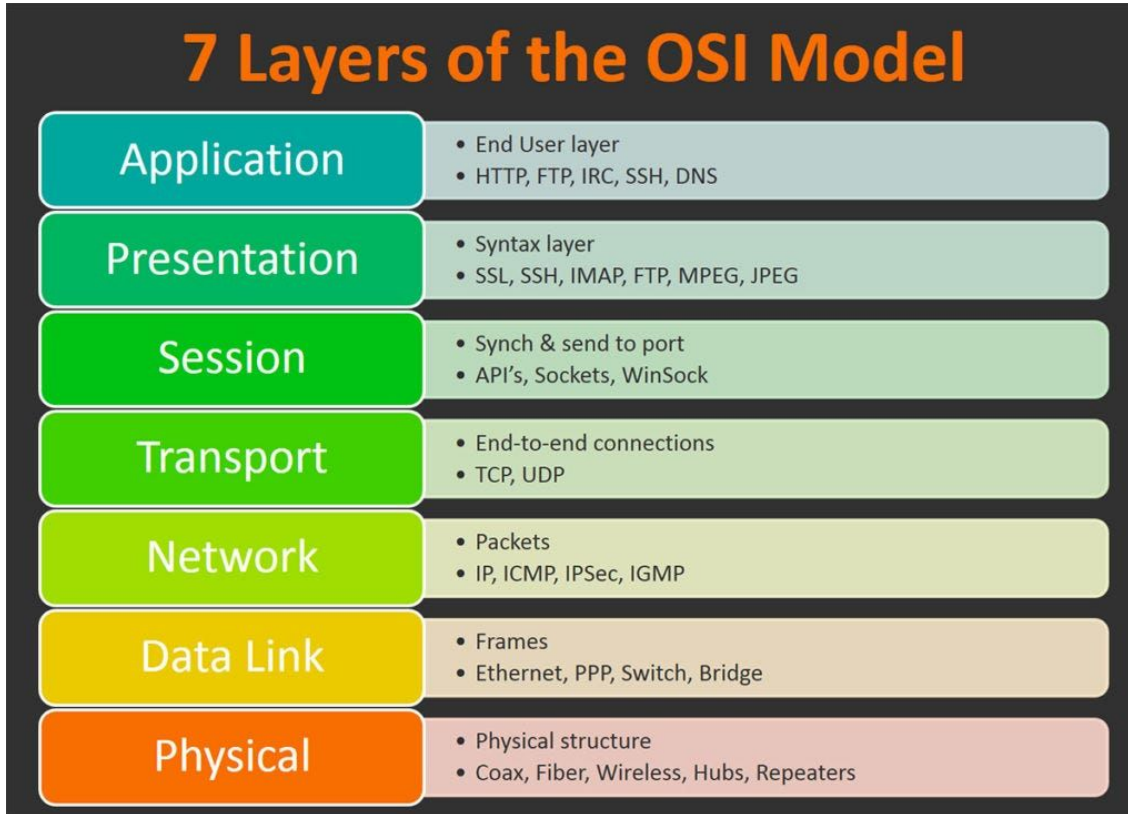
**Firewalls** commonly work on layer 3-4 (Network & Transport) however advanced firewalls are capable of providing layer 4-7 protection

# OSI & TCP/IP MODEL

- The OSI/ISO and TCP/IP models serve as fundamental frameworks for understanding network communication and data transfer. While the OSI model provides a comprehensive reference for communication between systems, TCP/IP forms the backbone of the internet
- In this section we will study Networking reference frameworks (OSI & TCP/IP models) that facilitate communication between devices in a network

# OSI Reference Model

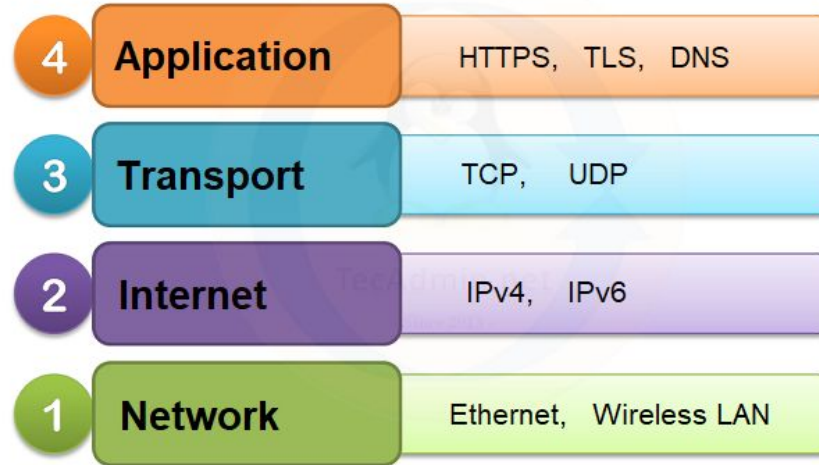
## 7 Layers of the OSI Model



The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes **computing functions into a universal set of rules and requirements in order to support interoperability between different products and software**. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers.

# TCP/IP Reference Model

- TCP/IP model is the concise version of OSI model
- TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers
- The model is often referred to as the TCP/IP stack



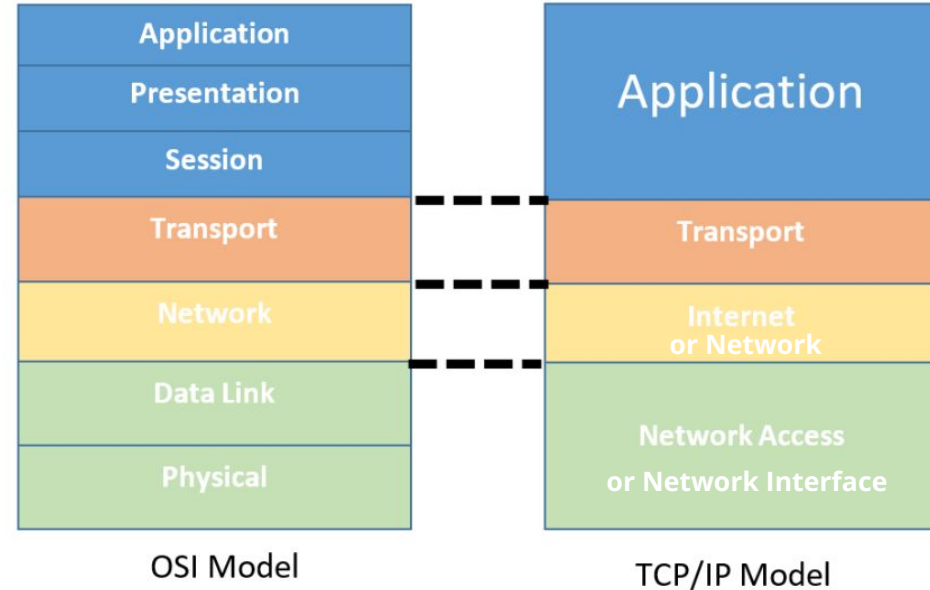
# TCP/IP Model Evolution

- The OSI reference model was the first communication model and was termed as general-purpose model because of its ability to fit in any type of network but without fitting the protocols in. Due to its inability to fit protocols, TCP/IP reference model which is commonly known as Internet Model was developed in year 1983 by US Military Wing called ARPANET.
- **In 1983 January 1, TCP/IP was made active permanently for the commercial use. From then, TCP/IP has made a revolution in the field of networking and telecommunication as it was able to overcome the drawbacks of general purpose OSI Model.**
- **TCP/IP stands for Transmission Control Protocol Internet Protocol**, with the help of which, protocol implementation over the network can be achieved.
- The TCP/IP model also has a layered architecture which allows easy data communication along with the facility of integrating multiple protocols. The layout remains similar to OSI Model but the number of layer, their functionalities and properties got changed.
- This Internet Model (TCP/IP) comprises of only four layers as compared to seven layers of OSI Model. These four layers are generated by combining the layers of OSI model internally so that protocols can be implemented. These layers have fixed positions too and their positions cannot be altered.



# 7-Layer OSI vs 4-Layer TCP/IP

- OSI - 7 Layer Model
  - The open systems interconnection (OSI) model is a conceptual framework used to describe the **flow of information from one computing device to another** operating in a networking environment. It is protocol independent.
- TCP/IP - 4 Layer Model
  - Simplified version of OSI model.
  - Provides a communication protocols suite using which **network devices can be connected to the Internet**. It relies on standardized protocols



## What's the difference between two models?

TCP/IP is a practical model that addresses specific communication challenges and relies on standardized protocols. In contrast, OSI serves as a conceptual comprehensive, protocol-independent framework designed to encompass various network communication methods.

**TCP/IP model can be thought as the practical interpretation of the conceptual OSI model**

# Practical Example of Reference Model Application

- The OSI and TCP/IP models serve as fundamental frameworks for understanding network communication and data transfer. While the OSI model provides a comprehensive reference for communication between systems, **TCP/IP forms the backbone of the internet.**
- Now let's run through a **real world example** of network communication between two devices considering OSI model layers:
  - <https://www.youtube.com/watch?v=LANW3m7UgWs>

# TCP/IP MODEL

- TCP/IP model is the one upon which the internet communication is based on.
- In this section we will study the functionality provided by each layers of TCP/IP models.

# Commonly used Protocols in Each Layer of TCP/IP Model

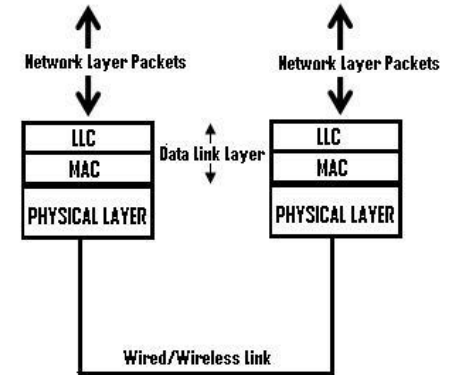
TCP/IP Layers	TCP/IP Protocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP Connection-oriented		UDP Connection-less		
Network Layer	IP IPv4 & IPv6	ARP	ICMP	IGMP	
Network Interface Layer	Ethernet (most commonly used)	Token Ring		Other Link-Layer Protocols	

Commonly  
used

# Network Interface (or Network Access) Layer

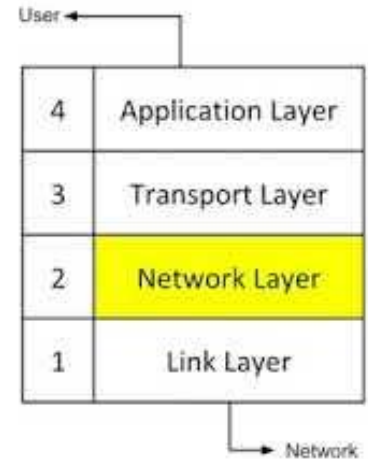
- The Network Access Layer is the lowest layer of the TCP/IP protocol hierarchy & it combines layers 1 (Physical) and 2 (Data link) of the OSI model.
- The protocols at this layer perform three distinct functions:
  - a. They define how to use the network to transmit a frame, which is the data unit passed across the physical connection.
  - b. They exchange data between the computer and the physical network.
  - c. They deliver data between two devices on the same network.
- **Ethernet has evolved as the industry's de-factor protocol for modern networks**
- Ethernet has two sub layers:
  - a. **Media Access Control (MAC)** Sublayer :— MAC sublayer provides an interface with the network adapter.
  - b. **Logical Link Control (LLC)** Sublayer :— LLC sublayer is responsible for error-checking functions for frames delivered also responsible for managing links between communicating devices.

OSI Model	TCP/IP Stack
Data Link	Network Access/Link
Physical	



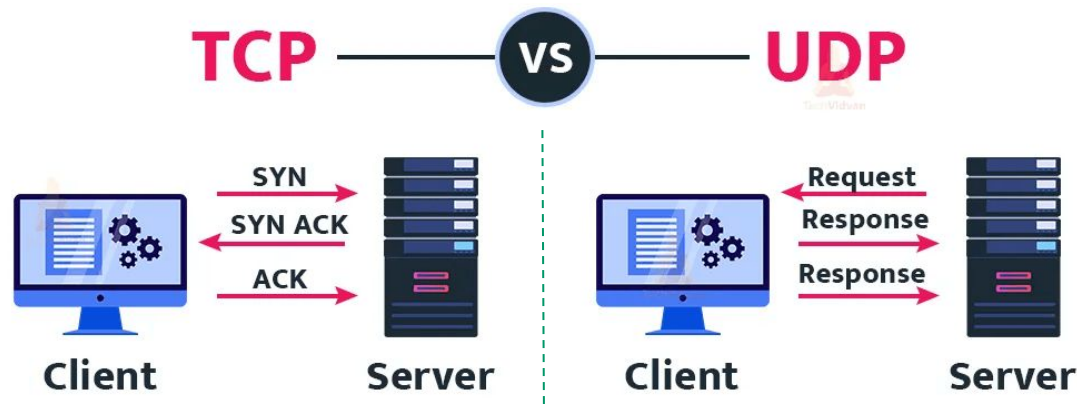
# Internet Layer (or Network Layer)

- The Internet layer (or network layer) is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame.
- The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.
- Common protocols used in Network/Internet layer are:
  - **IP**: Two types: **IPv4** - 32 Bits & **IPv6** - 128 Bits
  - **ARP** - Address Resolution Protocol (Provides MAC  $\longleftrightarrow$  IP mapping)
  - **ICMP** - Internet Control Message Protocol
    - Frequently used in network troubleshooting
  - **IGMP** - Internet Group Messaging Protocol
    - Commonly used for multicasting applications e.g. IPTV



# Transport Layer

- The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts.
- The two most important protocols in the Transport Layer are TCP & UDP:
  - a) **Transmission Control Protocol (TCP)** - Connection-oriented, TCP provides reliable data delivery service with end-to-end error detection and correction which is also **known as three-way-handshake**
  - b) **User Datagram Protocol (UDP)** - Connection-less, UDP provides low-overhead, connectionless datagram delivery service.



# APPLICATION LAYER

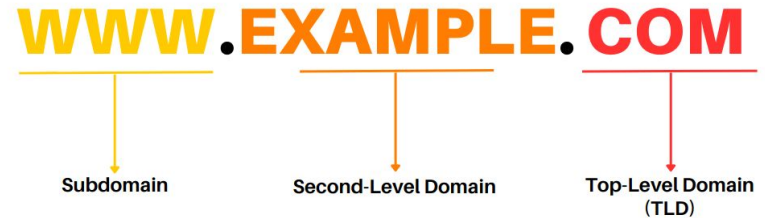
- Some of the commonly used network services/protocols used by Application layer include DNS, DHCP, NTP, SNMP, SMTP, NAT, NTP, FTP, TLS, TELNET HTTP etc



# DNS - Application Layer Network Services

- **DNS - Domain Name System:** A DNS server translates domain names that are easily understood and remembered by humans into the IP address of a remote application or server

```
hosts - Notepad
File Edit Format View Help
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com         # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
#      192.168.0.160    local.wahldev.com
#      192.168.0.160    beta.samastaonline.com
#      64.270.127.12     staging.thejakegroup.com
```



<https://www.youtube.com/watch?v=g6R9gRWIiK8>

# DHCP - Application Layer Network Services

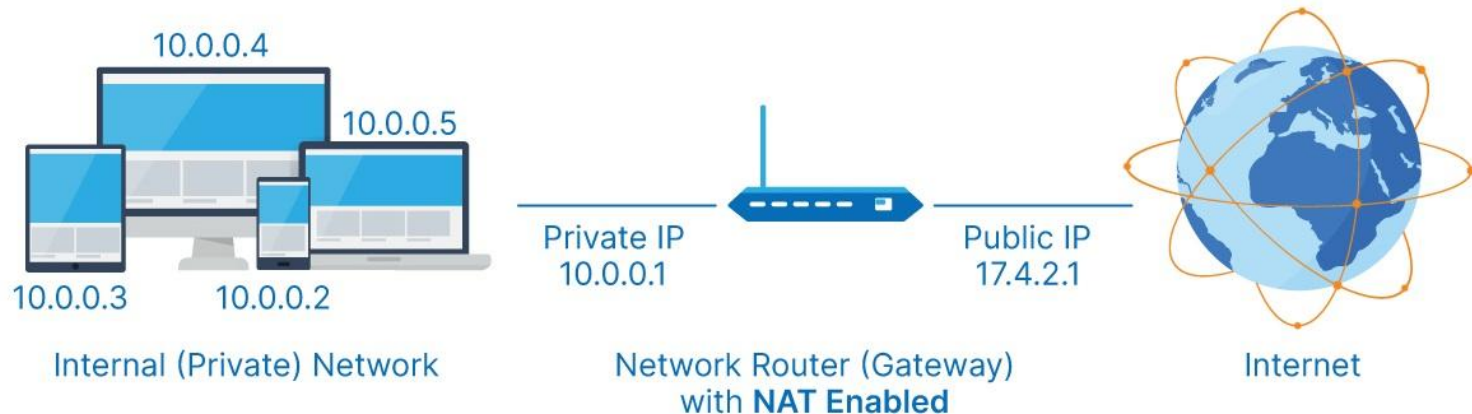
- **DHCP - Dynamic Host Configuration Protocol:** Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

<https://www.youtube.com/watch?v=kS42C3vqFco>



# NAT - Application Layer Network Services

- **NAT - Network Address Translation:** NAT stands for network address translation. It's a way of mapping an IP address space into another by modifying network address information in the IP header of packets
  - Typically it is used to map multiple private addresses inside a local network to a public IP address before transferring the information to the internet.

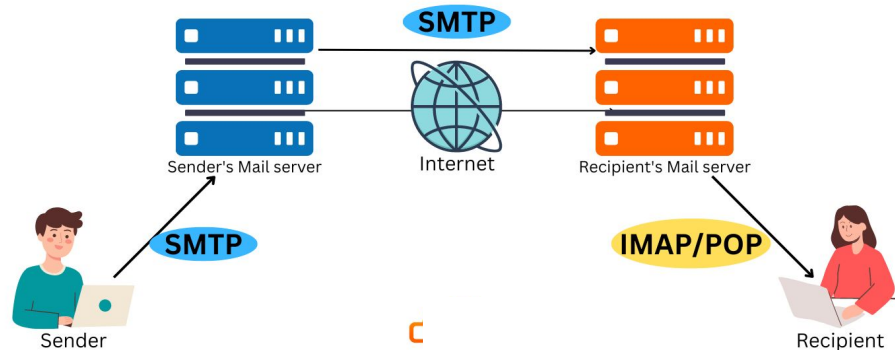


<https://www.youtube.com/watch?v=wE6hk2quigo>

# SMTP - Application Layer Network Services

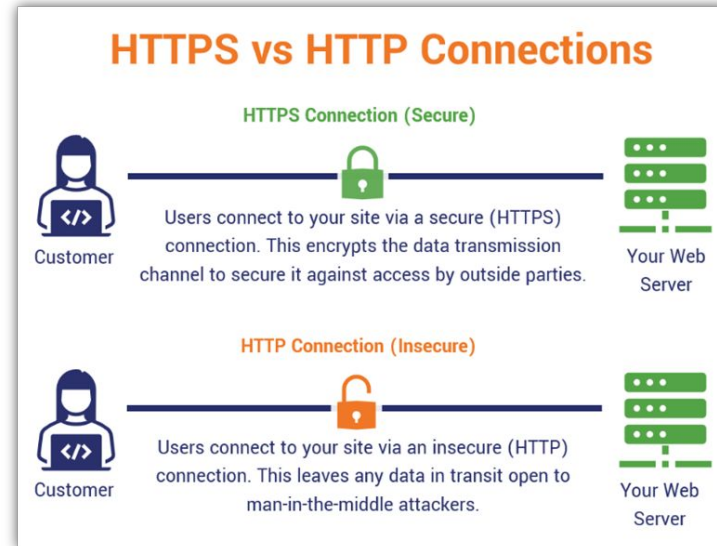
- **SMTP - Simple Mail Transfer Protocol:** The Simple Mail Transfer Protocol is an Internet standard communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages.
- With technology evolution, now most email clients typically use SMTP only for **sending out** messages to a mail server for relaying, and typically submit outgoing email to the mail server on port 587 or 465 per RFC 8314. For **receiving incoming** messages, IMAP (which replaced the older POP3) is becoming standard.
- Originally, the Simple Mail Transfer Protocol (SMTP) used TCP port 25. Today, SMTP should instead use port 587 — this is the port for encrypted email transmissions using SMTP Secure (**SMTPS**). Port 465 is also used sometimes for SMTPS. However, this is an outdated implementation and port 587 should be used if possible.

## SMTP (Simple Mail Transfer Protocol)



# HTTP - Application Layer Network Services

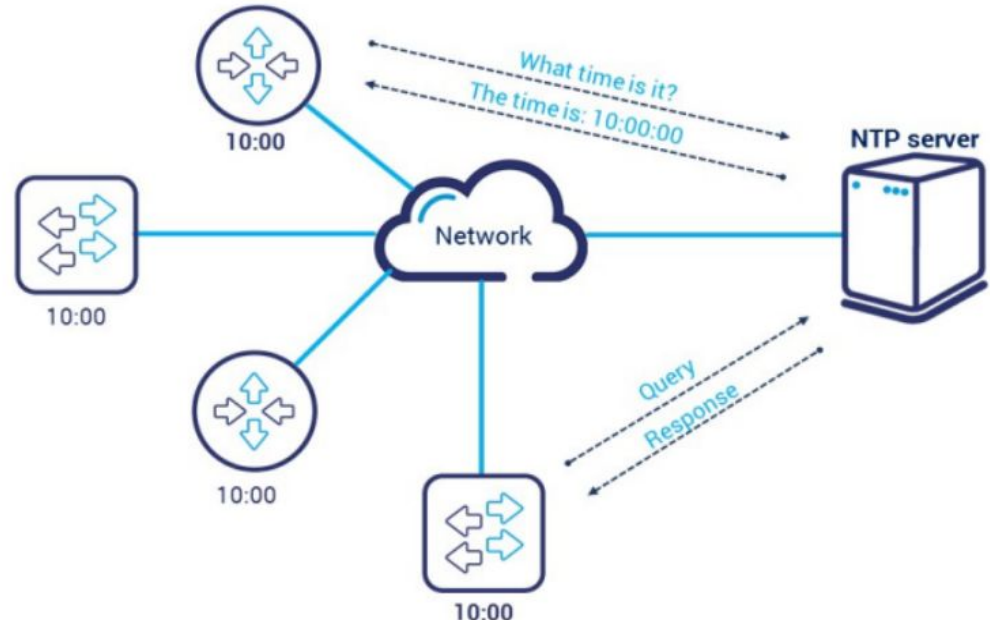
- **HTTP - Hypertext Transport Protocol:** The Hypertext Transfer Protocol (HTTP) is the foundation of the World Wide Web, and is used to load web pages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices.
- **HTTPS - Hypertext Transfer Protocol Secure** is an extension of the HTTP with encryption and verification. The only difference between the two protocols is that HTTPS uses TLS (previously SSL) to encrypt normal HTTP requests and responses, and to digitally sign those requests and responses. As a result, HTTPS is far more secure than HTTP.



<https://www.youtube.com/watch?v=w0QbnxKRD0w>

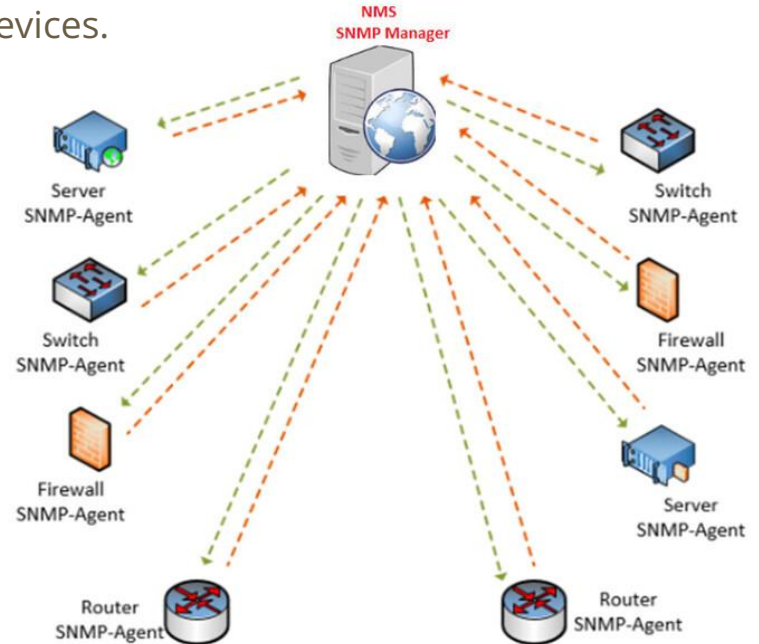
# NTP - Application Layer Network Services

- **NTP - Network Timing Protocol:** Network Time Protocol (NTP) is an internet protocol used to synchronize with computer clock time sources in a network. It belongs to and is one of the oldest parts of the TCP/IP suite. The term NTP applies to both the protocol and the client-server programs that run on computers.



# SNMP - Application Layer Network Services

- **SNMP - Simple Network Management Protocol:** Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP. SNMP is used for communication between routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices.



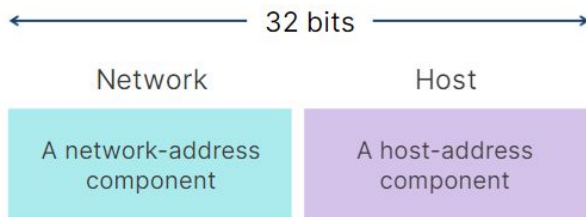
# IP ADDRESSING

- Most important aspect of any network is to provide connectivity from point-A to point-B



# Understanding IP Addressing

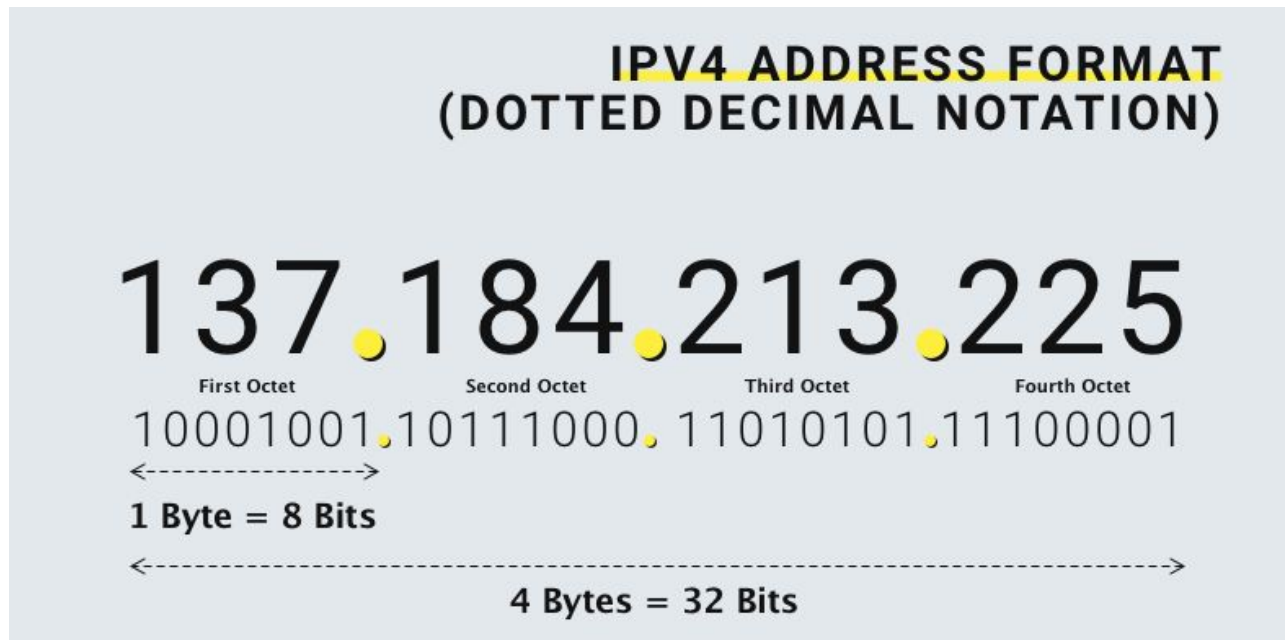
- IP is a Network/Internet Layer Protocol. It comes in two flavors of IPv4 & IPv6
- IPv6 - 128 Bits (advanced and futuristic)
- IPv4 - 32 Bits (old but commonly used however now deprecating)
  - 4 Octets of 8 bits each = 32 Bits (aka **dotted decimal notation**)
  - Divided into **Network** & **Host** Portion
  - Based on the Network & Host portion IP Addresses are categorized into four Classes - A, B, C, D, E
  - Class A, B, C are commonly used in the networks whereas Class D, E are special purpose address spac



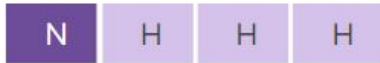
Class A	For governments
Class B	For medium-sized companies
Class C	For all other requestors
Class D	For multicasting
Class E	For research

<https://www.youtube.com/watch?v=eHV1aOnu7oM>

# IPv4 Address Format - Dotted Decimal Notation



## Class A



N = Network portion

H = Host portion

Class A addresses include:

Range of network numbers is  
0.0.0.0 through 127.255.255.255

Number of host addresses per  
major network = 16,777,214

## Class B



Class B addresses include:

Range of network numbers is  
128.0.0.0 through 191.255.255.255

Number of host addresses per  
major network = 65,534

## Class C



Class C addresses include:

Range of network numbers is  
192.0.0.0 through 223.255.255.255

Number of host addresses per  
major network = 254

# Four types of IP Addresses

**Public**

**Categories**

**Private**



**Static**

**Assignment**

**Dynamic**





## What's Next?

How to move further to  
being a new career?



# Gain Additional Networking Knowledge to make a career

## A. Start with Youtube Courses

- a. [Practical Networking - Networking Fundamentals Course](#) (15 videos - short & quick)
- b. [Network Direction Network Fundamental course](#) (28 videos - detailed)
- c. [Jeremy's IT Lab - Full CCNA Course](#) (118 videos - detailed)

## B. Enrich your Theoretical Concepts from other online material

- i. [Comptia Network+ Study Guide](#)
- ii. [CCNA Study Guide](#) Free
- iii. [CCNA Study Notes](#)
- iv. [Cisco Academy learning](#) Free courses

# Step by Step Guide to begin your Networking Career

- New to IT, you like Computer Networking but not sure how to move forward?
- Following my [8-steps guide](#) to begin your career journey

# Keep learning, keep growing

Learning is not attained by chance; it must be sought for with ardor and diligence."

– *Abigail Adams*



