



# Concept of Networking

By


Ashish Kumar

Sc-C

MC, Patna

# Contents

- ▶ Why we should learn Network & Networking?
- ▶ Introduction to computer Network
- ▶ Network topology
- ▶ OSI Model
- ▶ TCP/IP Model
- ▶ Transmission mode and Transmission Media
- ▶ How to prepare cable
- ▶ Internet
- ▶ Types of Internet Connection

- 
- ▶ Internet Vs Intranet Vs Arpanet with Milnet
  - ▶ Wireless Technology
  - ▶ Mobile Network Technology
  - ▶ Networking Protocols
  - ▶ How to setup Local Area Network
  - ▶ IP Address
  - ▶ IoT
  - ▶ Network Vulnerability % Securing Network and Networking
  - ▶ WAN Connection
  - ▶ Creating project on Networking

# Why we should learn Network & Networking?

- A NETWORK ADMINISTRATION CAN MANAGE -
- EDUCATION SERVICES.
- FINANCE AND INSURANCE
- ADMINISTRATIVE AND SUPPORT SERVICES.
- INFORMATION.
- COMPUTER SYSTEM DESIGN AND RELATED AREA.
- ENTERTAINMENT.
- MEDICAL.

# Introduction to computer Network.

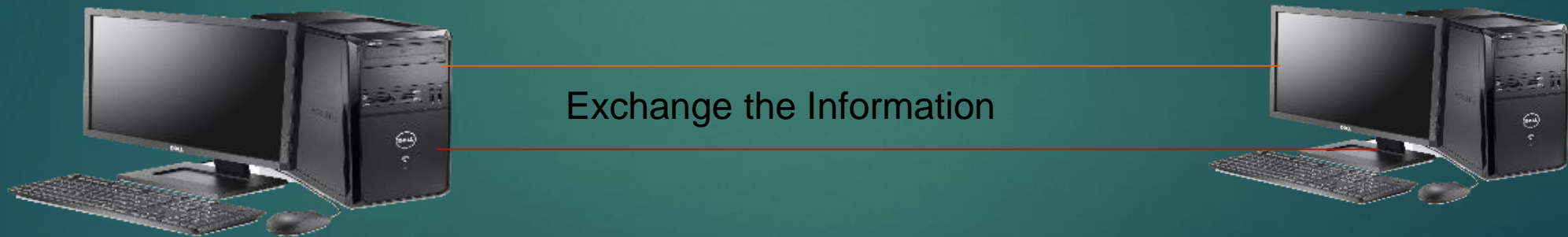
## ➤ What is network?

Network is a connection of multiple network devices via any medium is called network.



# What is Networking?

Networking is process of communication/Transmission of data between devices is called networking.

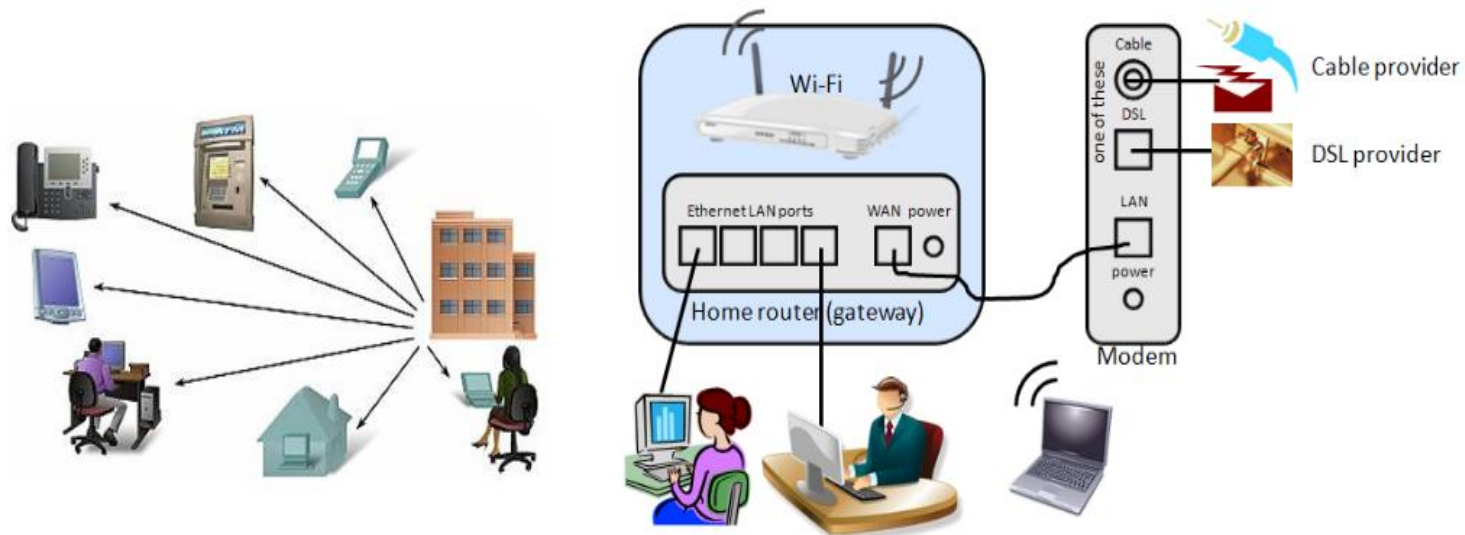


# What is Inter-networking.?

- ▶ Connect more than two network is known as Inter-networking.

## InterNetworking Devices

Video tutorials [www.arkit.co.in](http://www.arkit.co.in)





# Advantage of network and networking ?

1. Network admin can share resources over a LAN or WAN
2. Share Printer
3. Share file folder or data

## What is Point to point and Server client model ?

P2P Model – In this model only two devices are connected to each other is known as P2P Model





# Client-Server Model

The client – server model is the relationship between two computer in which one, the client, makes a service request from another, the server.

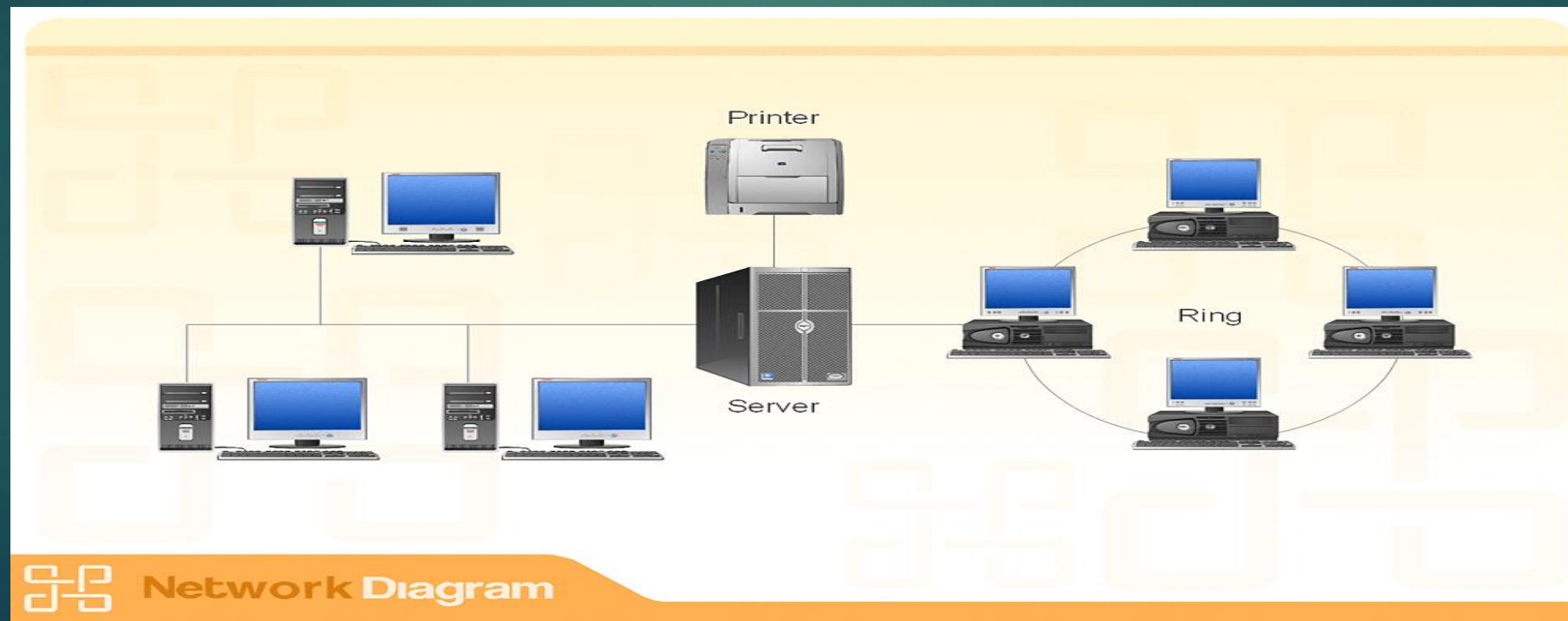


# What is Computer Network ? Types of Computer Network?

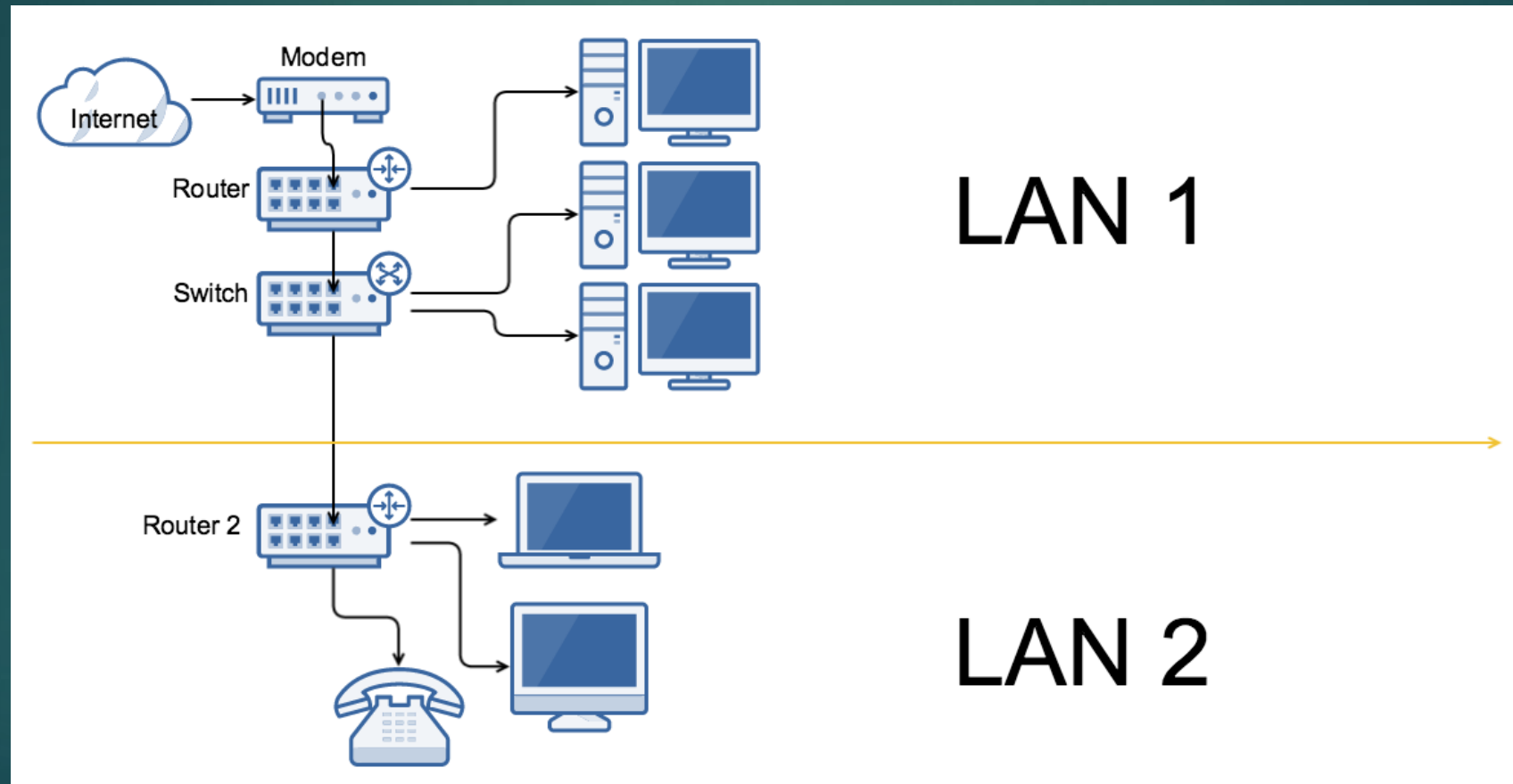
A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purposes of sharing resources located on or provided by the network nodes.

## LAN, MAN, WAN, CAN, PAN

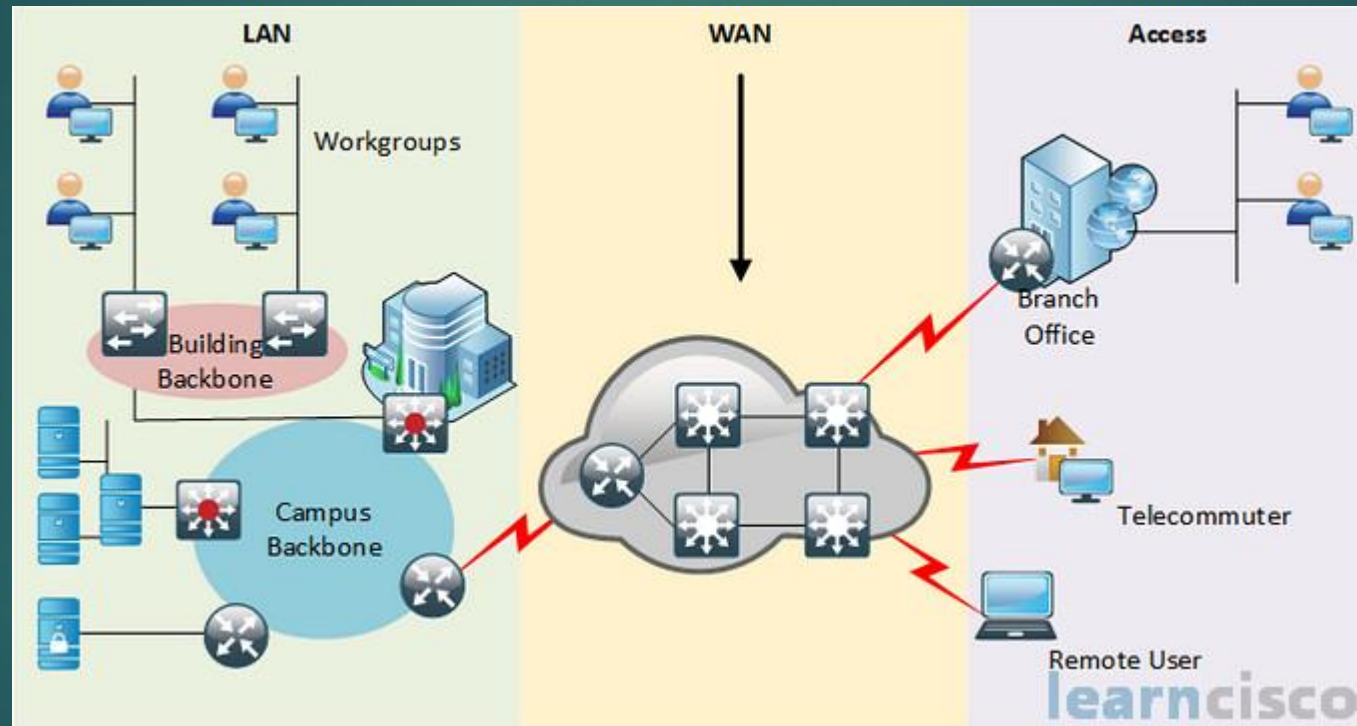
**LAN – Stands for Local Area Network. It established over a local area network like home, small office etc.**



**MAN** – It stand for metropolitan area network, established over two LAN or more than two



**WAN – It stand for wide area network it established geographical communication.**



# Advantages & Disadvantages of LAN, MAN, WAN, PAN, CAN

We can connect and share network resources and data or info over a local area or wide area network.

## Networking Terminology

1. **Node** - Any system or device connected to a network is also called node. For example, If a network connects a file server, five computer and two printer, there are eight node on the network. Each device on the network has a network address, such as a MAC address, which uniquely identifies each device.
2. **Hop** – In wired computer networking, including the internet, a hop occurs when a packet is passed from one network segment to next....The hop count refers to the number of intermediate devices through which data must pass between source and destination.
3. **Terminal** – Terminal is an interface where we can input instruction ( it is a command line interface)

## 4. Command

Command is a set of instruction which is used for particular task. In computing, a command is a directive to computer program to perform a specific task. It may be issued via a command –line interface, such as shell, or as input to a network service as part of network protocol, or as an event in a graphical user interface triggered by the user selecting an option in a menu.

## 5. SHELL

A shell is a computer programme that represent a command line interface Which allow you to control your computer using command. Entered with a keyboard instead of Controlling graphical user interface (GUIs) With a mouse keyboard combination.

## 6 . Virus

A virus is also a programme Which is very harmful for our system and information. It is a bad programme. An virus deleted our file or data.

## 7. Attack.

It is an activity which is performed by hacker or attacker to hack the data or confidential in formation.

## 8. Hacker

A person who have extraordinary knowledge in computer field and Hacker is bad person. Because he hacks the information, of victim or hack the confidential information.



## 9. Attacker

Attacker is also a hacker in computer technology.

## 10. Phishing

Phishing is a process to have the information online by hacker. Phishing is a site cloner or it is a technique which is used by hacker or attacker to create a fake website of any original site.

## 11. Vulnerability

Vulnerability is a technical term. In this we can find the lack of any computer programme services Or user can analyze the security setting in any computer machine.

## 12. OS

OS stand for operating system and It is used to create user interface between user and hardware. Also, we can say it's the enable or activate the hardware and provide interface

## 13. Firmware

It's also program also known as firmware. It is a small programme which is used to boot or activate the hardware of machine. Firmware is a software programme or set of instruction programmed on a hardware device. Firmware is Typically stored in a flash ROM

## 14. BIOS

The BIOS Software has a number of different role. But it's more important Role is to load the operating system when you turn on your computer.



## 15. Bandwidth.

The maximum amount of data transmitted over Internet connection in a given amount of time.  
Calculated in Mbps Megabits per second.

## 16. MBps

Megabytes per second

## 17. Mbps

Megabits per second (1 MBps = 8Mbps)

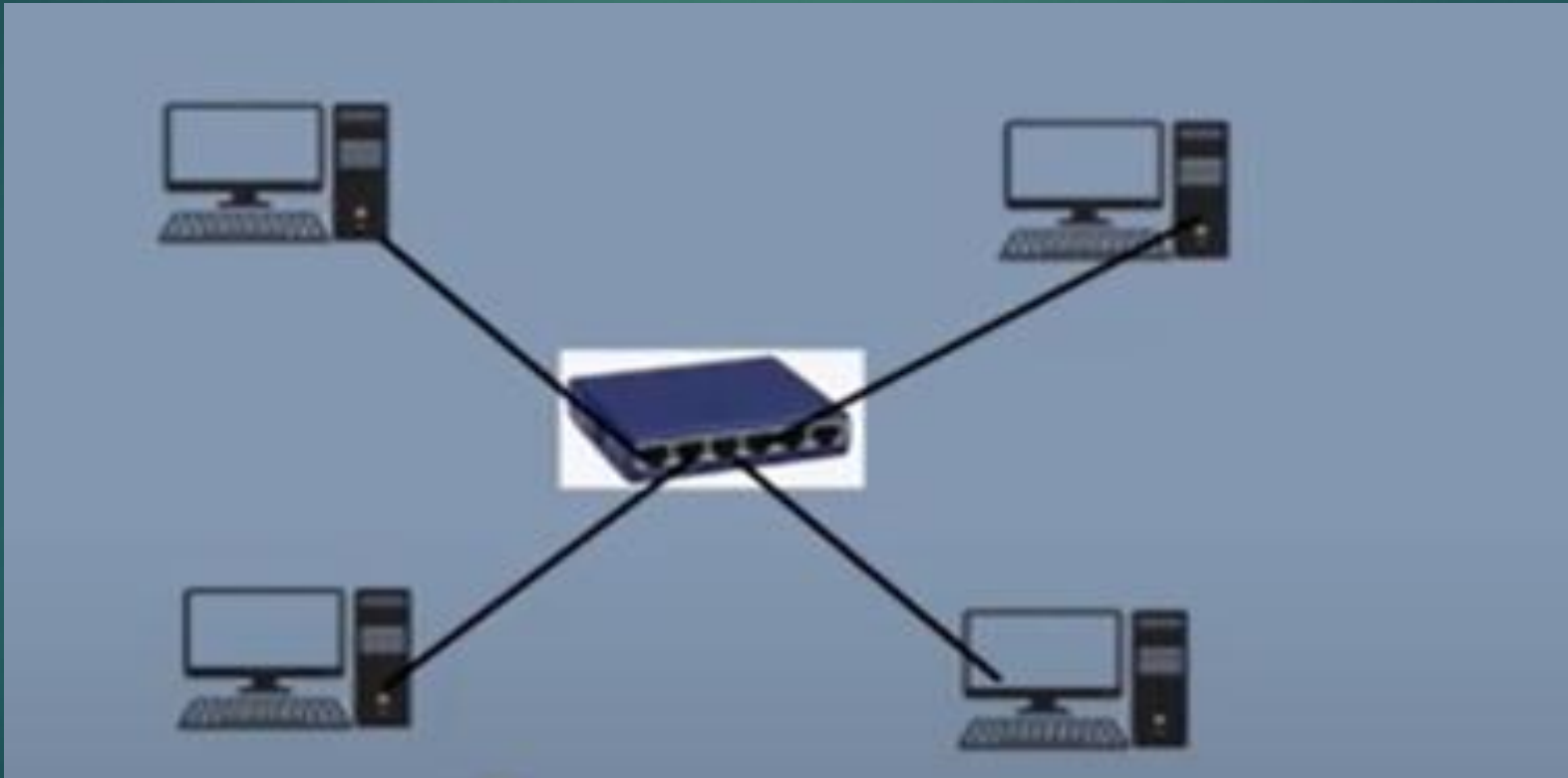
## 18. RF versus analogue signal.

RF stand for radio frequency. An analogue is also a signal used to connect and share the info from one point to another.

# Identifying an working of networking devices.

## Hub (Advantages and disadvantages)

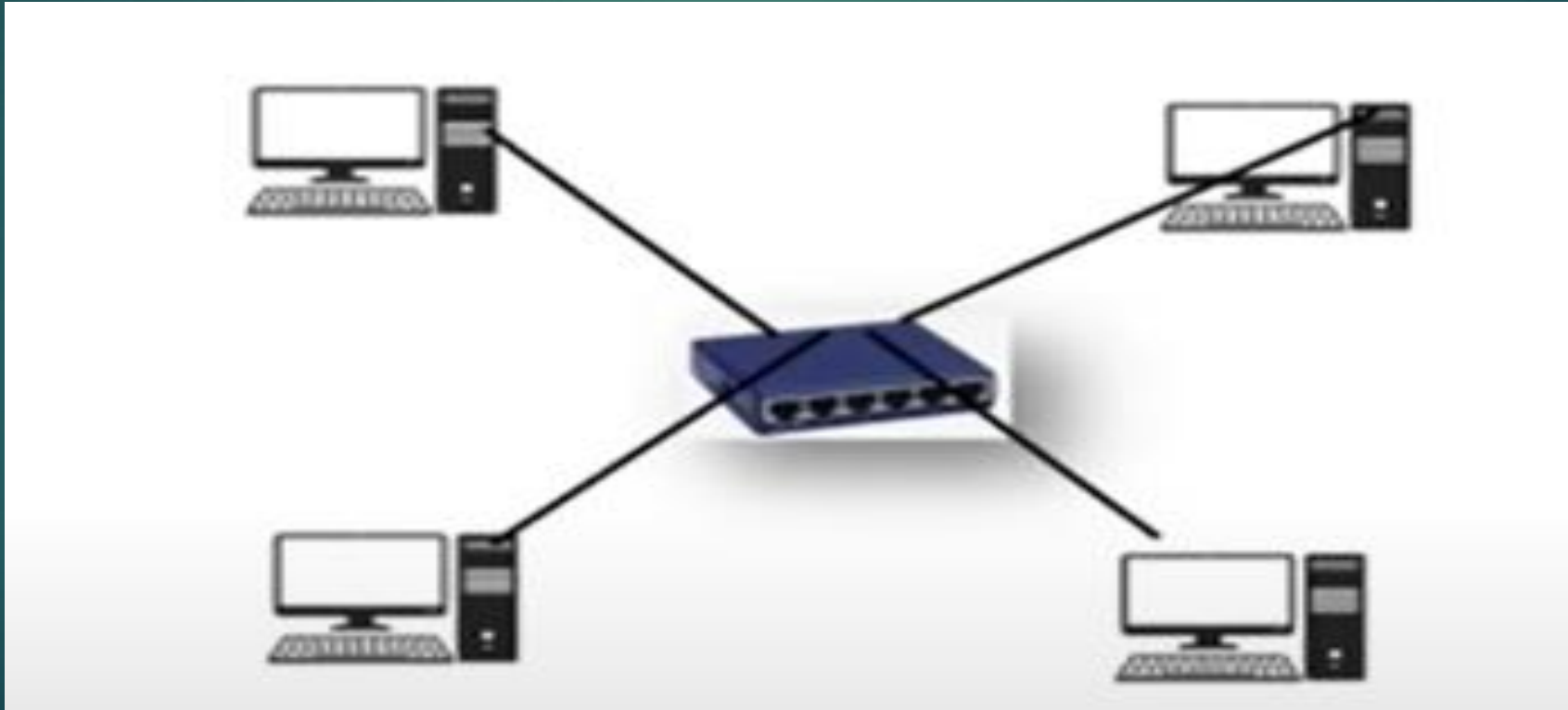
Hub is a networking device Which is used to connect multiple network device. As a central point and also it is used to connect Single Network connection segment and distribute it to a multiple device.



# Switch

Switch is also connecting multiple device in a LAN and connect single Network segment and distribute it into a multiple network device.

Centralized management connection, but switch is better than hub



# Difference between Switch and Hub

HUB	SWITCH
They operate in a physical layer of OSI model.	They operate in a data link layer of OSI model.
It is an not intelligent network device that send message to All port.	It is an intelligence network device that send message to
It primarily broadcast message.	It is supported, 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 port.	Collision do not occur since the communication is full duplex.
They are passive device. They don't have any software associated with it.	They are active devices equipped with network software.
They generally have fewer port of 4 or 8 or 12 port.	The number of ports is higher 4, 8,12 ,24, 48.

# Switch

## L2 and L3 switch.

L2 mean unmanageable switch because it has no features of routing.

And L3 is manageable switch and used to configure the routing protocols.

L3 Switch is costly from L2 switch.

L3 Switch is more secure, reliable for networking.



L2 SWITCH



L3 SWITCH

# SWITCHING

In this technology we can create a reliable communication path between source to destination.

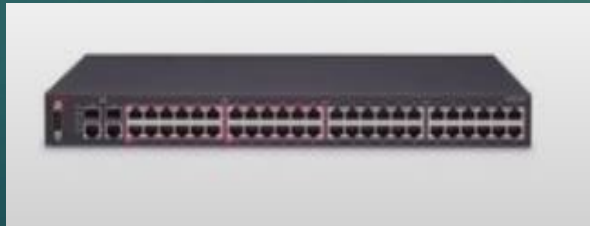
Circuit switching.- Method to end-to-end communication and establish the dedicated path.

Packet switching. - In this method we learnt to process of communication.(Switching)

1. Datagram Switching
2. Virtual Circuit Switching

Datagrams switching - In this process, one node send the data to another node independently. There is no dedicated path. Device are free to communicate the destination via any path.

1. Virtual packet switching.- Network admin can create a dedicated path before forward the packet



# Types of data transmission. ?

1. Unicast.
2. Multicast.
3. Broadcast

## What is FCS?

FCS stands for frame check sequence. In this process we learn the Frame checking process while transmitting the data.

## CAM Table

CAM Stand for content address memory. It is a switch technology and its Instore the IP and Mac table details or switching table details in switch technology over a network.





# ROUTERS

Router is L3 networking device and it is used to route the packet over the network.

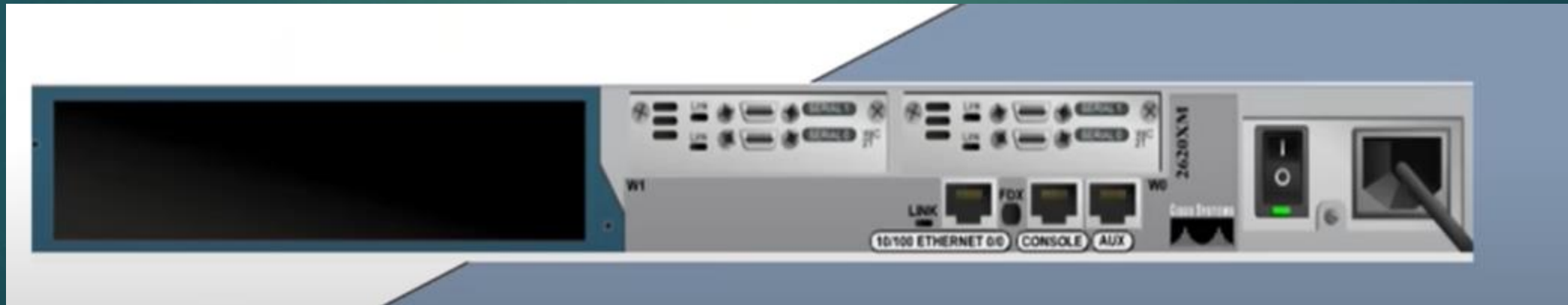
There is mainly two type of routers.

Router is a networking and L3 device which is used to manage the WAN network as well as LAN also.



# PORTS OF CISCO ROUTERS

1. Ethernet port - Which is used to connect PC or host or switches
2. Fast Ethernet - Which is used to connect PC or host or switches.
3. Gigabit Ethernet - Which is used to connect PC or host or switches.
4. Serial port.- It is used to connect router to router.
5. Consol Port - Used to access the router for configuration.
6. Auxiliary port - Used to connect modem. Call of Duty.



# CISCO ROUTER

To manage network.

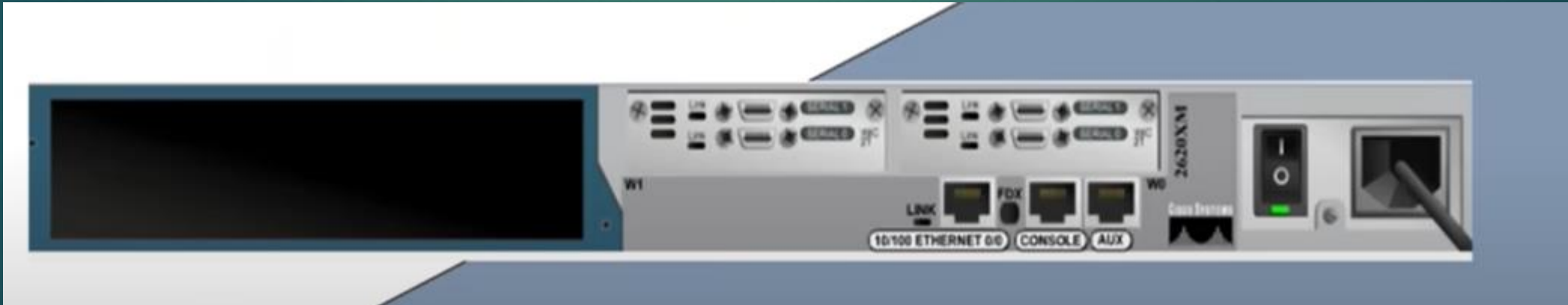
Connect different network IDs.

Provide best path.

Avoid collision and manage broadcast.

Traffic control and filter the packet.

Provide data security using various type of encryption protocols.



# CISCO vs BASIC ROUTER



CISCO ROUTER



BASIC ROUTER

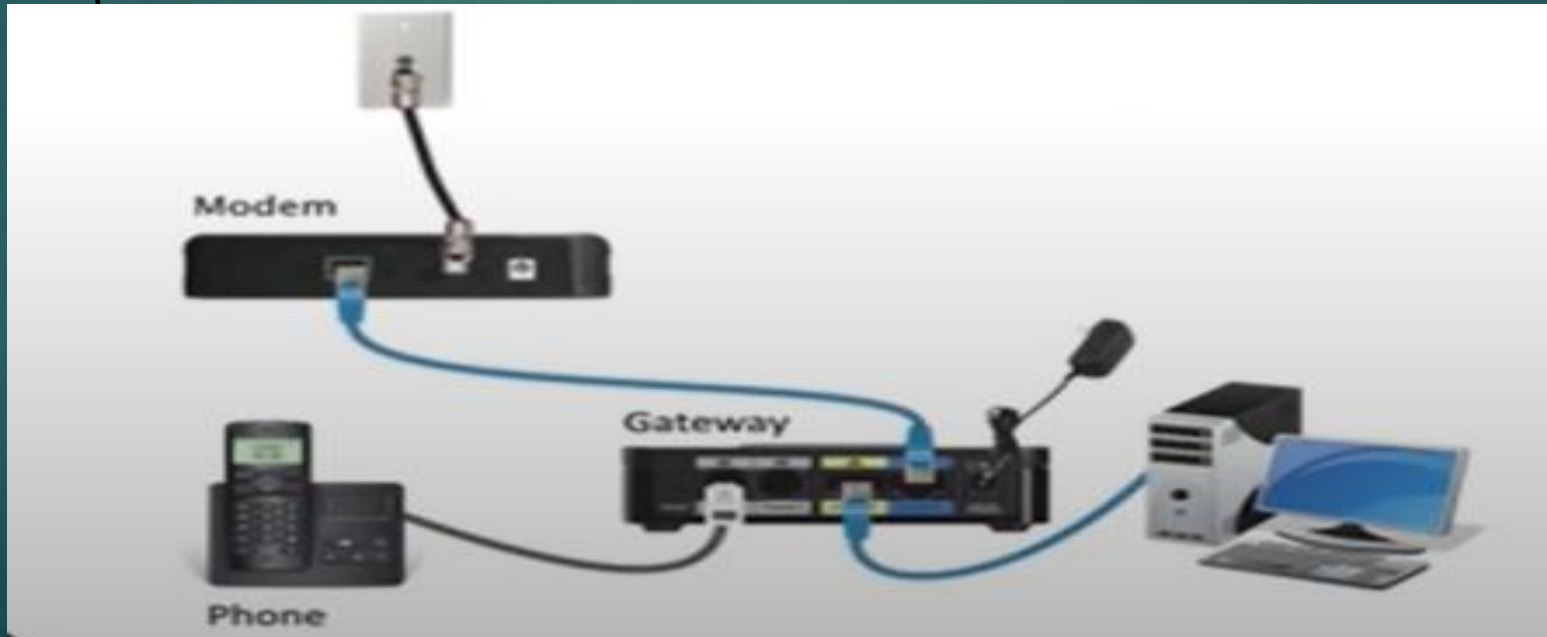
# MODEM

Modem is short for modulator demodulator.

It is a hardware component that allow a computer or other device such as router or switch to connect to the Internet.

It Convert or modulate an analogue signal from a telephone or cable wire to digital data(1s and 0s) that a computer can recognize.

Similarly, it convert digital data from a computer or other device into analogue signal that can be sent over a standard telephone line.

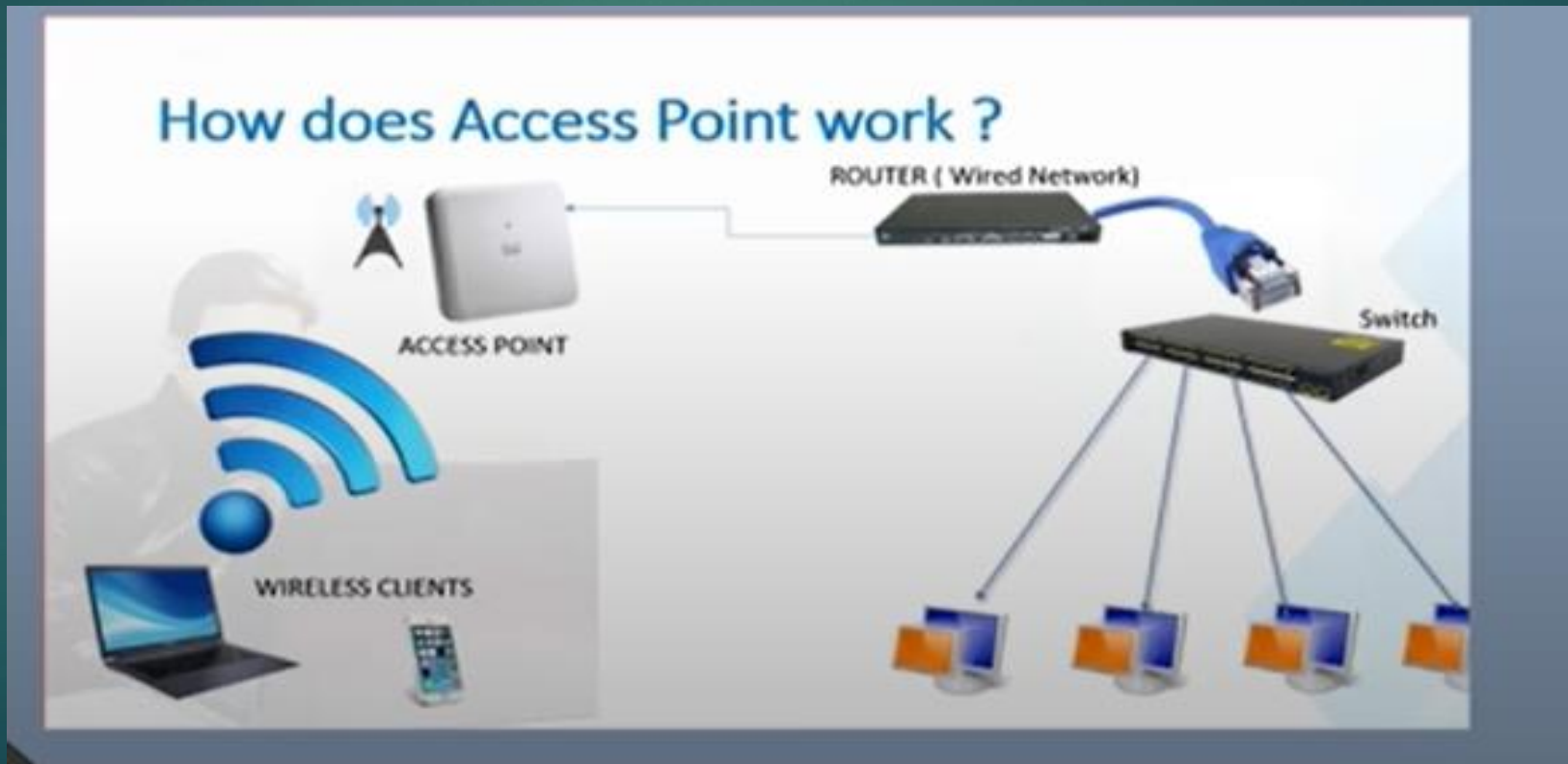


# ACCESS POINT

Access point is used to increase the network segment length over wired or wireless.

An Access point is a device that create a wireless local area network or WLAN, usually in office or large building.

An access point connect to a wired router, switch or hub via Ethernet cable and project WiFi signal to a designated area.





# FIREWALL

## Firewall and its types (NGFW, Palo Alto)

Firewall is a security point Which is used to filter the packet for incoming and outgoing connection and protect our network infrastructure.

There is two types of firewall.

1. Software based firewall.
2. Hardware based firewall.

1. Software based firewall.- Its built in technology in all OS and user can configure it using control panel.
2. Hardware based firewall - It is more secure and reliable for network security. But it is a costlier.



It has more features line.

User can monitor network device and create port security.

User can configure and control the port and access permission over a network.



# NIC

NIC stand for network interface card it is used to connect Internet to PC.

Types of NIC

1. Wired
2. Wireless



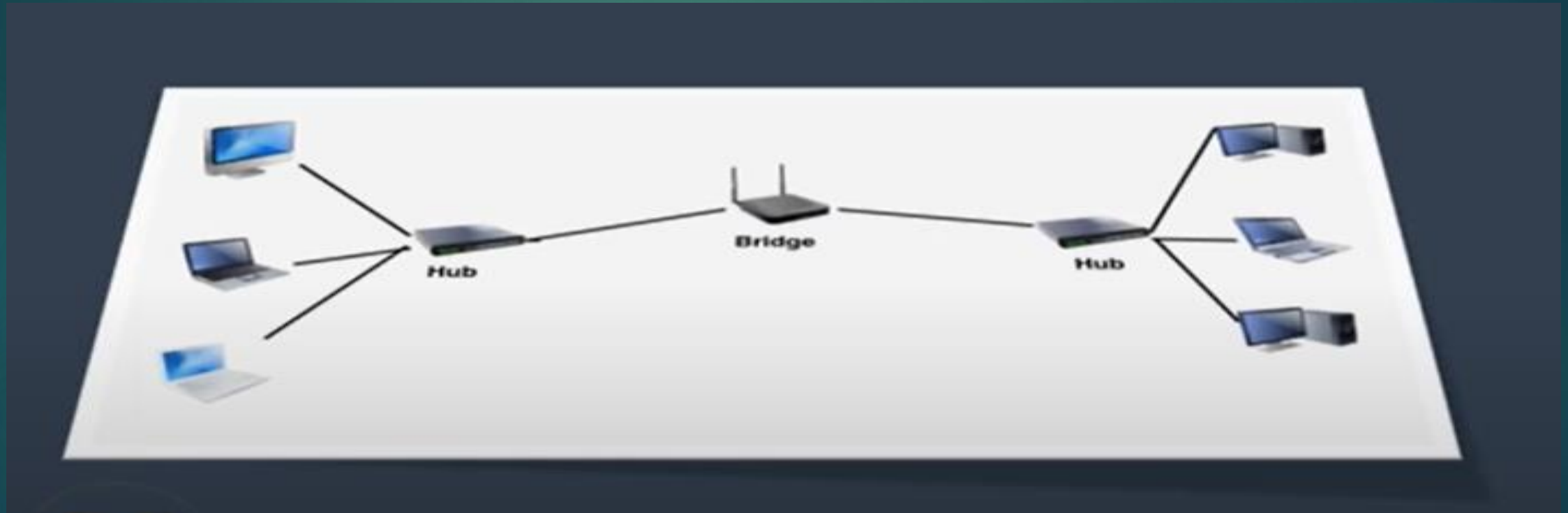
# SERVER

Server is a highly configure devices computer system which is used to provide services over LAN or WLAN.



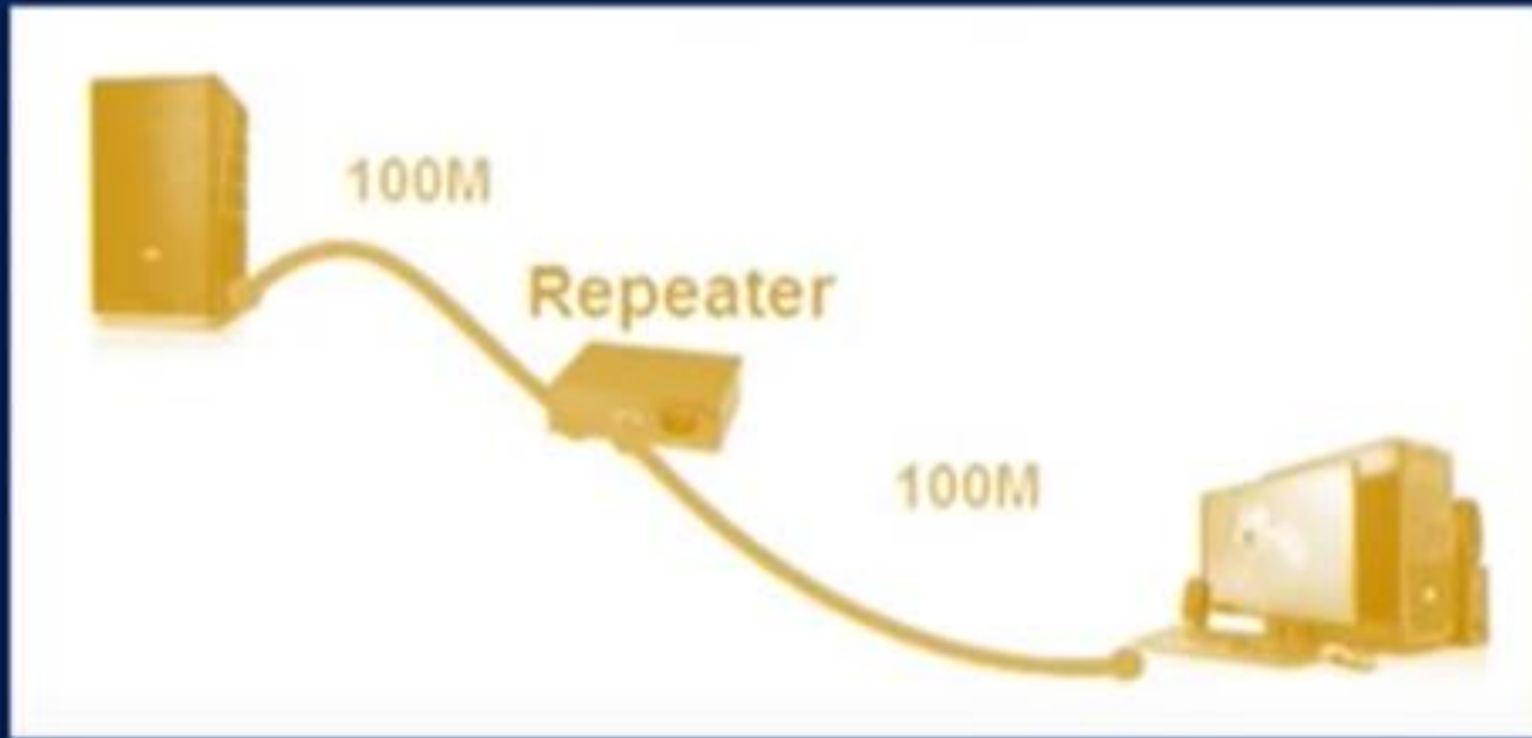
# BRIDGE

A network bridge is a computer networking device that creates a single aggregate network from multiple communication network or network segments. The function is called network bridging. Bridging is distinct from routing.



# REPEATER

In telecommunication, a repeater is an electronic device that receives a signal and retransmits it. Repeater are used to extend transmission so that the signal can cover longer distance or be received on the other side of an obstruction.



# LAPTOP/DESKTOP



NOTEBOOK/LAPTOP



DESKTOP

## PRINTER

Printer is a hardware device which is used to print the information.

1. Basic Printer
2. Network Printer



# RACK





# What is Topology?

Topology is an architecture or arrangement of networking devices over a network is known as topology

Types of topology.

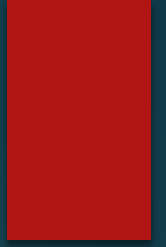
1. Physical topology.
2. Logical topology.

## Physical Design Consideration

- **Network application**
  - The type of network you plan to run will influence the cable you choose.
- **Upgrades**
  - Anticipate changes and upgrades in equipment and applications.
- **Life span**
  - Expect 10 years minimum and 20 years maximum.
- **Distance**
  - Review the maximum distance between your network switches and the farthest desktop.
- **Cable routing**
  - Consider the available space for running cables in the floor and ceiling.
- **Existing cable**
  - Is there existing or abandoned cable that needs to be removed?
- **EMI (electromagnetic interference)**
  - Don't forget to check for it.
- **Environment**
  - Any physical limitations that could affect your cable choice?



# BUS TOPOLOGY



All devices are connected to a single backbone cable.

One device is a failure, creating a problem in the entire network.

In bus topology, main cable and all the devices are connected to this main cable through one drop lines. There is a device called TAP that connect the drop line to main cable. Since all the data is transmitted over the main cable. There is a limit of drop lines and the distance a main cable can have.



## **Advantages of bus topology.**

1. Easy installation. Each cable need to be connected with a backbone cable.
2. Less cables required then mesh and star topology.

## **Disadvantages of bus topology**

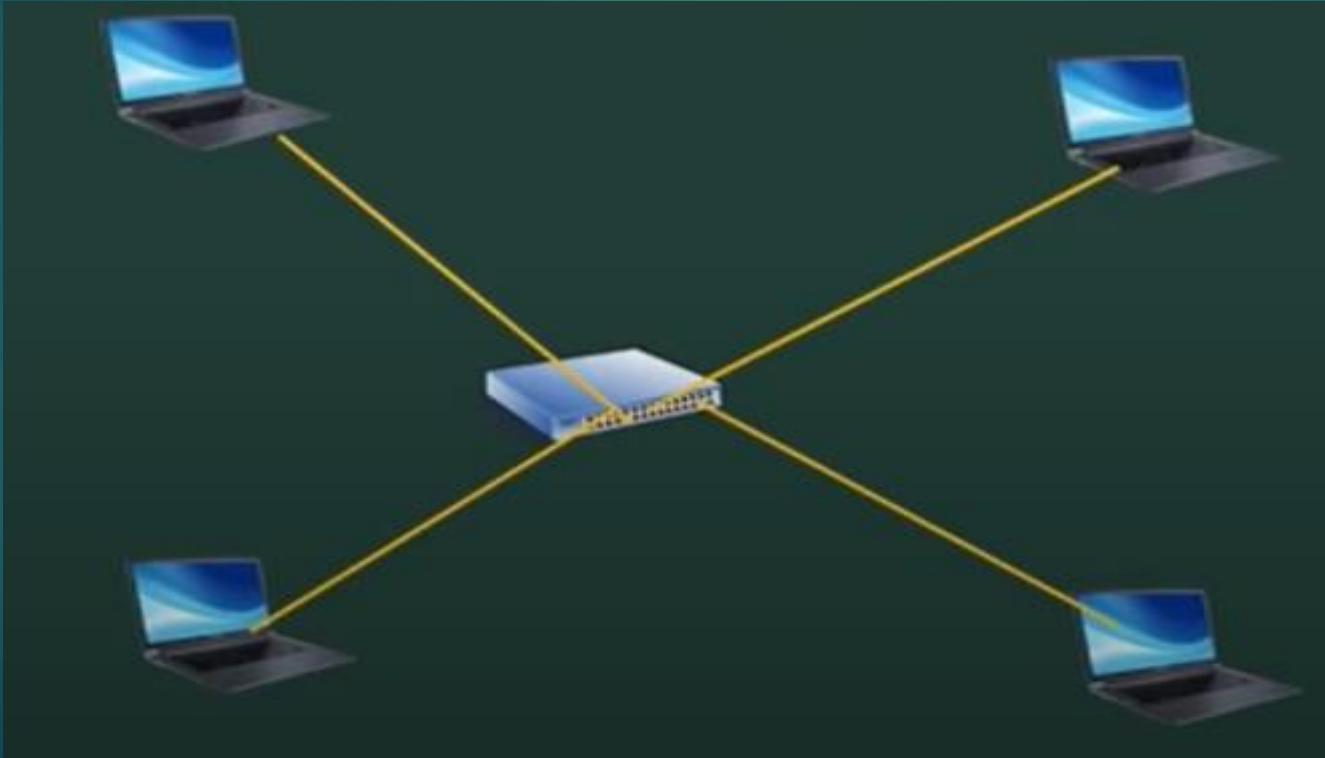
1. Difficulty in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with a backbone cable

# STAR TOPOLOGY

Star topology does not allow direct communication between devices or device must have to communicate through hub OR switch.

If one device want to send data to other device. It has to first send the data hub and then the hub transmit the data to designated device.

Best topology ever for networking of multiple device over a network.



## **Advantages of star topology.**

Less expensive because each device only need one I/O port and needs to be connected with hub with one link.

Easier to install.

Less amount of cable required because each device need to be connected with the hub only.

Robust if one Links fails another link will work just fine.

Easy fault detection because the link can be easily identified.

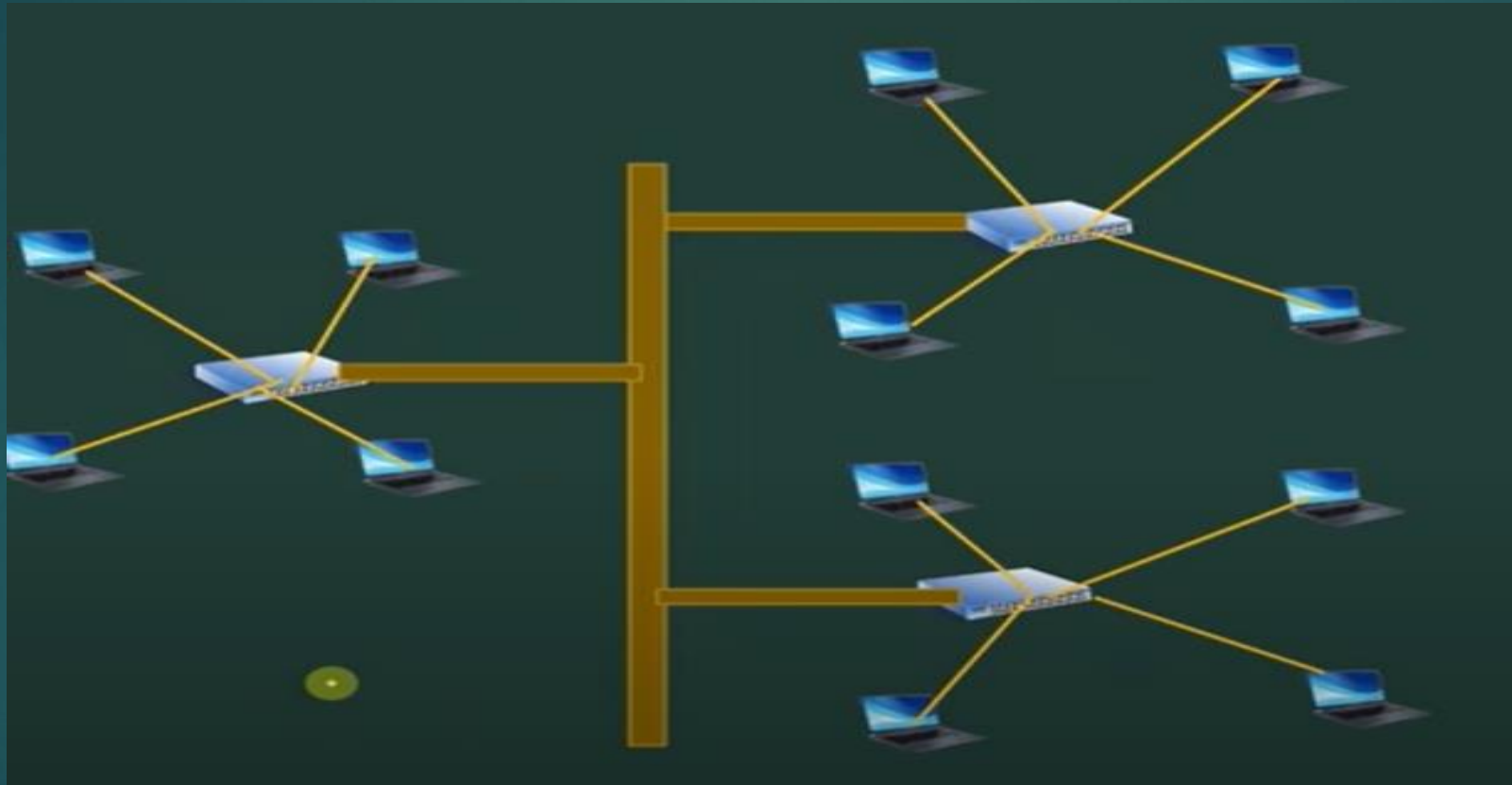
## **Disadvantage of star topology.**

If hub goes down, everything goes down. None of the devices can work without hub.

More resources and regular maintenance because it is the central system of star topology.

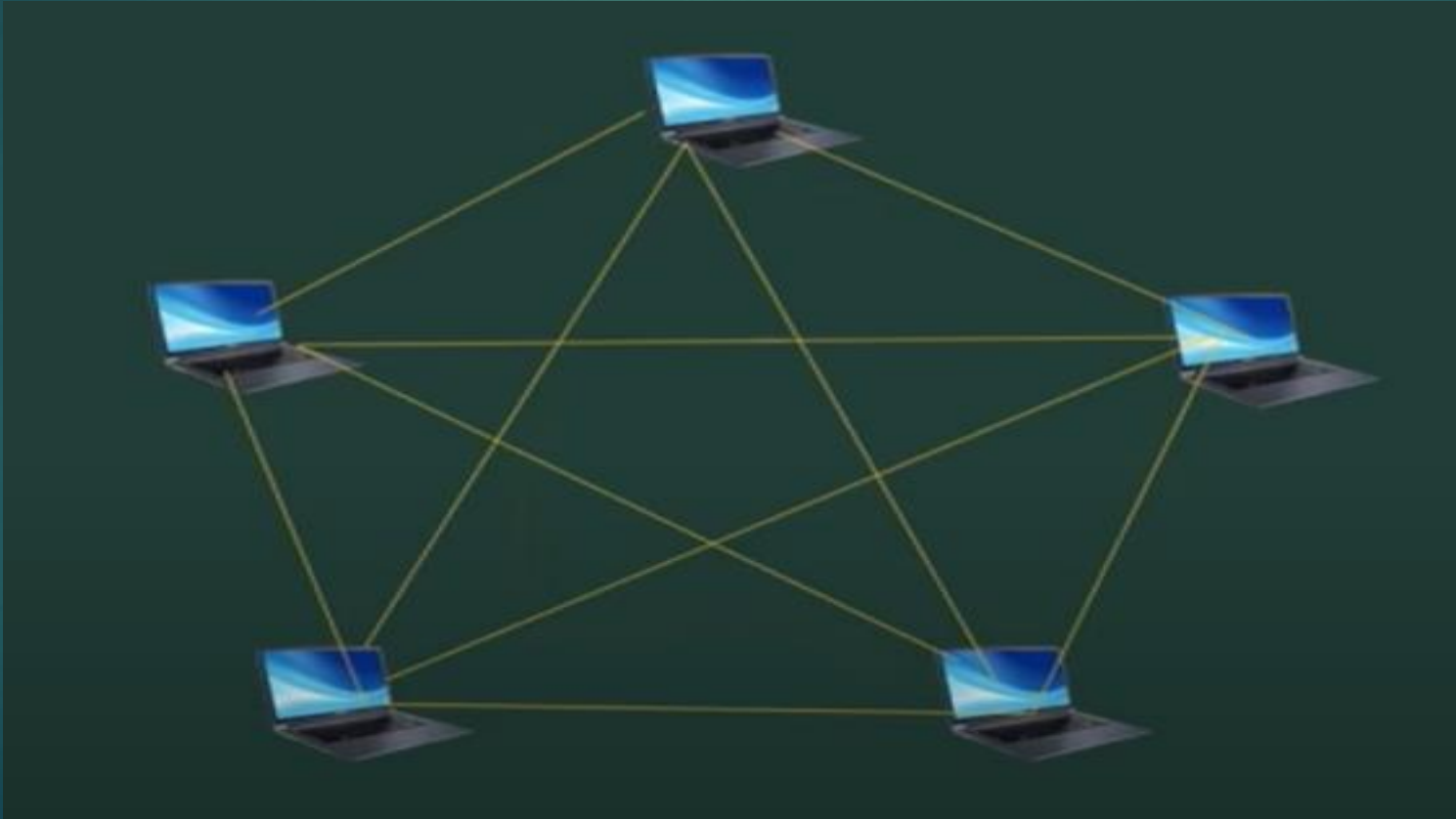
# TREE TOPOLOGY

It is the combination of bus and star topology and also it has features of both.



# MESH TOPOLOGY

In mesh topology, each devices connected to every other devices on the network through a dedicated point to point link. When we say dedicated, it means that the link only carry data for the two connected devices only.



# Advantages of mesh topology

No data traffic issue as there is a dedicated link between two devices, which means the link is only available for those two devices.

Mesh topology is reliable and robust as failure of one link does not affect other links and the communication between other devices on the network.

Mesh topology is secure because there is a point to point link that unauthorized access is not possible.

Fault detection is easy.

# Disadvantages of mesh topology

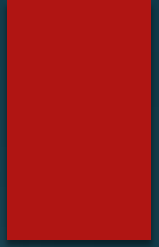
Amount of wires required to connect each system is Tedious and Headache

Since each device need to be connected with other device number of I/O port required must be huge.  
Scalability issue, because a device cannot be connected with large number of device with a dedicated point to point link.



# HYBRID TOPOLOGY

Hybrid topology is a collection of two or more topology with each other is known as hybrid topology.



## Advantages of hybrid topology

We can choose the topology based on requirements, for example. The scalability is our concern then we can use star topology instead of bus topology.

A scalable as we can further connect other computer networks with the existing network with different topologies.

## Disadvantages of hybrid topology

Fault detection is difficult

Installation is difficult.

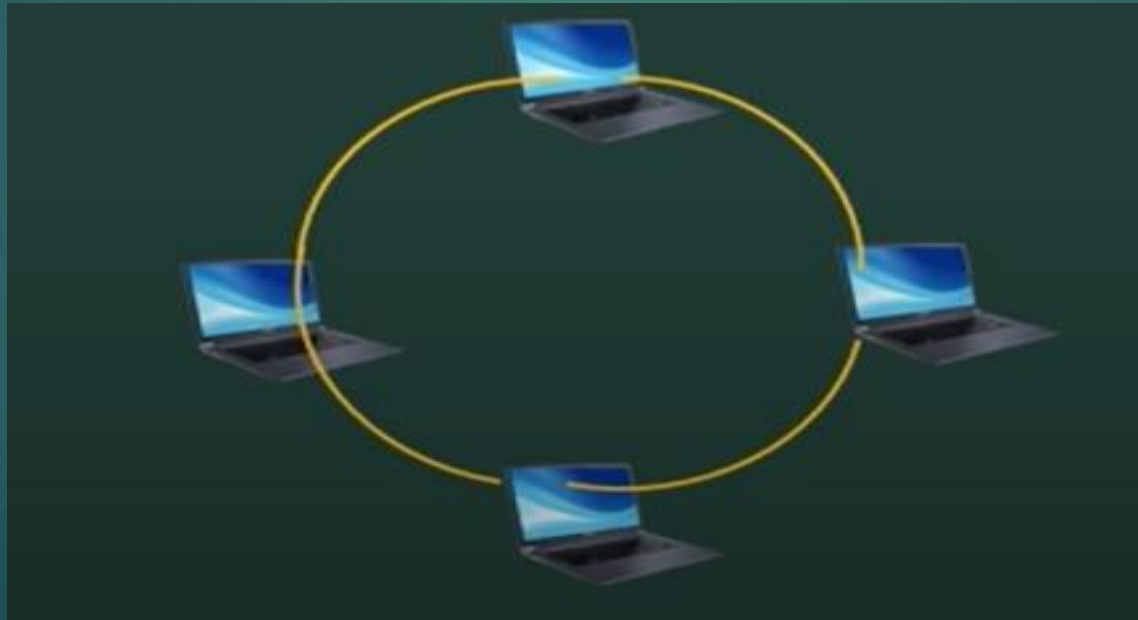
Design is complex, so maintenance is high, thus expensive.

# RING TOPOLOGY

Topology each devices connected with the two devices on either side of it.

There are two dedicated point to point link. A device has been the devices on either side of it. This structure form a ring thus it is known as ring topology.

If a device wants to send data to another device then it sends the data in One Direction, Each device in the ring topology has a repeater. If the received data is intended for other device, then repeater forward this data until the intended device received it.



## **Advantages of ring topology.**

- ▶ Easy to install.
- ▶ Managing is easier as to add or remove a device from a topology. Only two link are required to be changed.

## **Disadvantage of ring topology.**

- ▶ A link failure can fail the entire network as the signal will not travel forward due to failure.
- ▶ Data traffic issue. Since all the data is circulating in a ring.

# **DOUBLE RING TOPOLOGY**

In this topology, networking devices are connected to each other with a closed loop, while dual ring technology.

# OSI MODEL

- ▶ Introduction to OSI model.
- ▶ Layers of OSI model?
- ▶ Application layer.
- ▶ Presentation layer.
- ▶ Session layer.
- ▶ Transport layer.
- ▶ Network layer.
- ▶ Data link layer.
- ▶ Physical layer.
- ▶ How to Check Transmission. (USE CPT for live demonstration)



India

Sender



USA

Receiver

Application

Presentation

Session

Transport

Network

Data Link

Physical



Amitabh



Paresh



Shahrukh



Tonny



Nana



Dharmendra



Pankaj

Application

Presentation

Session

Transport

Network

Data Link

Physical

Pause (k)



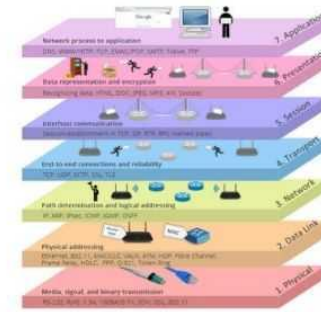
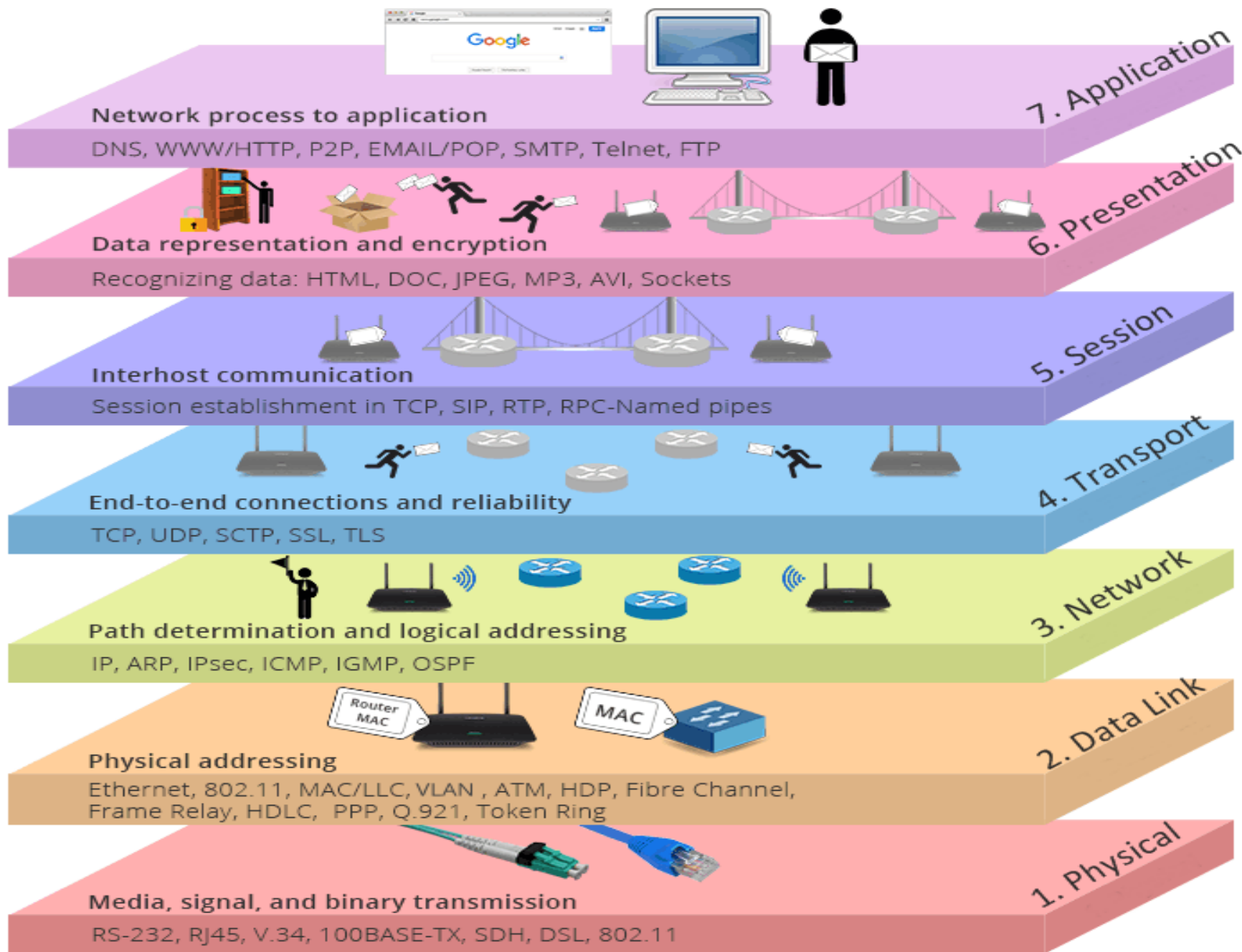
# Introduction to OSI model

OSI stand for open system interconnection and it is used to know the flow of data from A point to B point And OSI model was developed by International Organisation of Standardisation (ISO) in 1984, and it is now considered as architecture model for the Inter-computer communications

## Characteristics of the OSI model

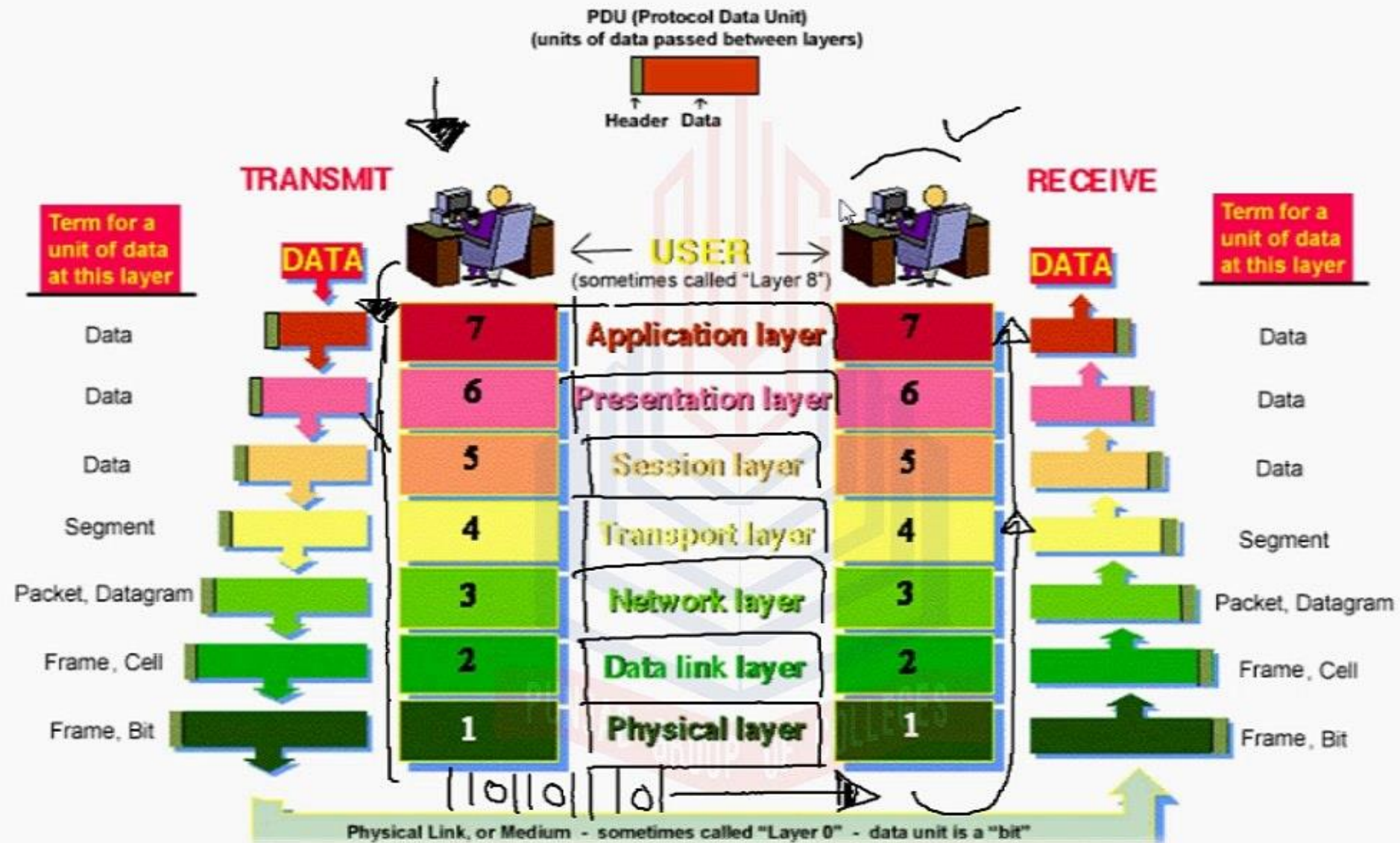






## The 7 Layers of OSI Model

# THE 7 LAYERS OF OSI





videoplayback.mp4

## 7 - Application Layer

An application layer is an abstraction layer that specifies the shared communications protocols and interface method used by hosts in a communication network. The Application layer abstraction is used in both of the standard model of computer networking: The Internet Protocol suite (TCP/IP) and the OSI model.

## 6 - Presentation Layer

The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.

## 5 - Session Layer

Session Layer protocol is used to check the session between end user.

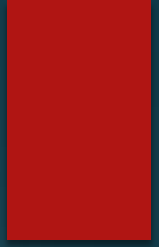
The session layer provides the mechanism for opening, closing and managing a session between end user application processes.

In cases of connection loss, this protocol may try to recover the connection. If a connection is not used for a long period, the session layer protocol may close it and reopen it.

Ping Command is used to check session is active or not.



# 4 - Transport Layer



Transport layer Protocol is showing the transmission process and information.

Used two protocol to carry the info/packets.

- ▶ The best known transport protocol of the Internet Protocol suite is the Transmission control Protocol (TCP).
- ▶ It is used for connection oriented transmission, where as the connectionless User datagram protocol (UDP) is used for the simpler messaging transmission.
- ▶ TCP is the more complex protocol, due to its stateful design Incorporating reliable transmission and the data stream services. Together, TCP and UDP compromise essentially all traffic on the Internet and are the only protocols implemented in every major Operating system.

# What Services can the transport layer provide ?

- ▶ **Connection oriented communication** : - The weakness of this method is that for each delivered message, There is a requirement for an acknowledgement adding considerable network load compared to self error correcting packets. The repeated request cause significant slowdown of network speed when defective byte stream or data grams are sent.
- ▶ **Same order delivery** :- Ensure that packet are always delivered in strict sequence by assigning them a number.
- ▶ **Data integrity** : - Using Checksums, the data integrity across all the delivery layers can be ensured. The checksum guarantee that the data transmitted is the same as the data received and that is not corrupted, missing or corrupted data can be resent by requesting retransmission from other layers.
- ▶ **Flow control.:** - ensure that the data is sent at a rate that is acceptable for both sides by managing data flow.
- ▶ **Traffic control.:** - Digital communication network are subject to bandwidth and processing speed restriction which can Mean huge amount of potential for data congestion on the network.
- ▶ **Multiplexing.:** - This multiplexing allows the use of simultaneous application over network, such as when different Internet browser are open on the same computer.

# 3 - Network Layer

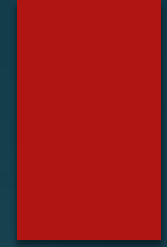
Network layer manages options pertaining to host and network addressing. Managing sub network and Internetworking.

Functions: -

- ▶ Addressing devices and networks.
- ▶ Populating routing tables or static routes.
- ▶ Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- ▶ Internet working between two different subnets.
- ▶ Delivering packet to destination with best effort.
- ▶ Provide connection oriented and connectionless mechanism



# 2 - Data Link Layer



Data link layer is responsible for Mac addressing and LLC control checking.

Data link layer is responsible for converting data stream to a single bit by bit and to send that over the underlying hardware.

At the receiving end data link layer, pick up data from hardware which are in the form of electrical signals. Assemble them in a recognizable frame format and handover to upper layer.

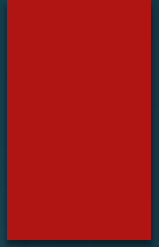
Data link layer has two sub layers:

1. Logical link control.: Flow control and error control.
2. Media. Access control : Physical address or permanent address for media control.

Functionality of data link layer.

1. Framing.
2. Addressing
3. Flow control.
4. Error control
5. Multi access
6. Synchronization.

# 1 - Physical Layer



Maintain the physical connectivity between networking devices.

This layer defines the hardware, equipment, cabling, wiring. Frequency, pulse is used to represent binary signals. etc.

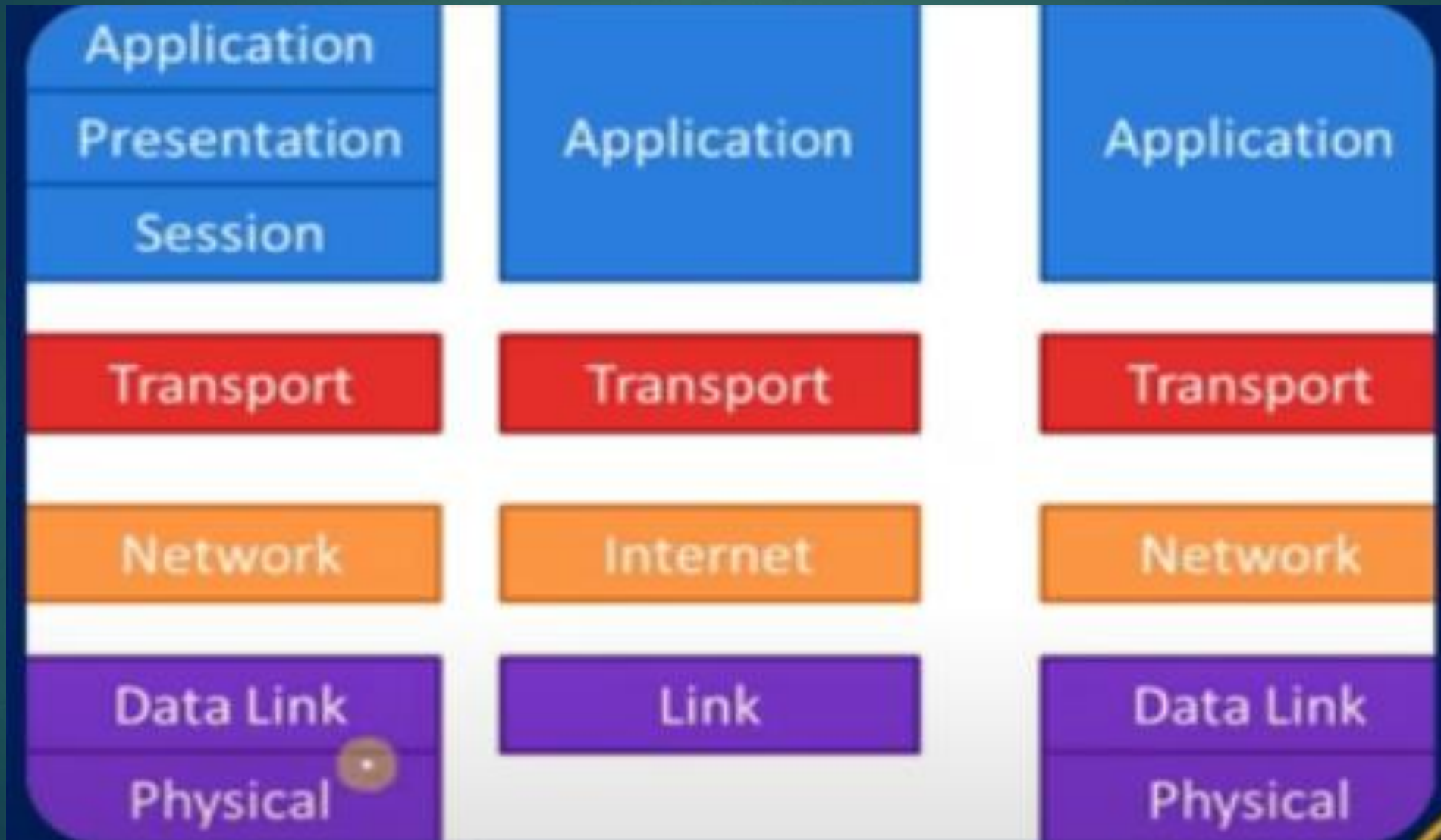
Signals of physical layer protocols.

1. Analogue.
2. Digital signal.

# TCP/IP Model

- ▶ Introduction to TCP IP model.
- ▶ Layers of TCP IP models.
- ▶ Process application layers.
- ▶ Two horse transport layer.
- ▶ Internet layer.
- ▶ Network Access link layer.
- ▶ Difference between OSI model and TCP IP model?

# Introduction to TCP IP model



# Advantages of TCP/IP

- ▶ It helps you to establish/set up a connection between different types of computers.
- ▶ It operates independently of the operating system.
- ▶ It supports many routing –protocols.
- ▶ It enables the internetworking between the organizations.
- ▶ TCP/IP models has a highly scalable client-server architecture.
- ▶ It can be used to established a connection between two computers.
- ▶



## OSI Model

It is developed by ISO (International Standard Organization)

OSI model provides a clear distinction between interfaces, services, and protocols.

OSI refers to Open Systems Interconnection.

OSI uses the network layer to define routing standards and protocols.

OSI follows a vertical approach.

OSI layers have seven layers.

In the OSI model, the transport layer is only connection-oriented.

In the OSI model, the data link layer and physical are separate layers.

Session and presentation layers are a part of the OSI model.

It is defined after the advent of the Internet.

The minimum size of the OSI header is 5 bytes.

## TCP/IP Model

It is developed by ARPANET (Advanced Research Project Agency Network).

TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.

TCP refers to Transmission Control Protocol.

TCP/IP uses only the Internet layer.

TCP/IP follows a horizontal approach.

TCP/IP has four layers.

A layer of the TCP/IP model is both connection-oriented and connectionless.

In TCP, physical and data link are both combined as a single host-to-network layer.

There is no session and presentation layer in the TCP model.

It is defined before the advent of the internet.

The minimum header size is 20 bytes.

# Transmission Mode and Transmission media

- ▶ What is Transmission?
- ▶ Transmission Mode and its Types
- ▶ Transmission Media and its Types.
- ▶ Twisted Pair cable (STP & UTP)
- ▶ FOC – Fibre Optic cable and Types of FOC
- ▶ Coaxial Cable and Types of Coaxial Cable
- ▶ How to prepare cable
- ▶ Color Code?
- ▶ Cross Cable
- ▶ Straight Cable/Patch Cable.

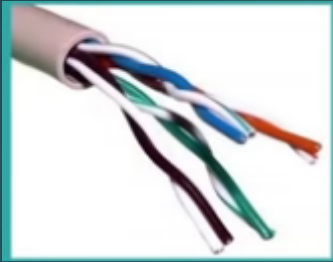


## What is Transmission?

- ▶ Transmission is a process in which user can send data or information using network device is known as Transmission.
- ▶ In simple language we can say it is the process of sharing information between devices.
- ▶ There is two types of transmission mode
- ▶ 1. Simplex mode
- ▶ 2. Duplex mode (HDX – Half Duplex mode, FDX- Full Duplex Mode.)
- ▶ **Simplex Mode** – It is one way communication and in this device can only send the data. Exp. Keyboard, mouse, mic etc.
- ▶ **Duplex Mode** - In this mode devices can send and receive the data.
- ▶ HDX – Half duplex mode support one way communication at a time. User cann't send and receive data simultaneously.
- ▶ FDX – In this technology user/ Device can send and receive the data simultaneously.

- ▶ Types of Transmission media
- ▶ 1. Wired Media (Note - wave, electromagnetic signal)
- ▶ 2. Wireless media (RF – Radio Frequency)

- ▶ Types of Wired Transmission Media



- ▶ Unshielded twisted pair cable



Shielded twisted pair cable



Fibre optic cable



Coaxial Cable

- ▶ Twisted pair Cable.
- ▶ Twisted pair cabling is a types of wiring in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility.
- ▶ 1. STP (Shielded twisted pair) cable has a fine wire mesh surrounding the wires to protect the transmission.
- ▶ 2. UTP (Unshielded twisted pair) cable does not shielded . Cable is used in older telephone network as well as network and data communication to reduce outside interference.
- ▶ Connector for Twisted pair cable.
- ▶ RJ45

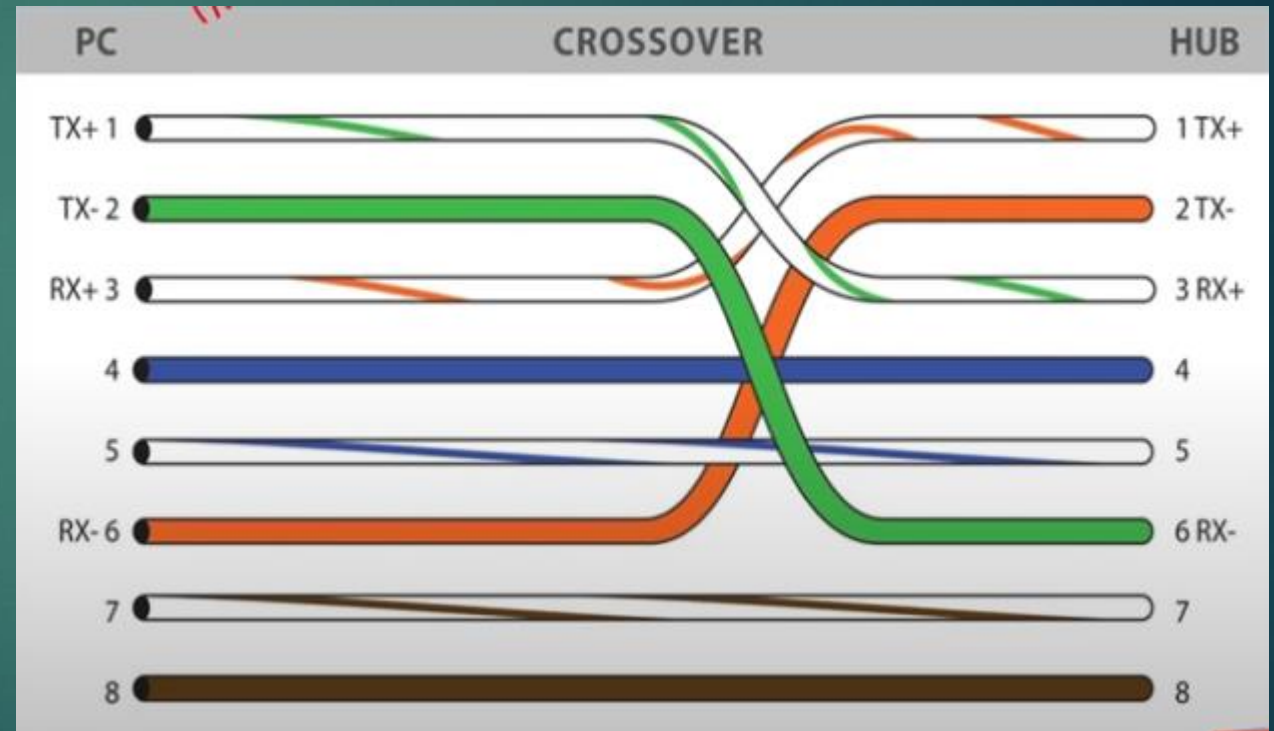
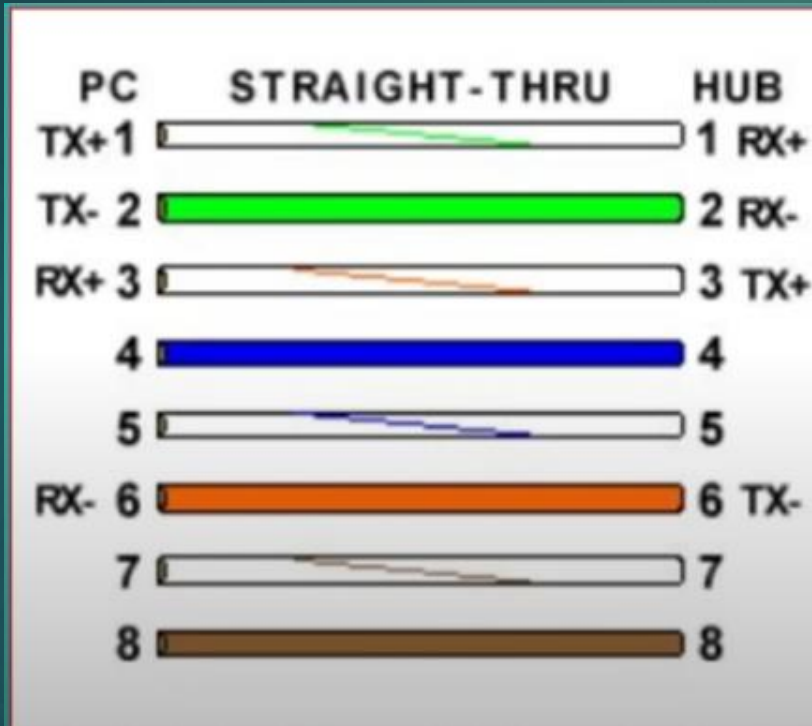


# Difference between STP and UTP

BASIS FOR COMPARISON	STP	UTP
Basic	STP (Shielded twisted pair) is a twisted pair cable enclosed in foil or mesh shield.	UTP (Unshielded twisted pair) is a cable with wires that are twisted together.
Noise and crosstalk generation	Less susceptible to noise and crosstalk.	High comparatively.
Grounding cable	Necessarily required	Not required
Ease of handling	Installation of cables is difficult comparatively.	Easily installed as cables are smaller, lighter, and flexible.
Cost	Moderately expensive.	Cheaper and does not require much maintenance.
Data Rates	Provides high data rates	Slow comparatively.
Max used	Less used	More used

# Cross Cable Vs Straight Cable

1. Cross Cable – It is used to connect similar device.
2. Straight or patch cables – It is used to connect dissimilar device.



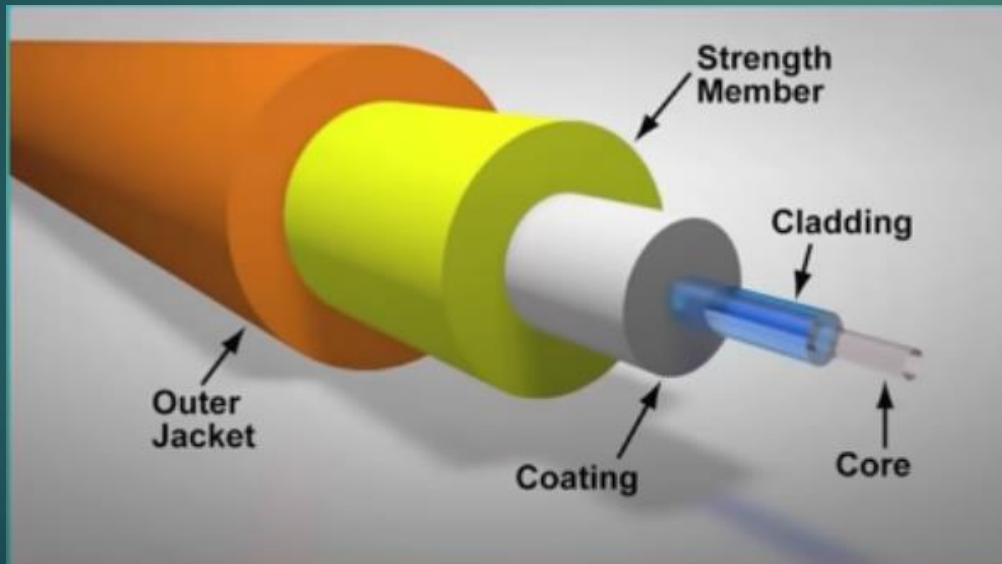



- ▶ Define 568A and 568 B
- ▶ TIA/EIA – 568A and 568 B are two standards for connecting category 3 and Category 5 wire connector
- ▶ Both are appropriate for high speed data through 568B is somewhat more common for installed wiring and 568A is more common in jumpers.
- ▶ There is no performance advantage either way.
- ▶ The only real difference between the two is the order in which the pairs are used (Orange and green)

EIA/TIA-568A:	EIA/TIA-568B:
Pin 1: White/Green	Pin 1: White/Orange
Pin 2: Green/White (or just plain Green)	Pin 2: Orange/White (or just plain Orange)
Pin 3: White/Orange	Pin 3: White/Green
Pin 4: Blue/White (or just plain Blue)	Pin 4: Blue/White (or just plain Blue)
Pin 5: White/Blue	Pin 5: White/Blue
Pin 6: Orange/White (or just plain Orange)	Pin 6: Green/White (or just plain Green)
Pin 7: White/Brown	Pin 7: White/Brown
Pin 8: Brown/White (or just plain Brown)	Pin 8: Brown/White (or just plain Brown)

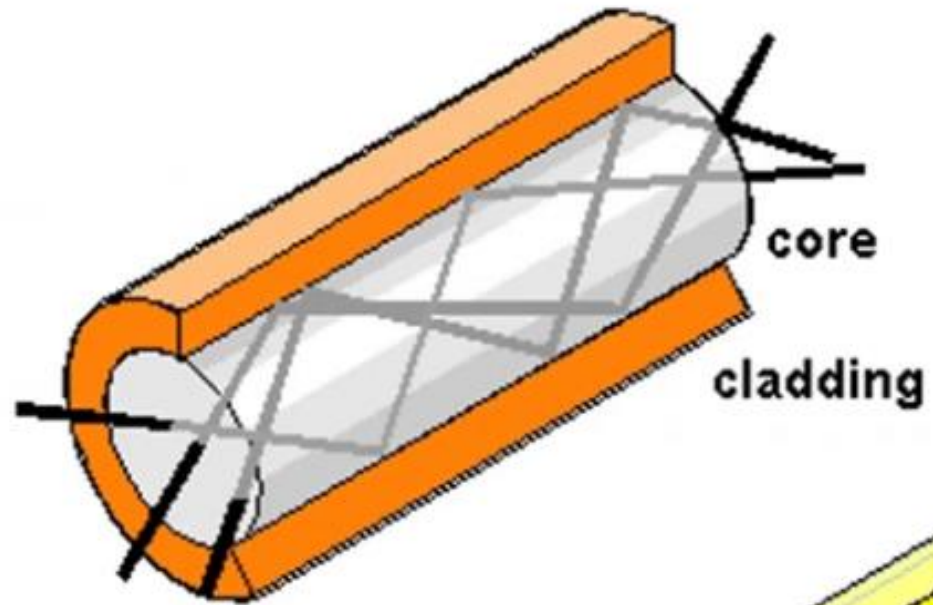


- ▶ What is Fibre Optic cable (FOC) ?
- ▶ A fibre optic cable also known as optical fibre cable, is an assembly similar to an electrical cable, but containing one or more optical fibre that are used to carry light.

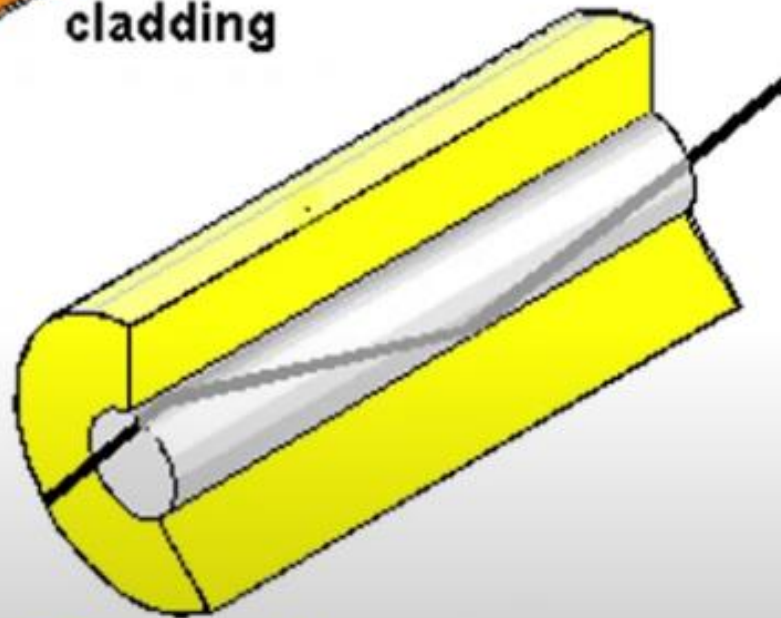


- 
- ▶ Types of Fibre Optic cable ?
  - ▶ There is two types of fibre optic cable
  - ▶ 1. Single mode fibre optic cable
  - ▶ 2. Multi mode fibre optic cable.
  - ▶ Single mode fibre optic cable
  - ▶ Single mode fibre optic cable has a small diametral core that allow only one mode of light to propagate.
  - ▶ Because of this, the number of light reflection created as the light through the core decreases, lowering attenuation and creating the ability for the signal to travel further
  - ▶ This application is typically used in long distance, higher bandwidth runs by Telco's CATV companies and college and Universities.
  - ▶ Multimode fibre optic cable
  - ▶ It has a large diametral core that allow multiple modes of lights to propagate. Because of this, the number of light reflection created as the light passes through the core increases, creating the ability for more data to pass through at a given time.
  - ▶ Because of the high dispersion and attenuation rate with this types of fibre, the quality of the signal is reduced over long distance. This application is typically used for short distance data and audio/video application in LAN.
  - ▶ RF broadband signal, such as what cable companies commonly use, cannot be transmitted over multimode fibre.

# Single mode and Multimode FOC



Multimode



Singlemode

# Internet

- ☐ What is internet?
- ☐ How does internet work?
- ☐ Owner of internet?
- ☐ IANA, ARIN, ICANN, IEEE, IETF





# What is Internet?



# How does internet work ?







The Internet Assigned Numbers Authority is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and Internet numbers.



The American Registry for Internet Numbers is the regional Internet registry for Canada, the United States, and many Caribbean and North Atlantic islands. ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers.



The Internet Corporation for Assigned Names and Numbers is an American multistakeholder group and nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation.



The Institute of Electrical and Electronics Engineers is a professional association for electronic engineering and electrical engineering with its corporate office in New York City and its operations center in Piscataway, New Jersey.



The Internet Engineering Task Force is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite. It has no formal membership roster or membership requirements.



# Types of Internet Connection

- ☐ Broadband
- ☐ Leased Line
- ☐ Cellular network



Cellular network

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called "cells", each served by at least one fixed-location transceiver, but more normally three cell sites or base transceiver stations.

these base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell



# Broadband

- Broadband is not a dedicated connection between your premises and the local exchange. It is variable bandwidth, asymmetric, meaning faster for downloads than for uploads, and subject to contention with other users.
- A leased line is a dedicated connection between your premises and the local exchange. It is fixed bandwidth and offers identical upload and download speeds and is not subject to contention with other users.

## Leased Line

A leased line is a private telecommunications circuit between two or more locations provided according to a commercial contract. It is sometimes also known as a private circuit, and as a data line in the UK. Typically, leased lines are used by businesses to connect geographically distant offices.



# Internet Vs Intranet vs Arpanet with Milinet

- ▶ Internet
- ▶ Intranet
- ▶ Arpanet
- ▶ Milnet

**Intranet** – An intranet is a computer network for sharing information, collaboration tools, operational systems and other computing services within an organization usually to the exclusion of access by outsiders.

**Arpanet** - The ARPANET ( An acronym for advance research projects agency network) was the first wide area package switching network with distributed control and one of the first networks to implements the TCP/IP protocol suits . Both technologies became the technical foundation of the internet

**Protocols** : 1822 protocols, NCP, TCP/IP    **Closed :1990**

**Milnet** – In computer networking MILNET was the name given to the part of the ARPANET internetwork designated for unclassified united states department of Defence traffic. MILNET was physically separated from ARPANET in 1983



# Wireless Technology

- ❑ Introduction to wireless network
- ❑ How does wireless network work?
- ❑ Types of wireless standard? With explanation
- ❑ How to setup wireless network and Wi-Fi router configuration?
- ❑ Advantages and disadvantages of wireless network

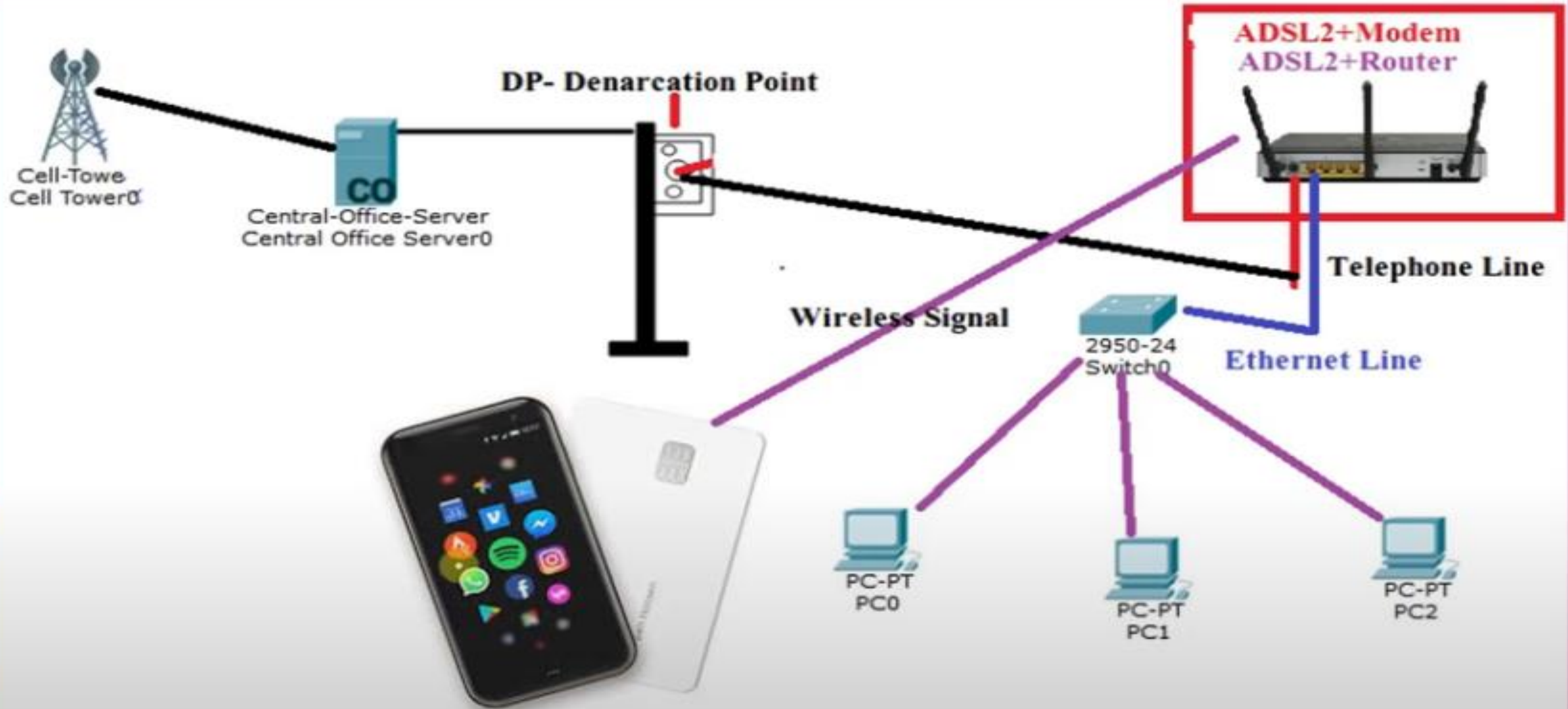


**Introduction to wireless network:-** Wireless Network technology connect networking devices using Radio Frequency. So we can connect all networking devices wirelessly. But it cover small area in compare of wired technology.

We can use this technology over a small area like home, small office, schools For wireless communication.



# How does wireless network work ?



# Wireless Security

**Open (risky):** Open Wi-Fi networks have no passphrase. You shouldn't set up an open Wi-Fi network—seriously, you could have your door busted down by police.

**WEP 64 (risky):** The old WEP protocol standard is vulnerable and you really shouldn't use it.

**WEP 128 (risky):** This is WEP, but with a larger encryption key size. It isn't really any less vulnerable than WEP 64.

**WPA2-PSK (TKIP):** This uses the modern WPA2 standard with older TKIP encryption. This isn't secure, and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network.

**WPA2-PSK (AES):** This is the most secure option. It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. **You should be using this option.** On some devices, you'll just see the option "WPA2" or "WPA2-PSK." If you do, it will probably just use AES, as that's a common-sense choice.

**WPAWPA2-PSK (TKIP/AES):** Some devices offer—and even recommend—this mixed-mode option. This option enables both WPA and WPA2, with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have, but also allows an attacker to breach your network by cracking the more vulnerable WPA and TKIP protocols.

# Wireless standard

STANDARD	FREQUENCY	SPEED
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz/5GHz	600Mbps
802.11ac	Up to 5GHz	More than 1Gbps



# How to setup wireless network and Wi-Fi router configuration?



## Advantages and disadvantages of wireless Network

1. Convenience
2. Expandability
3. Deployment
4. Productivity
5. Mobility
6. Cost
7. Security

# Mobile Network Technology

- ▶ What is Cellular Network?
- ▶ Generation of Mobile Networking ?
- ▶ Telecom (Mobile Operators)?

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land area called “cells” each served by at least one fixed location transceiver, but more normally, three cell sites or base transceiver station.

## Generation of Mobile Network

Features	1G	2G	3G	4G	5G
Start/Development	1970/1984	1980/1999	1990/2002	2000/2010	2010/2015
Technology	AMPS, NMT, TACS	GSM	WCDMA	LTE, WiMax	MIMO, mm Waves
Frequency	30 KHz	1.8 Ghz	1.6 - 2 GHz	2 - 8 GHz	3 - 30 Ghz
Bandwidth	2 kbps	14.4 - 64 kbps	2 Mbps	2000 Mbps to 1 Gbps	1 Gbps and higher
AccessSystem	FDMA	TDMA/CDMA	CDMA	CDMA	OFDM/BDMA
Core Network	PSTN	PSTN	Packet Network	Internet	Internet

# PROTOCOLS

- ☐ What is protocol?
- ☐ IP
- ☐ TCP
- ☐ UDP
- ☐ ARP
- ☐ RARP
- ☐ POP
- ☐ IMAP
- ☐ SMTP
- ☐ SNMP
- ☐ FTP
- ☐ HTTP
- ☐ HTTPS
- ☐ NTP
- ☐ DNS
- ☐ DHCP





**Protocols:-** it is a set of rule for particular object.    Networking Technology using various types of protocols to manage the network and share the information from one network device to other network device.

**IP:-**     IP stand for internet protocols and it is used to connect one pc to others.

**TCP:-** TCP stand for transmission control protocol and this protocol allow pc to share data with reliability, security, slow, and also manage the packets. And TCP provide acknowledgement.

**UDP :-** User Datagram Protocol – this protocol allow pc to carry the data with fast, unreliable, insecure, and UDP does not provide any types of acknowledgement and it is used for video streaming also.

**ARP-** Address Resolution Protocol- it is used to find Mac address from IP address. ARP work on switch devices.

**RARP-** Reverse address resolution protocol- it is used to find IP address from mac address and work oppo.. Of ARP.

**DNS-** Stand for Domain name system- it is used to find the ip to name like xyz.com=10.0.0.10

**DHCP-** Stand for Dynamic Host configuration protocol and it is used to manage IP over a network. Its provide Dynamic IP or auto ip over a network.

POP:- Post Office protocols this protocol is used to receive the email.

IMAP- Stand for internet message access protocol and **Internet Message Access Protocol (IMAP)** means that all of your email is saved on your Internet Service Provider's servers. If you are using IMAP, you can run an email program at home and an email program at work and both programs will access the same set up messages and folders.

SMTP: - Simple mail transfer protocol – used to send email messages.

FTP- File Transfer Protocol used to upload and download.

HTTP- Hyper Text Transfer Protocol – use to access Web data.

HTTPS:-

NTP- Network Time Protocol- Is used to manage network router and server time to sync the time.



TCP	UDP
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP doesn't supports Broadcasting.	UDP supports Broadcasting.

# IP ADDRESS

- ☐ What is IP?
- ☐ Types of IP?
- ☐ IPv4
- ☐ IPv6
- ☐ Classes of ipv4
- ☐ Host id & Network Id
- ☐ Subnet mask
- ☐ VLSM
- ☐ Subnetting
- ☐ Gateway
- ☐ How to configure IP address subnet mask and gateway?

# IP – Internet protocol and assign on computer for computer identity

It is unique address it may be decimal or hexadecimal An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

An IP address serves two main functions: host or network interface identification and location addressing

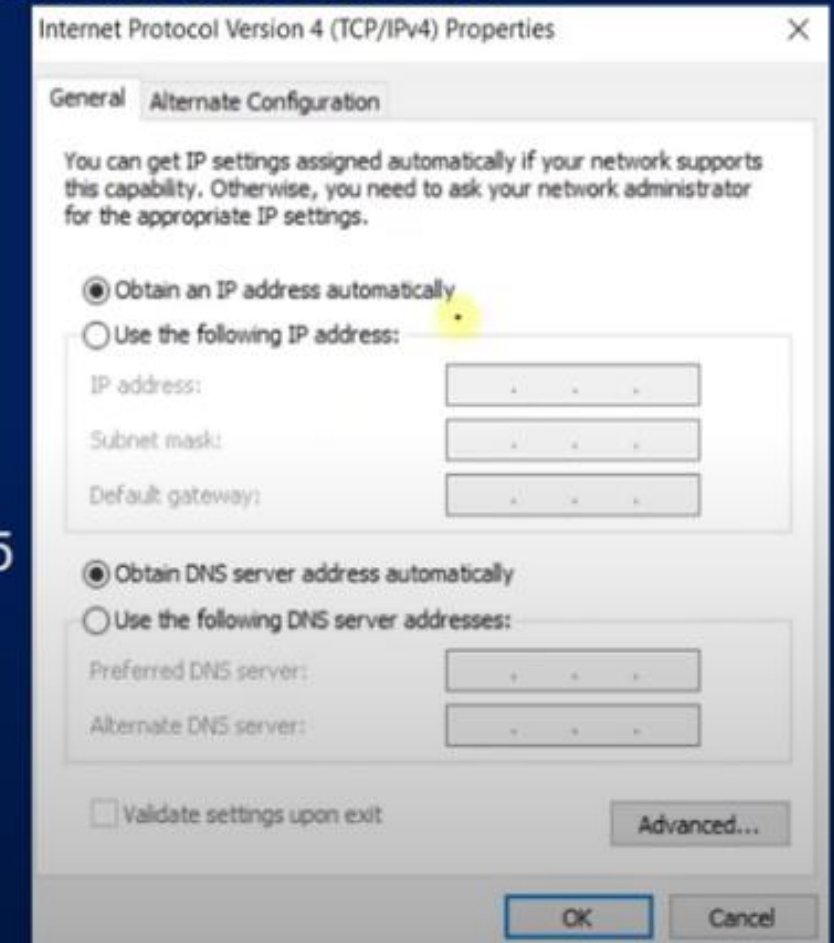
Categorized in two part

1- Network id

2- Host id

IPv4 address is 202.56.215.200 or 10.0.0.0 or 10.0.0.100, 172.168.0.25

IPV6 Address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334



Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel



Ipv4	ipv6
32 bit address	128 bit address
Classful address	Classless address
5 class	No class
4 block	8 block
8bit/block	16bit/block
Small Network	Geographical Network

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel



● **Subnet Mask:-** is used to identify network id and host id

● **How to identify Class of IP address**

Class	Range
A	1-126
B	128-191
C	192-223
D	224-239
E	240-255

Class	Subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

- ▶ Private IP
- ▶ Public IP
- ▶ Loop Back IP

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

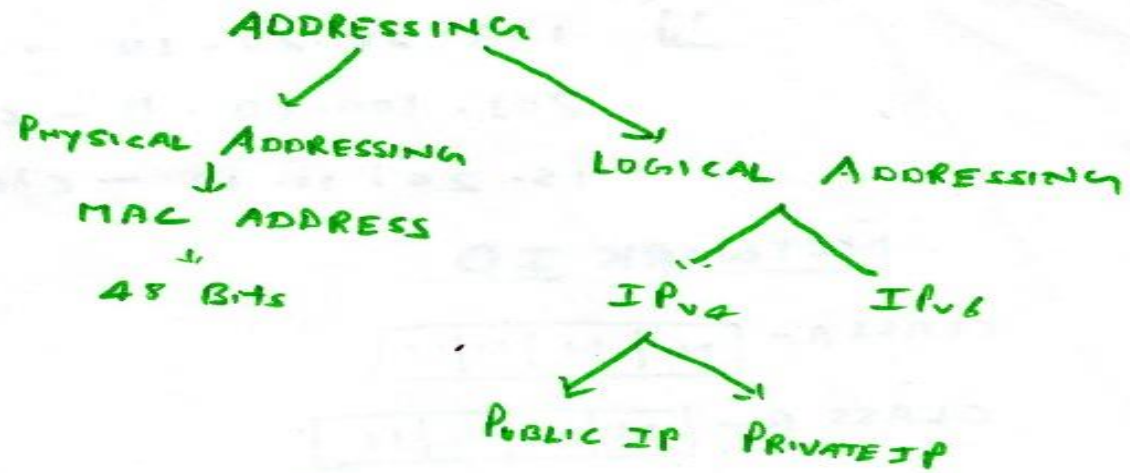
Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

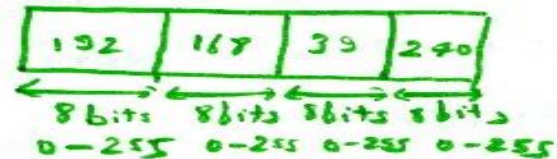
OK Cancel



## IPv4

- INTERNET PROTOCOL
- 32 Bit LOGICAL ADDRESS
- 4 OCTET

IP ADDRESS → NETWORK ID + HOST ID



## CLASSES

- CLASS A → 1.0.0.0 to 126.0.0.0 (LARGE N/w)
- CLASS B → 128.0.0.0 to 191.255.0.0
- CLASS C → 192.0.0.0 to 223.255.255.0 (SMALL N/w)
- CLASS D → 224 - 239 - MULTICAST
- CLASS E → 240 - 255 - RESEARCH
- LOOP BACK ADDRESS - 127.0.0.0

(i) 137.20.20.10 - class ?  
 203.100.10.0 - class ?  
 15.20.10.10 - class ?

### NETWORK ID

CLASS A - 

N	H	H	H
---	---	---	---

CLASS B - 

N	N	H	H
---	---	---	---

CLASS C - 

N	N	N	H
---	---	---	---

Network Bit  
Represented by - 1

Host Bit  
Represented by - 0

Q.9 How to find N/w ID.

115.10.0.15 - class ?

115.0.0.0 - NETWORK ID.

(iii) 196.10.10.10 - Class ?

196.10.10.0 NETWORK ID

### SUBNET MASK

115.10.10.20  
CLASS-A IP

N	H	H	H
---	---	---	---

N/w, 115.10.10.10 - Host

11111111

00000000.00000000

→ Convert Binary - 255.0.0.0

Subnet Mask

(iii) 160.10.20.10 - Class-B

N	N	H	H
---	---	---	---

11111111.11111111.00000000.00000000

↓ ↓  
255.255.0.0

Subnet Mask of Class-B

## BINARY CONVERSION

o Convert IP address into Binary  
192.168.37.200

S.14

$2^7$   $2^6$   $2^5$   $2^4$   $2^3$   $2^2$   $2^1$   $2^0$   
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓  
128 64 32 16 8 4 2 1

$\begin{array}{r} 128 \\ 16 \\ \hline 192 \end{array}$

192 { 1 1 0 0 0 0 0 0 }

$\begin{array}{r} 128 \\ 32 \\ 8 \\ \hline 168 \end{array}$

168 { 1 0 1 0 1 0 0 0 }

$\begin{array}{r} 128 \\ 32 \\ 4 \\ \hline 168 \end{array}$

37 { 0 0 1 0 0 1 0 1 }

$\begin{array}{r} 128 \\ 32 \\ \hline 160 \end{array}$

200 { 1 1 0 0 1 0 0 0 }

$\begin{array}{r} 128 \\ 16 \\ 8 \\ \hline 200 \end{array}$



## PRIVATE IP

CLASS A - 10.0.0.0

CLASS B - 172.16.X.X — 172.31.X.X

CLASS C - 192.168.0.0 to 192.168.255.255

} Range  
of  
Private  
Address

## BROADCAST ID

this is used to broadcast the message. (max. host part max. value)

Q IP - 150.10.20.30

Network ID ?

Broadcast ID ?

No. of usable host ?

Ans

150.10.0.0 - N/w ID.

150.10.255.255 - Broadcast ID.

$2^{16} - 2 = 65,534$  IP. n. of usable host.

Q IP - 11.200.200.160

Network ID ?

Broadcast ID ?

No. of usable host ?

Ans



N/w ID - 11.0.0.0

Broadcast ID - 11.255.255.255

No. of usable -  $2^{24} - 2 = 16,777,214$



gac

IP, 4 - Limited

① Use Private IP - 10.2.2

①  $U_{AC} \perp P_0$

③ Submitting

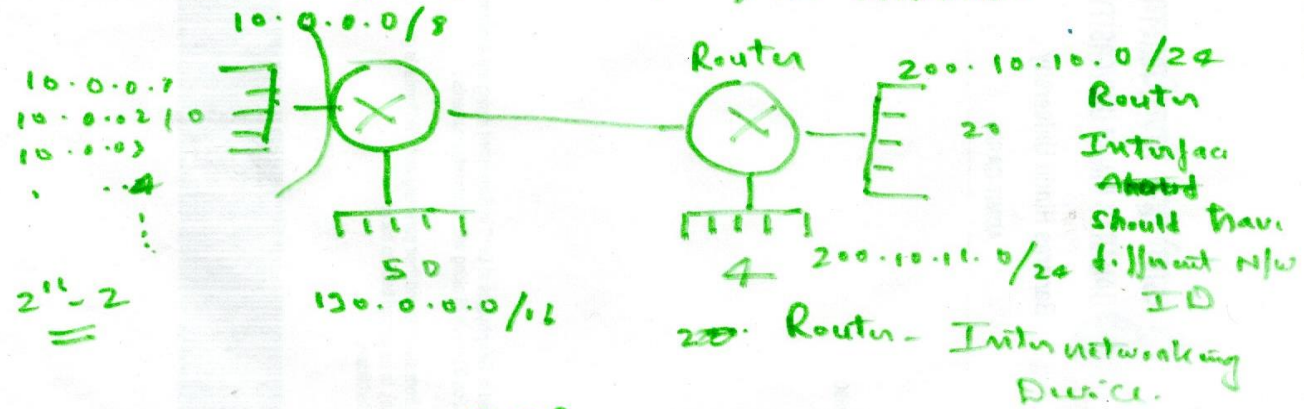
### Subnetting.



## Network within a Network

22

### Logically division of IP Address.

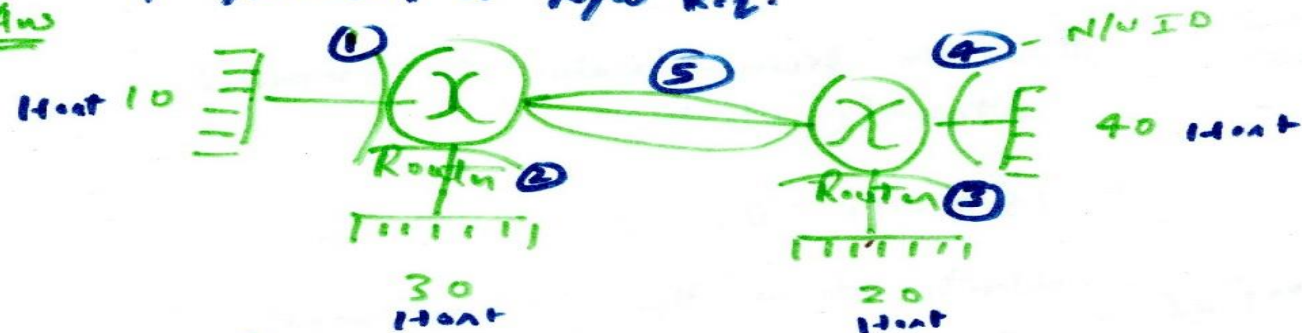


CIDR

## Q How To Do SUBNETTING ?

- ✓ According to Host Req.
- ✓ According to N/w Req.

Ans



we have Class-C 197.10.10.0/24 - CIDR

Soln

Step-1

197.10.10.0  
n/w      Host → Convert into Binary

Step-2

197.10.10.00000000

Step-3

Condition has to satisfy

$$2^n - 2 \geq 40$$

$$n = 1, 2, 3, 4 \dots$$

$$2^1 - 2 \geq 40 \times$$

$$2^2 - 2 \geq 40 \times$$

$$2^6 - 2 = 64 - 2 = 62 \geq 40 \quad \checkmark$$

$$n = 6$$

Step-4

197.10.0.00000000  
197.10.0.11000000

Reserve for Host  
Host bit → 0  
N/w bit → 1

197.10.0.0 <sup>128 64 32 16 8 4 2 1</sup>  
<sub>↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑</sub>  
 11000000

Step-5

Add the decimal value of borrowed network bit

197.10.0.192

Step-6

Write down the Subnet mask.

255.255.255.192

class's subnet      borrowed n/w bit

Step-7

Now write down the Subnet ID

197.10.10.0/26 - Subnet 10-3

Subnet mask 255.255.255.192

Subnet 2 197.10.10.64/26 - 13.10

(Add 64 in next ID)

197.10.10.64/26

Subnet-3

197.10.10.128/26.

Subnet-4

197.10.10.192/26

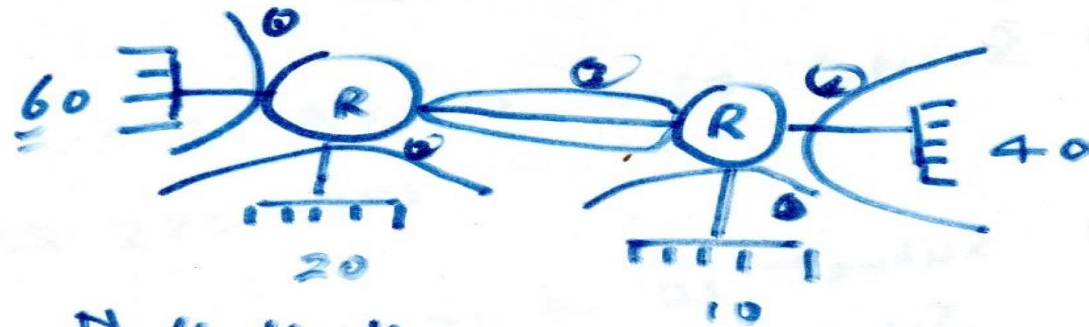
Subnet-5

?



# SUBNETTING OF CLASS-A IP

class-A - 12.0.0.0



(i)  $2^N - 2 \geq 60$   
 $2^N - 2 \geq 60$

(ii)  $12.00000000.00000000.00000000$

(iii)  $2^N - 2 \geq 60$   
 $2^1 - 2 = 0$   
 $2^2 - 2 = 2$   
 $2^3 - 2 = 8 - 2 = 6$   
 $2^4 - 2 = 16 - 2 = 14$   
 $2^5 - 2 = 32 - 2 = 30$   
 $2^6 - 2 = 64 - 2 = 62$   
 $64 - 2 \geq 60$   
 $62 \geq 60$

(iv)  $N = 60$

h/w bit - 1  
 host bit - 0

Reserved for  
 host (in)

(v)  $12.00000000.00000000.00000000$

(vi) 12. 11111111. 11111111. 11000000  
 (vii) 12. 255. 255. 192  
 (viii) Subnet Mask. class A - 255.0.0.0  
 1255.255.255.192

(ix) Subnet ID → 12.0.0.0/26  
 Subnet Mask - 255.255.255.128 CIDR  
 B-ID - 12.0.0.63/26.

(x) 2nd Subnet -  
 12.0.0.64/26  
 B-ID - 12.0.0.127/26

2nd last  
 subnet -  
 mask

3rd Subnet - 12.0.0.128/26

4th Subnet - 12.0.0.192/26

5th Subnet - 12.0.1.0/26

6th Subnet - 12.0.1.64/26

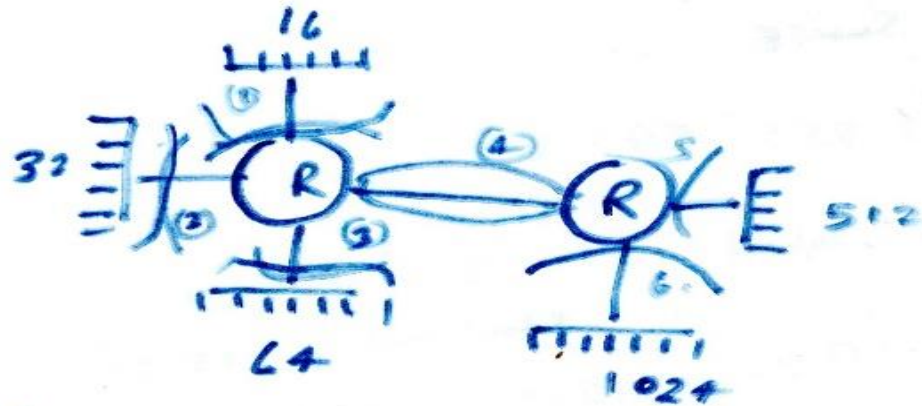
7th Subnet - 12.0.1.128/26

... 12.0.2.0 ...

4:59 PM  
 5:00 PM



Q



$$\text{I.P} = 12.0.0.0$$

(i)  $12.0.0.0$

(ii)  $12.00000000.00000000.00000000$

(iii)  $2^m - 2 \geq 1024$

$$2^8 = 256$$

$$2^{10} - 2 \geq 1024$$

$$2^9 = 512$$

$$2^{10} = 1024$$

$$1024 - 1022 \neq 1024$$

$$2^{11} - 2 = 2048 - 2 = 2046 \geq 1024$$

$$n = 11$$

(iv)  $12.00000000.00000000.00000000$

w/w      Host

$$12.11111111.11110000.00000000$$

128 32 16 8 4 2 1

## SUNEE

(5)  $12.255.248.0$

(6) 1<sup>st</sup> Subnet ID  $\rightarrow 12.0.0.0/21$   
Subnet mask  $\rightarrow 255.255.248.0$

B-ID  $- 12.0.7.255/21$

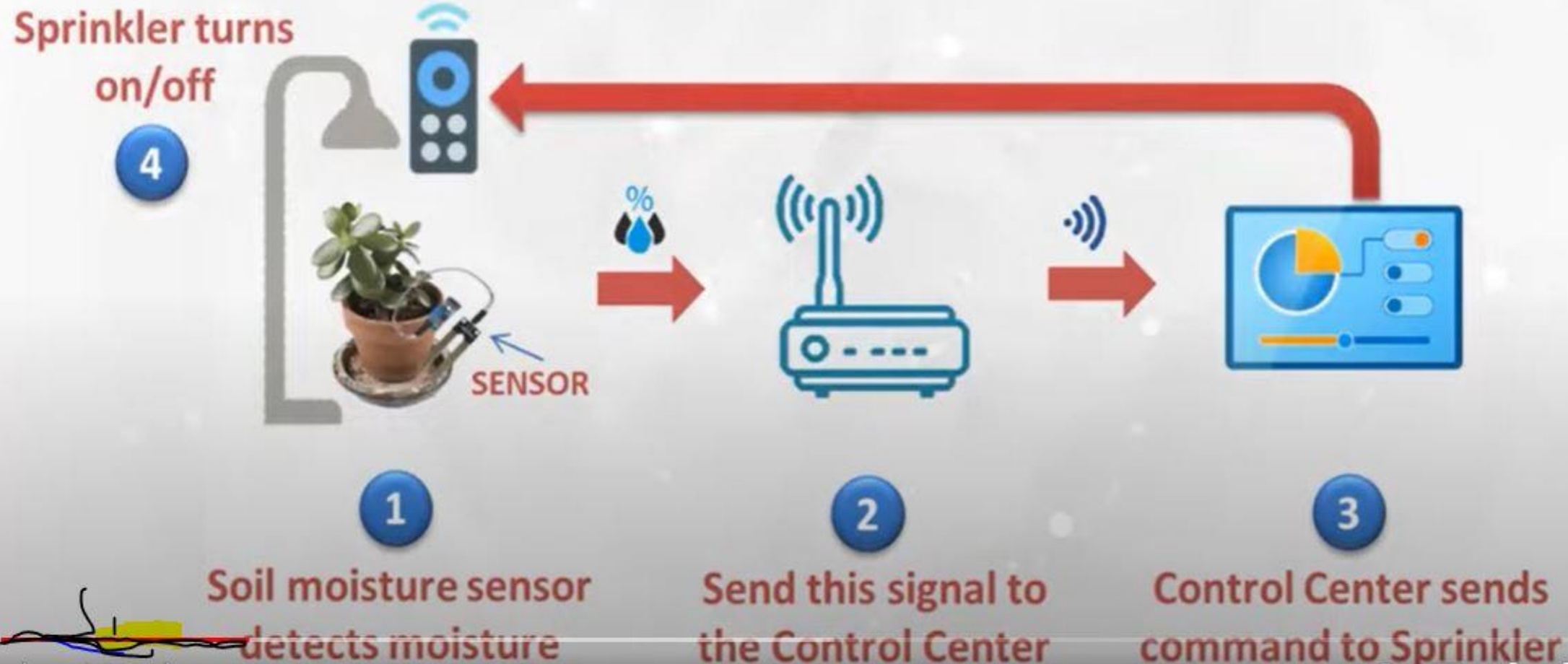
2<sup>nd</sup> Subnet ID  $- 12.0.8.0/21$

3<sup>rd</sup> Subnet ID  $- 12.0.16.0/21$

4<sup>th</sup> Subnet ID  $- 12.0.24.0/21$

# Internet Of Things (IoT)

Taking everyday things, **embedding** them with **electronics, software, sensors** and then **connecting them to internet** and enabling them to **collect and exchange data without human intervention** is called as the **Internet of Things (IoT)**





# Internet Of Things ( IOT )



# Components Of IOT



There are four main components based on which an internet of things ecosystem works on. They are required for end to end implementation of IOT



DEVICES/SENSORS



CONNECTIVITY



DATA PROCESSING



USER INTERFACE



# Sensors

A sensor is a device that measures physical input from its environment and converts it into data that can be interpreted by a computer.



# Sensors

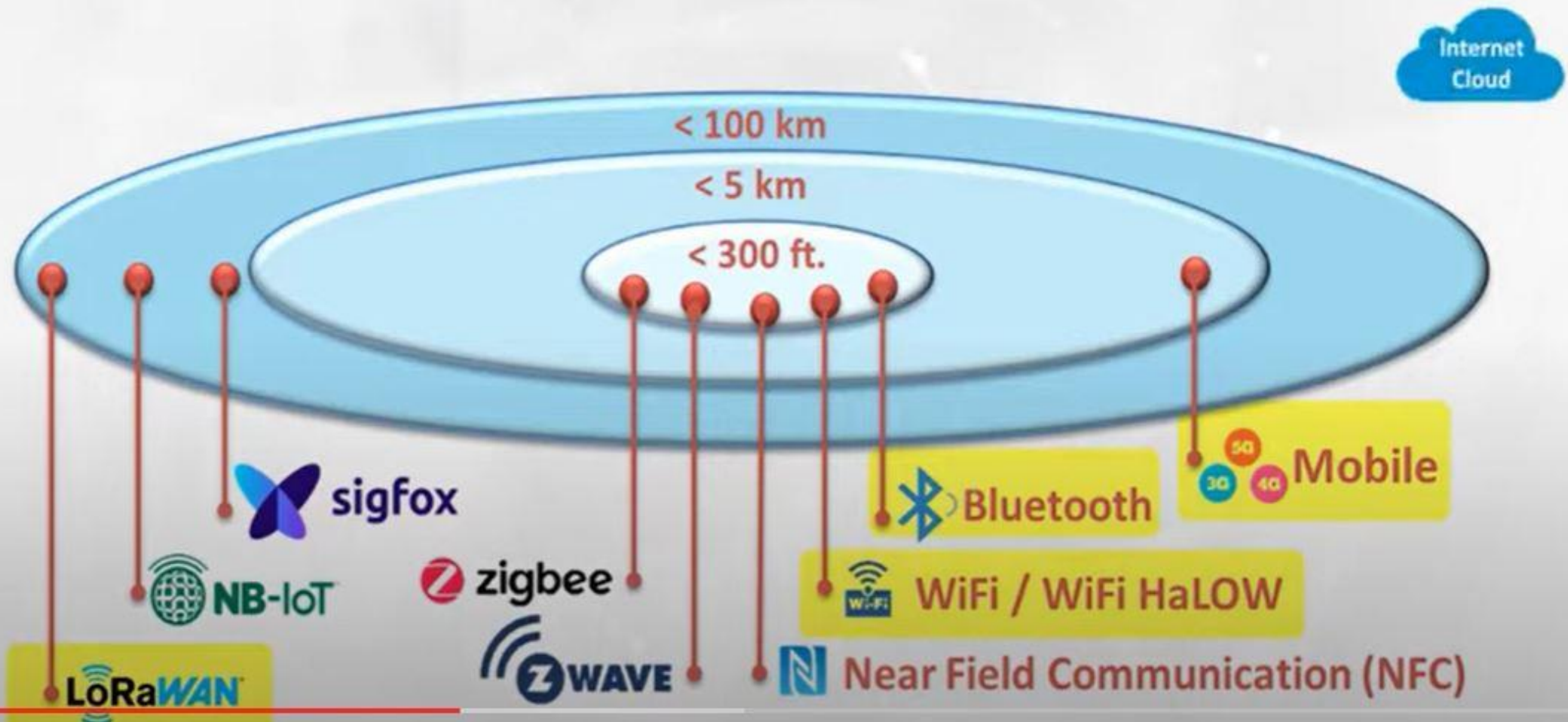
A sensor is a device that measures physical input from its environment and converts it into data that can be interpreted by a computer.





# Connectivity

Several Communication Protocols and Technologies are used in IOT to connect to Internet cloud. Depending upon Range, Cost, Power usage, Data rate etc. the right one is used.



# Data Processing

In the processing stage, a computer transforms the raw data into information. The transformation is carried out by using different data manipulation techniques



Data Aggregation



Data Extraction



Data Classification



Data Analytics



# User Interface



The information processed is made available to the end-user in some way, like giving Alerts, Notifications, monitoring continuous feed or controlling the system remotely



Alerts



Notifications



Live Trends



Remote Control



# Application of IOT

- Crop Monitoring
- Soil & Water Management

- SMART IDs
- SMART Board

- SMART Supply Chain
- Industrial Automation

## Healthcare



- Bio Sensors
- Wearable Devices



## Agriculture



## SMART Homes



- Centralized Monitoring
- Smart Switches



## Education



- SMART IDs
- SMART Board



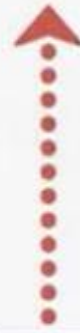
## Retail



- Smart Shelves
- Digital Signage



## Industries



- SMART Supply Chain
- Industrial Automation



# Network Vulnerability & Securing Network and Networking

- ❑ What is vulnerability?
- ❑ How to check network vulnerability?
- ❑ How to secure our network?

**Vulnerability** Existence of a weakness, design or implementation error that can lead to an unexpected event compromising the security of the system.





# National knowledge network:

*Welcome to 10,000,000,000 bits per second !*



# WHY?

- ▶ Computational Resource Access
- ▶ Critical Mass of Scientists in Key Areas
- ▶ Common Country-wide Classrooms
- ▶ Increased Peer Group Interaction
- ▶ Data Bases Sharing Online

# Application Requiring High Bandwidth

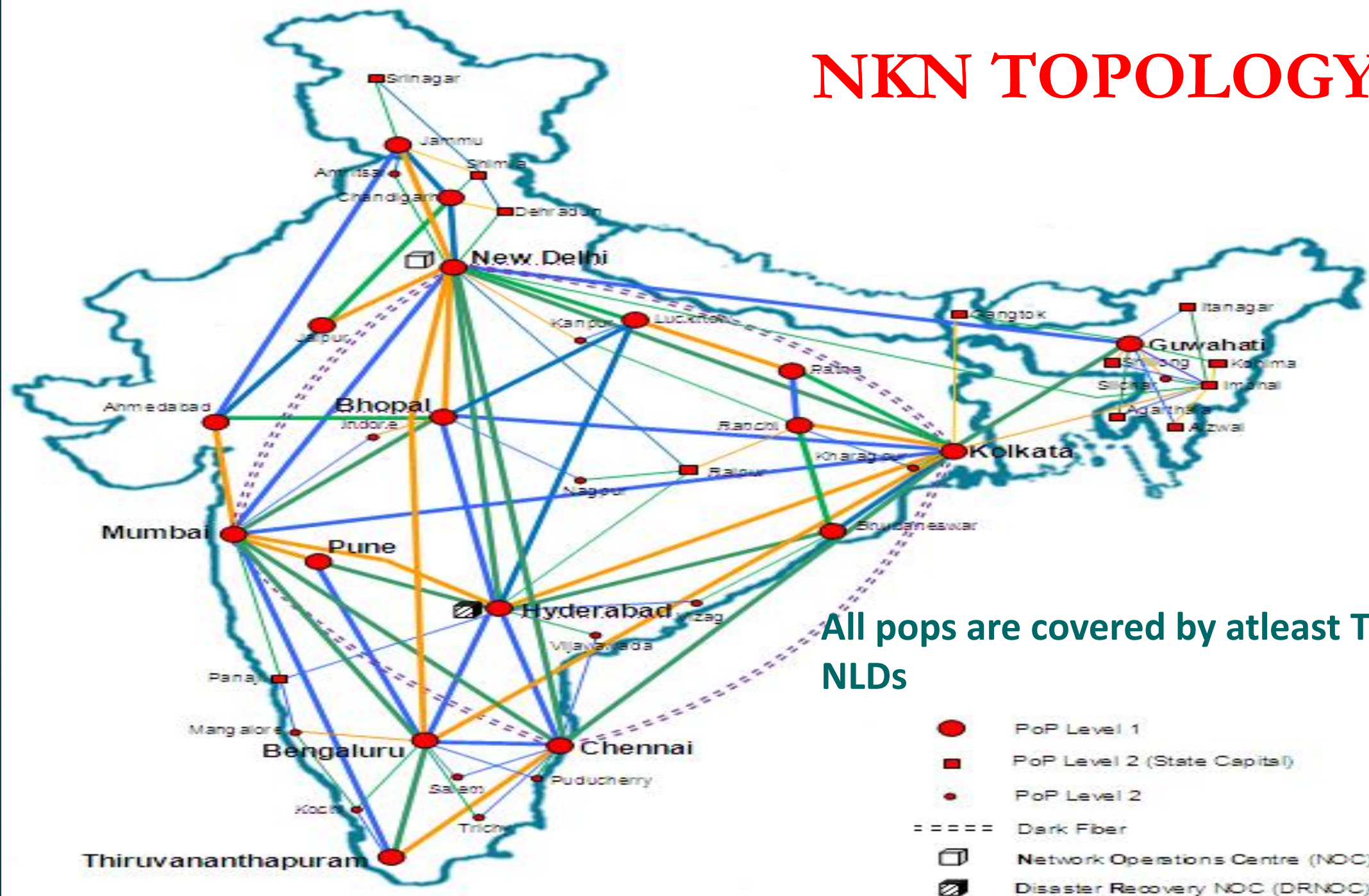
- ▶ Virtual Laboratories
- ▶ Collaborative Mega Science Projects
- ▶ Innovative Info-Bio-Nano Experiments
- ▶ Non-invasive Medicare for Diseases like Cancer
- ▶ Diagnostic Domes as Public Health Centers in Rural Areas
- ▶ Country-wide Classroom
- ▶ University without Walls
- ▶ Voice Conferencing among Researchers
- ▶ Video Conferencing among Researchers
- ▶ On-line access to Electronic Resources

# Life @ 10 Gbps

120

- ▶ Scenario #1: Education
- ▶ Scenario #2: Research
- ▶ Scenario #3: HealthCare
- ▶ Scenario #4: Governance
- ▶ Scenario #5: FarmCare
- ▶ Scenario #6: HPC: Weather Modeling

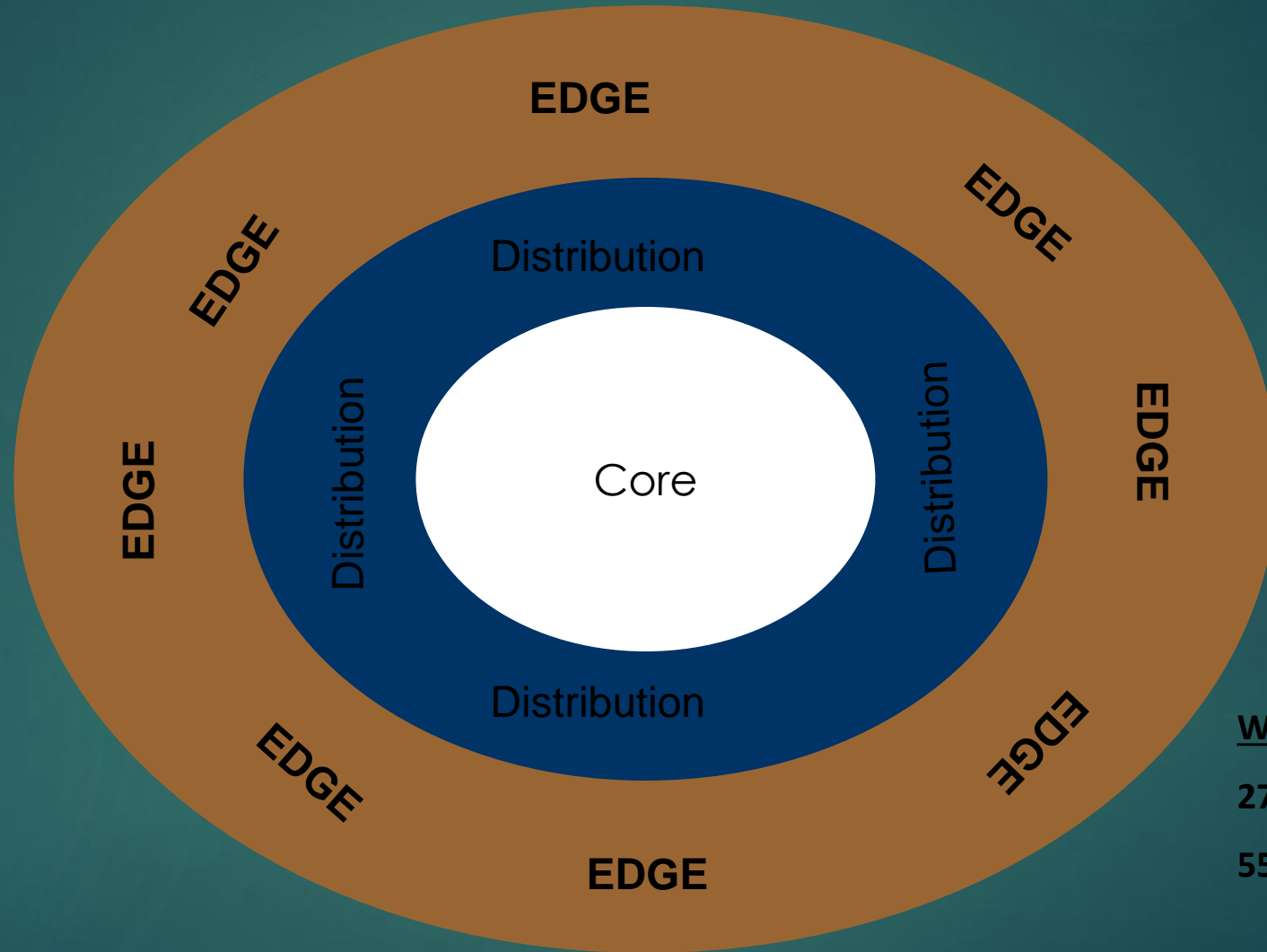
# NKN TOPOLOGY



All pops are covered by atleast Two NLDs



## NKN Topology



### Current status

15 POPS

78 Institutes have been  
connected

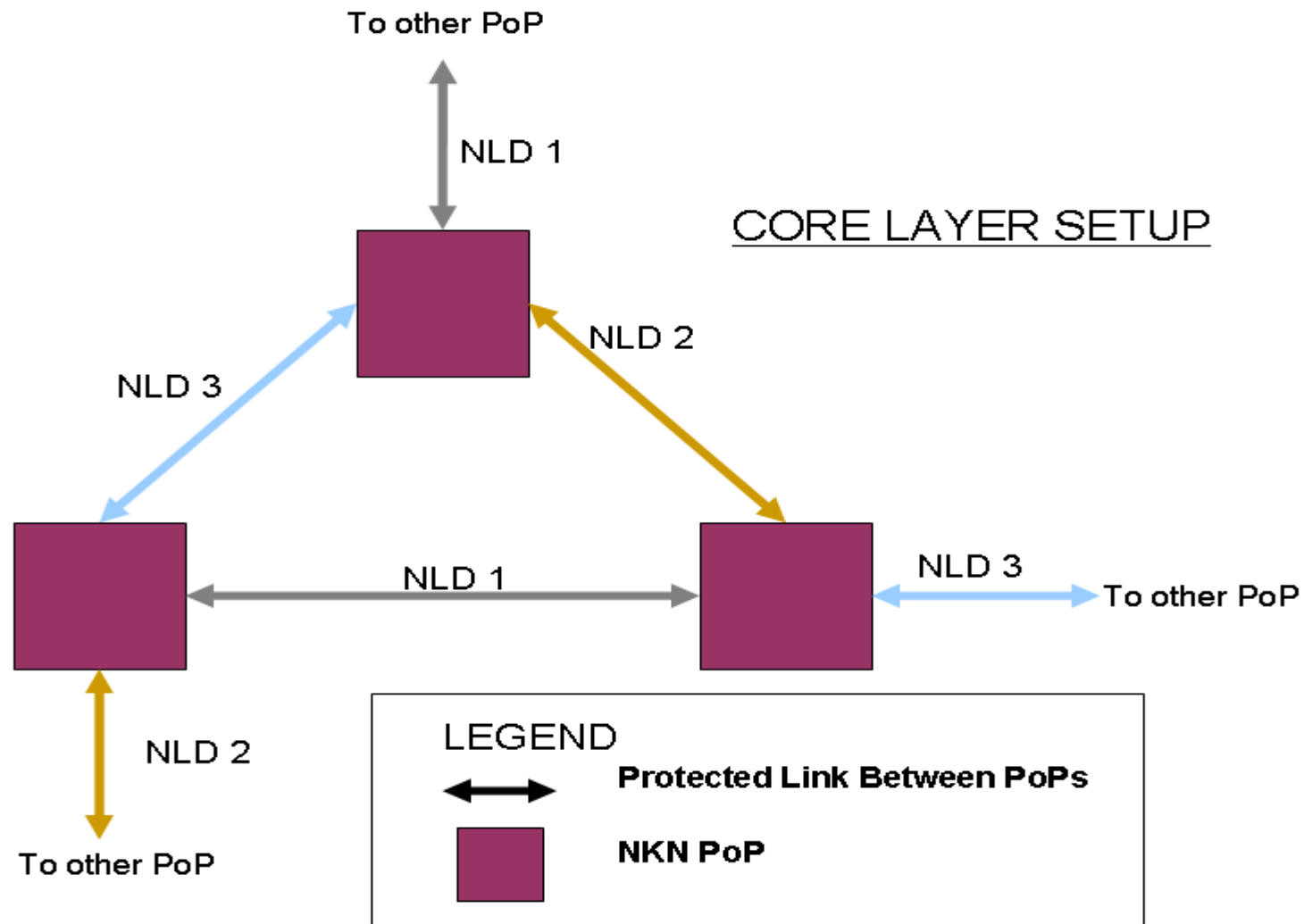
### Work in progress for

27 POPS

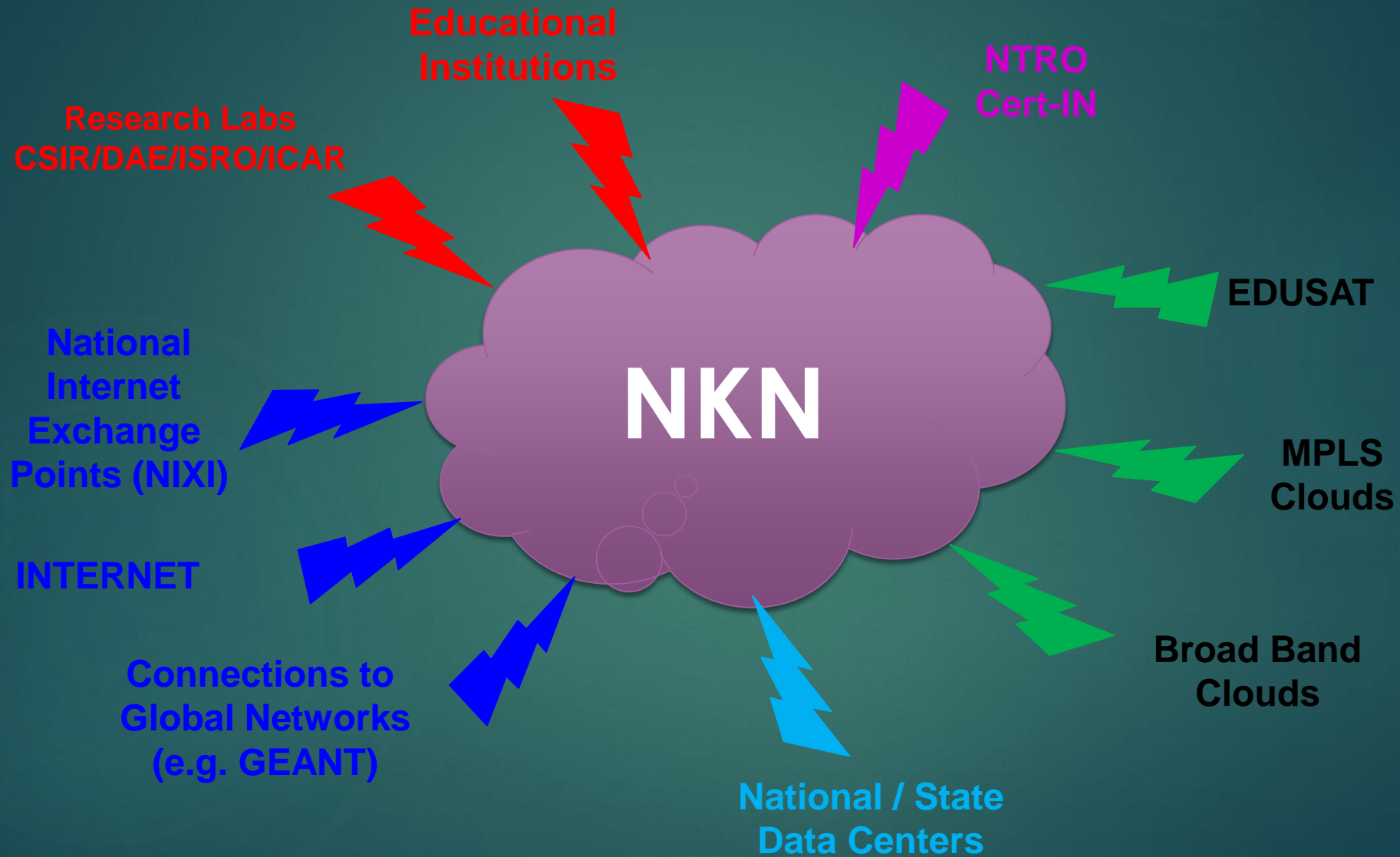
550+ Institutes

# Features NKN

- High Capacity, Highly Scalable Backbone
- Provide QoS and Security
- Wide Geographical Coverage
- Common Standard Platform
- Bandwidth from Many NLD's
- Highly Reliable & Available by Design
- Test beds ( for various implementation)
- Dedicated and Owned.



**Achieve Higher Availability**





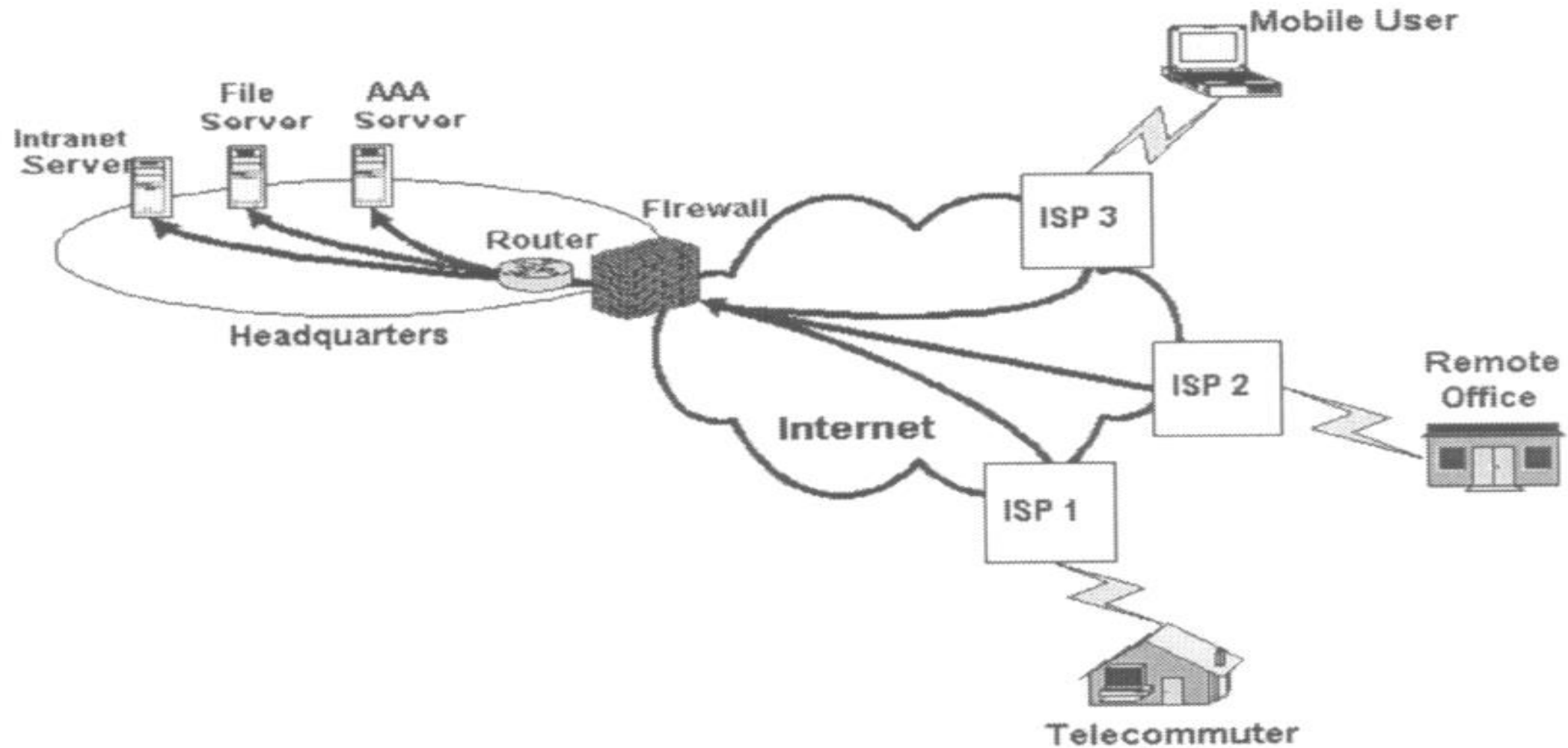
# What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Became popular as more employees worked in remote locations.
- Terminologies to understand how VPNs work.

# Private Networks vs. Virtual Private Networks

- ★ Employees can access the network (Intranet) from remote locations.
- ★ Secured networks.
- ★ The Internet is used as the backbone for VPNs
- ★ Saves cost tremendously from reduction of equipment and maintenance costs.
- ★ Scalability

# Remote Access Virtual Private Network



# Brief Overview of How it Works

- ✓ Two connections – one is made to the Internet and the second is made to the VPN.
- ✓ Datagrams – contains data, destination and source information.
- ✓ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✓ Protocols – protocols create the VPN tunnels.



# Four Critical Functions

- ❑ Authentication – validates that the data was sent from the sender.
- ❑ Access control – limiting unauthorized users from accessing the network.
- ❑ Confidentiality – preventing the data to be read or copied as the data is being transported.
- ❑ Data Integrity – ensuring that the data has not been altered

# Encryption

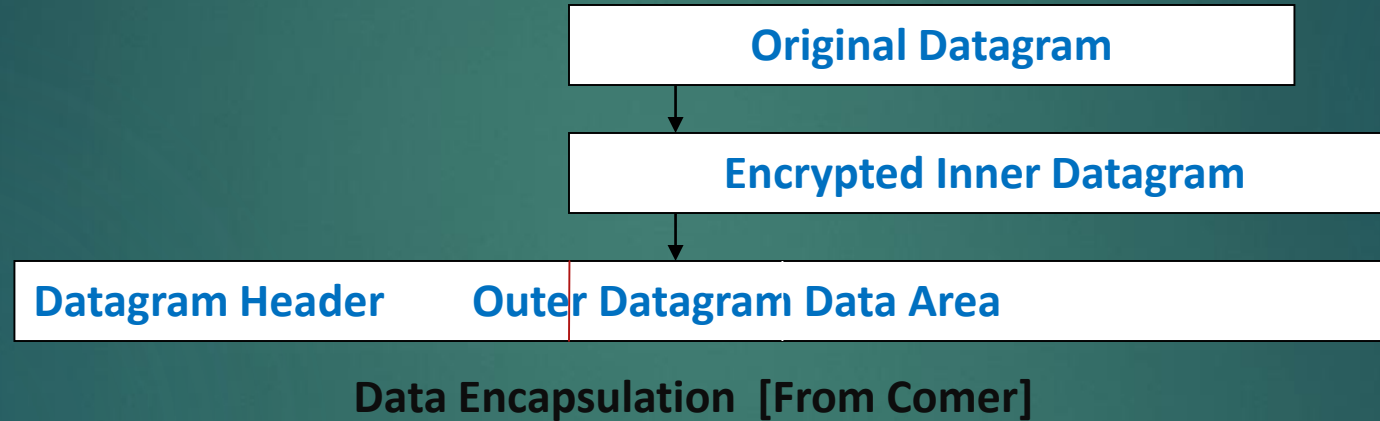
- ▶ Encryption -- is a method of “scrambling” data before transmitting it onto the Internet.
- ▶ Public Key Encryption Technique
- ▶ Digital signature – for authentication

# Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.

# Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.



**Two types of end points:**

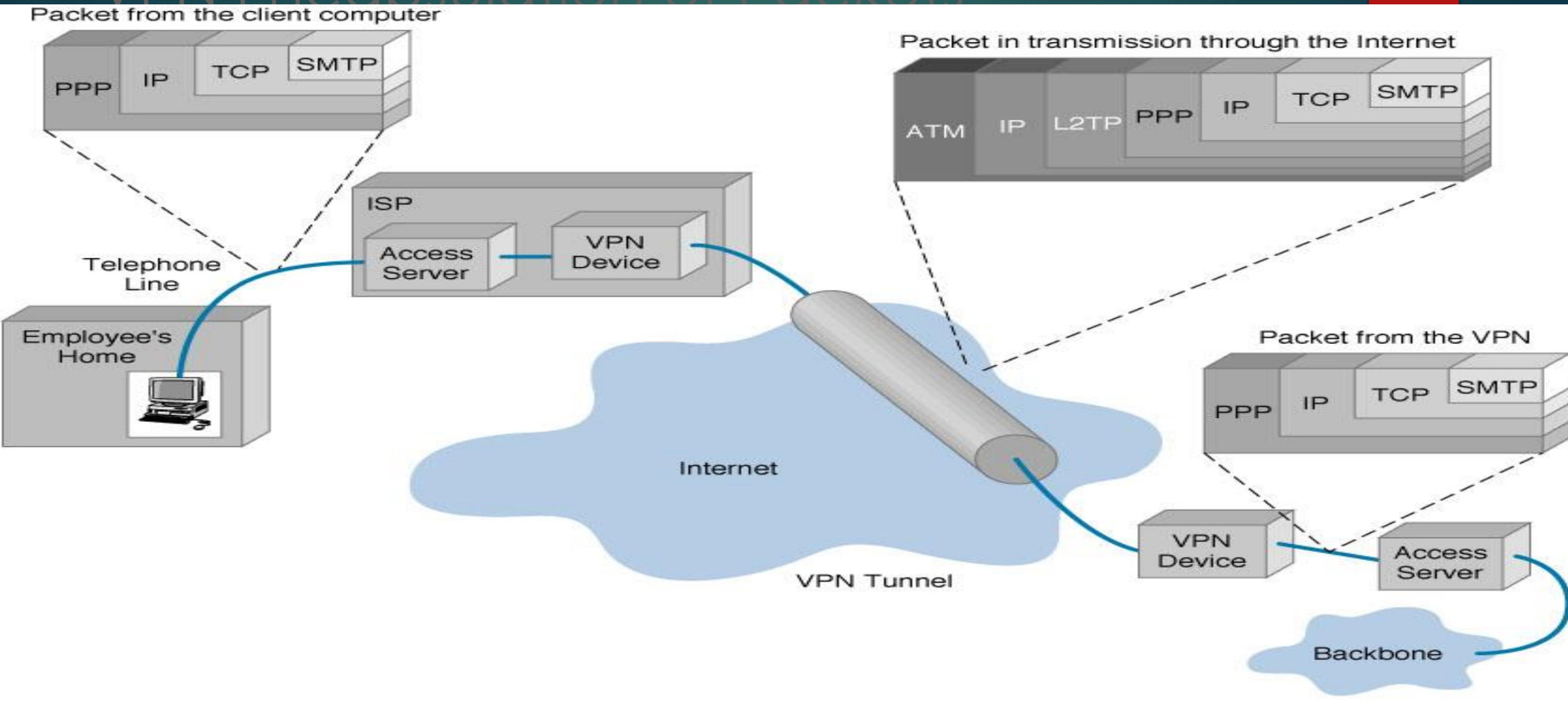
- ☐ Remote Access
- ☐ Site-to-Site



# Protocols used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security

# VPN Encapsulation of Packets

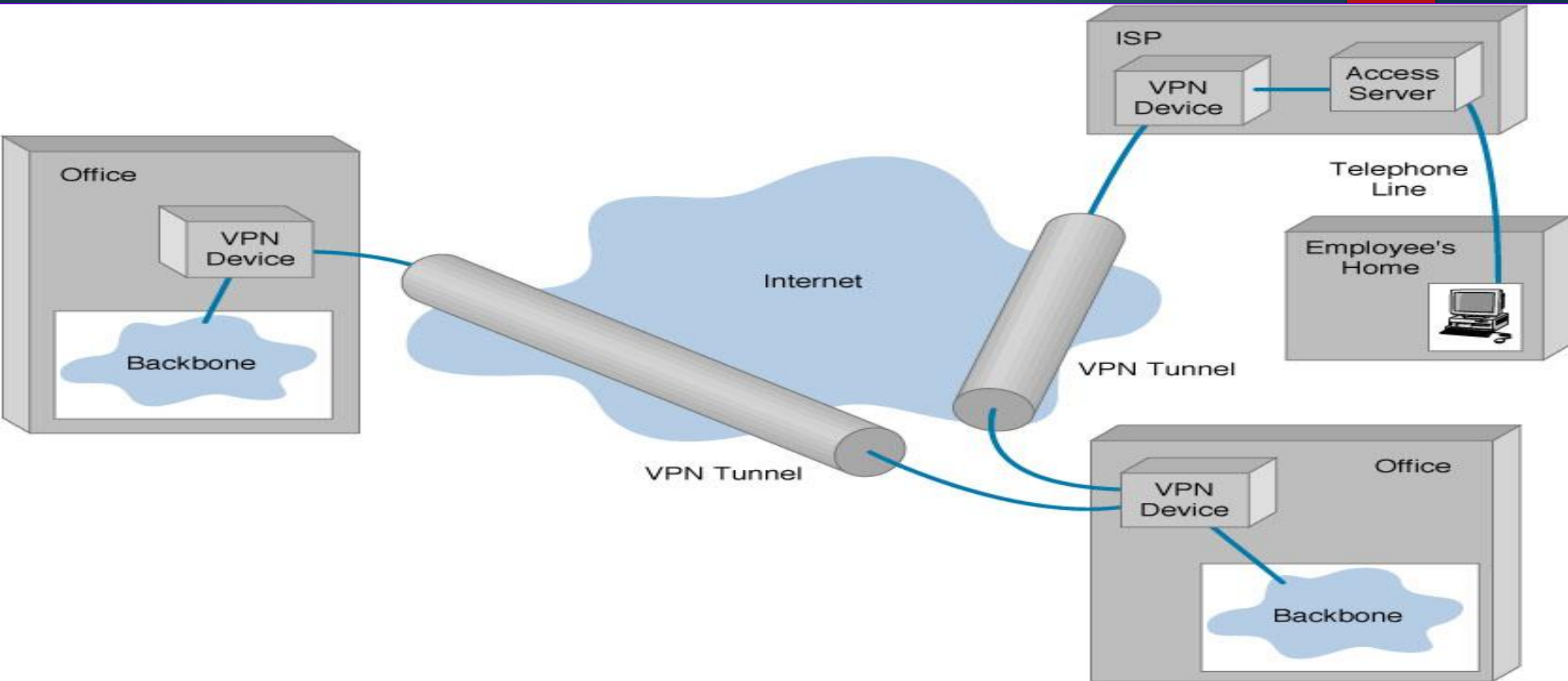


# Types of Implementations

- ❑ What does “implementation” mean in VPNs?
- ❑ 3 types
  - ❑ Intranet – Within an organization
  - ❑ Extranet – Outside an organization
  - ❑ Remote Access – Employee to Business

# Virtual Private Networks (VPN)

## Basic Architecture





# Device Types

- ▶ What it means
- ▶ 3 types
  - ▶ Hardware
  - ▶ Firewall
  - ▶ Software

# Device Types: Hardware

- ▶ Usually a VPN type of router

## Pros

- Highest network throughput
- Plug and Play
- Dual-purpose

## Cons

- Cost
- Lack of flexibility

# Device Types: Firewall

- ▶ More security?

## Pros

- “Harden” Operating System
- Tri-purpose
- Cost-effective

## Cons

- Still relatively costly

# Device Types: Software

- ▶ Ideal for 2 end points not in same org.
- ▶ Great when different firewalls implemented

## Pros

- Flexible
- Low relative cost

## Cons

- Lack of efficiency
- More labor training required
- Lower productivity; higher labor costs



# Advantages VS. Disadvantages



# Advantages: Cost Savings

- ▶ Eliminating the need for expensive long-distance leased lines
- ▶ Reducing the long-distance telephone charges for remote access.
- ▶ Transferring the support burden to the service providers
- ▶ Operational costs

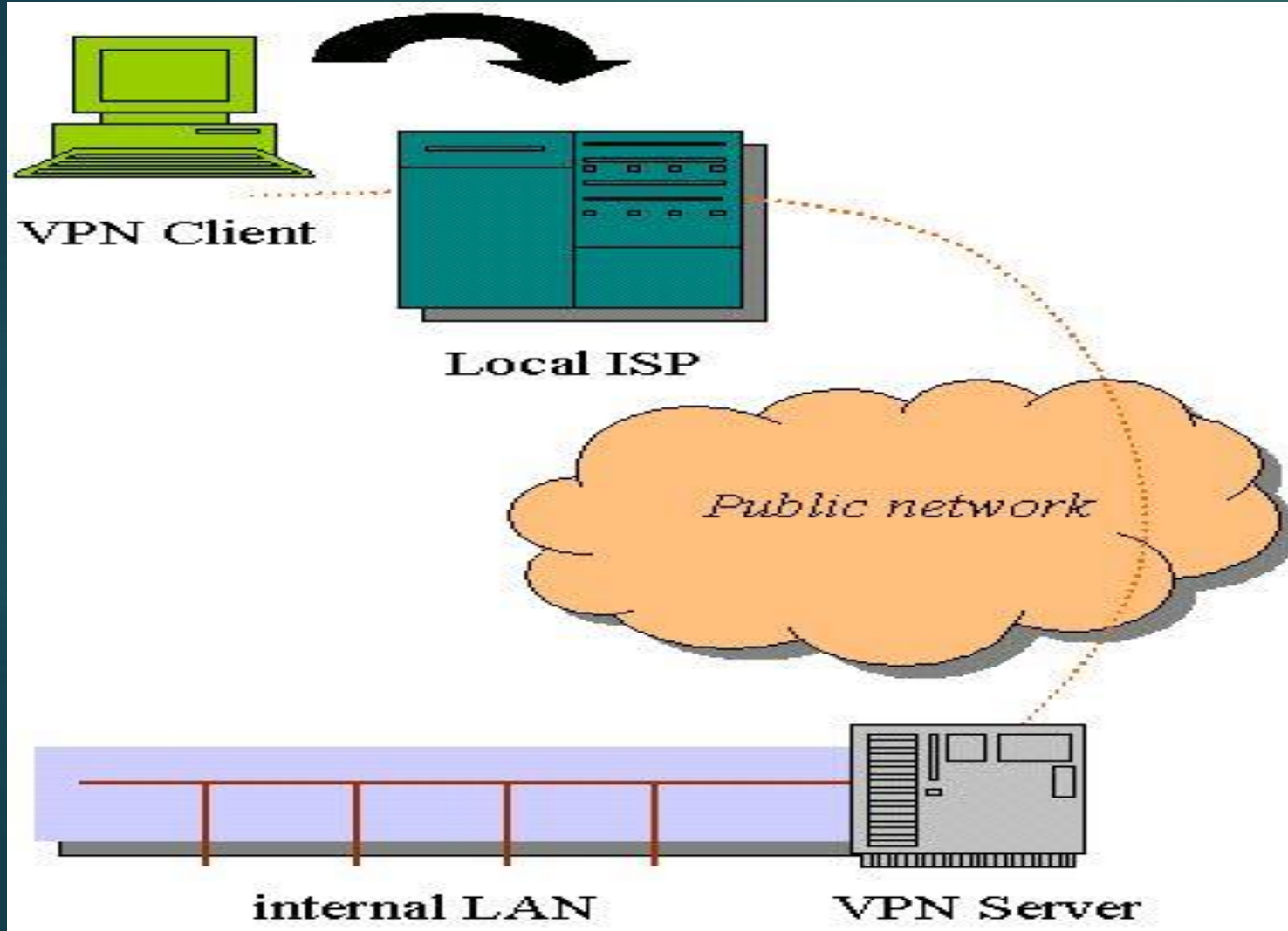
## Advantages: Scalability

- Flexibility of growth
- Efficiency with broadband technology

# Disadvantages

- ❏ VPNs require an in-depth understanding of public network security issues and proper deployment of precautions
- ❏ Availability and performance depends on factors largely outside of their control
- ❏ Immature standards
- ❏ VPNs need to accommodate protocols other than IP and existing internal network technology

# Site-to-Site VPNs



Application : Site to Site VPN

- ❁ Large-scale encryption between multiple fixed sites such as remote offices and central offices
- ❁ Network traffic is sent over the branch office Internet connection
- ❁ This saves the company hardware and management expenses

# Industries That May Use a VPN

- ❑ Healthcare: enables the transferring of confidential patient information within the medical facilities & health care provider
- ❑ Manufacturing: allow suppliers to view inventory & allow clients to purchase online safely
- ❑ Retail: able to securely transfer sales data or customer info between stores & the headquarters
- ❑ Banking/Financial: enables account information to be transferred safely within departments & branches
- ❑ General Business: communication between remote employees can be securely exchanged

# Where Do We See VPNs Going in the Future?

- ❁ VPNs are continually being enhanced.

*Example: Equant NV*

- ❁ As the VPN market becomes larger, more applications will be created along with more VPN providers and new VPN types.
- ❁ Networks are expected to converge to create an integrated VPN
- ❁ Improved protocols are expected, which will also improve VPNs.



# Virtual Private Networks (VPNs)

- **Virtual**

- Emulated connectivity over a public network

- **Private**

- Access limited to VPN members
- Total address and route separation

- **Network**

- A collection of customer sites

Site Connectivity with Leased Lines

Site Connectivity with VPN

Shared public network (Frame Relay, ATM, IP)

Cost reduction

Network efficiency

# Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL. Similar to the North American T-1, E1 is the European format for digital transmission. E1 carries signals at 2 Mbps (32 channels at 64Kbps, with 2 channels reserved for signaling and controlling), versus the T1, which carries signals at 1.544 Mbps (24 channels at 64Kbps).

# Basic MPLS Control Plane

**MPLS control plane**

**=**

**IP control plane**

**+**

**label distribution**

**Label distribution protocols are needed to**

- (1) create label ↔ FEC bindings**
- (2) distribute bindings to neighbors,**
- (3) maintain consistent label swapping tables**



**Thank you !**