BEGINNER TO EXPERT GUARANTEED

CCNA COURSE

ACCESS MORE COURSES PLAYLIST LINK IN DESCRIPTION

SUBSCRIBE!!!

CISCO CERTIFIED NETWORK ASSOCIATE

PREFACE

CCNA is the popular certification course by CISCO. CISCO is the most popular company in manufacturing and selling networking equipment globally. They conduct an exam named that consists of one hundred twenty questions. If you pass the exam, you can become CCNA certified. It is an Information Technology Certification Course. This course certifies your skills in network fundamentals, network access, IP connectivity, IP services, security fundamentals, automation, and programmability. This course is an associate-level course developed for network engineers.

1.CCNA Routing and Switching
2.CCNA Cyber Ops
3.CCNA Wireless
4.CCNA Cloud
5.CCNA Data Center
6.CCNA Security
7.CCNA Collaboration
8.CCNA Industrial
9.CCNA Service Provider

CCNP

Course	CCNA
Full form	CISCO Certified Network Associate
Duration of Certification	3 Years
Fee Structure	150 USD to 350 USD
Course Type	Certification
Starting salary offered	4.5 Lacs to 8 Lacs Per Annum
Employment opportunities	Network Administrator Network Engineer Network and Support Technician System Engineer Network Designer Network Planner Network Implementer Network Optimizer Network Support Executive Security Specialist Security Administrator Support Engineer

Top Recruiters of CCNA Certified Professionals

1.TATA Consultancy Services
2.Reliance Communications
3.JIO Communications
4.Orient Technologies
5.HCL Technologies
6.Dimension Data
7.Tech Mahindra
8.Bharti Airtel
9.Vodafone
10.Wipro

TOPICS

1. BASIC NETWORKING FUNDAMENTALS
2. LAYER 2 & LAYER 3 SWITCHES EXPLANATION
3. ROUTERS & CISCO ROUTERS EXPLAINED
4. WAN & SOHO FULL BRIEFLY EXPLAINED
5. TYPES OF CABLES (TWISTED, COAXIAL & FIBER)
6. CABLE ISSUES (COLLISIONS, ERRORS & SPEED)
7. TCP & UDP FULL INFORMATION
8. IPV4 FULL ROCKET SCIENCE
9. IPV6 FULL ROCKET SCIENCE
10. SUBNETTING FULL ROCKET SCIENCE
11. UNICAST, MULTICAST, ANYCAST & BROADCAST
12. WIRELESS TERMS (SSID, CHANNEL & ENCRYPTION)
13. VIRTUALIZATION FUNDAMENTALS (VIRTUAL MACHINES)
14. WLAN FULL CONCEPTS EXPLAINED
15. VLAN FULL CONCEPTS EXPLAINED

TOPICS

16. OSI MODEL WITH ALL LAYERS
17. ACCESS POINTS WITH CONFIGURATIONS
18. WLC WITH FULL CONFIGURATION
19. PORTS FULL INFORMATION
20. CLOUD SERVICES BRIEF EXPLANATION
21. ROUTING WITH ROUTING TABLES CONCEPTS
22. FTP & TFTP FUNCTIONS & CAPABILITIES
23. SYSLOG SERVER WITH ALL FEATURES
24. SSH & TELNET WITH CONFIGURATION
25. UNDERSTANDING NETWORK SECURITY CONCEPTS
26. DNS & DHCP SERVICES WITH CONFIGURATION
27. DEFERNITE AUTHORIZATION & AUTHENTICATION
28. AUTOMATION & PROGRAMMING IN CCNA
29. REST BASED APIS (CRUD & DATA ENCODING)
30. DESIGNING AN INFRA USING ALL CONCEPTUAL SCENARIOS

1.

Basic Networking Fundamentals

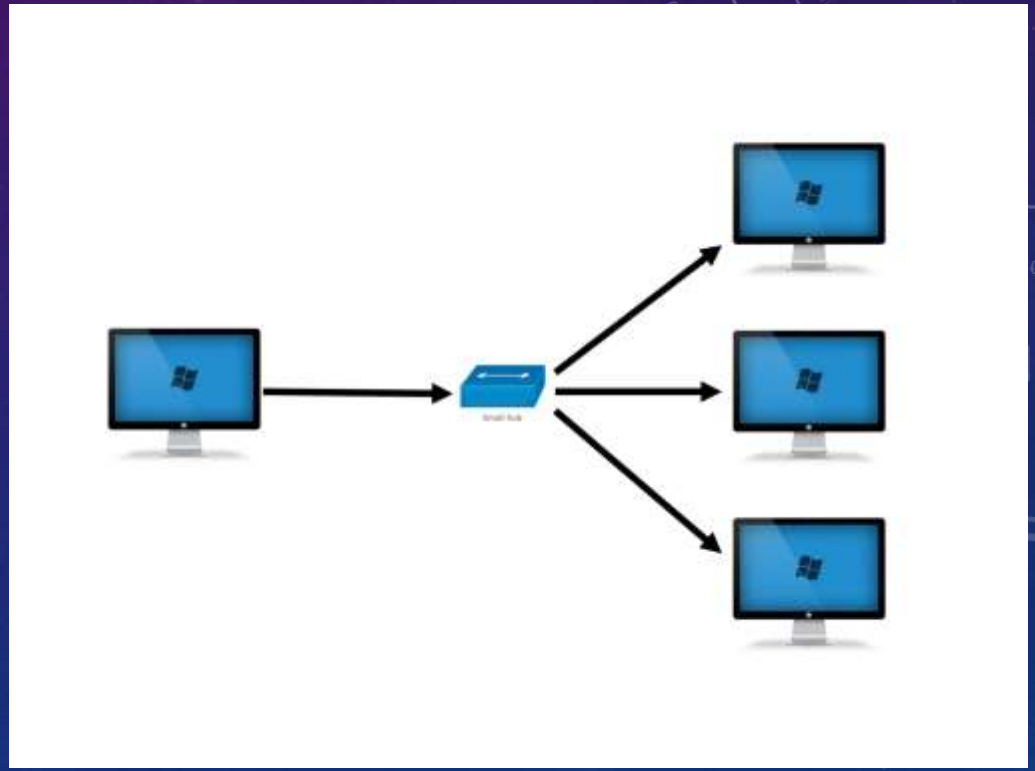
WHAT IS NETWORK ?

- A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.

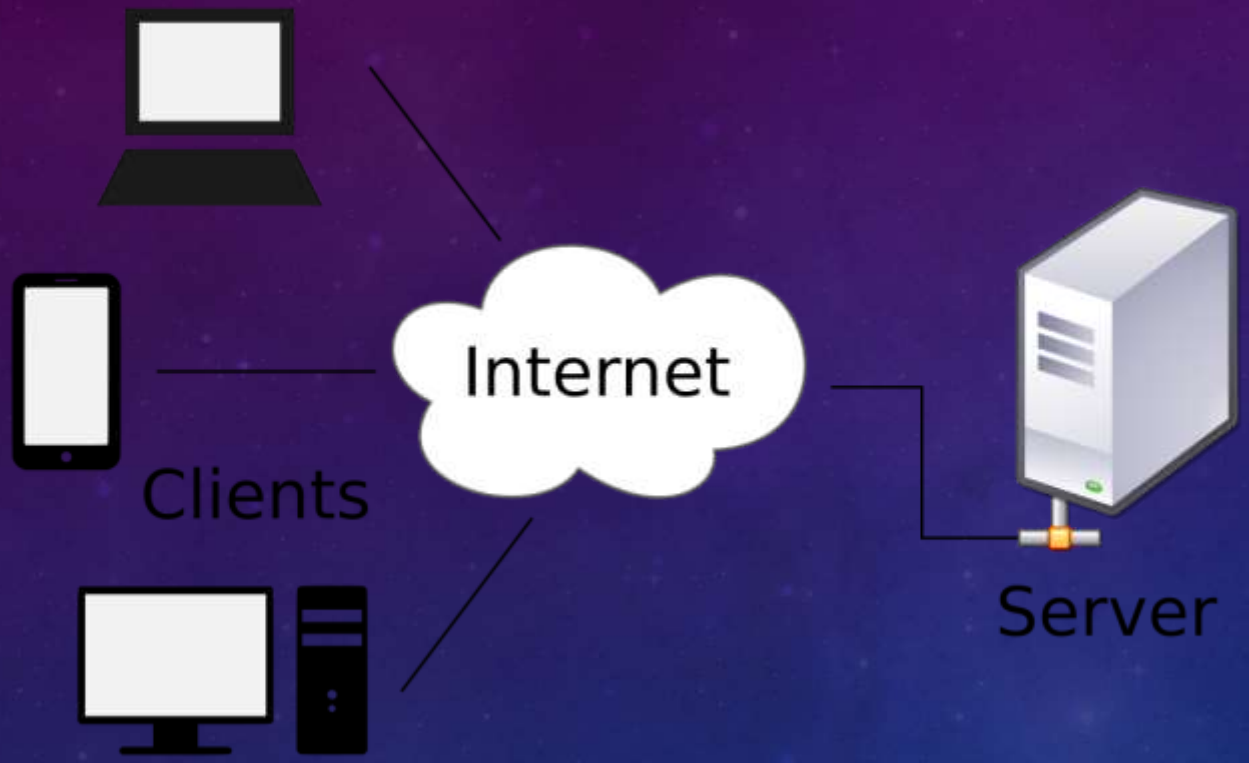
- The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

What is Networking ?

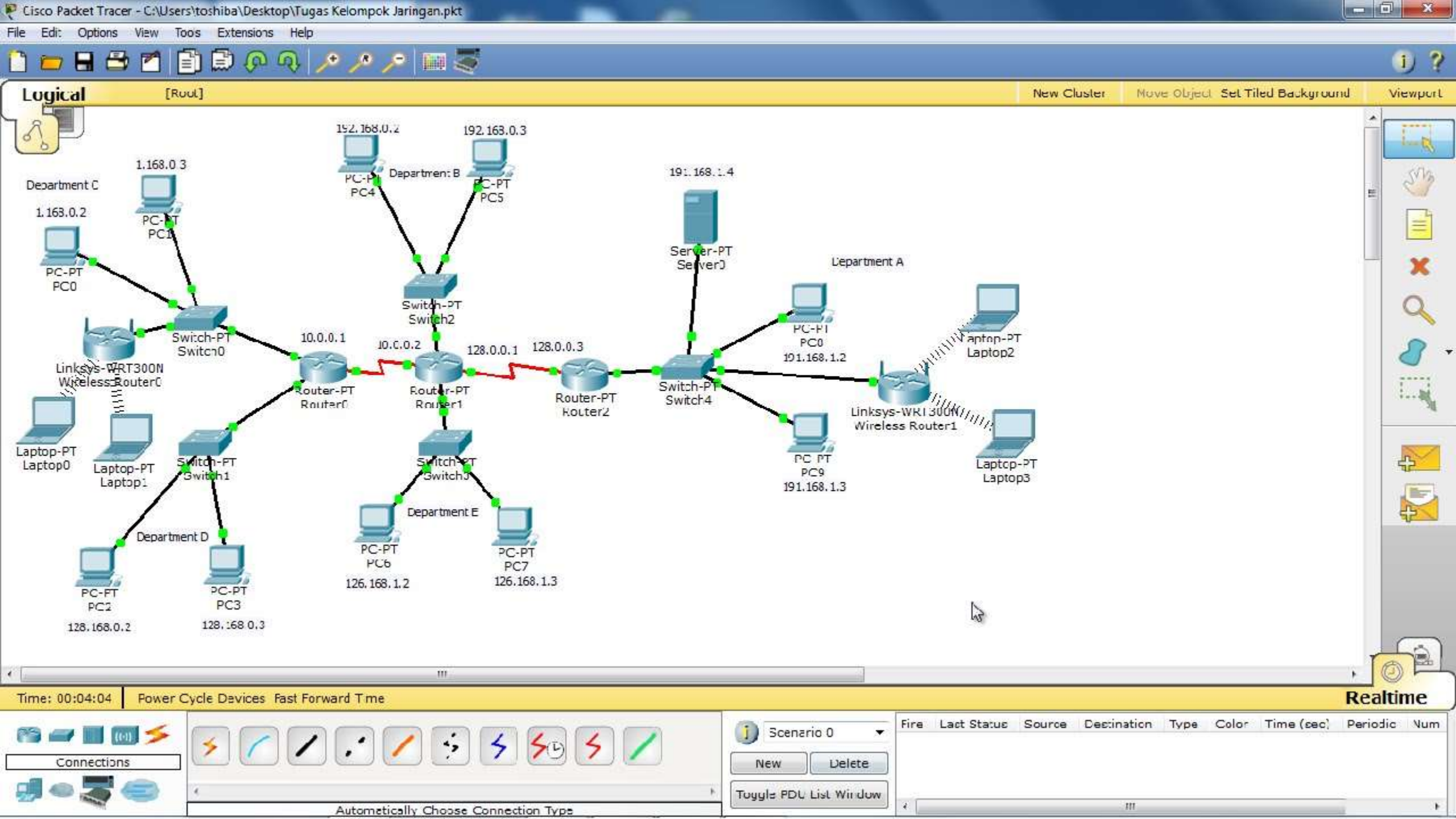
Networking, also known as computer networking, is the practice of transporting and exchanging data between nodes over a shared medium in an information system. Networking comprises not only the design, construction and use of a network, but also the management, maintenance and operation of the network infrastructure, software and policies.



Peer to Peer Model

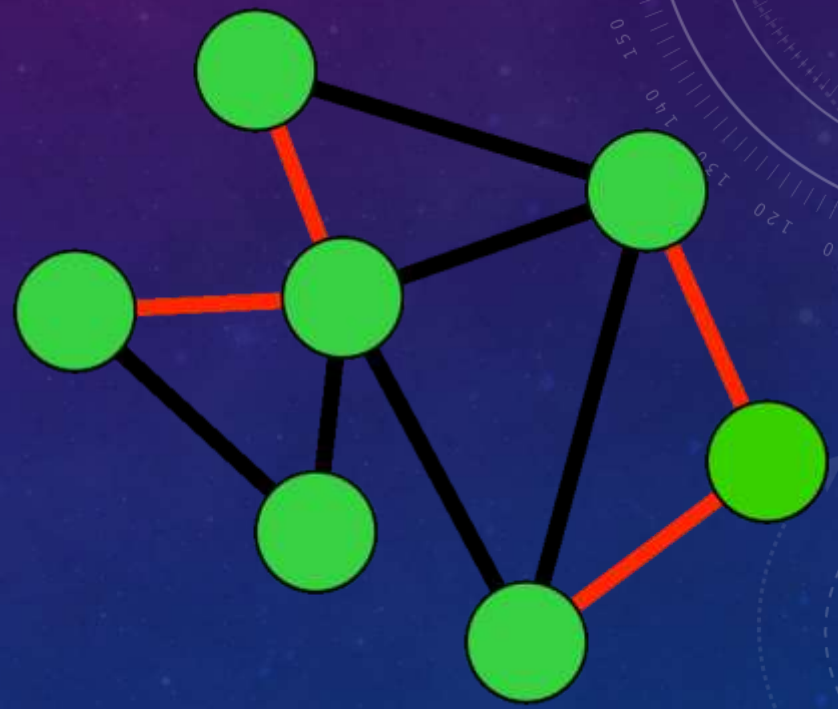


Client-Server Model


Cisco Packet Tracer - C:\Users\toshiba\Desktop\Tugas Kelompok Jaringan.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
192.168.0.2
192.168.0.3
Department B
PC-PT PC4
PC-PT PC5
1.168.0.3
Department C
1.168.0.2
PC-PT PC1
PC-PT PC0
Switch-PT Switch2
Server-PT Server0
Department A
Switch-PT Switch0
10.0.0.1
10.0.0.2
128.0.0.1
128.0.0.3
Linksys-WRT300N Wireless Router0
Router-PT Router0
Router-PT Router1
Router-PT Router2
Switch-PT Switch4
PC-PT PC0
191.168.1.2
Laptop-PT Laptop2
Linksys-WRT300N Wireless Router1
Laptop-PT Laptop0
Laptop-PT Laptop1
Switch-PT Switch1
Switch-PT Switch3
PC-PT PC9
191.168.1.3
Laptop-PT Laptop3
Department D
Department E
PC-PT PC6
126.168.1.2
PC-PT PC7
126.168.1.3
PC-PT PC2
128.168.0.2
PC-PT PC3
128.168.0.3
Time: 00:04:04
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num

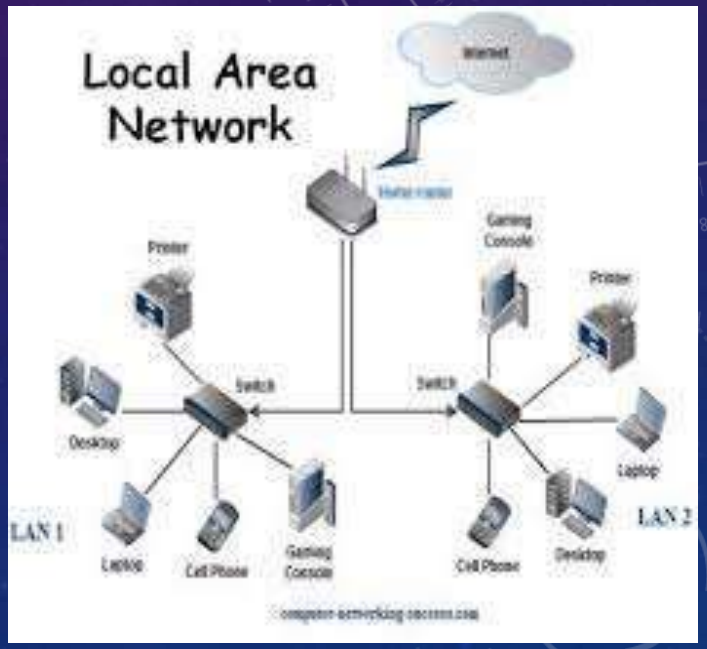
BASIC TYPES OF NETWORKS

1. Local Area Network **(LAN)**
2. Personal Area Network (PAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)
5. Campus Area Network (CAN)



LOCAL AREA NETWORK (LAN)

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users • • Is limited in size, typically spanning a few hundred meters, and no more than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's
- LAN's can be either wired or wireless. Twisted pair, coax or fibre optic cable can be used in wired LAN's.



PERSONAL AREA NETWORK (PAN)

- A PAN is a network that is used for communicating among computer devices, usually home.
- PAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users • • Is limited in size, typically spanning a few hundred meters
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's
- LAN's can be either wired or wireless. Twisted pair, coax or fibre optic cable can be used in wired LAN's.

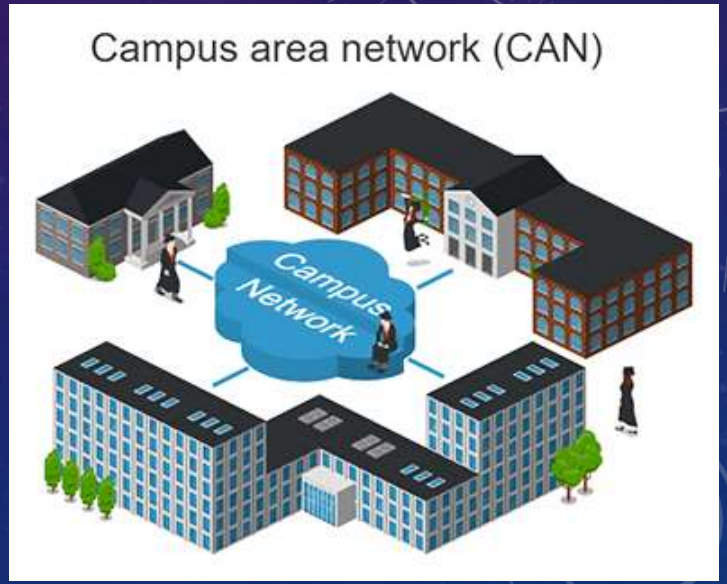
CAMPUS AREA NETWORK (CAN)

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area. A CAN is smaller than a wide area network (WAN) or metropolitan area network (MAN).

- A CAN is also known as a corporate area network (CAN).

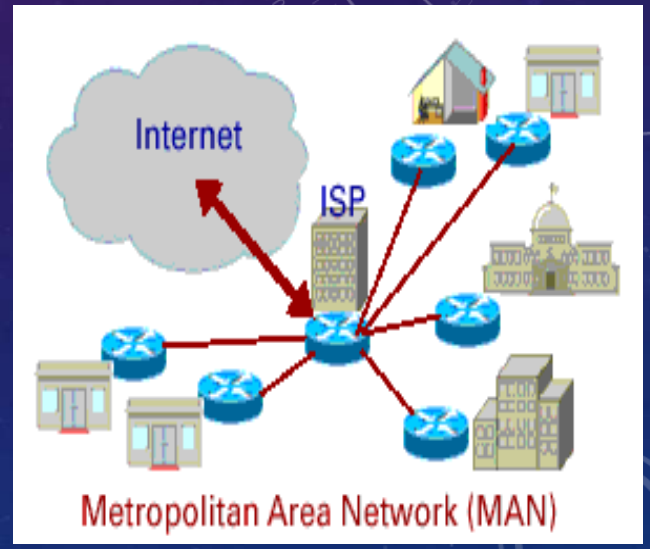
- CAN benefits are as follows:

Cost-effective
Wireless, versus cable
Multidepartmental network access



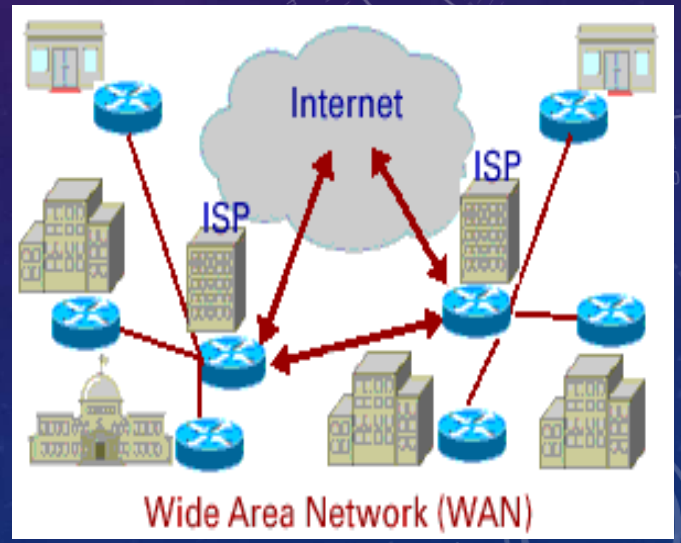
METROPOLITAN AREA NETWORK (MAN)

- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.



WIDE AREA NETWORK (WAN)

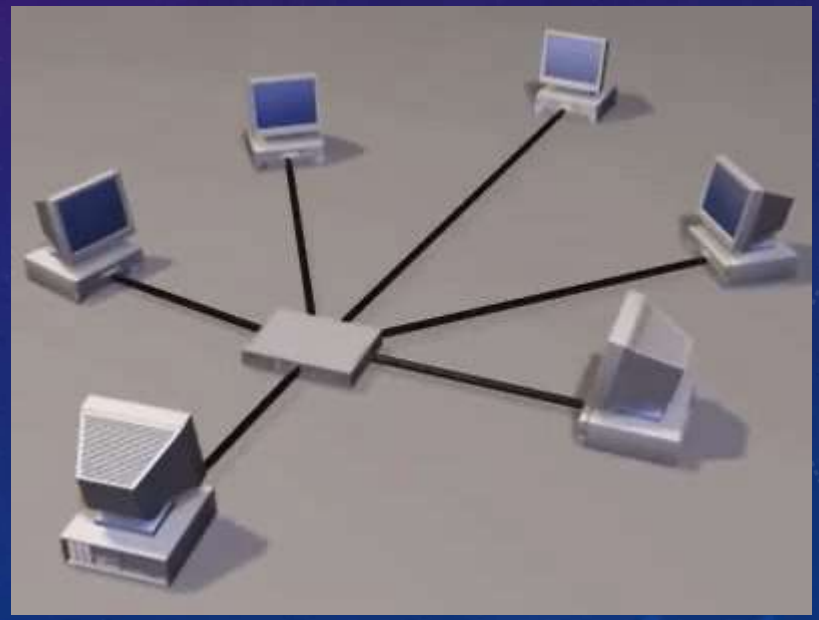
- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.



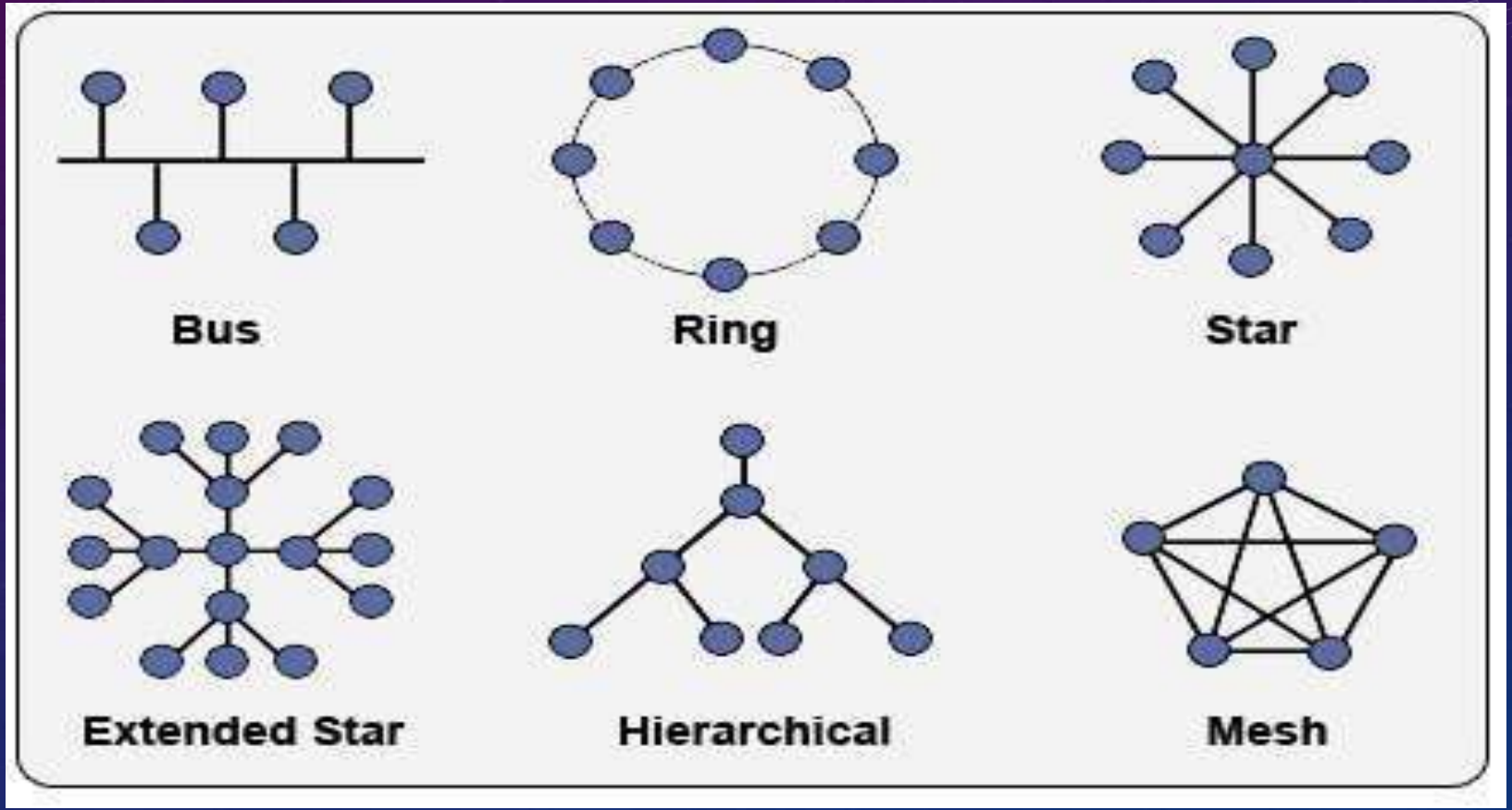
TOPOLOGY

- Topology refers to the layout of connected devices on a network.
- Here, some logical layout of topology.

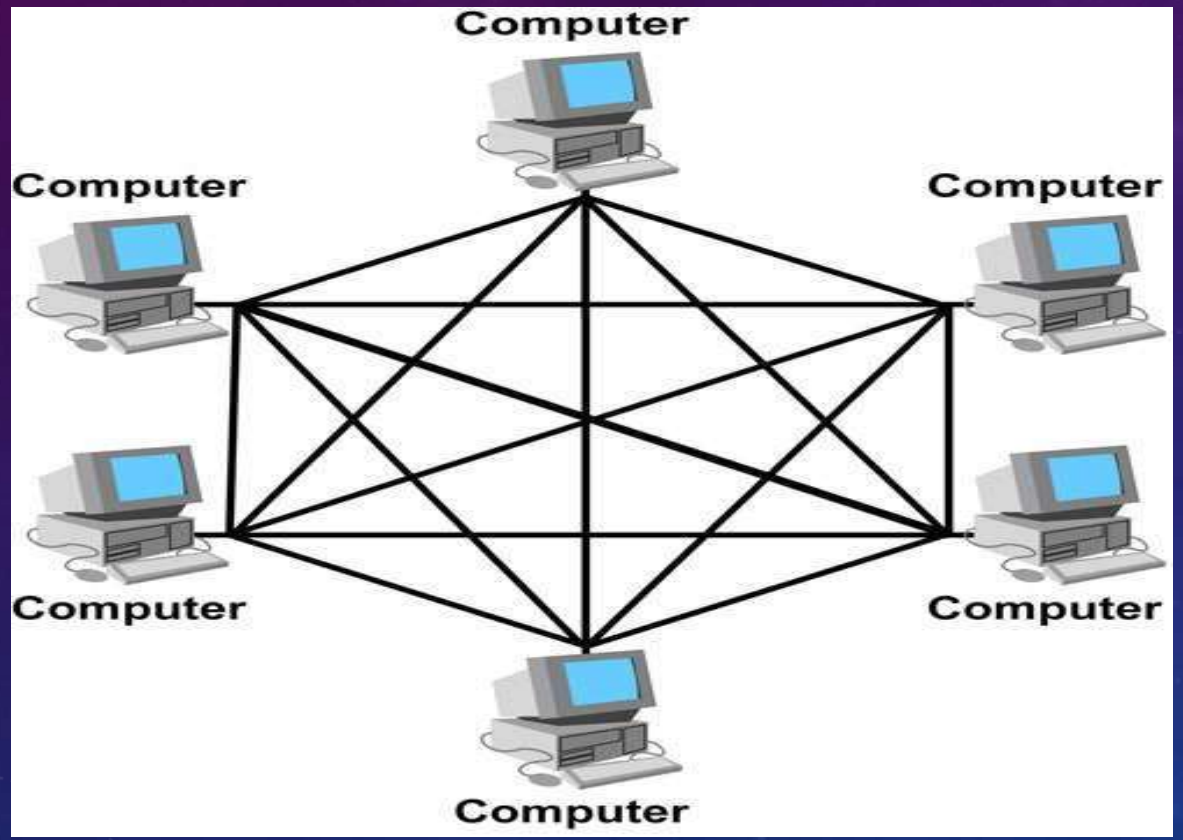
  - Mesh
  - Star
  - Ring
  - Line
  - Bus
  - Tree
  - Hybrid

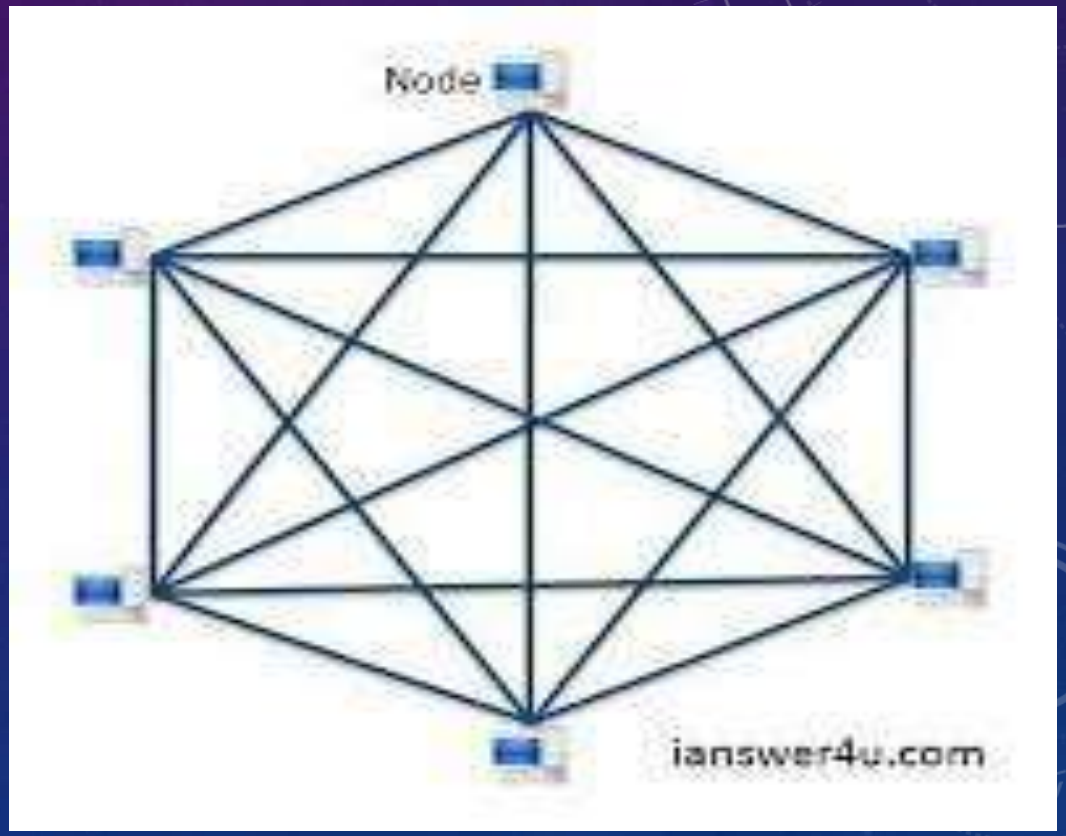


NETWORK TOPOLOGY

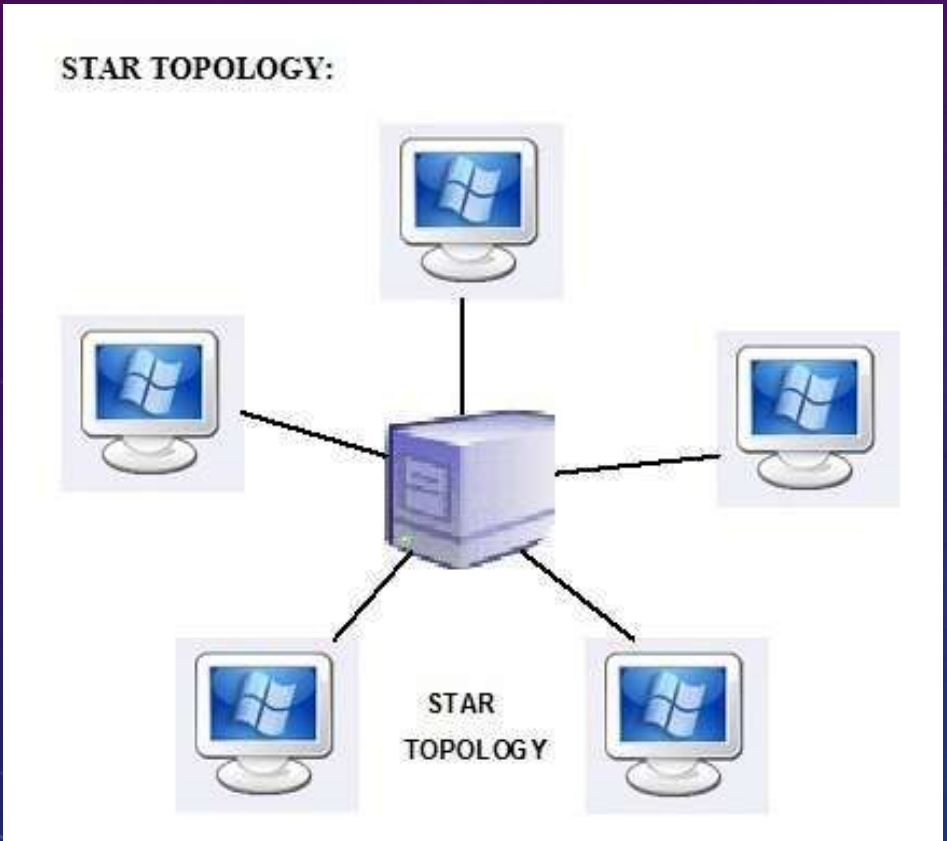


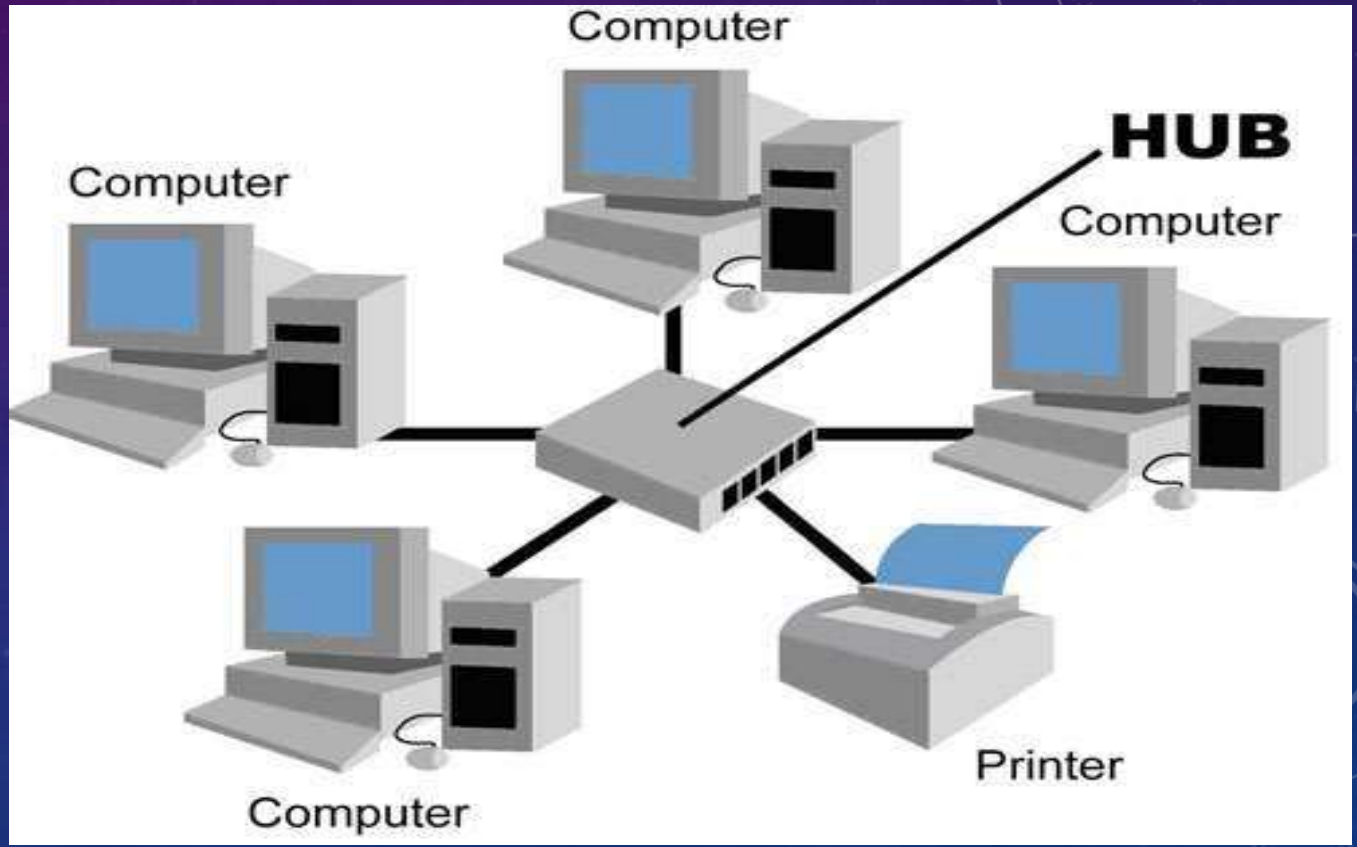
Mesh Topology



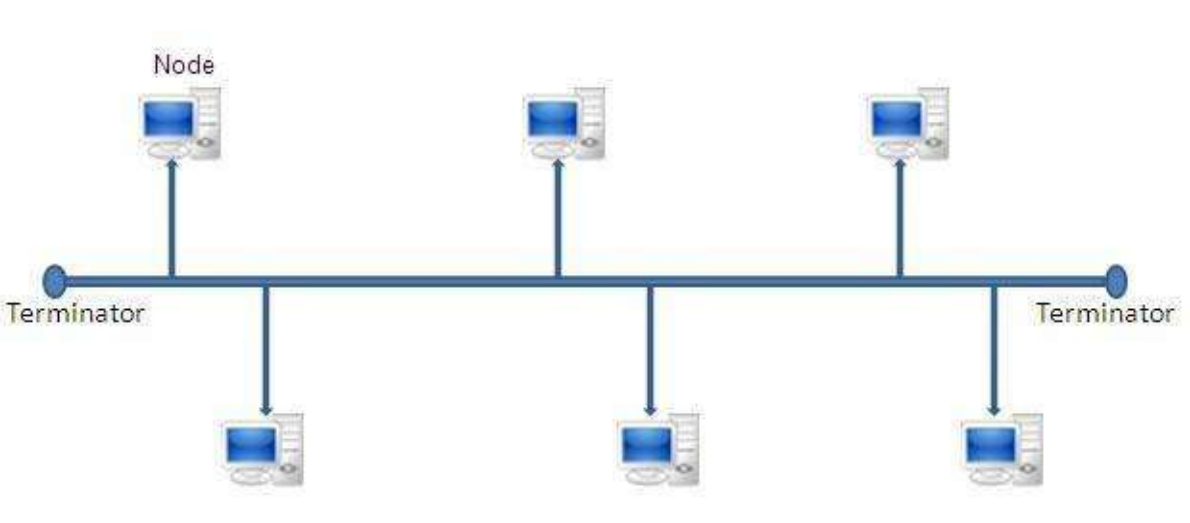


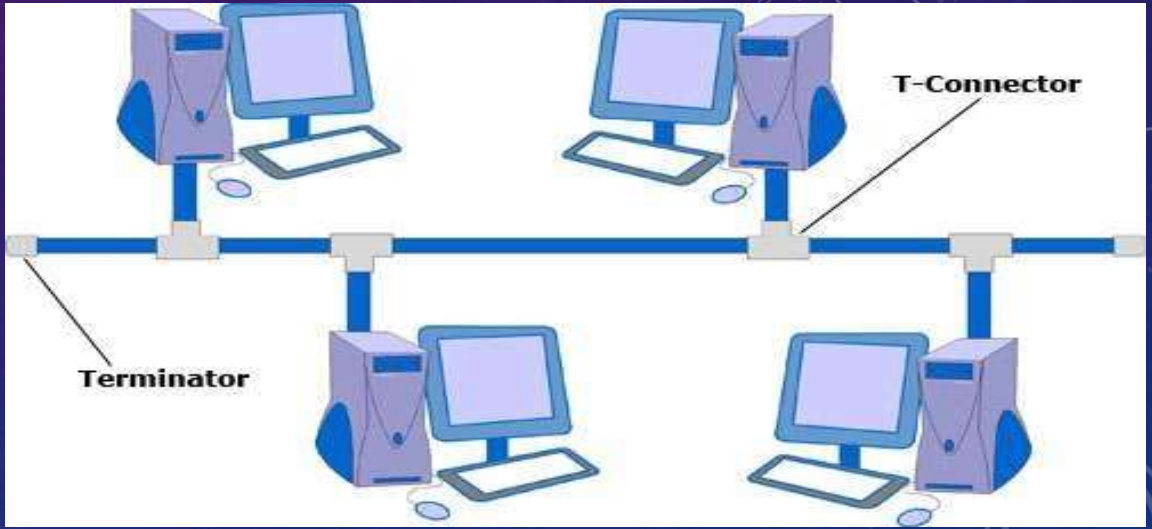
Star Topology



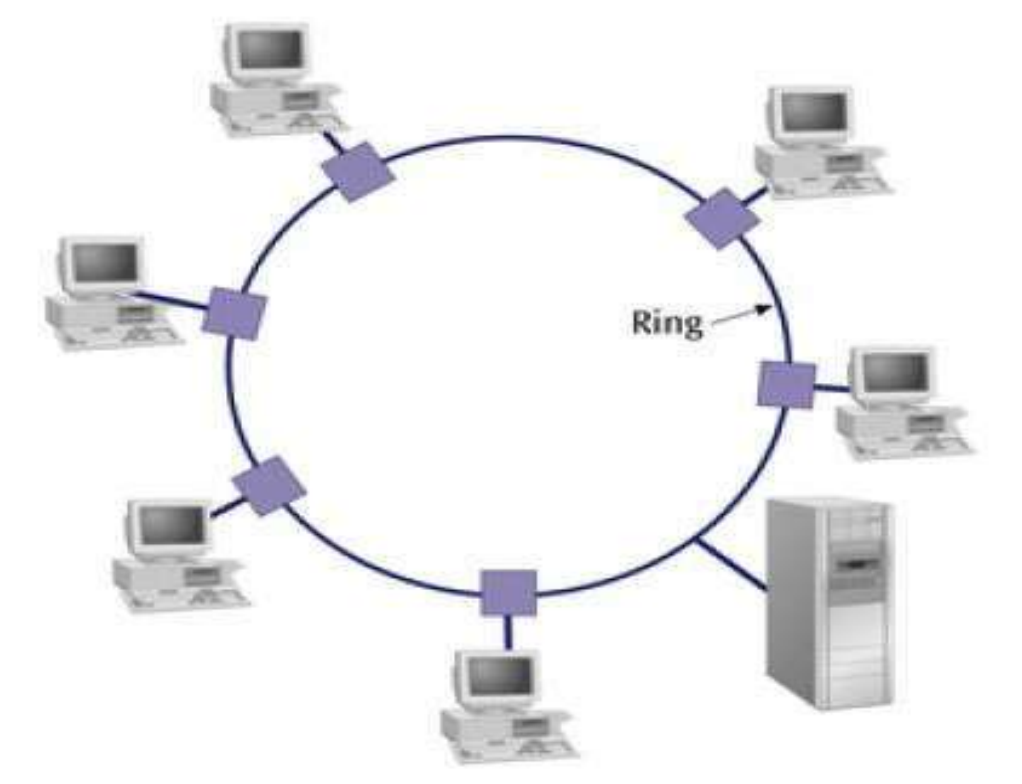


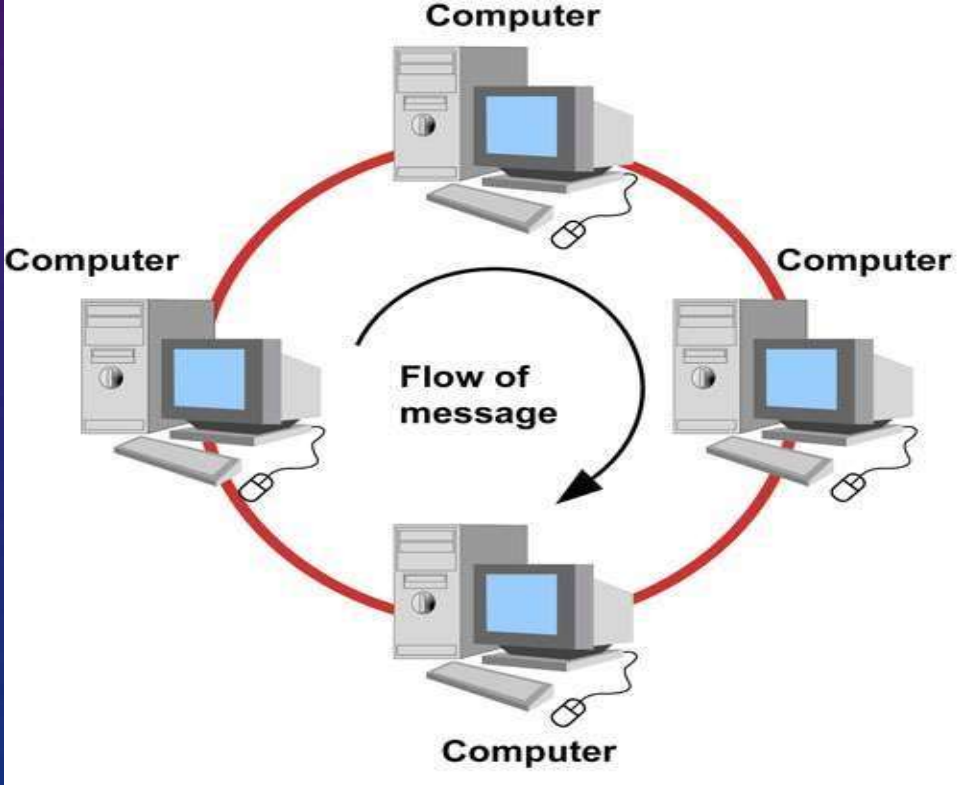
BUS TOPOLOGY



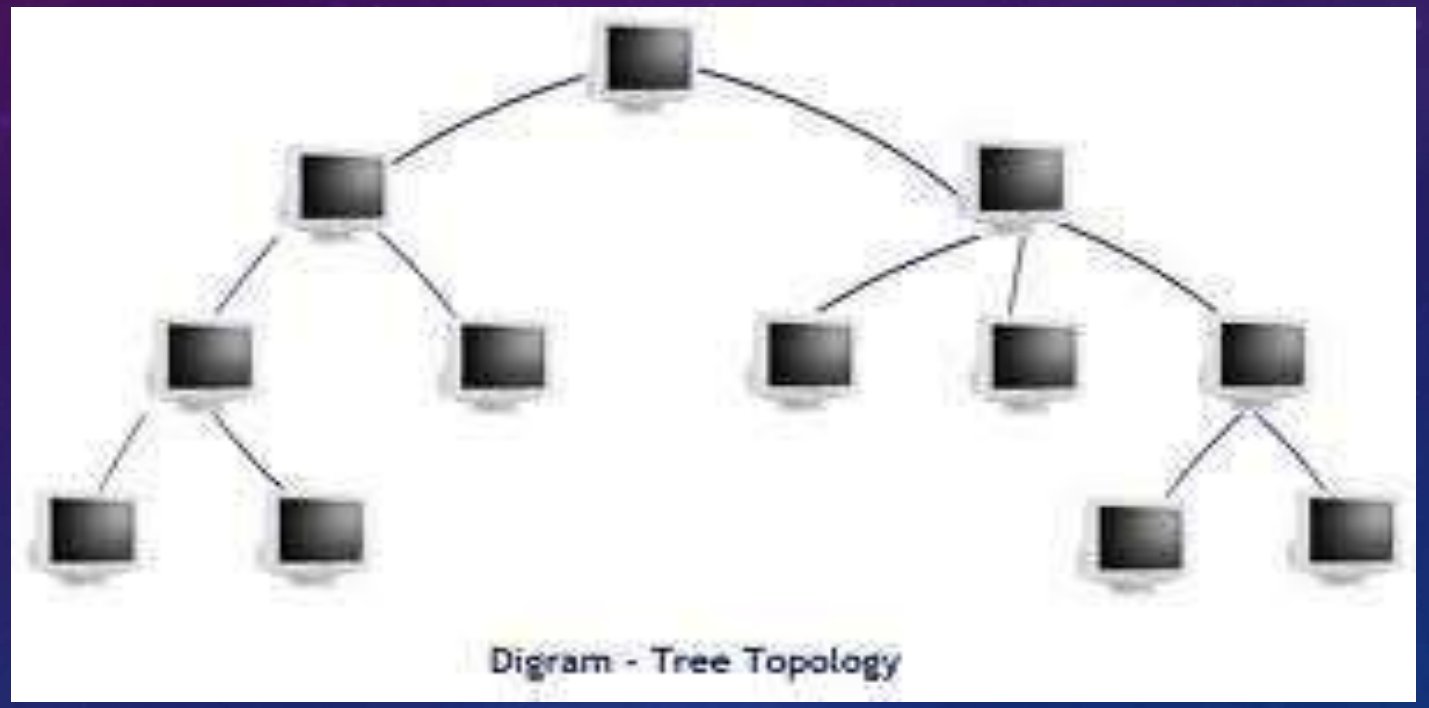


RING TOPOLOGY





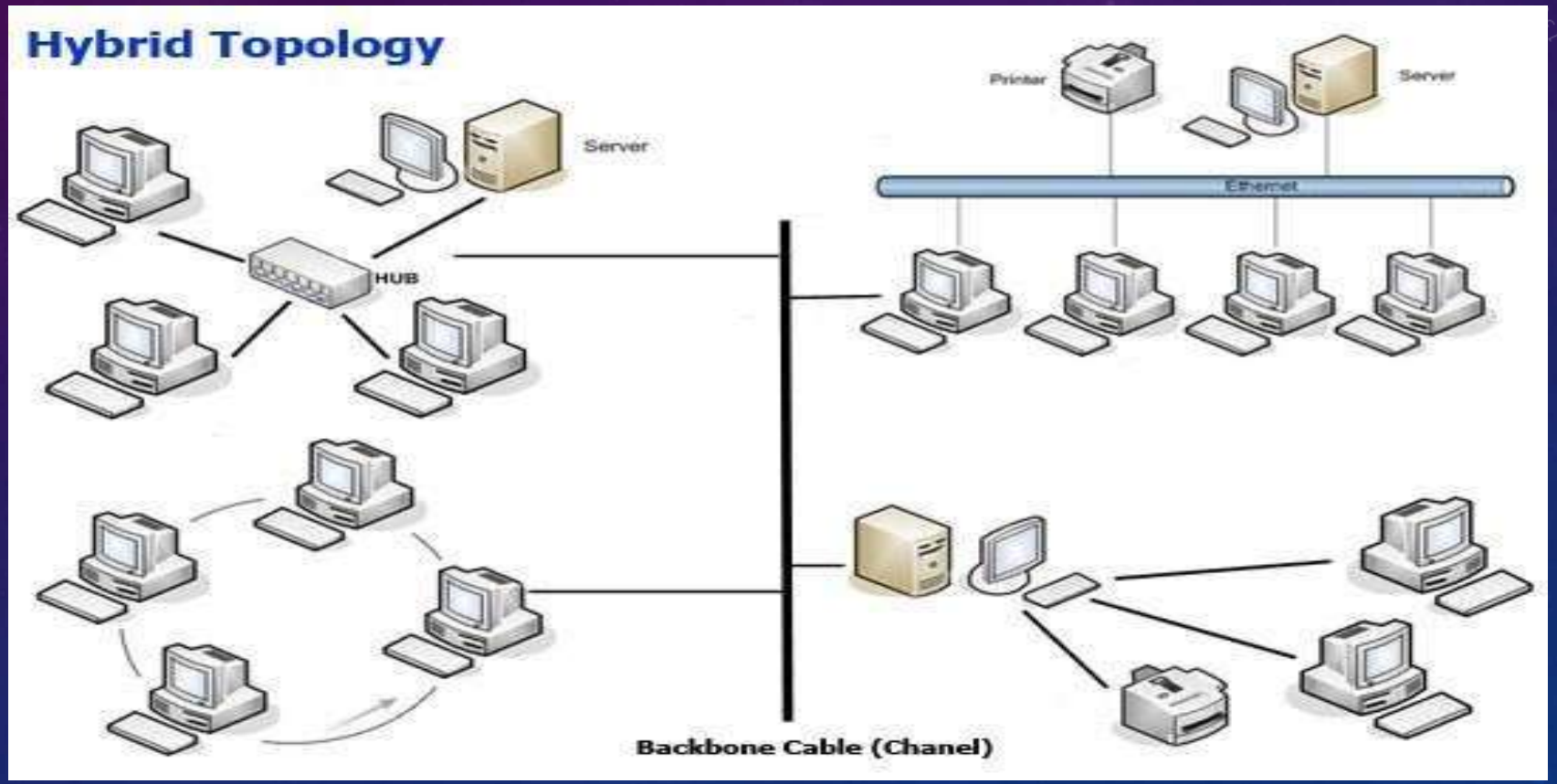
TREE TOPOLOGY



Digram - Tree Topology

HYBRID TOPOLOGY

- A network which contain all type of physical structure and connected under a single backbone channel.



INTRODUCTION

- To connect LANs, connecting devices are needed and various connecting devices are such as bridge, switch, router, hub, repeater.
- Types of Networking Devices :-

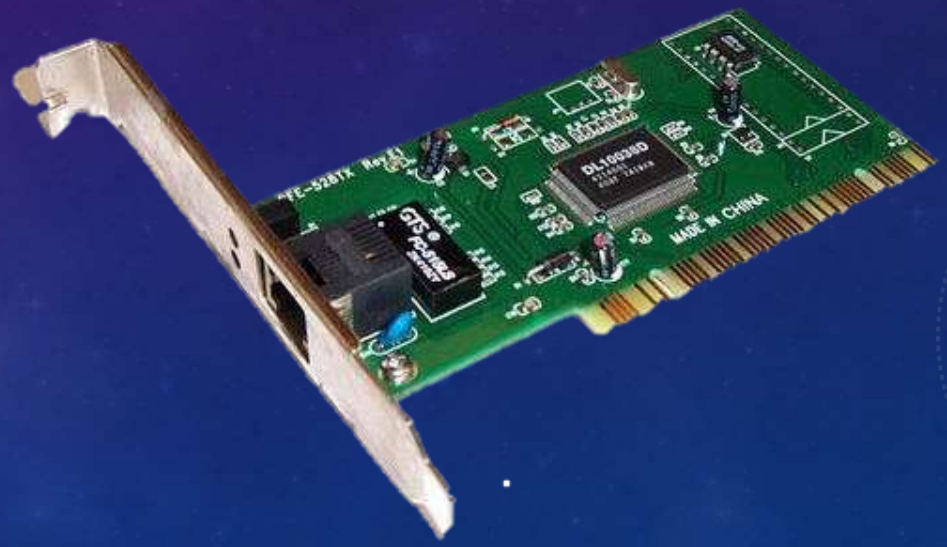
1. NIC Card
2. Repeater
3. Hub
4. Bridge
5. Switch
6. Gateway
7. Router
8. Modem

NIC OR NETWORK CARD

It stands for Network Interface Controller. NIC used to connect the ethernet cable (RJ-45 Connector) with the PC. It is a Card which have Mac Address written on it.

Components of NIC:-

1. Metal Expansion Card
2. Boot ROM Chip
3. 32 bit PCI Controller
4. Activity LED
5. RJ-45 LAN Port



REPEATERS

Repeater used to regenerate or replicate a signal. It removes the unwanted noise in an incoming signal, it works on Layer 1 of OSI Model

It is used in some scaled area and it refine the signals and manage the proper speed of the network

HUB

It is a Networking Device which simply receive data from one port and transfer on all the other ports. HUBs are commonly used to connect segments of LAN. Hub Works on Physical layer of OSI Model

It used in where you have to create multiple ethernet with the help of a nnetworking device. It comes with different port segment like 6,12 & 24

Bridge

Bridge Devices inspect incoming network traffic and determine whether to forward or discard it according to its intended destination it operates on data link layer

A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.

Switch

A Switch can recieve input or signal from any of one port and transmit it on all the ports. Ethernet LAN is used to connect to a switch that correct system. It works on Data link layer of OSI Model

It is a small device that transfers data packets between multiple network devices such as computers, routers, servers or other switches

Gateway

Gateway Connects two networks together with the help of gateway devices like firewire & router. It is a node between the public network and private network which makes some security with the help of identification

A gateway is a networking device that connects two networks using different protocols together. it also acts as a "gate" between two networks.

Router

Router is a networking device which is used to provide interaction between two different networks. Router are also used for provide the routes to the data and devices that are connected in network. Router are used to establish internetwork communication

A router inspects a given data packet's destination Internet Protocol address (IP address), and provide connection to the nodes with the main network. It gives you wired and wireless both connectivities.

MODEM

”Modulator-Demodulator” A modem or broadband modem is a hardware device that connects a computer or router to a broadband network. It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize.

The main difference between the two devices is that a modem lets you connect to the internet, while a router distributes that connection to different devices. A modem is your gateway to the web, while a router is a central hub for your devices.

2.

L2 & L3 Switches Explanation

Switch

A Switch can recieve input or signal from any of one port and transmit it on all the ports. Ethernet LAN is used to connect to a switch that correct system. It works on Data link layer of OSI Model

It is a small device that transfers data packets between multiple network devices such as computers, routers, servers or other switches

Switch L2 vs L3

Layer 2 Switching

- Send “frames” to destination on the basis of MAC address.
- Work with MAC address only
- Used to reduce traffic on local network..

Layer 3 Switching

- Packets are forwarded at Layer 3, just as a router would do.
- It also performs dynamic routing in the same way in which a router performs
- Mostly Used to implement VLAN (Virtual Local area network)

Lets Verify…

3.

Routers & CISCO Routers Explained

Router

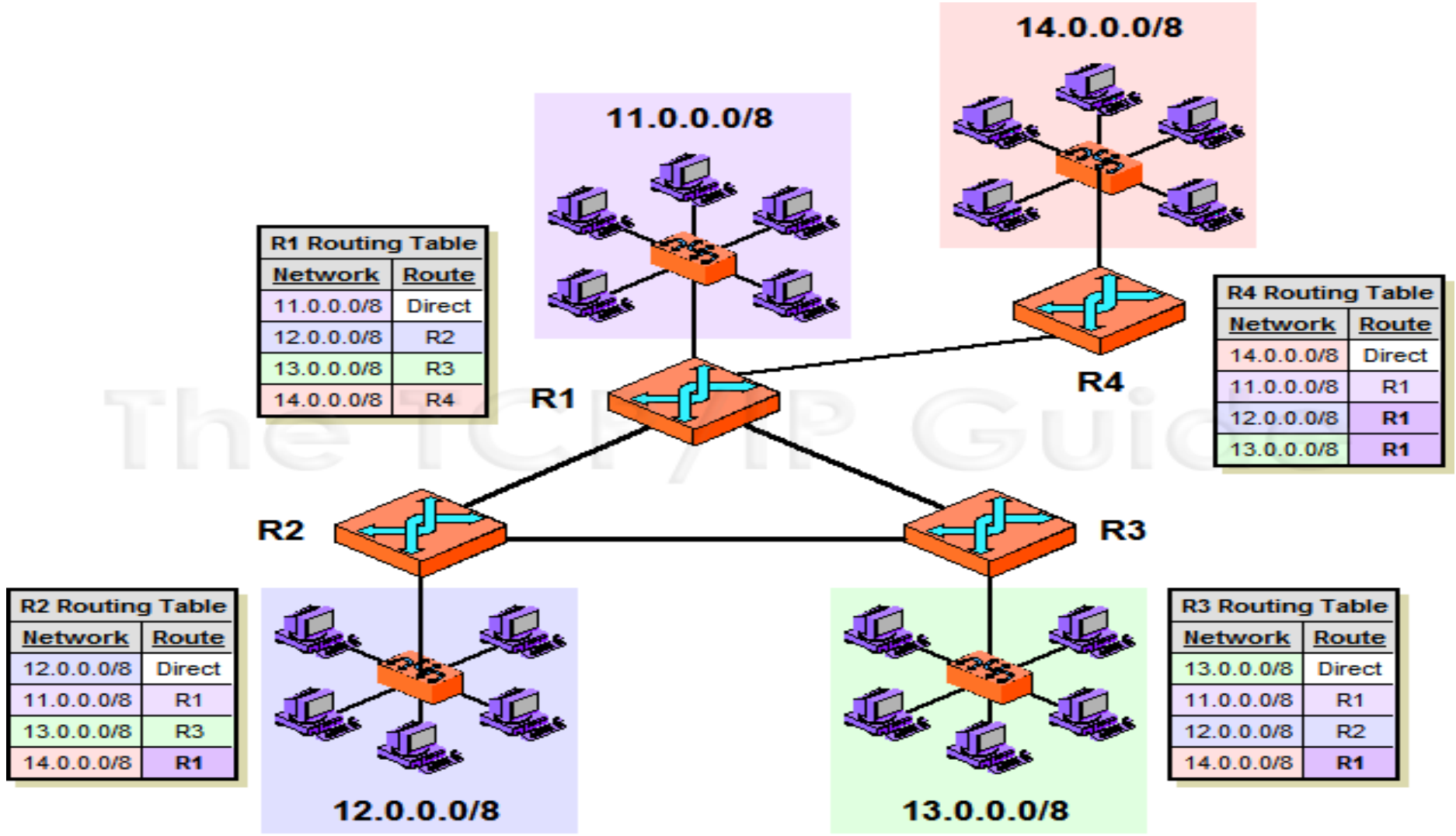
Router is a networking device which is used to provide interaction between two different networks. Router are also used for provide the routes to the data and devices that are connected in network. Router are used to establish internetwork communication

A router inspects a given data packet's destination Internet Protocol address (IP address), and provide connection to the nodes with the main network. It gives you wired and wireless both connectivities.

Router Working?

- Unicast, broadcast, telecast and anycast?
- Routing Tables?

IP ROUTES AND ROUTING TABLES



R1 Routing Table	
Network	Route
11.0.0.0/8	Direct
12.0.0.0/8	R2
13.0.0.0/8	R3
14.0.0.0/8	R4

R4 Routing Table	
Network	Route
14.0.0.0/8	Direct
11.0.0.0/8	R1
12.0.0.0/8	**R1**
13.0.0.0/8	**R1**

R2 Routing Table	
Network	Route
12.0.0.0/8	Direct
11.0.0.0/8	R1
13.0.0.0/8	R3
14.0.0.0/8	**R1**

R3 Routing Table	
Network	Route
13.0.0.0/8	Direct
11.0.0.0/8	R1
12.0.0.0/8	R2
14.0.0.0/8	**R1**

Top 5 Types of Router

1. Wireless :- It is present in office, home or railway station, etc. It creates a wireless signal. Suppose you are in office, we can connect to the internet using wireless signals because your laptop is within the range. We can provide security to routers by entering user id and password. When we try to connect to the router, it will ask for a password and UserId.

2. Wired Router :- Name itself defines its meaning. Wire is available to connect to the network. If we visit a bank or small college or office, we can observe that PC or Laptop is connected to the internet using Ethernet cable and that is the wired router. It has a separate Wi-Fi access point.

3. Edge Router :- It seats at the edge of the backbone of the network and can connect to the core routers. It can be wired or wireless and will distribute internet data packets between one or more networks.

4. Core Router :- It can forward IP packets at full speed on all of them. It will distribute internet data packets within the network. But core will not distribute internet data packets between networks.

5. Virtual Router :- virtual routers are pieces of software that allow computers and servers to operate like routers. They'll share data packets just as physical routers do. They can offer more flexibility than physical devices since they can be scaled as the business grows

Lets Configure…

4.

WAN & SOHO Full Briefly Explained

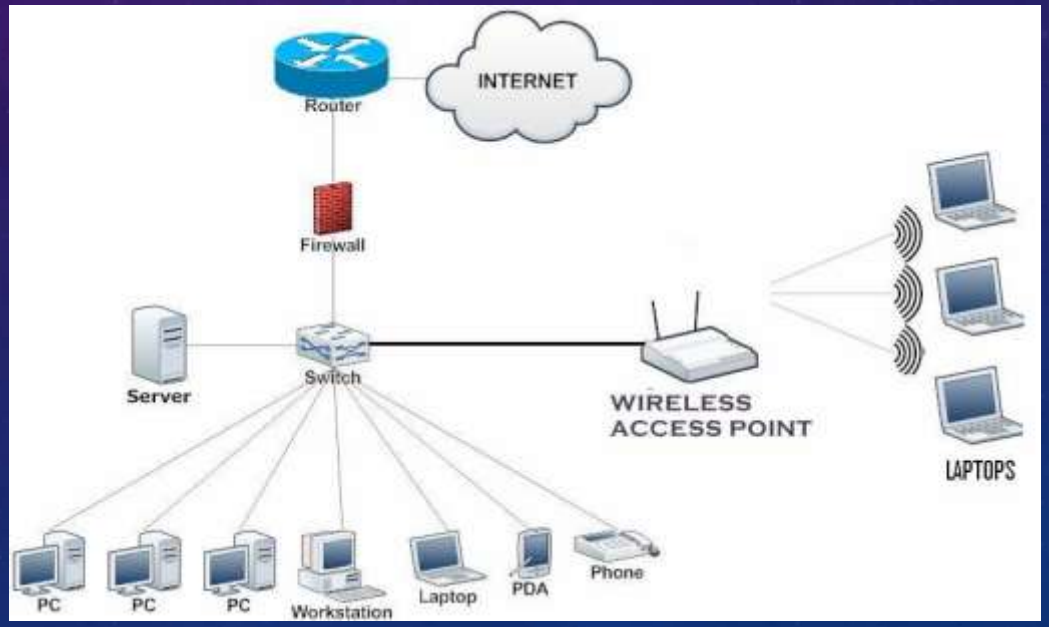
What Is a WAN? Wide-Area Network

In its simplest form, a wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

- Packet switching
- TCP/IP protocol suite
- Router
- ATM
- Frame Relay
- Multiprotocol Label Switching

What is SOHO network

SOHO networks are small LANs (Local Area Networks). Typically, SOHO networks consists of less than 10 computers. Network service servers like DNS server, email server, web server etc., are typically configured outside SOHO network.
A SOHO network can be a small wired Ethernet LAN or made of both wired and wireless computers.



What is SOHO Routers

A SOHO router is a broadband router built and marketed for small offices and home offices. Since the workload for these types of businesses is primarily on the internet, they require a local area network (LAN), which means their network hardware is structured specifically for that purpose. A SOHO network can be a mixed network of wired and wireless computers. Since these types of networks are meant for businesses, they may also include printers and sometimes voice over IP (VoIP) and fax over IP technology.

Lets Configure…

5.

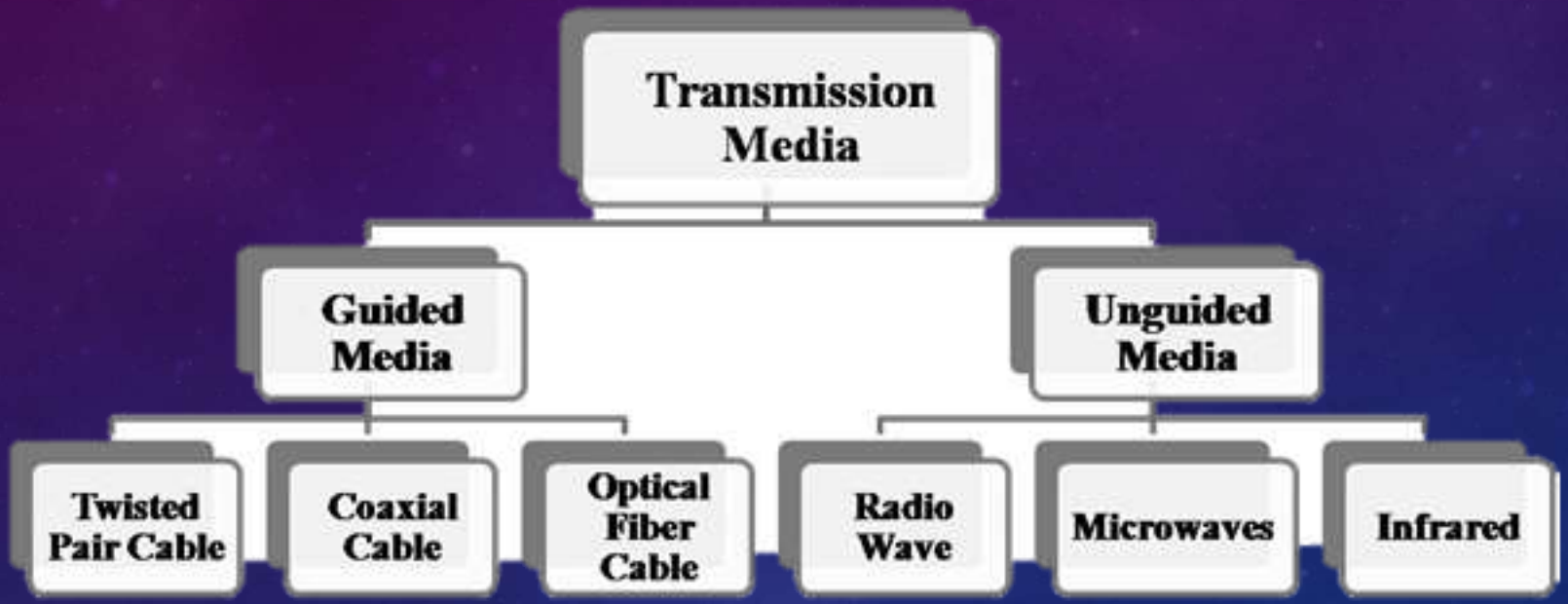
Types of Cables (Twisted, Coaxial & Fiber)

WHAT IS TRANSMISSION MEDIA ?

In data communication,

- **Transmission media** is a pathway that carries the information from sender to receiver.
- We use different types of cables or waves to transmit data.
- Data is transmitted normally through electrical or electromagnetic signals.

Transmission Media Types?

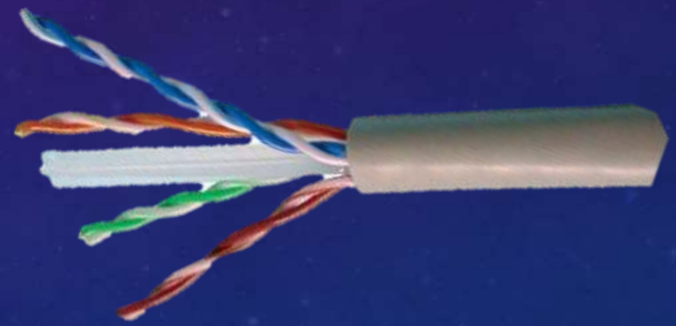


Twisted-Pair Cable

One of the earliest guided transmission media is twisted pair cables. A twisted pair cable comprises of two separate insulated copper wires, which are twisted together and run in parallel. The copper wires are typically 1mm in diameter.

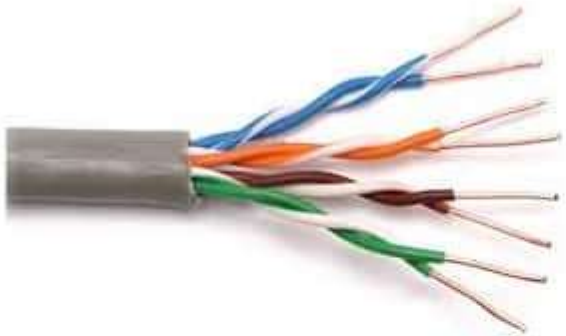
Applications

- In telephone lines
- In DSL lines
- In LANs



Types

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)



UTP Cable

- Pair of unshielded wires wound around each other

STP Cable

- Pair of wires wound around each other placed inside a protective foil wrap

UTP Categories

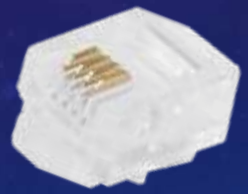
UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

What are RJ connectors?

RJ Connectors are a family of push-and-click connectors for twisted-pair wiring in telephone and network wiring. RJ stands for Registered Jack. RJ types define both a jack or receptacle (female) and a plug (male) type of connector.

The most common types of RJ connectors are as follows:

RJ-11 connector: A 4-wire or 6-wire telephone-type connector



RJ-45 connector: An 8-wire telephone-type connector

RJ-48 connector: An 8-wire telephone-type connector TP

Co-axial Cable

Coaxial cable is commonly **used by cable** operators, telephone companies, and internet providers around the world to convey data, video, and voice communications to customers. It has also been **used** extensively within homes.

Applications

- In analog telephone networks: carry about 10,000 voice signals.
- In digital telephone networks: data rate of 600 Mbps.
- In cable TV networks
- In traditional Ethernet LANs
- In MANs

Types

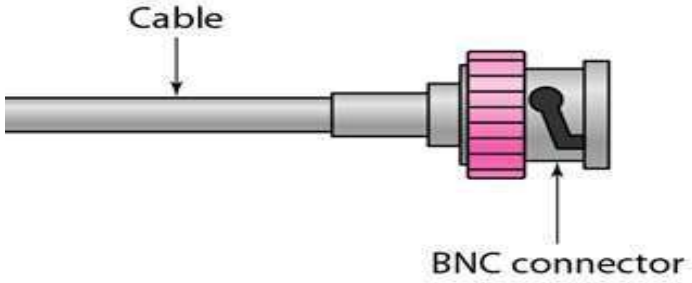
- RG – 59
- RG – 58
- RG – 11

- Has impedance of 75W and used in cable TV

- Has impedance of 50W and used in thin Ethernet

- Has impedance of 50W and used in thick Ethernet

BNC Connectors – Bayone Neil Concelman




AUDIO/VIDEO SCART

Optic Fiber Cable

A fiber optic cable is made of glass or plastic and transmit signals in the form of light. These are not affected by electrical noise. Though fiber optic cables last longer, the installation cost is high. Since these cables are di-electric, no spark hazards are present.

Applications

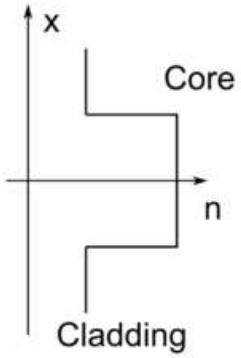
- Used in telephone systems
- Used in sub-marine cable networks
- Used to link computer networks
- Used in CCTV surveillance cameras
- Used for connecting fire, police, and other emergency services.

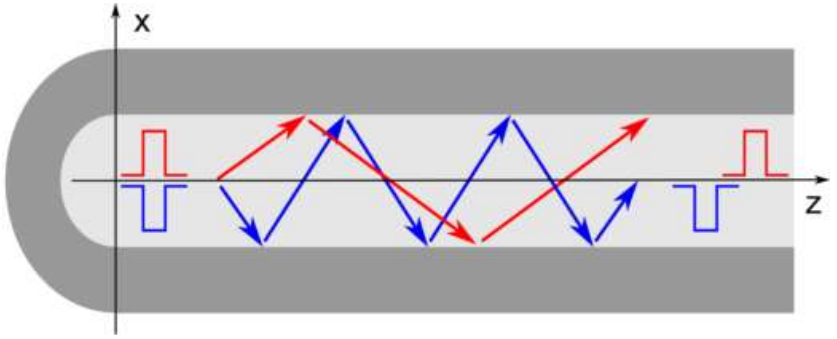
Types

- **Single-mode fiber** − These are excited with laser.
- **Multi-mode fiber** − These are excited with LED.

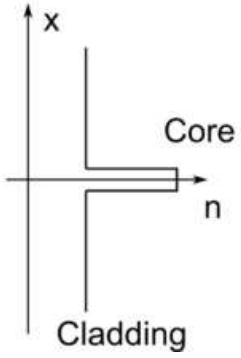
- Has lower bandwidth fair cost and designed for long distance

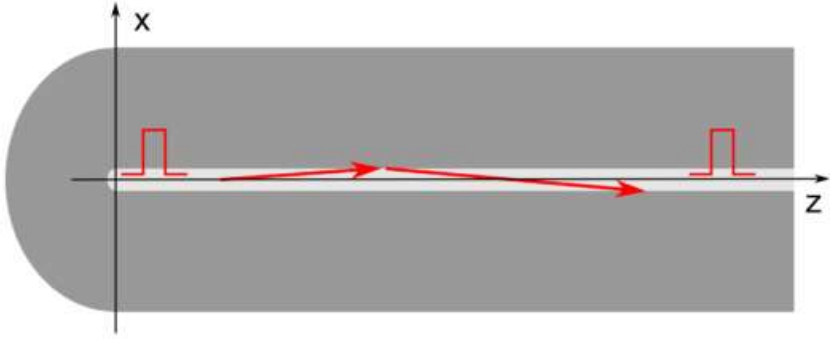
(a) Multimode fiber





(b) Single-mode fiber



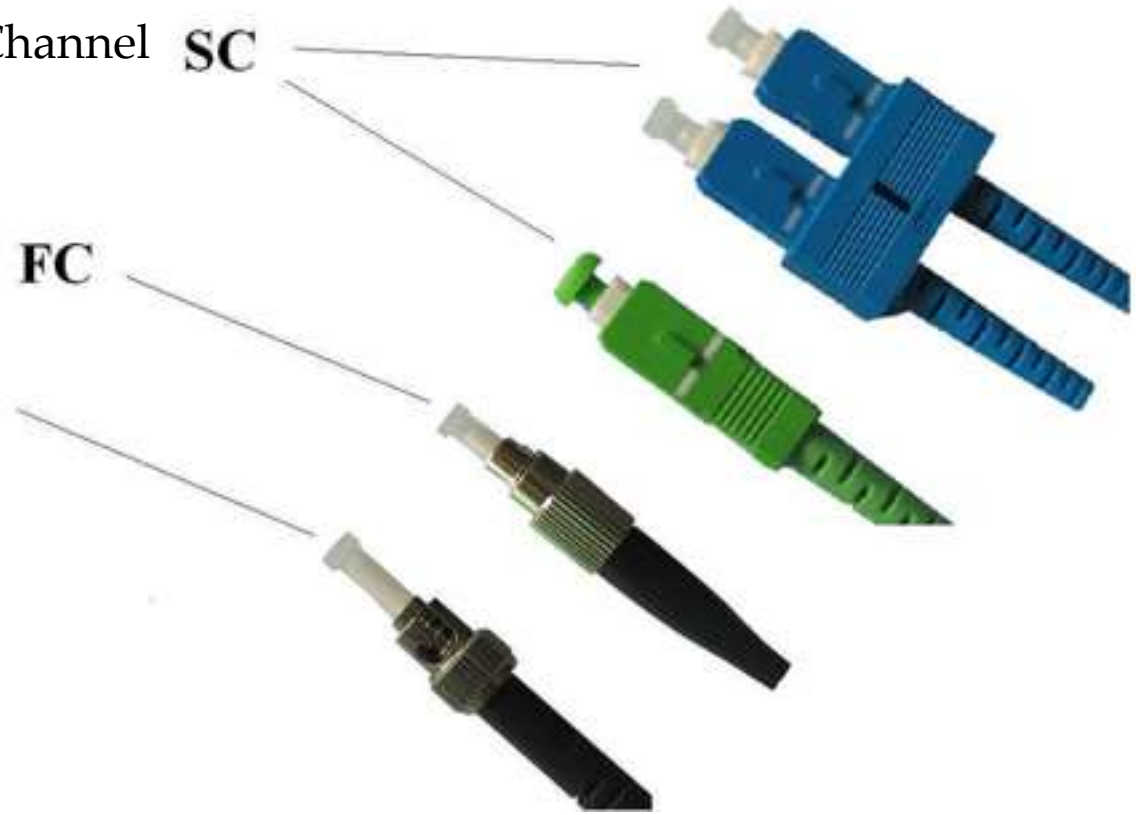


- Has higher bandwidth costly and designed for short distance

Subscriber Channel **SC**

Ferrule Connector **FC**

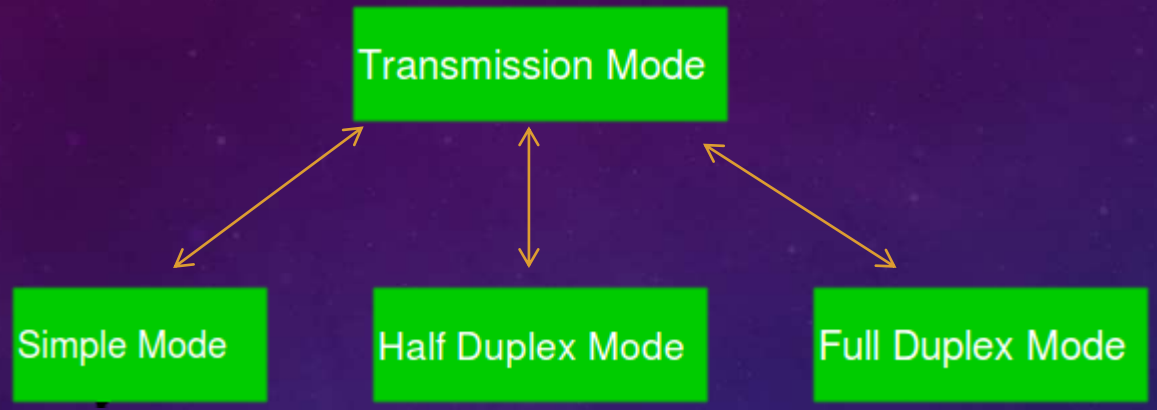
Straight Tip **ST**

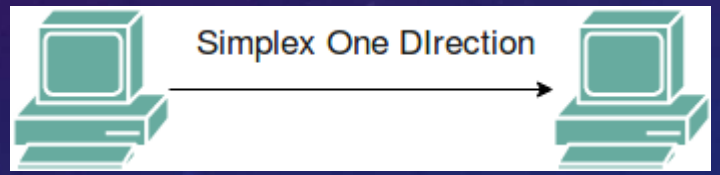


6.

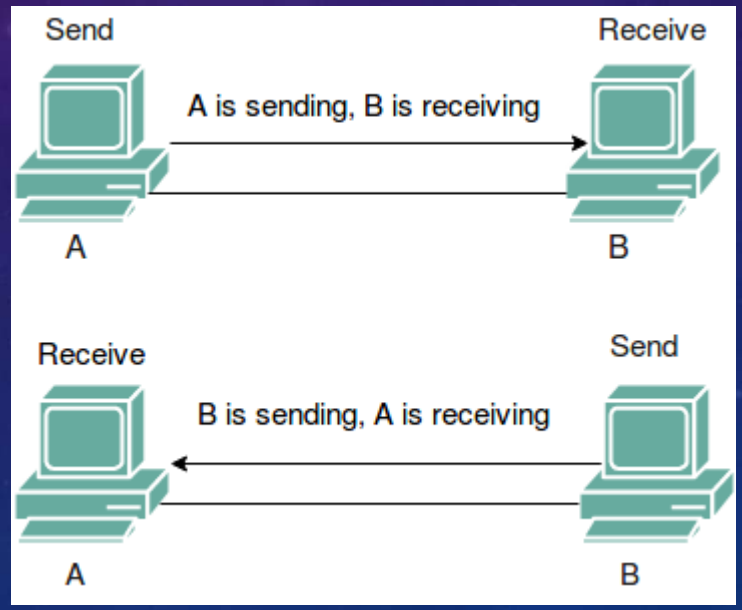
Cable issues (Collisions, Speed & Issues)

Collision?

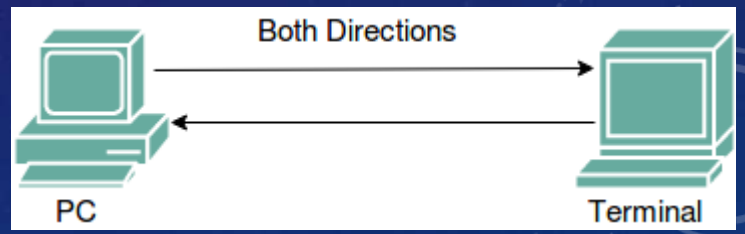




Simplex Mode



Half-Duplex Mode



Full-Duplex Mode

Speed

Causes of Less Speed

1. Long Distance Transmission
2. Poor Quality Conductor
3. Poor Contact with Source or Destination
4. Problem with Connector
5. Wire maybe not settled properly.

Measuring unit

Normally we measure speed of wire with MBPS & GBPS according to their distance between source & destination. Best example is from Optic Fiber 10BaseT or 100BaseT.

Issues?

1. Your cabling does not meet standards

Cable standard must be arranged systematic Electronic Industries Association (EIA) and the Telecommunications Industry Association (TIA).

2. The cables and connectors are not compatible

Using different components from different manufacturers may cause compatibility issues that are sure to affect your network's performance.

3. The crimp cords are of poor quality

While Crimping the crimp tool does not get fit and stretch wire into the Connector as a result the connector does not set on the wire properly.

4. The cables are not properly installed

Improper installation, whether it's due to fast installation or irresponsible or less experienced person installation.

7.

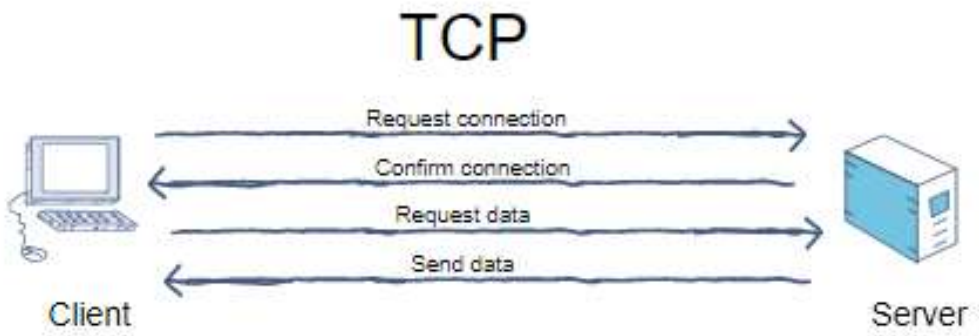
TCP & UDP Full Information

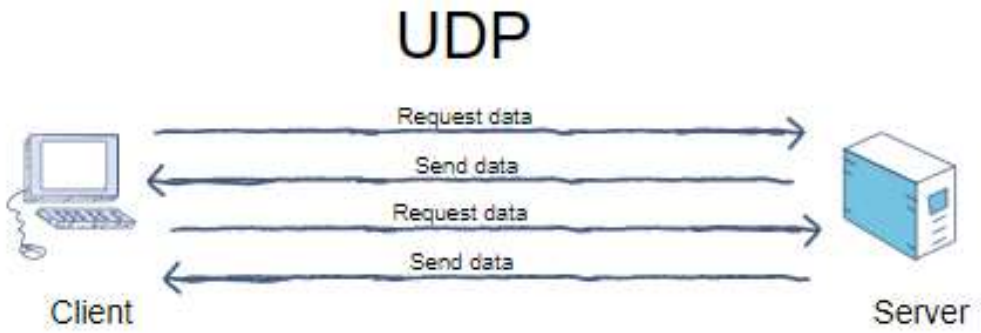
What is TCP?

Transmission Control Protocol (TCP) is a connection-oriented protocol that computers use to communicate over the internet. It is one of the main protocols in TCP/IP networks. TCP provides error-checking and guarantees delivery of data and that packets will be delivered in the order they were sent.

What is UDP?

User Datagram Protocol (UDP) is a connectionless protocol that works just like TCP but assumes that error-checking and recovery services are not required. Instead, UDP continuously sends datagrams to the recipient whether they receive them or not.





Reliability

TCP is reliable. Data sent using a TCP protocol is guaranteed to be delivered to the receiver. If data is lost in transit it will recover the data and resend it.

vs

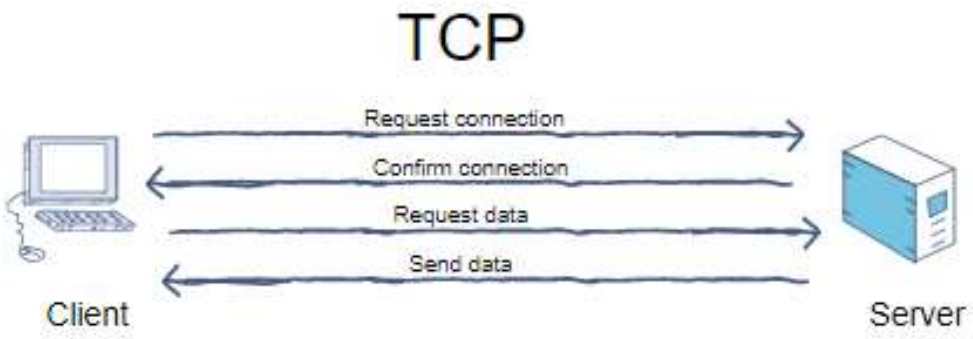
UDP is unreliable, it does not provide guaranteed delivery and a datagram packet may become corrupt or lost in transit.

Speed

TCP is slower than UDP because it has a lot more to do. TCP has to establish a connection, error-check, and guarantee that files are received in the order they were sent.

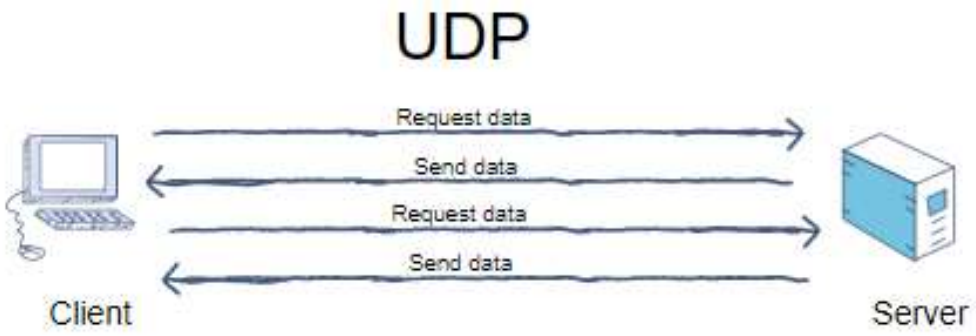
Ordering

TCP does ordering and sequencing to guarantee that packets sent from a server will be delivered to the client in the same order they were sent. On the other hand, UDP sends packets in any order.



Flow control

TCP uses a flow control mechanism that ensures a sender is not overwhelming a receiver by sending too many packets at once. UDP does not provide flow control. With UDP, packets arrive in a continuous stream or they are dropped.



Usage

TCP is best suited to be used for where timing is less of a concern.

- World Wide Web (HTTP, HTTPS)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)
- Email (SMTP, IMAP/POP)

UDP is best for applications that require speed and efficiency.

- VPN tunneling
- Streaming videos
- Online games
- Live broadcasts
- Voice over Internet Protocol (VoIP)

Let’s Explore Protocols & Ports of TCP & UDP

8.

IPv4 Full Rocket Science

What is IP Address?

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.

IP ADDRESSING IPV4

- An IP address basically a 32-bit address that uniquely universally defines connection of host or a router to the Internet. IP address is unique.
- Introduced by IANA (Internet Assigned Numbers Authority).
- 32 bit is divided into 4 equal parts of 8-8 bits separated by dotted decimal notation. It is in the range of minimum 0.0.0.0 to 255.255.255.255.
- Each 8 bit group is known by OCTET.

VARIOUS IP CLASSES

IP has five different classes differentiated by characteristics.

- Class-A ranges from 0 to 127
- Class-B ranges from 128 to 191
- Class-C ranges from 192 to 223
- Class-D ranges from 224 to 239
- Class-E ranges from 240 to 255

First Octet is defines the class of particular IP e.g. - 128.11.3.31 is follow in class –B

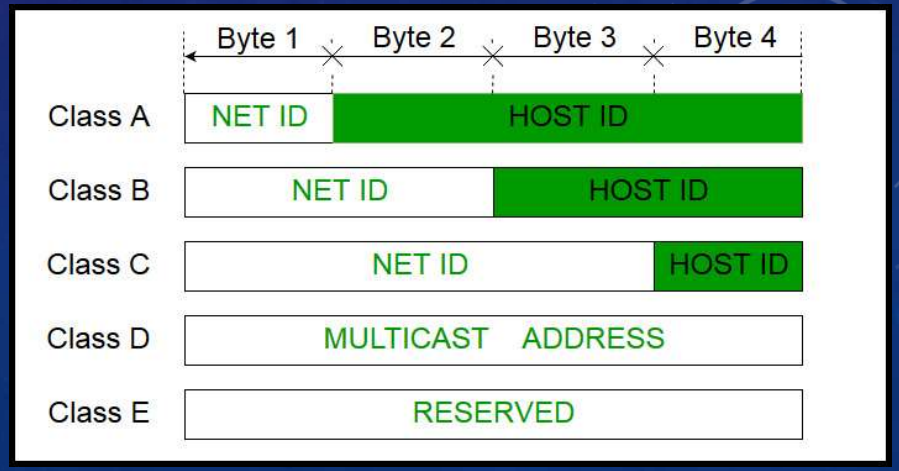
127.0.0.0 to 127.255.255.255 is a range of look back IP.

Class-A

This IP ranges from 0 to 126 Decimal value in first octet. And 1st octet defines network part and remaining three octet defines the Host part. It patterns like this NHHH (N-Network; H- Host).

First 8bits defines network and remaining 24 bits defines host parts. It has a highest nos. of address 2^{31}.which is about 16,277,216.

Lie between 10.1.1.1 to 126.255.255.255



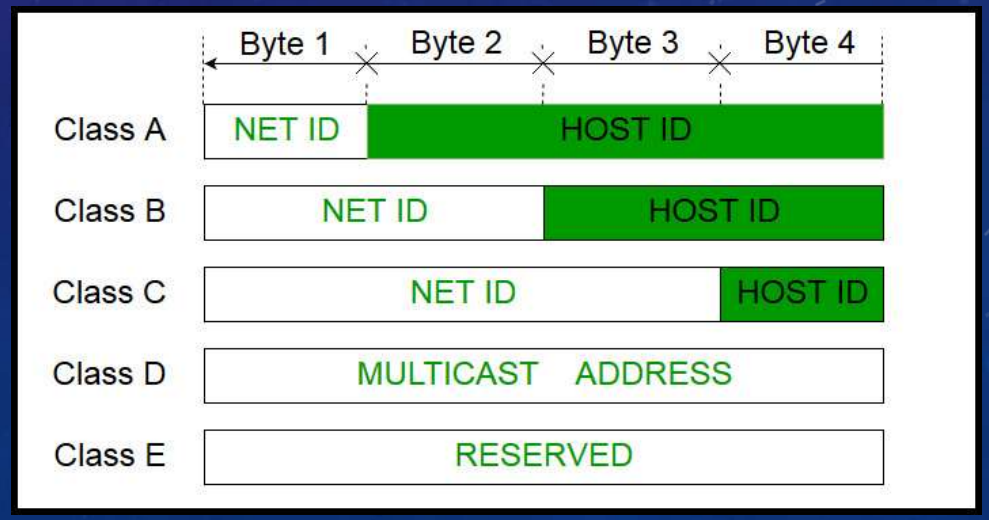
Class B

This IP ranges from 128 to 191 Decimal value in first octet. And 1st two bit defines network part and remaining two octet defines the Host part. It patterns like this NNHH (N-Network; H-Host).

First 16 bits defines network and remaining 16 bits defines host parts.

It has a highest nos. of address 2^{30}.which is about 65,536.

IP ranges from 128.16.0.0 to 172.31.255.255.

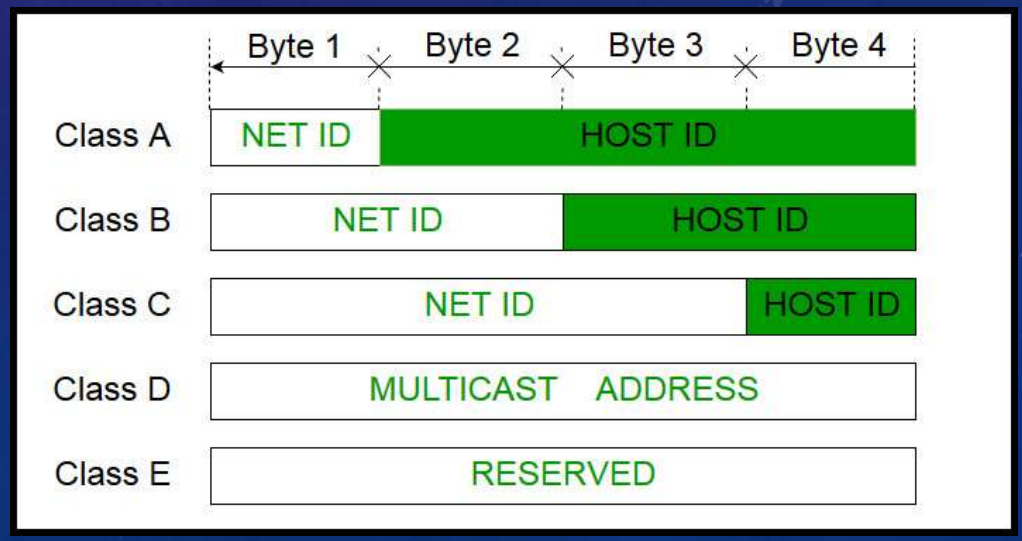


Class C

This IP ranges from 192 to 223 Decimal value in first octet. And 1st three bit defines network part and remaining one octet defines the Host part. It patterns like this NNNH (N-Network; H-Host).

First 24 bits defines network and remaining 8 bits defines host parts. It has a highest nos. of address 2^{29}.which is about 53,68,70,912

IP ranges from 192.168.0.0 to 223.255.255.0.

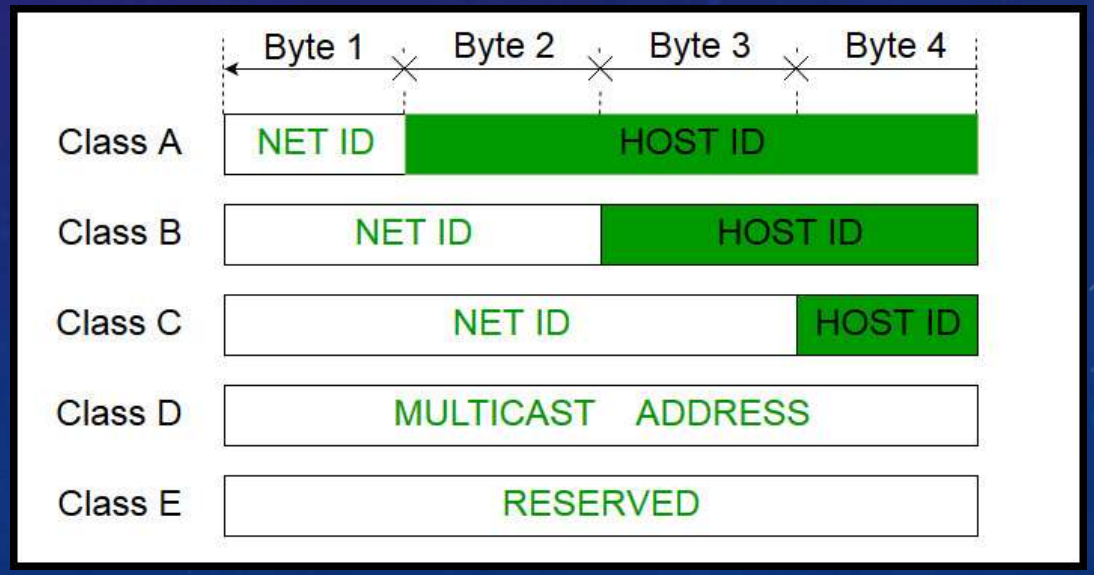


Class-D

This IP ranges from 224 to 239 Decimal value in first octet.

It is not usually use in general applications.

It is use in Special purpose applications known as Multicast.

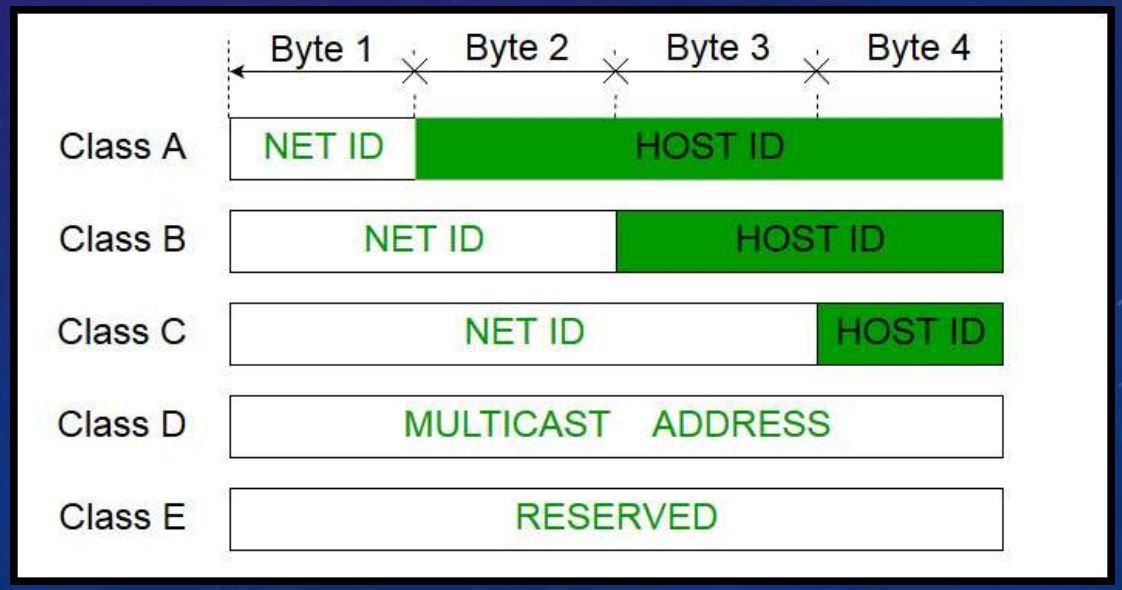


Class-E

This IP ranges from 240 to 255 Decimal value in first octet. It is not usually use in general applications.

It is reserved range of IP by R & D (Research and Development) department.

Usually, Class-A to C is supported by PC and Class-D and E is not supported.



IPv4 Conversion to Binary

192.168.102.45

9.

IPv6 Full Rocket Science

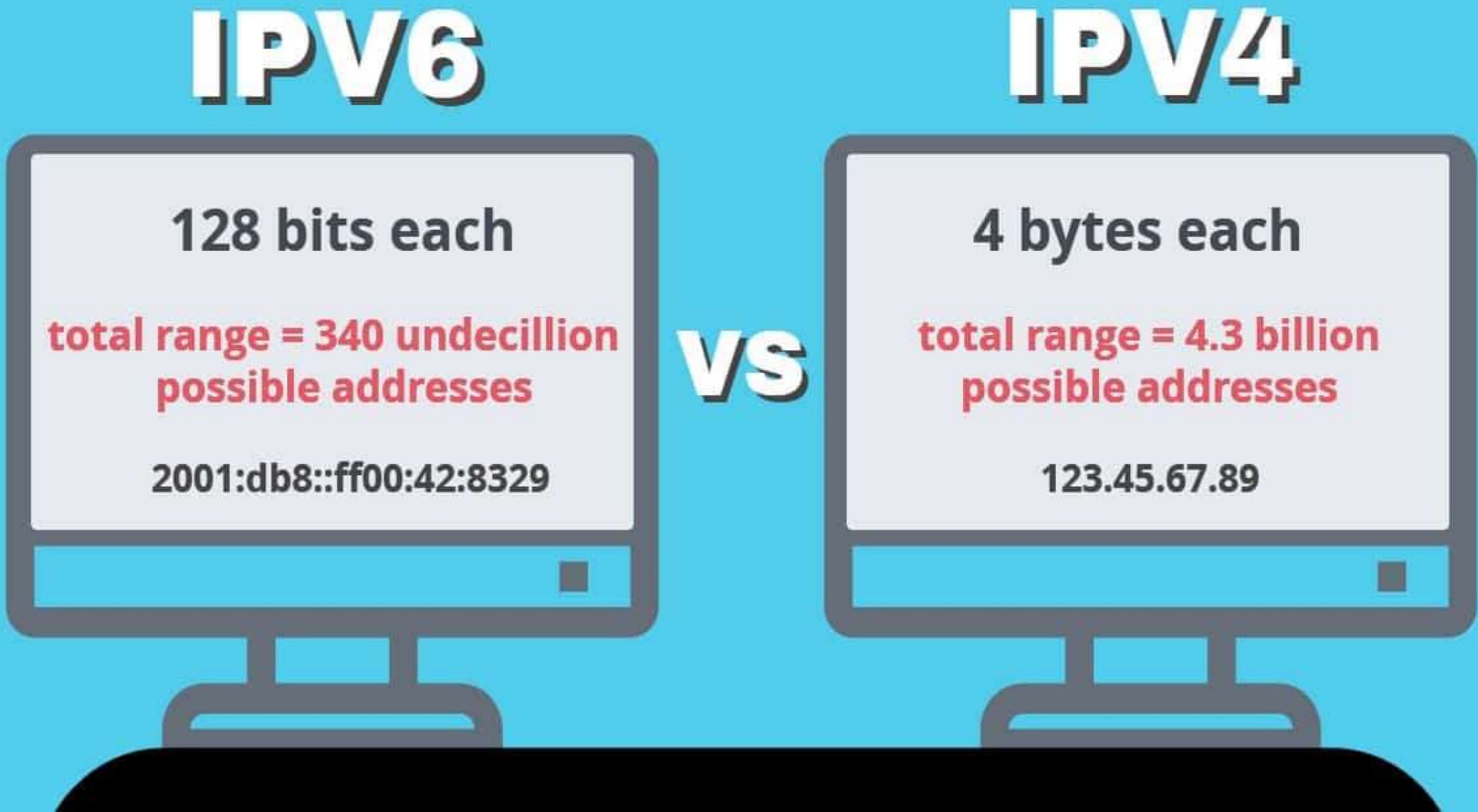
IP ADDRESSING IPV6

- An IP address basically a 128-bit address that uniquely universally defines connection of host or a router to the Internet. IP address is unique.
- Introduced by IANA (Internet Assigned Numbers Authority).
- total of 4,294,967,296 unique IP addresses can be assigned to hosts.
- IP is like 2001:db8:1234::f350:2256:f3dd/64
- It supports Unicast. Telecast & Multicast.
- It doesn’t have Classes like ipv4

KEY COMPARISONS

Between IPv4 vs IPv6

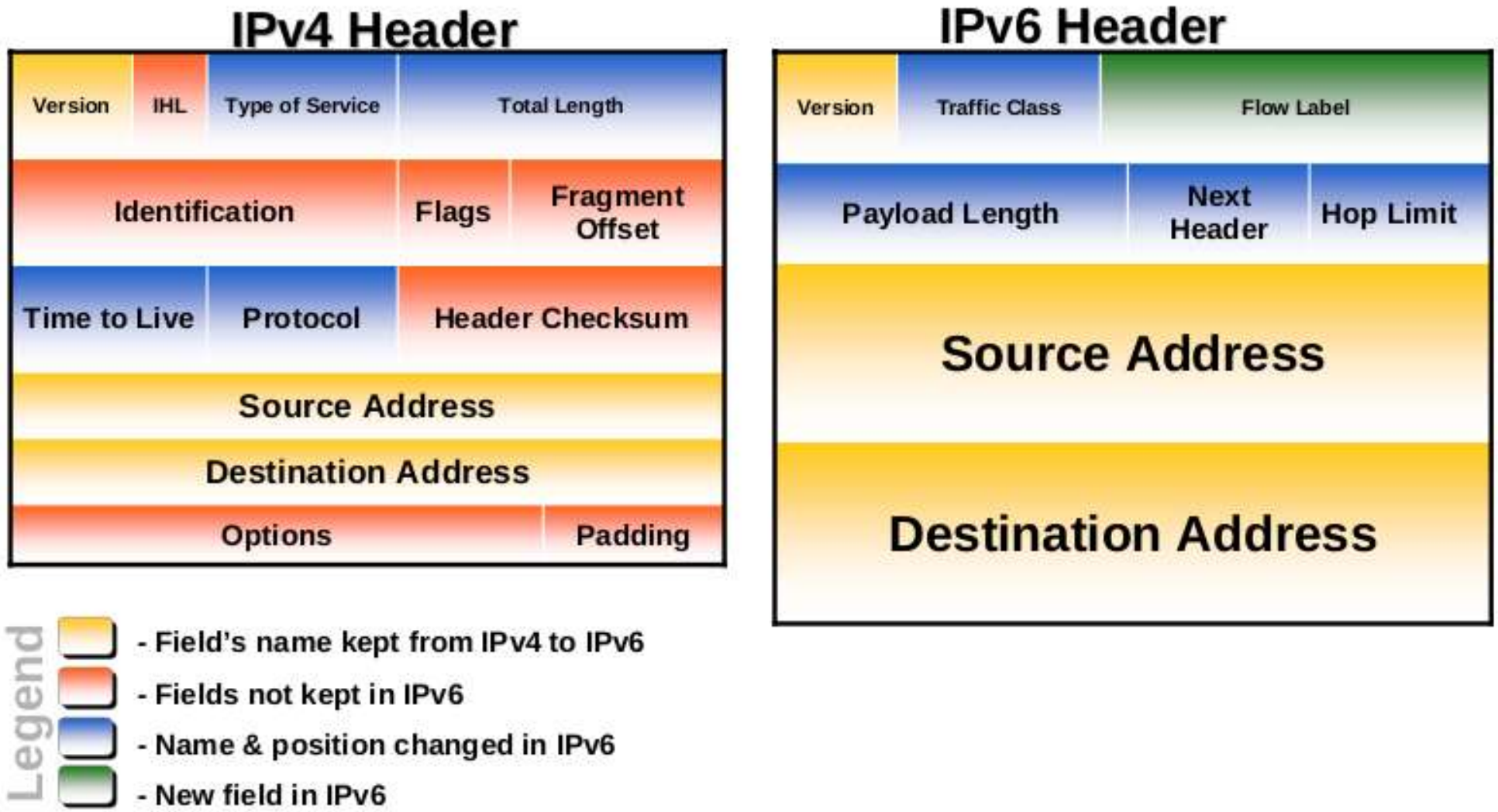
	IPv4	IPv6
Address	32 bits (4 bytes)	128 bits (16 bytes)
Packet Size	576 bytes required, fragmentation optional	1280 bytes required without fragmentation
Packet Fragmentation	Routers and sending hosts	Sending hosts only
Packet Header	Does not identify packet flow for QoS handling	Contains Flow Label field that specifies packet flow for QoS handling
	Includes a checksum	Does not include a checksum
	Includes options up to 40 bytes	Extension headers used for optional data
DNS Records	Pointer (PTR) records, IN-ADDR.ARPA DNS domain	Pointer (PTR) records, IP6.ARPA DNS domain
IP To MAC Tesolution	Broadcast ARP	Multicast Neighbor Solicitation
Local Subnet Group Management	Internet Group Management Protocol (IGMP)	Multicast Listener Discovery (MLD)
Broadcast	Yes	No
Multicast	Yes	Yes
IPSec	Optional	Required


IPV6
128 bits each
total range = 340 undecillion possible addresses
2001:db8::ff00:42:8329
VS
IPV4
4 bytes each
total range = 4.3 billion possible addresses
123.45.67.89

IPv6 Conversion to Binary

fe80::412c:c691:d7db:519b

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

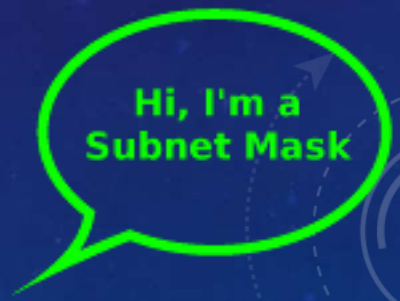

IPv4 Header
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Legend
- Field's name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6

10.

Subnetting Full Rocket Science

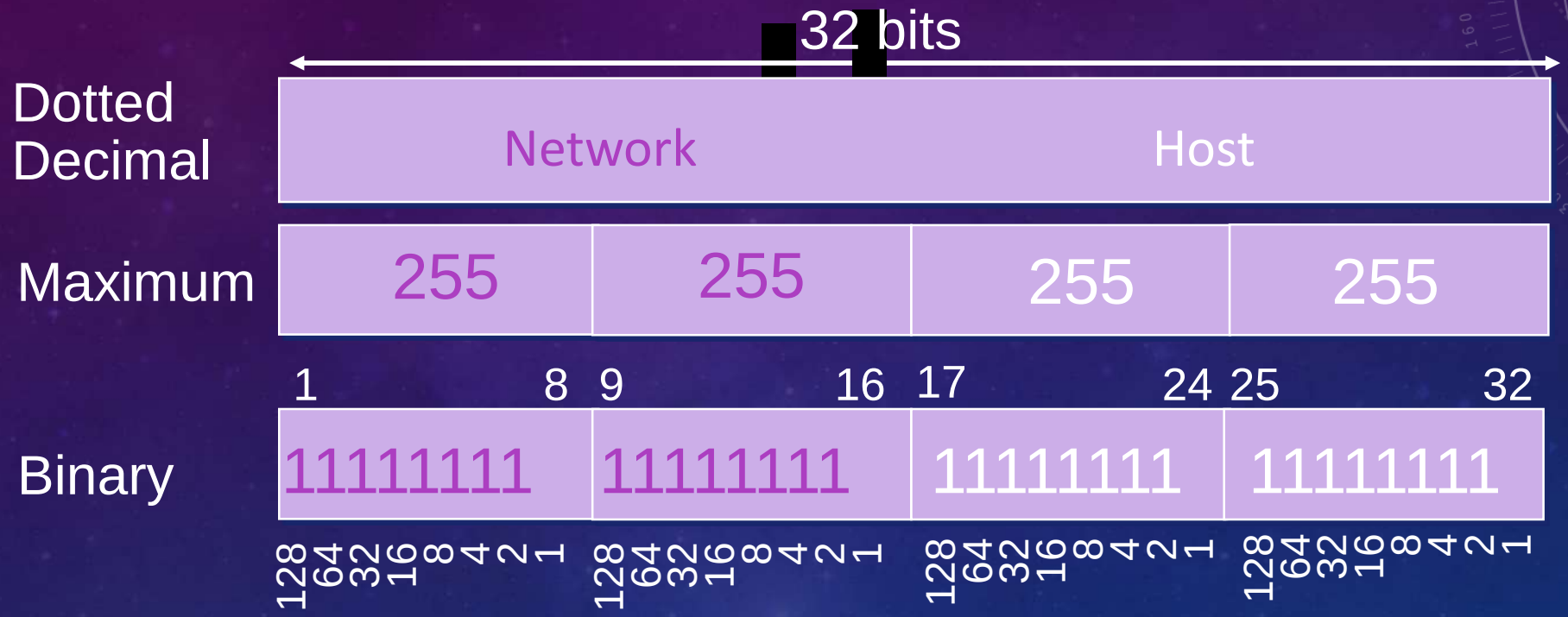
What Is Subnet Mask?

A subnet mask is a 32-bit number that segments an existing IP address in a TCP/IP network. It is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network. Subnet mask divides the IP address into a network address and host address, hence to identify which part of IP address is reserved for the network and which part is available for host use.

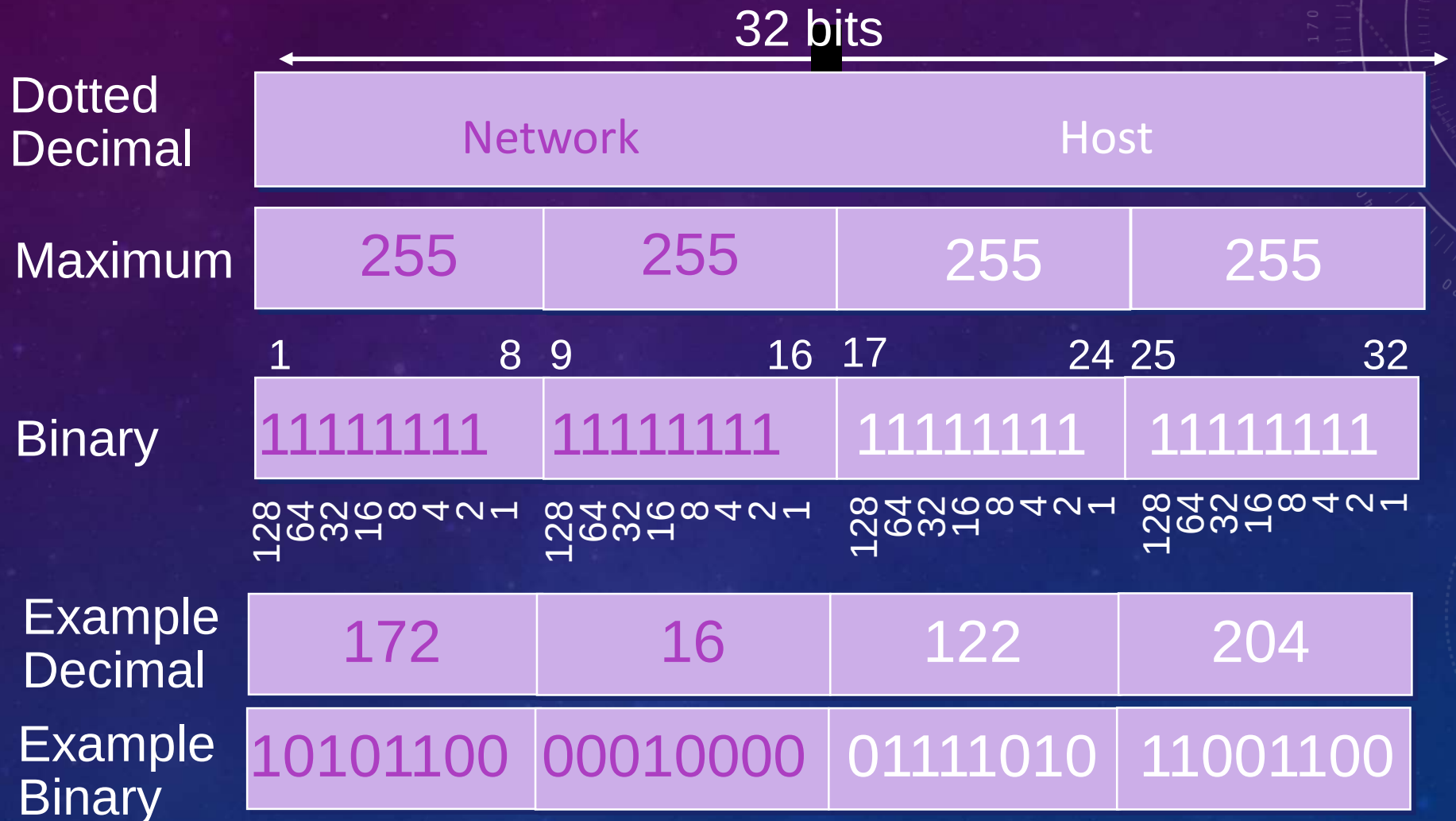


255.255.255.0

IP ADDRESSING

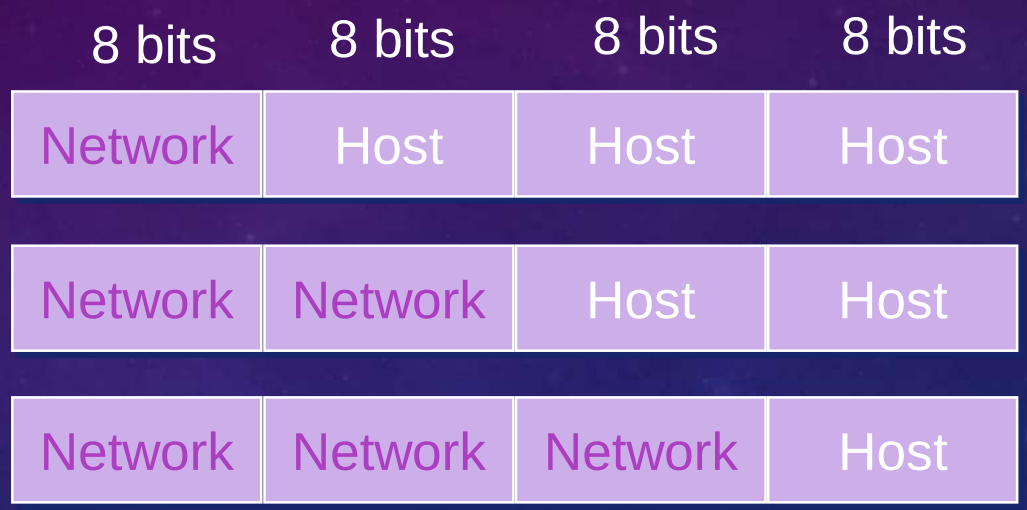


IP ADDRESSING

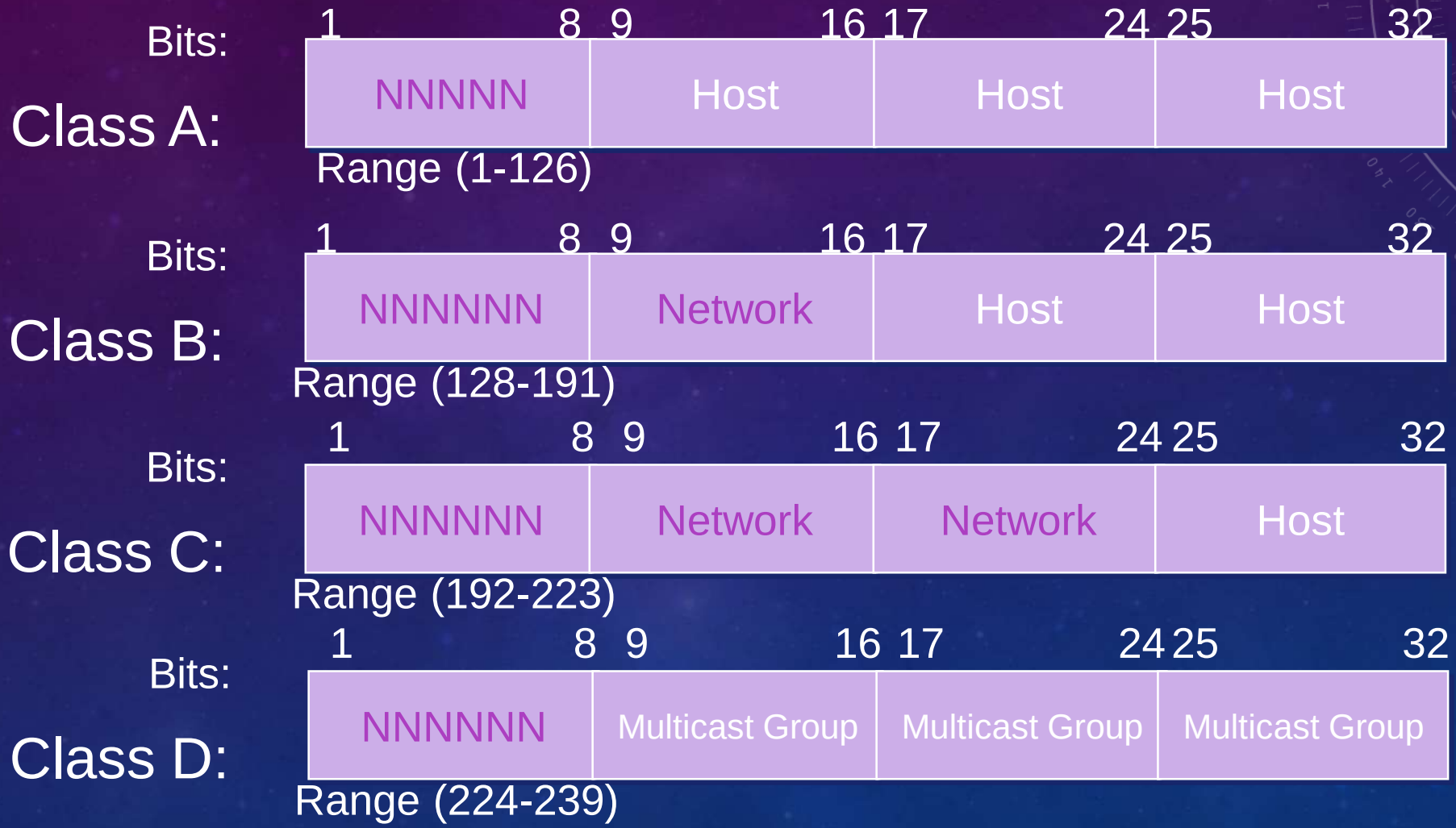


IP ADDRESS CLASSES

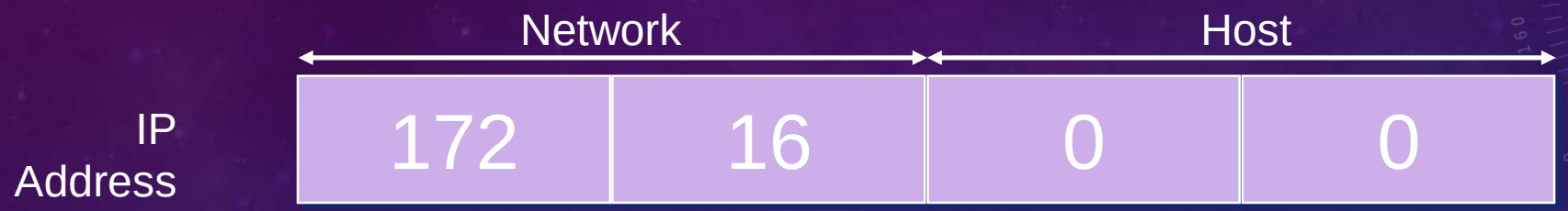
- Class A:
- Class B:
- Class C:
- Class D: Multicast
- Class E: Research

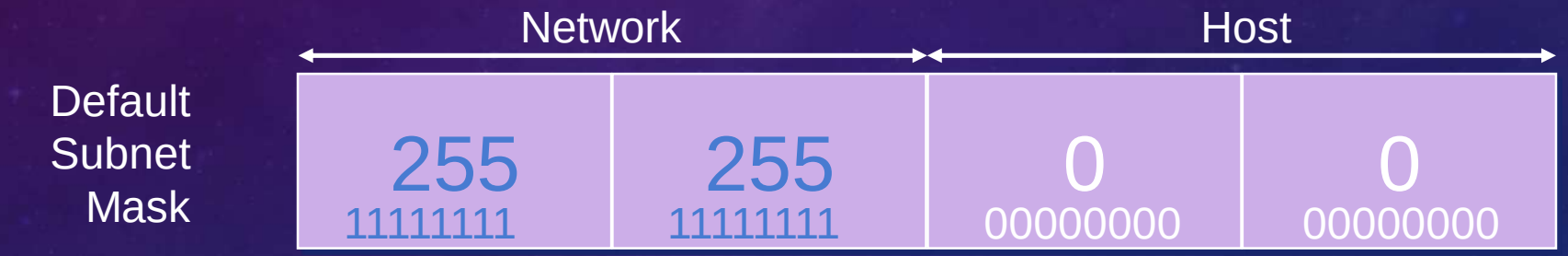


IP ADDRESS CLASSES



SUBNET MASK

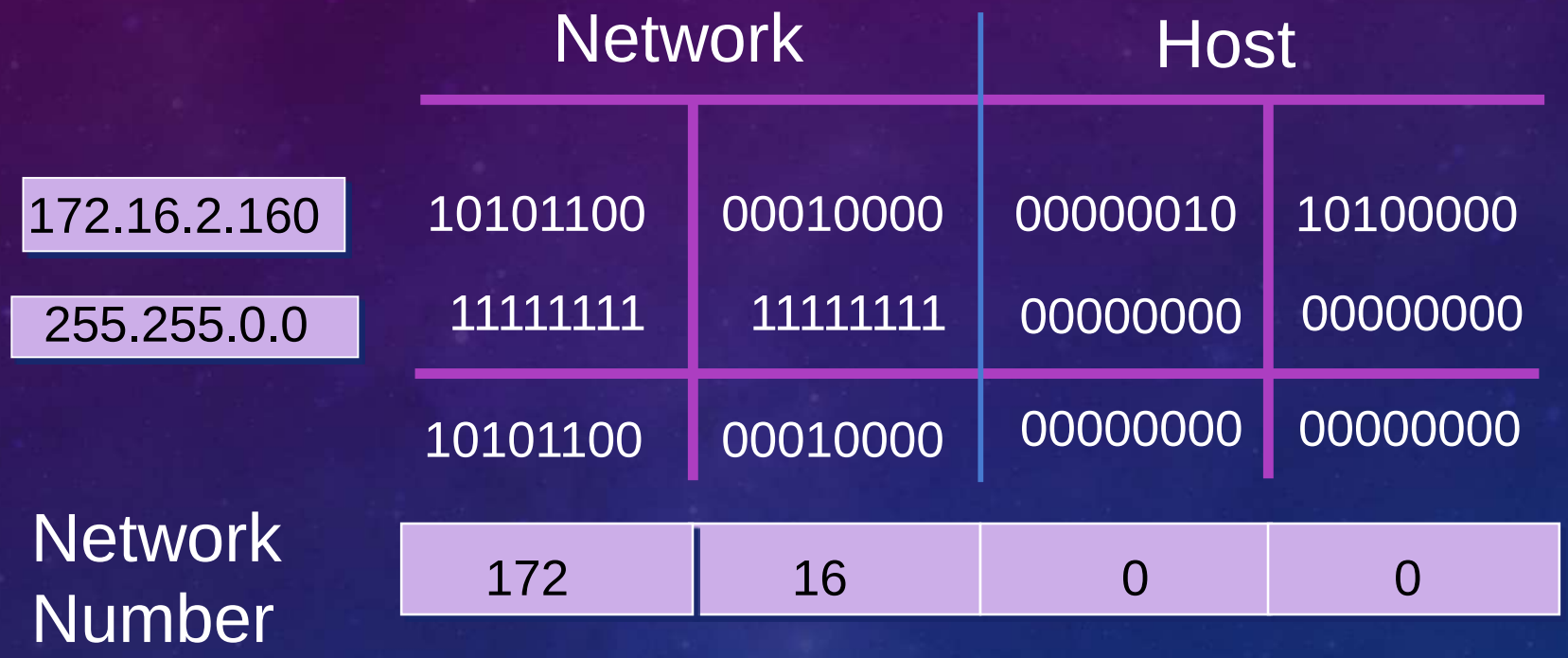




Also written as "/16" where 16 represents the number of 1s in the mask.

Also written as "/24" where 24 represents the number of 1s in the mask.

SUBNET MASK WITHOUT SUBNETS



- Subnets not in use—the default

SUBNET MASK WITH SUBNETS

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000

Network Number

172	16	2	0

- Network number extended by eight bits

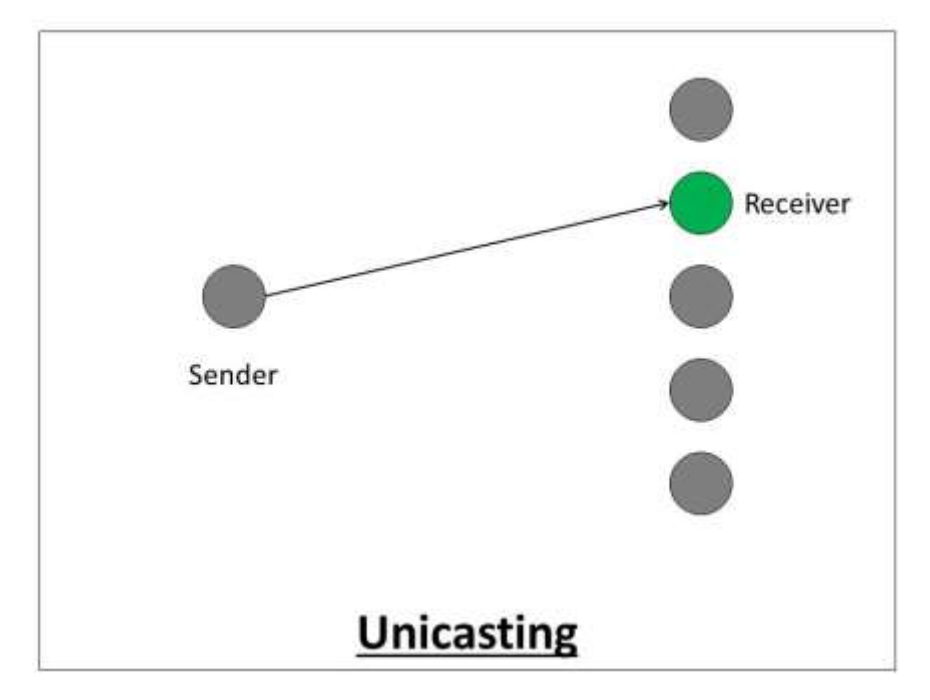
Let’s Discuss!

11.

Unicast, Multicast, Anycast & Broadcast

UNICAST

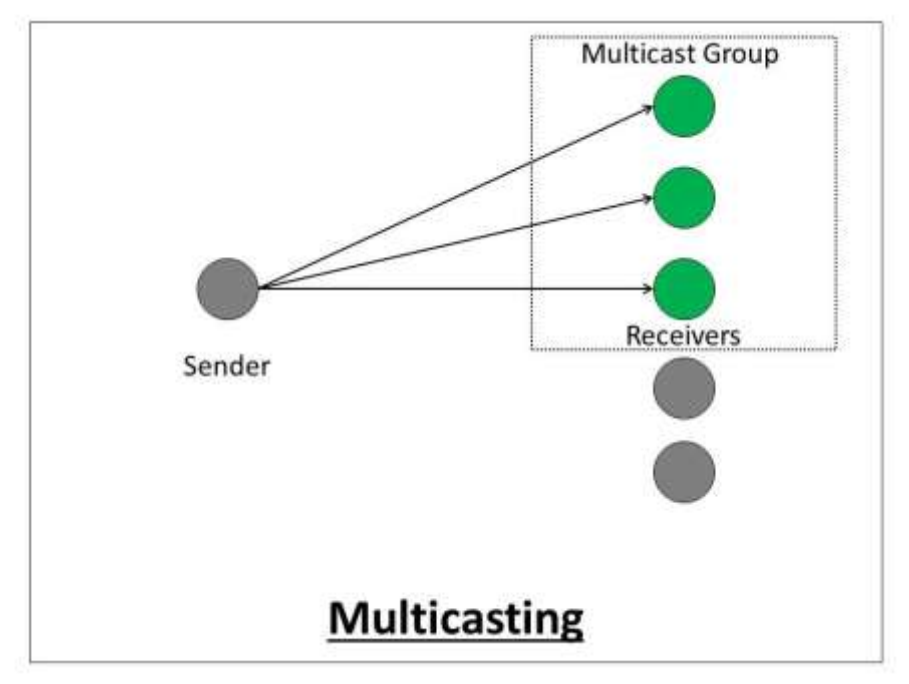
Unicast is the communication that there is only one receiver. This is one-to-one communication.



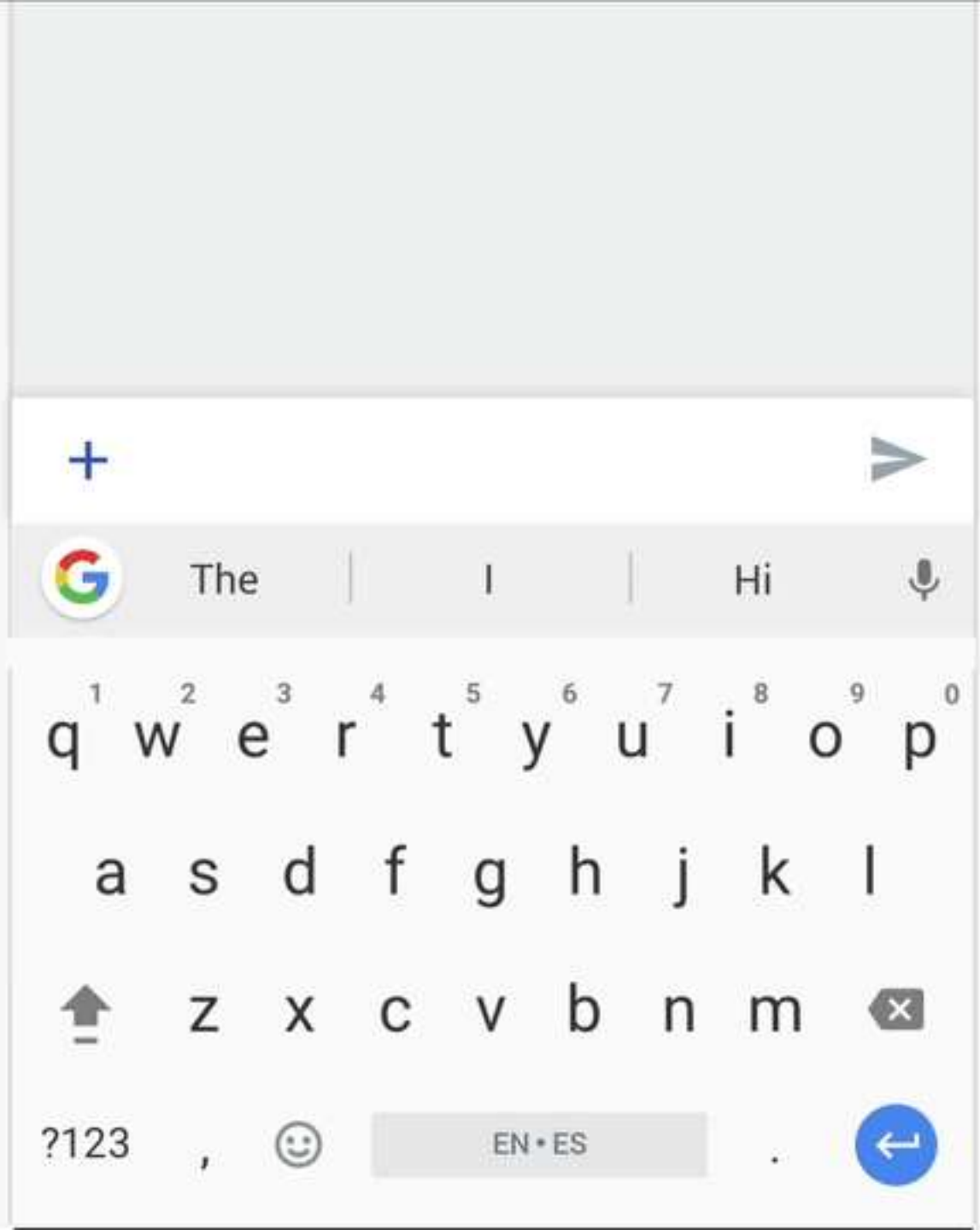
Example – Phone Call

MULTICAST

Multicast is the communication that there is one more receiver. Only the members of the multicast group receive the multicast traffic.

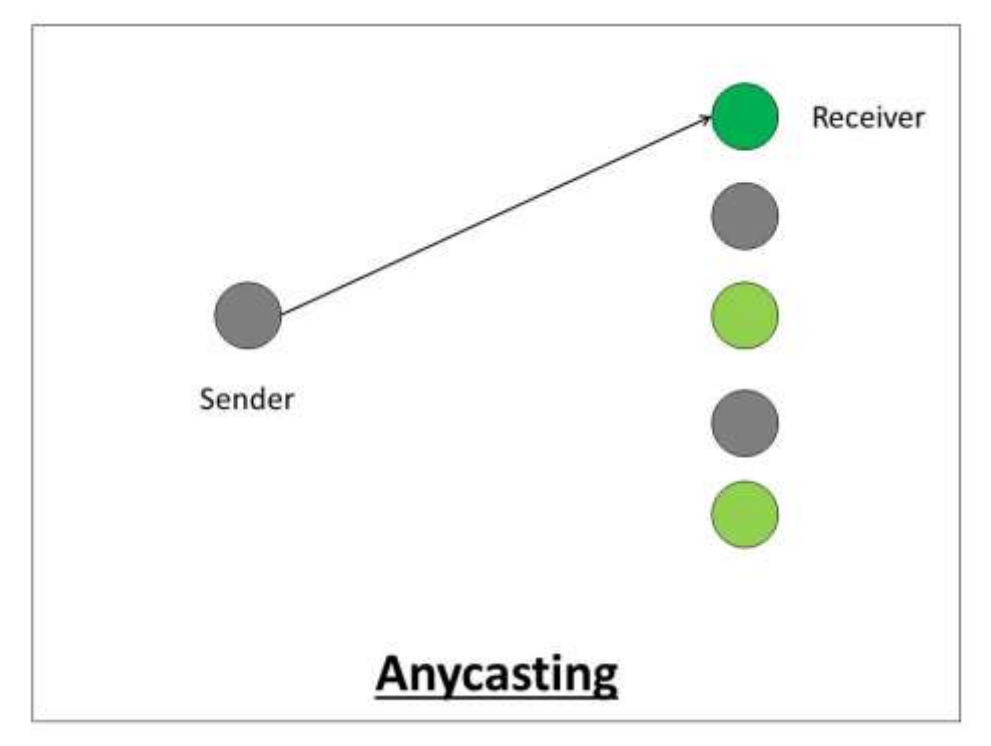


Example – Group Chatting


The
I
Hi
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123
,
EN • ES
.

ANYCAST

Anycast is the communication that is developed with **IPv6**. With anycast, the traffic is received by the nearest receiver in a group of the receivers that has the same IP.

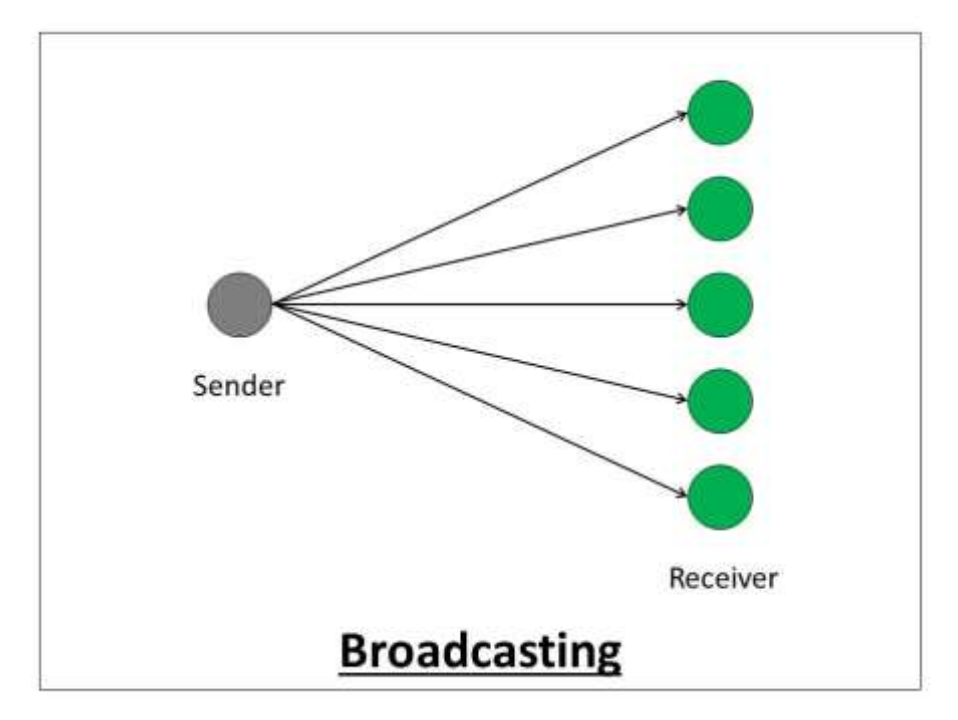


Example – DNS Route


Near

BROADCAST

Broadcast is also the communication that there is one more receiver but this time, all the receivers receive broadcast traffic.



Example – TV provider

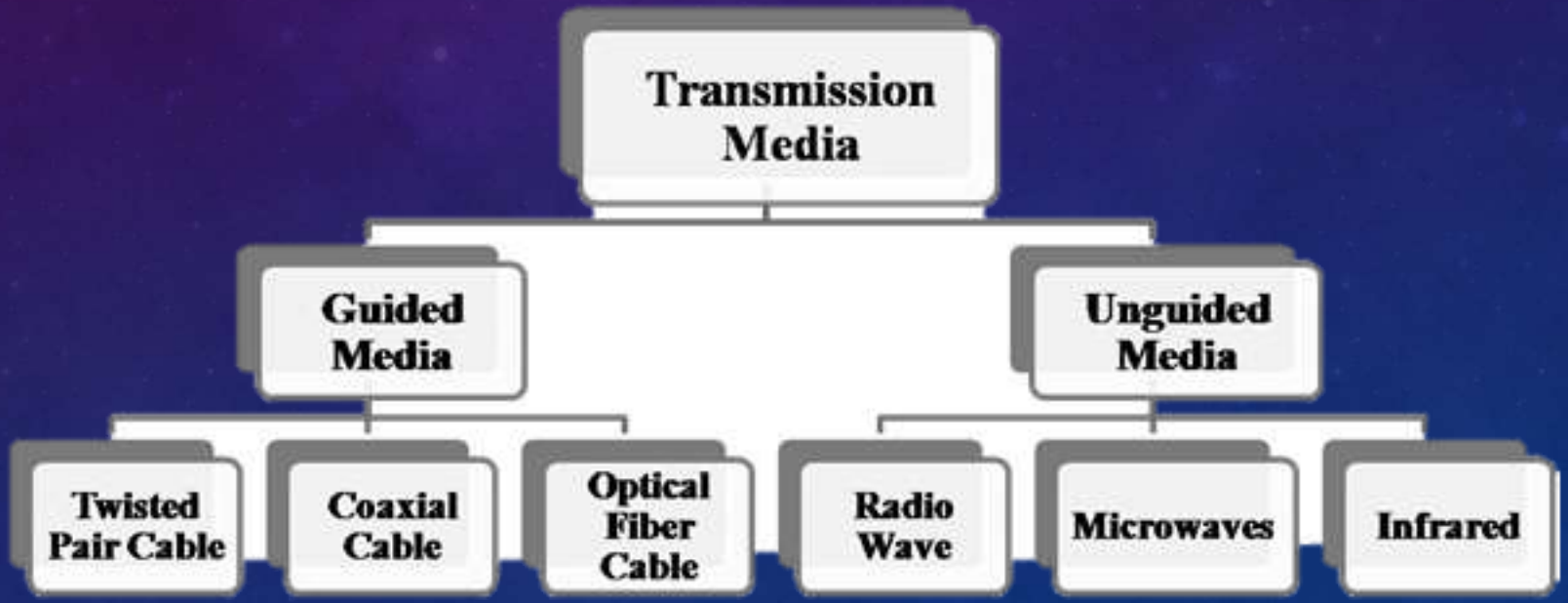
12.

Wireless Terms (SSID, Channel & Encryption)

UnGuided Transmission

•An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

Transmission Media Types?



Radio waves

•Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.

•Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.

•The range in frequencies of radio waves is from 3Khz to 1 khz.

•In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.

•An example of the radio wave is **FM radio**.

Advantages Of Radio transmission:

•Radio transmission is mainly used for wide area networks and mobile cellular phones.

•Radio waves cover a large area, and they can penetrate the walls.

•Radio transmission provides a higher transmission rate.

Microwaves

Microwaves are of two types:
•Terrestrial microwave
•Satellite microwave communication.

•Terrestrial microwave

•**Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
•**Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
•**Short distance:** It is inexpensive for short distance.
•**Long distance:** It is expensive as it requires a higher tower for a longer distance.
•**Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

•Satellite microwave

•The coverage area of a satellite microwave is more than the terrestrial microwave.
•The transmission cost of the satellite is dependent of the distance from centre of the coverage area.
•Satellite communication is used in mobile and wireless communication applications.
•It is easy to install.
•It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.
- It supports high bandwidth, and hence the data rate will be very high.
- Uses in Remote Control, Thermal Imaging Cameras, Xray and MRI Machines

WI-FI & BLUETOOTH

WI-FI

- What is Wi-Fi

Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. ... Internet connectivity occurs through a wireless router.

BLUETOOTH

Bluetooth is wireless communication standard which allows electronic devices to connect and interact with each other. It can be found in a number of gadgets, from smartphones, to loudspeakers, to laptops and more

Bluetooth™

Wi-fi Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

Bluetooth Evolution

Year Introduced	Bluetooth Version	Feature
2004	2.0	Enhanced Data Rate
2007	2.1	Secure Simple Pairing
2009	3.0	High Speed with 802.11 Wi-Fi Radio
2010	4.0	Low-energy protocol
2013	4.1	Indirect IoT device connection
2014	4.2	IPv6 protocol for direct internet connection
2016	5.0	4x range, 2x speed, 8x message capacity + IoT

Wireless Terms

SSID :- A Wi-Fi network's **SSID** is the technical term for its network name.

Channel :- A **channel** is the medium through which our wireless networks can send and receive data.

Bandwidth :- How much data capacity the network can carry.

DHCP :- Dynamic Host Configuration Protocol used to generate automatic IP.

APIPA :- When DHCP fails APIPA applied in such Network.

Wired Encryption Protocol (WEP) :- WEP is a security algorithm introduced to provide **data confidentiality for wireless networks**.

WPA and WPA2 :- WPA (Wi-Fi Protected Access) and **WPA2** are two of the security measures that can be used to protect wireless networks. **WPA** uses TKIP (Temporal Key Integrity Protocol) while **WPA2** is capable of using TKIP or the more advanced AES algorithm.

PSK: Pre-shared Key or Personal mode.

13.

Virtualization Fundamentals (Virtual machines)

What is Virtualization?

Virtualization is the process of creating a software-based, or virtual, representation of something, such as virtual applications, servers, storage and networks. It is the single most effective way to reduce IT expenses while boosting efficiency and agility for all size businesses.

Benefits of Virtualization

Virtualization can increase IT agility, flexibility and scalability while creating significant cost savings. Greater workload mobility, increased performance and availability of resources, automated operations – they're all benefits of virtualization that make IT simpler to manage and less costly to own and operate. Additional benefits include:

- Reduced capital and operating costs.
- Minimized or eliminated downtime.
- Increased IT productivity, efficiency, agility and responsiveness.
- Faster provisioning of applications and resources.
- Greater business continuity and disaster recovery.
- Simplified data center management.
- Availability of a true Software-Defined Data Center.

Virtualization???

Hyper-V

Let’s Take an Example…

14.

WLAN Full Concepts Explained

What is WLAN or Wireless Local Area Networks

WLAN is a wireless network communication over short distances using radio or infrared signals. WLAN is marketed as a Wi-Fi brand name. Any components that connect to a WLAN is considered as a station and falls into one of two categories.

•**Access point (AP)**: AP transmit and receive radio frequency signals with devices able to receive transmitted signals. Usually, these devices are routers.

•**Client:** It may comprise a variety of devices like workstations, laptops, IP phones, desktop computers, etc. All work-stations that are able to connect with each other are known as BSS (Basic Service Sets).

Examples of WLAN includes,
- WLAN adapter
- Access point (AP)
- WLAN router
- Cable, connectors and so on.

Types of WLAN
- Infrastructure
- Peer-to-peer
- Bridge
- Wireless distributed system

WLAN Important Components

•**Radio Frequency Transmission** :- Radio frequencies range from the frequencies used by cell phones to the AM radio band. Radio frequencies are radiated into the air by antennas that create radio waves.

•**WLAN Standards** :- To establish WLAN standards and certifications, several organizations have stepped forward. Organization has set regulatory agencies to control the use of RF bands. Introduced by IEEE (Institute of Electrical and Electronic Engineers)

•**ITU-R** :- ITU (International Telecommunication Union) co-ordinate spectrum allocation and regulations among all of the regulatory bodies in each country.

802.11 Standards and Wi-Fi protocols :- The IEEE (Institute of Electrical and Electronic Engineers) 802 Standard comprises a family of networking standards that cover the physical layer specifications of technologies from Ethernet to wireless. The IEEE 802.11 uses the Ethernet protocol and CSMA/CA for path sharing.

•**Wi-Fi Alliance** :- Wi-Fi alliance ensures interoperability among 802.11 products offered by various vendors by providing certification.

WLAN Security

WLAN is vulnerable to various security threats like,

- Unauthorized access
- MAC and IP spoofing
- Eavesdropping
- Session Hijacking
- DOS (denial of service) attack

Implementing WLAN

1.Ad-hoc mode: In this mode, the access point is not required and can be connected directly. This setup is preferable for a small office (or home office). The only drawback is that the security is weak in such mode.

2.Infrastructure mode: In this mode, the client can be connected through the access point. Infrastructure mode is categorized in two modes:

- **Basic Service Set (BSS):** BSS provides the basic building block of an 802.11 wireless LAN.
- **Extended Service Set (ESS)**: It is a set of connected BSS

Let’s Configure…

15.

VLAN Full Concepts Explained

Virtual LAN (VLAN)

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divides broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

Types of VLANs

•A Protocol VLAN- which has traffic handled based on its protocol. A switch will segregate or forward traffic based on the traffics protocol.

•Static VLAN- also referred to as port-based VLAN, needs a network administrator to assign the ports on a network switch to a virtual network; while:

•Dynamic VLAN- allows a network administrator just to define network membership based on device characteristics, as opposed to switch port location.

Advantages –

•**performance** –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destination.

•**formation of virtual groups** – As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.

•**security** – In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.

•**Flexibility** – VLAN provide flexibility to add, remove the number of host we want.

•**Cost reduction** – VLANs can be used to create domains which eliminate the need for expensive routers.

Let’s Configure…

16.

OSI Model with All Layers

INTRODUCTION

Open systems interconnection basic reference model (OSI reference model or **OSI model**) is an abstract description for layered communications and computer network protocol design. It was developed as part of the **open systems interconnection** (**OSI**) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the application, presentation, session, transport, network, data-link, and physical layers. It is therefore often referred to as the **OSI seven layer model**.

Dad

D

And we're trying new things

NO

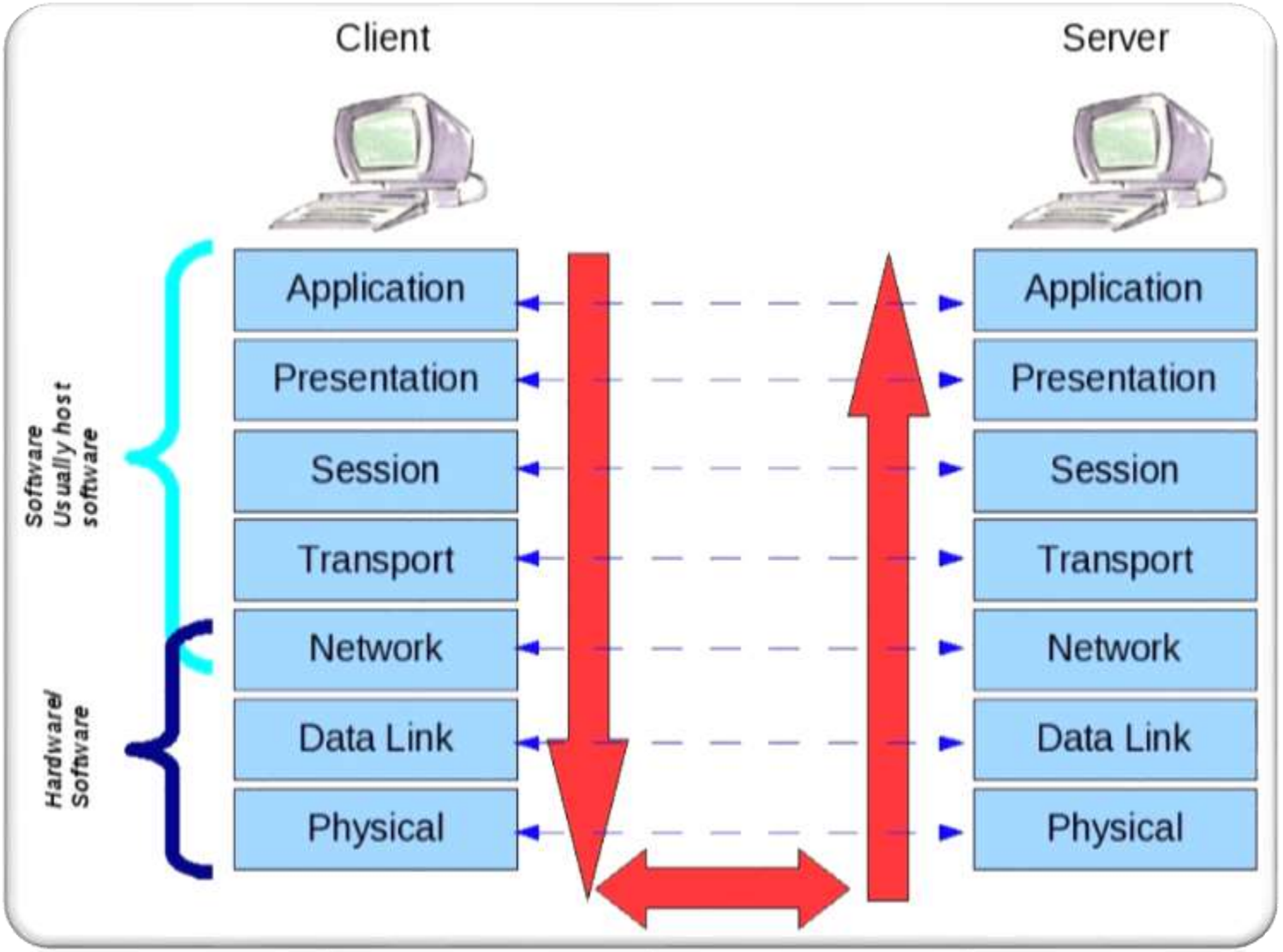
Mom

M

So we've changed the locks

Message

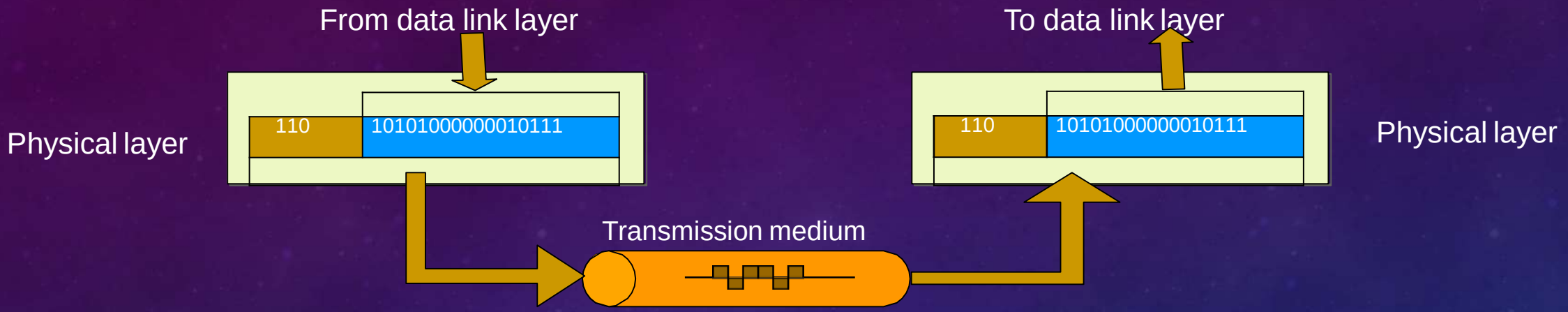
OSI MODEL


Client
Server
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Presentation
Session
Transport
Network
Data Link
Physical
Software
Usually host
software
Hardware/
Software

DATA, PROTOCOL & ACTIVITIES

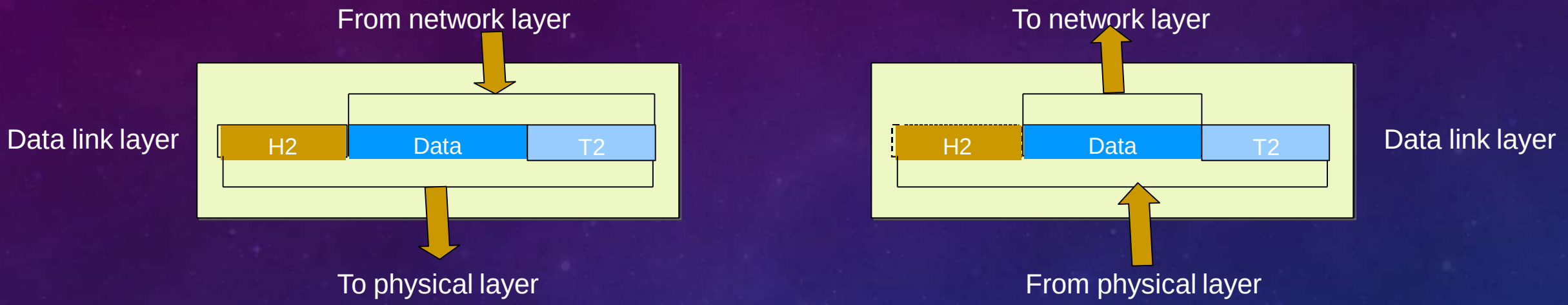
OSI Layers	TCP/IP Suit	Activities
Application	**Application** Telnet, FTP, SMTP, HTTP, DNS, SNMP, *Specific address* etc…	To allow access to network resources
Presentation	**Presentation**	To Translate, encrypt, and compress data
Session	**Session**	To establish, manage, and terminate session
Transport	**Transport** SCTP, TCP, UDP, Sockets and *Ports address*	To Provide reliable process-to-process Message delivery and error recovery
Network	**Network** IP, ARP/RARP, ICMP, IGMP, *Logical address*	To move packets from source to destination; to provide internetworking
Data Link	**Data Link** IEEE 802 Standards, FDDI, PPP, *Physical address*	To organize bits into frames; to provide Hop-to-hop delivery
Physical	**Physical** Medium, Coax, Fiber, 10base, Wireless	To Transmit bits over a medium; to provide Mechanical and electrical specifications

PHYSICAL LAYER



- One of the major function of the physical layer is to move data in the form of electromagnetic signals across a transmission medium.
- Its responsible for movements of individual bits from one hop (Node) to next.
- Both data and the signals can be either *analog* or *digital*.
- Transmission media work by conducting energy along a physical path which can be wired or wireless
  - Physical characteristics of interface and medium (Transmission medium)
  - Representation of bits (stream of bits (0s or 1s) with no interpretation and encoded into signals)
  - Data rate (duration of a bit, which is how long it last)
  - Synchronization of bits (sender and receivers clock must be synchronized)
  - Line configuration (Point-to-Point, Point-to-Multipoint)
  - Physical topology
  - Transmission mode (Simplex, half duplex, full duplex)

DATALINK LAYER

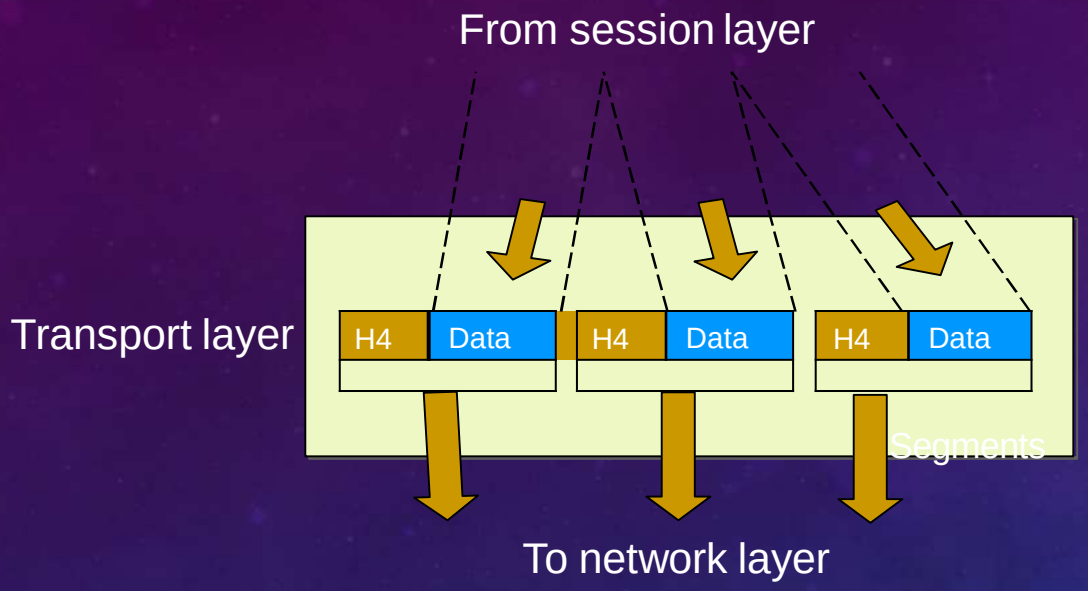


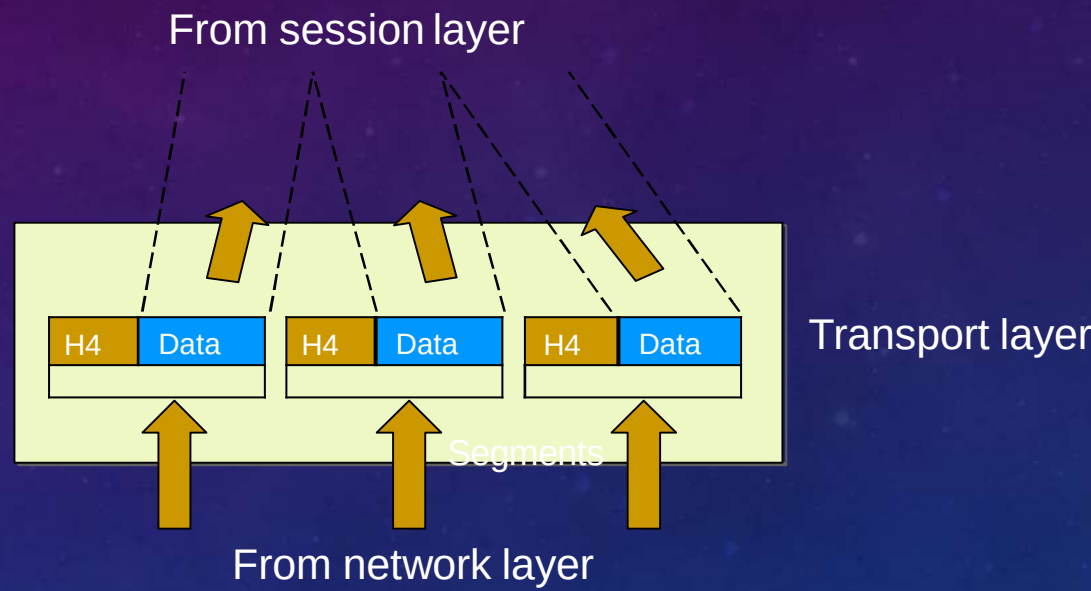
- Data link layer is responsible for moving frames from one hop (Node) to the next.
- Concerned:
  - Framing (stream of bits into manageable data units)
  - Physical addressing (MAC Address)
  - Flow Control (mechanism for overwhelming the receiver)
  - Error Control (trailer, retransmission)
  - Access Control (defining master device in the same link)

NETWORK LAYER

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Concerned:
  - Logical addressing (IP Address)
  - Routing (Source to destination transmission between networks)

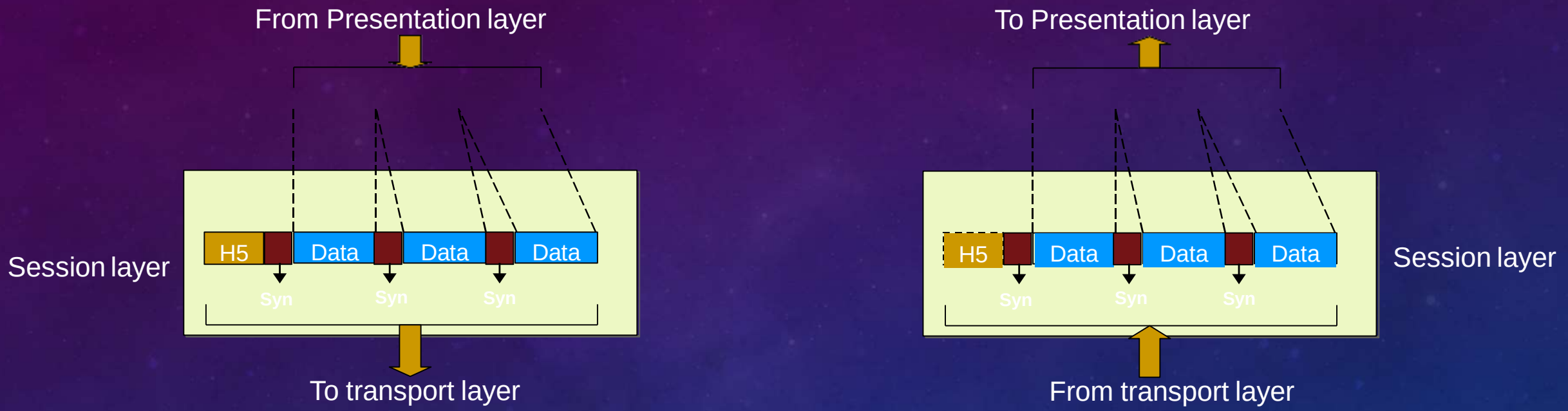
TRANSPORT LAYER





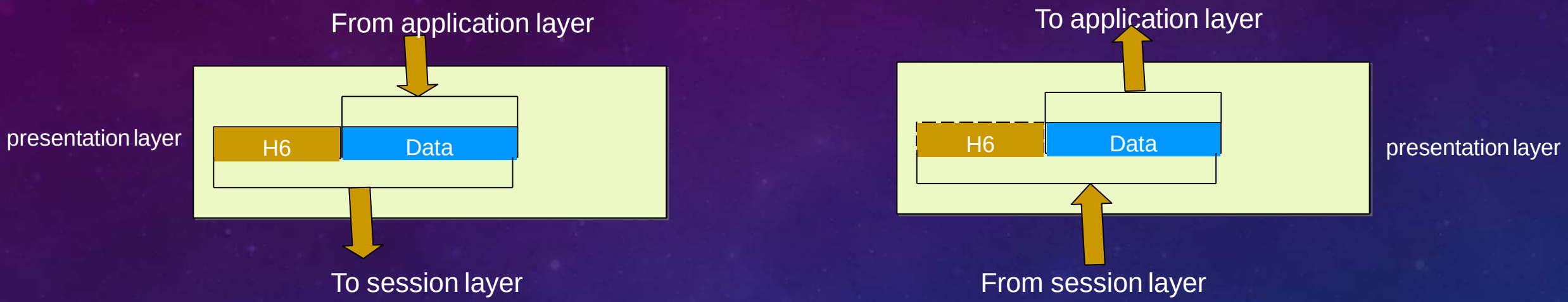
- The transport layer is responsible for the delivery of a message from one process to another
- Concerned:
  - Service-point addressing (Port address)
  - Segmentation and reassembly (Sequence number)
  - Connection control (Connectionless or connection oriented)
  - Flow control (end to end)
  - Error Control (Process to Process)

SESSION LAYER



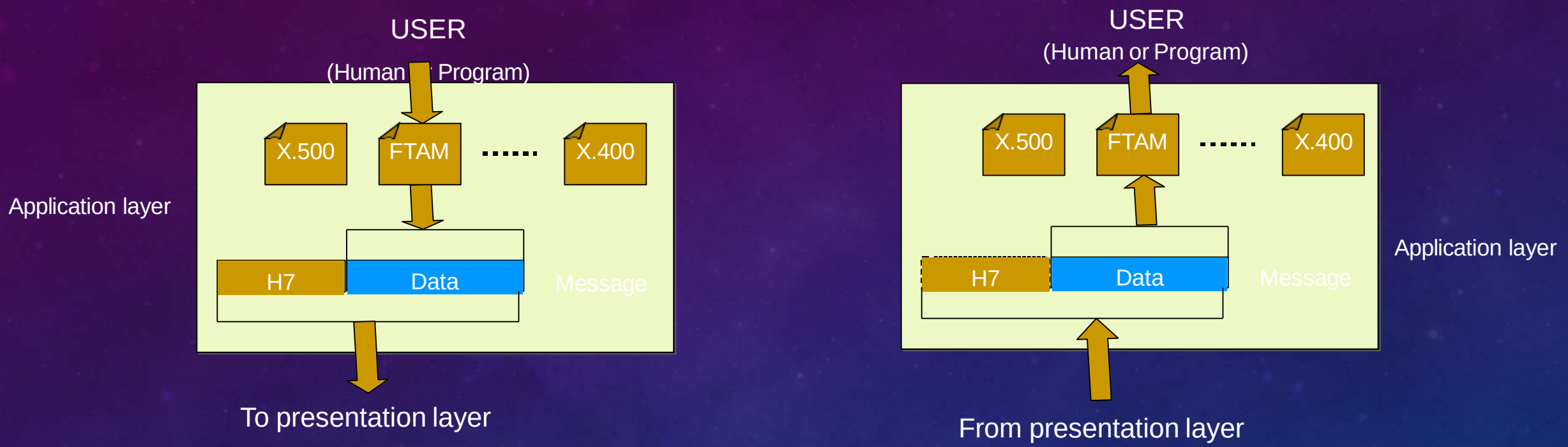
- The session layer is responsible for dialog control and synchronization
- Concerned:
  - Dialog Control (Half Duplex/Full duplex)
  - Synchronization (Synchronization points, process inline within same page)

PRESENTATION LAYER



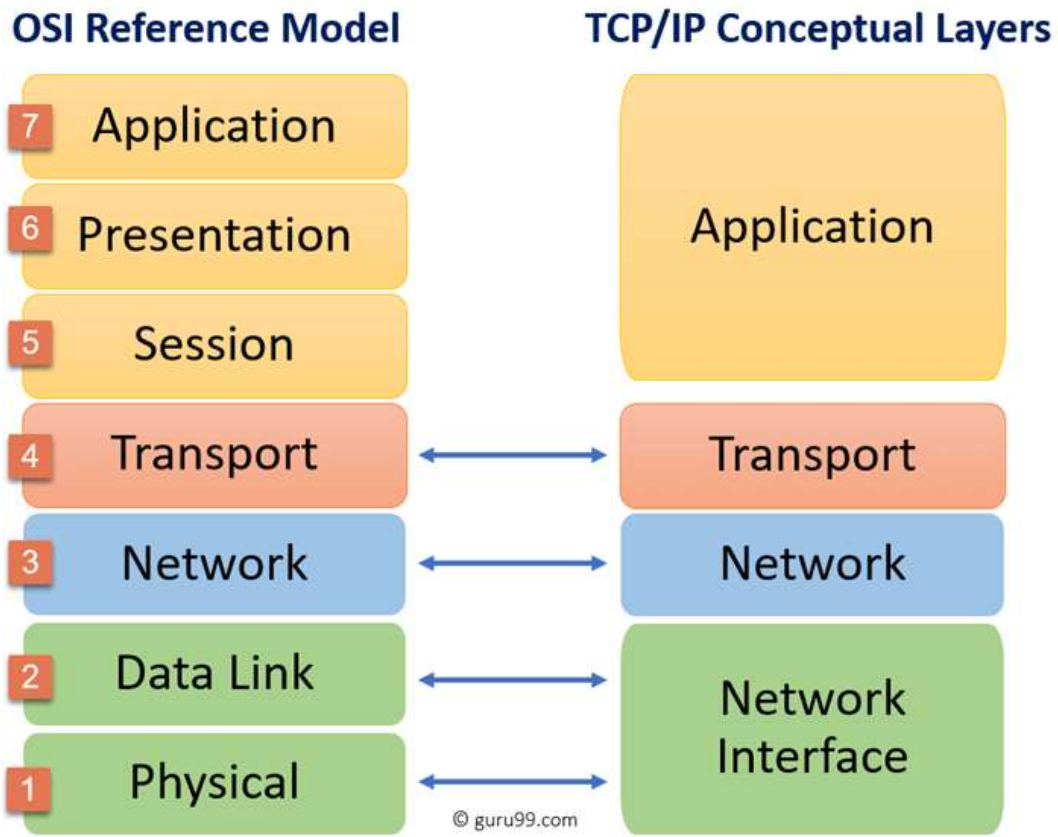
- The presentation layer is responsible for translation, compression and encryption
- Concerned:
  - Translation (interoperability between different encoding system)
  - Encryption (Privacy schemes)
  - Compression (data compression)

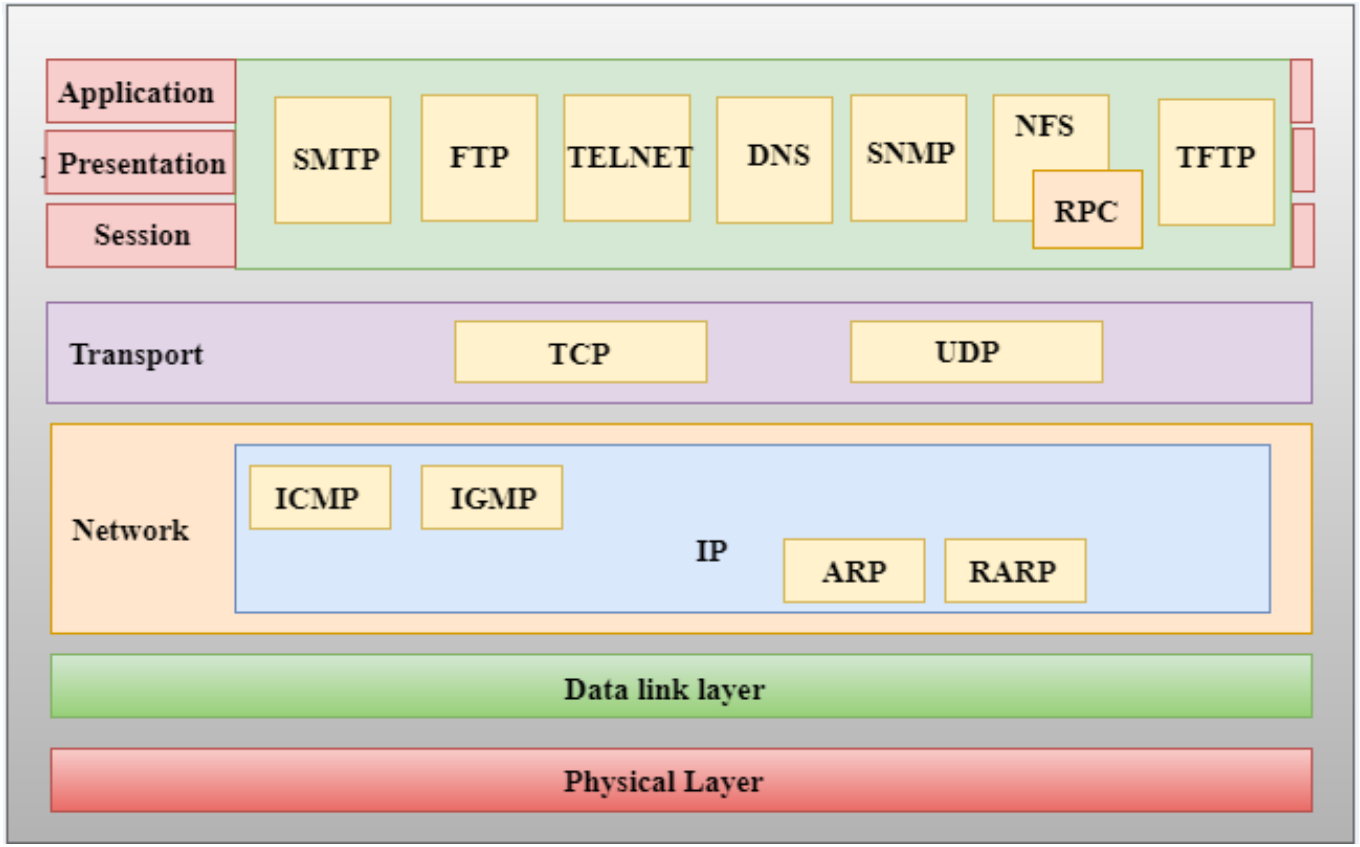
APPLICATION LAYER



- The application layer is responsible for providing services to the user.
- Concerned:
  - Network virtual terminal (Software)
  - File transfer, access and management
  - Mail services
  - Directory services (access to distributed database sources for global information about various objects and services)

OSI and TCP/IP Model





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

OSI
VS
TCP/IP

17.

Access Points with Configurations

Access point?

An access point is the device that allows multiple wireless devices to connect with each other. Just like a HUB or switch connects multiple devices together in a single or multiple wired LAN networks, an access point connects multiple wireless devices together in a single wireless or multiple wireless networks. An access point can also be used to extend the wired network to the wireless devices.

- Standalone Access Point :-A standalone access point provides the same functionality in wireless network which a switch or hub provides in the wired network. It provides connectivity between the different wireless devices. It accepts frame from the connected device and, based on its physical address, forwards it to the destination device.

- Multifunction Access Point :- A multifunction access point is the combination of two or more devices. In this combination an additional device or devices are merged with the access point to provide the additional functionalities along with existing functionality of the access point.

- Controlled Access Point :- controlled by a central unit which is known as WLC Wireless LAN Controller. A WLC control multiple controlled access points in a network.

Key points

- Access point connects multiple wireless devices together in a single wireless network.
- Access point supports both type of standards; Ethernet and Wi-Fi.
- Access point uses radio signals to provide the connectivity.
- Based on functionality an access point can be categorized in three types; standalone, multifunction and client.
- A standalone access point works in the wireless network exactly as the switch works in the wired network.
- To control the unauthorized access, Access point uses authorization.

Let’s Configure…

18.

WLC with Full Configuration

What Is a WLAN Controller?

A WLAN is a wireless architecture that aims to meet changing network demands. A WLAN controller manages wireless network access points that allow wireless devices to connect to the network.

Does my organization need a WLAN controller?

If WLAN controller is embedded in the access point. You are able to manage the entire Wi-Fi network through an access point. Security is another important consideration for any organization, with hacking and data breaches in the news every day. Cisco WLAN controllers battle all kinds of threats to your business based on user ID and location thanks to built-in security features

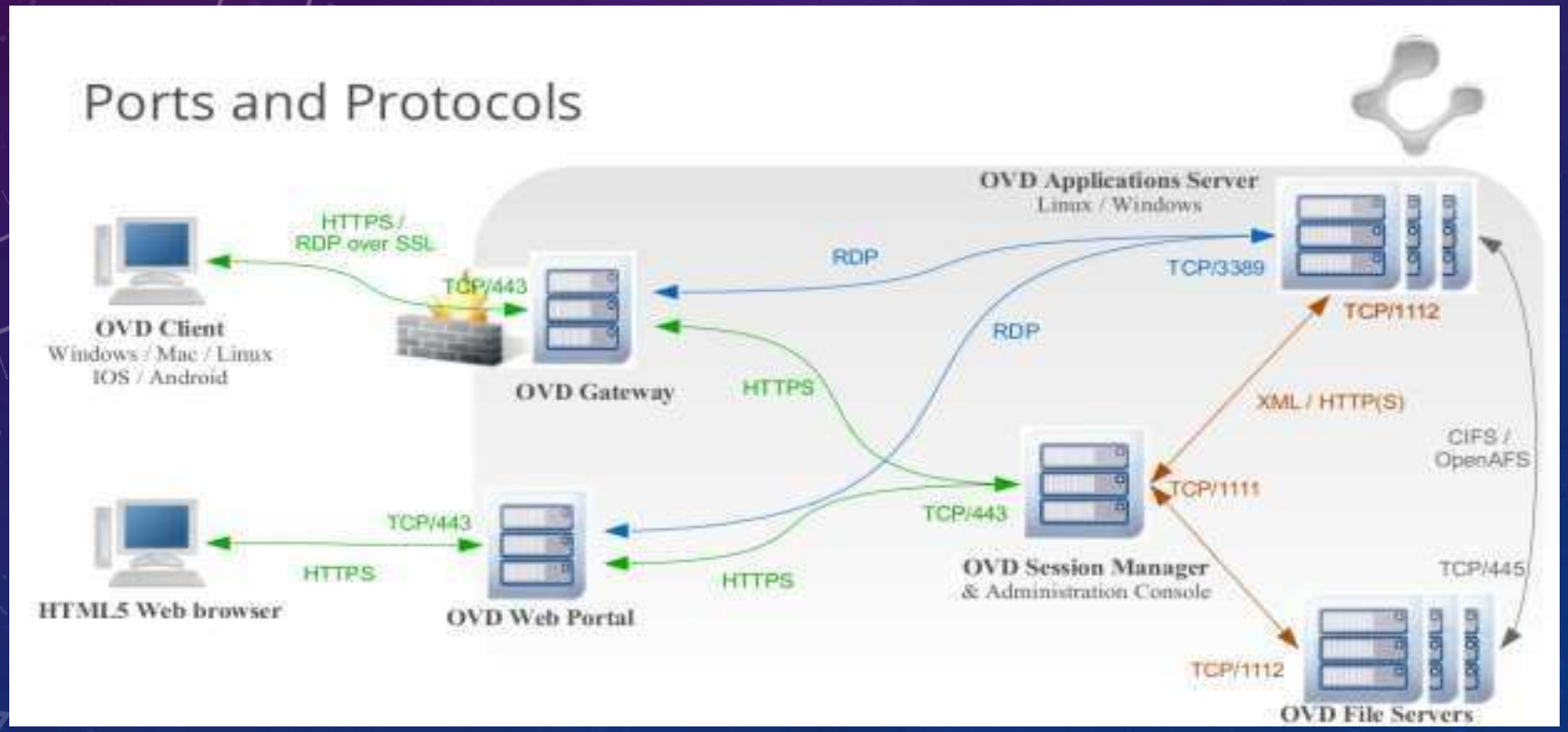
Let’s Configure…

19.

Ports Full Information

Network Ports

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

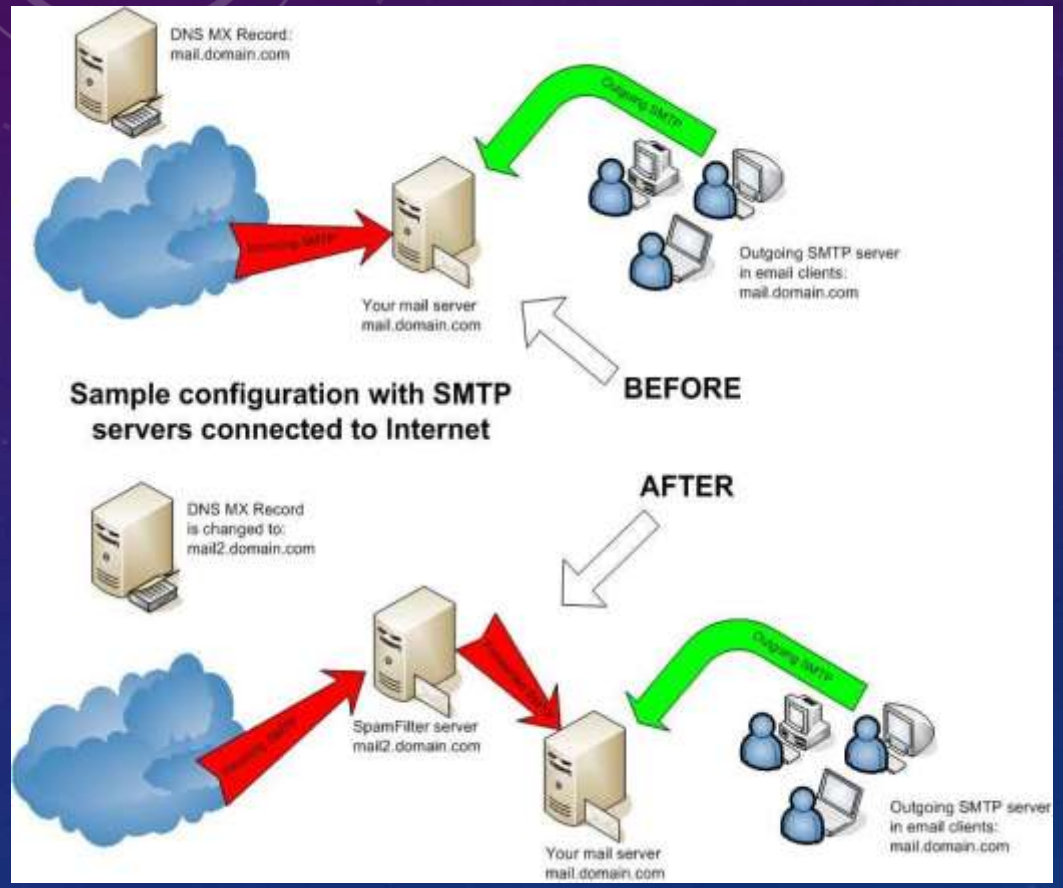


Example

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

Simple Mail Transfer Protocol (SMTP)

- Port number (25)
- SMTP stands for Simple Mail Transfer Protocol
- Main protocol for moving email on the Internet. The sender initiates SMTP transfers
- SMTP is used for two primary functions, it is used to transfer mail (email) from source to destination between mail servers and it is used by end users to send email to a mail system.



Port Forwarding

In computer networking, port forwarding or port mapping is an application of network address translation that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

20.

On-Premises & Cloud Services Explanation

Cloud computing

Cloud computing is the delivery of on demand computer system resources, requiring no active management and usually includes applications such as storage and processing power. With a Cloud-based subscription model, there is no need to purchase any additional infrastructure or licenses. In exchange for an annual fee, a cloud provider maintains servers, network and software for you.

On premise

With on premise software, from implementation to running of the solution, everything is done internally; whereby maintenance, safety and updates also need to be taken care of in-house. Once the software is purchased, it is then installed on your servers; requiring additional power servers, database software and operating systems to be purchased. With no third-party involvement, you assume complete ownership.

CLOUD vs. ON-PREMISE

OVERVIEW

• Low-cost up front • Predictable cost over time • No hardware/server investments	• Reduced initial price
• May end up spending more over the course of the system's life cycle	• Upfront investment can be seen as riskier • Have to pay for hardware and servers • Responsible for IT maintenance and setup

SETUP

• Quick and easy (done by your vendor) • Adding new users and instances is easy • Remote access requires no work on your part	• Setup is done by you, giving you greater control over the process
	• Implementation may take much longer • Responsible for setting up remote access • Adding users and instances may be costly

CUSTOMIZATION

• Greater consistency and stability • More vendor support for customizations	• Direct database access is possible, enabling complex customizations
• Direct database access is not allowed for security reasons, which may limit complex customization	• Bespoke integrations may break when the vendor updates the software

MAINTENANCE

• Server and hardware taken care of by vendor • Updates, patches and fixes are installed automatically and regularly	
	• Perform updates, patches and fixes yourself • Maintain supporting servers, hardware, resources

SECURITY & DISASTER RECOVERY

• Security and backups taken care of by vendor	• Security is in your hands; greater personal control over your data
• Security and backups taken care of by vendor – quality of data center will vary	• Security is in your hands; you are responsible for data breaches and server failures • You carry cost of backups and server redundancy

21.

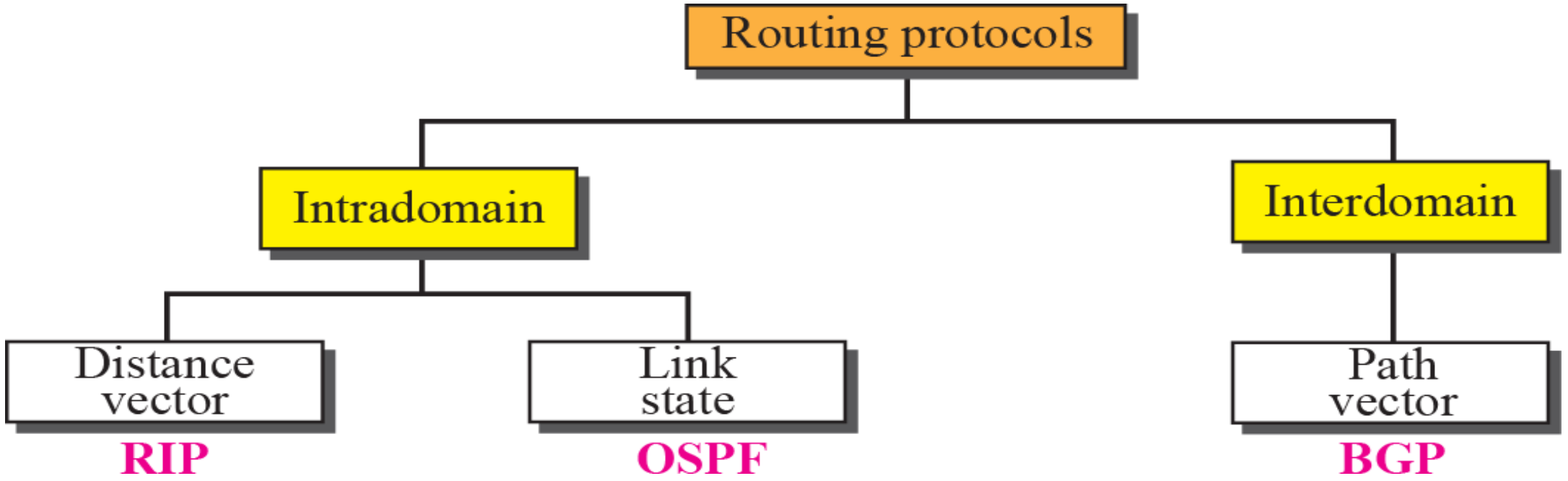
Routing with Routing Tables Concepts

INTER- AND INTRA-DOMAIN ROUTING

Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems.

An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is called intra-domain routing. Routing between autonomous systems is called inter-domain routing

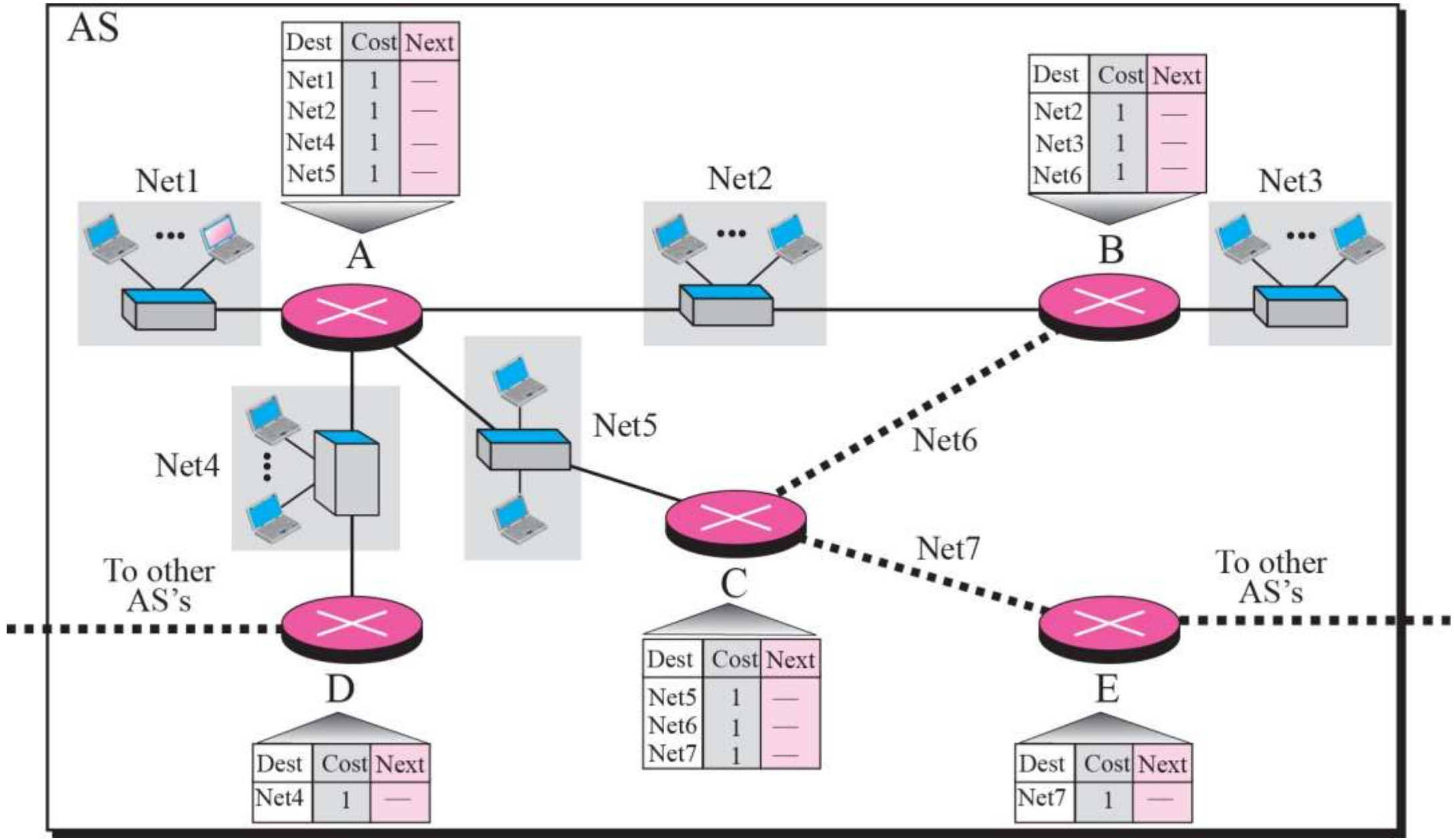
POPULAR ROUTING PROTOCOLS



DISTANCE VECTOR ROUTING

Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems.

An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is called intra-domain routing. Routing between autonomous systems is called inter-domain routing


AS
Dest Cost Next
Net1 1 —
Net2 1 —
Net4 1 —
Net5 1 —
Net1
A
Net2
Dest Cost Next
Net2 1 —
Net3 1 —
Net6 1 —
B
Net3
Net4
Net5
Net6
Net7
To other AS's
C
Dest Cost Next
Net5 1 —
Net6 1 —
Net7 1 —
D
Dest Cost Next
Net4 1 —
E
Dest Cost Next
Net7 1 —
To other AS's

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net6	1	—

After receiving record 1

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net6	1	—

After receiving record 2

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net4	2	A
Net6	1	—

After receiving record 3

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net4	2	A
Net5	2	A
Net6	1	—

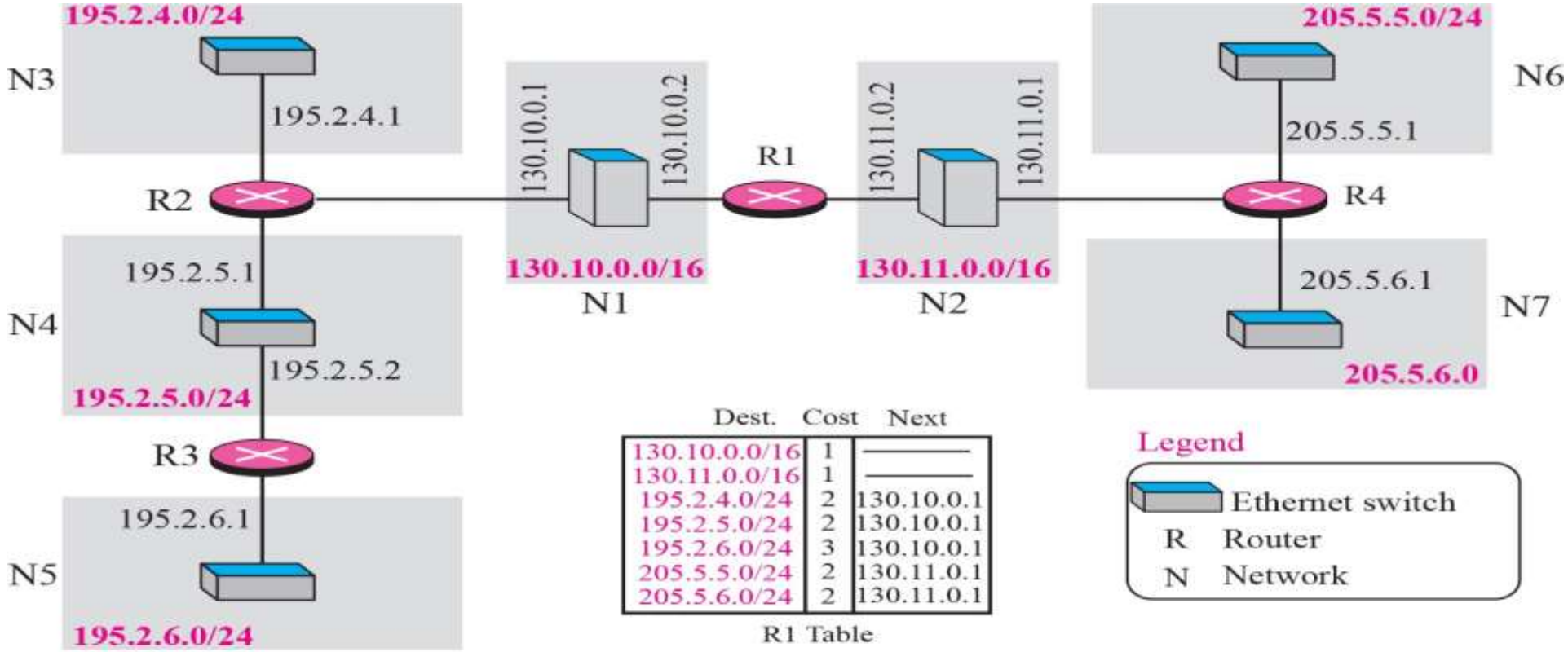
After receiving record 4

RIP

The Routing Information Protocol (RIP) is an intra-domain (interior) routing protocol used inside an autonomous system.

It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations.

EXAMPLE OF A DOMAIN USING RIP



Dest.	Cost	Next
130.10.0.0/16	1	———
130.11.0.0/16	1	———
195.2.4.0/24	2	130.10.0.1
195.2.5.0/24	2	130.10.0.1
195.2.6.0/24	3	130.10.0.1
205.5.5.0/24	2	130.11.0.1
205.5.6.0/24	2	130.11.0.1

R1 Table

Legend

Ethernet switch
R Router
N Network

Dest.	Cost	Next
130.10.0.0/16	1	———
130.11.0.0/16	2	130.10.0.2
195.2.4.0/24	1	———
195.2.5.0/24	1	———
195.2.6.0/24	2	195.2.5.2
205.5.5.0/24	3	130.10.0.2
205.5.6.0/24	3	130.10.0.2

R2 Table

Dest.	Cost	Next
130.10.0.0/16	2	195.2.5.1
130.11.0.0/16	3	195.2.5.1
195.2.4.0/24	2	195.2.5.1
195.2.5.0/24	1	———
195.2.6.0/24	1	———
205.5.5.0/24	4	195.2.5.1
205.5.6.0/24	4	195.2.5.1

R3 Table

Dest.	Cost	Next
130.10.0.0/16	2	130.11.0.2
130.11.0.0/16	1	———
195.2.4.0/24	3	130.11.0.2
195.2.5.0/24	3	130.11.0.2
195.2.6.0/24	4	130.11.0.2
205.5.5.0/24	1	———
205.5.6.0/24	1	———

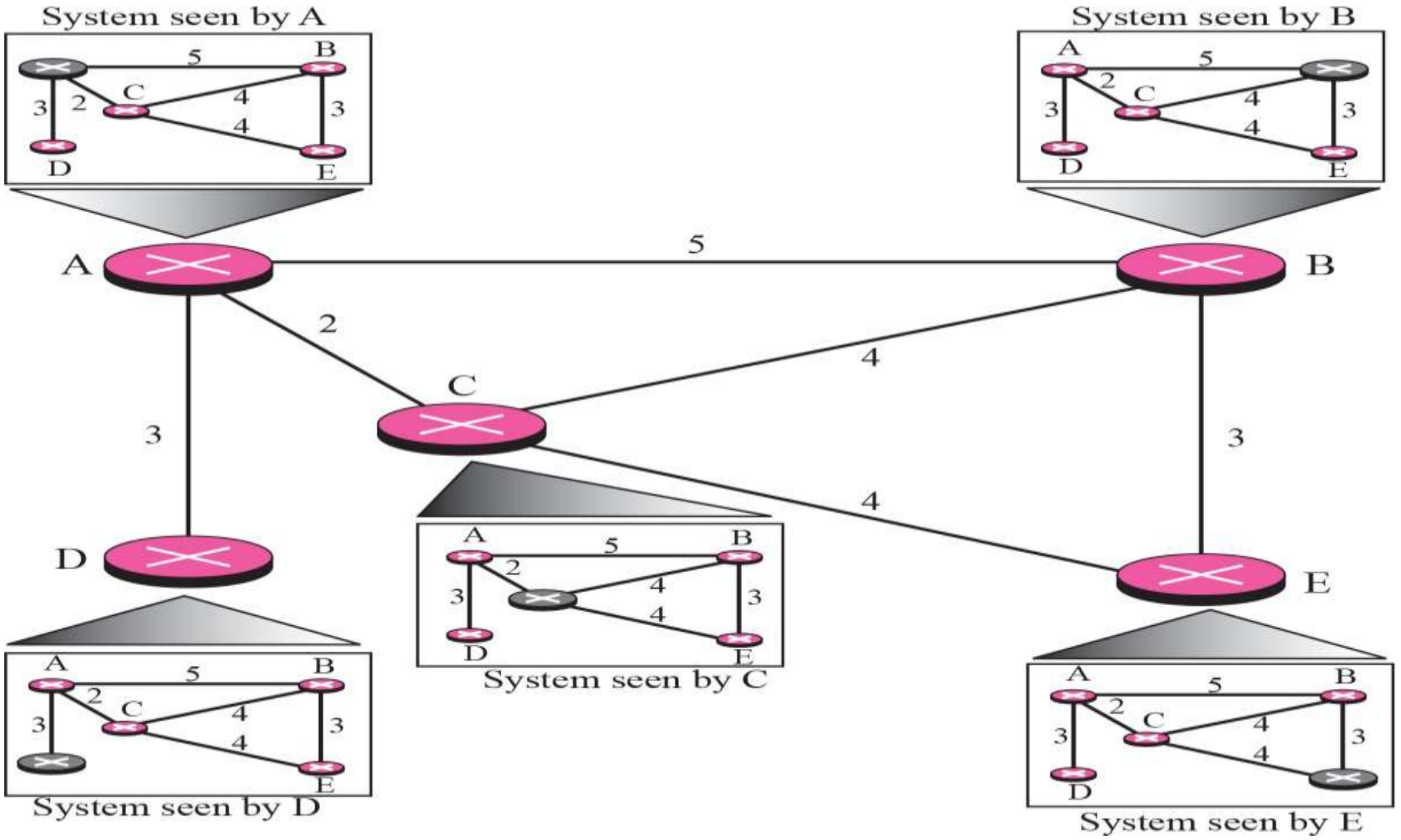
R4 Table

LINK STATE ROUTING

Link state routing has a different philosophy from that of distance vector routing.

In link state routing, if each node in the domain has the entire topology of the domain—the list of nodes and links, how they are connected including the type, cost (metric), and the condition of the links (up or down)—the node can use the algorithm to build a routing table.

CONCEPT OF LINK STATE ROUTING

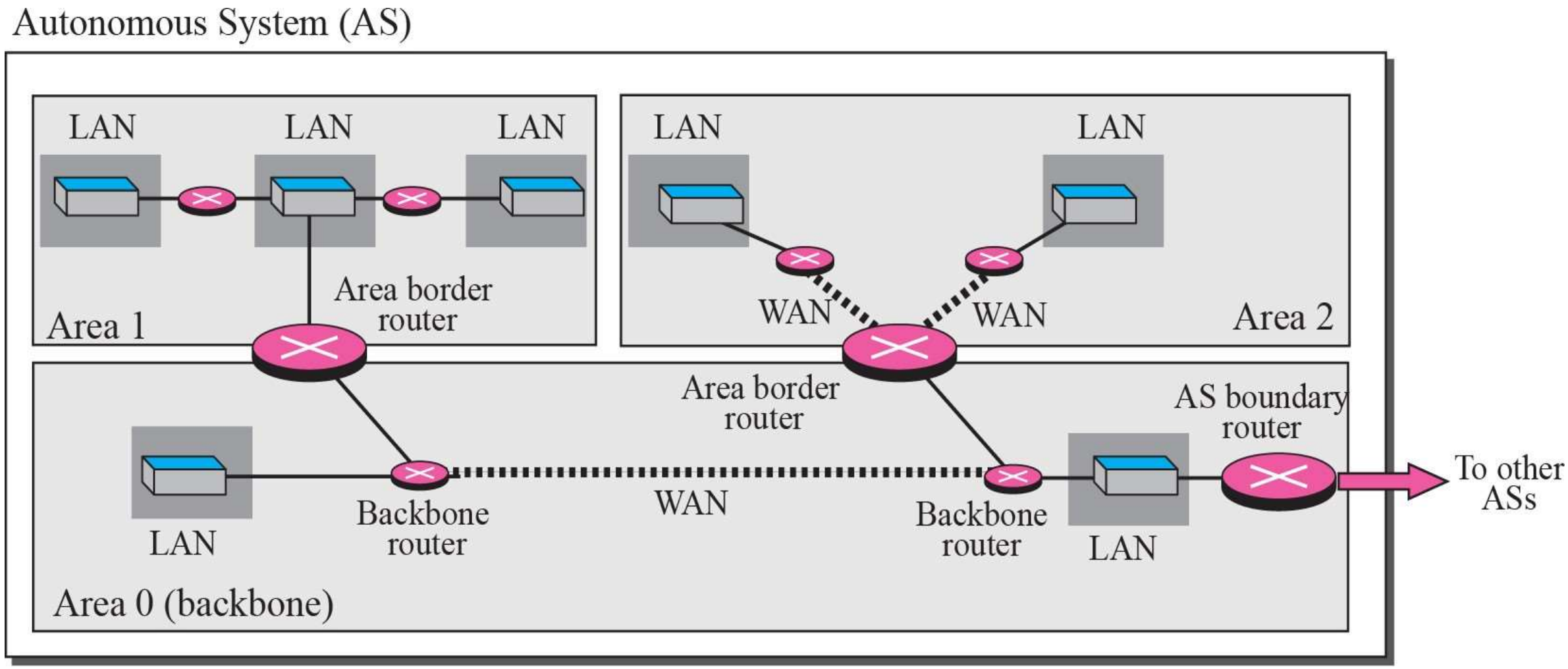


OSPF

The Open Shortest Path First (OSPF) protocol is an intra-domain routing protocol based on link state routing. Its domain is also an autonomous system.

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First).

AREAS IN AN AUTONOMOUS SYSTEM

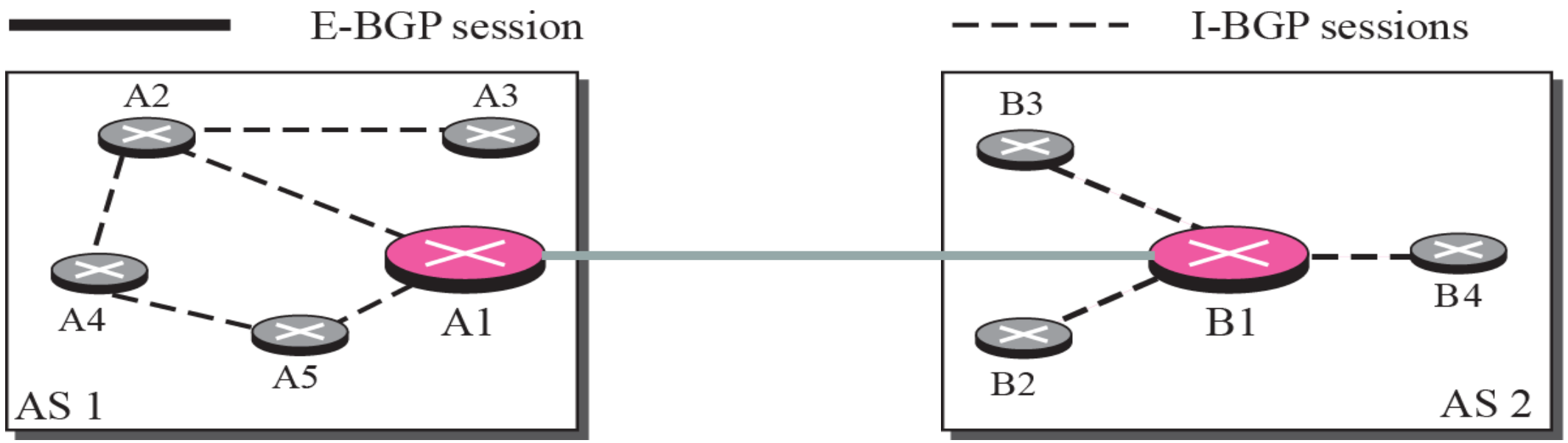


BGP

Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.

BGP (**Border Gateway Protocol**) is the **protocol** underlying the global **routing** system of the internet. It manages how packets get routed from network to network through the exchange of **routing** and reachability information among edge routers.

INTERNAL AND EXTERNAL BGP SESSIONS



22.

FTP & TFTP Functions & Capabilities

FTP

FTP stands for File Transfer Protocol. This type of protocol is used to transfer or copies the file from one host to another host. But there may be some problems like different file name and different file directory while sending and receiving file in different hosts or systems.

TFTP

TFTP stands for Trivial File Transfer Protocol. TFTP is used to transfer a file either from client to server or from server to client without the need of FTP feature. Software of TFTP is smaller than FTP. TFTP works on 69 Port number and its service is provided by UDP.

S.NO	FTP	TFTP
1.	FTP stands for File Transfer Protocol.	TFTP stands for Trivial File Transfer Protocol.
2.	The software of FTP is larger than TFTP.	While software of TFTP is smaller than FTP.
3.	FTP works on two ports: 20 and 21.	While TFTP works on 69 Port number.
4.	FTP services are provided by TCP.	While TFTP services are provided by UDP.
5.	The complexity of FTP is higher than TFTP.	While the complexity of TFTP is less than FTP complexity.
6.	There are many commands or messages in FTP.	There are only 5 messages in TFTP.
7.	FTP need authentication for communication.	While TFTP does not need authentication for communication.
8.	FTP is generally suited for uploading and downloading of files by remote users.	While TFTP is mainly used for transmission of configurations to and from network devices.

Let’s Configure…

23.

Syslog Server with all features

What is a Syslog Server

System Logging Protocol (Syslog) is a way network devices can use a standard message format to communicate with a logging server. It was designed specifically to make it easy to monitor network devices.

Syslog has three layers as part of the standard definition:

- **Syslog content:** The information in the event message
- **Syslog application:** The layer that generates, routes, interprets, and stores the message
- **Syslog transport:** The layer that transmits the message

What Does Syslog Do?

Syslog provides a way for network devices to send messages and log events. For this to work, Syslog has a standard format all applications and devices can use. A syslog message contains the following elements:

- Header
- Structured data
- Message

Let’s Configure…

24.

SSH & telnet with Configuration

SSH

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. In addition to providing secure network services, SSH refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network

Telnet

A general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Based on command based alias. You need to give instruction to get the result.

PARAMETER	SSH	Telnet
Security	Highly secured	Less secured than SSH
Port number	Uses TCP port number 22	Uses TCP port number 23
Data format	SSH sends all the data in encrypted format. SSH uses a secure channel to transfer data over the network	Telnet sends the data in plain text.
Authentication	SSH uses public key encryption in order to authenticate the remote users	Telnet uses no authentication mechanisms
Data Privacy	Usernames and Passwords can be prone to malicious attack	Data sent using this protocol cannot be easily interpreted by the hackers.
Public/Private network recommendation	Suitable for Public networks	Suitable for private networks
Vulnerabilities	Can be considered a replacement of telnet since has overcome many of security issues of telnet	Is older than SSH and has many vulnerabilities than SSH.
Bandwidth usage	High bandwidth usage	Low bandwidth usage
Operating system	All popular Operating systems	Used in Linux and Windows Operating system.

Let’s Configure…

25.

Understanding Network Security Concepts

Network Security

Network Security is very important for any organization. So, it need to be understand the basic concepts of Network Security. vulnerabilities we may have in our networks, the threats that we may face and some of the attacks.

1.Vulnerability – this are the weaknesses that we may have in the network. They may be as a result of the technology in use, the configuration on our devices or poor or weak security policies. In our networks, we need to plan for security carefully and consider these factors, a comprehensive security policy would be crucial in ensuring that data in our network is not accessed due to weak security on our devices.

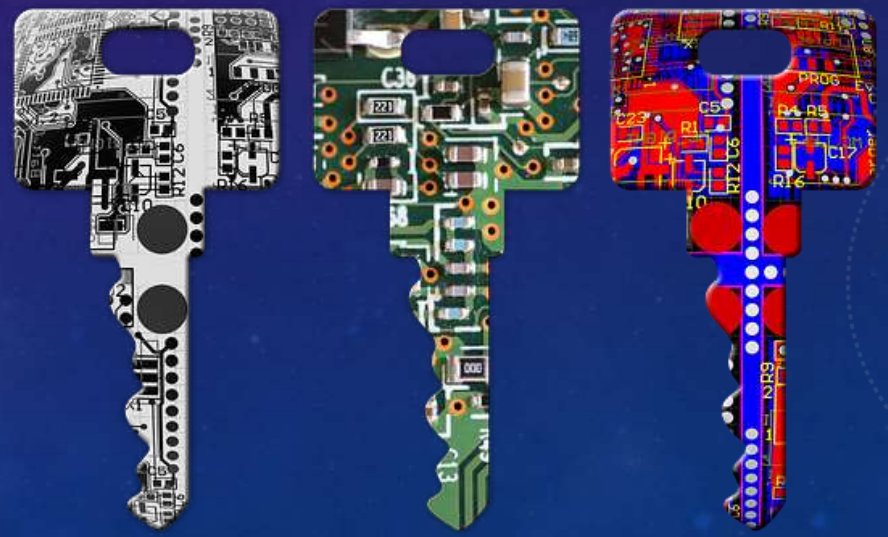
2.Threats – in network security, anyone who has the skill and the interest to manipulate any of the vulnerabilities, is known as a threat. These individuals or groups may be motivated by many factors such as money, power, and thrill seeking among others. Whatever the motive may be, threats to network security pose a major challenge for administrators since they may access information that is sensitive or even cripple the network.

3.Attacks – these are the methods that are used by the threats to access the network. There are a number of attacks that can be used to access our network. They may be aimed at the network infrastructure through methods such as dumpster diving, or aimed at users using methods such as social engineering.

Securing the network

The security issues in the network are many and cannot be covered in one chapter, the various methods used by attackers to access networks have grave and far reaching effects, as such, we will focus on protecting routers and switches in this course. Some of the protection methods we will look at include:

1.Physical security
2.Passwords
3.SSH
4.Port security



1. Physical Security

Physical threats to network devices are a major issue. Physical attacks may cripple an enterprise's productivity due to outage of network services. The four classes of physical threats are:

1.Hardware threats-damage to network infrastructure such as servers, routers and switches.

Sol :- The location used for storing networking equipment as well the wiring closets, should only be accessed by authorized person. All the entrances should be secured and monitoring should be implemented by using CCTV cameras.

2.Environmental threats– these are the threats that are brought about by storing the networking equipment in unsuitable places; the hardware may be subjected to extreme temperatures or extreme humidity.

Sol :- The environment should be controlled to mitigate the environmental factors. the humidity, temperature, and other environmental factors should be monitored. The network control room should ideally be in a room where the conditions can be controlled effectively.

3.Electrical faults – the equipment that is used in our networks relies on electricity to work, as such, any sudden change in the electrical power supplied to the network devices is a major threat.

Sol :- The electrical threats may be mitigated by using UPS systems, so that the networking devices don’t draw their power directly from the mains. There should be backup systems such as generators and inverters so as to maintain network connectivity in case of power outage.

4.Maintenance threats – from time to time, we may need to run maintenance checks on our network devices, the use of untrained technicians can pose a major threat to the network devices.

Sol :- Maintenance threats should be mitigated by using well trained personnel. All the cables should be well labeled, maintenance logs should be maintained, and there should be availability of spare parts that are critical to maintaining connectivity.

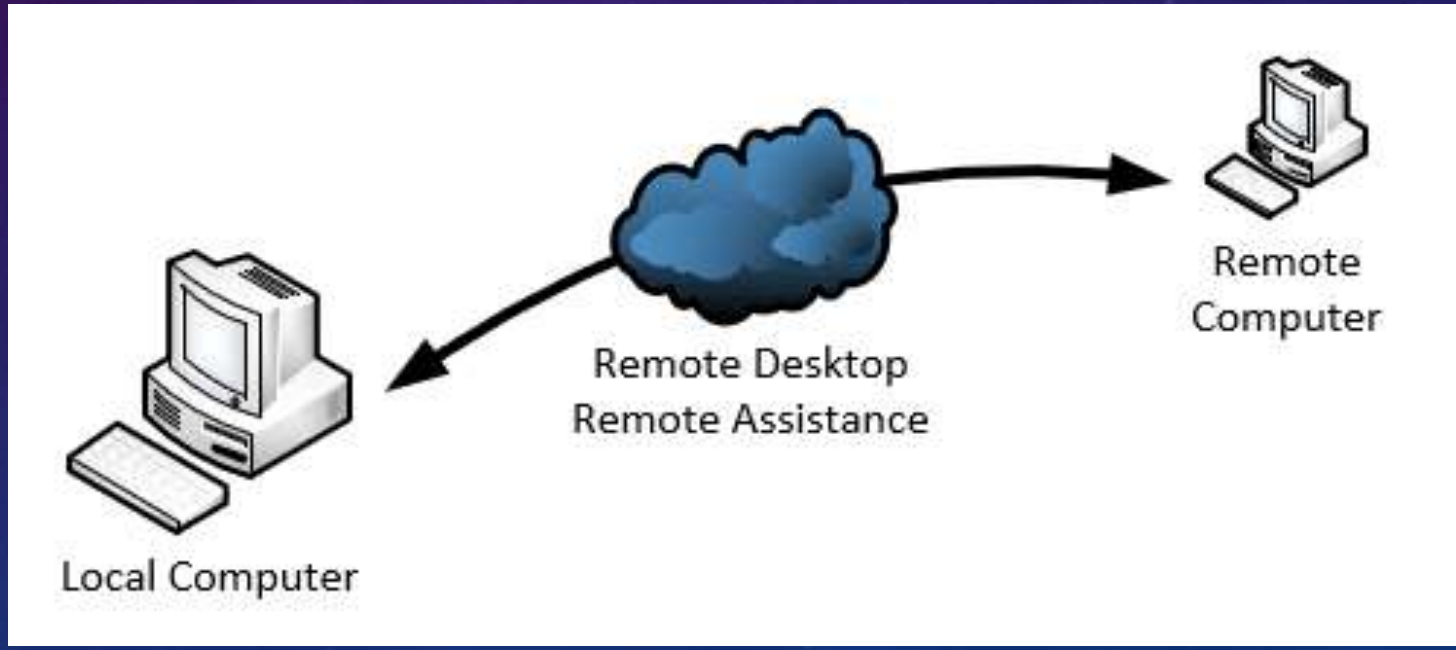
2. Passwords

Use of encrypted passwords is also better than passwords that have been stored in plain text. Use those services
Which makes sure to transmit your data encrypted. It is very important because sometime the attacker attacks
In your data by analyzing your data packets.

- Use Complex password at least 8 letters and alphabets.
- Use Special symbols and signs in password like $,%,&,*
- Do not use common password like 12345678
- Do not enter your credential by following untrusted links
- Try to make password with combination of alphanumeric and symbols

3. SSH (secure shell)

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. In addition to providing secure network services, SSH refers to the suite of utilities that implement the SSH protocol. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network



4. Port security

Port security is important in switch security. Unused ports are a major security issue since they can be used to attack the network. As discussed in the chapter on switch operation, securing switchports includes:

1. Using static or sticky mac-address mappings to ports
2. Configuring maximum number of ports that can access a switchport.
3. Configuring violation measures such as protect, restrict and shutdown.
4. Shutdown unused ports
5. Assign unused ports to a VLAN

26.

DNS & DHCP Services with Configuration

DNS

The main **function** of **DNS** is to translate domain names into IP Addresses, which computers can understand. It also provides a list of mail servers which accept Emails for each domain name.
Each domain name in **DNS** will nominate a set of name servers to be authoritative for **its** **DNS** records.

DHCP

Dynamic Host Configuration Protocol (**DHCP**) is a network management protocol **used** to automate the process of configuring devices on IP networks. **DHCP** stands for dynamic host configuration protocol and is a network protocol used on IP networks where a **DHCP** server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

Let’s Configure…

27.

Defernite Authorization & Authentication

Authorization???

Authentication???

28.

Automation & Programming in CCNA

How automation impacts network management

Traditional networks vs Controller-based networking

Let’s Automate…

29.

Rest Based APIs (CRUD & Data Encoding)

CRUD

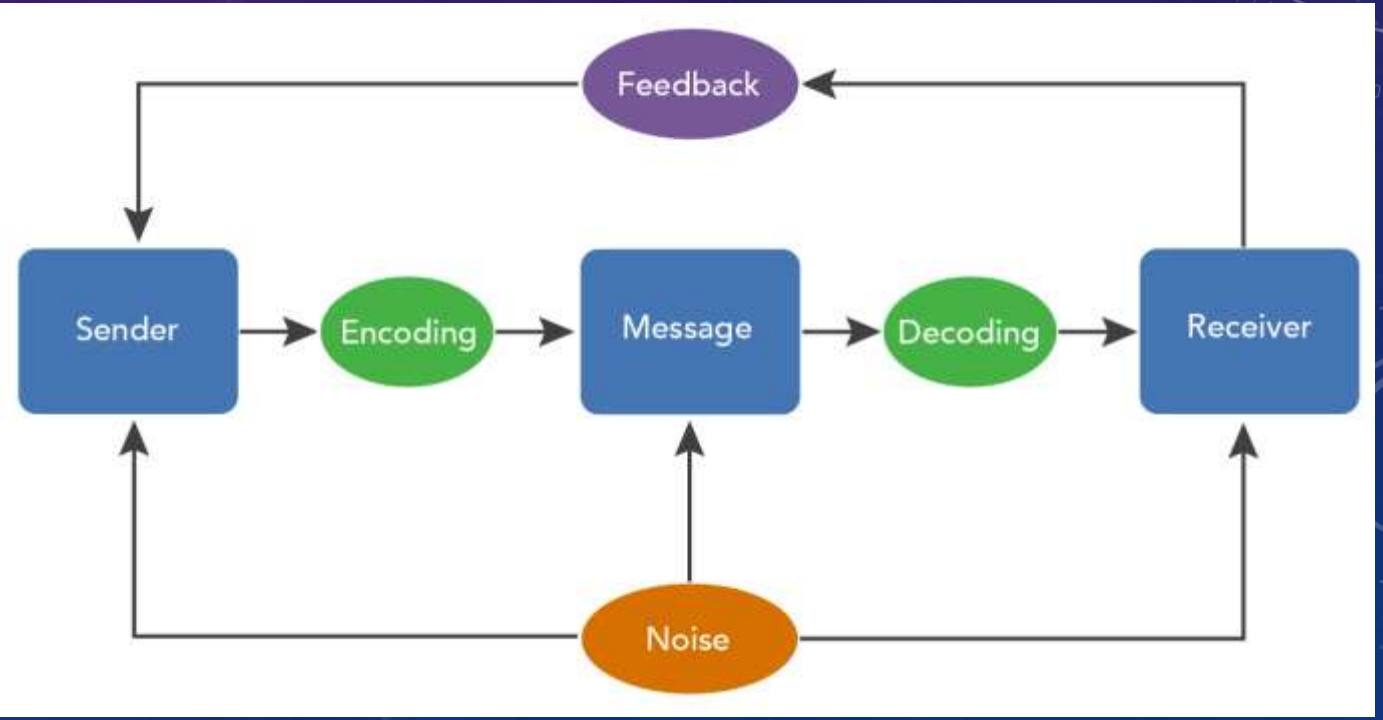
Create, Read, Update, Delete

When we are building APIs, we want our models to provide four basic types of functionality. The model must be able to Create, Read, Update, and Delete resources. Computer scientists often refer to these functions by the acronym CRUD. A model should have the ability to perform at most these four functions in order to be complete. If an action cannot be described by one of these four operations, then it should potentially be a model of its own.

```
“book”: {
  "id": <Integer>,
  “title”: <String>,
  “author”: <String>,
  “isbn”: <Integer>
}
```

Data Encoding

Data Encoding Techniques. **Encoding** is the process of converting the **data** or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of **data**. Decoding is the reverse process of **encoding** which is to extract the information from the converted format.



30.

Designing an Infra using all Conceptual Scenarios

Let’s Understand…

Hope Guys You got the point of the Video