Different networking devices:

What are network devices?

Network devices, or networking **hardware, are physical devices** that are required for communication and interaction between hardware on a computer network.

Types of network devices:

Here is the common network device list:

- **Repeater**
- **Bridge**
- **Hub**
- **Switch**
- **Router**
- **Gateway**

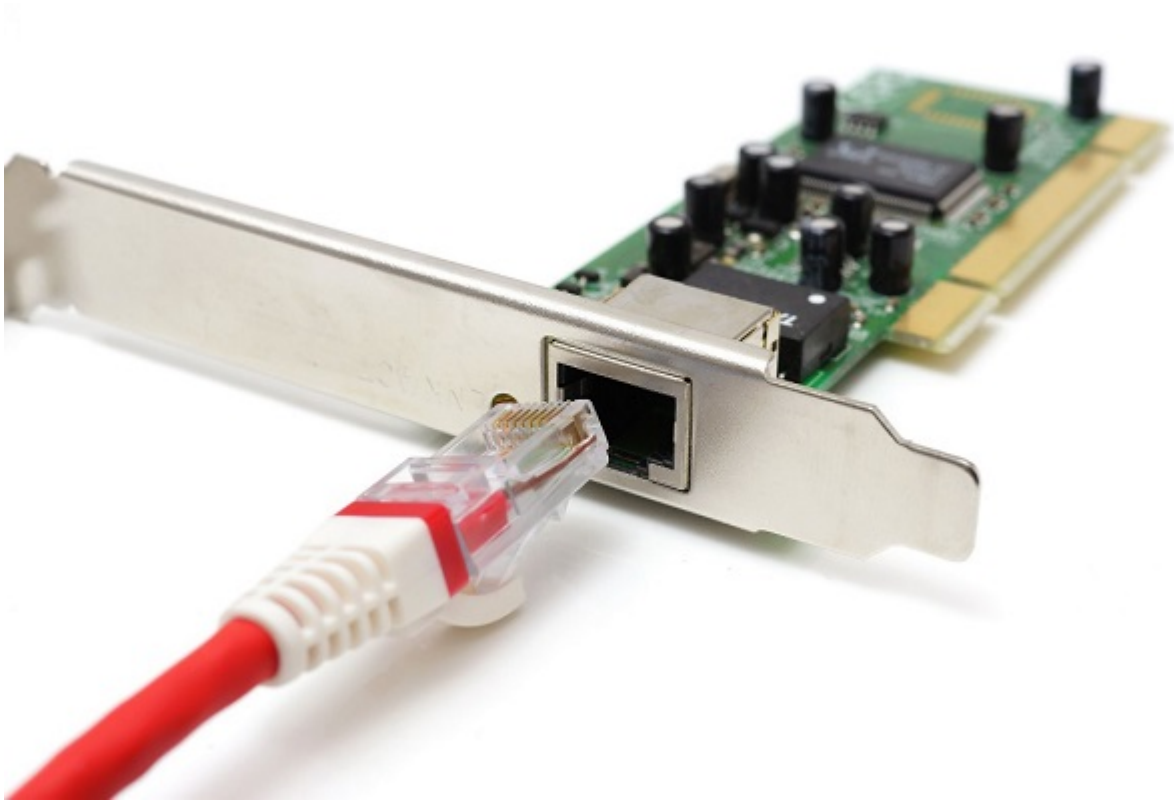
These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be **inter-network or intra-network**. Some devices are installed on the device, like **NIC card or RJ45 connector**, whereas some are part of the network, like router, switch, etc.

RJ45 Connector:

RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an **8-pin jack** used by devices to **physically connect to Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for **Ethernet LANs are twisted pair** ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

Ethernet Card:

Ethernet card, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and **communicate with other devices on the LAN**. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket** where network cable is physically plugged in.



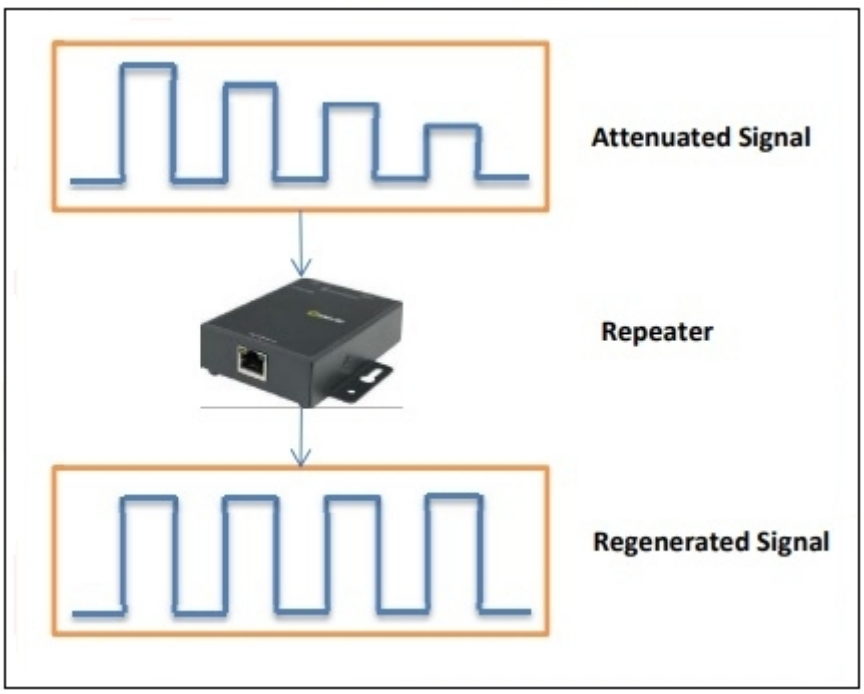
Ethernet card speeds may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of **10 Mbps**. However, modern cards support fast Ethernets up to a speed of **100 Mbps**. Some cards even have capacity of **1 Gbps**.

1. **Repeater** – A repeater operates at the **physical layer**. Its job is to **regenerate the signal** over the same network before the signal

becomes too weak or corrupted so as to extend the length to which the **signal can be transmitted over the same network**. An important point to be noted about repeaters is that they do **not amplify the signal**. **When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.** It is a **2 por**t device.

2. Repeaters remove the unwanted noise in an incoming signal. **It increases a signal's strength,** so **it can be transmitted and received over a greater distance without a loss in quality**. Network repeaters receive and retransmit incoming electrical, wireless or optical signals.
3. Whenever a repeater receives a signal through one of its ports, **it repeats or sends the incoming signal onto the other port.** Its main use is to amplify and regenerate signals.

Figure 14.19 Repeater



Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the **length of the LAN or coverage area of cellular networks**. This problem is alleviated by installing repeaters at certain intervals.

Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

- **Analog Repeaters** − They can only amplify the analog signal.
- **Digital Repeaters** − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

- **Wired Repeaters** − They are used in wired LANs.
- **Wireless Repeaters** − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

- **Local Repeaters** − They connect LAN segments separated by small distance.
- **Remote Repeaters** − They connect LANs that are far from each other.

Advantages of Repeaters

- Repeaters are simple to install and can easily extend the length or the coverage area of networks.
- They are cost effective.
- **Repeaters don't require any processing overhead**. The only time they need to be investigated is in case of degradation of performance.
- They can connect signals using different types of cables.

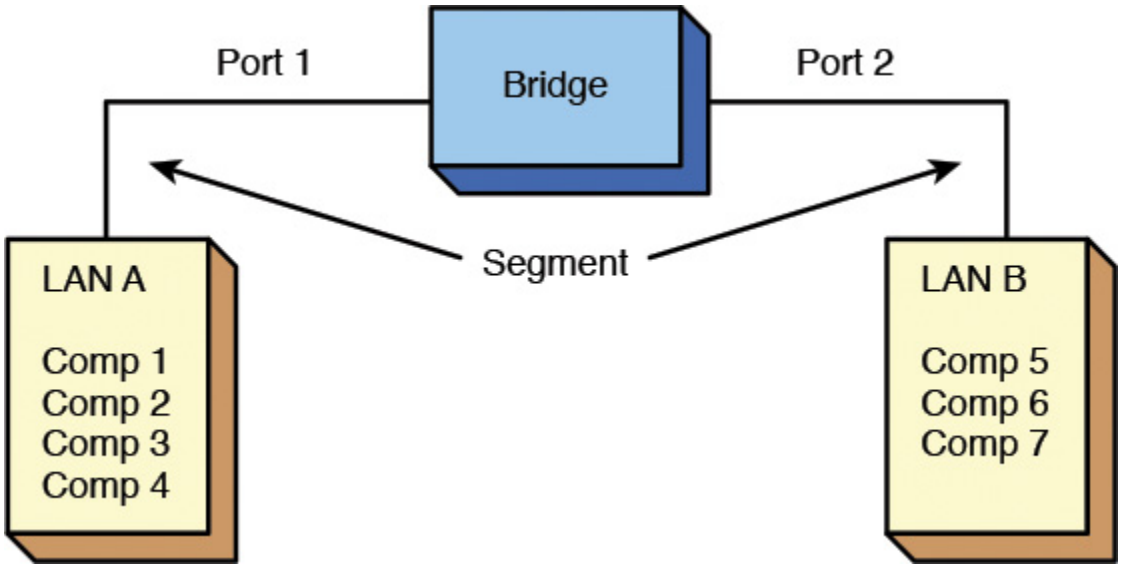
Disadvantages of Repeaters

- Repeaters **cannot connect dissimilar networks.**
- They **cannot differentiate** between actual signal and noise.
- They **cannot reduce network traffic** or congestion.

- Most networks have limitations upon the number of repeaters that can be deployed.

Bridge:

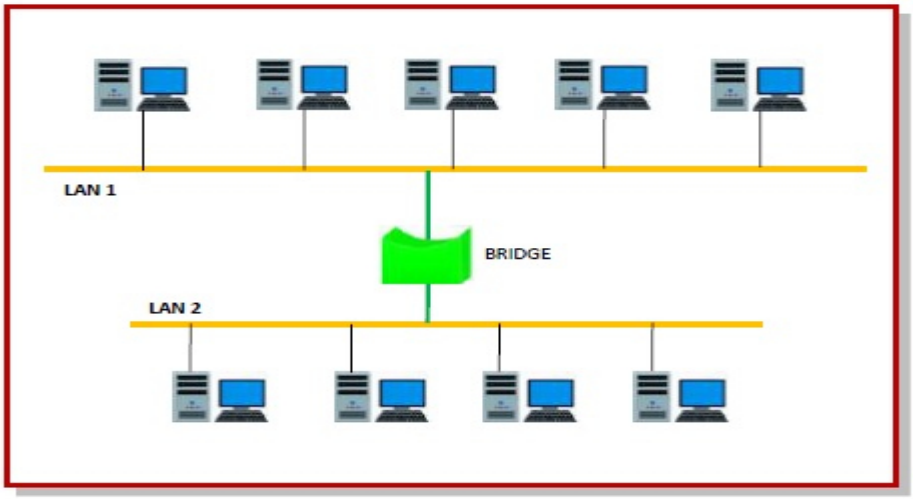
A bridge is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model. It interprets data in the **form of data frames**. In the physical layer, **the bridge acts as a Repeater which regenerates the weak signals,** while in the data-link layer, it checks the **MAC (Media Access Control)** address of the data frames for its transmission.



A bridge is a network device that **connects multiple LANs** (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network.

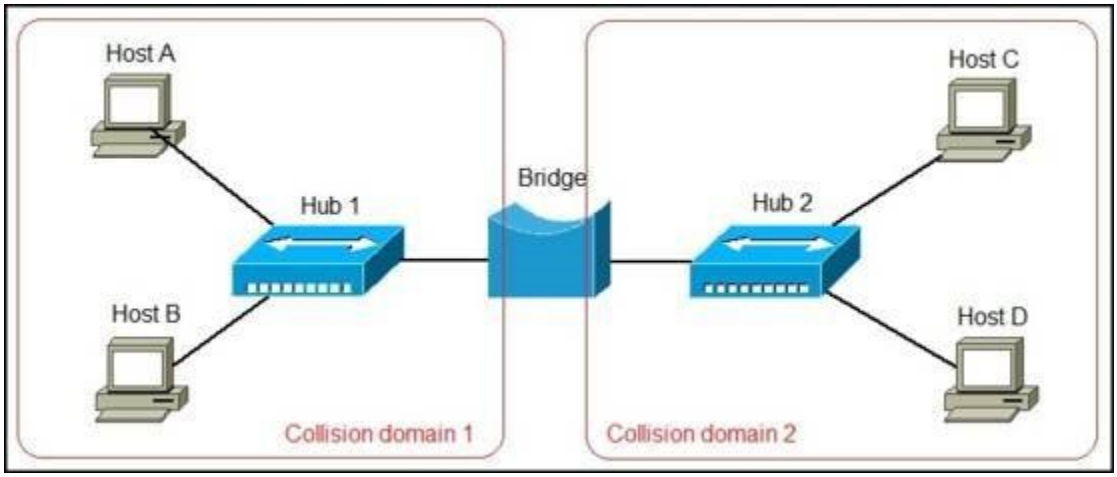
Bridges operate at the data link layer of the OSI model and hence also referred as **Layer 2 switches.**

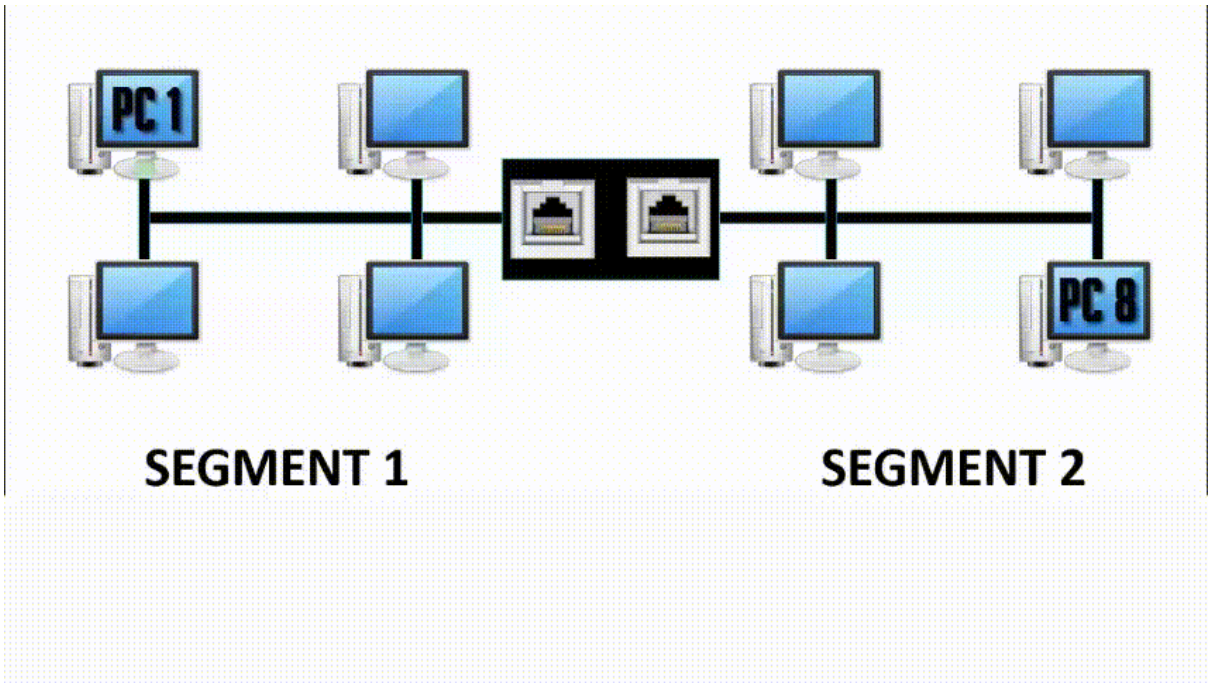
The following diagram shows a bridges connecting two LANs −



Uses of Bridge:

- **Bridges connects two or more different LANs** that has a **similar protocol** and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since **they operate at data link layer, they transmit data as data frames**. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
    - If the frame has a **destination MAC (media access control) address in the same network,** the bridge passes the frame to that node and then discards it.
    - If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the **destination MAC address is not available, bridges can broadcast data frames to each node**. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.





Functions of Bridges in Network:

The main functions of bridges in a computer network include the following.

- This networking device is used for **dividing local area networks into several segments.**
- In the **OSI model, it works under the data link layer**.
- It is used to store the address of MAC in PC used in a network and also used for diminishing the network traffic.

Advantages/Disadvantages of Bridge in Computer Network:

The advantages are

- It acts as a **repeater to extend a network**
- Network traffic on a segment can be reduced by subdividing it into network communications
- Collisions can be reduced.

- Bridges increase the available bandwidth to individual nodes because fewer network nodes share a collision domain
- It **avoids waste BW (bandwidth)**
- The length of the network can be increased.
- Connects different segments of network transmission

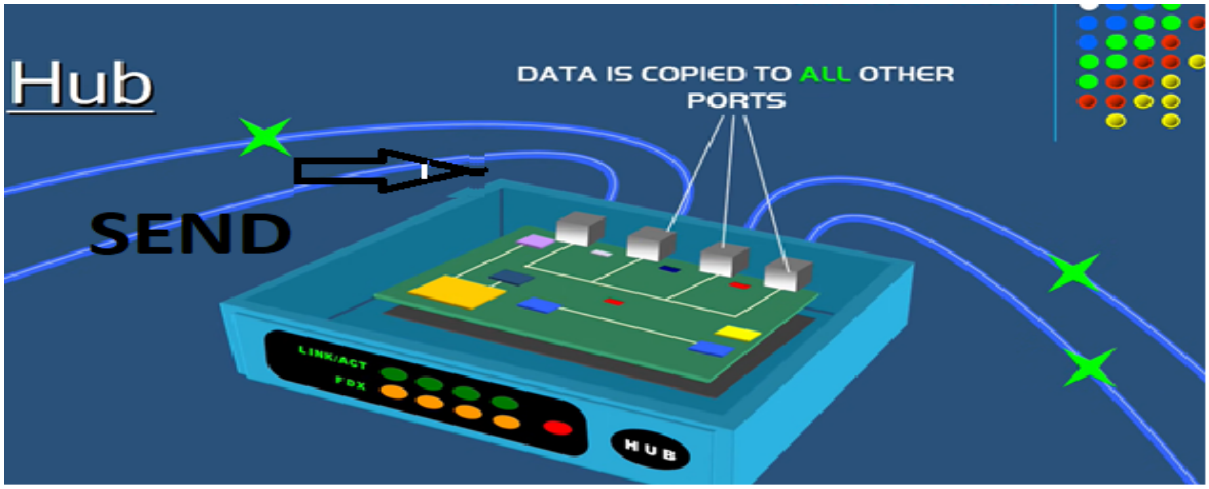
The disadvantages are

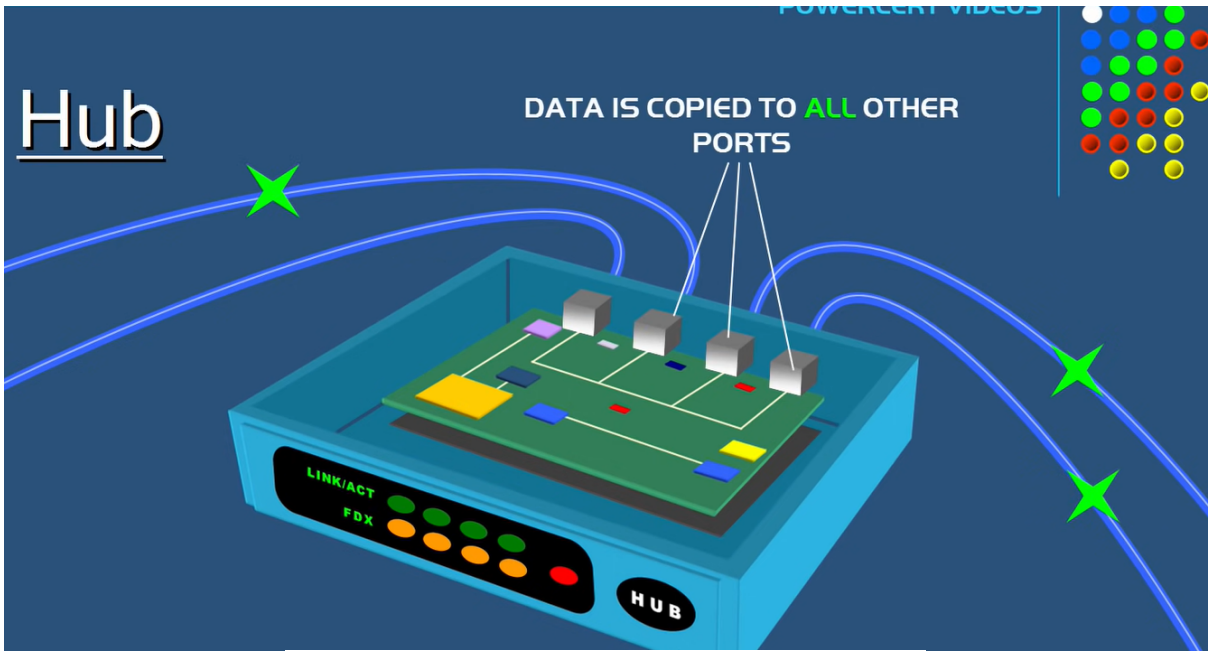
- It is unable to read specific IP addresses because they are more troubled with the MAC addresses.
- They cannot help while building the **network between the different architectures of networks.**
- It transfers all kinds of broadcast messages, so they are incapable to stop the scope of messages.
- These are expensive as we compare with repeaters
- **It doesn't handle more variable & complex data load** which occurs from WAN.

Hubs:

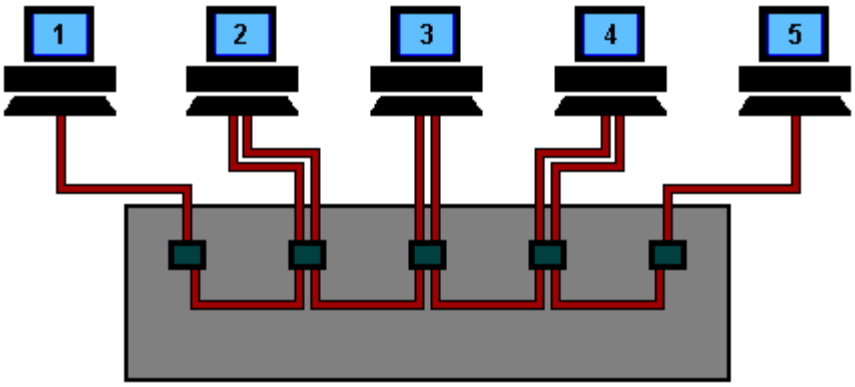
A hub is a **physical layer networking** device which is **used to connect multiple devices in a network**. They are generally used to connect computers in a LAN.

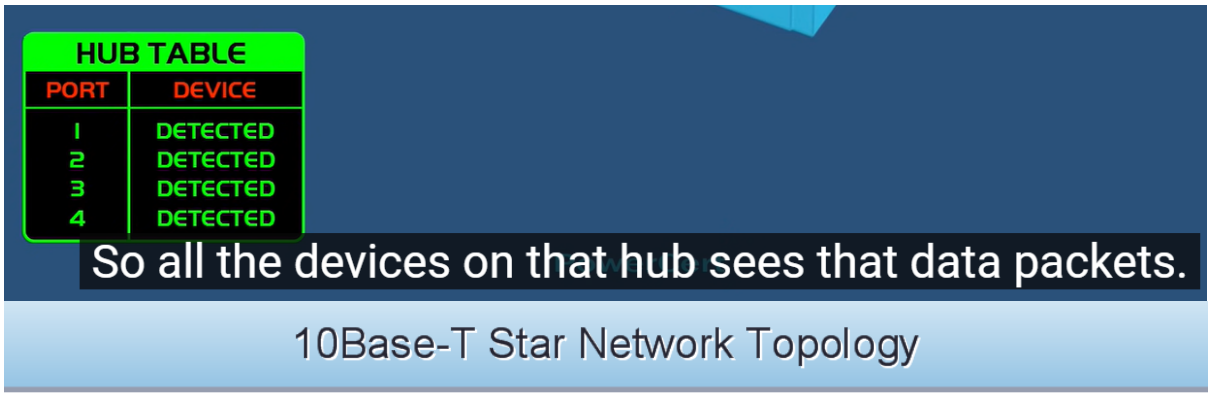
A hub **has many ports** in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a **data frame arrives at a port, it is broadcast to every other port**, without considering whether it is destined for a particular destination or not.

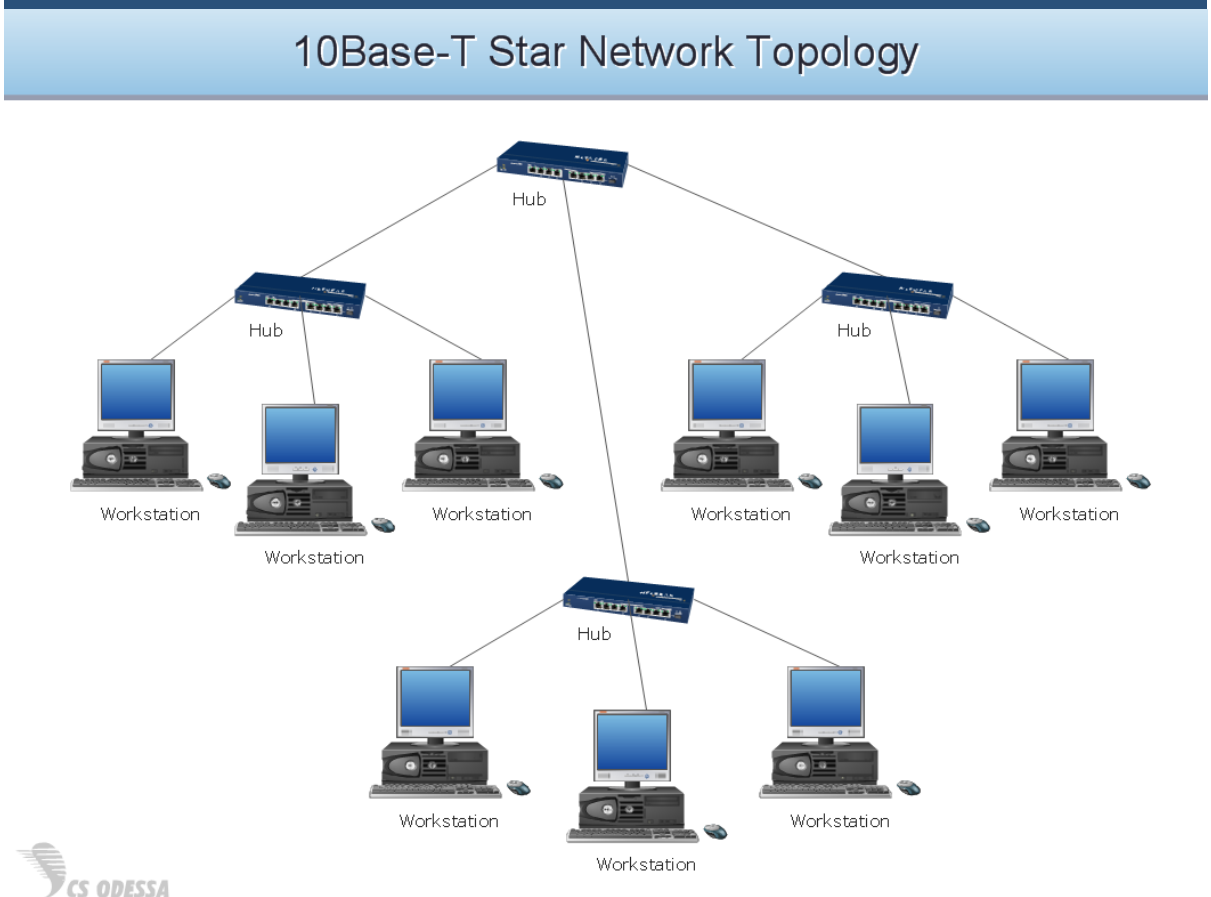

Hub
DATA IS COPIED TO ALL OTHER PORTS
SEND
LINK/ACT
FDX
HUB


Hub
DATA IS COPIED TO ALL OTHER PORTS
LINK/ACT
FDX
HUB


Hub







Applications of Hub

The important applications of a hub are given below:

- Hub is used to create small home networks.
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.
- It can be used to create a device that is available thought out of the network.

Advantages of Hub

- It provides support for different types of Network Media.
- It can be used by anyone as it is very cheap.
- It can easily connect many different media types.
- The use of a hub does not impact on the network performance.
- Additionally, it can expand the total distance of the network.

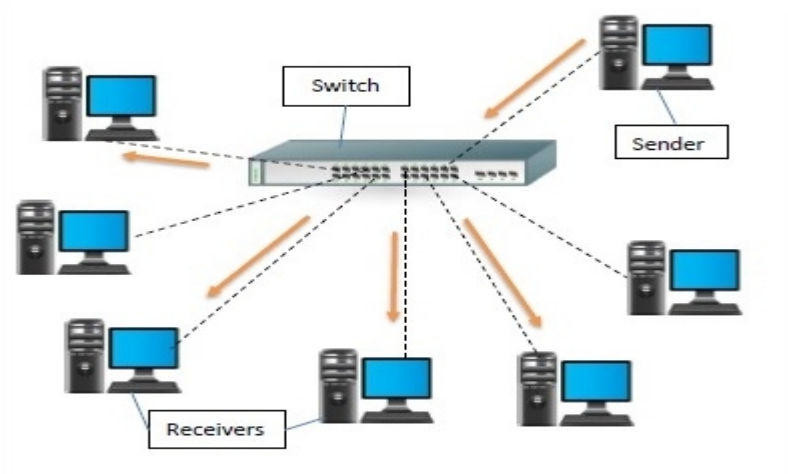
Disadvantages of Hub

- It has **no ability to choose the best path of the network**.
- It does not include mechanisms such as collision detection.
- It does not operate in full-duplex mode and cannot be divided into the Segment.
- It cannot reduce the network traffic as it has no mechanism.
- It is not able to filter the information as it transmits packets to all the connected segments.
- Furthermore, it is not capable of connecting various network architectures like a ring, token, and ethernet, and more.

Switches:

A switch is a **data link layer networking** device which connects devices in a network and uses packet switching to send and receive data over the network.

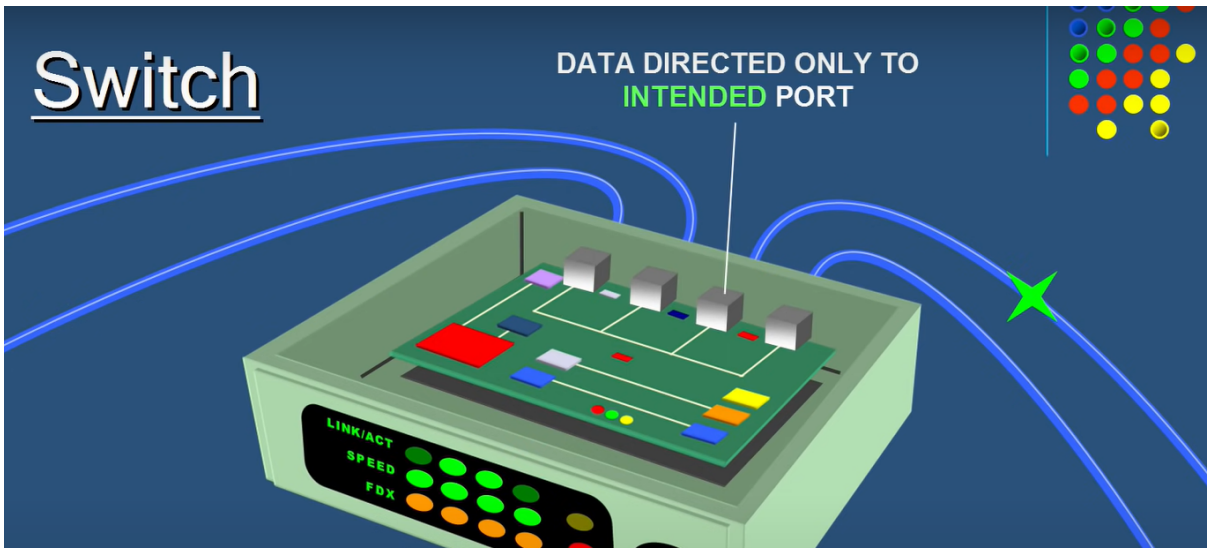
Like a hub, a switch also has many ports, to which computers are plugged in. However, when a **data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s)**. Thus, it supports both **unicast and multicast** communications.

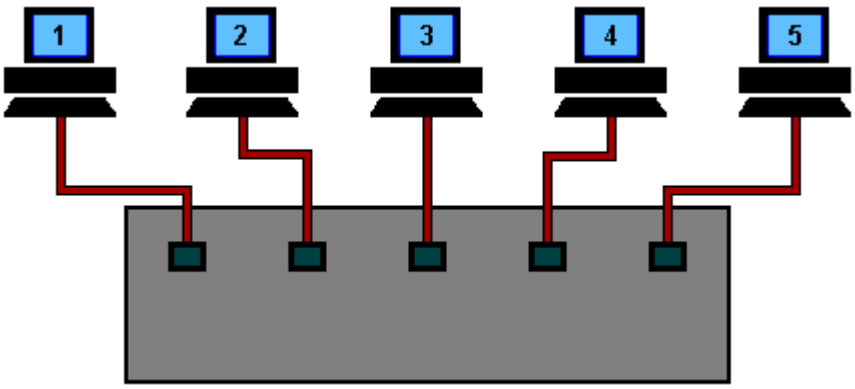


Features of Switch:

Here, are important features of switch:

- It is Datalink layer device (Layer 2)
- It works with fixed bandwidth
- It maintains a MAC address table
- Allows you to create virtual LAN
- It works as a multi-port bridge
- Mostly comes with 24 to 48 ports
- Supports half and full-duplex transmission modes





SWITCH TABLE		
PORT	DEVICE	MAC ADDRESS
1	DETECTED	00-04-5A-63-A1-66
2	DETECTED	90-02-7B-C2-C0-67
3	DETECTED	32-07-9A-92-A2-00
4	DETECTED	72-00-FA-63-A9-66

Advantages of Switch:

Here, are pros/benefits of using Switch

- It helps you to reduce the number of broadcast domains.
- Supports VLAN's that can help in Logical segmentation of ports
- Switches can make use of CAM table for Port to MAC mapping

Disadvantages of Switch:

Here, are cons/drawbacks of using Switch:

- Not as good as a router for limiting Broadcasts

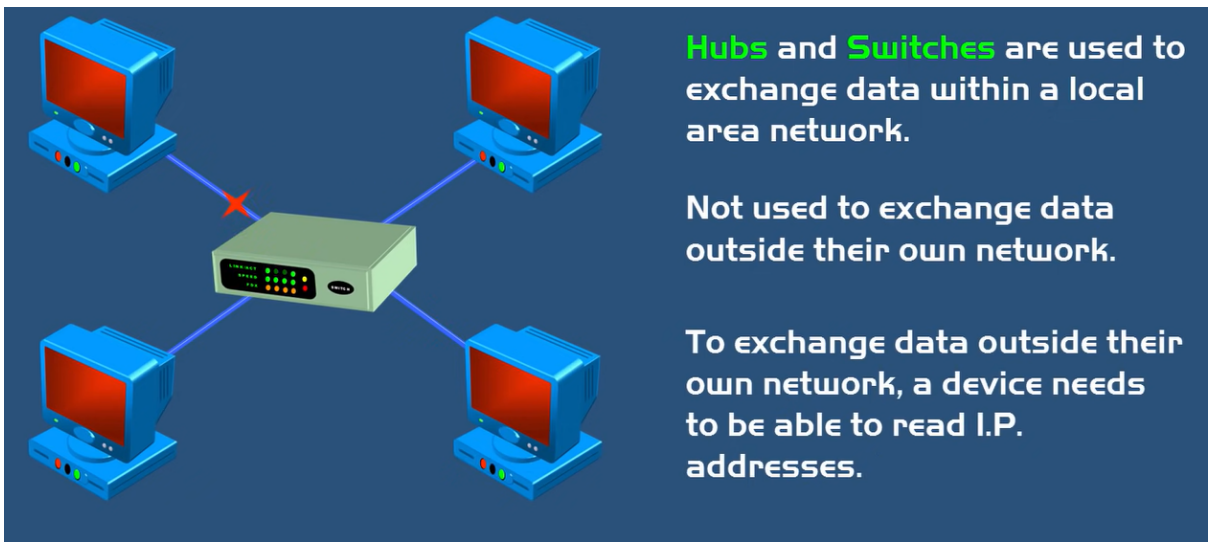
- Communication between VLAN's requires inter VLAN routing, but these days, there are many Multilayer switches available in the market.
- Handling Multicast packets that requires quite a bit of configuration & proper designing.
- Reduces the number of Broadcast domains

Difference between Bridge and Switch in Networking	
BRIDGE	**SWITCH**
Bridge works in **data link layer** of OSI model	Switch works in data link layer and **network layer** of OSI model.
The bridge has only **two ports**	Switch has **multiple numbers of ports.**
The bridge is used to **connect two LAN segment** using the same topology.	The switch is used to **connect devices** to the same network.
The bridge can operate only in half-duplex mode	Switch can operate in both half duplex and full duplex mode.
The performance of bridge is **slower then switch**	The performance of Switch is **faster than a bridge**.

Differences between Hub and Switch

Hub	Switch
They operate in the **physical layer** of the OSI model.	They operate in **the data link layer** of the OSI model.
Uses **electrical signal** orbits	Uses **frame & packet**

It is a **non-intelligent** network device that **sends message to all ports**.	It is **an intelligent network** device that sends message to **selected** destination ports.
It primarily **broadcasts** messages.	It is supports **unicast, multicast and broadcast**.
Transmission mode is **half duplex**.	Transmission mode is **full duplex.**
Collisions may occur during setup of transmission when more than one computer place data simultaneously in the corresponding ports.	Collisions do not occur since the communication is full duplex.
They are passive devices; they **don't have any software** associated with it.	They are active devices, equipped with **network software.**
The **speed** of the hub network is up to **10 Mb per second.**	The **speed** of switch is **10/100 Mbps, 1 Gbps, and 10 Gbps.**
They generally have **fewer ports of 4/12.**	The number of **ports** is higher – **24/48**.



What is a Router?

The router is a physical or virtual internetworking device that is designed to **receive, analyse, and forward data packets** between computer networks. A router **examines a destination IP address of a given data packet**, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

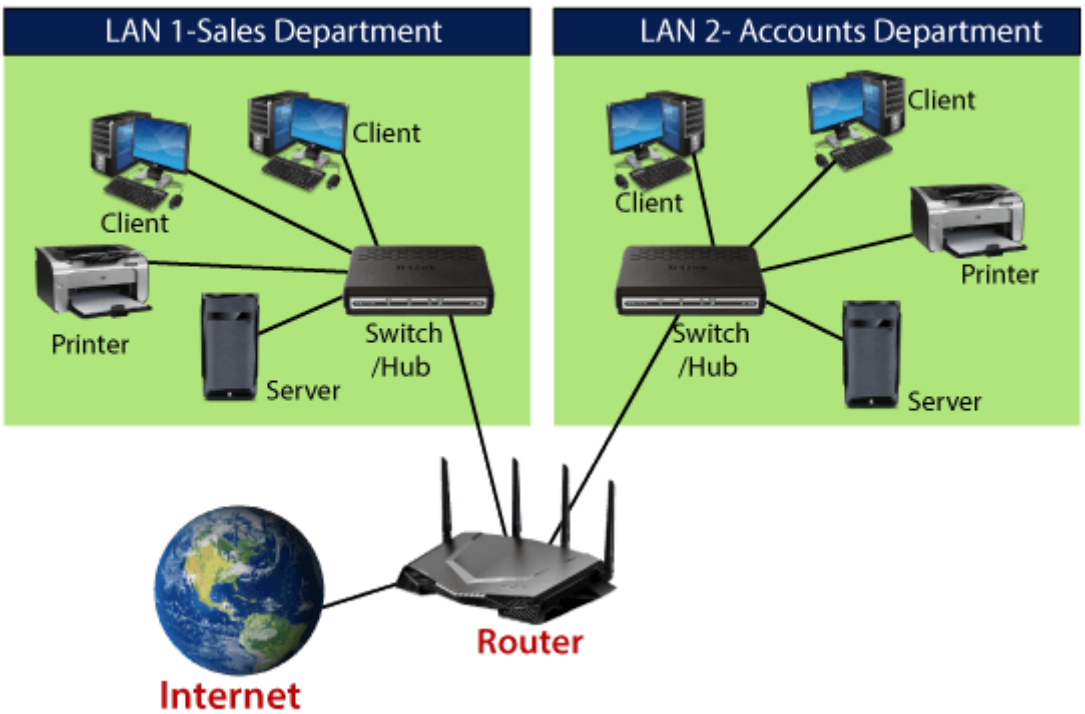
- A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments.
- It shares information with other routers in networking.
- It uses the **routing protocol** to transfer the data across a network.
- Furthermore, it is more **expensive** than other networking devices like switches and hubs.

A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer. **It uses protocols such as ICMP to communicate between two or more networks.** *It is also known as an **intelligent device** as it can calculate the best route to pass the network packets from source to the destination automatically.*

A **virtual router is a software function** or software-based framework that performs the same functions as a physical router. It may be used to **increase the reliability of the network** by virtual router redundancy protocol, which is

done by configuring a virtual router as a default gateway. A virtual router runs on commodity servers, and it is packaged with alone or other network functions, like **load balancing, firewall packet filtering,** and wide area network optimization capabilities.

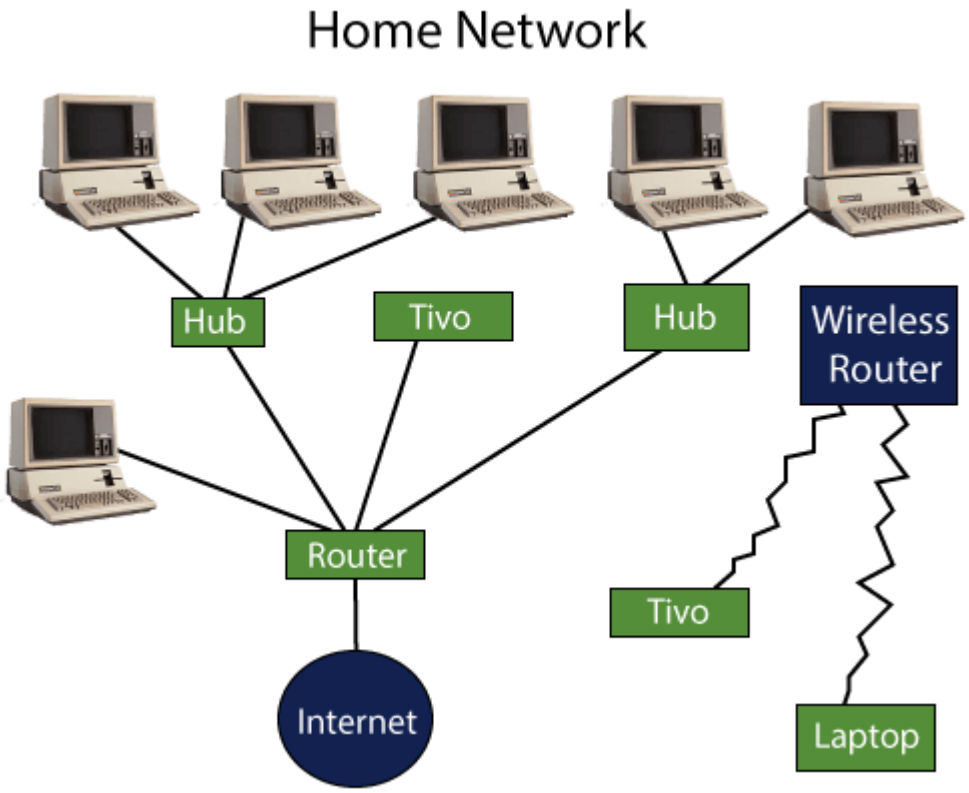
- A router is a **hardware device which is used to connect a LAN with an internet connection.** It is used to receive, analyse and forward the incoming packets to another network.
- A router works in a **Layer 3 (Network layer)** of the OSI Reference model.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.



Why Routers?

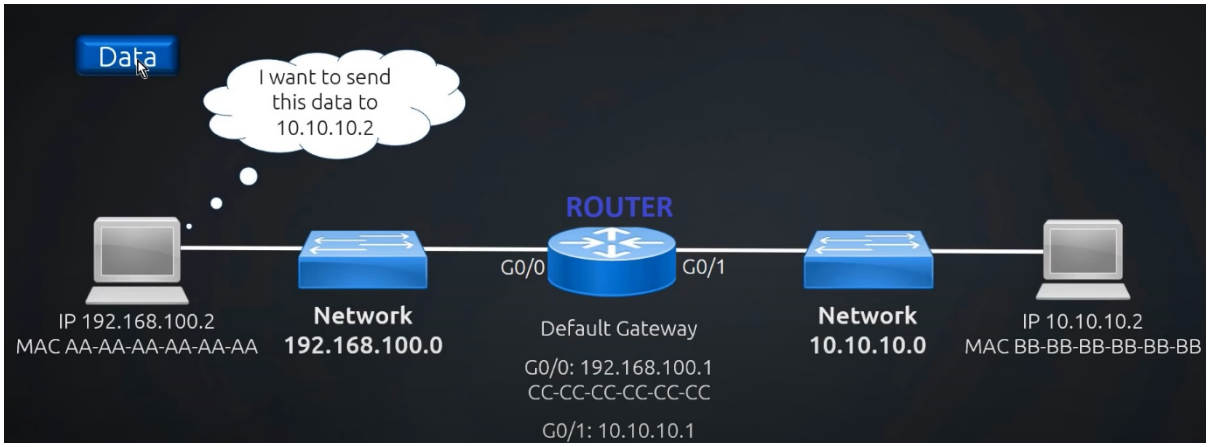
A router is more capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network. For example, a **hub is a basic networking device that is mainly used to forward the data between connected devices, but it cannot analyse or change anything with the transferring data. On the** other hand**, the router has the capability to analyse and modify the data while**

transferring it over a network, and it can send it to another network. For example, generally, routers allow sharing a single network connection between multiple devices.

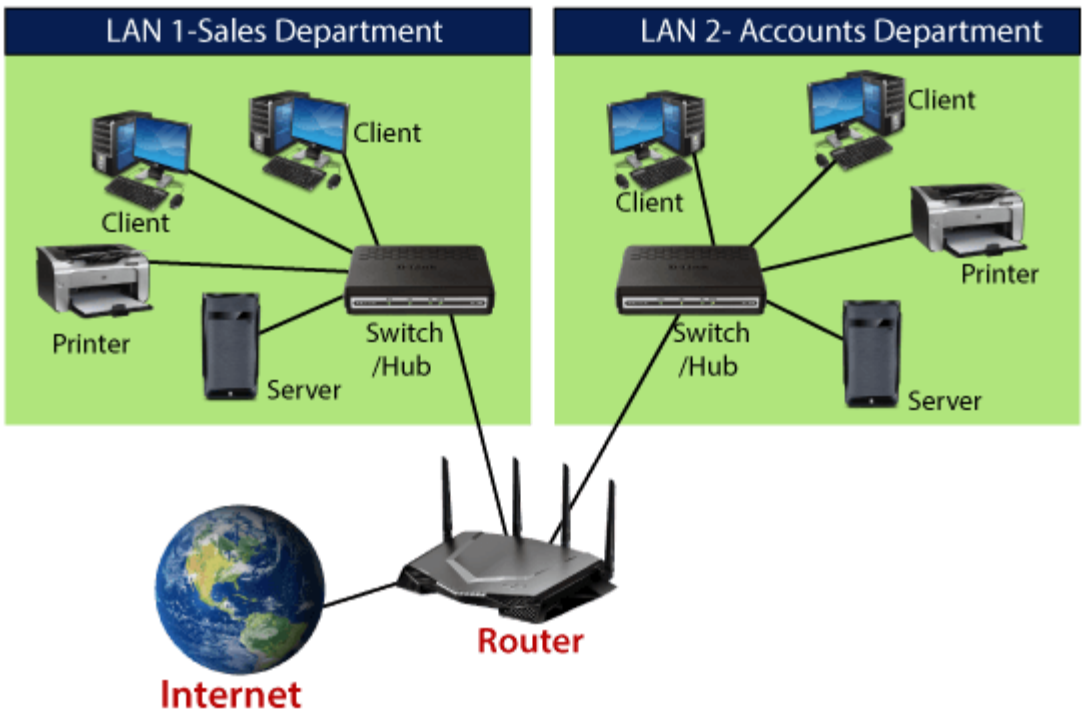


How does Router work?

A router analyzes a destination IP address of a given packet header and compares it with the **routing table to decide the packet's next path.** The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that **compute the best path to forward the data to the given IP address.**



Routers use a **modem** such as a cable, fibre, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the **routing tables** to determine where to send data and from where the traffic is coming.



A routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.

There are **two types of tables** in the router that are **static and dynamic**. The static routing tables are **configured manually**, and the dynamic routing tables are **updated automatically** by dynamic routers based on network activity.

Features of Router

- A router works on the **3rd layer (Network Layer)** of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides **high-speed internet connectivity** with the different types of **ports like gigabit, fast-Ethernet, and STM link port**.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the **unwanted interference**, as well as carry out the data encapsulation and decapsulation process.
- Routers provide the **redundancy** as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Types of Routers:

There are various types of routers in networking; such are given below:

1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.

Wireless routers are capable of generating a wireless signal in your home or office, and it allows the computers to connect with routers within a range, and use the internet. If the connection is indoors, the range of the wireless router is about 150 feet, and when the connection is outdoors, then its range is up to 300 feet.

Furthermore, you can make more secure wireless routers with a password or get your IP address. Thereafter, you can log in to your router by using a user ID and password that will come with your router.

2. Brouter: A brouter is a **combination of the bridge and a router**. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these **two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network**.

3. Core router: A core router is a type of router that can route the **data within a network,** but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.

4. Edge router: An edge router is **a lower-capacity device that is placed at the boundary of a network**. It allows an **internal network to connect with the external networks**. It is also called as an **access router**. It uses an External **BGP (Border Gateway Protocol**) to provides connectivity with remote networks over the internet.

There are two types of edge routers in networking:

- **Subscriber edge router**
- **Label edge router**

The **subscriber edge router** belongs to an end-user organization, and it works in a situation where it acts on a border device.

The **label edge router** is used in the boundary of Multiprotocol Label Switching (MPLS) networks. It acts as a gateway between the LAN, WAN, or the internet.

5. Broadband routers: Broadband routers are mainly used to provide high-speed internet access to computers. It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).

All broadband routers have the option of three or four Ethernet ports for connecting the laptop and desktop systems. A broadband router is configured and provided by the internet service provider (ISP). It is also known as a **broadband modem**, asymmetric digital subscriber line (**ADSL**), or digital subscriber line (**DSL**) modem.

Benefits of Router

There are so many benefits of a router, which are given below:

- **Security:** Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- **Performance enhancement:** It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.
- **Reliability:** Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.
- **Networking Range:** In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a **repeater (Regenerating the signals).** The physical range can be as per the requirement of a

particular installation, as long as a router is installed before the maximum cable range exceeds.

Difference between Bridge and Router:

Bridge	Router
A bridge is a networking device that is used to connect two local area networks (LANs) by using media access control addresses and transmit the data between them.	A router is also a networking device that sends the data from one network to another network with the help of their IP addresses.
A bridge is able to connect **only two different LAN segments.**	A router is capable of **connecting the LAN and WAN.**
A bridge transfers the data in the **form of frames.**	A router transfers the **data in the form of packets.**
It sends data based on the **MAC address of a device.**	It sends data based on **the IP address of a device.**
The bridge has only **one port** to connect the device.	The router has **several ports** to connect the devices.
The bridge **does not use any table** to forward the data.	The router uses a **routing table** to send the data.

Difference between Switch and Router:

Switch	Router
It connects **multiple networked** devices in the network.	It connects **multiple switches & their corresponding networks.**
It works on the **data link** layer of the OSI model.	It works on the **network layer of the OSI model.**
It is used **within a LAN.**	It can be used **in LAN or MAN**.
A switch **cannot perform NAT** or Network Address Translation.	A router can **perform Network Address Translation.**
The **switch takes more time** while making complicated routing decisions.	A router can take a routing decision **much faster** than a switch.
It provides only **port** security.	It provides security measures to **protect the network** from security threats.
It comes in the category of **semi-Intelligent devices.**	It is known as **an Intelligent** network device.
It works in **either half or full-duplex transmission** mode.	It works in the **full-duplex transmission mode**. However, we can change it manually to work on half-duplex mode.

It sends information from one device to another in the form of **Frames (for L2 switch) and the form of packets** (for L3 switch).	It sends information from **one network to another network in the form of data packets.**
Switches can only work with the **wired network.**	Routers can work with both **wired & wireless networks.**
Switches are available with different ports, such as **8, 16, 24, 48, and 64.**	A router contains two ports by default, such as **Fast Ethernet Port**. But we can also add the serial ports explicitly.
It uses the CAM (Content Addressable Memory) table for the source and destination **MAC address**.	It uses the routing table to get the **best route for the destination IP.**

Difference between Hub Switch and Router in tabular form:

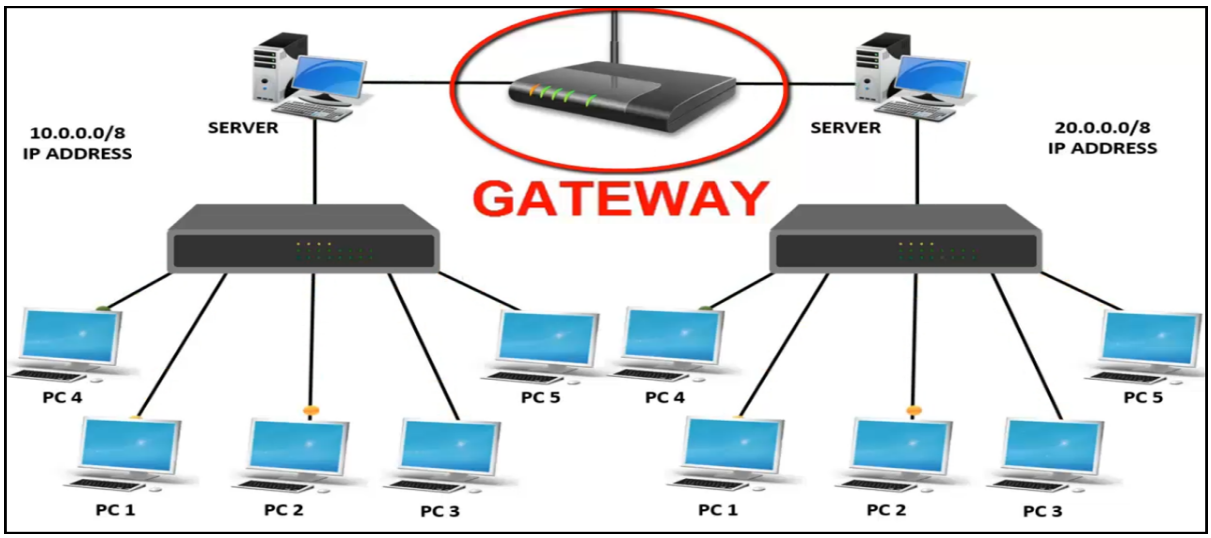
HUB	*SWITCH*	*ROUTER*
Hub is a broadcast device.	The switch is a multicast device.	The router is a routing device.
Hub works in the physical layer of the OSI model.	The switch works in the data link layer and network layer of the OSI model.	The router works in the network layer of the OSI model.
Hub is used to connect devices to the same network.	The switch is used to connect devices to the network.	The router is used to connect two different networks.
Hub sends data in the form of bits.	The switch sends data in the form of frames.	The router sends data in the form of packets.
Hub works in **half-duplex**.	The switch works in **full-duplex**.	The router works in full-duplex.
Only one device can send data at a time.	Multiple devices can send data at a time.	Multiple devices can send data at a time.
Hub does not store any MAC	Switch stores the **IP**	Router stores the IP Address

address of a node in the network.	**Address** and **MAC address** of **nodes** used in a network.	and MAC address of nodes used in a network.

What is Gateway

A gateway is a networking device that connects two networks using different protocols together.

it also acts as a “gate” between two networks. It may be a router, firewall, server, or other devices that enable traffic to flow in and out of the network.



Here, Network 1 is assigned with the IP Address 10.0.0.0/8, and Network 2 is assigned with the IP address 20.0.0.0/8. **As these two are different networks, it cannot communicate with each other. Therefore, we use a centralized device called a router**.

Now, whatever data is sent by Network 1 into Network 2 or vice versa, it will go through the centralized device router. Like this, here router is acting as a gateway as it is the main gate to enter into a different network.

Now, here is the most complicated and confusing question. If this device can act as a gateway then what is the use of gateway device in a network.

The router can communicate between two different networks using the same protocol on the other hand **gateway is used to communicate between two different networks using a different protocol**. For this reason, **the gateway is also called a protocol converter**.

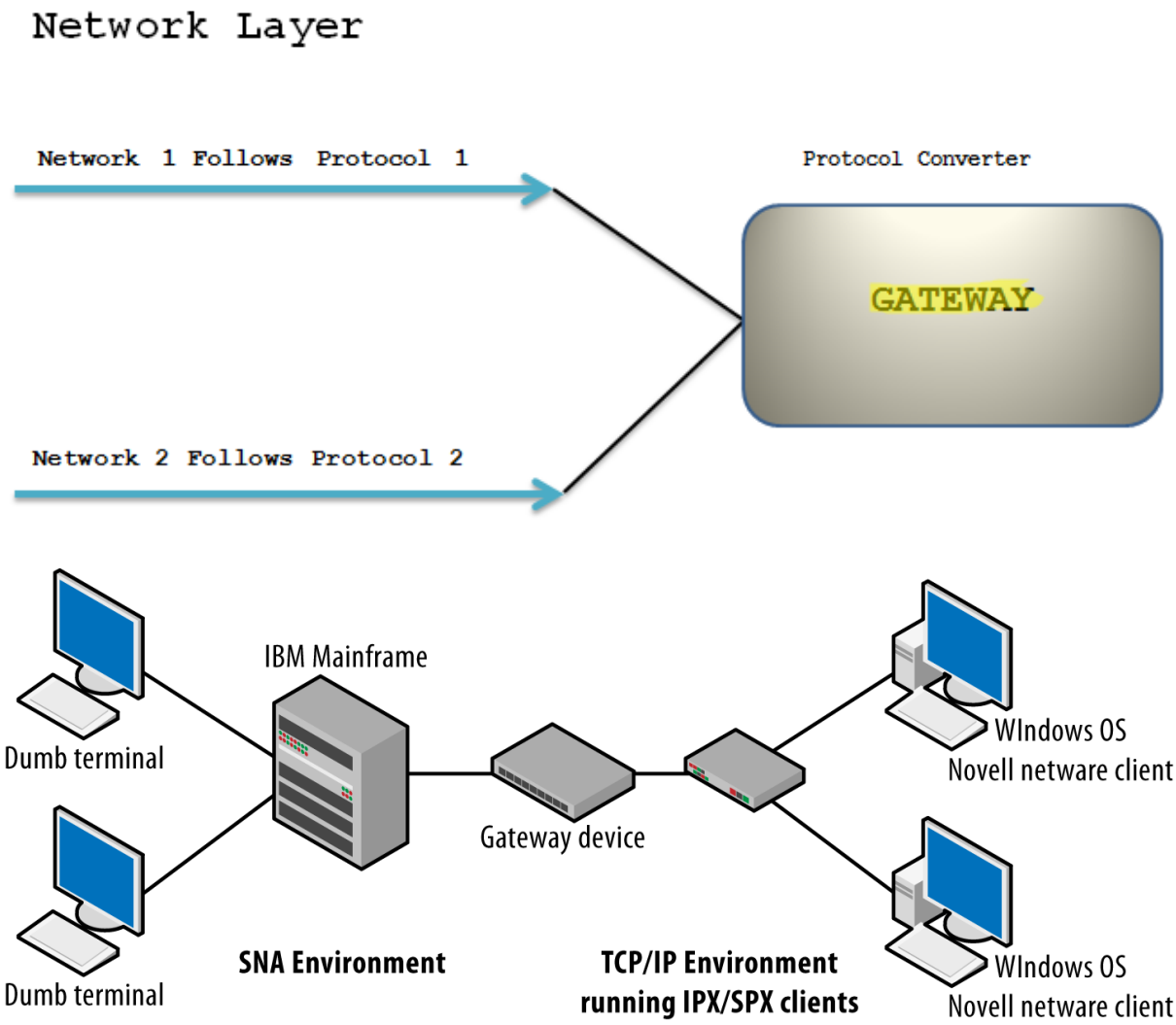


Figure 1-4. Mixed architecture topology

Another example is a network of Apple computers running AppleTalk while connecting to a network of Windows machines running TCP/IP.

NOTE: Systems Network Architecture (SNA-IBM), AppleTalk, Novell Netware (IPX/SPX), and the Open System Interconnection (OSI) model.

Features	Router	Gateway
Definition	A Router is a networking layer system used to manage and forward data packets to computer networks.	A gateway is simply a device or hardware that acts as a "**gate**" between the networks. It could also be defined as a node that acts as an entry for other network nodes.
Working Principle	Usually, routers run on the 3rd layer of the protocol and transmit the packets from one system to another. A router chooses the network's path to transport the data packets.	Gateway interprets the network system as endpoints from one packet to another.
Hosting	It is available only to dedicated applications.	It is hosted on the dedicated application, physical servers, and virtual applications.
Networks	It routes the data packets via similar networks(protocols).	It connects two dissimilar networks(protocols).
Deployment	It is deployed on the router hardware in a specific appliance.	The gateway is deployed as the virtual or physical server or the specific appliance.
OSI Layer	It can operate only on **3** and **4** layers.	It can operate only on the **5** layers.
Dynamic Routing	Router supports dynamic routing.	Gateway doesn't support dynamic routing.
Associated terms	The router is also called a wireless router and an Internet router.	The gateway is also called a gateway router, proxy server, and voice gateway.
Component's Operating	The router operates by installing different routing data	The gateway works by distinguishing between the

Process	for different networks, and the destination address is based on traffic.	network structure and the components available outside the network.

NOTE:

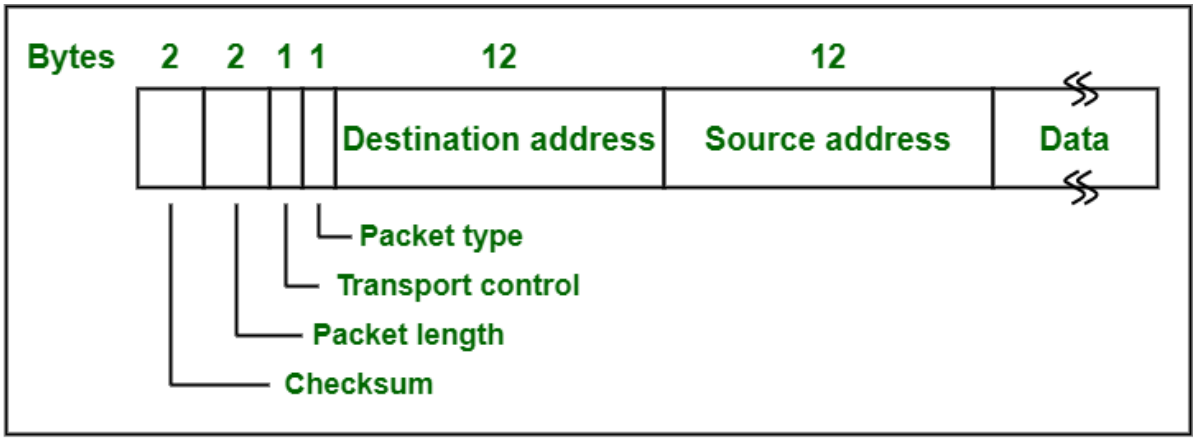
The Internet IP protocol and Novell's IPX are examples of routed protocols. Other examples include DECnet, AppleTalk, Novell NetWare, Open Systems Interconnect (OSI), Banyan VINES, and Xerox Network System (XNS).

CP/IP examples of routing protocols are the Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Enhanced IGRP (EIGRP)

Novell NetWare is most popular and widely used network system in PC world.

Protocols in Novell Netware :

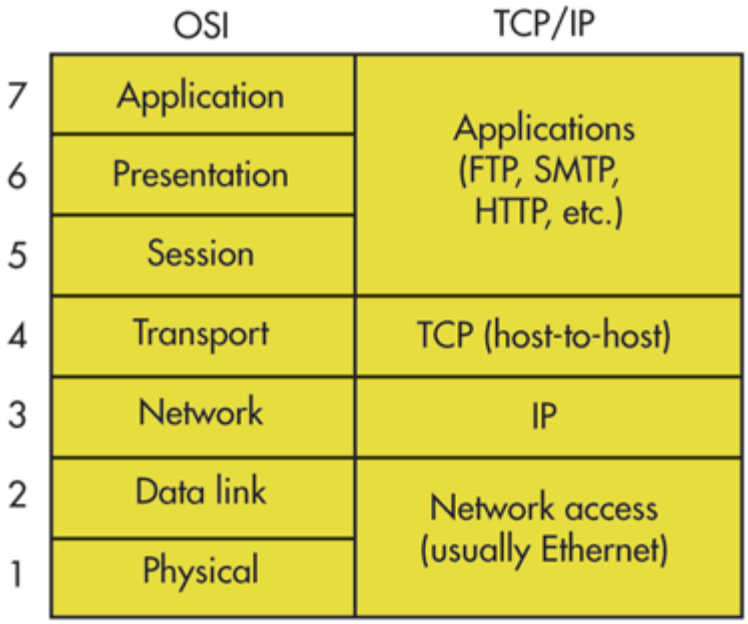
- **Internet Package Exchange (IPX) –**
  Network layer generally runs unreliable connectionless internetwork protocol. It is called Internet Package Exchange (IPX) protocol. This protocol is simply used for routing and showing path to packets to move from one network node to another network throughout internetwork.
  Format of IPX is shown below:

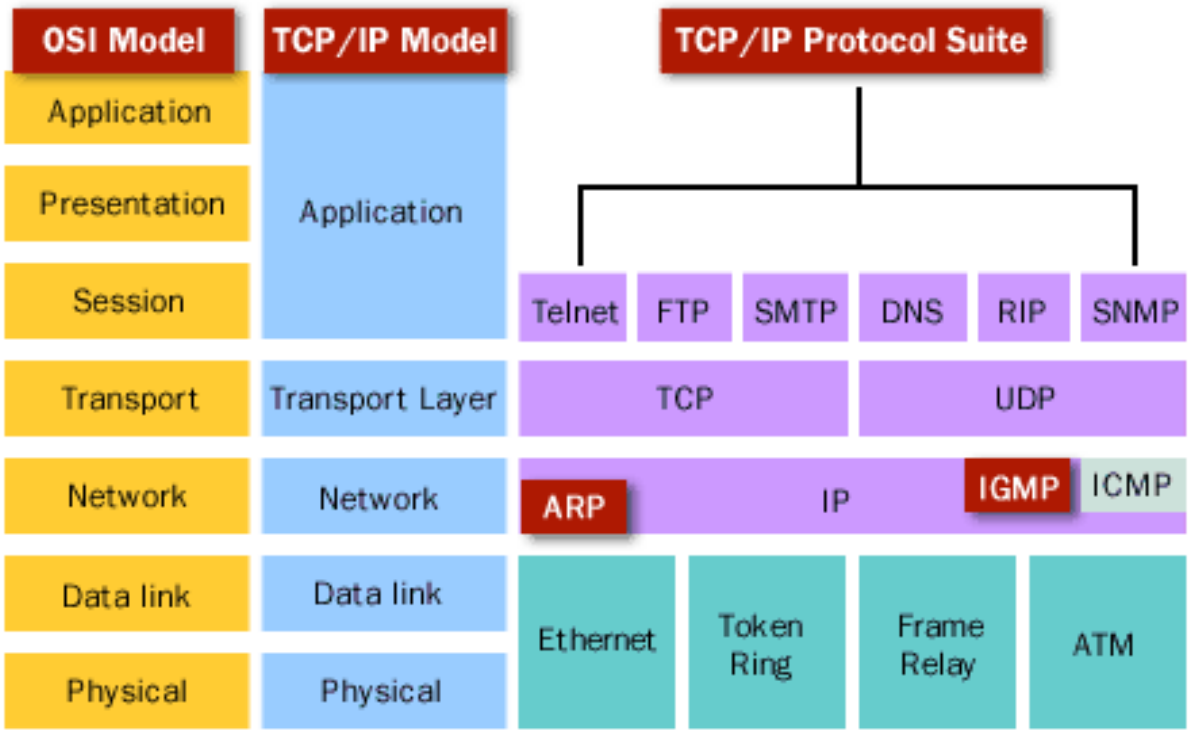


A Novell NetWare IPX Packet

- **NetWare Core Protocol (NCP) –**
  NCP is type of network protocol that is used in many products from Novell, Inc. It is actually Novell client-server protocol used for mainly Local Area Network (LAN). It is generally connected to NetWare Operating systems (OS). It also works with alternating operating systems along with UNIX, Linux, and Windows NT.

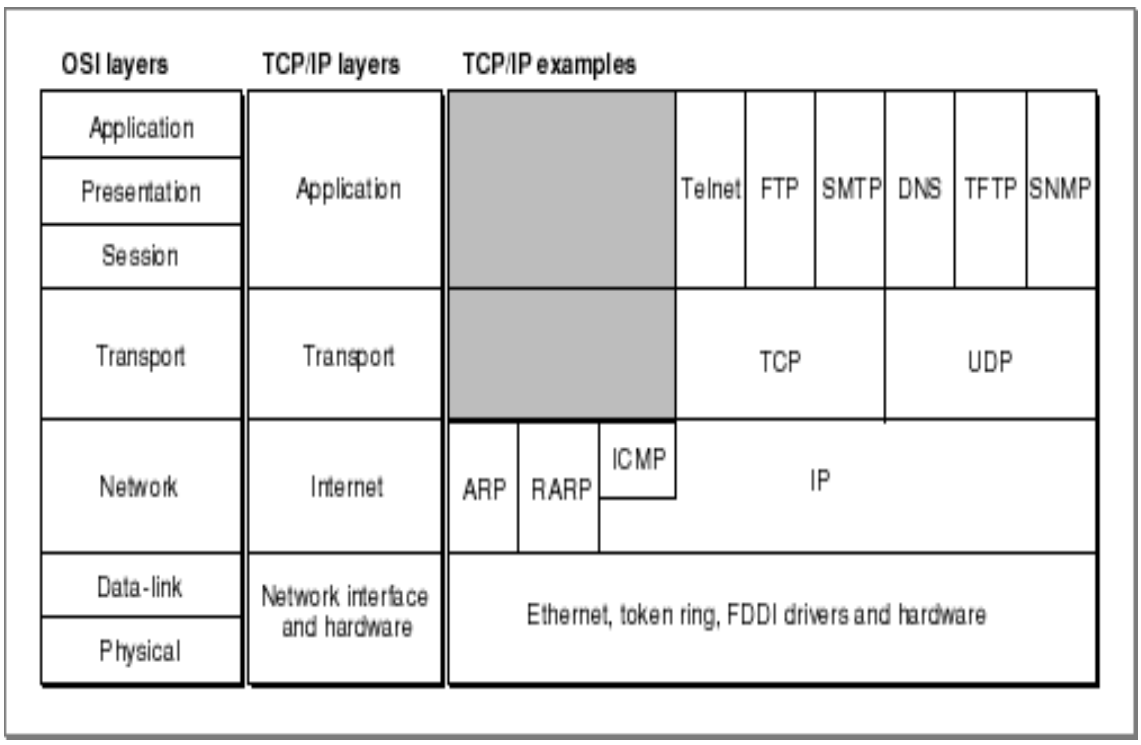
- **Sequenced Packet Exchange (SPX) –**
  SPX is also type of network protocol that is used by Novell Netware. SPX is also supported by other operating systems. It is nowadays considered legacy protocol as it has largely been replaced by TCP/IP. This protocol is simply used for handling packet sequencing in Novell Netware network.

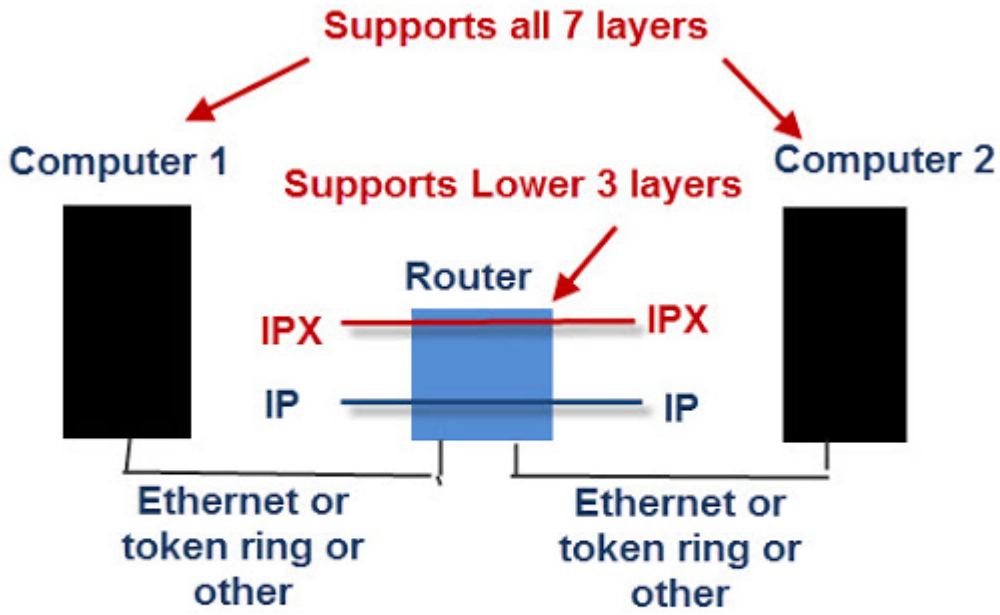

OSI
TCP/IP
7
Application
6
Presentation
5
Session
Applications (FTP, SMTP, HTTP, etc.)
4
Transport
TCP (host-to-host)
3
Network
IP
2
Data link
1
Physical
Network access (usually Ethernet)


OSI Model
TCP/IP Model
TCP/IP Protocol Suite
Application
Presentation
Session
Application
Telnet
FTP
SMTP
DNS
RIP
SNMP
Transport
Transport Layer
TCP
UDP
Network
Network
ARP
IP
IGMP
ICMP
Data link
Data link
Physical
Physical
Ethernet
Token Ring
Frame Relay
ATM

OSI (Open Source Interconnection) 7 Layer Model

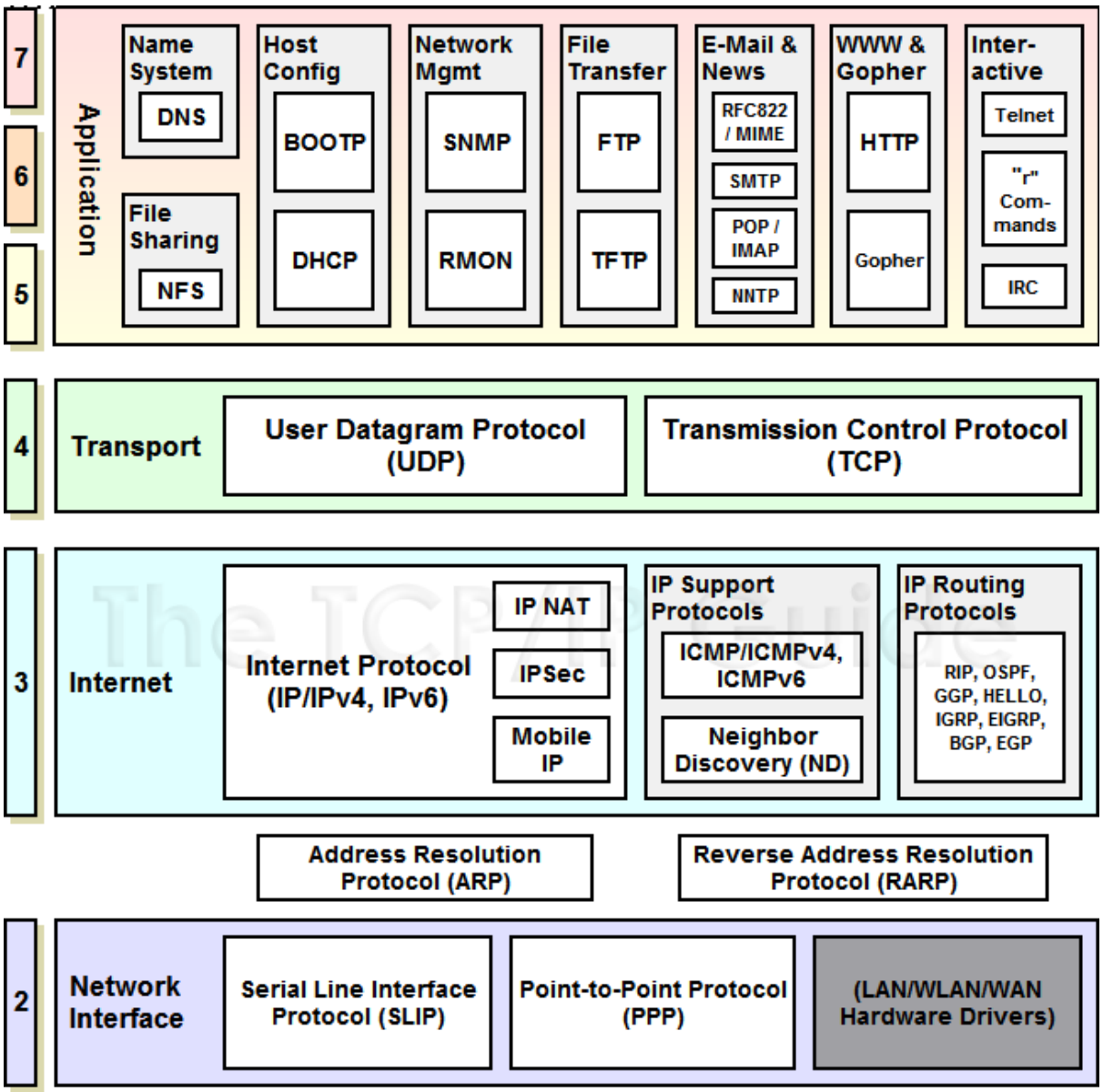
Layer	Application/Example		Central Device/ Protocols	
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP	
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**	





End To End Connections and OSI

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard InstrumentationTools.com


7
6
5
Application
Name System
DNS
File Sharing
NFS
Host Config
BOOTP
DHCP
Network Mgmt
SNMP
RMON
File Transfer
FTP
TFTP
E-Mail & News
RFC822 / MIME
SMTP
POP / IMAP
NNTP
WWW & Gopher
HTTP
Gopher
Inter-active
Telnet
"r" Com-mands
IRC
4
Transport
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
3
Internet
Internet Protocol (IP/IPv4, IPv6)
IP NAT
IPSec
Mobile IP
IP Support Protocols
ICMP/ICMPv4, ICMPv6
Neighbor Discovery (ND)
IP Routing Protocols
RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
2
Network Interface
Serial Line Interface Protocol (SLIP)
Point-to-Point Protocol (PPP)
(LAN/WLAN/WAN Hardware Drivers)

OSI Model

The Open Systems Interconnected (OSI) model divides the network into seven layers and explains the routing of the data from source to destination. It is a theoretical model which explains the working of the networks. It was developed by the International Organization for Standardization (ISO) for their network suite. Here are the details of OSI's seven layers:

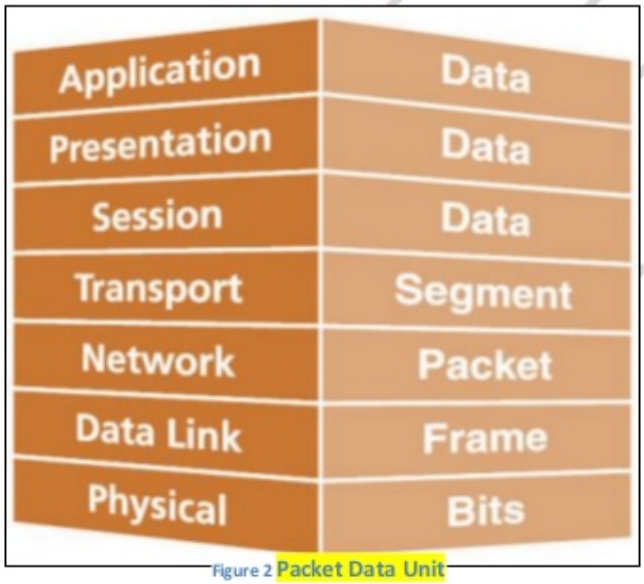


Figure 2 Packet Data Unit

1. **Physical Layer:** As the name suggests, this is the layer where the physical connection between two computers takes place. The data is transmitted via this physical medium to the destination's physical layer. The popular protocols at this layer are Fast Ethernet, ATM, RS232, etc.

2. **Data Link Layer:** The main function of this layer is to convert the data packets received from the upper layer into frames, and route the same to the physical layer. Error detection and correction is done at this layer, thus making it a reliable layer in the model. It establishes a logical link between the nodes and transmits frames sequentially.

3. **Network Layer:** The main function of this layer is to translate the network address into physical MAC address. The data has to be routed to its intended destination on the network. This layer is also responsible to determine the efficient route for transmitting the data to its

This layer can be used to connect different network types like ATM, Token ring, Ethernet, LAN, etc.

2. **Internet Layer:** This layer is also known as the Network Layer. The main function of this layer is to route the data to its destination. The data that is received by the link layer is made into data packets (IP datagrams). The data packets contain the source and the destination IP address or logical address. These packets are sent on any network and are delivered independently. This indicates that the data is not received in the same order as it was sent. The protocols at this layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), etc.

3. **Transport Layer:** This layer is responsible for providing datagram services to the Application layer. This layer allows the host and the destination devices to communicate with each other for exchanging messages, irrespective of the underlying network type. Error control, congestion control, flow control, etc., are handled by the transport layer. The protocol that this layer uses is TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP gives a reliable, end-to-end, connection-oriented data transfer, while UDP provides unreliable, connectionless data transfer between two computers.

4. **Application Layer:** It provides the user interface for communication. This is the layer where email, web browsers or FTP run. The protocols in this layer are FTP, SMTP, HTTP, etc.

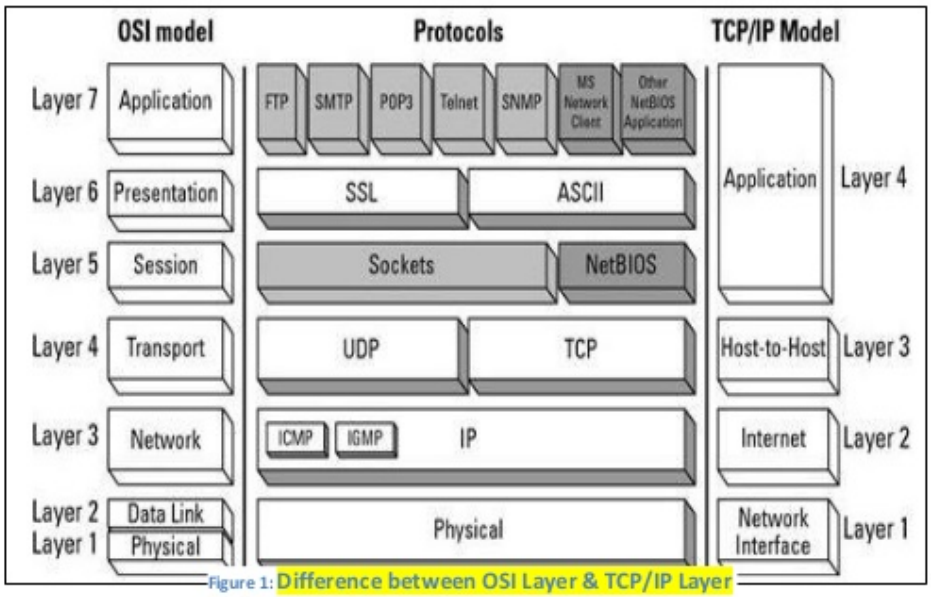
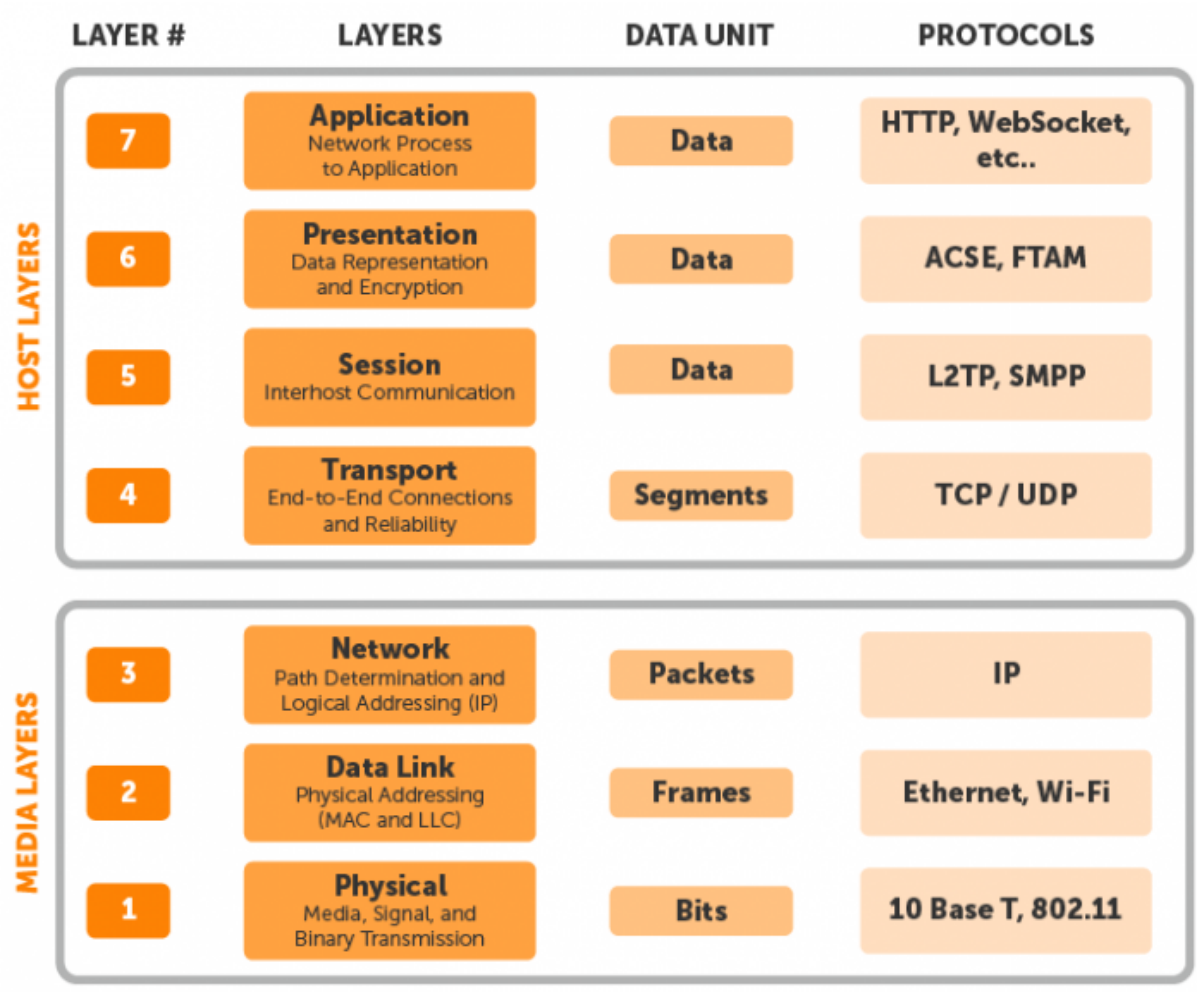
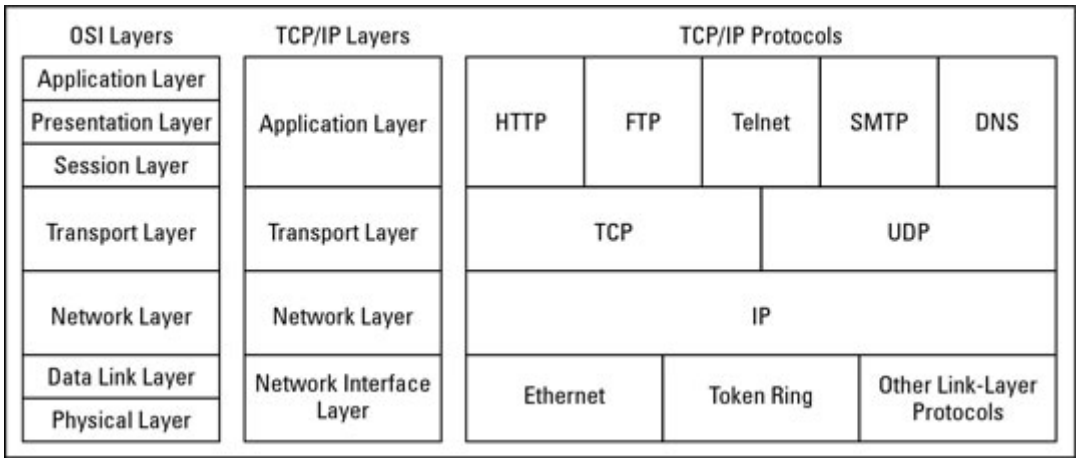
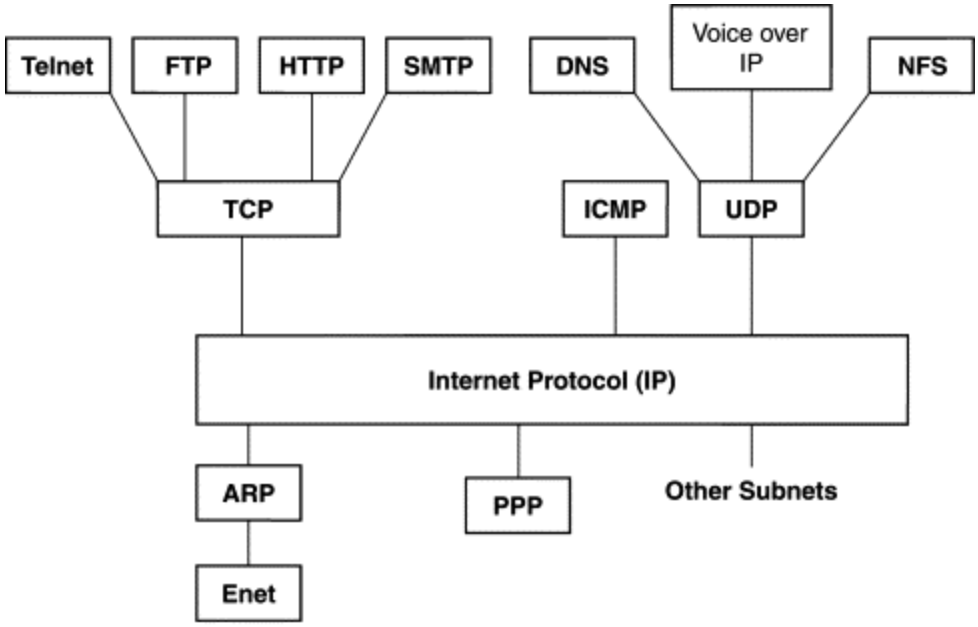


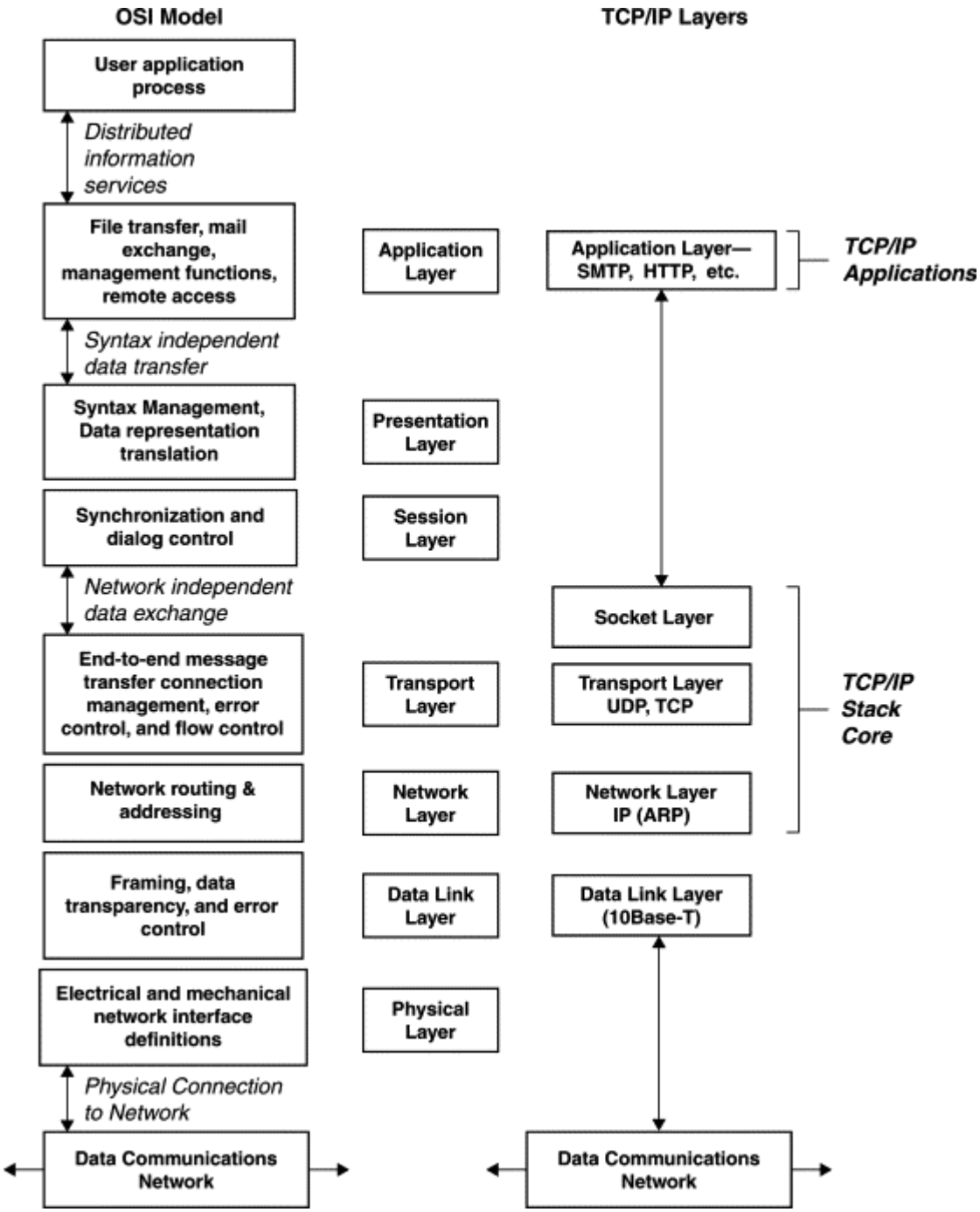
Figure 1: Difference between OSI Layer & TCP/IP Layer

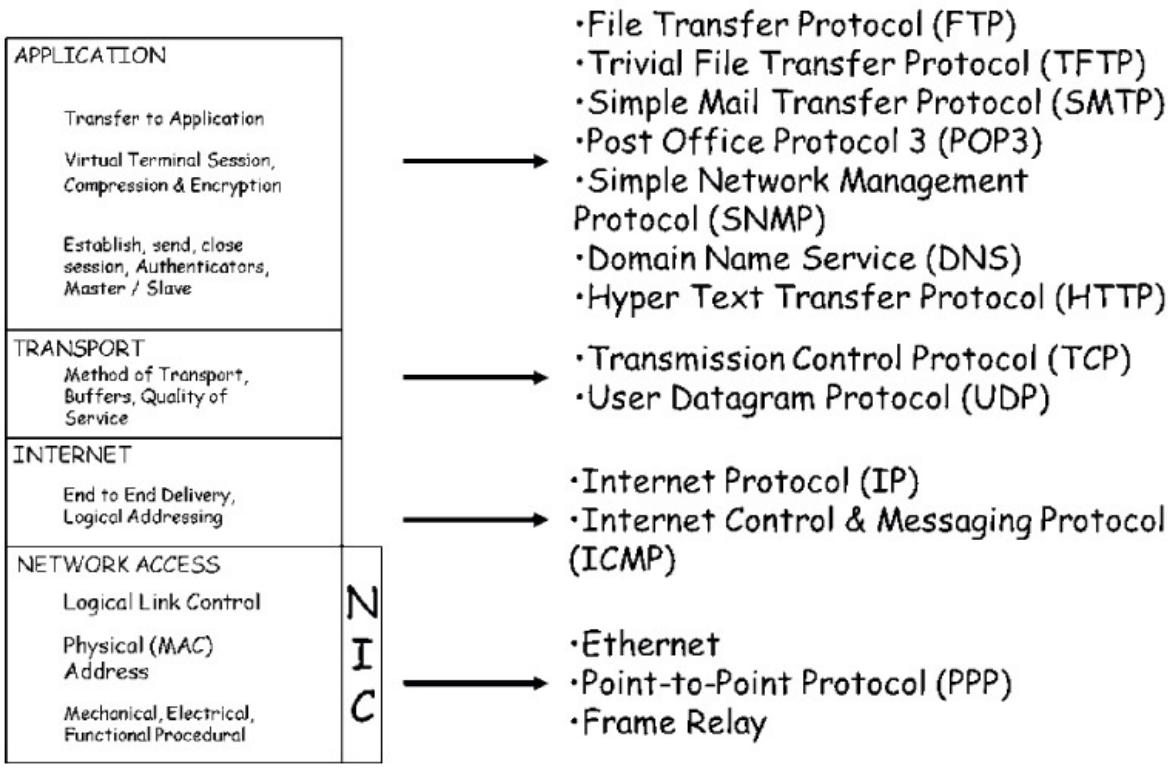

LAYER #
LAYERS
DATA UNIT
PROTOCOLS
HOST LAYERS
7
Application
Network Process to Application
Data
HTTP, WebSocket, etc..
6
Presentation
Data Representation and Encryption
Data
ACSE, FTAM
5
Session
Interhost Communication
Data
L2TP, SMPP
4
Transport
End-to-End Connections and Reliability
Segments
TCP / UDP
MEDIA LAYERS
3
Network
Path Determination and Logical Addressing (IP)
Packets
IP
2
Data Link
Physical Addressing (MAC and LLC)
Frames
Ethernet, Wi-Fi
1
Physical
Media, Signal, and Binary Transmission
Bits
10 Base T, 802.11

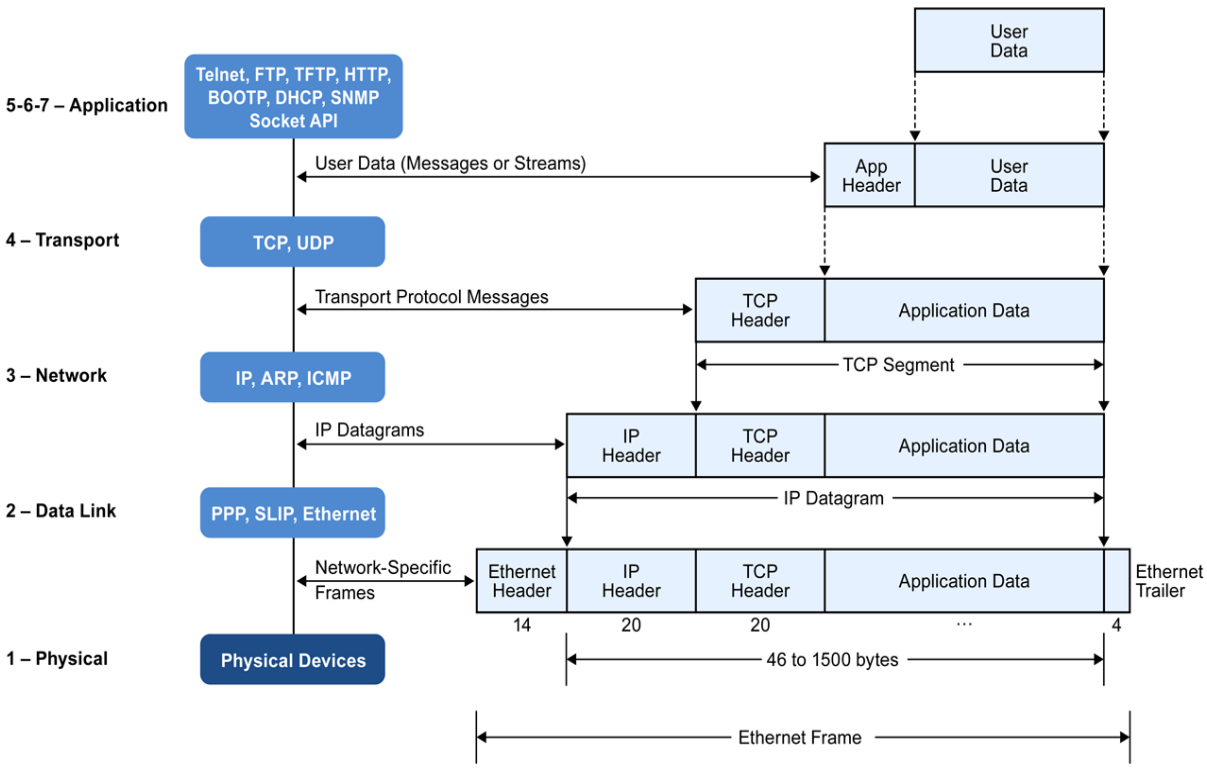

OSI Layers
TCP/IP Layers
TCP/IP Protocols
Application Layer
Presentation Layer
Session Layer
Application Layer
HTTP
FTP
Telnet
SMTP
DNS
Transport Layer
Transport Layer
TCP
UDP
Network Layer
Network Layer
IP
Data Link Layer
Physical Layer
Network Interface Layer
Ethernet
Token Ring
Other Link-Layer Protocols

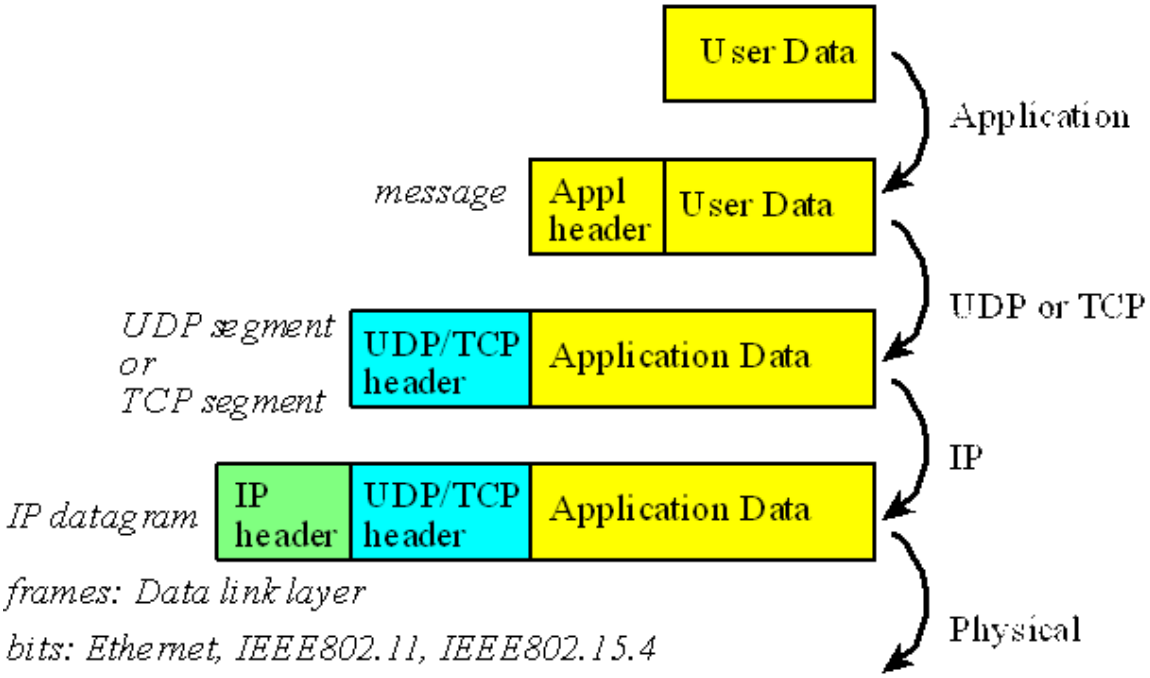


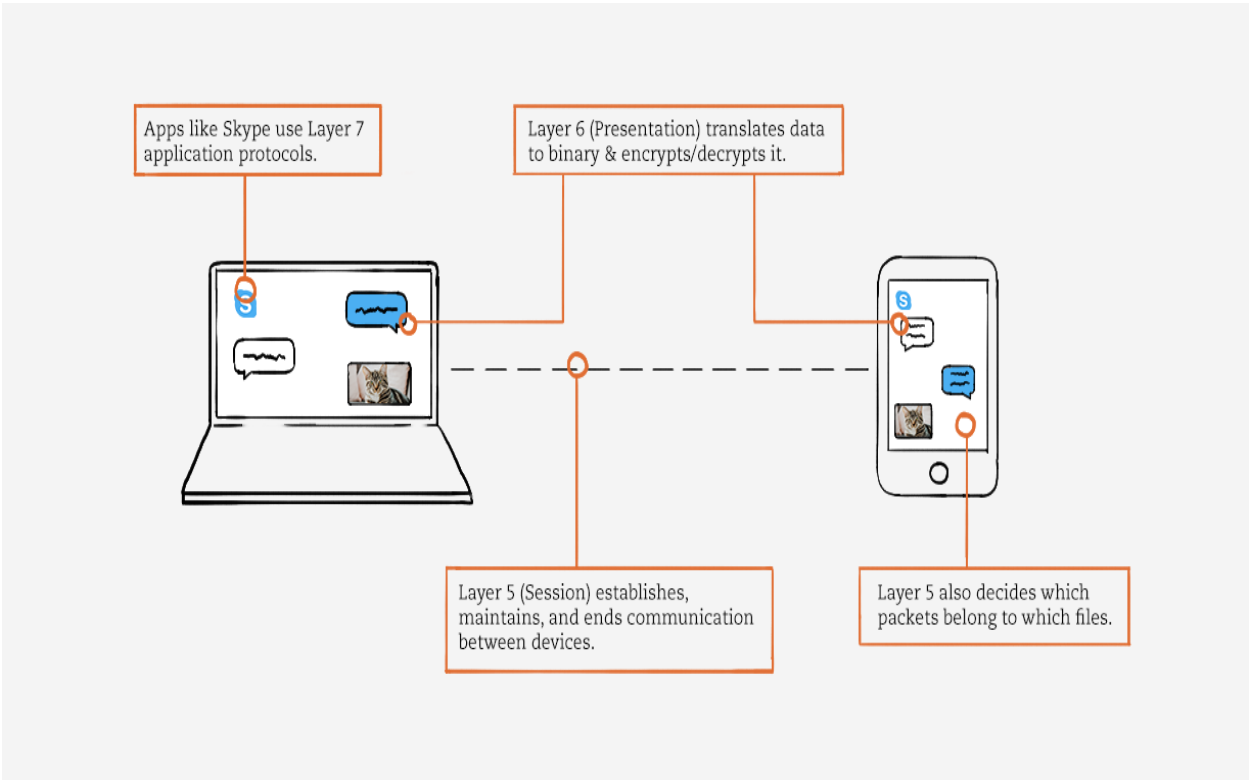
FTP: File transfer protocol
SMTP: Simple mail transport protocol
HTTP: Hyper text transfer protocol
PPP: Point-to-point protocol
ARP: Address resolution protocol
ICMP: Internet control message protocol
UDP: User datagram protocol
TCP: Transmission control protocol

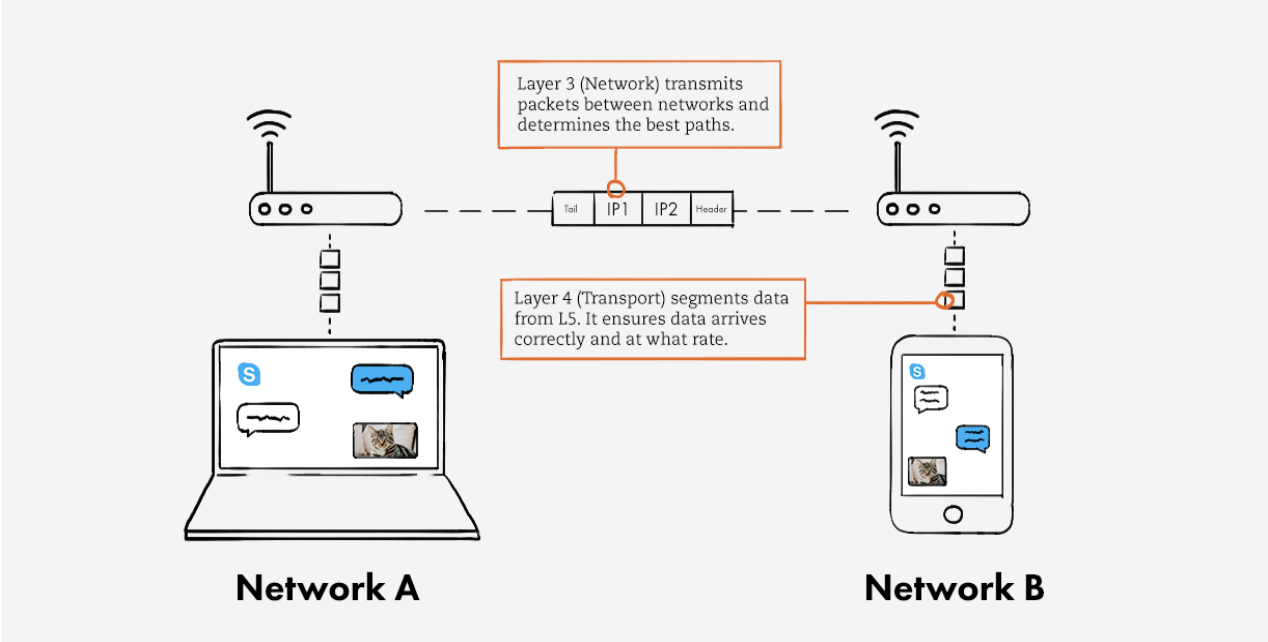

OSI Model
TCP/IP Layers
User application process
Distributed information services
File transfer, mail exchange, management functions, remote access
Application Layer
Application Layer— SMTP, HTTP, etc.
TCP/IP Applications
Syntax independent data transfer
Syntax Management, Data representation translation
Presentation Layer
Synchronization and dialog control
Session Layer
Network independent data exchange
Socket Layer
End-to-end message transfer connection management, error control, and flow control
Transport Layer
Transport Layer UDP, TCP
TCP/IP Stack Core
Network routing & addressing
Network Layer
Network Layer IP (ARP)
Framing, data transparency, and error control
Data Link Layer
Data Link Layer (10Base-T)
Electrical and mechanical network interface definitions
Physical Layer
Physical Connection to Network
Data Communications Network
Data Communications Network

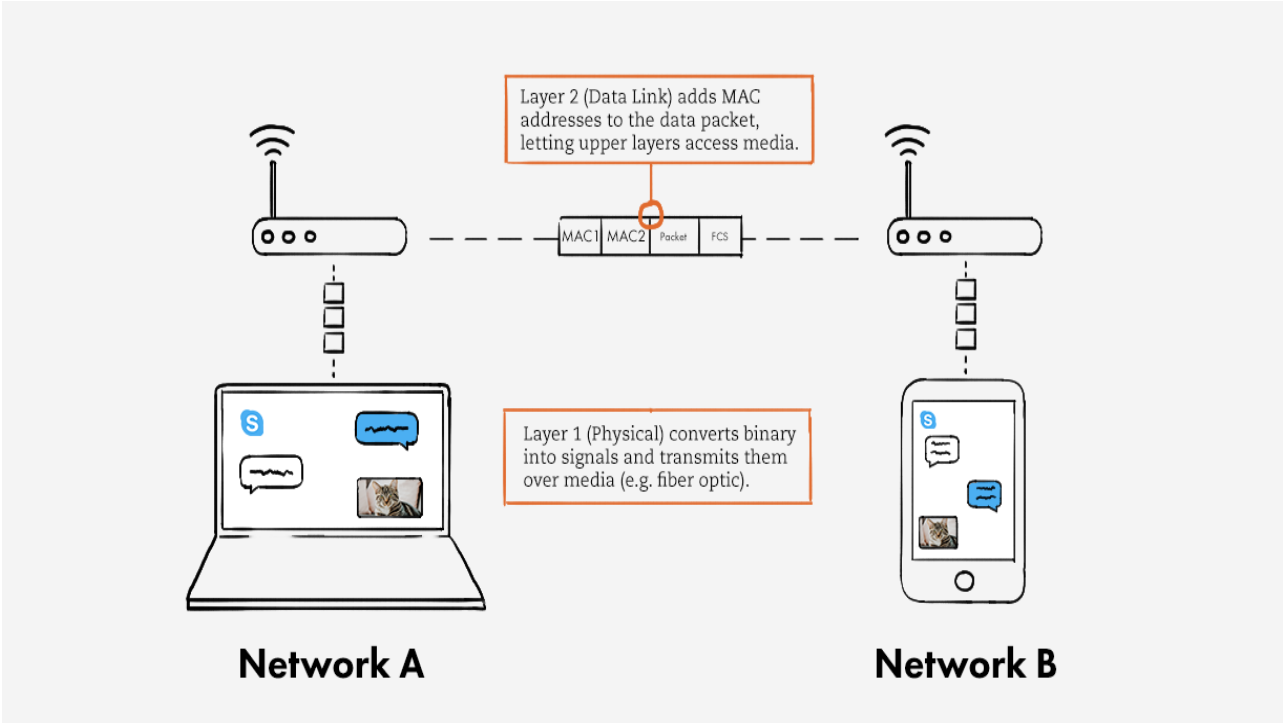

APPLICATION
Transfer to Application
Virtual Terminal Session, Compression & Encryption
Establish, send, close session, Authenticators, Master / Slave
TRANSPORT
Method of Transport, Buffers, Quality of Service
INTERNET
End to End Delivery, Logical Addressing
NETWORK ACCESS
Logical Link Control
Physical (MAC) Address
Mechanical, Electrical, Functional Procedural
NIC
·File Transfer Protocol (FTP)
·Trivial File Transfer Protocol (TFTP)
·Simple Mail Transfer Protocol (SMTP)
·Post Office Protocol 3 (POP3)
·Simple Network Management Protocol (SNMP)
·Domain Name Service (DNS)
·Hyper Text Transfer Protocol (HTTP)
·Transmission Control Protocol (TCP)
·User Datagram Protocol (UDP)
·Internet Protocol (IP)
·Internet Control & Messaging Protocol (ICMP)
·Ethernet
·Point-to-Point Protocol (PPP)
·Frame Relay


5-6-7 – Application
Telnet, FTP, TFTP, HTTP, BOOTP, DHCP, SNMP Socket API
User Data
User Data (Messages or Streams)
App Header
User Data
4 – Transport
TCP, UDP
Transport Protocol Messages
TCP Header
Application Data
TCP Segment
3 – Network
IP, ARP, ICMP
IP Datagrams
IP Header
TCP Header
Application Data
IP Datagram
2 – Data Link
PPP, SLIP, Ethernet
Network-Specific Frames
Ethernet Header
IP Header
TCP Header
Application Data
Ethernet Trailer
14
20
20
...
4
1 – Physical
Physical Devices
46 to 1500 bytes
Ethernet Frame

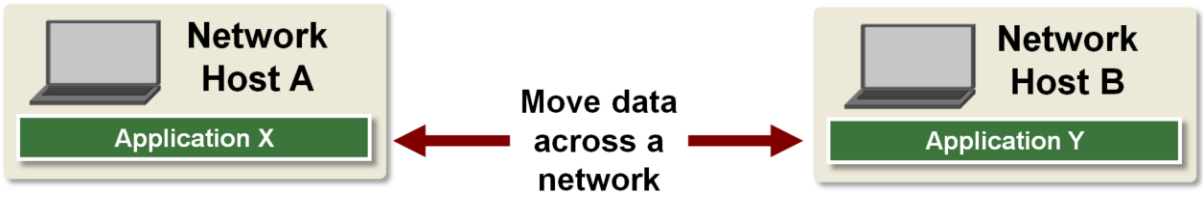

User Data
Application
message
Appl header
User Data
UDP or TCP
UDP segment or TCP segment
UDP/TCP header
Application Data
IP
IP datagram
IP header
UDP/TCP header
Application Data
frames: Data link layer
bits: Ethernet, IEEE802.11, IEEE802.15.4
Physical

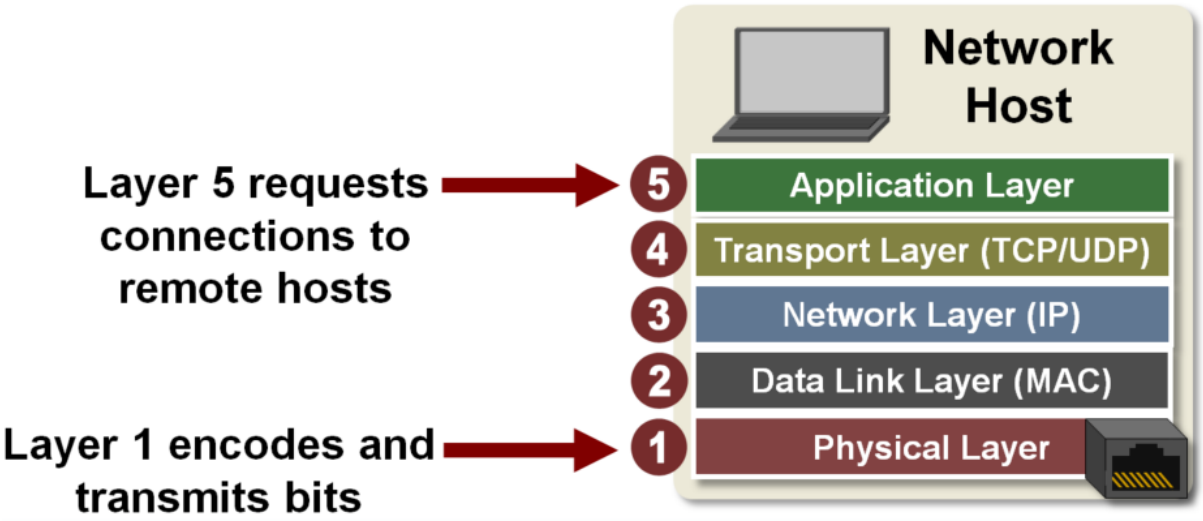

Apps like Skype use Layer 7 application protocols.
Layer 6 (Presentation) translates data to binary & encrypts/decrypts it.
Layer 5 (Session) establishes, maintains, and ends communication between devices.
Layer 5 also decides which packets belong to which files.

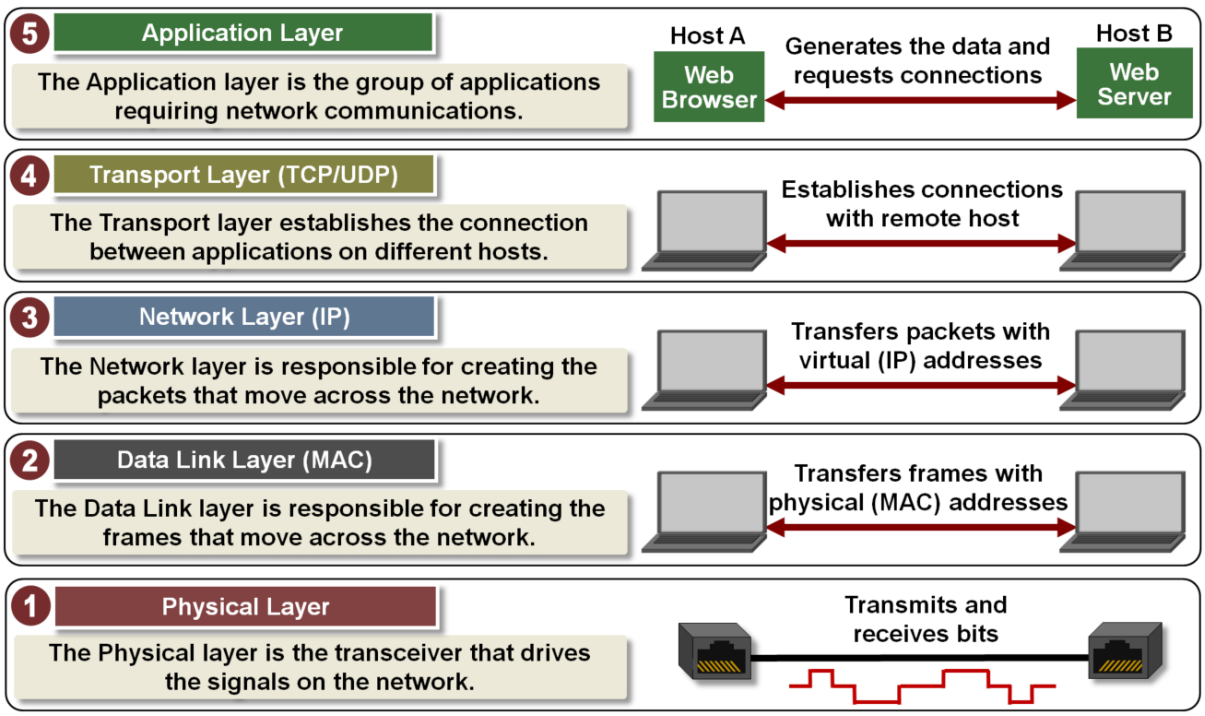


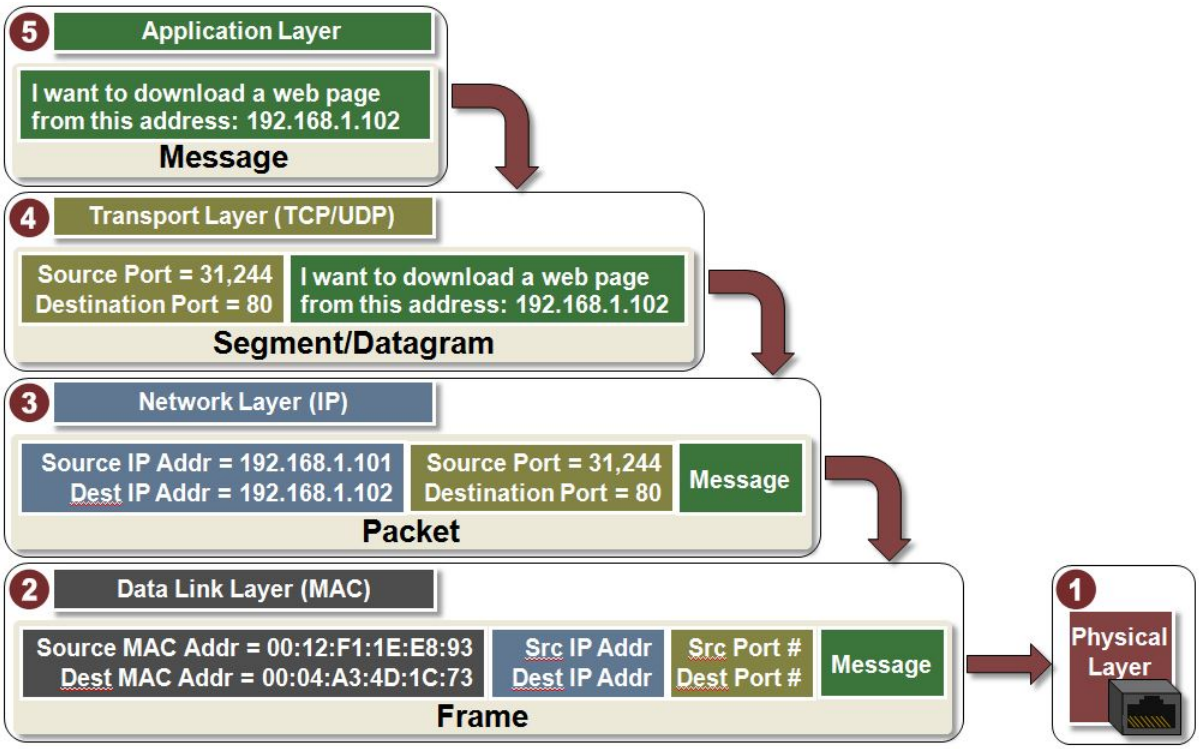


Basic Needs for TCP/IP Communication:

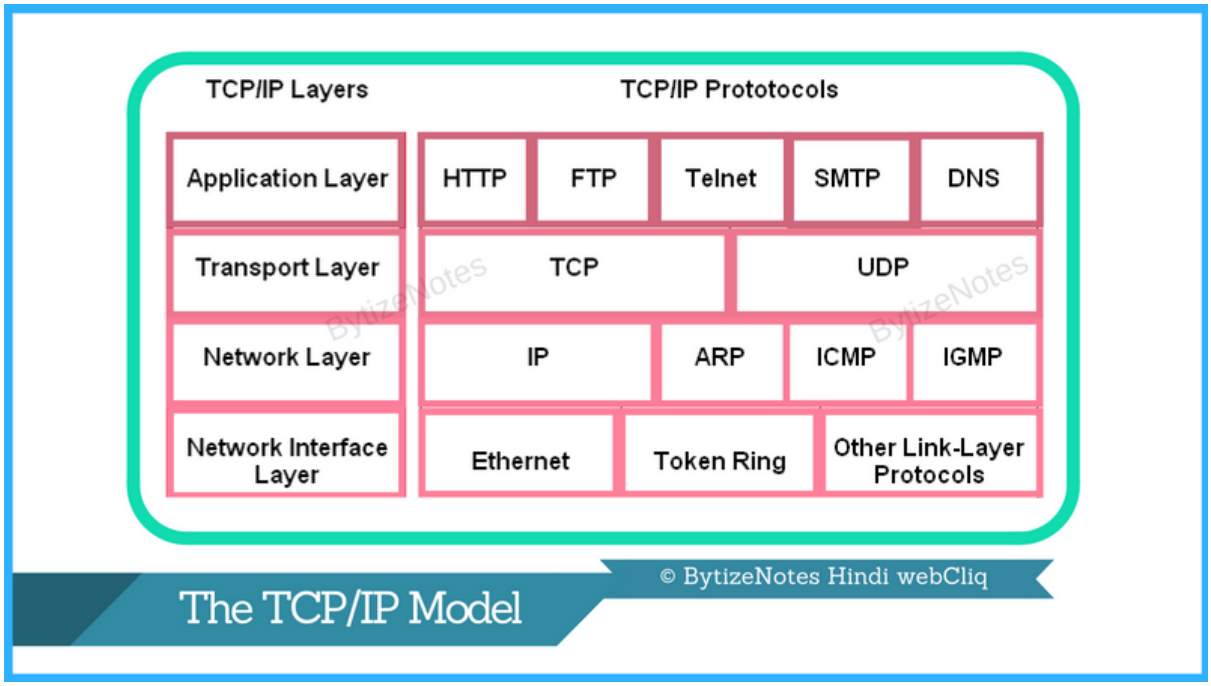


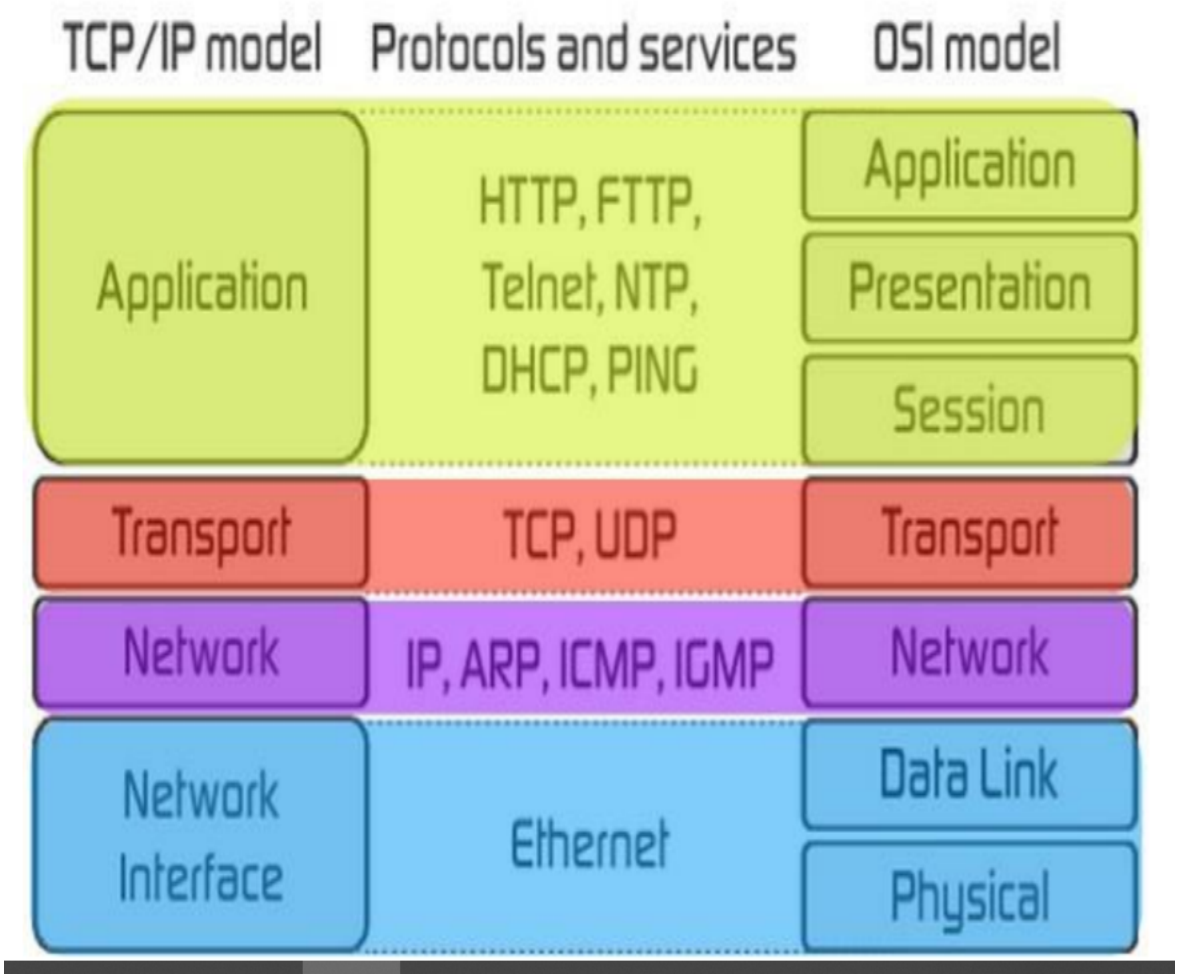

Network Host
Layer 5 requests connections to remote hosts
5 Application Layer
4 Transport Layer (TCP/UDP)
3 Network Layer (IP)
2 Data Link Layer (MAC)
Layer 1 encodes and transmits bits
1 Physical Layer


5 Application Layer
The Application layer is the group of applications requiring network communications.
Host A
Web Browser
Generates the data and requests connections
Host B
Web Server
4 Transport Layer (TCP/UDP)
The Transport layer establishes the connection between applications on different hosts.
Establishes connections with remote host
3 Network Layer (IP)
The Network layer is responsible for creating the packets that move across the network.
Transfers packets with virtual (IP) addresses
2 Data Link Layer (MAC)
The Data Link layer is responsible for creating the frames that move across the network.
Transfers frames with physical (MAC) addresses
1 Physical Layer
The Physical layer is the transceiver that drives the signals on the network.
Transmits and receives bits



Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a


TCP/IP Layers
TCP/IP Prototocols
Application Layer
HTTP
FTP
Telnet
SMTP
DNS
Transport Layer
TCP
UDP
Network Layer
IP
ARP
ICMP
IGMP
Network Interface Layer
Ethernet
Token Ring
Other Link-Layer Protocols
BytizeNotes
BytizeNotes
© BytizeNotes Hindi webCliq
The TCP/IP Model


TCP/IP model
Protocols and services
OSI model
Application
HTTP, FTTP, Telnet, NTP, DHCP, PING
Application
Presentation
Session
Transport
TCP, UDP
Transport
Network
IP, ARP, ICMP, IGMP
Network
Network Interface
Ethernet
Data Link
Physical

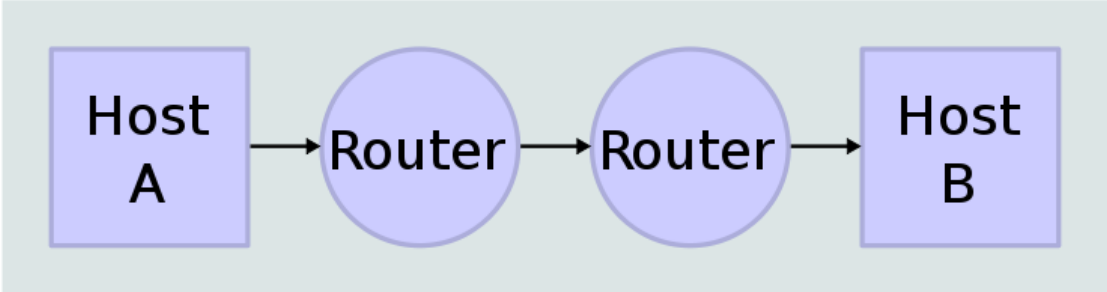
UDP v/s TCP		
Characteristics/ Description	**UDP**	**TCP**
General Description	Simple High speed low functionality "wrapper" that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms
Overhead	Very Low	Low, but higher than UDP
Transmission speed	Very High	High but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.

Difference Table : HTTP vs TCP

PARAMETER	TCP	HTTP
Acronym for	Transmission Control Protocol	Hypertext Transfer Protocol
OSI Layer	Transport Layer (Layer 4)	Application Layer (Layer 7)
Philosophy	TCP protocol is used for session establishment between two machine.	HTTP protocol is used for content access from web server.
TCP ports	No Port number	HTTP uses TCP's port number 80.
Authentication	TCP-AO (TCP Authentication	HTTP does not perform

	Option)	authentication.
Usage	TCP is used extensively by many internet applications.	HTTP is useful in transferring smaller files like web pages.
State	Connection-Oriented Protocol	Stateless but not session less
Type of Transfer	Establishes Connection between Client and Server.	Transfers records between the Web client and Web server.
URL	No URL	When you are managing HTTP, HTTP will appear in URL.
Communication	3-Way Handshake (SYN, SYN-ACK, ACK)	One-way communication system.
Use	HTTP, HTTPs, FTP, SMTP, Telnet	Most widely used for web based applications
Download speed	The speed for TCP is slower.	HTTP is faster than TCP.

Network Topology



Data Flow