# Introduction to CCNA Course

# Cisco Systems

- Worldwide leader in IT and networking.
- Help companies of all sizes transform on how people connect, communicate, and collaborate.
- HQ in US - San Jose, California

# Cisco Products

- Routers
- Switches
- Firewalls
- IP Phones
- Wireless Access Points
- Wireless Controllers

# Other Networking Vendors

Juniper Networks - Routers, Switches, Firewalls

Palo Alto - Security Devices

Check Point - Security Devices

Barracuda- Security, Storage, Cloud services

# Cisco Certification Track

1

**CCNA-**
**Cisco Certified Network Associate**

2

**CCNP-**
**Cisco Certified Network Professional**

**Specialization-**
**Cisco Certified Specialist Certification**

3

**CCIE-**
**Cisco Certified Internetwork Expert**

4

**CCDE-**
**Cisco Certified Design Expert**

**CCAr-**
**(Architecture) Comprehensive Capital Analysis and Review**

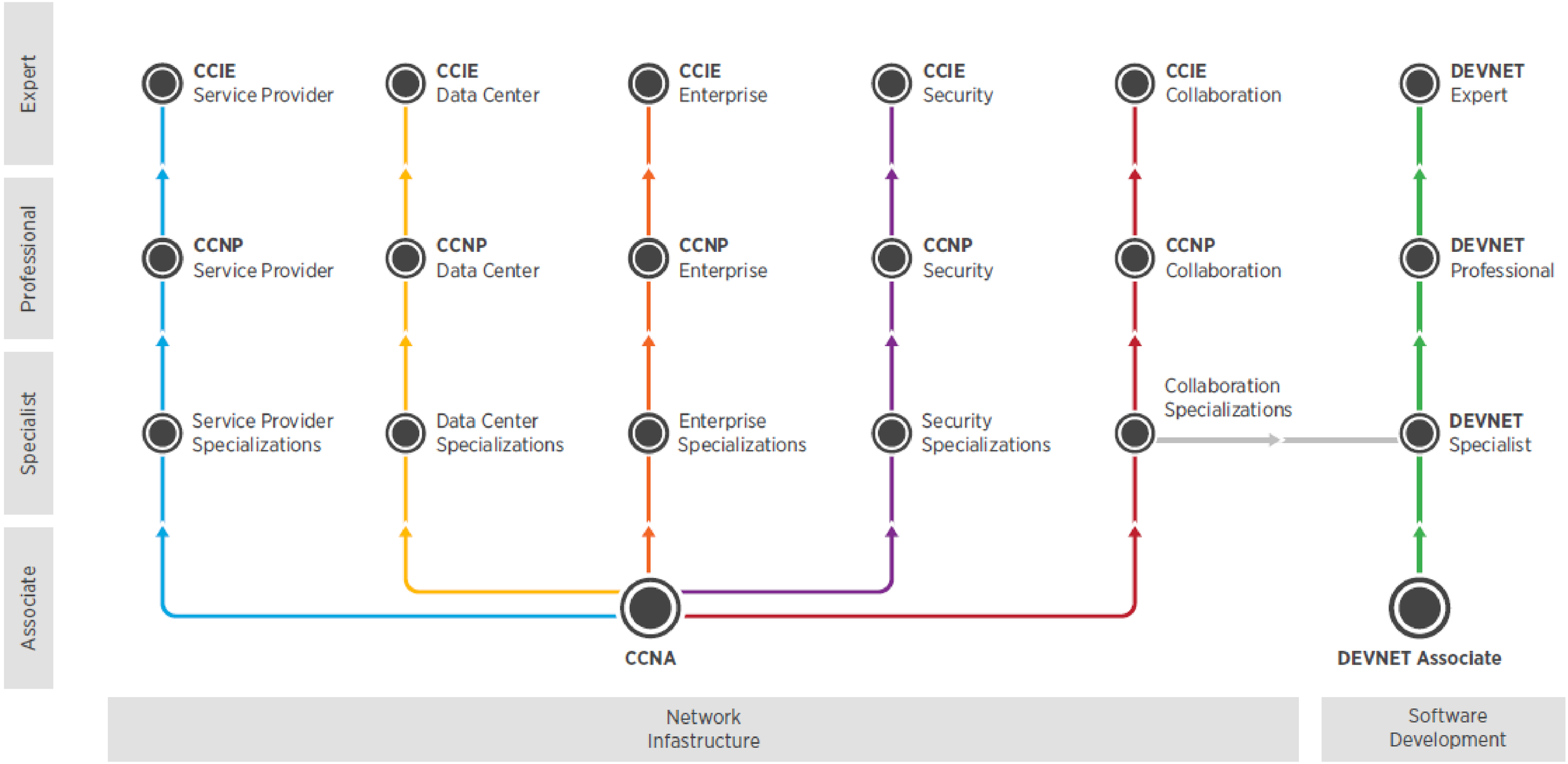
# Old CCNA Syllabus

- CCNA Enterprise
- CCNA Security
- CCNA Data Center
- CCNA Service Provider
- CCNA Collaboration
- CCNA Wireless

# New CCNA Syllabus

**CCNA 200-301**

# Cisco Certification Track



# Cisco Certified Network Associate

Course Code : 200 - 301

Examination Cost : $300 USD (1 paper)

Duration : 120 minutes

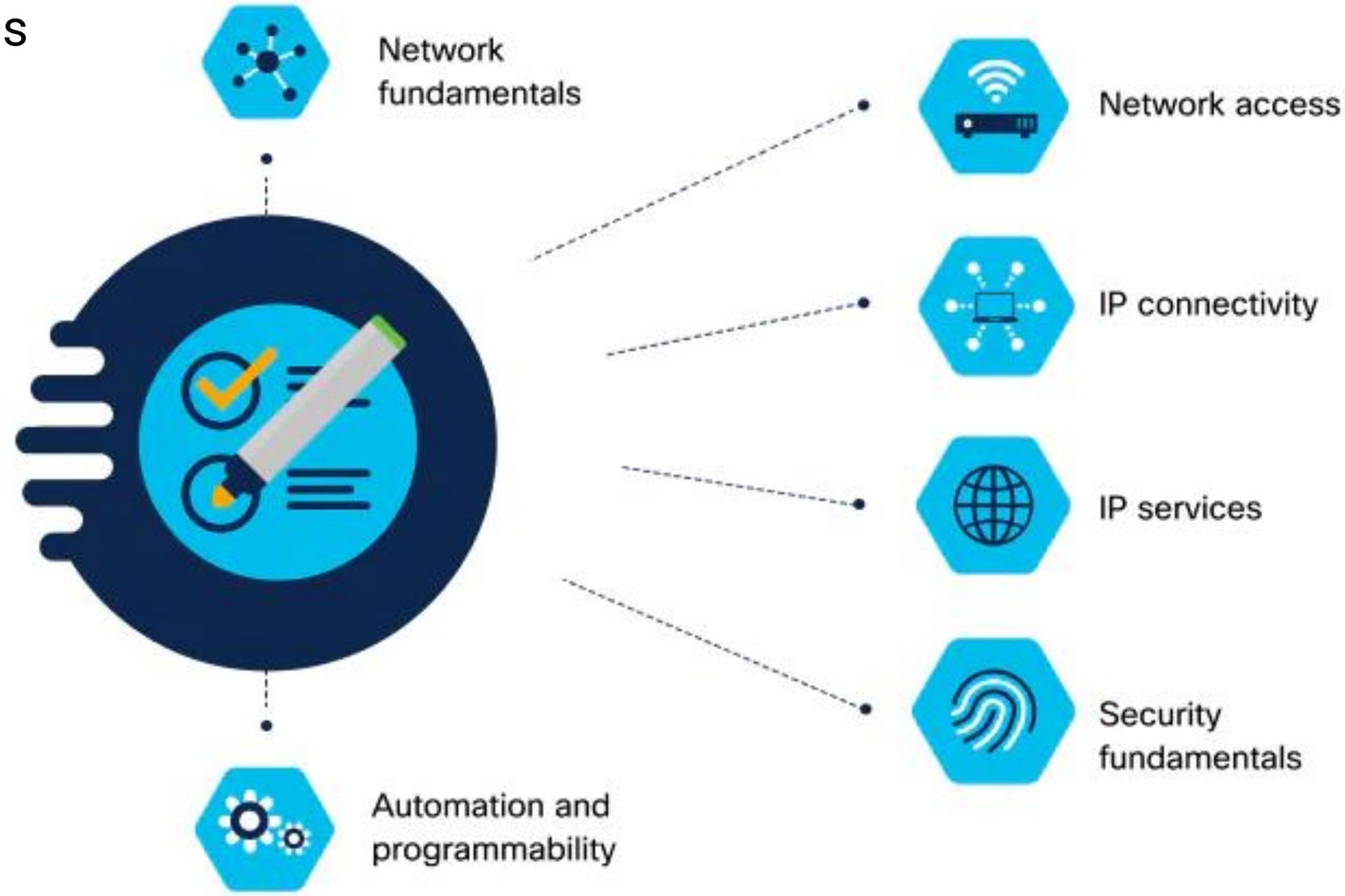
Validity : 3 years

Questions : 60 to 80

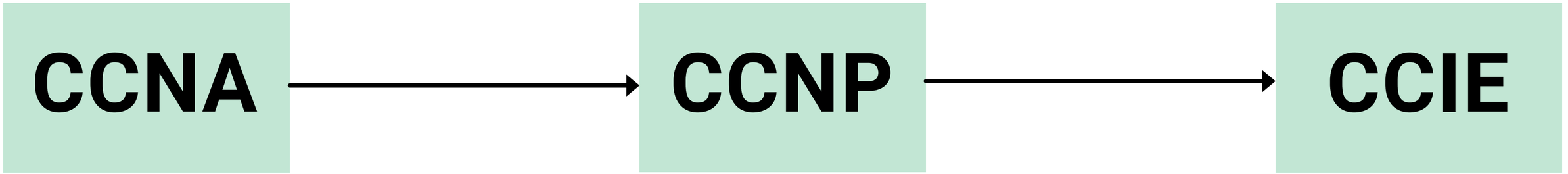
Passing score : 85 percent

# CCNA Modules

- Networking fundamentals
- IP Connectivity
- Network Access
- IP Service
- Security Fundamentals
- Wireless
- Automation



# Time Duration




1 Month

3 Months

4 Months

# Software or tool used : Cisco Packet Tracer

Cisco Packet Tracer 8.0.1 (64 bit):

- Computer with one of the following operating systems: Microsoft Windows 8.1, 10 (64bit), Ubuntu 20.04 LTS (64bit) or macOS 10.14 or newer.
- 4GB of free RAM
- 1.4 GB of free disk space

Cisco Packet Tracer 8.0.1 (32 bit):

- Computer with one of the following operating systems: Microsoft Windows 8.1, 10 (32bit)
- 2GB of free RAM
- 1.4 GB of free disk space

# Network Components

# What is a network?

# What is a Topology?

Topology defines the structure of how all the components are interconnected to each other in a network.

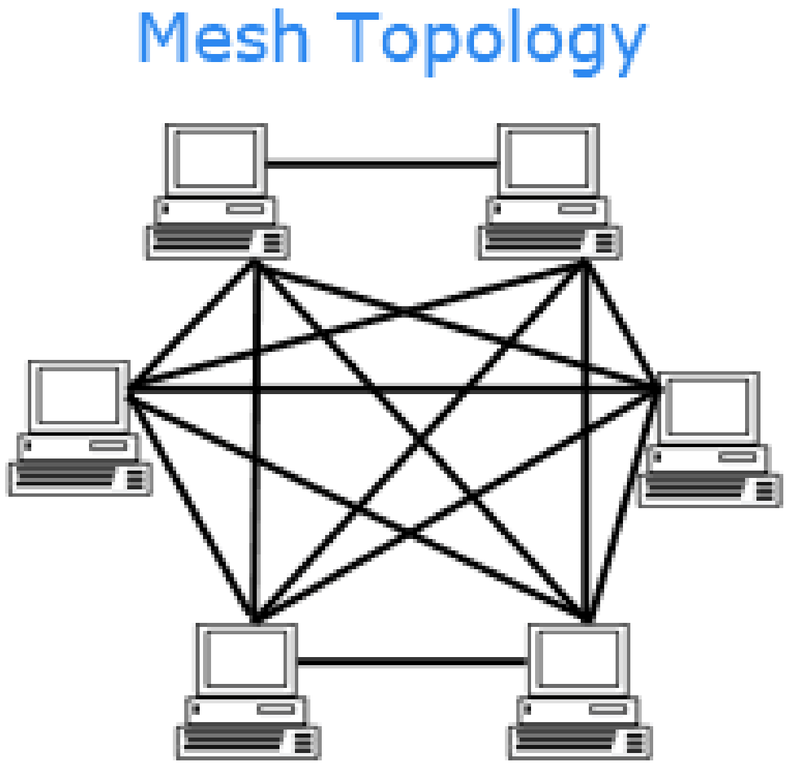
## Types of topologies:

1) Mesh Topology

2) Star Topology

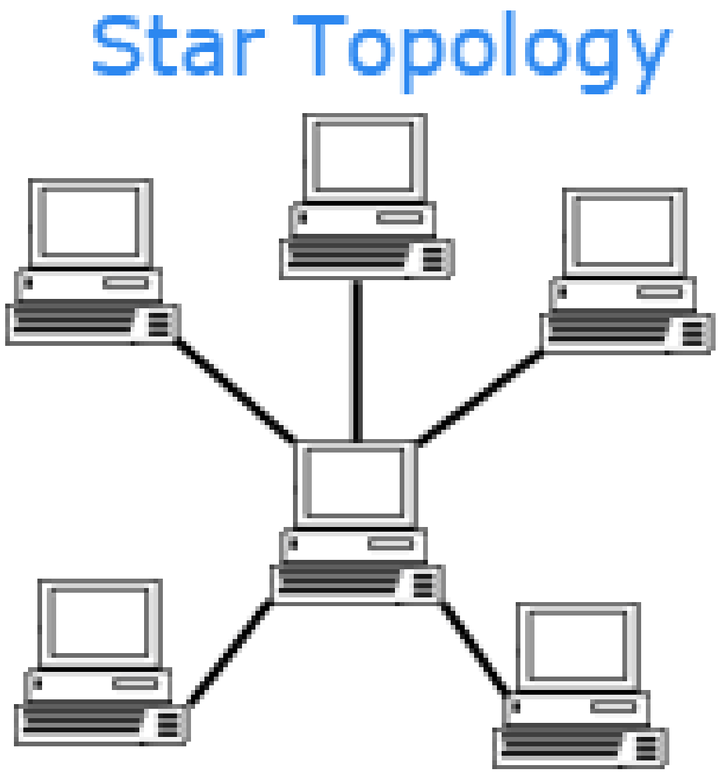
# Mesh topology:

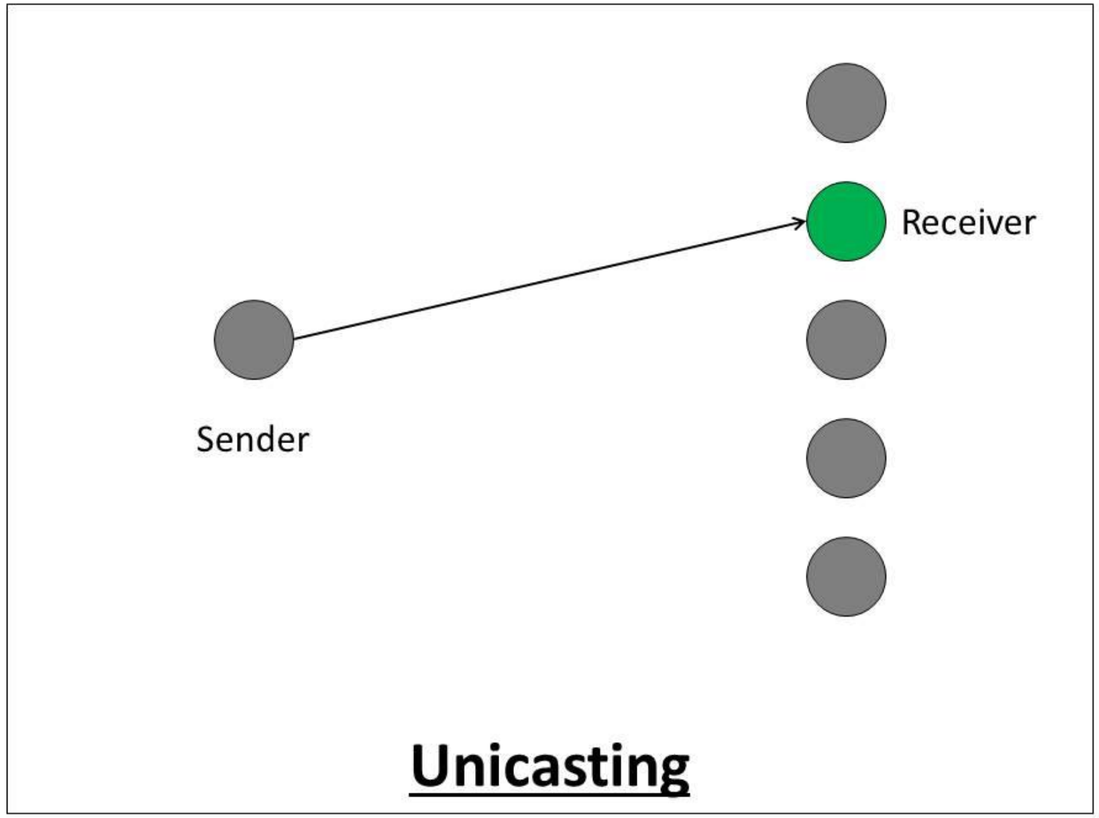
A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks.



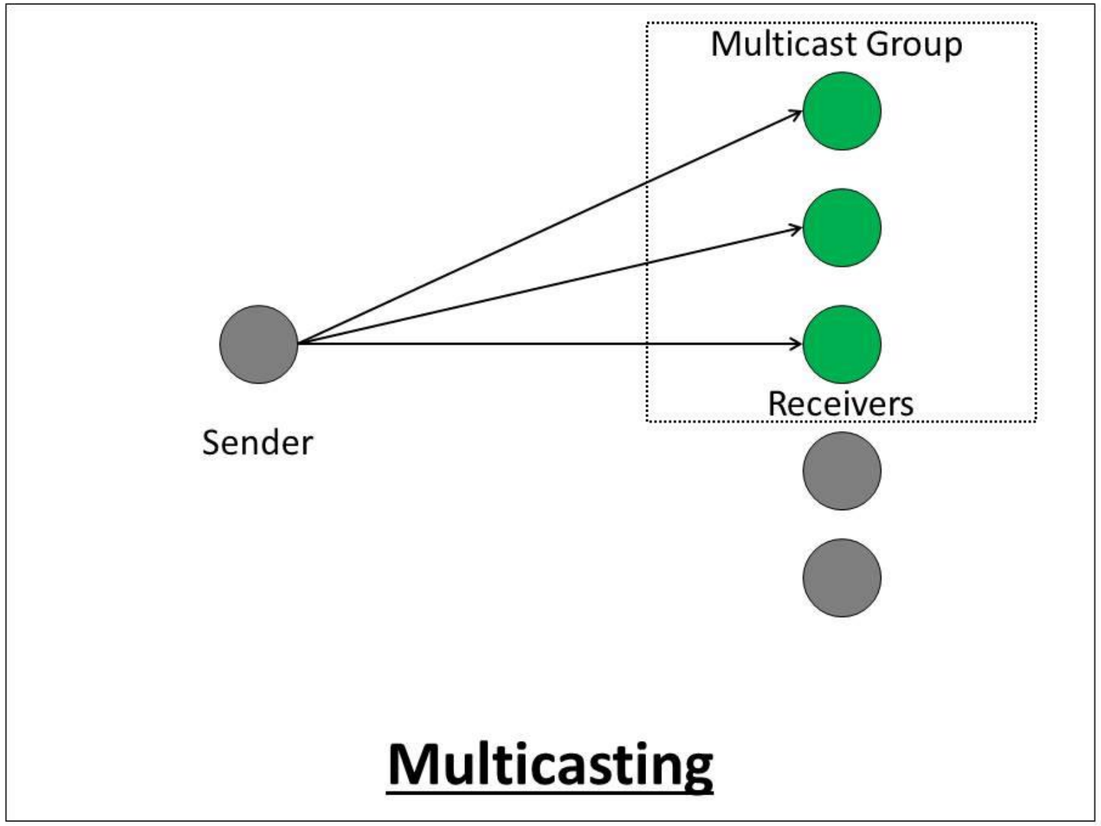
## Star topology:

Star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients.

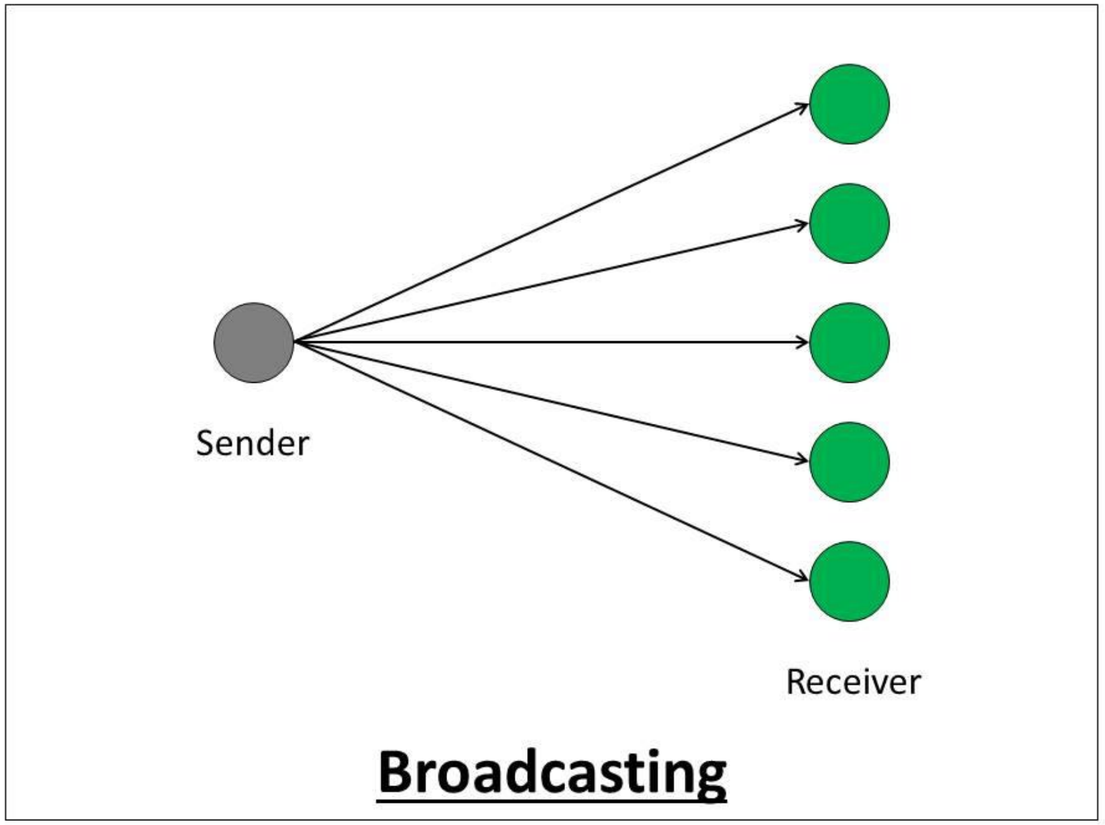


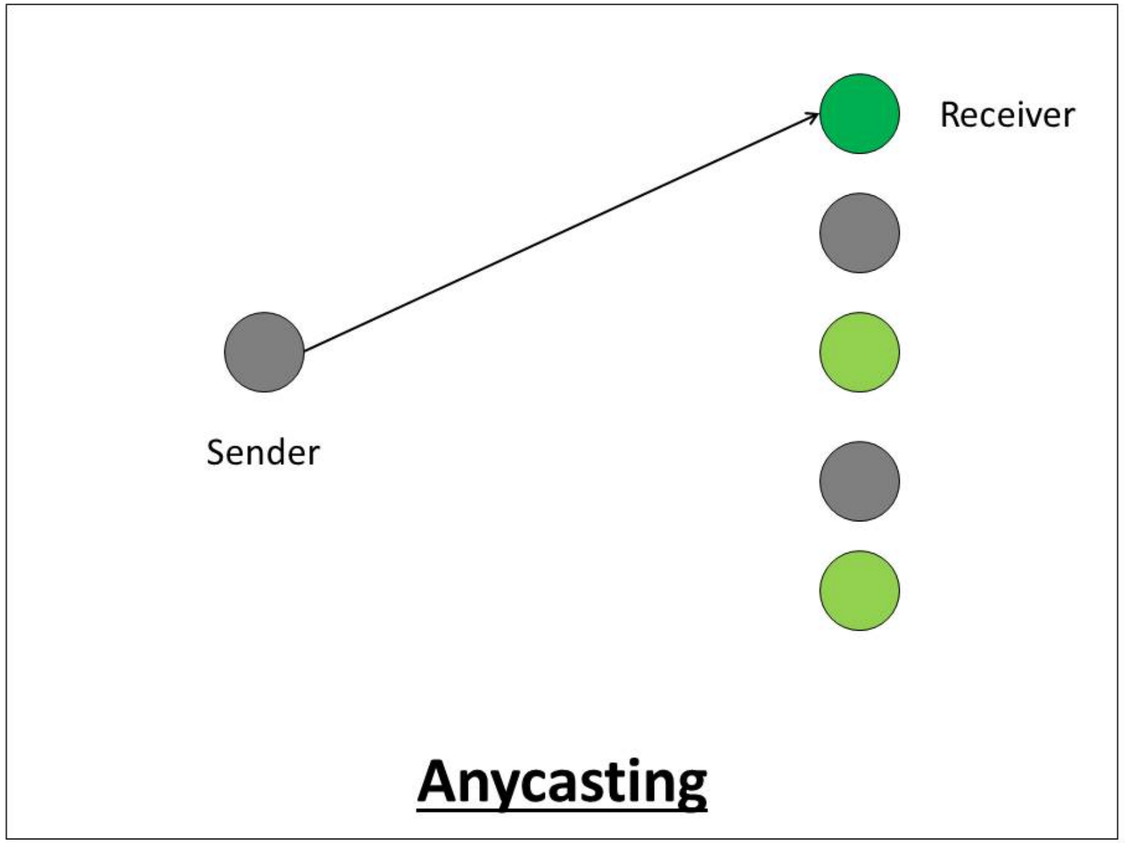


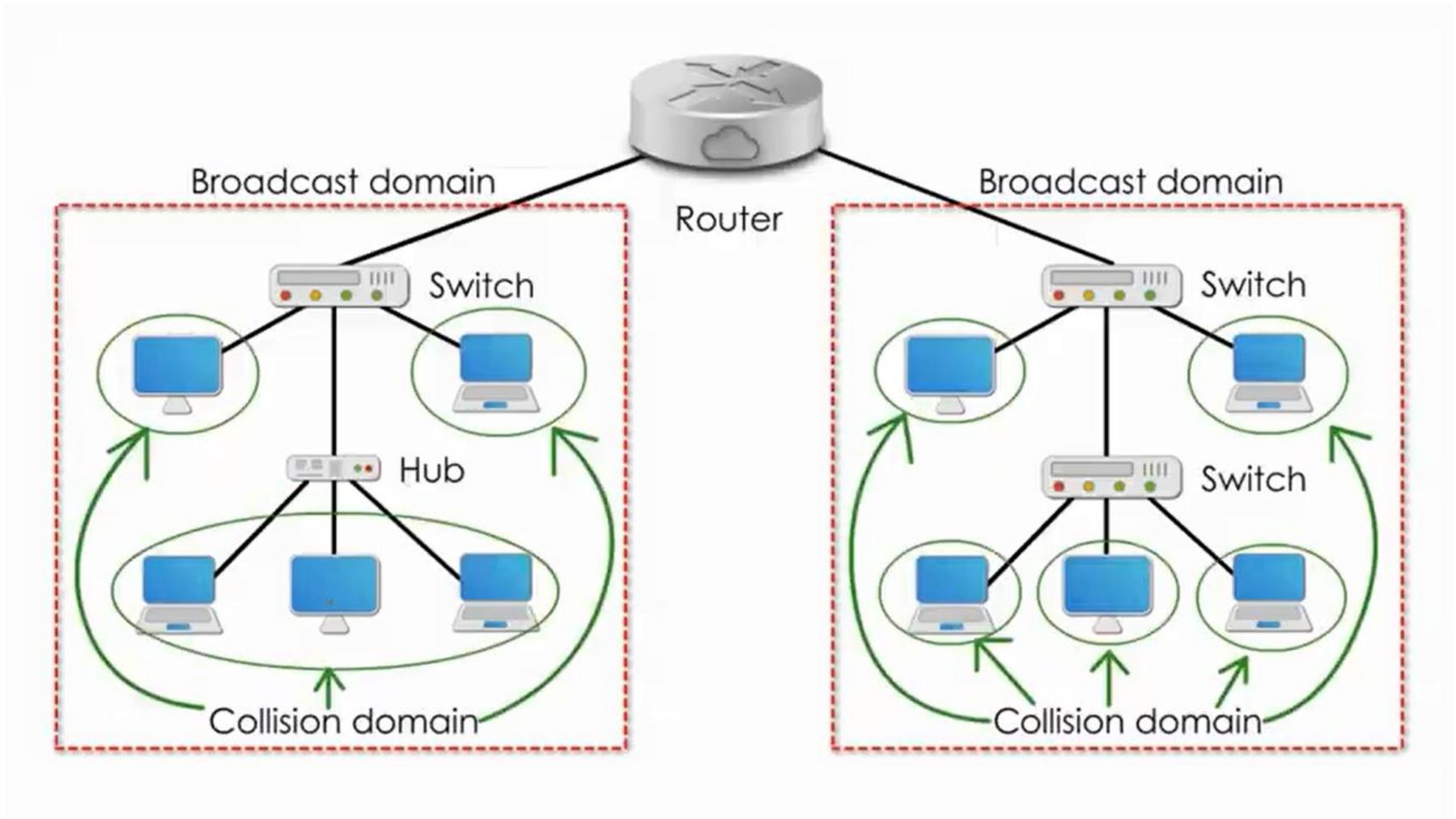

**Unicasting**



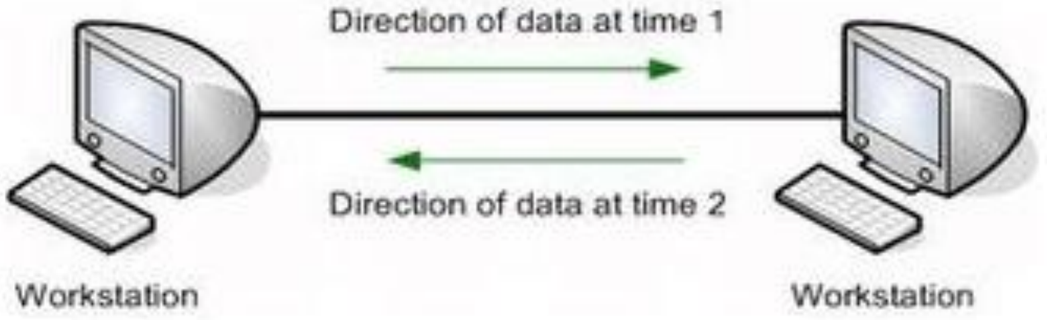

**Multicasting**


Sender
Receiver
Broadcasting

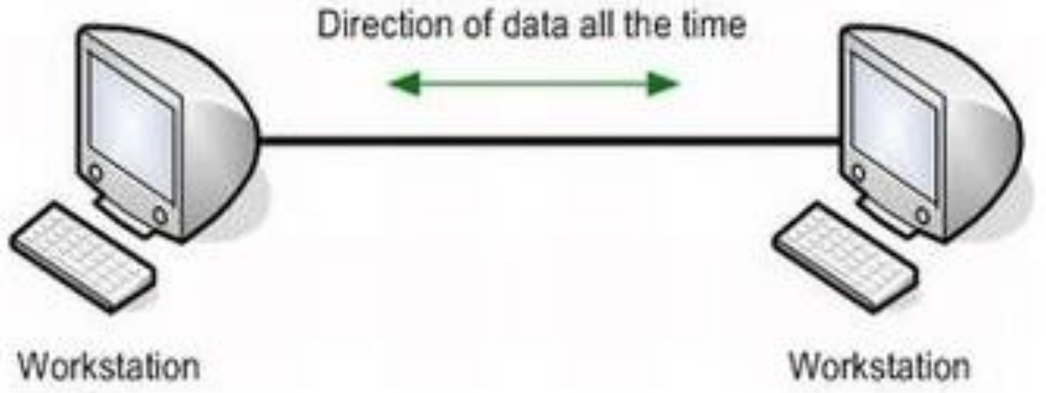

Receiver
Sender
Anycasting

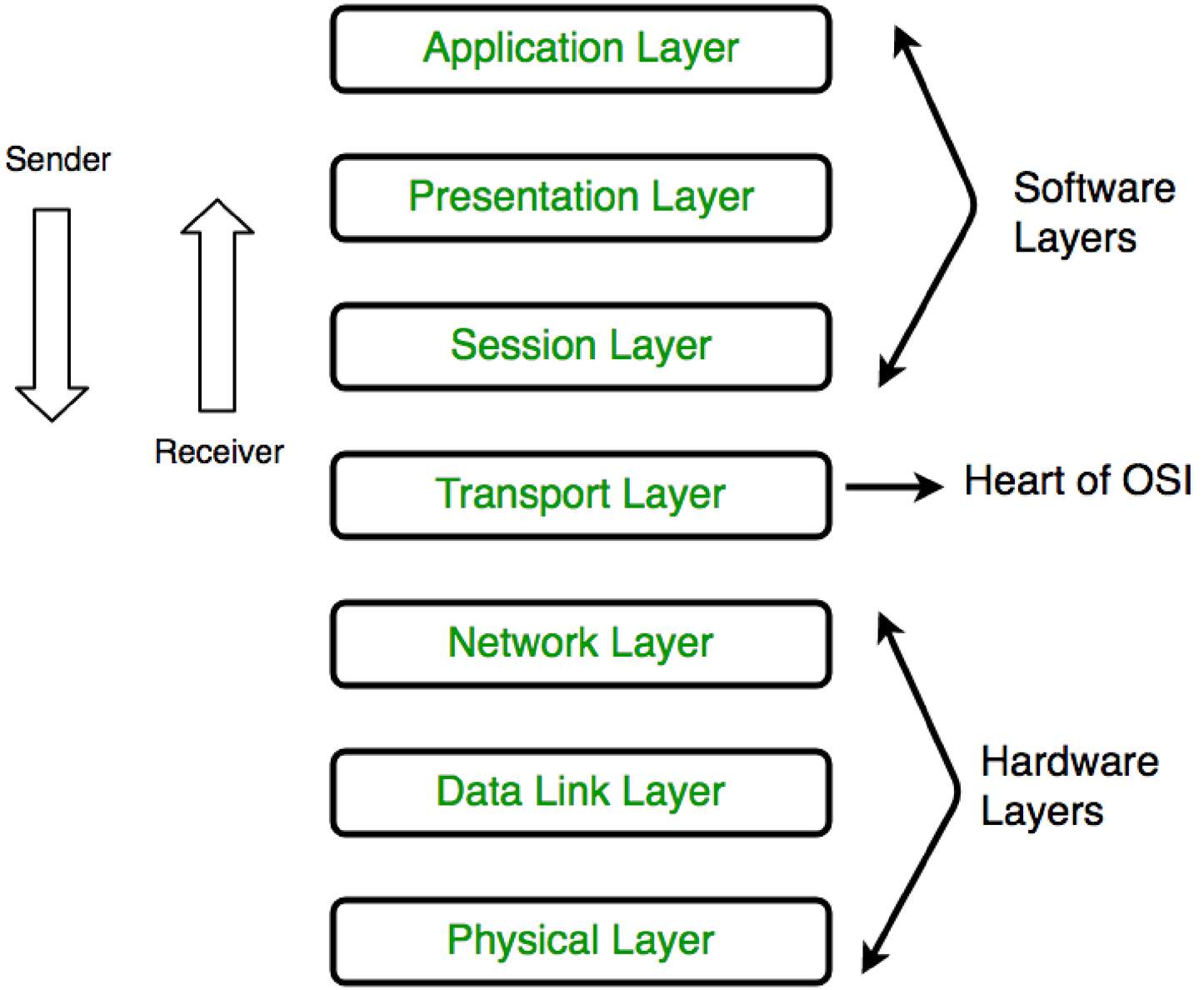

Broadcast domain
Router
Broadcast domain
Switch
Hub
Switch
Switch
Collision domain
Collision domain

## Half Duplex




## Full Duplex




Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Sender
Receiver
Software Layers
Heart of OSI
Hardware Layers

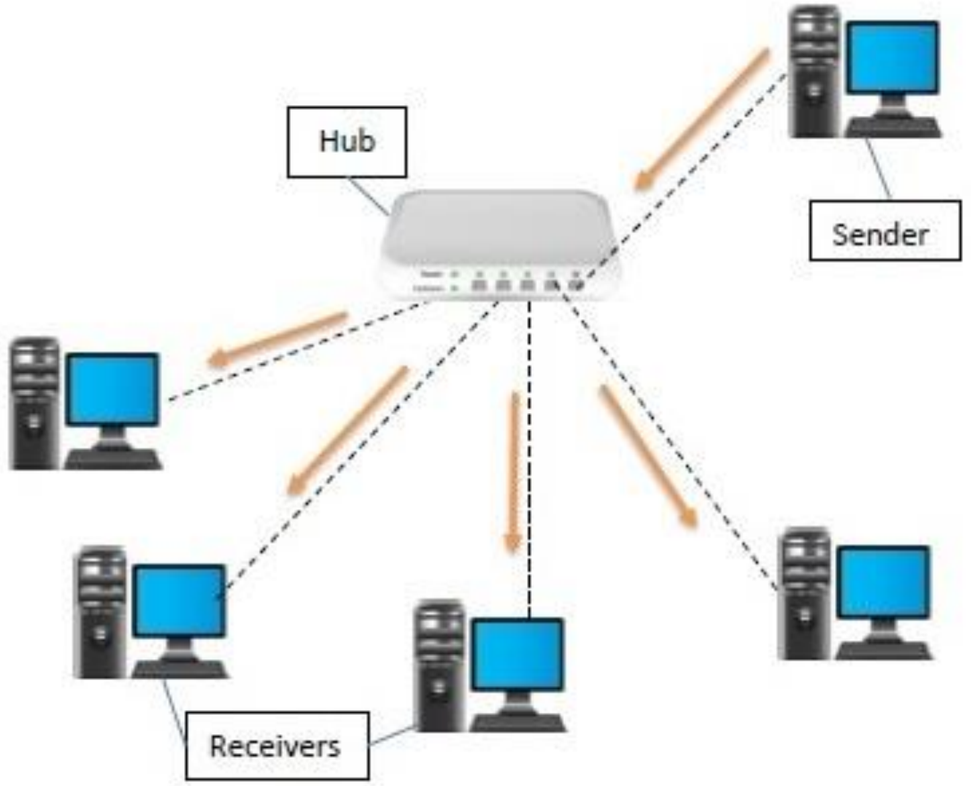
# Types of Addresses

1) IP Address/Logical address:
a) IPv4 - 32 bit
b) IPv6 - 128 bit

2) Mac address/Physical address- 48 bit

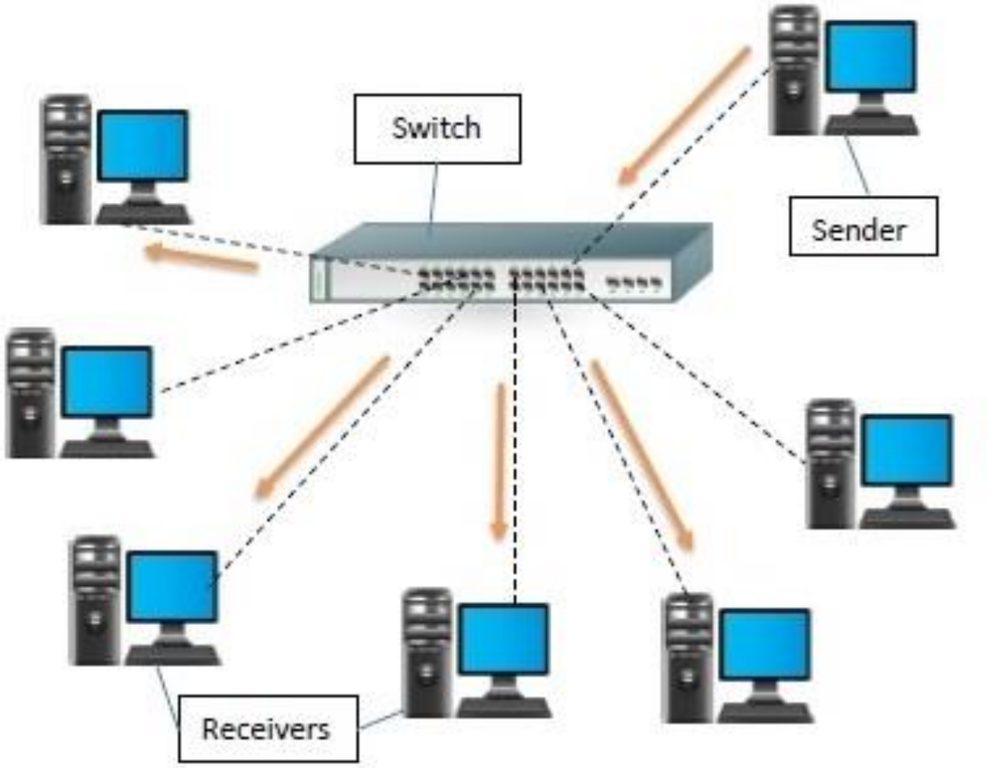
# HUB:-

1) It is a layer 1 device
2) It is a dumb device
3) It has single broadcast domain
4) It has single collision domain
5) Half duplex



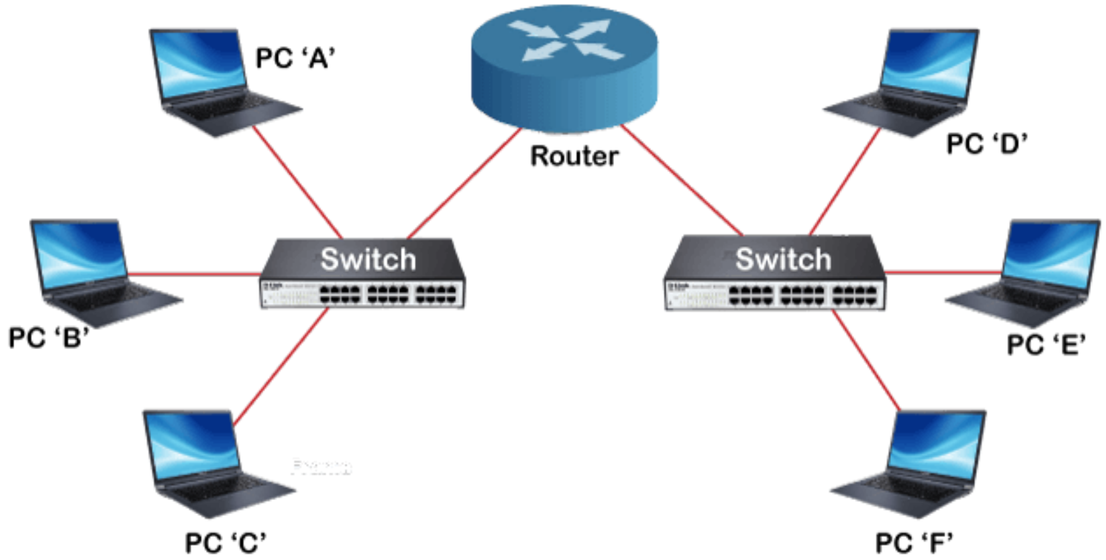
# SWITCH:-

1) It is a layer 2 device
2) It is an intelligent device
3) It has single broadcast domain
4) It has active port collision domain
5) Full duplex



# Router:-

1) It is a layer 3 device
2) It is an intelligent device
3) It has active port broadcast domain
4) It has active port collision domain
5) Full duplex




Connection of networks through Router

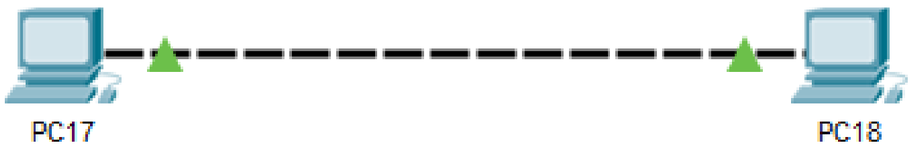
# Types of cables used for connecting network devices

**1) Straight-Through Cable:-**

Straight-through cables are needed to connect a switch port to a router or a host. It is used to connect different types of devices. This is your standard ethernet patch cable.

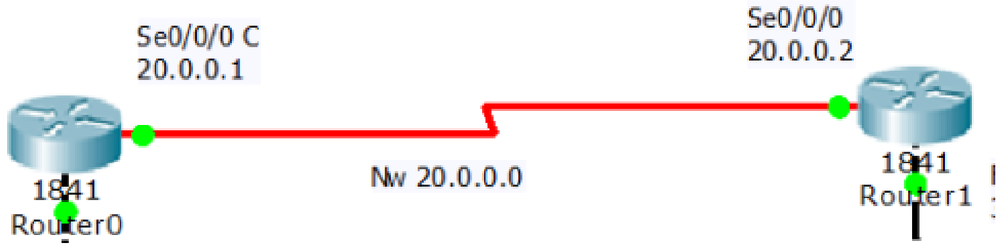

**2) Crossover Cable:-**

Crossover cables are used to connect similar types type of devices.



## Serial Cable (DCE/DTE):-

DTE/DCE cables are used to connect two routers via their serial interfaces.

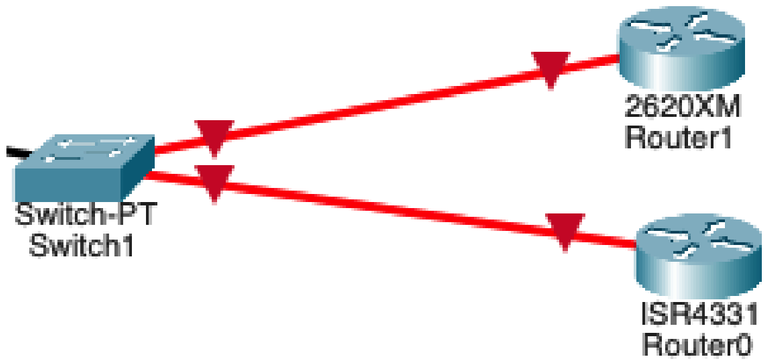



## Console Cable (rollover):-

Console cables (aka "rolled cables") allow you to connect a host device directly to a router or switch's console port. They are blue color cables.


## Fiber Cable:-

Fiber optic cables transmit large amounts of data at very high speeds. This technology is therefore widely used in internet cables. As compared to traditional copper wires, fiber optic cables are less bulky, lighter, more flexible, and carry more data.



# IP Addresses and Subnetting

# Types of Addresses

1) IP Address/Logical address:
a) IPv4 - 32 bit (Dot-decimal notation)
example: 192.168.10.1
b) IPv6 - 128 bit (Hexadecimal format)
example: 2402:3a80:d0b:32ab:8929:45f3:4a3d:650c

2) Mac address/Physical address- 48 bit (Hexadecimal format)
example: 5C-5F-67-95-CF-EF

# IPv4 Address

1) An IP address is a unique address that identifies a device on the internet or a local network.
2) IP stands for "Internet Protocol"
3) An IP address is a string of numbers separated by dot.
4) It is 32 bit in size.
5) It has four octets and each octet is 8 bit
6) Each number in the set can range from 0 to 255
7) The full IP addressing range goes from 0.0.0.0 to 255.255.255.255
8) Total 2^32 IP addresses are there in IPv4
9) Decimal format : 192.168.10.1
10) Binary format: 11000000.10101000.00001010.00000001

# Decimal to Binary conversion

| Division | Quotient | Reminder |
|---|---|---|
| 172/2 | 86 | 0 |
| 86/2 | 43 | 0 |
| 43/2 | 21 | 1 |
| 21/2 | 10 | 1 |
| 10/2 | 5 | 0 |
| 5/2 | 2 | 1 |
| 2/2 | 1 | 0 |
| ½ | 0 | 1 |

# Binary to decimal conversion

| Base | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
|---|---|---|---|---|---|---|---|---|
| Weight | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Example | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

# Classes in IPv4 address

## IPv4 address are divided into 5 Classes:-

1.Class A: 1.0.0.0 to 126.255.255.255
2.Class B: 128.0.0.0 to 191.255.255.255
3.Class C: 192.0.0.0 to 223.255.255.255
4.Class D: 224.0.0.0 to 239.255.255.255
5.Class E: 240.0.0.0 to 255.255.255.255

- 0.0.0.0 is not used anywhere
- 127.0.0.0 is a loopback address
- Class A,B,C are used for assignment  purpose
- Class D is used for Multicast group
- Class E is used for research purpose

# First octet range

1.Class A: 1 to 126 : 00000001 to 01111111

2.Class B: 128 to 191 : 10000000 to 10111111

3.Class C: 192 to 223 : 11000000 to 11011111

4.Class D: 224 to 239 : 11100000 to 11101111

5.Class E: 240 to 255 : 11110000 to 11111111

# Subnetting

Subnetting means dividing  the network to economically assign the IP address to devices.

There are two types of Subnetting:-

Classful Subnetting: Using default subnet mask
Classless Subnetting: Using custom subnet mask

**Network Bit:**
Represents the network to which a machine belong

**Host Bit:**
Represents IP address of that particular machine

**Subnet mask:**
•A value which helps to identify network portion and host portion of an IP address
•In binary format, it consists of continuous 1s and then continuous 0s
•Network bits are represented by 1s
•Host bits are represented by 0s

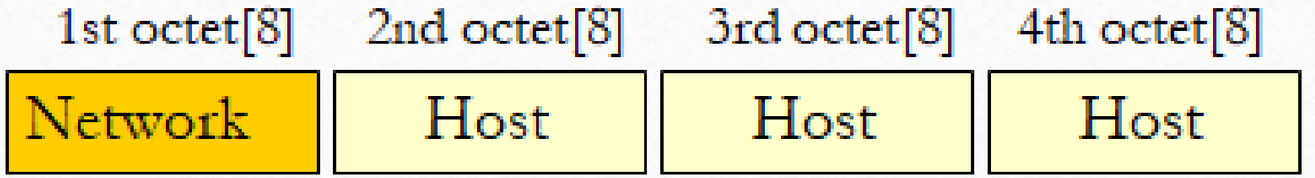
# Default Subnet Mask

## 1 = Network & 0 = Host

| | 1st octet[8] | 2nd octet[8] | 3rd octet[8] | 4th octet[8] |
|---|---|---|---|---|
| CLASS A | Network | Host | Host | Host |
| Subnet Mask | 11111111 . | 00000000 . | 00000000 . | 00000000 |
| Default SM | 255 . | 0 . | 0 . | 0 |
| CLASS B | Network | Network | Host | Host |
| Subnet Mask | 11111111 . | 11111111 . | 00000000 . | 00000000 |
| Default SM | 255 . | 255 . | 0 . | 0 |
| CLASS C | Network | Network | Network | Host |
| Subnet Mask | 11111111 . | 11111111 . | 11111111 . | 00000000 |
| Default SM | 255 . | 255 . | 255 . | 0 |

# Class A IP Addressing

- CLASS A




Network Bits - 8

Host Bits - 24

# Class A IP Addressing

No. of Networks = Available Bits - 8

= But First bit is fix i.e. 0

= Bits for Manipulating = 8-1 = 7

= $2^{7}$ = 128

= But Network 0 & 127 are Reserved

= 128-2= 126 [ 1 through 126 ]

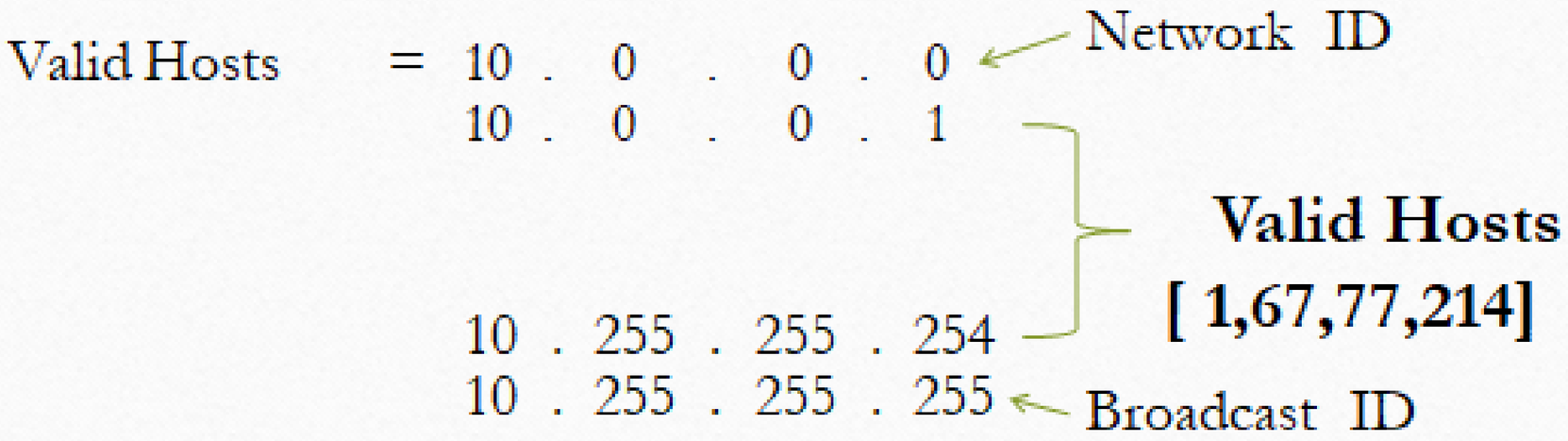
No. of Hosts per Network = Available Bits - 24

= $2^{24}$ = 1,67,77,216

= But Host Address of all 1's & 0's are Reserved

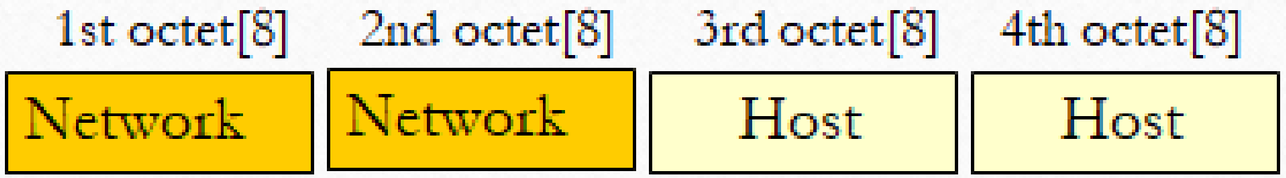
= 1,67,77216-2 = 1,67,77,214

# Class A IP Addressing



# Class B IP Addressing

- CLASS B




Network Bits - 16

Host Bits - 16

# Class B IP Addressing

No. of Networks = Available Bits - 16

= But First bit Two(2) bits are fix i.e. 10

= Bits for Manipulating = 16-2 = 14

= $2^{14}$ = 16384 [ 128.0 through 191.255 ]

No. of Hosts per Network = Available Bits - 16

= $2^{16}$ = 65,536

= But Host Address of all 1's & 0's are Reserved

= 65,536 -2 = 65,534

# Class B IP Addressing

Valid Hosts = 172 . 16 . 0 . 0 ← Network ID

172 . 16 . 0 . 1

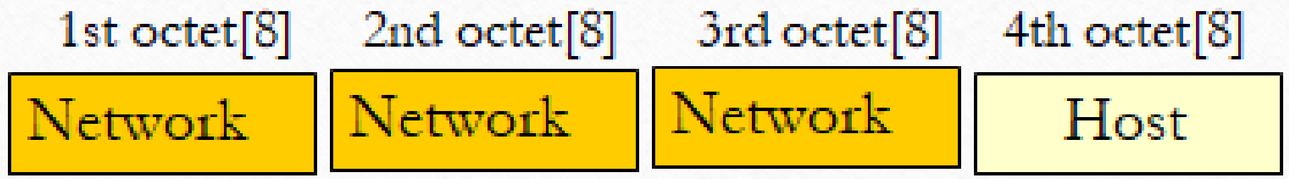
172 . 16 . 255 . 254

**Valid Hosts**
**[ 65,534 ]**

172 . 16 . 255 . 255 ← Broadcast ID

# Class C IP Addressing

- CLASS C




Network Bits - 24

Host Bits - 8

# Class C IP Addressing

No. of Networks = Available Bits - 24

= But First bit Three(3) bits are fix i.e. 110

= Bits for Manipulating = 24-3 = 21

$= 2^{21} = 20,97,152$

[ 192.0.0.0 through 223.255.255.255 ]

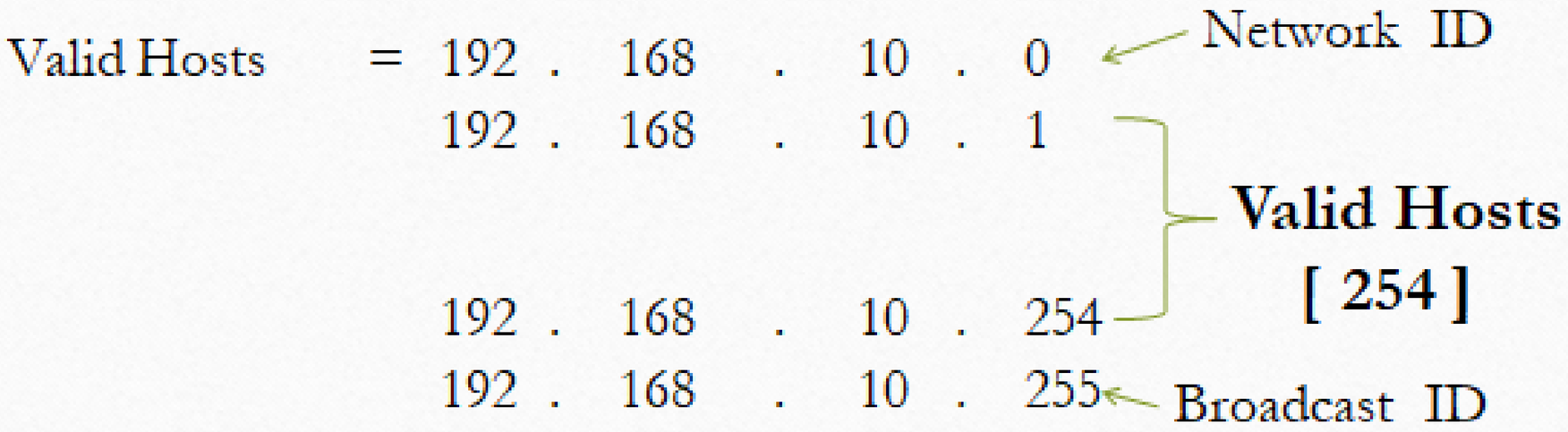
No. of Hosts per Network = Available Bits - 8

$= 2^{8} = 256$

= But Host Address of all 1's & 0's are Reserved

= 256 -2 = 254

# Class C IP Addressing



**Class A:-**

- N.H.H.H (11111111.00000000.00000000.00000000)
- Subnet Mask: 255.0.0.0
- Slash value: /8
- Network bits: 8
- Host bits: 24
- Number of Networks: 126 (2^7-2)
- Number of Hosts per Network: 16,777,214 (2^24-2)

**Class B:-**

- N.N.H.H (11111111.11111111.00000000.00000000)
- Subnet Mask: 255.255.0.0
- Slash value: /16
- Network bits: 16
- Host bits: 16
- Number of Networks: 16,382 (2^14)
- Number of Hosts per Network: 65,534 (2^16-2)

**Class C:-**

- N.N.N.H (11111111.11111111.11111111.00000000)
- Subnet Mask: 255.255.255.0
- Slash value: /24
- Network Bits: 24
- Host Bits: 8
- Number of Networks: 2,097,150 (2^21)
- Number of Hosts per Network: 254 (2^8-2)

**Range of Subnet mask:-**

- Class A: /8 to /15
- Class B: /16 to /23
- Class C: /24 to /30

# Private and Public IP Address

Public IP address are costly and they need to be purchased by ISP

Private IP range:
Class A: 10.0.0.0 to 10.255.255.255
Class B: 172.16.0.0 to 172.31.255.255
Class C: 192.168.0.0 to 192.168.255.255

# FLSM, VLSM and OSI Model

# FLSM

## FLSM - Fixed length subnet masking

| Team | No. of PCs | Subnet Mask | Wastage |
|---|---|---|---|
| 1) IT | 120 | /25 | 8 |
| 2) HR | 60 | /25 | 68 |
| 3) Sales | 28 | /25 | 100 |

Network: 10.0.0.0 /25
Subnet mask: 255.255.255.128
Same Subnet mask for all the teams

# VLSM

VLSM - Variable length subnet masking

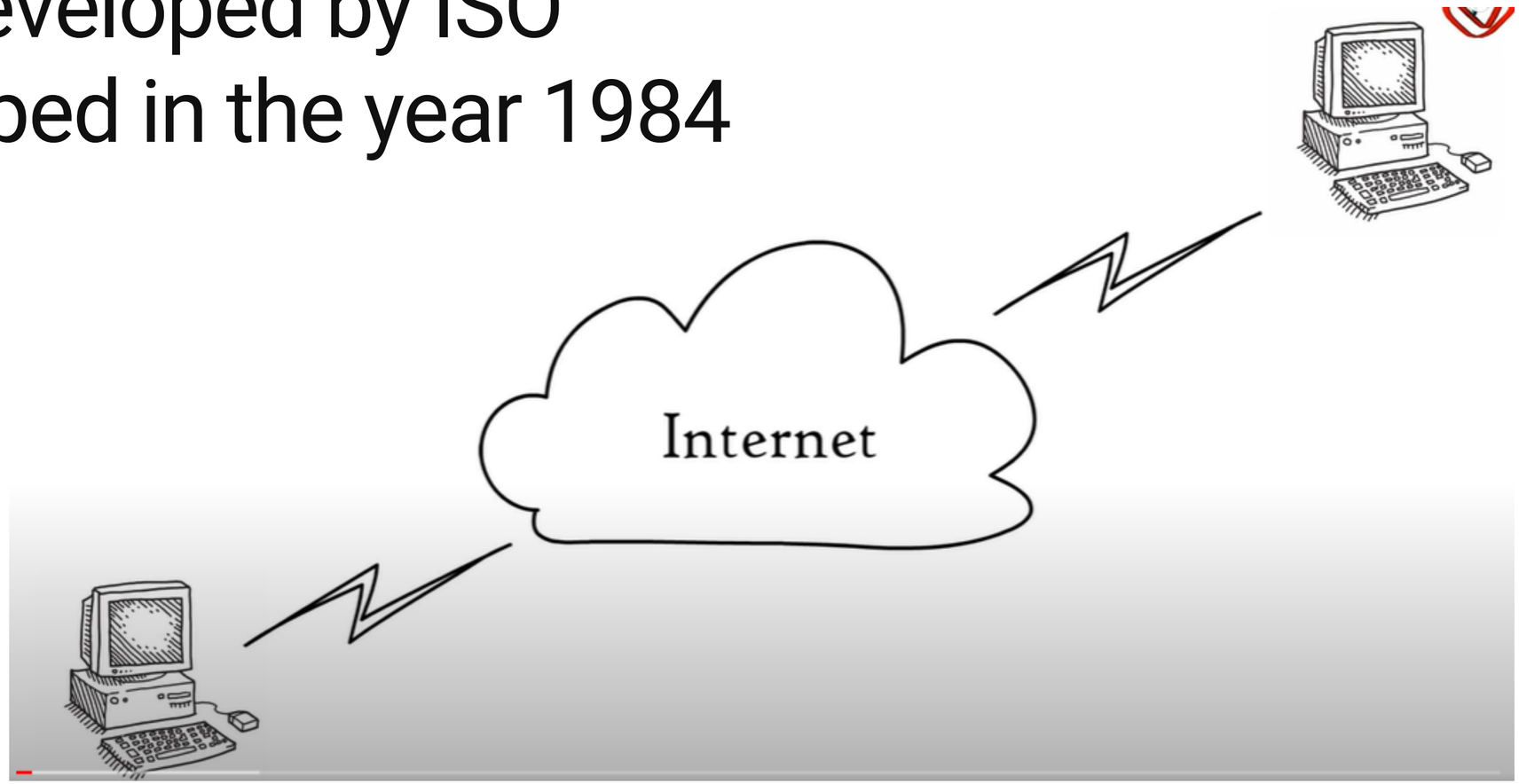
| Team | No. of PCs | Subnet Mask | Wastage |
|---|---|---|---|
| 1) IT | 120 | /25 | 8 |
| 2) HR | 60 | /26 | 4 |
| 3) Sales | 28 | /27 | 4 |

Network used: 10.0.0.0
Subnet mask for IT: 255.255.255.128 (/25)
Subnet mask for HR: 255.255.255.192 (/26)
Subnet mask for Sales: 255.255.255.224 (/27)

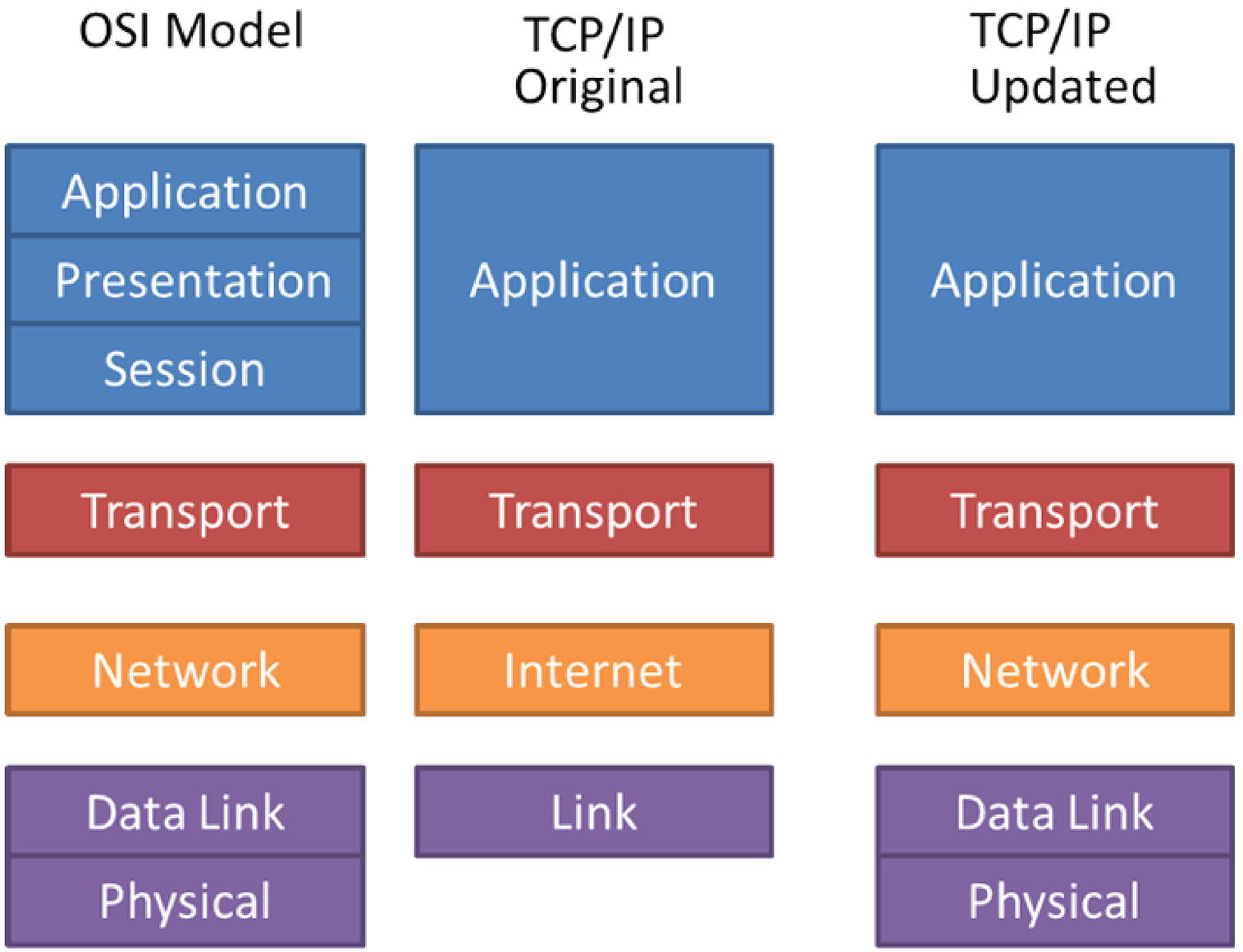
# OSI MODEL

# What is OSI Model and why do we need it ?

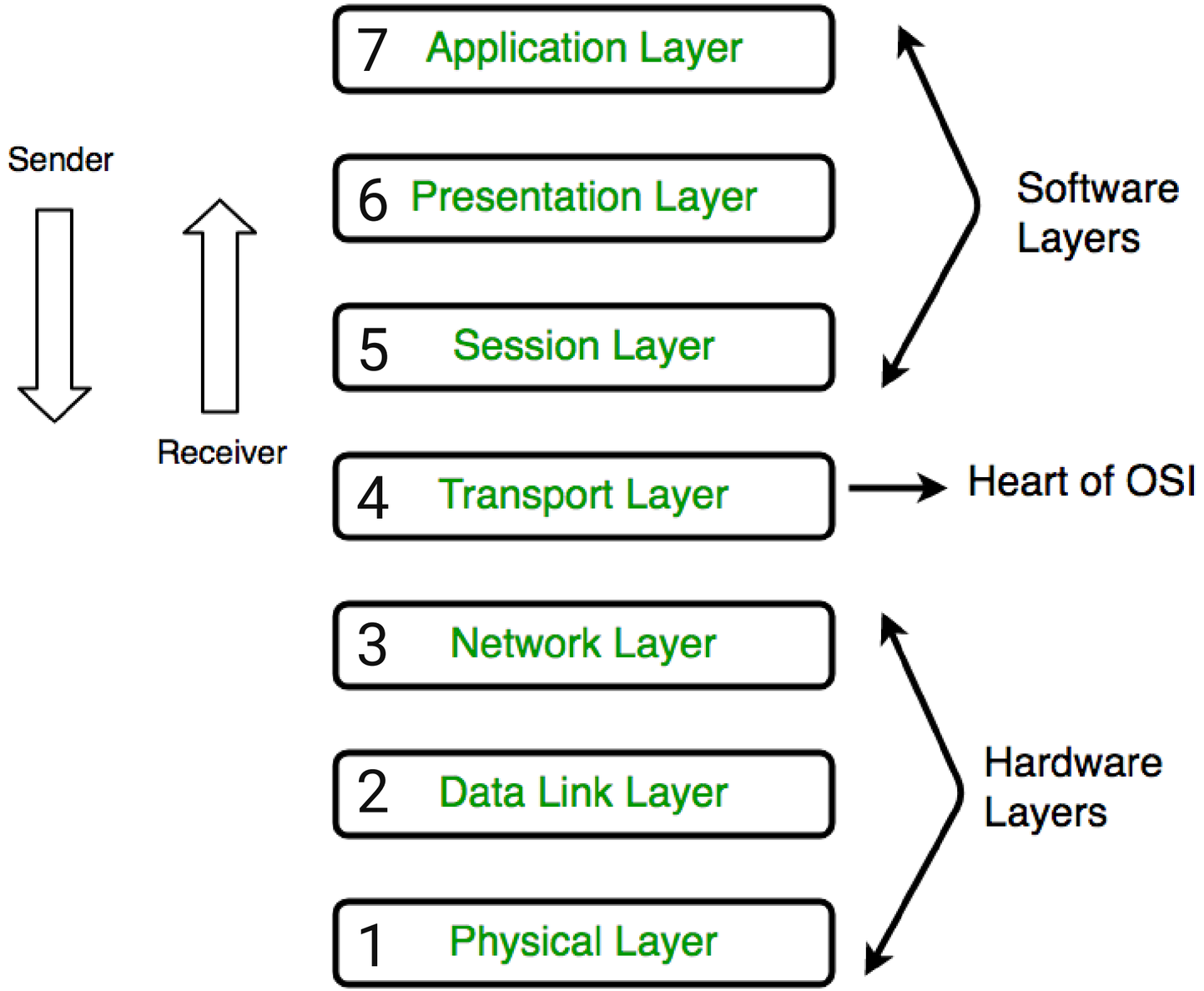
- Open Systems Interconnection
- It has been developed by ISO
- It was developed in the year 1984



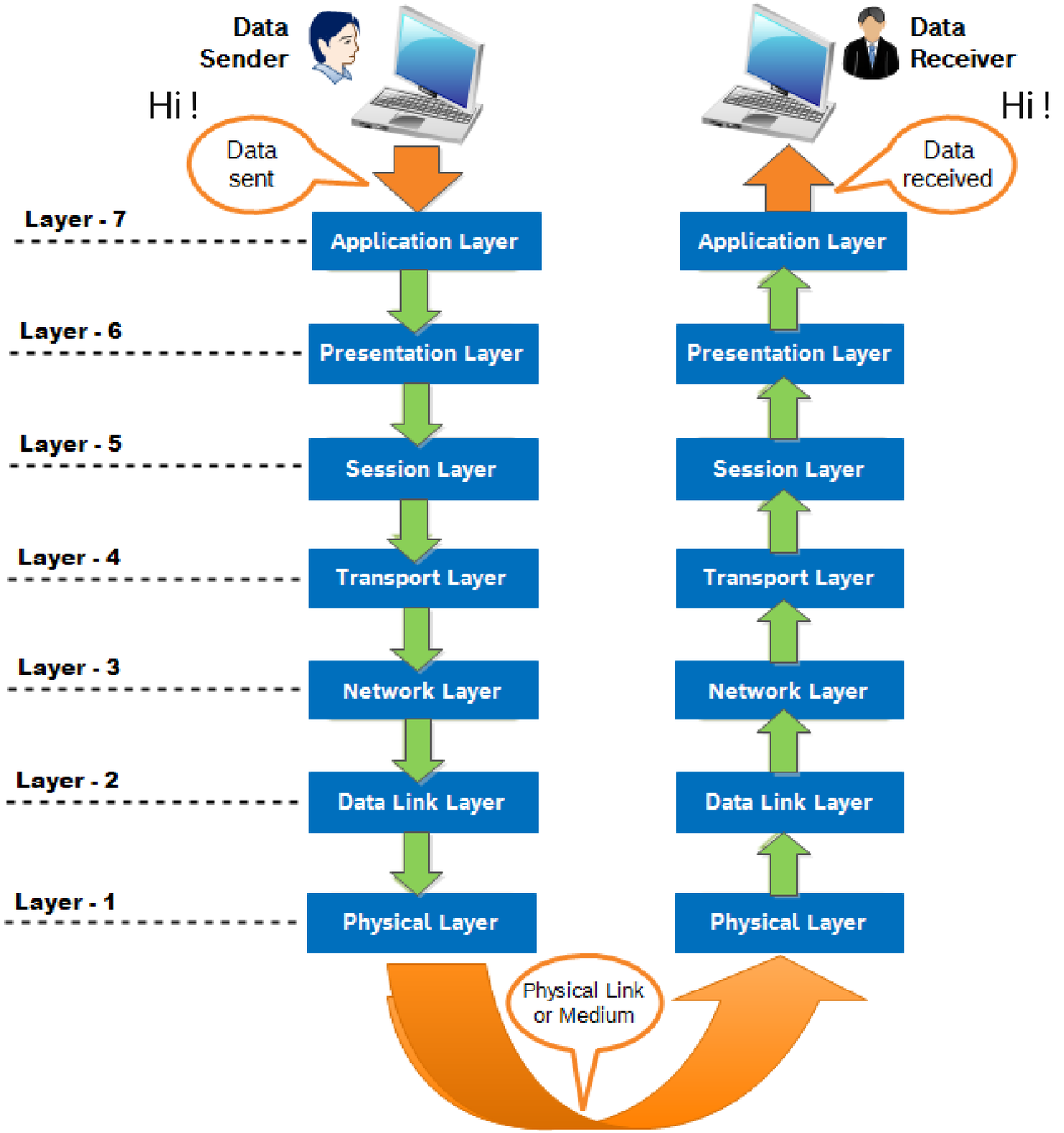
ISO developed OSI model in 1984.




ARPANET developed TCP/IP model


Sender
Receiver
7 Application Layer
6 Presentation Layer
5 Session Layer
4 Transport Layer
3 Network Layer
2 Data Link Layer
1 Physical Layer
Software Layers
Heart of OSI
Hardware Layers

# How data travels from sender to receiver ?

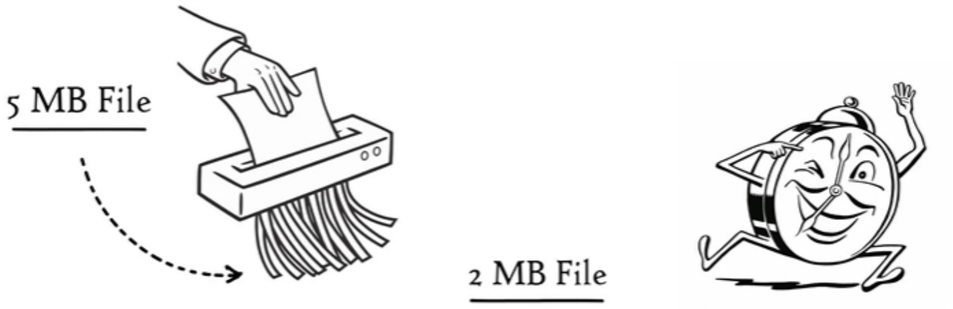


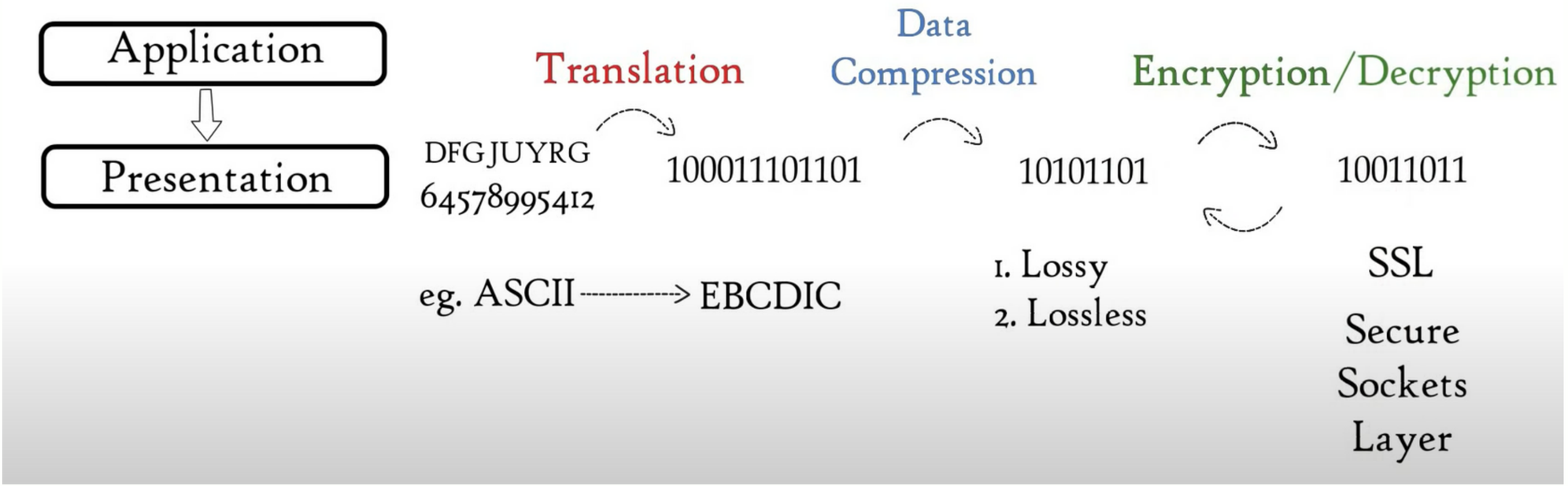
# 7.Application layer:

- This layer is 7th layer in OSI model and is user interface layer
- Network applications (Chrome, Firefox) use application layer to use the different protocol service
- Application layer protocols
    - FTP - used for file transfer
    - HTTP/HTTPS - used for browsing
    - SMTP - used for email service
    - Telnet/SSH - used for virtual access

# 6.Presentation layer:

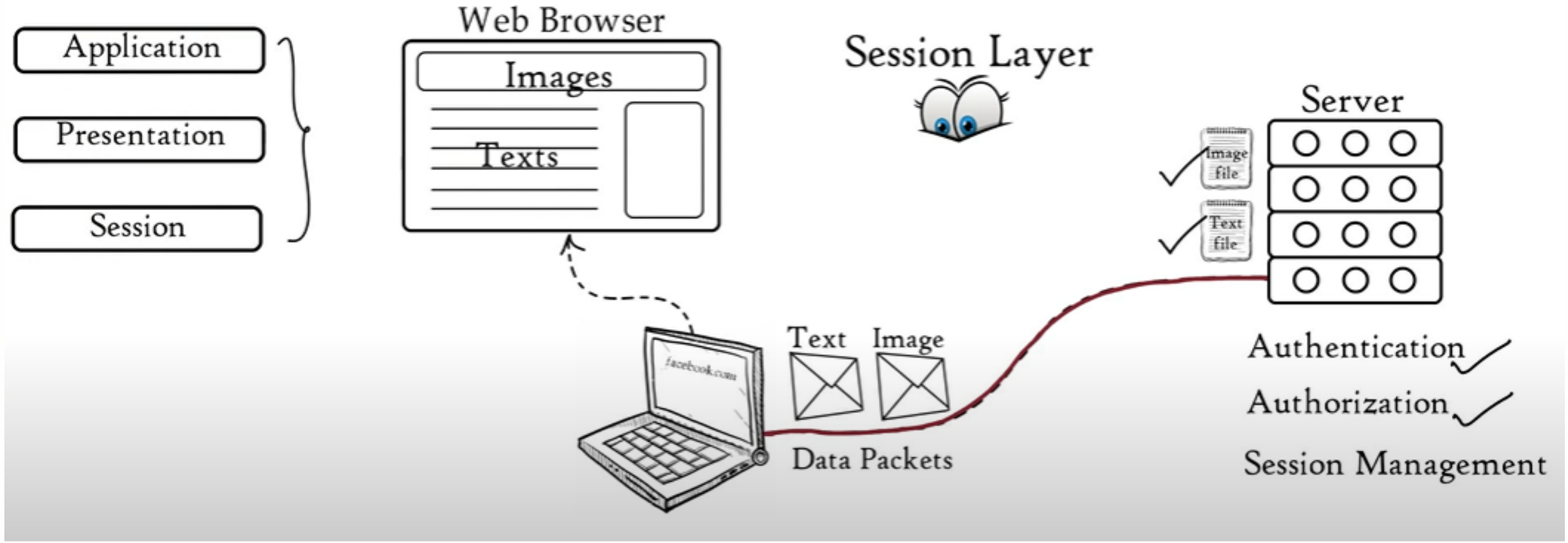
- Translation
- Compression
- Encryption/Decryption



# 5.Session layer:

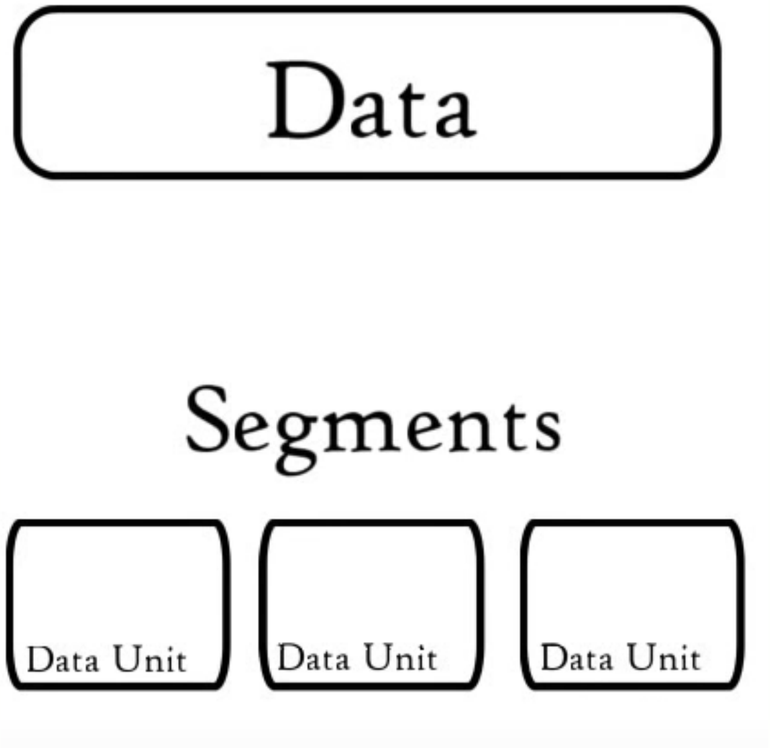
- Session establishment, maintenance and termination
- Authentication
- Authorization

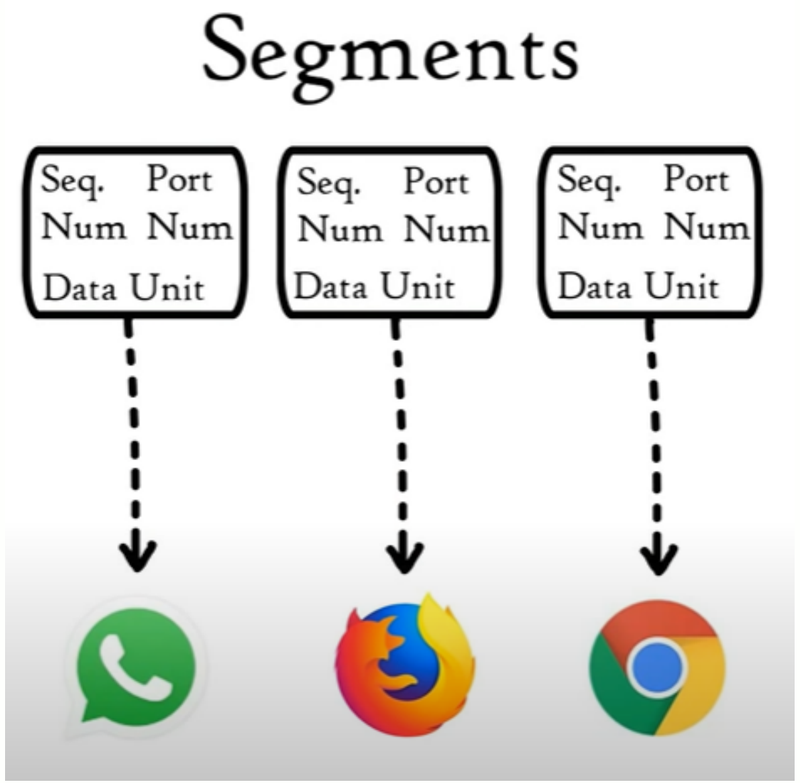


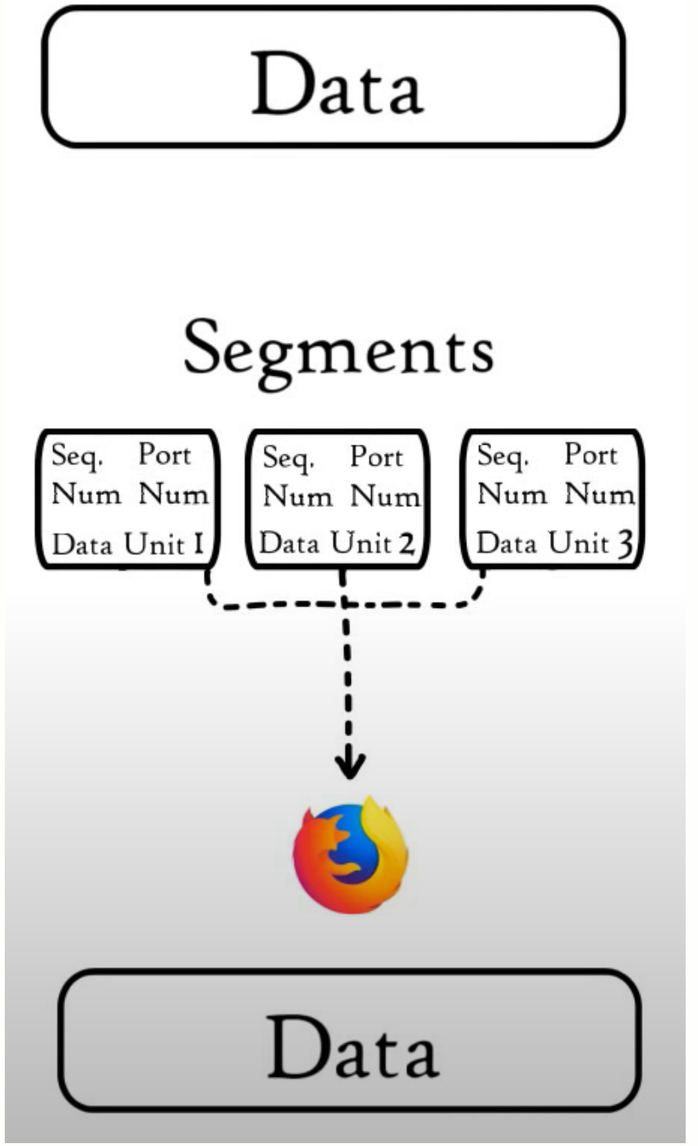
# 4.Transport layer:

- Segmentation
- Flow Control
- Error Control
- Connection and connectionless Transmission

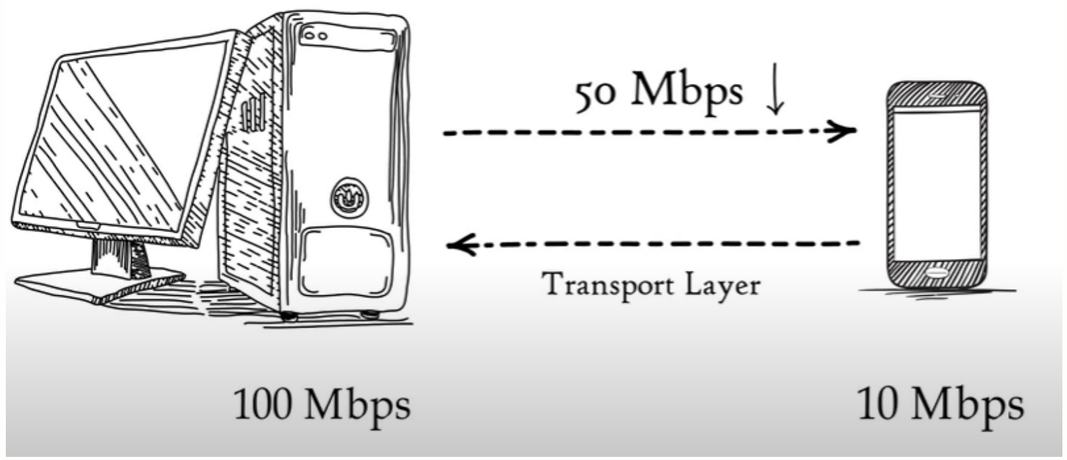
# Segmentation:

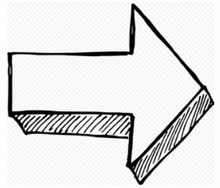


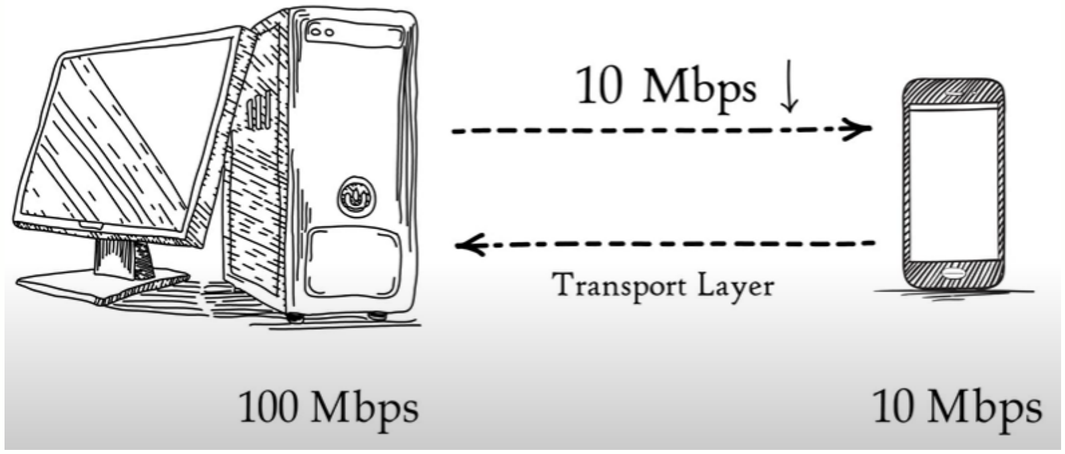



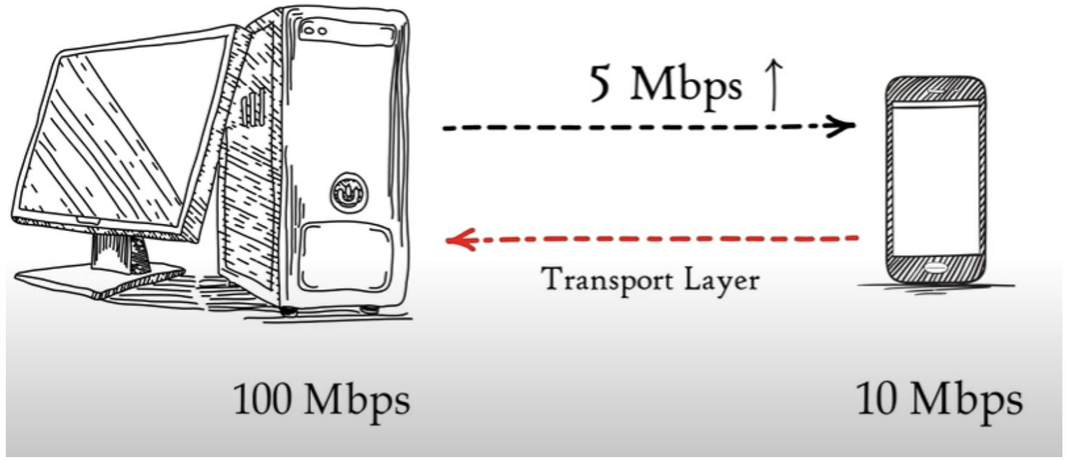



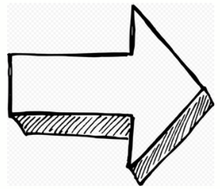
# Flow Control:

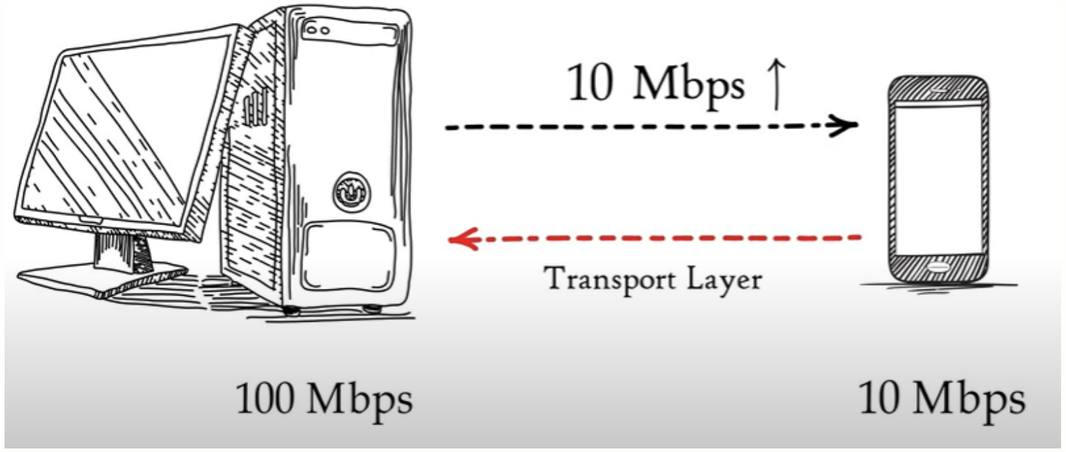


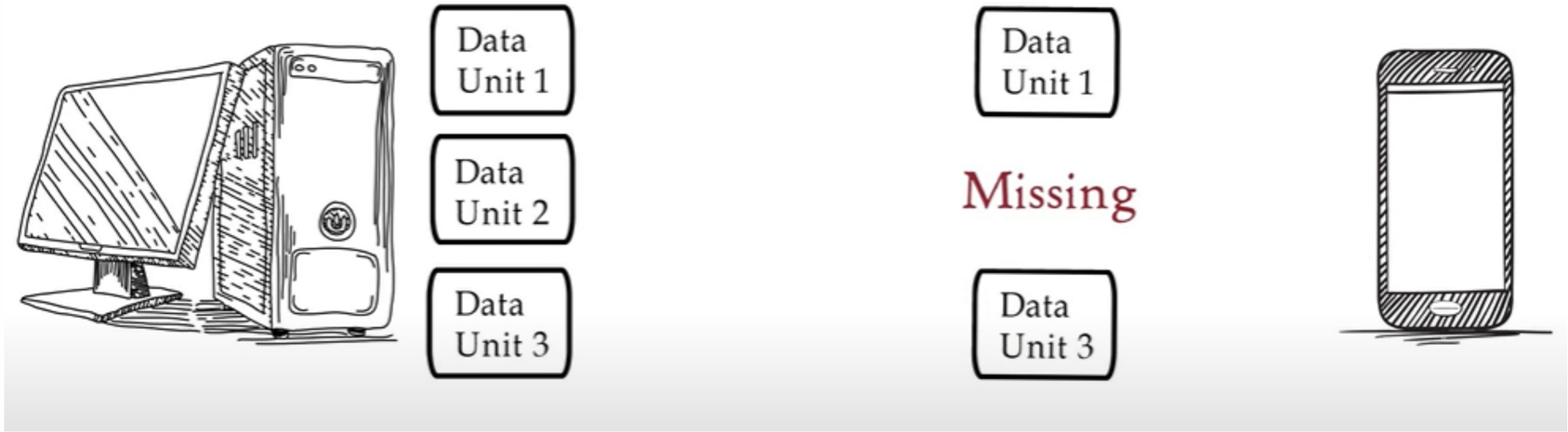


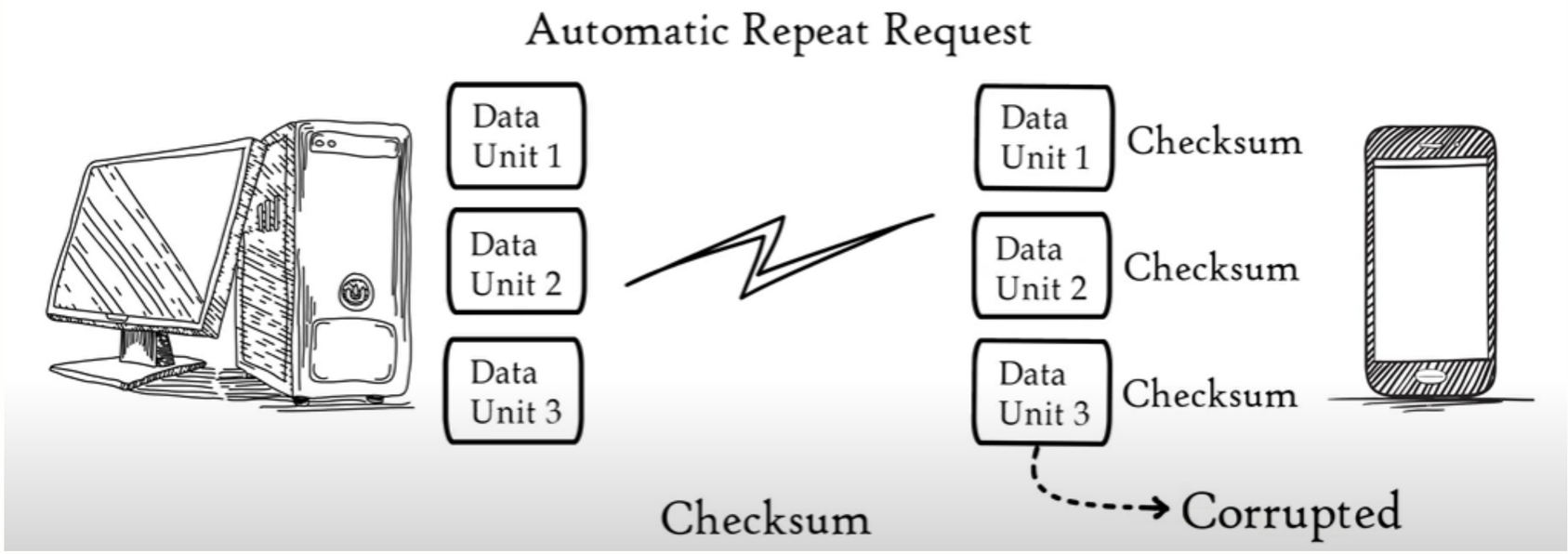





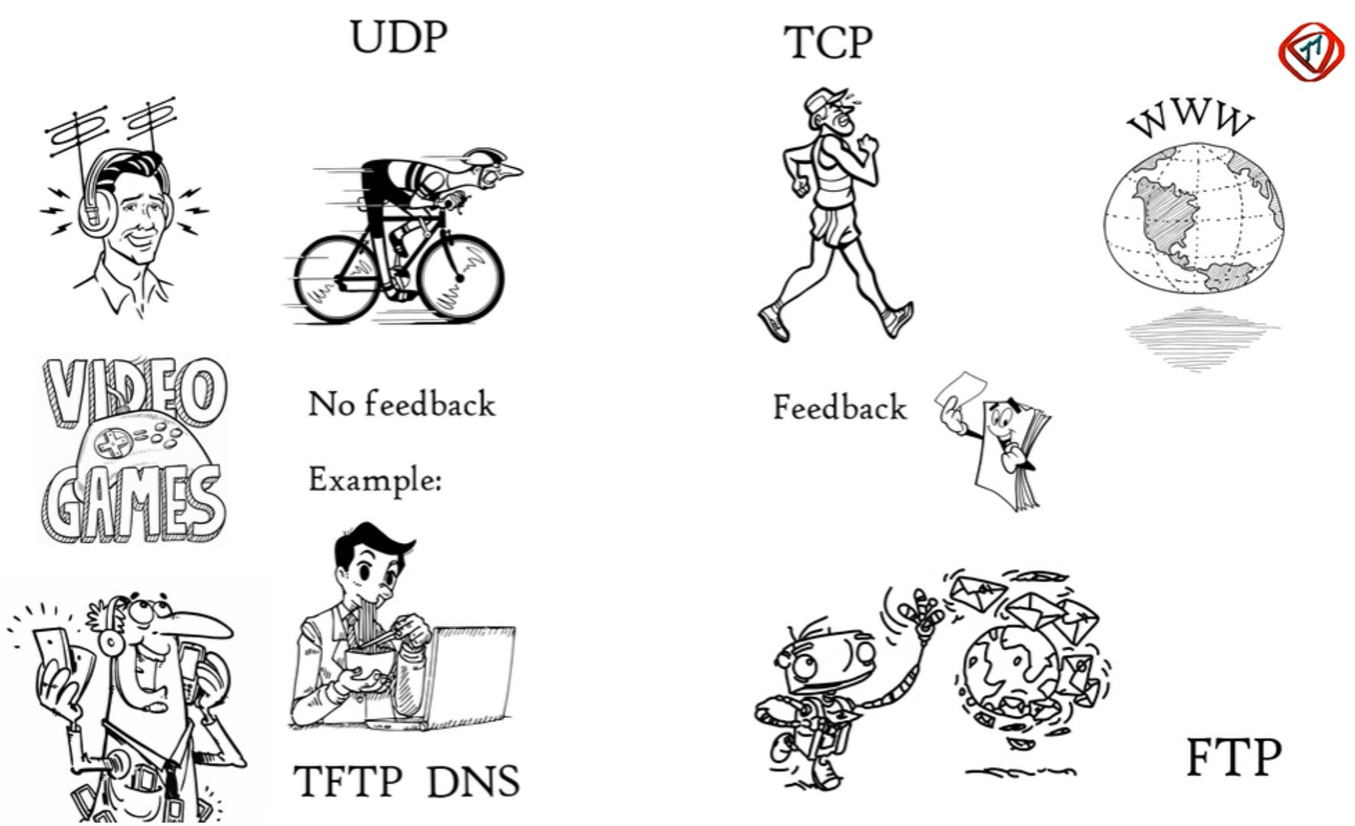
# Error control:



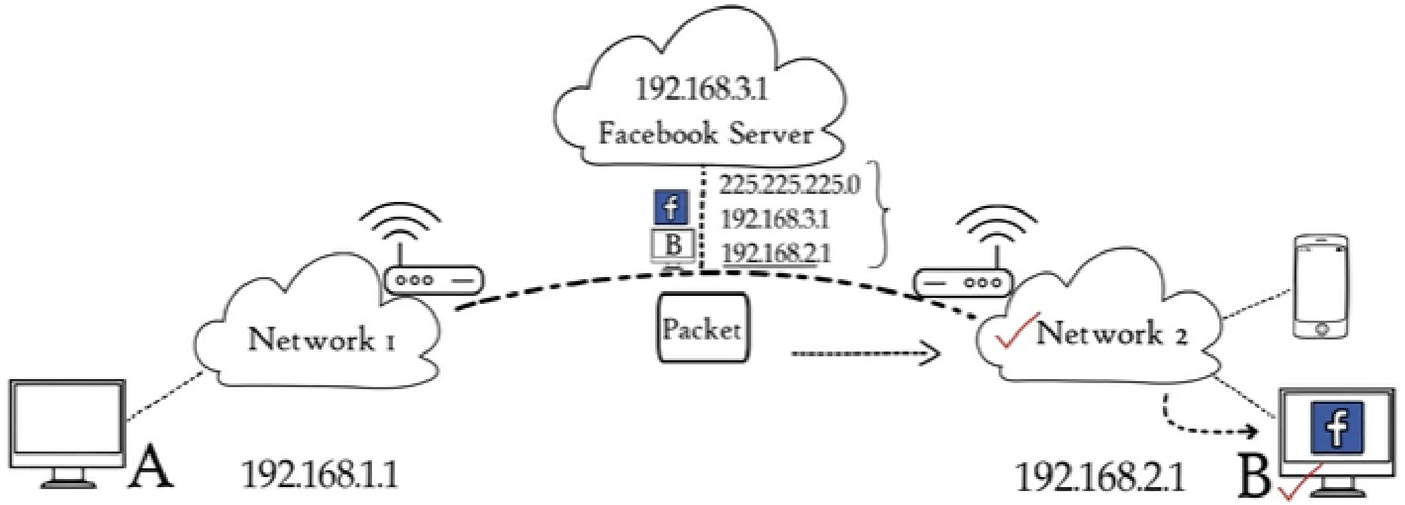
# Connection and connectionless Transmission :

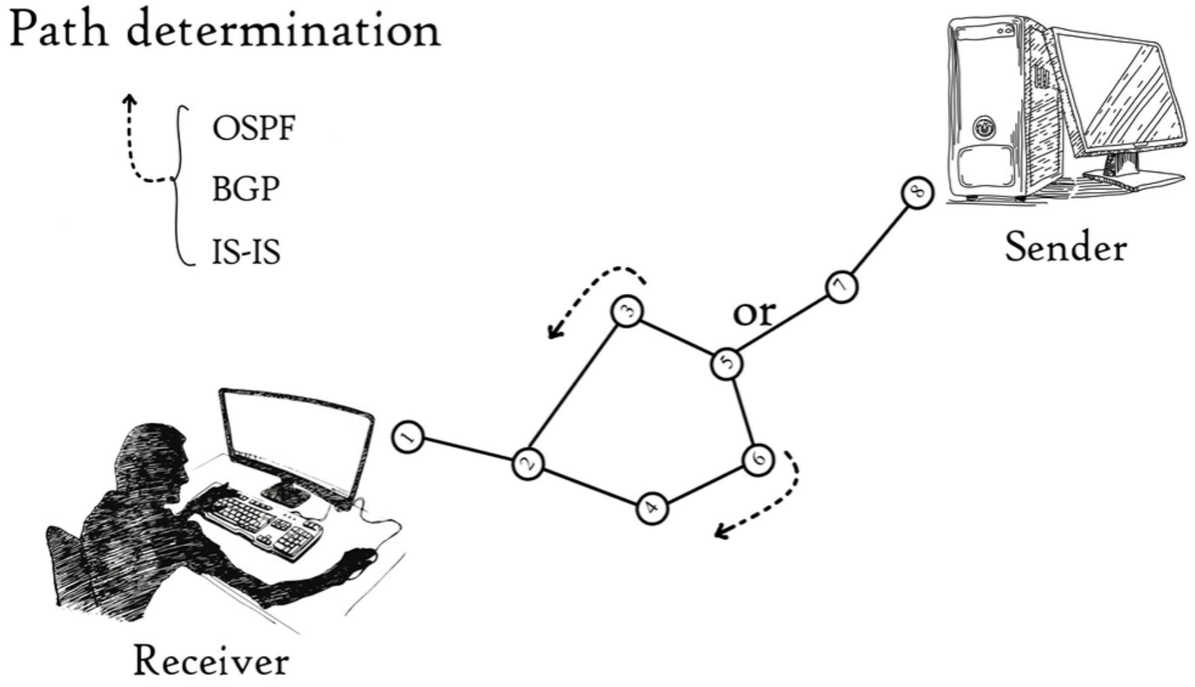
- For connection-oriented TCP is used
- For connectionless UDP is used



# 3.Network layer:

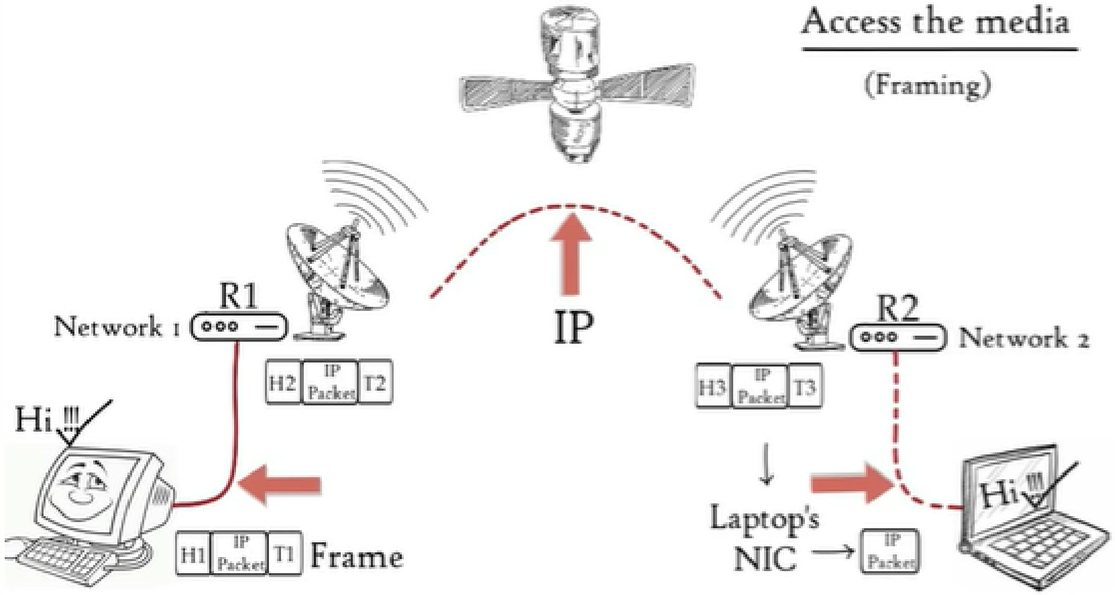
- Logical addressing
- Routing
- Path determination

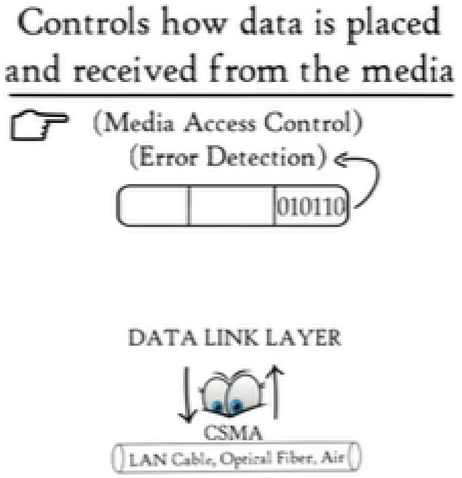


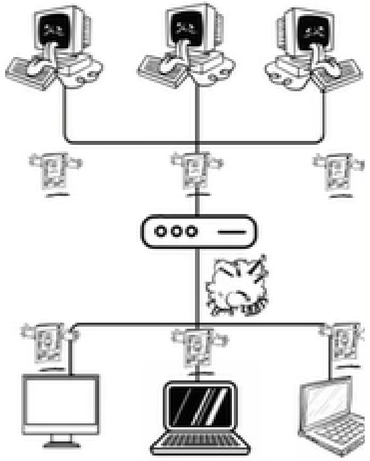



# 2.Data link layer:

- Framing
- Error detection
- Directs the frame to correct destination

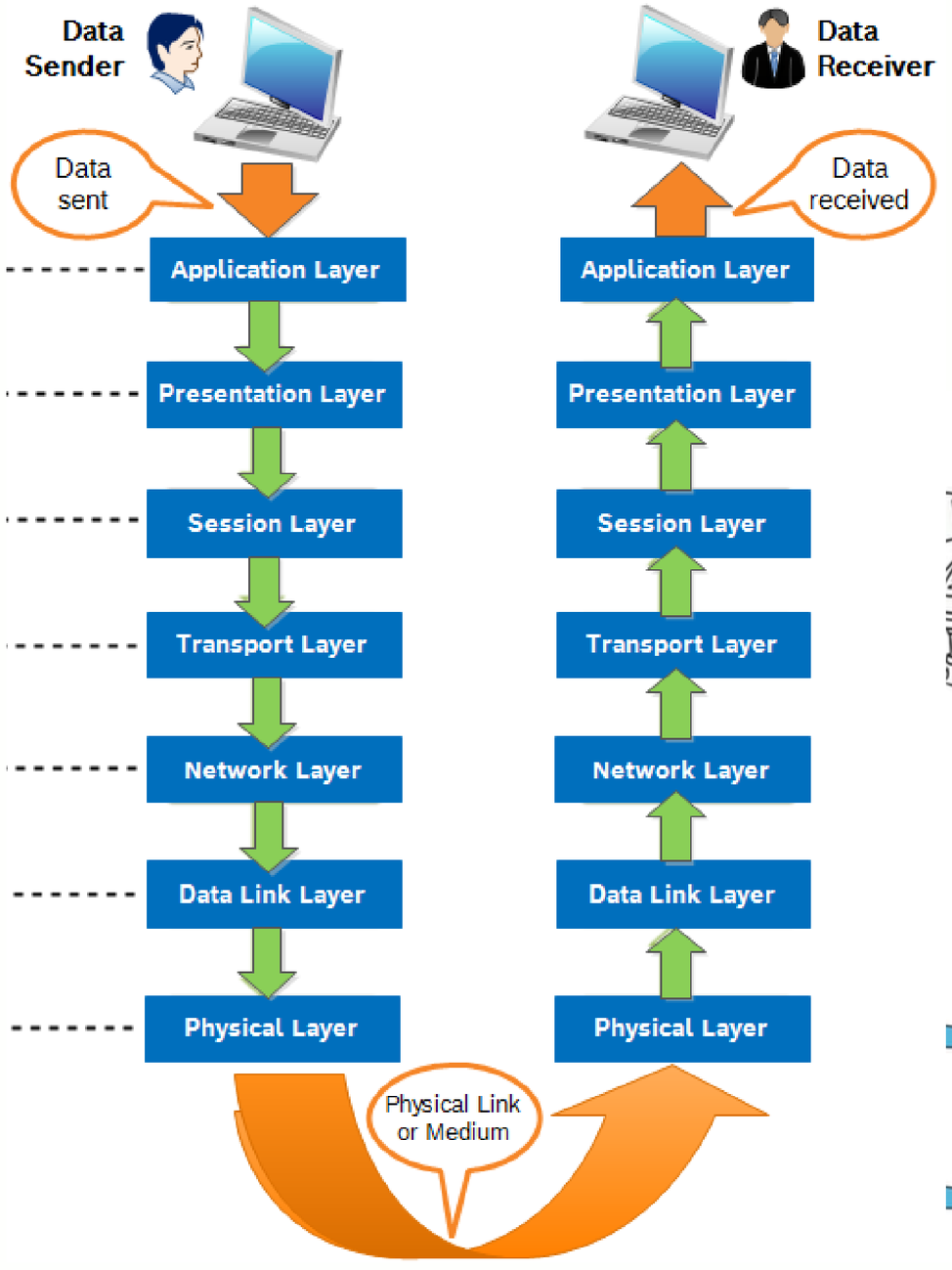


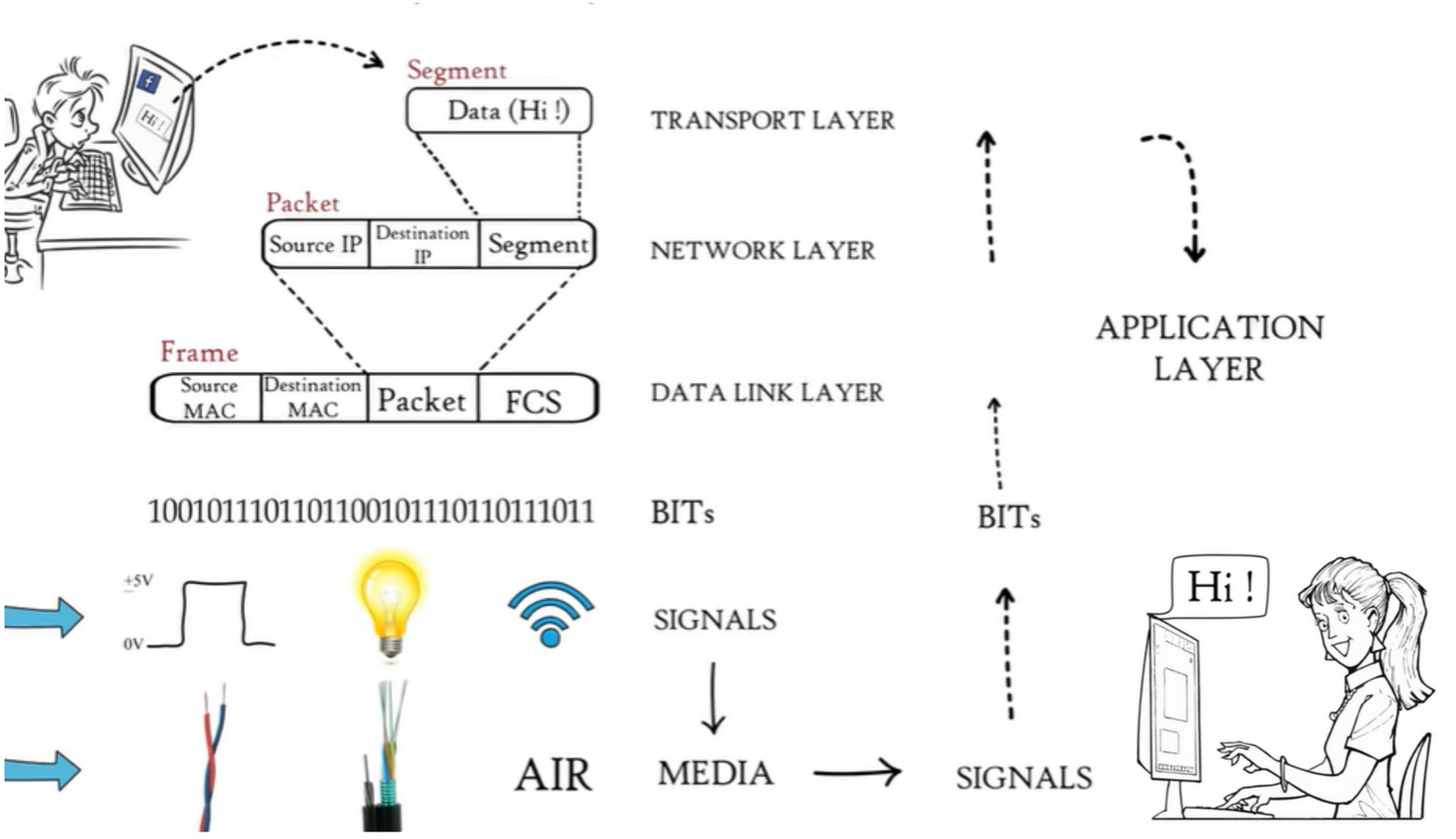



# 1.Physical layer:

- Physical layer converts Bits into electrical signals
- Transports these electrical signal from source to destination


Data Sender
Data Receiver
Data sent
Data received
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Physical Link or Medium


Segment
Data (Hi !)
TRANSPORT LAYER
Packet
Source IP
Destination IP
Segment
NETWORK LAYER
APPLICATION LAYER
Frame
Source MAC
Destination MAC
Packet
FCS
DATA LINK LAYER
10010111011011001011101101110 11
BITs
BITs
+5V
0V
SIGNALS
AIR
MEDIA
SIGNALS
Hi !

# TCP, UDP and Router Components

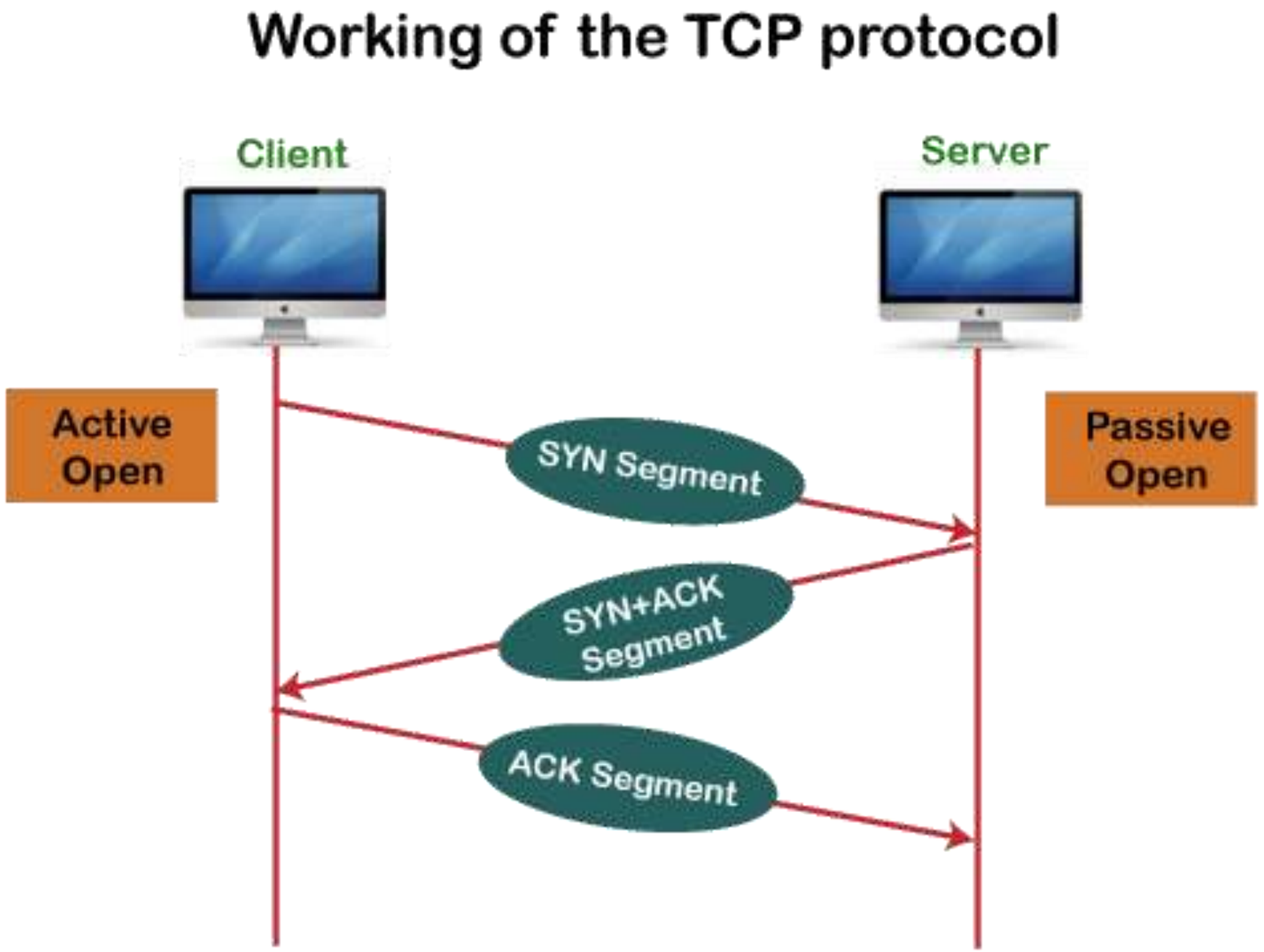
# TCP:-

- The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP to ensure reliable transmission of packets.
- TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets.
- TCP Protocol number is 6.

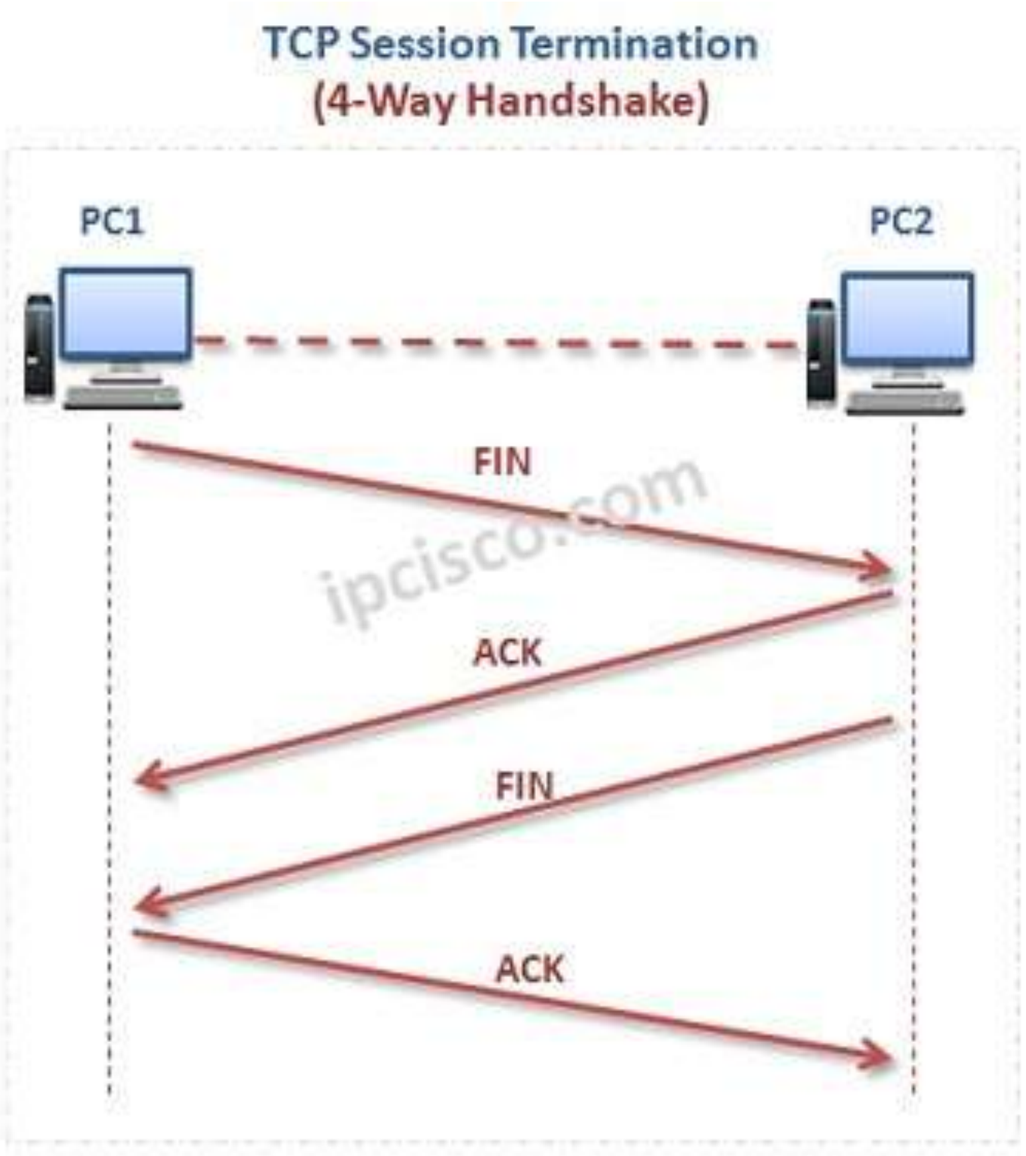
# UDP:-

- The User Datagram Protocol (UDP) is a lightweight data transport protocol. UDP protocol number is 17
- UDP provides a mechanism to detect corrupt data packets, but it does not attempt to solve other problems that arise with packets, such as lost or out of order packets. That's why UDP is sometimes known as the Unreliable Data Protocol.
- UDP is simple but fast. It's often used for time-sensitive applications (such as real-time video streaming) where speed is more important than accuracy.

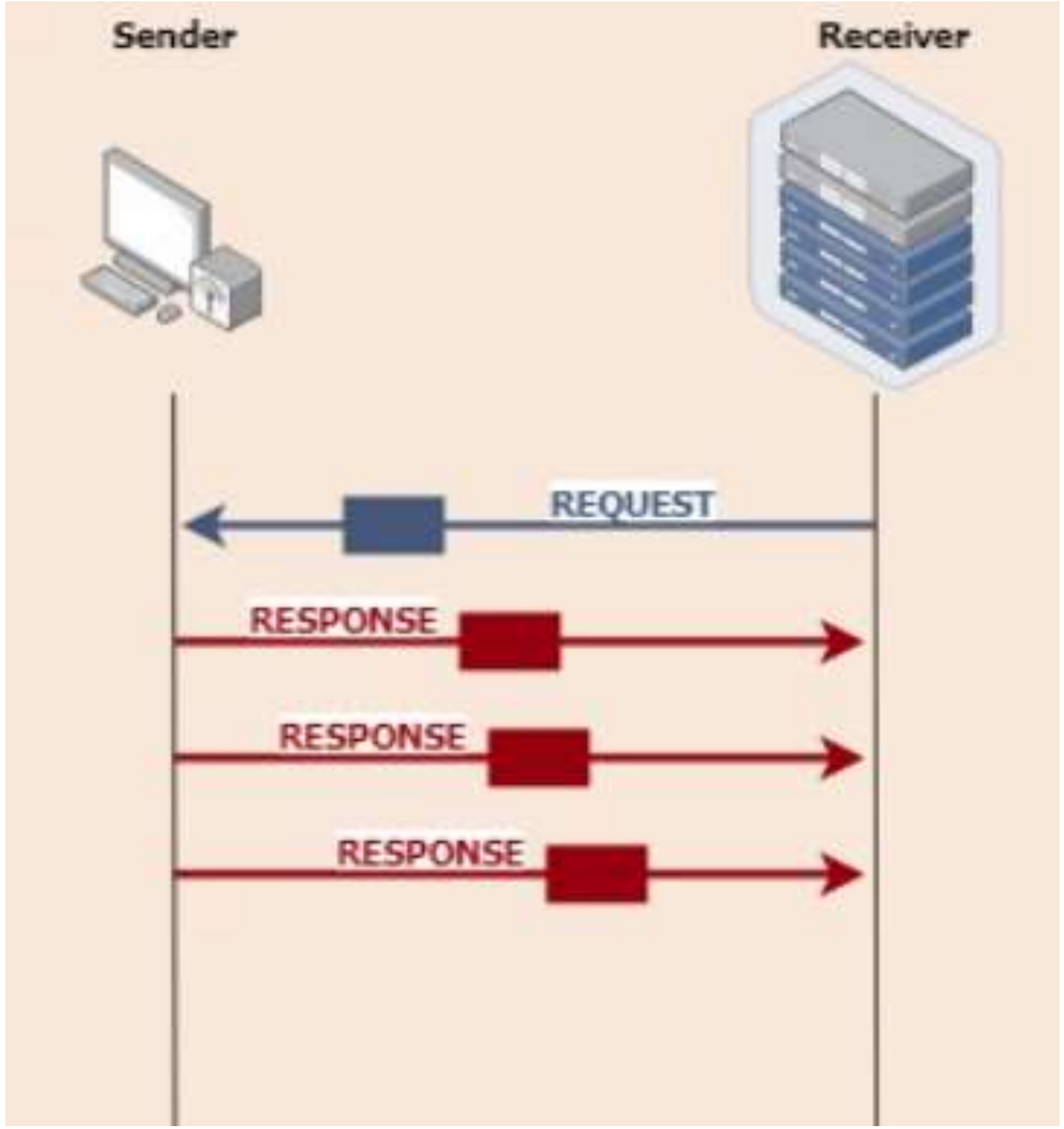
# TCP uses three way handshake in packet flow



# TCP uses four way handshake to end the session



# UDP packet flow:-

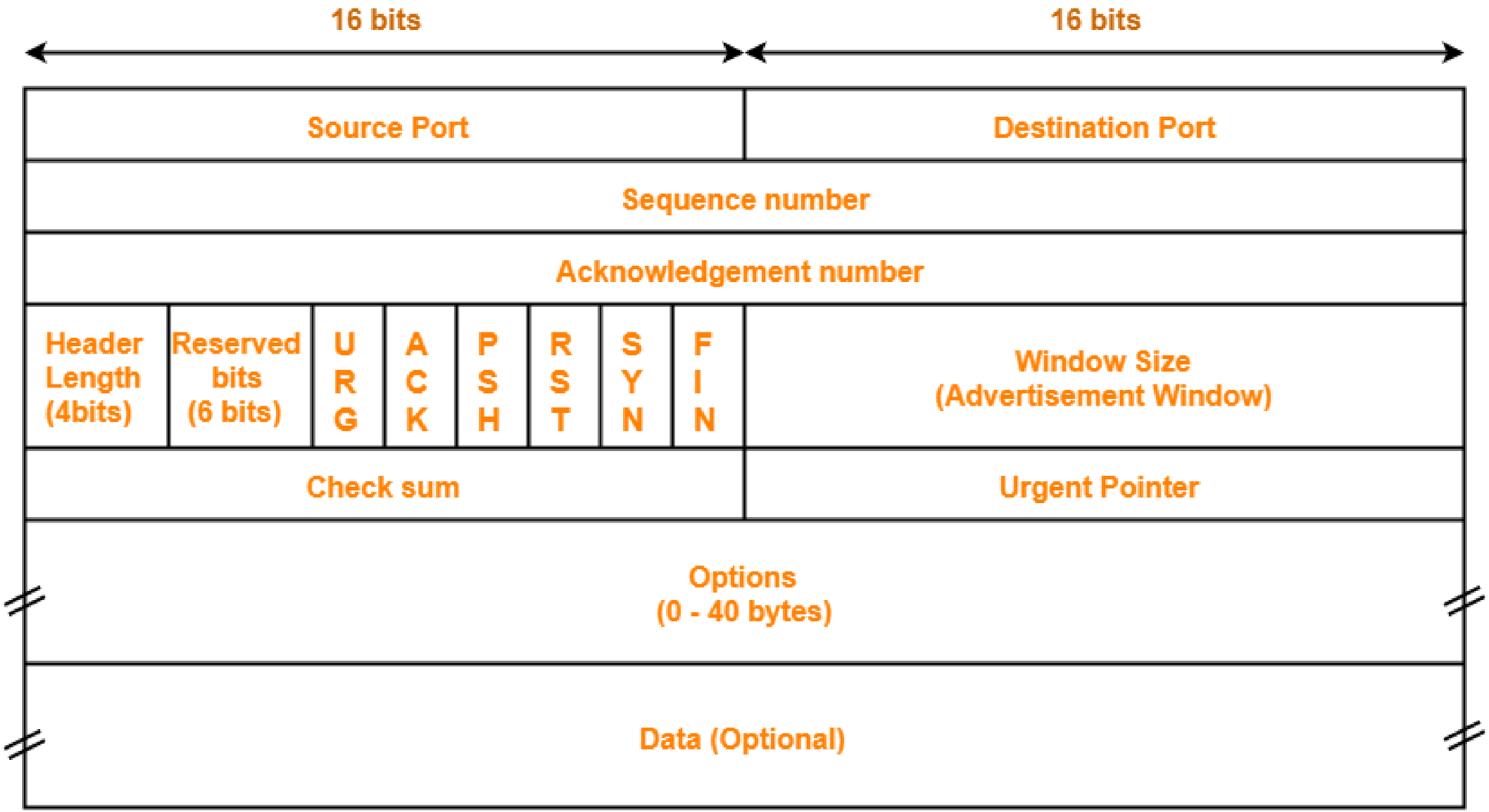


# TCP vs UDP

- Connected
- State Memory
- Byte Stream
- Ordered Data Delivery
- Reliable
- Error Free
- Handshake
- Flow Control
- Relatively Slow
- Point to Point

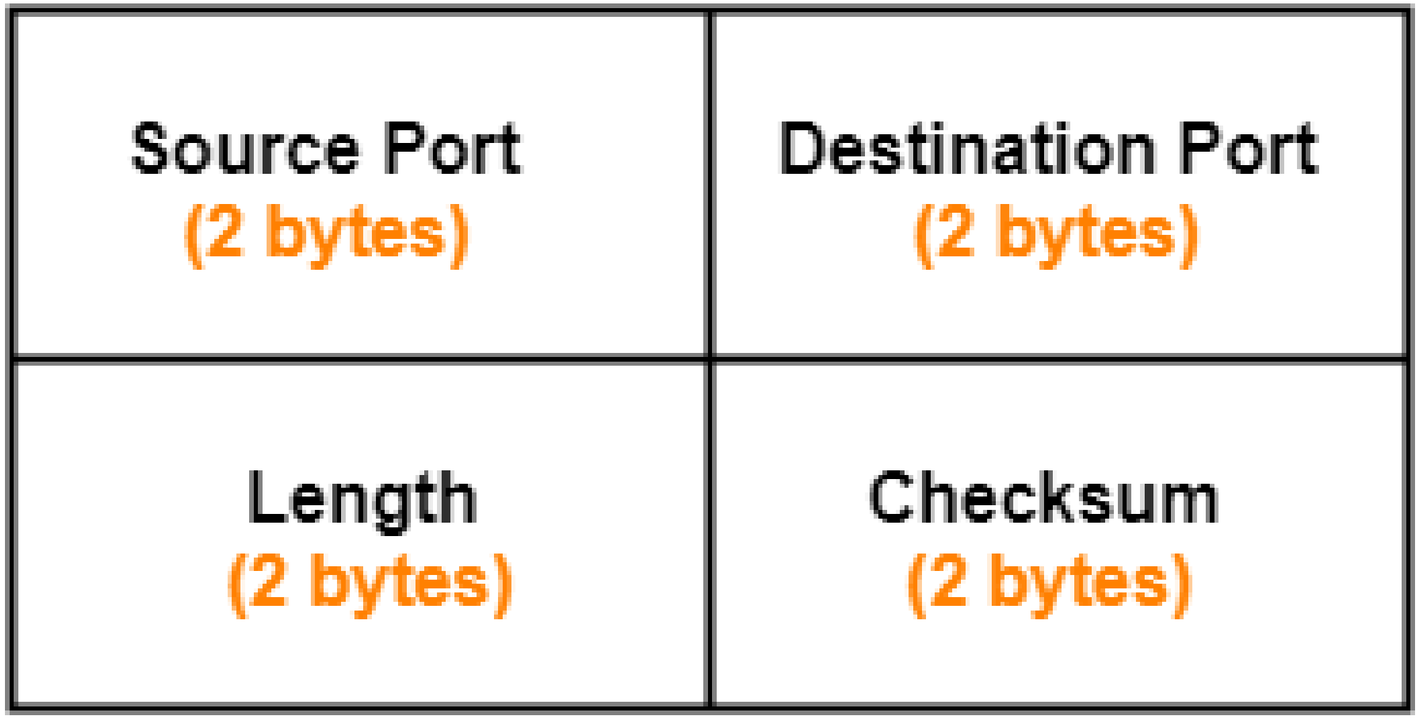
- Connectionless
- Stateless
- Packet/Datagram
- No Sequence Guarantee
- Lossy
- Error Packets Discarded
- No Handshake
- No Flow Control
- Relatively Fast
- Supports Multicast

# TCP header




TCP Header

# UDP header




UDP Header

# Characteristics of a Router:-

1) Router works on Layer 3 or Network Layer

2) Router is a intelligent device

3) Router has per port broadcst domain

4) Router has per port collision domain

5) Router uses IP addresses to communicate

# Components of a Router:-

1) ROM: Stores saved configuration

2) RAM: Stores running configuration

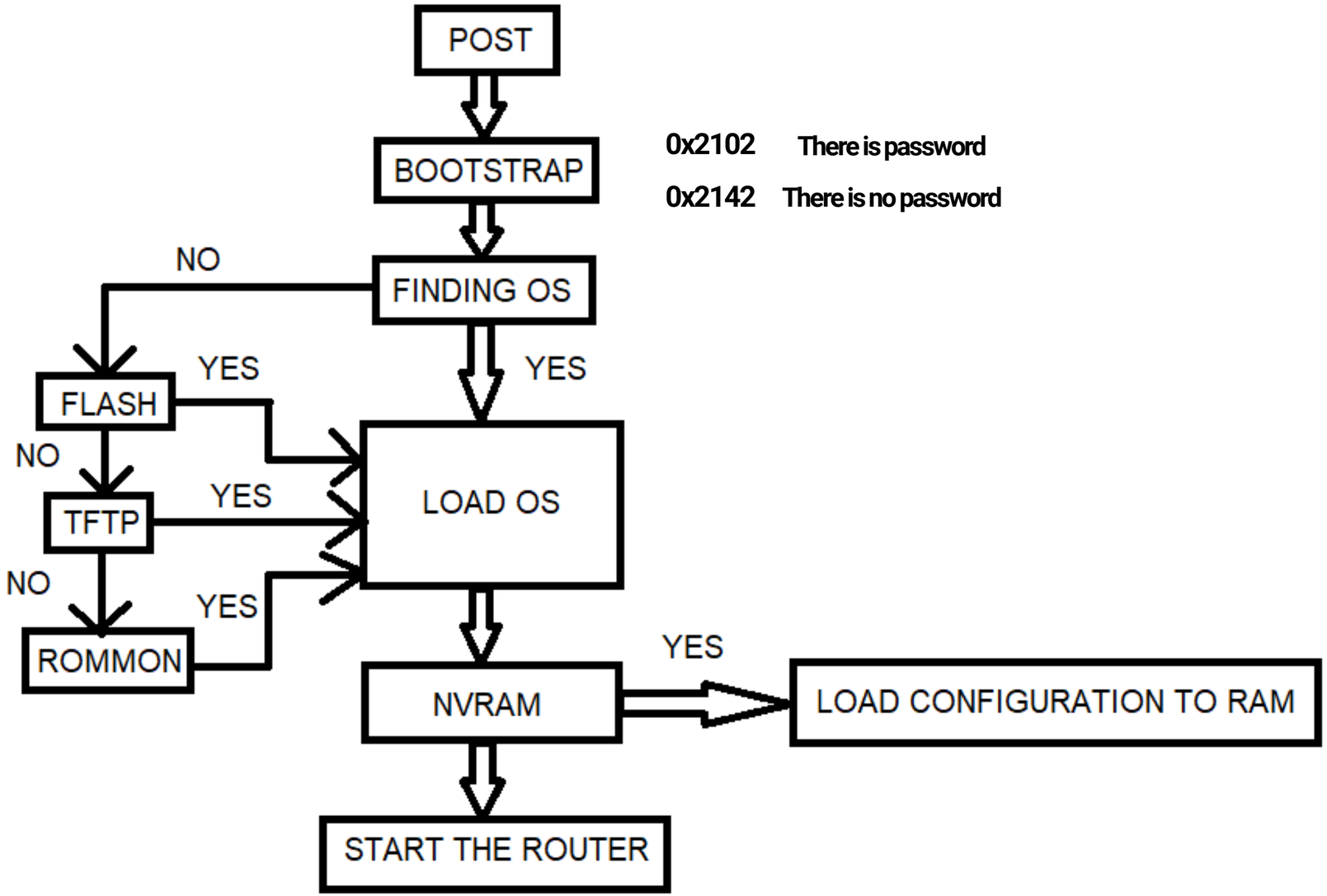
3) NVRAM: Stores startup configuration

4) FLASH: Contains operating system

5) BOOTSTRAP: Checks sequence number

6) POST: Checks Hardware configuration

# FLOWCHART OF A ROUTER




**0x2102** There is password

**0x2142** There is no password

# Router modes

**There are mainly 5 modes in router:**

1) User execution mode –
As soon as the interface up message appears and press enter, the router> prompt will pop up. This is called user execution mode. This mode is limited to some monitoring commands.

2) Privileged mode –
As we type enable to user mode, we enter into Privileged mode where we can view and change the configuration of router. Different commands like show running-configuration, show IP interface brief etc can run on this mode which are used for troubleshooting purpose.

3) Global configuration mode –

As we type configure terminal to the user mode, we will enter into the global configuration mode. Commands enter in these modes are called global commands and they affect the running-configuration of the router. In this mode, different configuration like making local database on router by providing username and password, can set enable and secret password etc.

4) Interface configuration mode –

In this mode, only configuration of interfaces are done. Assigning an IP address to an interface, bringing up the interface are the common tasks done in this mode.

5) ROMMON mode –

We can enter in this mode when we interrupt boot process of the router. Generally, we enter in this mode while password recovery process or Backing up of IOS on device like TFTP server. It is like BIOS mode of a PC.

Examples:

1) User execution mode: Router>
2) Privilege mode: Router#
3) Global Configuration mode: Router(config)#
4) Interface Configuration mode: Router(config-if)#

# PING, ICMP and ARP concepts

# How to check connectivity between two devices?

**PING (Packet InterNet Groper) test:**

The PING command is used to test the connection and latency between two network connections. The PING command sends packets of information to a specified IP Address and then measures the time it takes to get a response from the specified computer or device. PING works on ICMP protocol.

**Trace Route test:**

The TRACERT command is used to conduct a similar test to PING, but instead of displaying the time it takes to connect, it looks at the exact server hops required to connect your computer to the server.

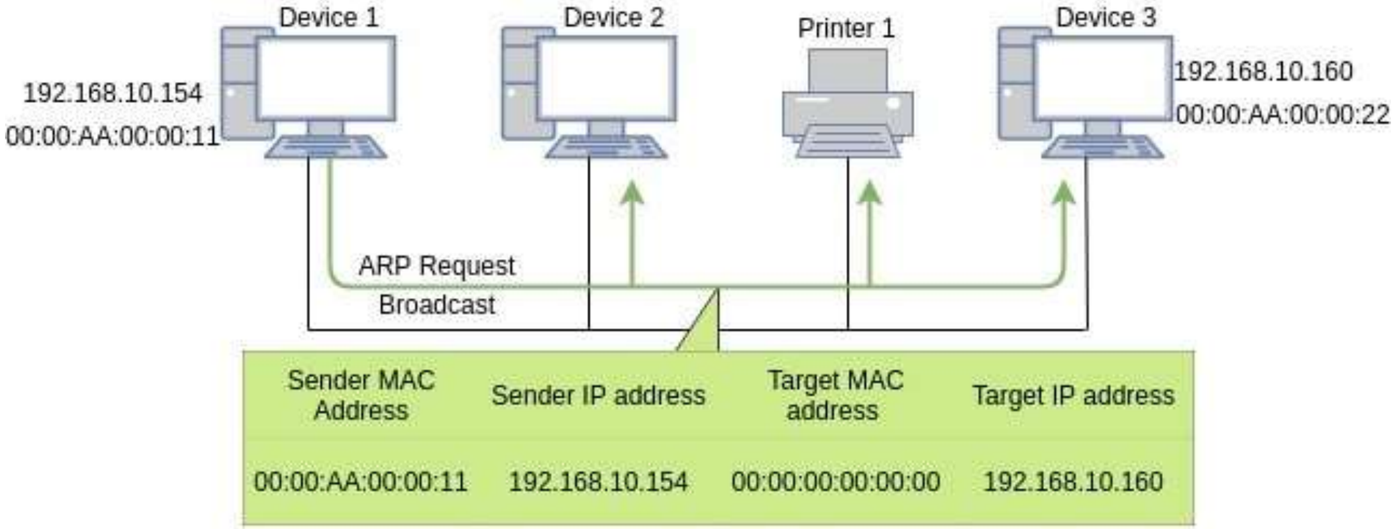
## ICMP (Internet Control Message Protocol) :

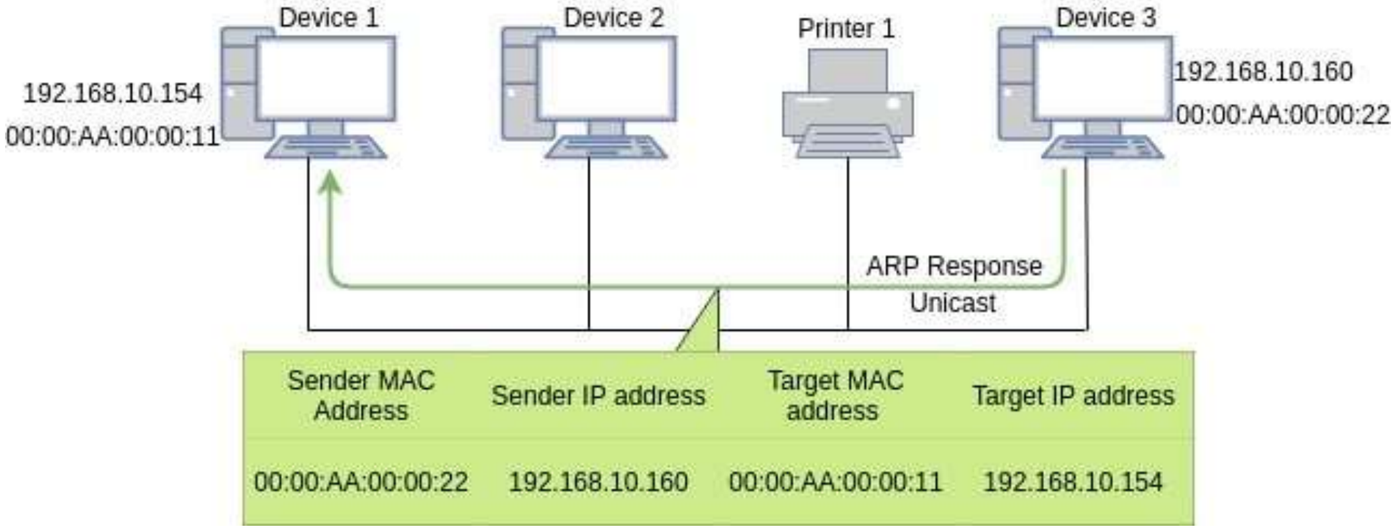
The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing.

## ARP (Address Resolution Protocol) :

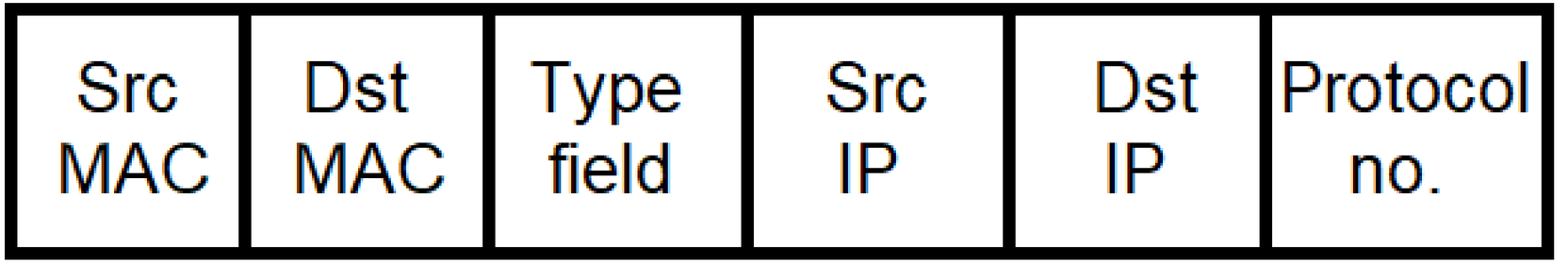
The Address Resolution Protocol(ARP) is a communication protocol used to discover the data-link layer address(Layer 2 address like Media Access Control(MAC) address) associated with an Internet layer address(Layer 3 address like IPv4 address).

ARP is a request-response or request-reply protocol in which one device sends a request to another device asking for some information, to which the other device will reply with the required information. It is a message exchange pattern. ARP packets are encapsulated by link layer and are distributed only in a particular network. As a result, ARP is said to be a link layer protocol.



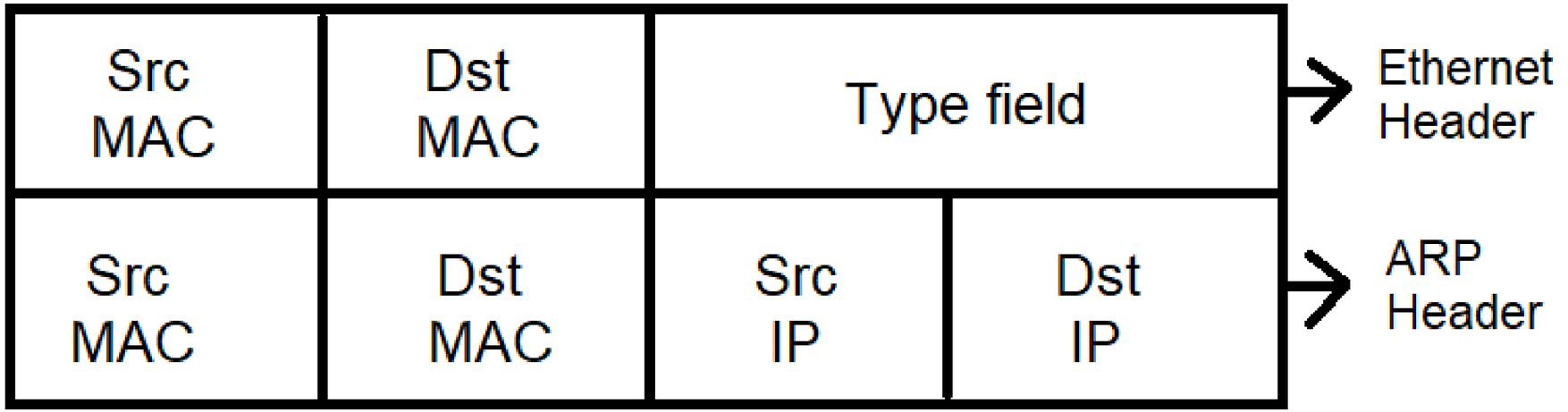
ICMP Packet:-




ICMP protocol number is 1

There are two types in ICMP packets
1) Echo request - type 8
2) Echo reply - type 0

ARP packet:-




There are two types of packets in ARP:-
1) ARP request (Opcode:- 0x0001)
2) ARP reply (Opcode:- 0x0002 )

## Garp (Gratuitous ARP):-

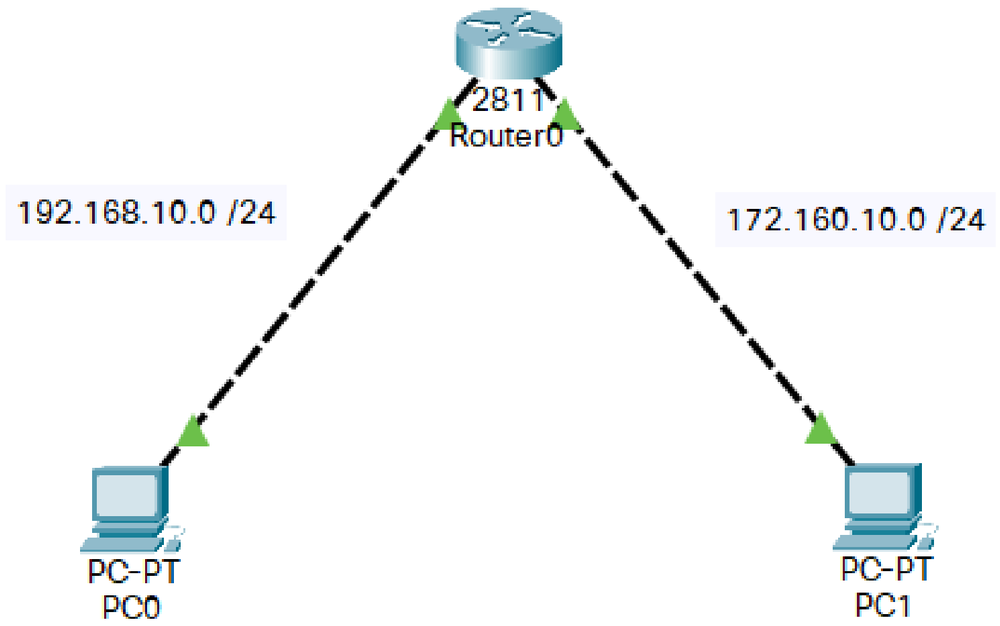
A Gratuitous ARP is an ARP Response that was not prompted by an ARP Request. The Gratuitous ARP is sent as a broadcast, as a way for a node to announce or update its IP to MAC mapping to the entire network.

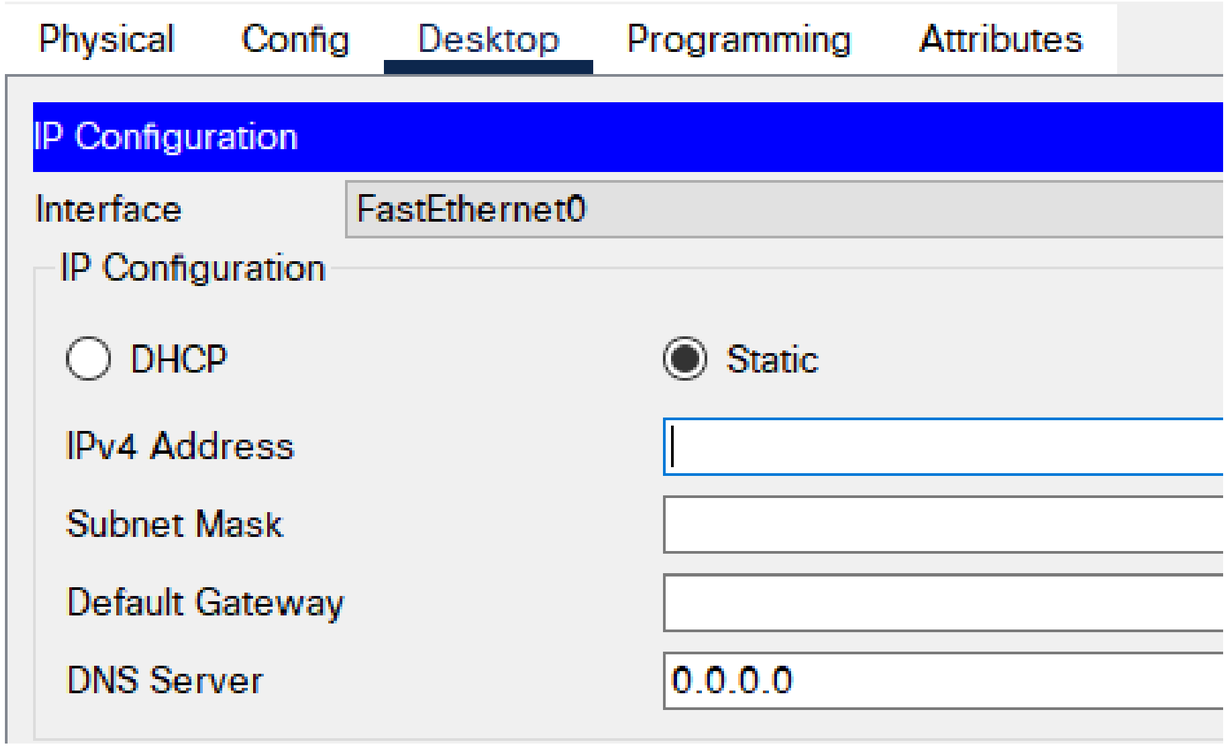
Garp is mainly used for:-
a) Redundancy purpose
b) To find out duplication

# Default gateway, Proxy ARP, Telnet and SSH

# Default gateway:-

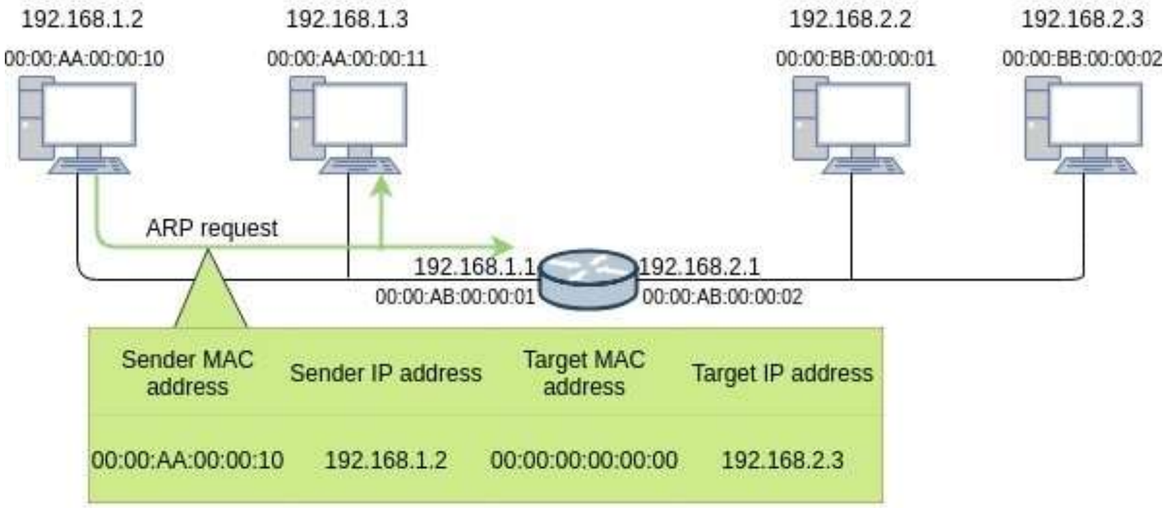
Default gateway is used for communicating to other network hosts.

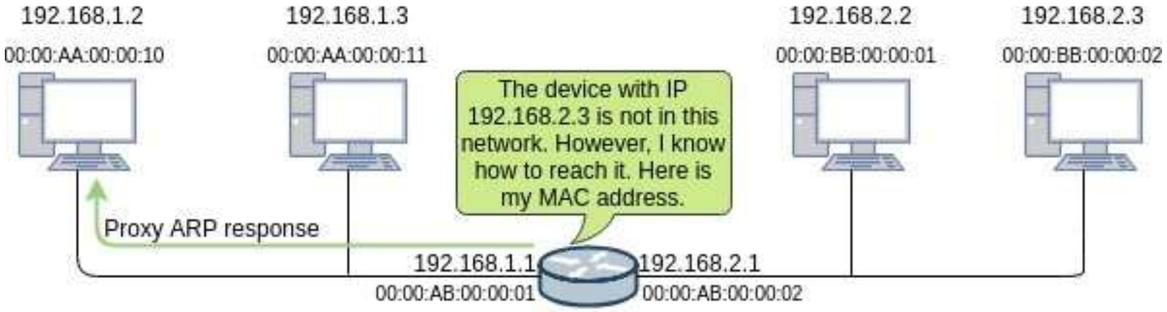


# Proxy ARP:

Proxy ARP is used to facilitate ARP exchanges in order to resolve IP addresses to MAC addresses in devices that are separated by routers in the same network or sub-network. Routers cannot forward Layer 2 packets and hence, ARP messages are never propagated outside of their networks. When a device wants to resolve the MAC address of another device in a different subnet, the router located between the two subnets acts as a proxy for the other device and responds to the ARP broadcast with its own MAC address.



# What is Telnet?

TELNET stands for TErminaL NETwork. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. Computer which starts connection known as the local computer. Computer which is being connected to i.e. which accepts the connection known as remote computer.

When the connection is established between local and remote computer during telnet operation whatever that is being performed on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

# Key points to remember about Telnet

- Telnet is an application-layer protocol and allows a user to connect to an account on another remote machine.
- Telnet uses port 23, which was designed specifically for local area networks.
- Telnet is the standard TCP/IP protocol for virtual terminal service.
- Telnet transfers the data in plain text.
- Telnet is vulnerable to security attacks.
- No privileges are provided for the user's authentication.
- Required low bandwidth usage.
- Used in Linux and Windows Operating system.

# What is SSH?

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution but any network service can be secured with SSH.

SSH provides a secure channel over an unsecured network by using a client–server architecture, connecting an SSH client application with an SSH server. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

SSH was designed as a replacement for Telnet and for unsecured remote shell protocols

# Key points to remember about SSH

- SSH is an application-layer protocol and allows a user to connect to an account on another remote machine in a secure way.
- SSH runs on port 22 by default, which you can change it.
- SSH works on TCP protocol
- SSH uses encrypted format to send data and also uses a secure channel.
- SSH helps you to overcome many security issues of Telnet.
- SSH is a more secure protocol, so it uses public-key encryption for authentication.
- Required high bandwidth usage.
- Used in all popular Operating systems.

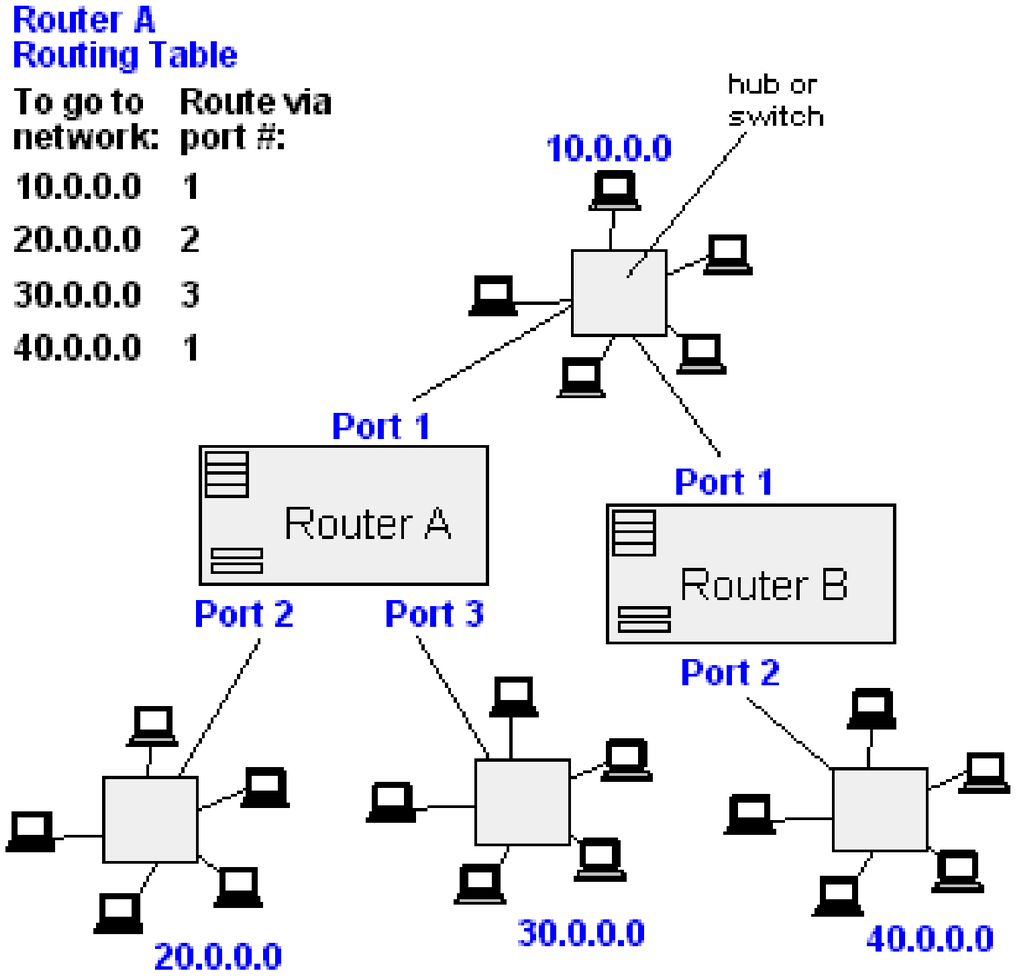
# Difference between SSH and Telnet

| SSH | Telnet |
|---|---|
| Highly secured | Less secured than SSH |
| Uses TCP port number 22 | Uses TCP port number 23 |
| 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. |
| SSH uses public key encryption in order to authenticate the remote users | Telnet uses no authentication mechanisms |
| Usernames and Passwords can be prone to malicious attack | Data sent using this protocol cannot be easily interpreted by the hackers. |
| Suitable for Public networks | Suitable for private networks |
| 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. |
| High bandwidth usage | Low bandwidth usage |
| All popular Operating systems | Used in Linux and Windows Operating system. |
| RFC 4253 specifies SSH server | Telnet was developed in 1969 beginning with RFC 15 and extended in RFC 854 |

# Routing Protocols- Static and Default

# What is routing?

Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation. In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.



# What is a route?

Route is the best path selected by a router to reach from source to destination.

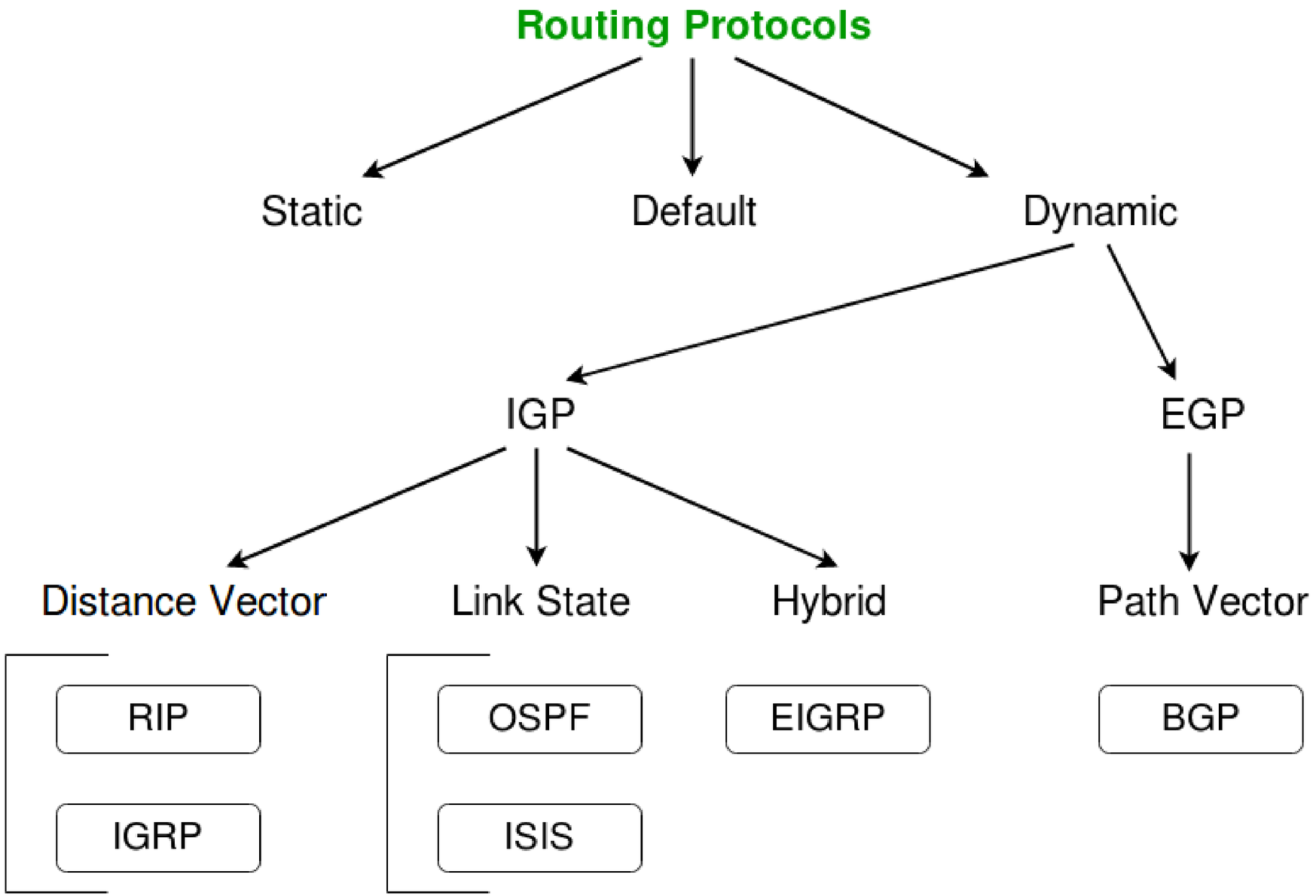
# What is a routing table?

Routing table is collection of routes to transfer data from one domain to another.

# What is an IP?

IP: The Internet Protocol specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

# Types of Routing Protocols



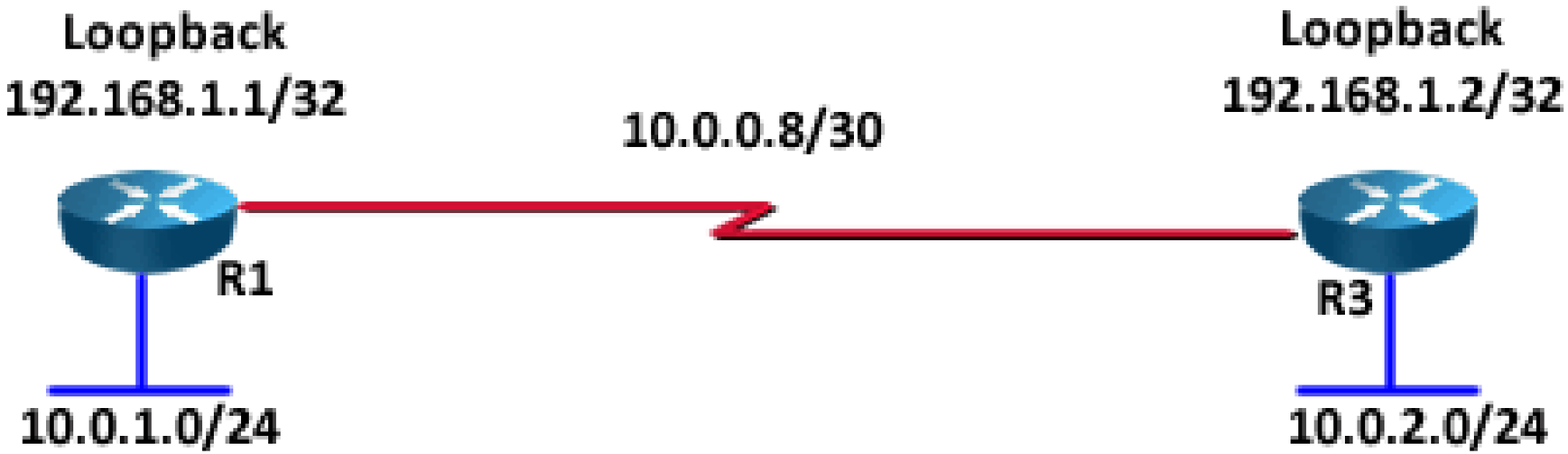
# What are Loopback Interfaces?

- Loopback interfaces are logical interfaces
- They allow you to assign an IP address to a router which is not tied to a physical interface
- Because they don't have any physical attributes which can fail, loopback interface never go down
- Loopbacks are treated as separate broadcast domain

# Uses of Loopback Interface

- Loopback is commonly used for traffic that terminates on the router itself
- Loopback is also used to identify the router (RID) in routing protocols.
- Loopback can be used for multiple tasks
- Loopback can be configured easily and multiple loopback can be created on a single router for testing purpose

# Loopback interface used in a topology



# Static Routing Protocol

Static routing is a process in which we have to manually add routes in routing table. AD value of static route is 1.

**Advantages:–**

1) No routing overhead for router CPU which means a cheaper router can be used to do routing.

2) It adds security because only administrator can allow routing to particular networks only.

3) No bandwidth usage between routers.

## Disadvantages:–

1) For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.

2) The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

## Configuration:-

ip route <network id> <subnet mask> <next hop>
example:
ip route 192.168.10.0 255.255.255.0 172.16.10.2

# Administrative Distance (AD):-

Administrative Distance (AD) is used to rate the trustworthiness of routing information received from the neighbor router. The route with the least AD will be selected as the best route to reach the destination remote network and that route will be placed in the routing table. It defines how reliable a routing protocol is. It is an integer value ranging from 0 to 255 where 0 shows that the route is most trusted and 255 means that no traffic will be passed through that route or that route is never installed in the routing table.

| Route sources | Default AD |
|---|---|
| Connected interface | 0 |
| Static route | 1 |
| External BGP | 20 |
| EIGRP | 90 |
| OSPF | 110 |
| RIP | 120 |
| External EIGRP | 170 |
| Internal BGP | 200 |
| Unknown | 255 (This route is not used) |

# Default Routing Protocol

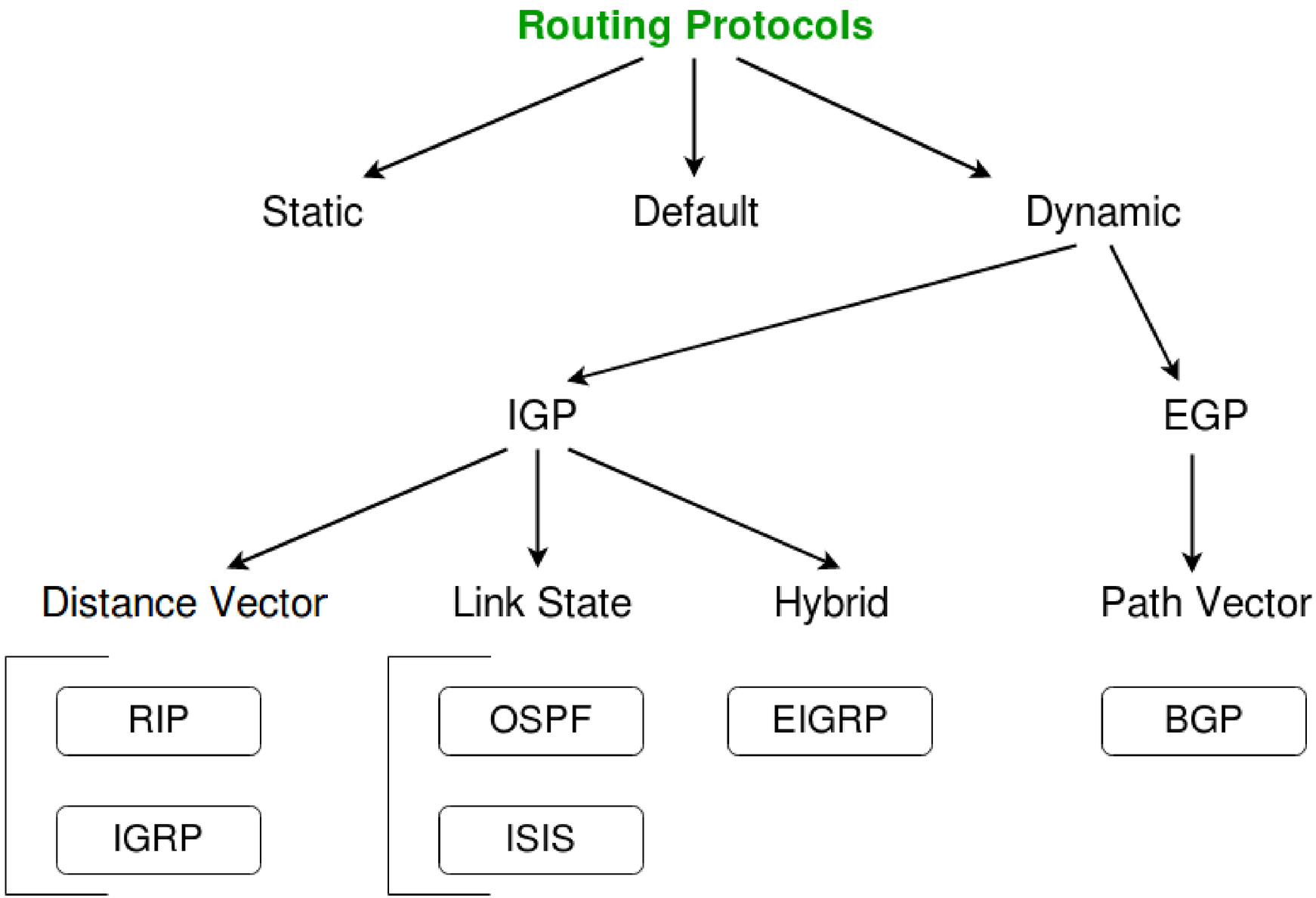
This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks. AD value is 1.

**Configuration –**

ip route 0.0.0.0 0.0.0.0 <next hop>
Example:
ip route 0.0.0.0 0.0.0.0 172.16.10.5

# Routing Protocols- Static, Default and Dynamic

# Types of Routing Protocols



# Static Routing Protocol

Static routing is a process in which we have to manually add routes in routing table. AD value of static route is 1.

**Advantages:–**

1) No routing overhead for router CPU which means a cheaper router can be used to do routing.

2) It adds security because only administrator can allow routing to particular networks only.

3) No bandwidth usage between routers.

## Disadvantages:–

1) For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.

2) The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

## Configuration:-

ip route <network id> <subnet mask> <next hop>
example:
ip route 192.168.10.0 255.255.255.0 172.16.10.2

# Default Routing Protocol

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

**Configuration –**

ip route 0.0.0.0 0.0.0.0 <next hop>
Example:
ip route 0.0.0.0 0.0.0.0 172.16.10.5

# Dynamic Routing Protocol

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

**A dynamic protocol have following features:**

1) The routers should have the same dynamic protocol running in order to exchange routes.
2) When a router finds a change in the topology then router advertises it to all other routers.

## Advantages –

1) Easy to configure.

2) More effective at selecting the best route to a destination remote network and also for discovering remote network.

## Disadvantage –

1) Consumes more bandwidth for communicating with other neighbors.

2) Less secure than static routing.

1) **RIP features:-**

a) RIP full form is Routing Information Protocol
b) RIP has two versions: RIP v1 and RIP v2
c) RIP v1 is classful, uses broadcast and RIP v2 is classless, uses multicast
d) It is a distance vector Protocol
e) Uses hop count and maximum hop count is 15
f) Works on Ballman Ford algorithm
g) Works on port number 520
h) Multicast address is 224.0.0.9
i) AD value of RIP is 120
j) RIP timers: Hello (30 sec), In-valid (30-180 sec), Hold-on (180-240 sec), Flush (240th sec)

## 2) **EIGRP features:-**

a) EIGRP full form is Enhanced interior gateway routing protocol
b) EIGRP is link state + distance vector protocol i.e hybrid
c) EIGRP works on protocol number 88
d) EIGRP has two AD values
e) AD value is 90 for internal and 170 for external
f) EIGRP has metric values
g) Metric values are: K1-Bandwidth, K2-Load, K3-Delay, K4-Realibility, K5-MTU
h) EIGRP multicast address is 224.0.0.10
i) EIGRP timers: Hello (5 sec), Death (15 sec)
j) EIGRP has 5 packets
k) EIGRP packets are: Hello, Acknowledgement, Update, Query and Reply

## 3) OSPF features:-

a) OSPF full form is Open shortest path first
b) OSPF is a link state protocol
c) OSPF works on protocol number 89
d) OSPF AD value is 110
e) OSPF has two Multicast IP address
f) Multicast IP address are: 224.0.0.5 (all) and 224.0.0.6 (DR/BDR)
g) OSPF works on Dijkstra's Algorithm
h) OSPF uses area (16 or 32 bit number) and process id (1-65535)
i) OSPF uses DR and BDR
j) OSPF is classless and supports VLSM/CIDR

l) OSPF has 7 neighborship states:

- Down: Database is down
- Init: Hello data packets are sent
- 2-way: DR and BDR election happens
- Ex-start: Master and slave election happens
- Ex-change: Exchanging of database happens
- Loading: Missed data packets are loaded
- Full: Successfully loaded database

k) OSPF packets: Hello, Database description, Link-state request, Link-state update, Link-state acknowledgement

m) DR election:

i) Highest priority (0-255, by default priority=1)

ii) Highest router id

n) BDR election

i) Second highest priority

ii) Second highest router id

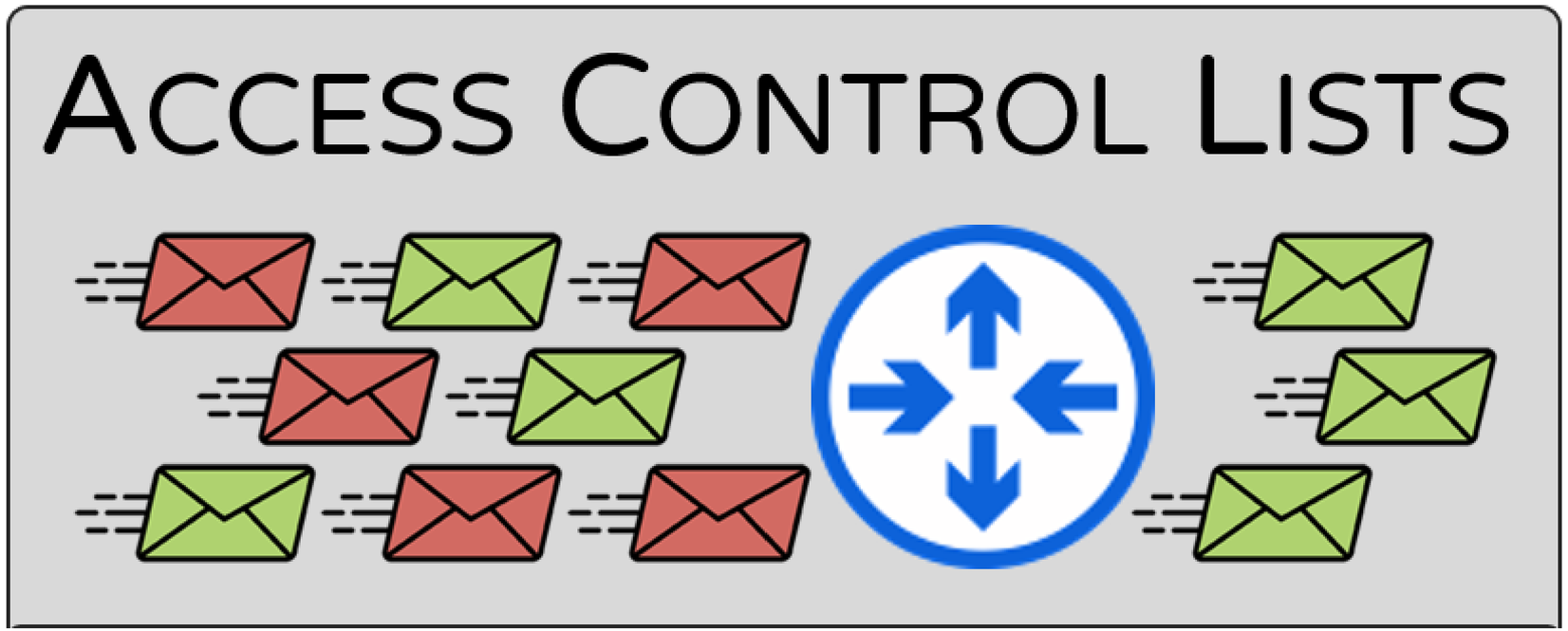
o) Router ID or RID selection:

- First preference- Manual RID
- Second preference- Loopback interface
- Third preference- Physical IP address

# ACL

# What is an ACL?

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.



# Inbound and Outbound Interface

Once the access-list is built, then it should be applied to inbound or outbound of the interface:

**1) Inbound Interface –**
The interface through which router receives the traffic in known as inbound interface. Traffic coming into the router is known as incoming traffic.

**2) Outbound Interface –**
The interface through which router transmits the traffic out in known as outbound interface. Traffic going out of the router is known as outgoing traffic.

# Types of ACL

- Standard Access-list
  - Named standard access list
  - Numbered standard access-list

- Extended Access-list
  - Named extended access list
  - Numbered extended access-list

# Difference between Standard ACL and Extended ACL

## Standard Access List

- The access-list number range is 1 – 99
- Can block a Network, Host and Subnet
- Two way communication is stopped
- All services are blocked.
- Implemented closest to the destination.
- Filtering is done based on only source IP address

## Extended Access List

- The access-list number range is 100 – 199
- Can block a Network, Host, Subnet and Service
- One way communication is stopped
- Selected services can be blocked.
- Implemented closest to the source.
- Checks source, destination, protocol, port no

# Redundancy Protocols and Translations

# What is FHRP?

- FHRP means First Hop Redundancy Protocol. FHRP is used to prevent network failure at a default gateway.
- This is achieved by configuring multiple routers with the same IP address, thus presenting an illusion of a single virtual router to the hosts.
- The IP address of the virtual router is configured on all hosts in that network or subnet as their default gateway.

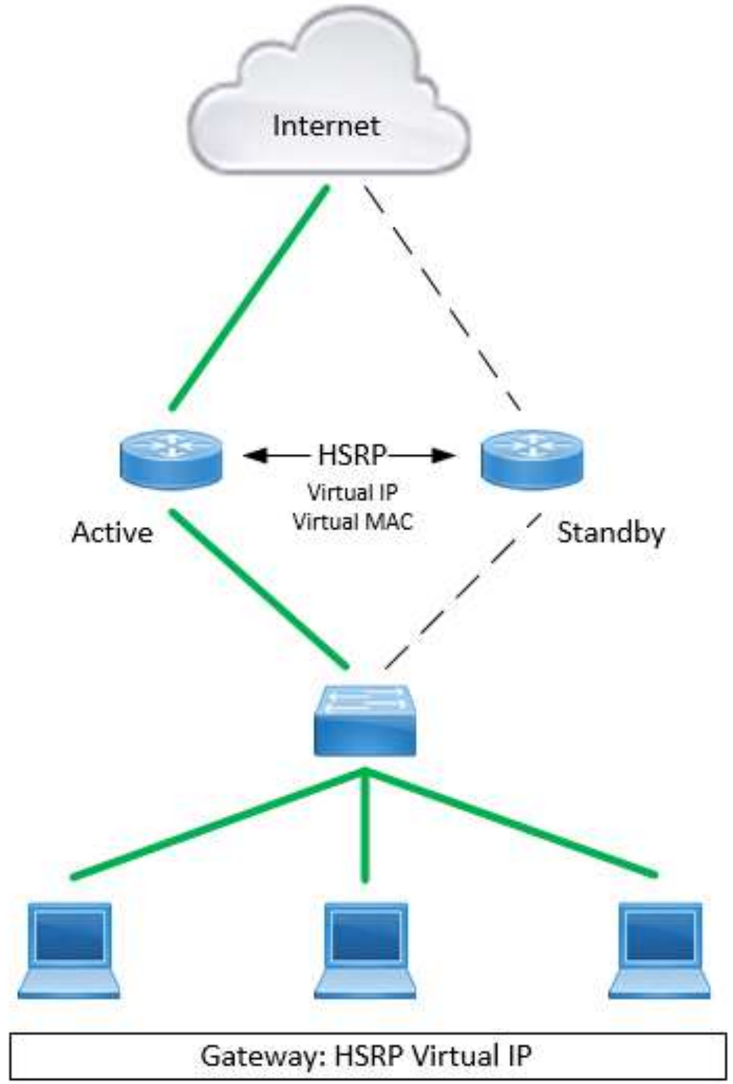
# Various FHRP Protocols

- **Hot Standby Router Protocol (HSRP)**
- **Virtual Router Redundancy Protocol (VRRP)**
- **Gateway Load Balancing Protocol (GLBP)**

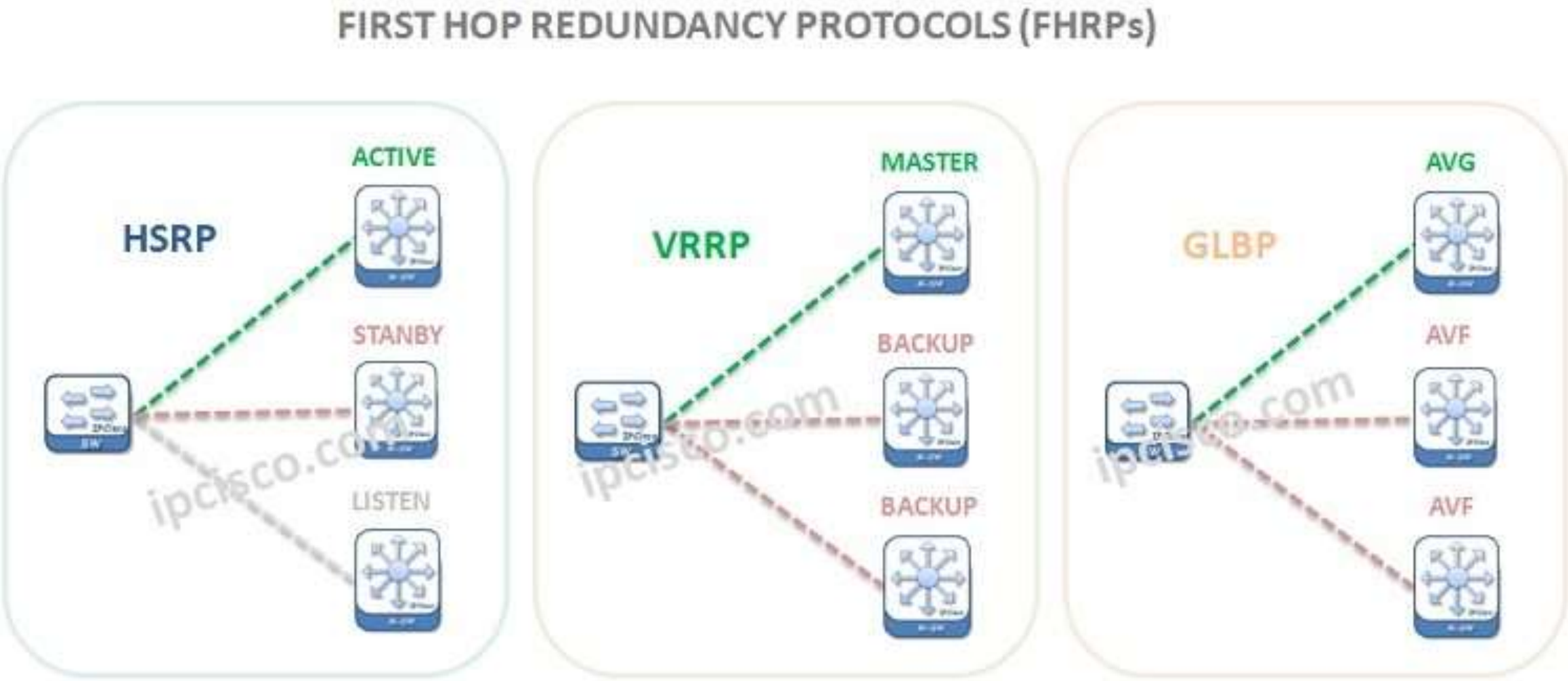
# Hot Standby Router Protocol (HSRP)

- HSRP is a Cisco proprietary protocol that enables the network engineer to configure multiple redundant routers that exist on the same subnet, each can be used as a gateway for the devices on the subnet.
- Without HSRP, each of the devices on the subnet would need to be individually configured to use a specific gateway, effectively not providing redundancy but limiting the number of clients that would be affected if a router were to go down.
- With HSRP, a group of routers (gateways) will be configured together, and a single HSRP virtual IP address will be created that are used by the devices on the subnet.

- The different routers in the HSRP will communicate to select a single active gateway that handles all live traffic. At this point, a single standby gateway is also selected.
- This standby gateway communicates with the active gateway via multicast and will detect should the active gateway fail.
- When this happens, one of the standby gateways will take over the duties of the active gateway and continue traffic forwarding without much (if any) delay. When this happens, a new standby gateway is also selected.



# Difference between HSRP, VRRP and GLBP



| Protocol | HSRP | VRRP | GLBP |
|---|---|---|---|
| Stands for | Hot Standby Router protocol | Virtual Redundancy Router Protocol | Gateway Load Balancing Protocol |
| Role of the Router | 1 active and 1 standby router | 1 master and 1 backup router | 1 AVG and 4 AVF routers- All are active |
| Use of IP | Use Virtual IP address | Can use real router ip address, if not, the one with highest priority become master | Use Virtual IP address |
| Stanndard | Cisco | IEEE | Cisco |
| Election | Active Router:<br>1-Highest Priority<br>2-Highest IP (tiebreaker) | Master Router: (*)<br>1-Highest Priority<br>2-Highest IP (tiebreaker) | Active Virtual Gateway:<br>1-Highest Priority<br>2-Highest IP (tiebreaker) |
| Tracking | Yes | Yes | Yes |
| Preempt | Yes | Yes | Yes |
| Timer adjustments | Yes | Yes | Yes |
| Traffic type | 224.0.0.2 – udp 1985 (version1)<br>224.0.0.102-udp 1985 (version2) | 224.0.0.18 – IP 112 | 224.0.0.102 udp 3222 |

# What is Translation?

- To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required.
- Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- PAT is a process where it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the table.

# Types of Translations:

## 1) Static NAT –

- In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting.
- These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.
- Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

# 2) Dynamic NAT –

- In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses.
- If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
- Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time.
- If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses.
- NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

# 3) Port Address Translation (PAT) –

- In this, many local (private) IP addresses can be translated to a single registered IP address.
- Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address.
- This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

# DHCP, DNS, FTP and TFTP

# What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in networks to dynamically assign IP addresses & other network configuration information like default gateway, mask, DNS server address etc. DHCP is a layer 7 protocol and works on UDP. DHCP uses port no. 67 for server and 68 for client.

DHCP server automatically assigns IP address to various devices in network. This in turn reduces work of Network Administrator to manually assign IP address to various devices.

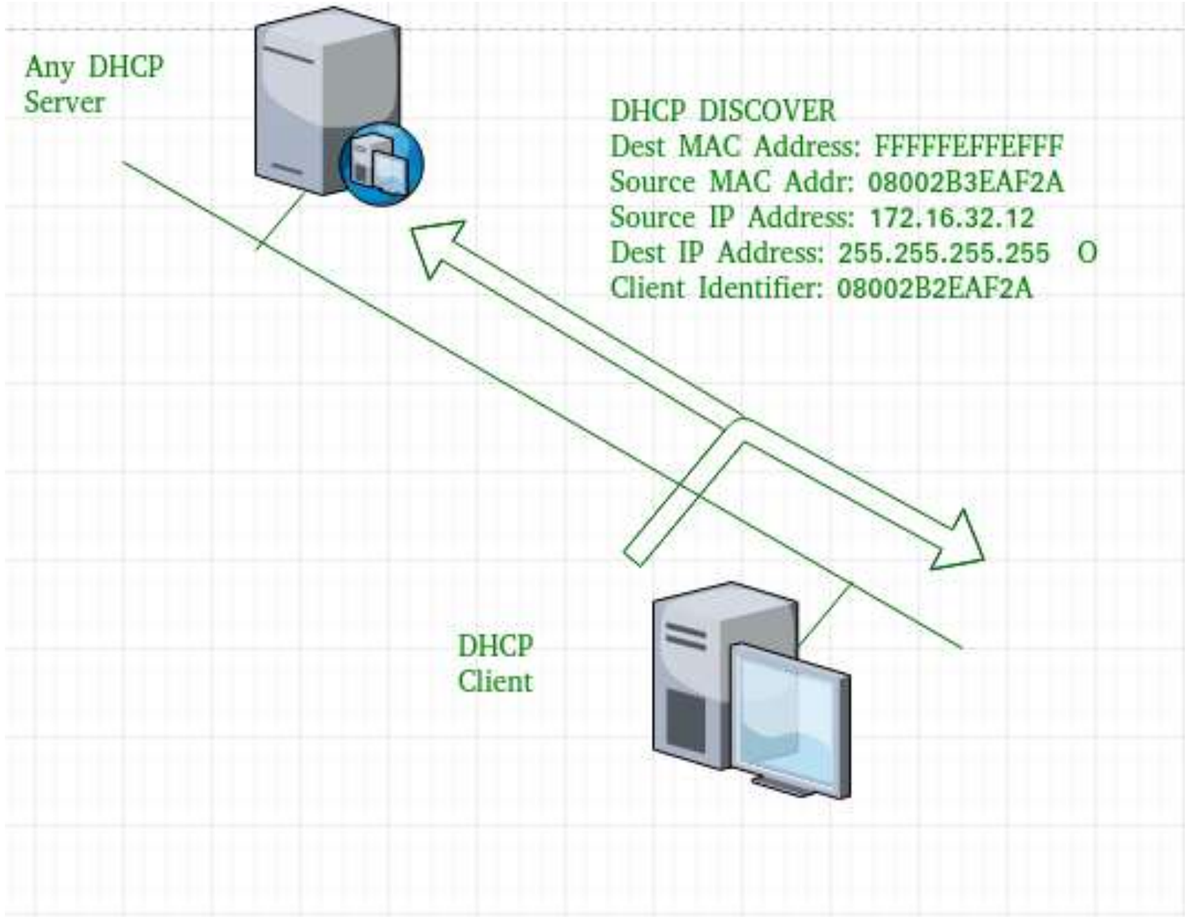
Automatic IP address assignment process undergoes four message exchange. These messages are abbreviated as Discover, Offer, Request & Acknowledgement (DORA).

# The following table gives the details of DORA messages -

| Message | Detail |
| --- | --- |
| Discover | This is message sent by DHCP client to discover a DHCP server. |
| Offer | Sent by DHCP server to lease unique IP address and other parameters needed to client. |
| Request | Sent by DHCP client asking server to lease parameters listed in Offer message. |
| Acknowledgement | Sent by DHCP server to assign IP address, mask, default router & DNS server address to client. |

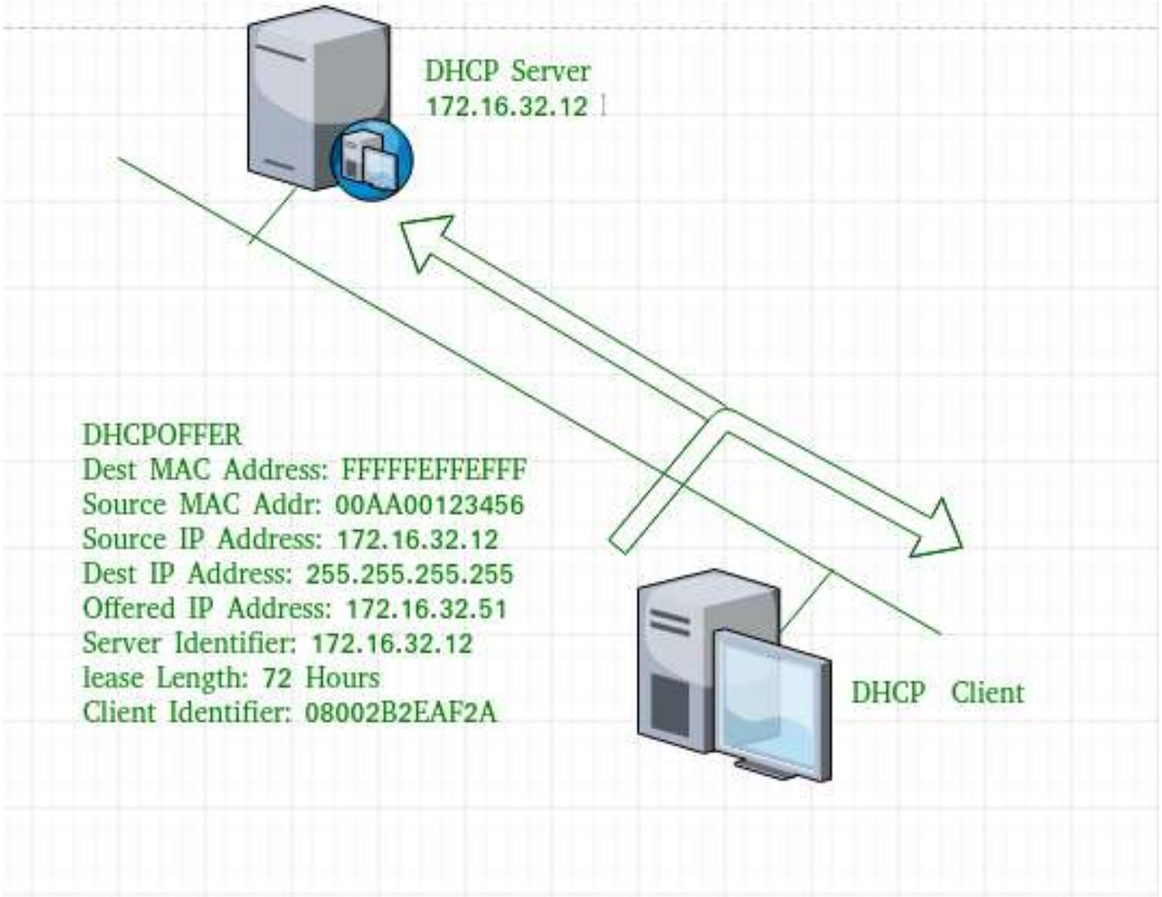
# DHCP discover message –

This is a first message generated in the communication process between server and client. This message is generated by Client to host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long



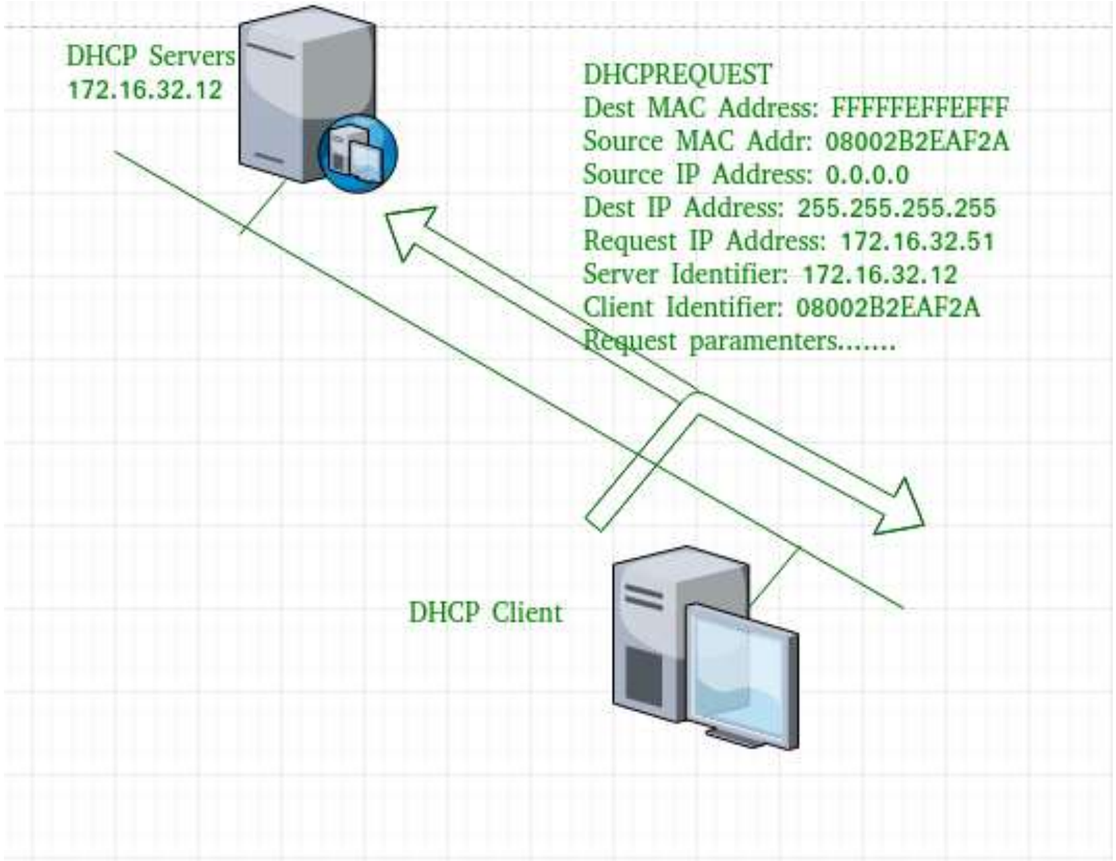
# DHCP offer message –

The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.



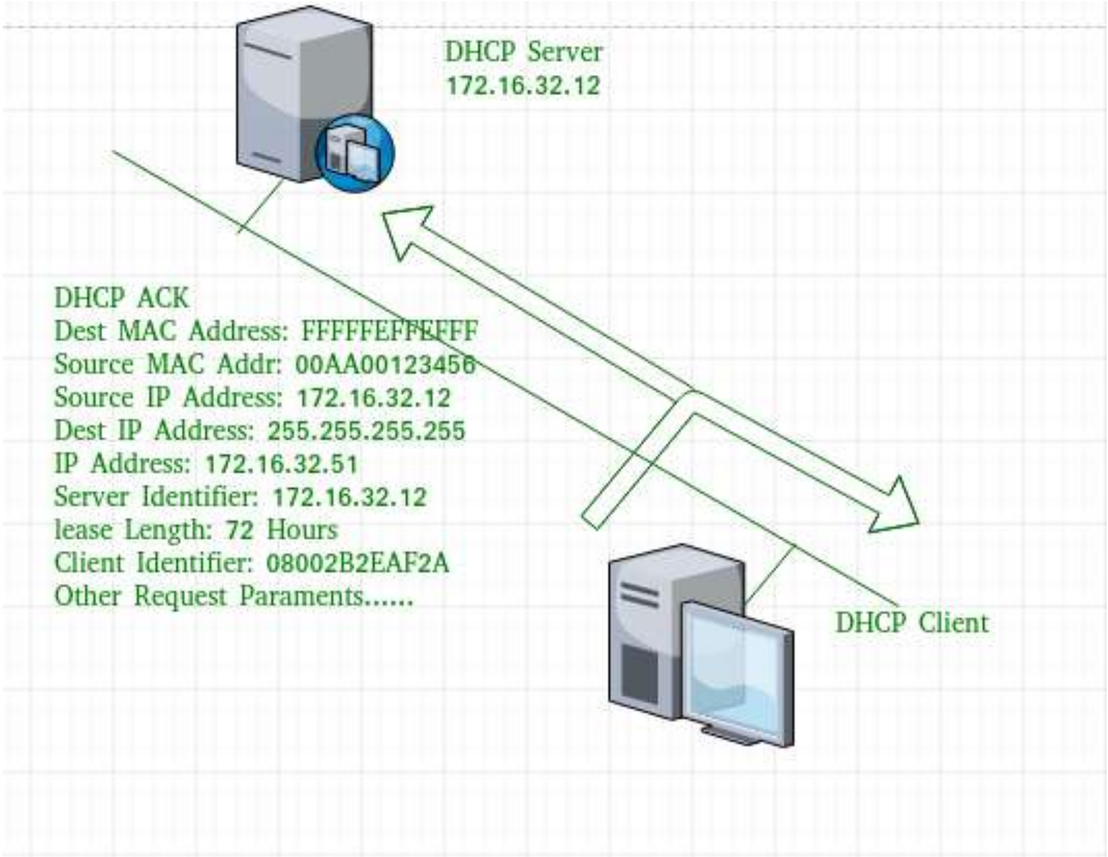
# DHCP request message –

When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address .A Client ID is also added in this message.



# DHCP acknowledgement message –

In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.



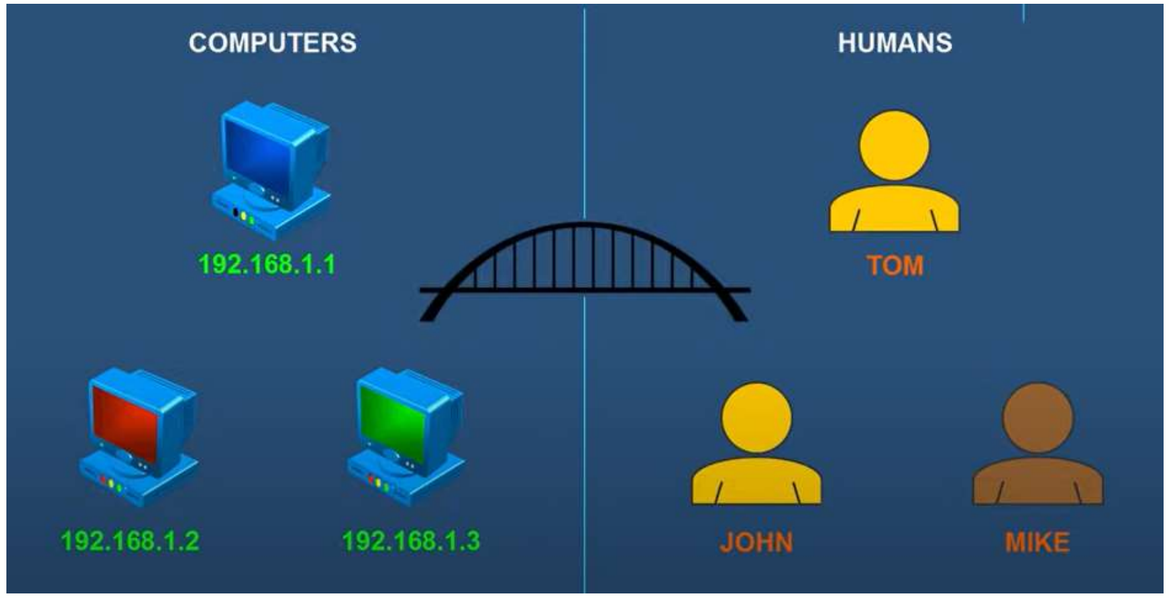
# The advantages of using DHCP include:

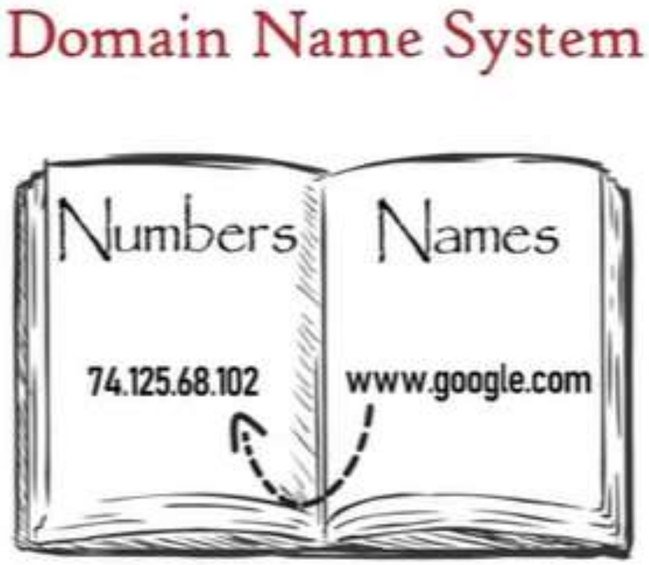
- Centralized management of IP addresses
- Ease of adding new clients to a network
- Reuse of IP addresses reducing the total number of IP addresses that are required
- Simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

# DNS SERVICE

# What is DNS?

- Domain name system
- Resolves domain names to IP addresses and vice  versa
- DNS is a application layer protocol
- DNS work on port number 53 and uses UDP and TCP



# Types of DNS Servers:

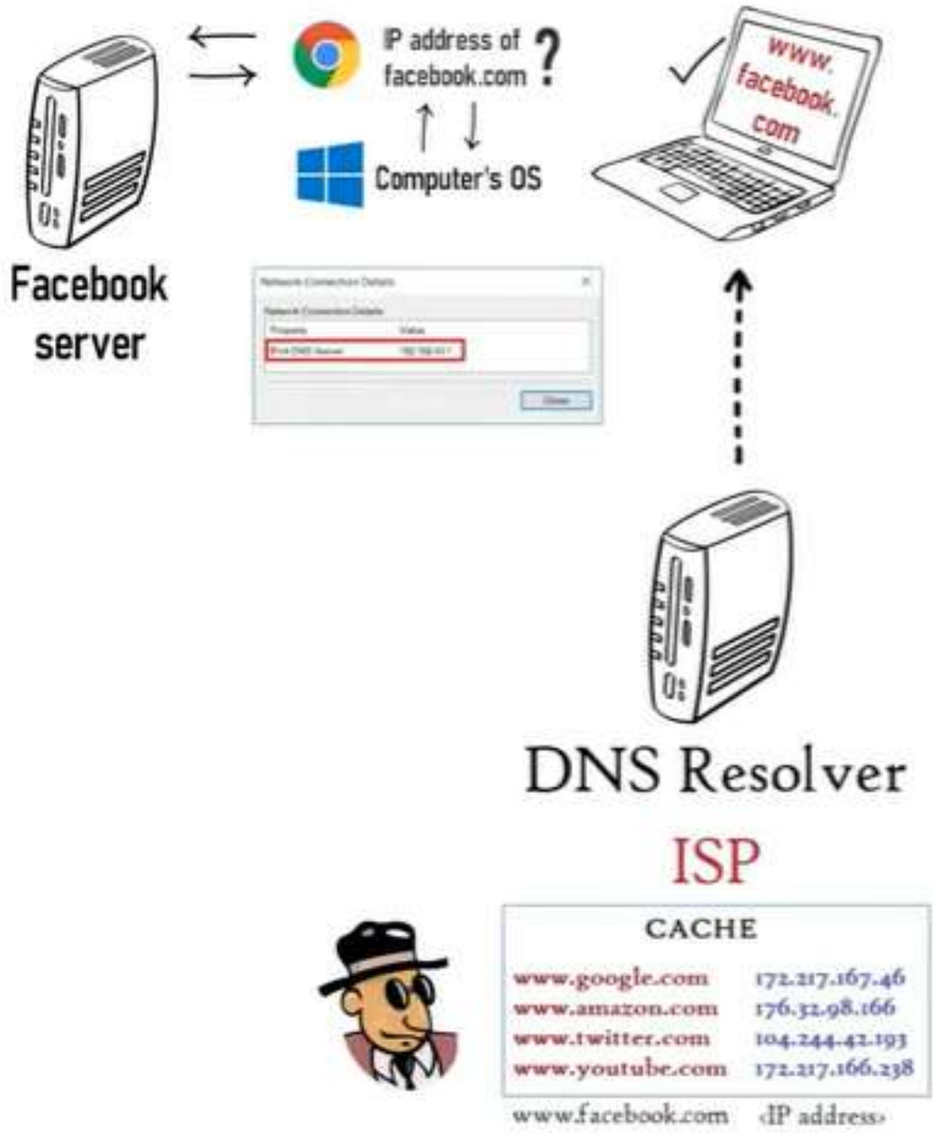
DNS recursive resolver/DNS resolver

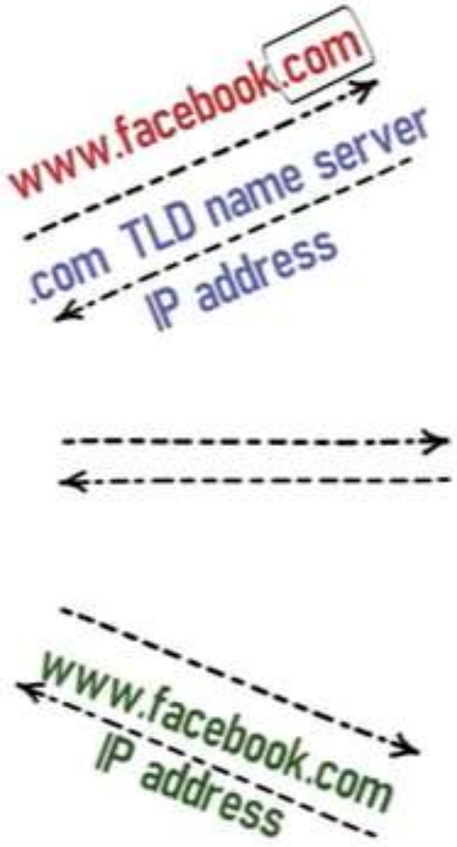
Root name server

Top Level Domain/TLD name server

Authoritative name server

# How a computer loads a website using DNS ?




Root name server

13 sets

letter.root-servers.net

www.root-servers.org

TLD name server

.com TLD name server

.net TLD name server

Authoritative name server

Last server in DNS

stores the website's IP address

# FTP AND TFTP

# 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. And in FTP, secure channel is provided to transfer the files between the hosts or systems. FTP works on two ports: 20 and 21 One for data and another is for connection control.

# TFTP

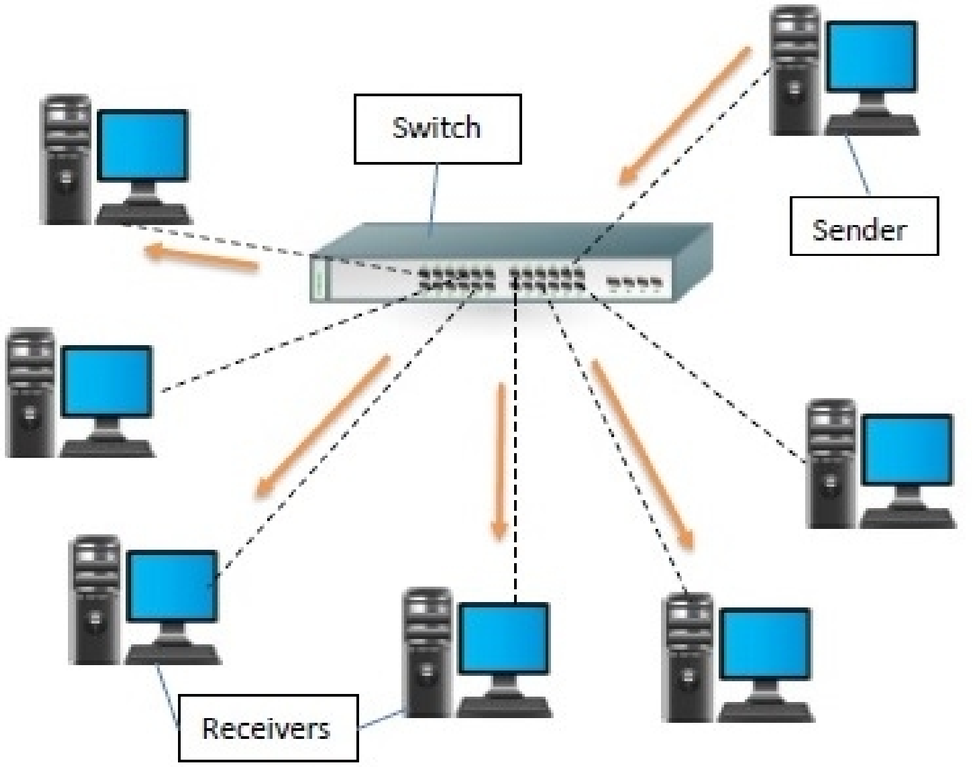
TFTP stands for Trivial File Transfer Protocol. TFTP is used to transfer a file either from client to server or from server to client without the need of FTP feature. Software of TFTP is smaller than FTP. TFTP works on 69 Port number and its service is provided by UDP.

| 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. |
| 9. | FTP is a reliable transfer protocol. | While; TFTP is an unreliable transfer protocol. |
| 10. | FTP is based on TCP. | While; TFTP is based on UDP. |
| 11. | FTP is slower. | TFTP is faster as compared to FTP. |

# Switch, VLAN, Switchport

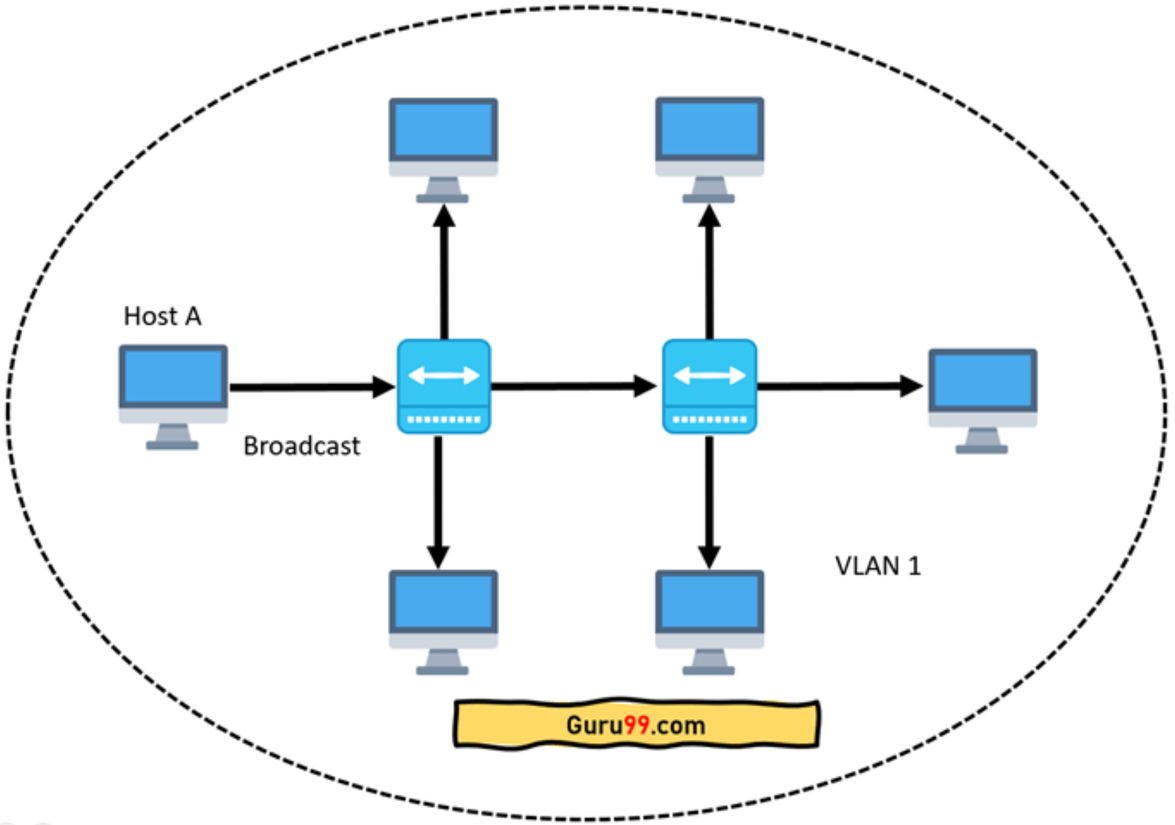
# SWITCH:-

1) It is a layer 2 device
2) It is an intelligent device
3) It has single broadcast domain
4) It has active port collision domain
5) Full duplex



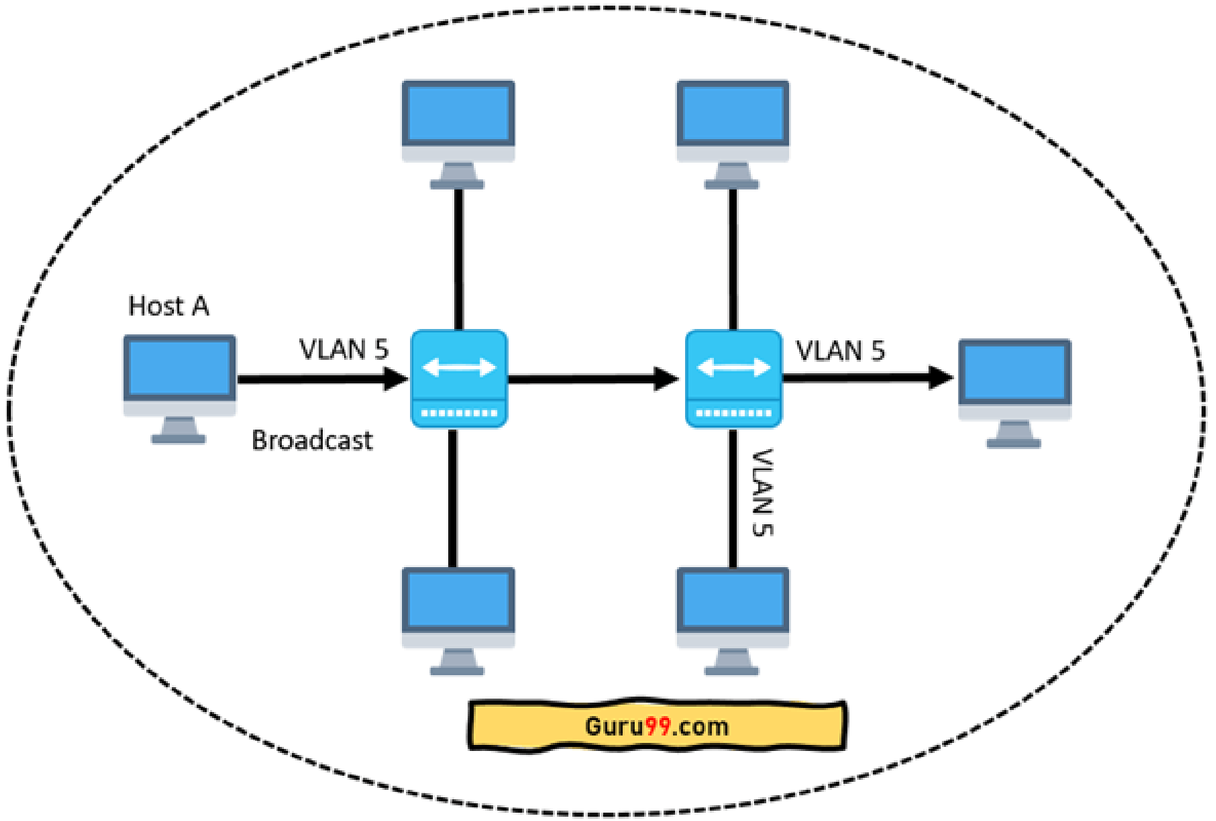
# What is VLAN?

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.



Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place.



VLAN in networking is a virtual extension of LAN. A LAN is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other applications.

## VLAN Ranges:-

| Range | Description |
|---|---|
| VLAN 0-4095 | Reserved VLAN, which cannot be seen or used. |
| VLAN 1: | This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used. |
| VLAN 2-1001: | It is a normal VLAN range. You can create, edit, and delete it. |
| VLAN 1002-1005: | These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN. |
| VLAN 1006-4094: | It is an extended range of VLANs. |

# Application/Purpose of VLAN

- VLAN is used when you have more devices on your LAN.
- It is helpful when you have a lot of traffic on a LAN.
- VLAN is ideal when a group of users need more security or being slow down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

# Advantages of VLAN

- VLAN reduces the size of broadcast domains.
- VLAN allows you to add an additional layer of security.
- It can make device management simple and easier.
- Higher performance and reduced latency.
- VLANs provide increased performance.
- VLAN removes the physical boundary.
- It lets you easily segment your network.
- It helps you to enhance network security.
- You can keep hosts separated by VLAN.
- You do not require additional hardware and cabling, which helps you to saves costs.

# What Is a Switch Port?

On a network switch, the switch port is the physical opening where a data cable can be plugged in. Generally, switch ports are rectangular on three sides with a V-shaped point on either the top or the bottom.

Types of ports in a switch:

a) Access Port

b) Switch Port

c) Hybrid Port

An **access port** connects a network host to a single VLAN and manages data traffic for that virtual network. Because data can only go back and forth on the designated VLAN, an access port handles untagged Ethernet frames.

A **trunk port** usually connects to another switch, and it's able to interact with several VLANs. On a complex network with multiple VLANs, a trunk port manages data transfer to and from those virtual networks. To do so, a trunk port recognizes frame tags that specify the intended destination for the data.

A **hybrid port** can function like both an access port and a trunk port. It can manage both tagged and untagged frames, and it can receive data from more than one VLAN. Both user devices and network devices can be connected through a hybrid port.

# Spanning-Tree Protocol and EtherChannel

# What is STP?

Spanning Tree Protocol (STP) is a switching protocol that prevents layer 2 loops created by the redundant links. STP enables switches to become well-informed of each other so that they can negotiate a Loop-Free path through the network.

# How Spanning Tree Protocol (STP) works?

STP chooses one of the switches in the network as a Root Bridge, which will be used as a reference point. Then calculates all the redundant paths to that root bridge, picks one path which is best to forward frames, and blocks other redundant paths.
Due to this redundant path blocking happens, switching Loops are prevented.

# What are BPDU messages?

All the switches switch over information to select the root bridge and for configuration of the network. This is done through the messages called Bridge Protocol Data Unit (BPDU). Each switch compares the parameters in the BPDU messages that it sends to one neighbor switch with the one that it receives from another neighbor switch.

# What are the Types of BPDU?

There are two types of BPDUs as below:-

1) Configuration – This Configuration BPDU is used for spanning-tree protocol (STP) assessment.

2) Topology Change Notification (TCN) – This TCN BPDU is used to state the changes in the network topology

# What is a Bridge ID?

Bridge ID is 8 bytes long. It includes both the priority and the MAC address of the device. In the STP domain, this bridge ID is used to elect the root bridge.

# How Root bridge is elected in the STP domain?

In the STP domain, the bridge with the lowest Bridge ID is elected as the root bridge. This means a switch with the lowest priority will elect as the root bridge, and if two or more switches have the same priority then switch with the lowest mac address will elect as the Root Bridge.

# What are the steps of STP working?

Following are the steps of STP working:

- Elect Root Bridge in the Network Topology.
    - Calculate Path cost and Root Path cost for every bridge. (Optional)
- Assign the Root Ports on Non-Root Bridges.
- Assign the Designated Ports on all the bridges.
- Assign the Non-Designated Ports.

# Explain different types of STP Port Roles?

**Root port** – The root port is always on Non-Root Bridge. It is always the port on the link directly connected to the root bridge, or the port on the link which is the shortest path to the root bridge. It is always in the forward state.

**Designated port** – A designated port can be on both the root Bridge & non-root Bridge. Also, all ports of the root bridge are designated port. A designated port is one that has the best (lowest) cost to the root bridge. It will be marked as a forwarding port.

**Forwarding port** – A forwarding port can send and receive i.e. forwards frames.

**Blocked port** – A blocked port is the port that is used to avoid the switching loops. It is also called a Non-designated port. It only listens to BPDU messages. Any port other than root & designated port is a blocked port.

# Explain different types of STP Timers?

STP uses three timers – 1) Hello 2) Forward Delay 3) Maximum Age timer. These timers make sure that a switched network converges properly before a bridging loop can form due to redundant links.

**Hello timer** – The time interval between configuration BPDU messages sent by the root bridge. It is 2 seconds by default.

**Forward Delay timer** – This is the time interval that a switch port spends in both the Listening and Learning states before going to forward state. The default value is 15 seconds.

**Max (Maximum) Age timer** – Maximum length of time a BPDU information can be stored before discarding it. It can also be defined as a time interval that a switch stores BPDU information without receiving an update. By default, it is 20 seconds.

# What are the different port states in STP?

**1. Disabled** – A port in the disabled state does not take part in the STP.

**2. Listening** – A port in the listening state sends and listens to BPDU messages to make sure no loops occur on the switched network. The port also arranges to forward data frames without populating the MAT – MAC address table.

**3. Learning**– A port in the learning state populates the MAC address table (MAT) but doesn't forward data frames. The port still sends and receives BPDU messages as in the listening state.

**4. Forwarding** – The port in the forwarding state can send and receive data frames, collect MAC addresses in its address table, send and receive BPDU messages. This port is now a fully functioning switch port within the spanning-tree topology.

**5. Blocking** – A port in the blocking state does not forward frames. It only listens to BPDU messages. The function of the blocking state is to prevent the use of looped paths.

## What is Root Port?

After the Root bridge is elected, every other Switch i.e. Non-Root bridge in the STP domain must select its single port to reach the Root bridge. The port with the lowest Root path cost is assigned as the root port. It is always in the forwarding state.

Only Non-Root bridges have a Root port and Root bridge will never have a root port.

# What is Path or Link or STP Path Cost value?

The Spanning Tree Path Cost Value is inversely correlated to the bandwidth of the link means low cost represents high bandwidth. Therefore a path with a low cost value is superior than a path with high cost value.

| *Bandwidth* | *Cost* |
|---|---|
| 4 Mbps | 250 |
| 10 Mbps | 100 |
| 16 Mbps | 62 |
| 45 Mbps | 39 |
| 100 Mbps | 19 |
| 155 Mbps | 14 |
| 1 Gbps | 4 |
| 10 Gbps | 2 |

# BPDU Guard and BPDU Filter

**BPDU Guard:-**

Once BPDU Guard is enabled it will keep an eye open for any BPDU's entering the access ports. Our main aim to have a predictable topology and not allow other switches outside our control onto our network. If a rogue switch is introduced into our topology it will in most cases transmit a BPDU, if the rogue switch has "better" values than the existing Root Bridge it will cause a topology change in the switched network. Any topology change is bad news for the users. By configuring the "BPDU Guard" feature on the access-ports enables the spanning-tree protocol to shut the port down in the event that it receives a BPDU packet.

**BPDU Filter:-**

BPDU filter on the other hand just filters BPDUs in both directions, which effectively disables STP on the port.Bpdu filter will prevent inbound and outbound bpdu but will remove portfast state on a port if a bpdu is received.

# Types of Layer 2 Protocols

| Protocol | Standard | Resources Needed | Convergence | Numbers of Trees |
|---|---|---|---|---|
| STP | 802.1D | Low | Slow | One |
| PVST+ | Cisco | High | Slow | One for every VLAN |
| RSTP | 802.1w | Medium | Fast | One |
| Rapid PVST+ | Cisco | Very high | Fast | One for every VLAN |

# What is EtherChannel?

The EtherChannel is a port link accretion technology or port-channel structural design used primarily on Cisco switches. EtherChannel allows assemblage of a number of real Ethernet links. By assembling them, it establishes a logical Ethernet link for the assurance of providing fault-tolerance and high-speed links. EtherChannel can be established between switches, routers and servers. A maximum of 8 Fast Ethernet or 8 Giga Ethernet ports can be assembled together when forming an EtherChannel.

# What are the available mechanisms for configuring EtherChannel?

There are 3 mechanisms you can choose to configure EtherChannel:

**1)Port Aggregation Protocol (PAgP):** This is the Cisco Proprietary Protocol. PAgP working modes are – Auto and Desirable.

**2) Link Aggregation Control Protocol (LACP):** This is the IEEE protocol with Standard 3ad. LACP working modes are – Passive and Active

**3) Static (On)**

# Trunking, Tagging, DTP and VTP

# Trunking

A trunk is a single channel of communication that allows multiple entities at one end to correspond with the correct entity at the other end. It is a “link” that carries many signals at the same time, creating more efficient network access between two nodes.

With VLAN trunking, it’s possible to extend a VLAN across the network. When you implement multiple VLANs across a network, trunk links are necessary to ensure that VLAN signals remain properly segregated for each to reach their intended destination. This is also more efficient, as multiple VLANs can be configured on a single port.

| ISL | IEE 802.1Q |
| --- | --- |
| Cisco standard | Does not modify Ethernet frame |
| Adds a 26-byte header and 4-byte trailer | Industry standard |
| | Adds a 4-byte tag in the middle of original Ethernet frame |
| | Native VLAN frames are not tagged while traversing over trunk links |

# DTP: Dynamic Trunking Protocol,

DTP, Dynamic Trunking Protocol, is a trunking protocol that is developed and proprietary to Cisco which is used to automatically negotiate trunks between Cisco switches. Trunk negotiations are managed by DTP only if the port is directly connected to each other.

Ethernet trunk interfaces support various trunking modes. Those interfaces can be configured as a trunk or non-trunk, or to initiate negotiating trunking to a neighbor interface or is waiting to receive a trunking negotiation message from another directly connected interface. Most Cisco switches nowadays use IEEE 802.1Q as their trunking type of choice because of less overhead compared to Inter-Switch Link (ISL).

# DTP switchport modes

Switchport mode access – an access port does not act as a trunk interface and only allows one VLAN through that port. An interface in access mode becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.

Switchport mode trunk – the trunk mode enables the interface to be set in permanent trunking mode and establishes negotiations to convert the neighboring link to become a trunk link though the switch interface becomes a trunk even if the neighbor interface is not.

Switchport mode dynamic auto – this DTP mode makes the interface passively waits to receive a negotiation message to make itself a trunk, at which point the switch will respond and negotiate whether to use trunking. The switch interface becomes a trunk port if the neighboring interface is set to trunk or dynamic desirable mode.

Switchport mode dynamic desirable – this DTP mode lets the port to initiates trunking with another port by sending a negotiation message to dynamically choose whether to start using trunking. The interface becomes a trunk port if the neighboring interface is set to trunk mode, dynamic desirable mode, or dynamic auto mode.

Switchport nonegotiate – this command disables Dynamic Trunking Protocol.

| Switchport Mode | dynamic desirable | dynamic auto | trunk | access |
|---|---|---|---|---|
| dynamic desirable | trunk | trunk | trunk | access |
| dynamic auto | trunk | access | trunk | access |
| trunk | trunk | trunk | trunk | access |
| access | access | access | access | access |

# VLAN Trunking Protocol (VTP) –

VTP is CISCO proprietary protocol used to maintain consistency throughout the network or user can say that synchronizing the VLAN information in same VTP domain. VTP allows you to add, delete and rename VLANs which is then propagated to other switches in the VTP domain. VTP advertisements can be sent over 802.1Q, and ISL trunks.

Requirements –

1. The VTP version must be same on the switches user wants to configure
2. VTP domain name must be same on the switches
3. One of the switches must be a server
4. Authentication should match if applied

# VTP modes – There are 3 modes:

1) Server – The switches are set to this mode by default. This mode allows you to create, add and delete VLANs. The changes you want to made should be done in this mode. Any changes that is done on this mode(on a particular switch) will be advertised to all the switches that are in same VTP domain.

2) Client – In this mode, the switches receives the updates and can also forward the updates to other switches(which are in same VTP domain). The updates received here is not saved in NVRAM so all the configuration will be deleted if the switch is reset or reloaded i.e the switches will only learn and pass the VTP summary advertisements to the other switches.

3) Transparent – This mode only forwards the VTP summary advertisements through trunk link. The transparent mode switches can make their own local database which keep secret from other switches. The whole purpose of transparent mode is to forward the VTP summary advertisements but not to take part in the VLAN assignments.

# QOS and VPN

# Quality-of-Service (QoS)

Quality of Service (also known as QoS) is a set of technologies, tools and approaches that you can apply to a network. The goal of QoS is to guarantee the network's ability to reliably run applications and traffic despite limited capacity. Some QoS tools and technologies do their jobs by handling different packets differently, throttling bandwidth in certain circumstances, and changing priorities on the fly.

# What Are the Categories of Quality of Service Technologies?

There are six categories of Quality of Service technologies:

Classification

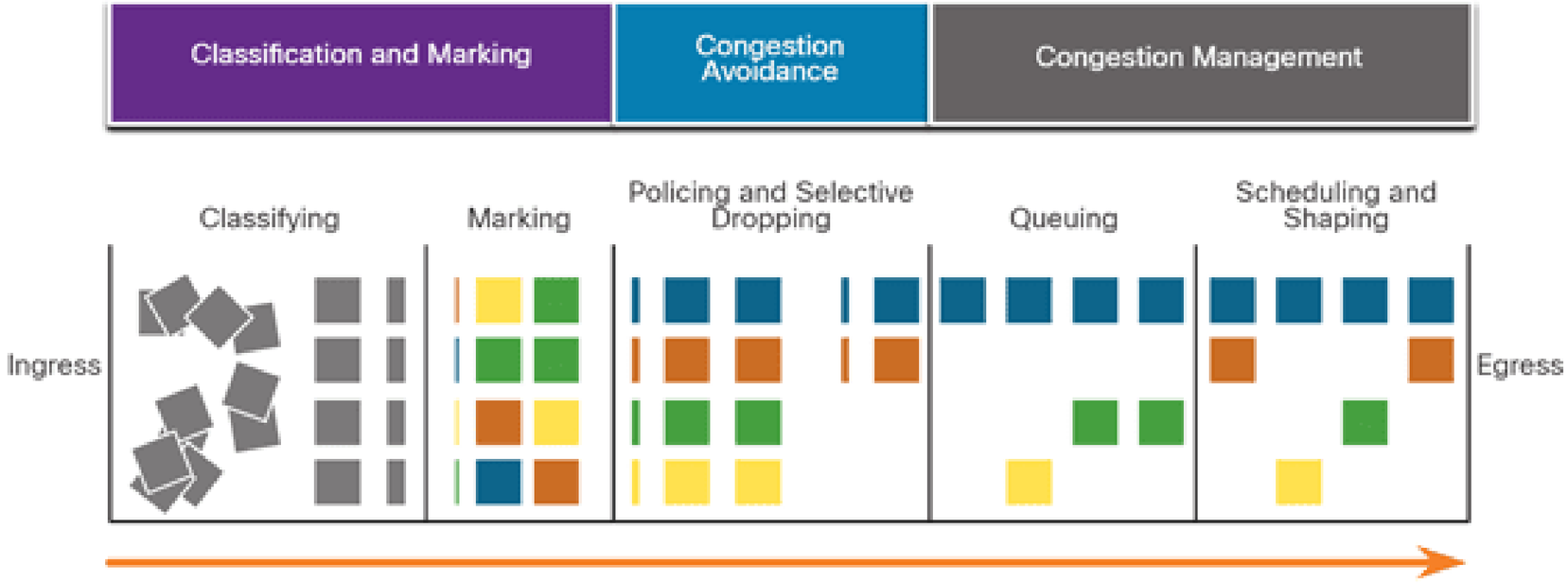
Marking,

Policing

Shaping

Congestion Avoidance

Queuing



## What is Classification in QoS?

Classification is at the core of QoS. Classification is the ability for a device to identify different traffic types so you can properly prioritize one over the other.

## What is Marking in Quality of Service?

Marking is actually one of the optional ones. Marking involves tagging a packet as it enters the router so that subsequent devices can recognize the traffic without needing to spend processor time inspecting it.

## What is QoS Policing?

Quality of Service Policing allows you to set an upper limit, and when traffic hits that amount, the tool cuts the traffic and doesn't allow any more.

## What is Shaping in Quality of Service?

Shaping is a little bit like Policing, but it's a kinder, gentler version. Shaping is for traffic that we care about. Policing might kill the packets to save bandwidth. But Shaping tools hold the excess data in memory and try to transmit it at a later time.

## What is QoS Congestion Avoidance?

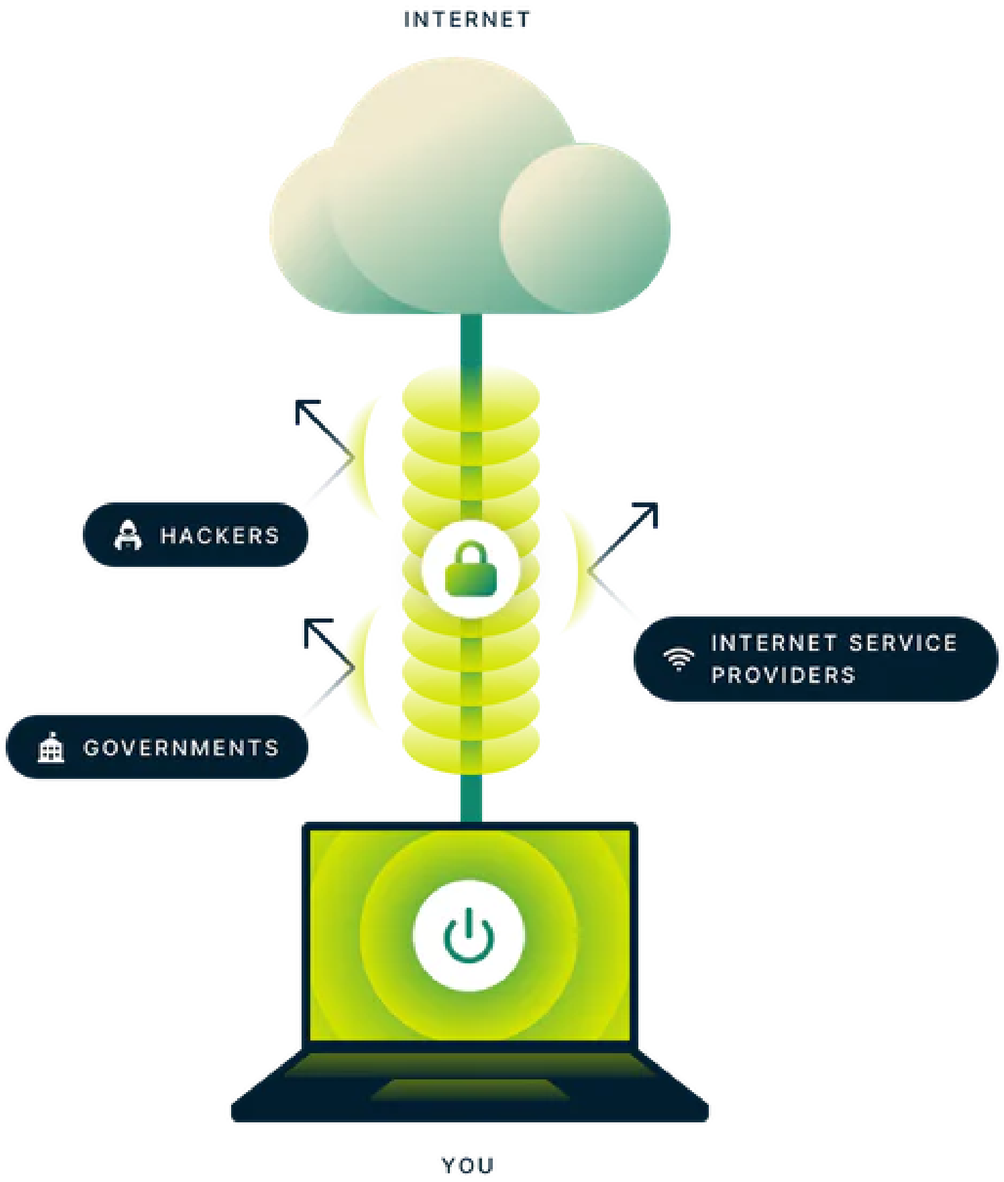
Congestion Avoidance QoS tools shut down the possibility of congestion by watching for certain limits on a router and then taking action. As a router's traffic builds up, Congestion Avoidance tools look for the devices that run the highest risk of consuming the entire bandwidth amount.

## What is Queuing in Quality of Service?

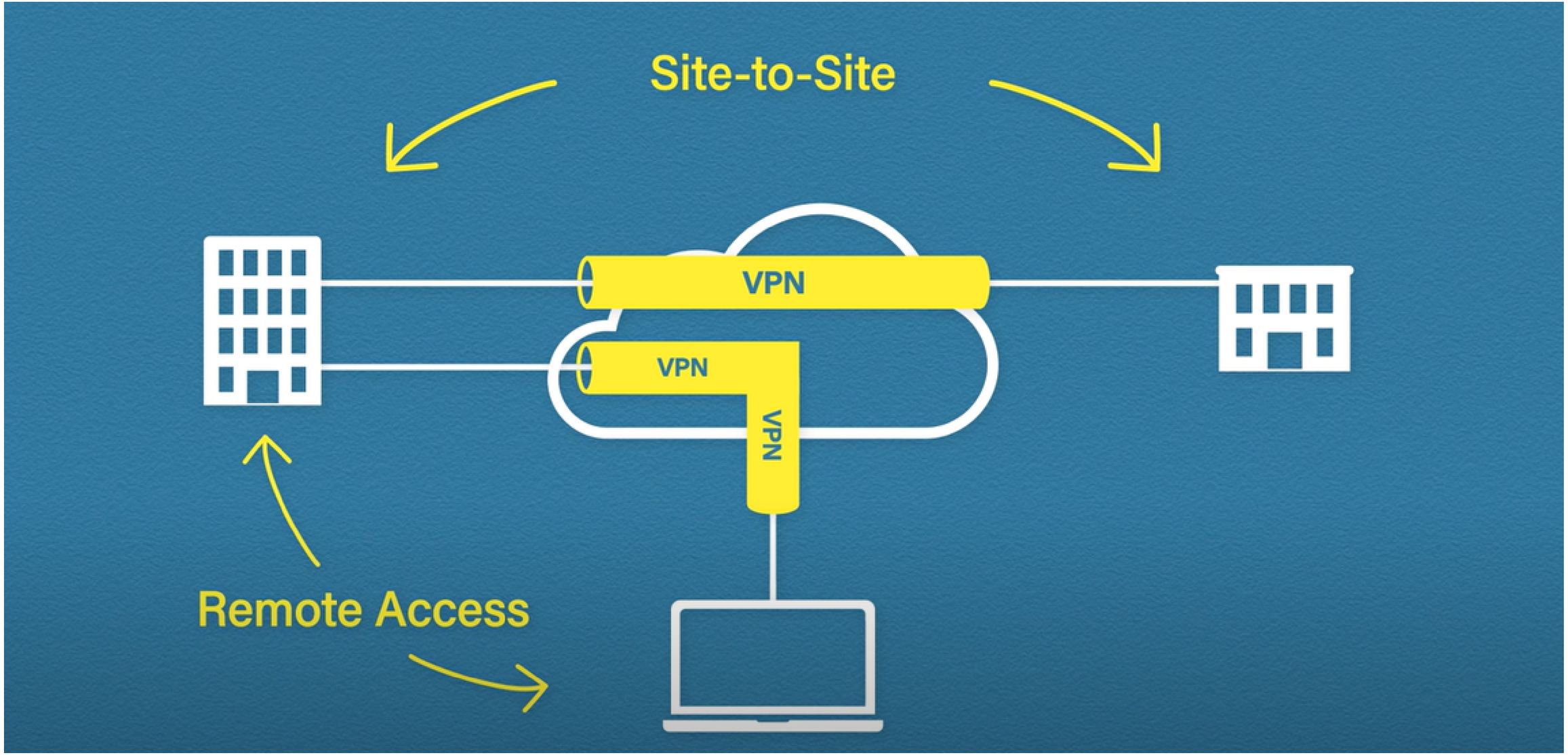
With Queuing tools, you can instruct a router to shuffle packets around to put the most important traffic first.

# What is a VPN?

A VPN (virtual private network) is the easiest and most effective way for people to protect their internet traffic and keep their identities private online. As you connect to a secure VPN server, your internet traffic goes through an encrypted tunnel that nobody can see into, including hackers, governments, and your internet service provider.



# Site-to-site and Remote Access VPN



| S.NO | Site to site VPN | Remote access VPN |
|---|---|---|
| 1. | In site to site VPN, IPsec security method is used to create an encrypted tunnel from one customer network to remote site of the customer. | In remote access VPN, Individual users are connected to the private network. |
| 2. | Site to site VPN does not need setup on each client. | Remote access VPN may or may not needed setup on each client. |
| 3. | Site to site VPN does not require every user to initiate the VPN tunnel setup. | Remote access VPN require every remote access user to initiate the VPN tunnel setup. |
| 4. | Site to site VPN supports IPsec technology. | While Remote access VPN supports SSL and IPsec technology. |
| 5. | In site to site VPN, multiple users are not allowed. | In remote access VPN, multiple users are allowed. |

# Types of VPN encryption

**Symmetric-key:**
This is where the key for encryption and decryption is the same, and both communicating parties must possess the same key in order to communicate.

**Public-key:**
Here, software is used to create sets of public and private keys. The public key is used to encrypt data, which is then sent to the owner of the private key. They then use this private key to decrypt the messages.

**Handshake encryption (RSA)**
This is typically done through the RSA (Rivest-Shamir-Adleman) algorithm, which has essentially been the foundation of internet security for about two decades.

**Secure Hash Algorithm (SHA):**

In this process, a unique fingerprint is created to validate the TLS certificate – that is, to check you're connecting to the server you're supposed to be. Without this, a hacker could re-route your traffic to their own server instead of your VPN provider's.

## VPN Protocols:

1) SSL and TLS - Secure Socket Layer and Transport Layer Security
2) OpenVPN
3) IKEv2 - Internet Key Exchange version 2
4) L2TP - Layer 2 Tunnelling Protocol
5) SSTP - Secure Socket Tunnelling Protocol
6) WireGuard
7) PPTP - Point-to-Point Tunnelling Protocol (PPTP)

# SNMP, Syslog and AAA

# What is SNMP?

Simple Network Management Protocol (SNMP) is an Internet Standard protocol used for monitoring and managing network devices connected over an IP. SNMP collects data from different network devices like routers, switches, firewalls, printers, servers, CCTV cameras, and wireless access points that are SNMP enabled and organizes them. With a set of operational standards for management, SNMP aids in network fault detection and analysis. Thus, SNMP is an integral part of interoperability between both the monitored and the monitoring systems. SNMP generally uses User Datagram Protocol (UDP) port number 161/162. The Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) protocols are also used at times.

# Why do you need SNMP monitoring tools?

Network admins generally manage the devices in a network and allocate and free up ports and interfaces to ensure continuous uptime and bandwidth-hog-free network operations. Closely monitoring SNMP devices is a major part of this. SNMP monitoring requires an admin to configure the SNMP agent to send the monitoring data to an SNMP manager. Since the network management tool takes care of monitoring, admins can focus on performing corrective measures.

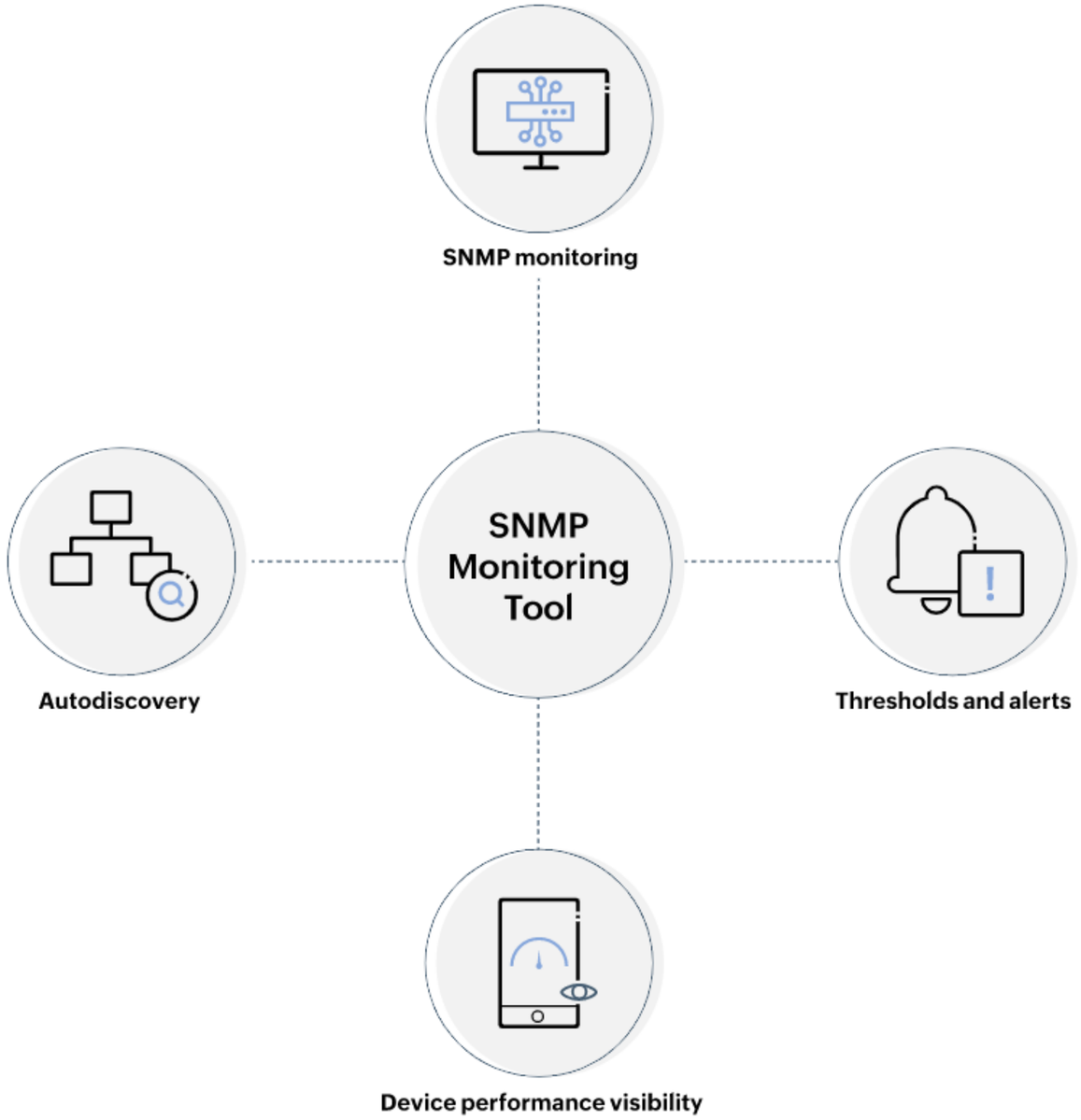
SNMP monitoring tools are necessary to:

1) Automatically discover, monitor, and manage network devices.

2) Monitor key performance metrics at the device and interface level.

3) Obtain complete visibility and granularity into the performance of network devices.

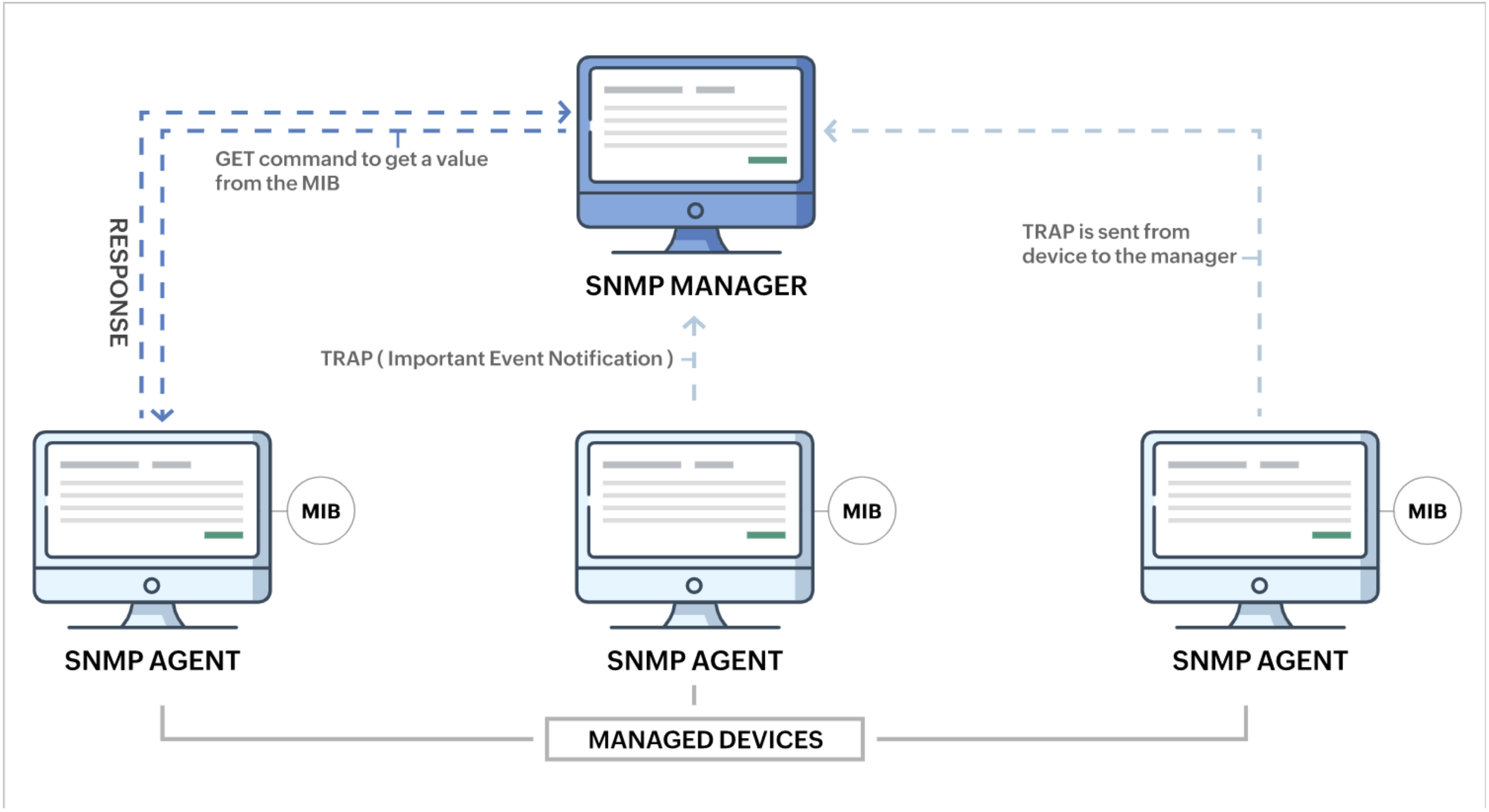
4) Configure threshold limits and generate alerts in case of anomalies.



# How does SNMP work?

Traffic flows across your network from different sources. SNMP communicates with the whole network and the devices in it. As mentioned earlier, SNMP is preconfigured on devices, and once the protocol is enabled, the devices will store their performance stats. Each network server will have multiple MIB files. The device MIB files are queried to fetch the monitoring data. The working of SNMP revolves around its components, wherein each component contributes management of resources.

SNMP works by sending protocol data units, also known as SNMP GET requests, to network devices that respond to SNMP. All these communications are tracked, and network monitoring tools use them to fetch data from SNMP.


GET command to get a value from the MIB
RESPONSE
SNMP MANAGER
TRAP is sent from device to the manager
TRAP ( Important Event Notification )
MIB
MIB
MIB
SNMP AGENT
SNMP AGENT
SNMP AGENT
MANAGED DEVICES

# What are the components of SNMP?

SNMP manager

The SNMP manager is the central system used to monitor the SNMP network. Also known as a network management station (NMS), an SNMP manager is responsible for communicating with the SNMP-agent-implemented network devices. It runs on a host on the network. The manager queries the agents, gets responses, sets variables in them, and acknowledges events from them.

Managed devices

A managed device is an SNMP-enabled network entity that is managed by the SNMP manager. These are usually routers, switches, printers, or wireless devices.

## SNMP agent

An SNMP agent is a software process that responds to SNMP queries to provide status and statistics about a network node. SNMP agents play the most important role in management. They are locally located and associated with SNMP network devices from which they collect, store, and transmit monitoring data. Data is transmitted to the designated SNMP manager when queried.

## SNMP MIB

A management information base (MIB) forms an integral part of network management models. An SNMP MIB is a structure that defines the format of information exchange in an SNMP system.

## SNMP OID

Object Identifiers (OIDs) are identifiable by strings of numbers separated by dots.

# SNMP VS SYSLOG PROTOCOL

| S.No. | SNMP | SYSLOG |
|---|---|---|
| 1 | SNMP allows for remote monitoring of SNMP-Allowable device on network. | SYSLOG is a different protocol that can be used for exchanging log messages of varying degrees of severity to network device capable of receiving syslog messages. |
| 2 | SNMP is used to alert on critical actions, like the mentioned HSRP state changes. | SYSLOG is also collected, which allows me to dig deeper to figure out why the HSRP state change occurred. |
| 3 | SNMP works on Poll – Resource mechanism with SNMP Server polling the device for response on interface/ health /process. | SYSLOG works on PUSH mechanism on end device to send logging information. |
| 4 | SNMP is referred to get real time information. | SYSLOG is generally referred to acquire historical data. |
| 5 | End device configuration can be performed via SNMP set. E.g.: Reboot system | End device configuration cannot be performed via syslog set. |
| 6 | SNMP traps are shared in binary format. | Syslog events are shared in plain text. |
| 7 | Secure | Insecure |
| 8 | Active | Passive |
| 9 | Uses UDP port numbers 161 and 162. | Uses TCP/UDP port number 514 |

# What is AAA in networking?

AAA is a standard-based framework used to control who is permitted to use network resources (through authentication), what they are authorized to do (through authorization), and capture the actions performed while accessing the network (through accounting).

**1) Authentication –**

The process by which it can be identified that the user, which wants to access the network resources, valid or not by asking some credentials such as username and password. Common methods are to put authentication on console port, AUX port, or vty lines. As network administrators, we can control how a user is authenticated if someone wants to access the network.

**2) Authorization –**

It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

**3) Accounting –**

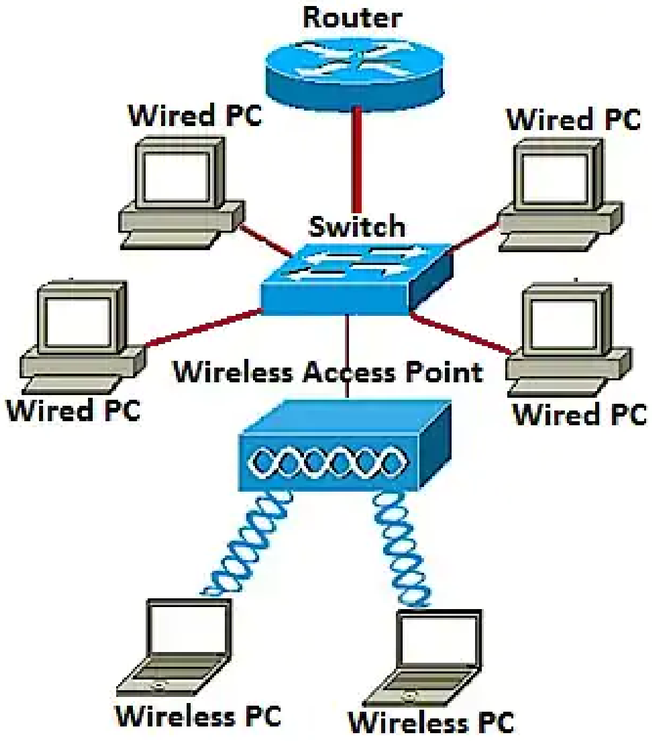
It provides means of monitoring and capturing the events done by the user while accessing the network resources. It even monitors how long the user has access to the network. The administrator can create an accounting method list to specify what should be accounted for and to whom the accounting records should be sent.

**Radius/Tacacs/Tacacs+ are few protocols of AAA framework to provide centralized authentication for users.**

# WAP, WLC and Wireless Security Protocols

# What is an Access Point?


A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables. An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.



# Advantages of Using Wireless Access Points

When you have both employees and guests connecting with desktops, laptops, mobile phones, and tablets, 20 devices on a wireless network adds up quickly. At 60 simultaneous connections each, access points give you the freedom to scale the number of devices supported on your network. But that's only one of the advantages of using these network enhancers—consider these points:

1) Business-grade access points can be installed anywhere you can run an Ethernet cable. Newer models are also compatible with Power over Ethernet Plus, or PoE+ (a combination Ethernet and power cord), so there is no need to run a separate power line or install an outlet near the access point.

2) Additional standard features include Captive Portal and Access Control List (ACL) support, so you can limit guest access without compromising network security, as well as easily manage users within your Wi-Fi network.

3) Select access points include a Clustering feature—a single point from which the IT administrator can view, deploy, configure, and secure a Wi-Fi network as a single entity rather than a series of separate access point configurations.

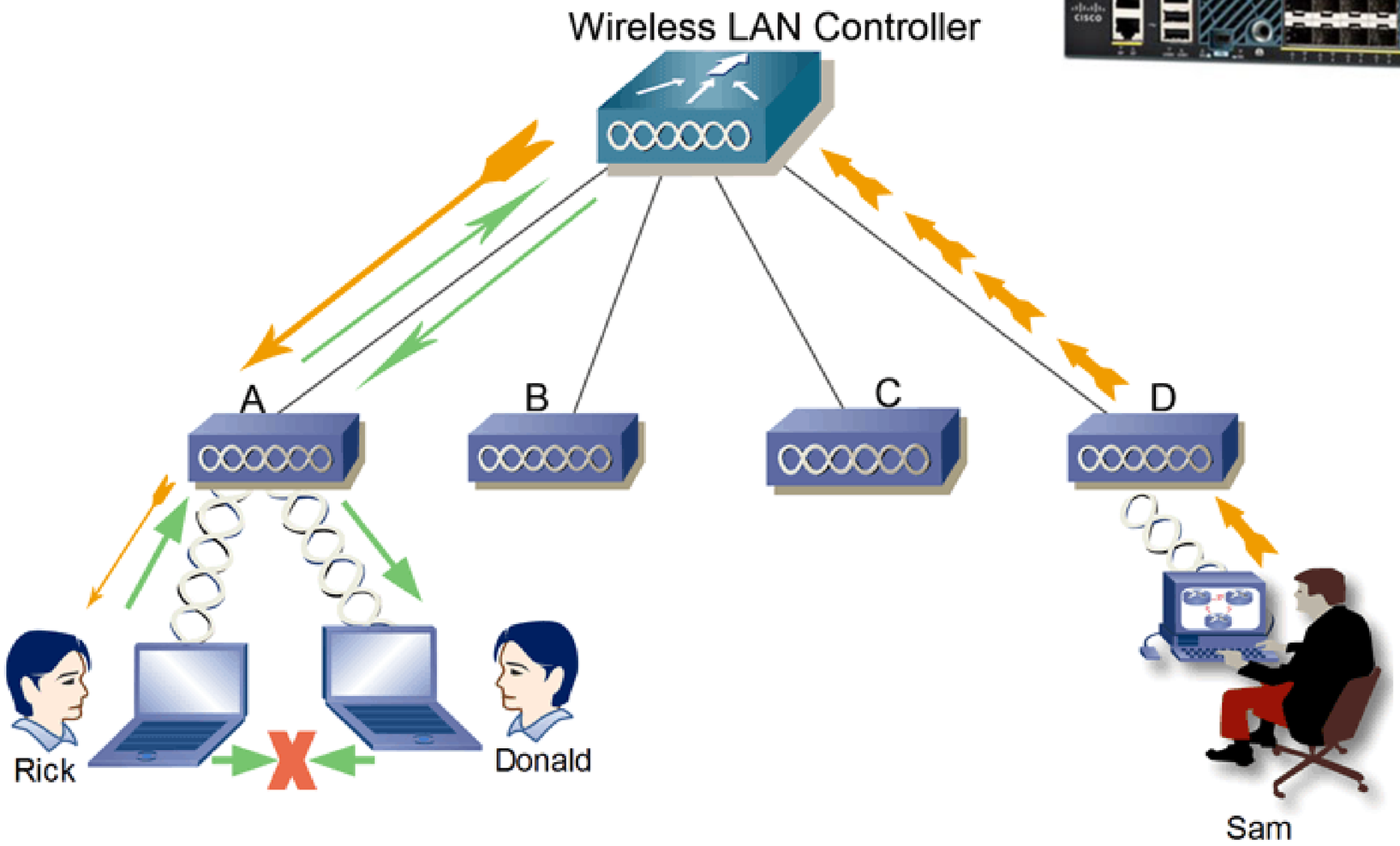
# What Is a Wireless LAN Controller (WLC)?

A Wireless LAN Controller (WLC) is a centralized device in the network which is used in combination with the Lightweight Access Point Protocol (LWAPP) to manage lightweight access points in large quantities by the network administrator or network operations center.

Also called “fat” access points, these access points on the network are managed, operated, and configured independently. The WLC automatically handles the configuration of wireless access points.

Because of its centralized position and brainpower, the Wireless LAN Controller is aware of the wireless LAN environment. It provides services that can lower the price of deployment, ease the management process, and provide several layers of security.

# Cisco Wireless Controller



# Functions of Wireless LAN Controller

**1) Traffic aggregation and processing for wireless devices function:**

When all traffic from wireless devices is routed via the controller, you can use it to encode it or divide it so that is sent to different networks or to be filtered to prioritize it according to the established quality policies.

**2) Management and operation function:**

These two functions enable you to utilize and manage the wireless local network in a much simpler manner.

**3) Local wireless function:**

In the case of the radio features of wireless technology, it is preferable to utilize the coordination and protection mechanisms in the radio spectrum for more efficient use in a particular area.

# Benefits of a Wireless LAN Controller

1) **It is secure**. With all the daily news about hacking and data breaches, security is an essential factor to have in mind for any organization. Wireless LAN Controller (WLC) fights against all kinds of threats to your organization based on user ID and location thanks to built-in security characteristics.

2) **It is centralized**. A centralized wireless controller provides malleability for deployment, which will lower the budget, planning instruments, and time spent organizing a wireless network in the business.

3) **It is simple**. Having a Wireless LAN Controller (WLC) will help you to administer and supervise your access points in the centralized hub.

# Wi-Fi Security Protocol Types Explained

**WEP—The first Wi-Fi Security Protocol:**

WEP stands for Wired Equivalent Privacy, and it was the first Wi-Fi security protocol approved in September 1999. It was initially expected to deliver the same security level as wired networks. A secondary function of WEP is said to prevent unauthorized access to a wireless network. However, it has been found that WEP is not as secure as desired. WEP is used at the two lowest layers of the OSI model – the data link and physical layers; it therefore does not offer end-to-end security. Nevertheless, at that time, cryptographic technology was restricted and the Wi-Fi devices were limited to 64-bit encryption. Even though the limitation was broken through and increased to 128-bit, there were also many security issues in WEP that made the keys easy to crack. WEP was a highly vulnerable wireless security protocol. IT was finally replaced by WPA.

**WPA—Temporary Enhancement for WEP:**

In 2003, as WEP gradually performed its weakness, WPA was adopted by the Wi-Fi Alliance as an alternative for WEP. 256-bit encryption technology was introduced to WPA, which is an obvious increase compared with the 64-bit and 128-bit encryption in the WEP system. In the WPA standard, there is a diversity between the two modes: WPA-Enterprise and WPA-Personal, which use different encryption methods. WPA-Personal is a common method to secure wireless networks, and it is suitable for most home networks. WPA-Enterprise provides the security needed for wireless networks in business environments where a RADIUS server is deployed.

**WPA2—Improvement Based on WPA:**

WPA2 was ratified as the new Wi-Fi security standard in 2004. The most significant improvement in the WPA2 security standard is the implementation of the Advanced Encryption Standard (AES), which provides higher security and performance.

There is still a vulnerability that brings security problems because a hacker can get access to a secured WPA2 network and get access to certain keys to attack other devices on the same network. It is a security issue that matters for enterprise networks, instead of home network users.

**WPA3—The Next-Generation Wi-Fi Security:**

With the aim to “simplify Wi-Fi security, enable more robust authentication and deliver increased cryptographic strength for highly sensitive data markets”, WPA3 was proposed by the Wi-Fi Alliance in June 2018. The advent of WPA3 remedies the protection against the flaws in WPA2 such as dictionary attacks. For public networks such as coffee shops or hotels, WPA3 has really good security because it will automatically encrypt the connection without any needs for credentials.

# IPv6 and Campus Networks

# Total number of  IP addresses in IPv4

4,294,967,296

# Total number of  IP addresses in IPv6

340,282,366,920,938,463,463,374,607,431,768,211,456

# IPv4 vs IPv6 size difference

# Octets, Hextets, dots and colons

# IPv6 converted to binary

2001:0db8:0000:0000:a111:b222:c333:abcd

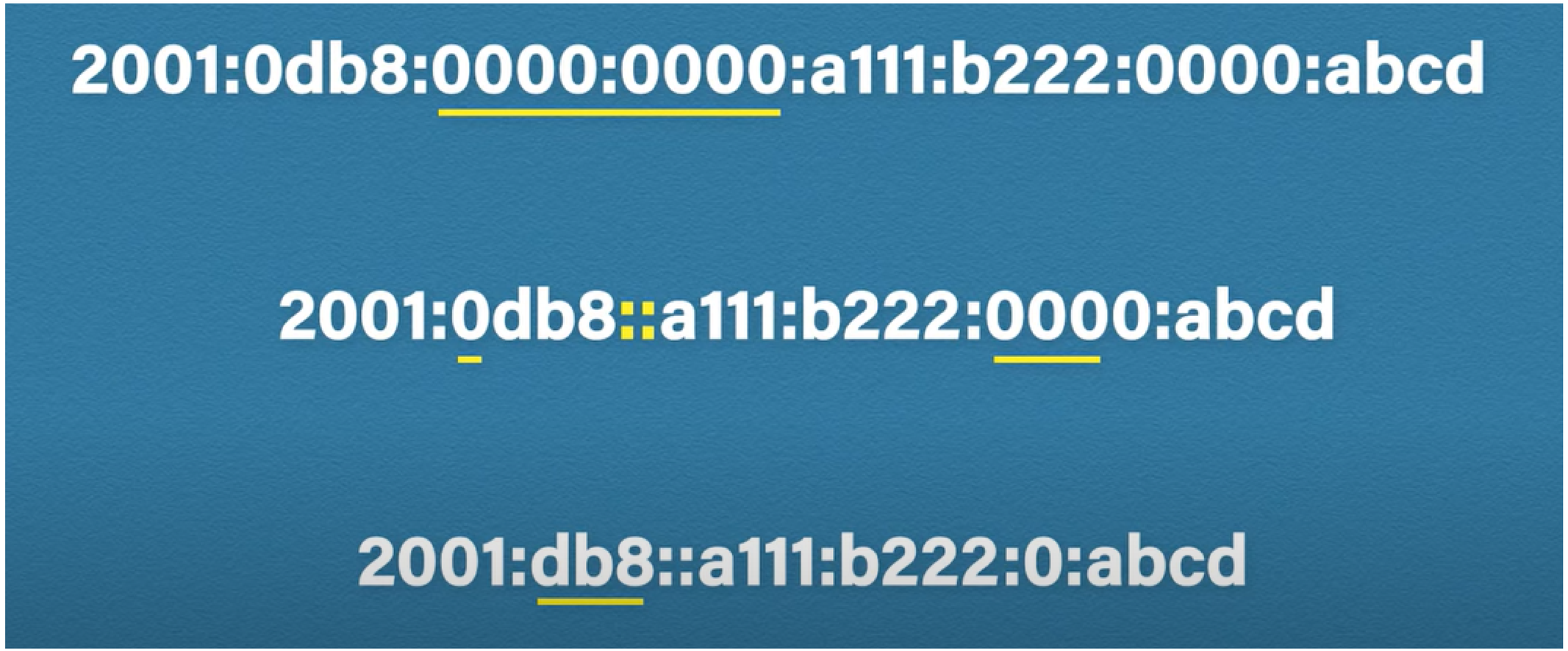
0010000000000001 0000110110111000 0000000000000000 0000000000000000 1010000100010001 1011001000100010 1100001100110011 1010101111001101

# Network Bit and Host Bit

NETWORK HOST

2001:0db8:0000:0000 a111:b222:c333:abcd /64

# IPv6 Shortening



# Types of addresses in IPv6

| | | |
|---|---|---|
| **GLOBAL UNICAST** | 2000::/3 | Publicly routable |
| **UNIQUE LOCAL** | FC00::/7 | Routable in the LAN |
| **LINK LOCAL** | FE80::/10 | Not routable |
| **MULTICAST** | FF00::/8 | Addresses for groups |
| **ANYCAST** | 2000::/3 | Shared address |

# Conversion of MAC address to Link Local Address

1) Add FFFE in the mid of mac-address
2) Inverse the 7th bit and convert to decimal
3) Add FE80 in starting
4) Remove the dots and group them
5) Add (:) after first segment

# Feature of IPv6

1) No broadcast traffic
2) Auto config for stateless and stateful
3) Mobility support
4) No NAT/PAT required but can do
5) Has native support for IPsec
6) Improved header
7) Anycast Support

# Campus Networks

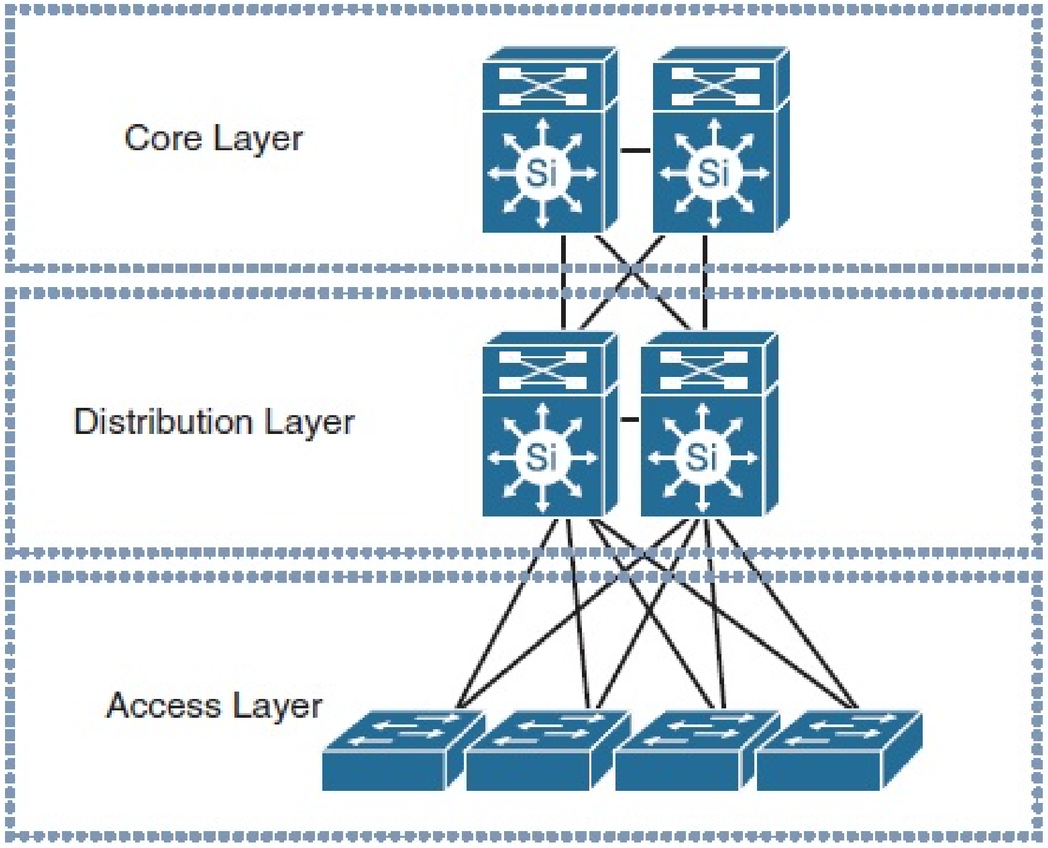



**Figure 3-1** *Three-Tier Network Design Model*

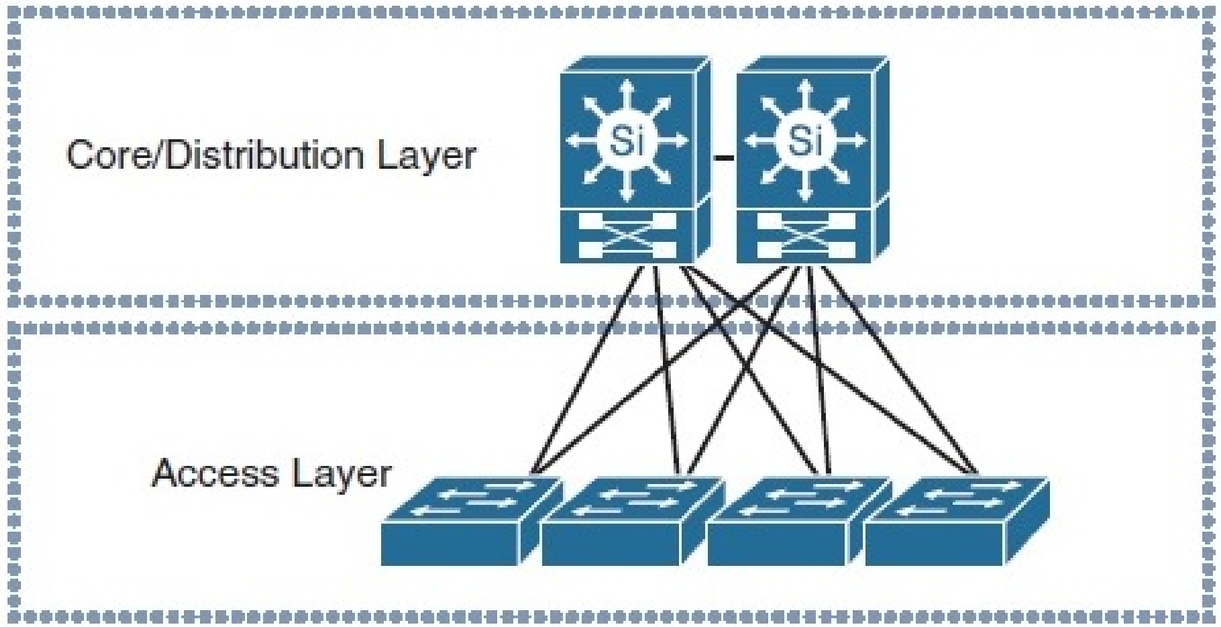
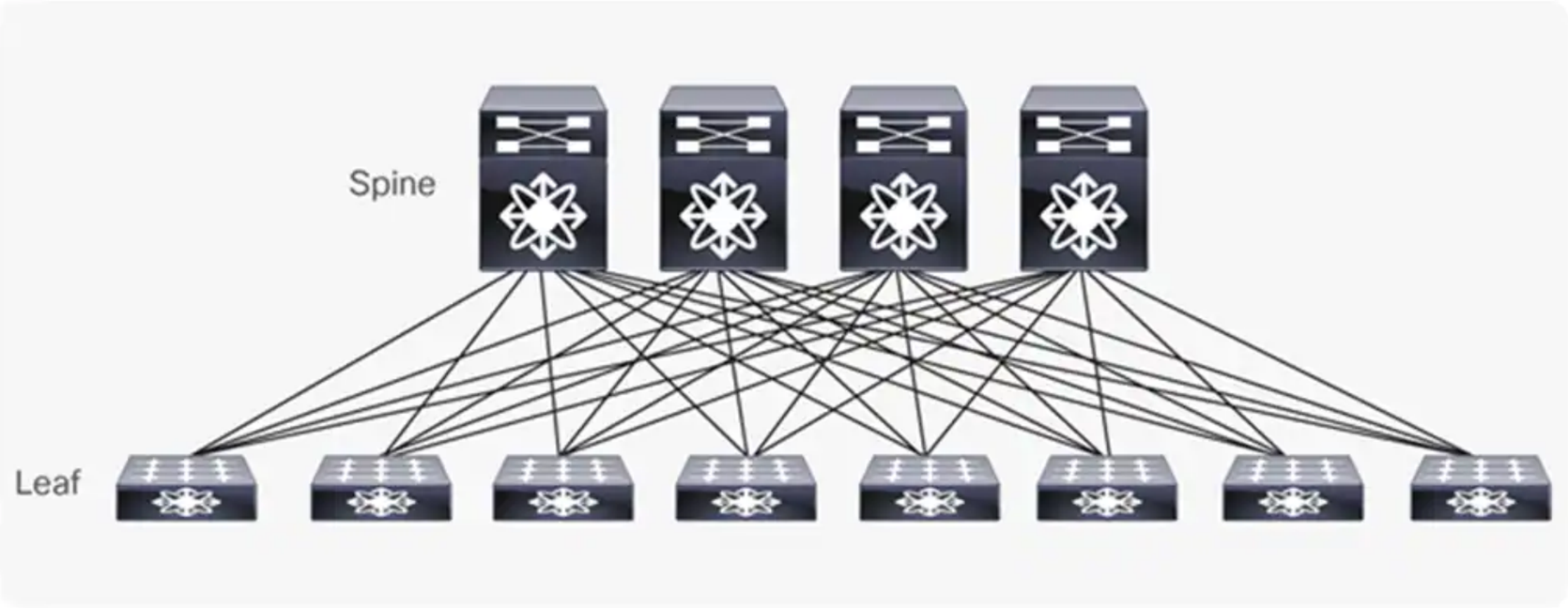


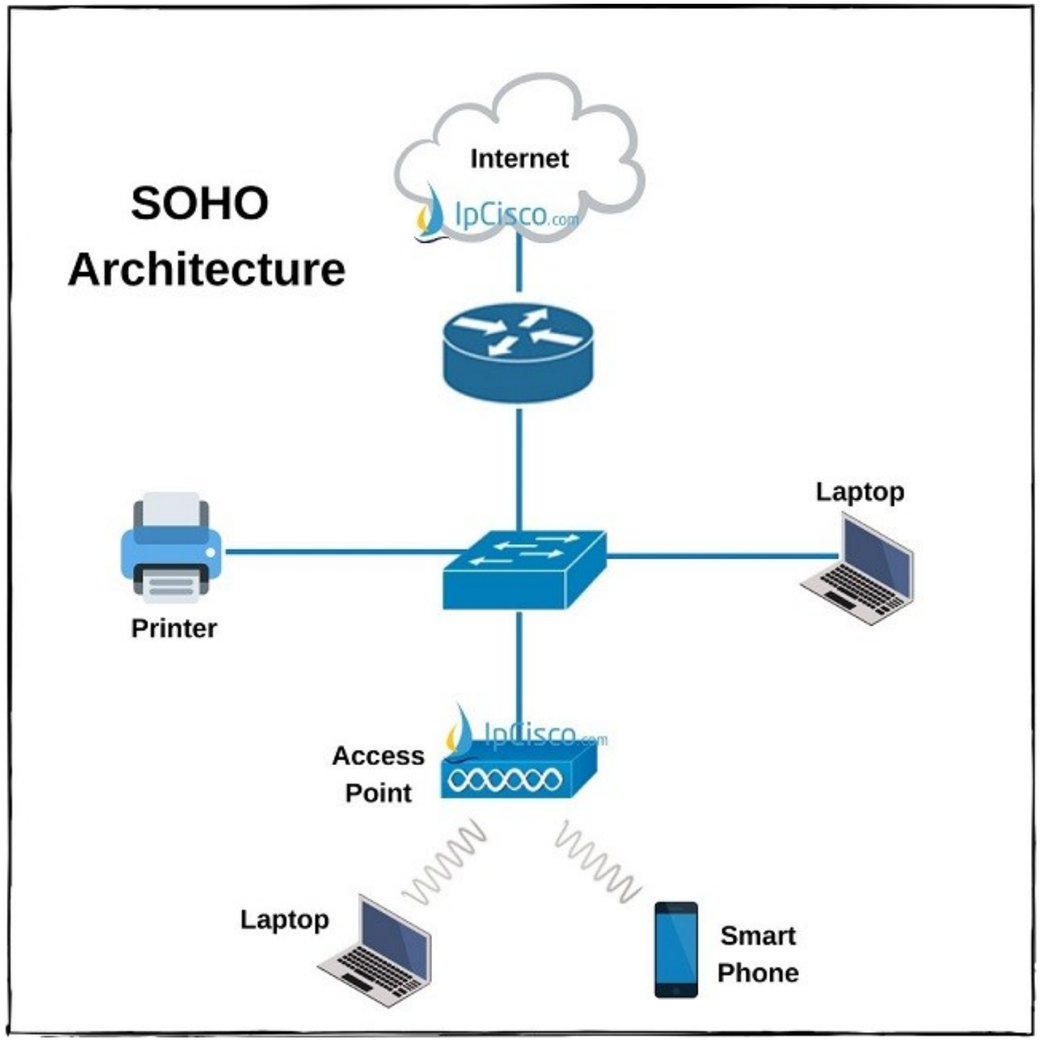

**Figure 3-2** *Two-Tier Network Design Model*

**Data flows from south to north and north to south.**

# Spine Leaf Architecture




**In spine leaf architecture data flows from east to west and west to east. Has lesser latency compared to 2 tier and 3 tier.**


SOHO
Architecture
Internet
IpCisco.com
Printer
Laptop
Access
Point
Laptop
Smart
Phone

# Automation

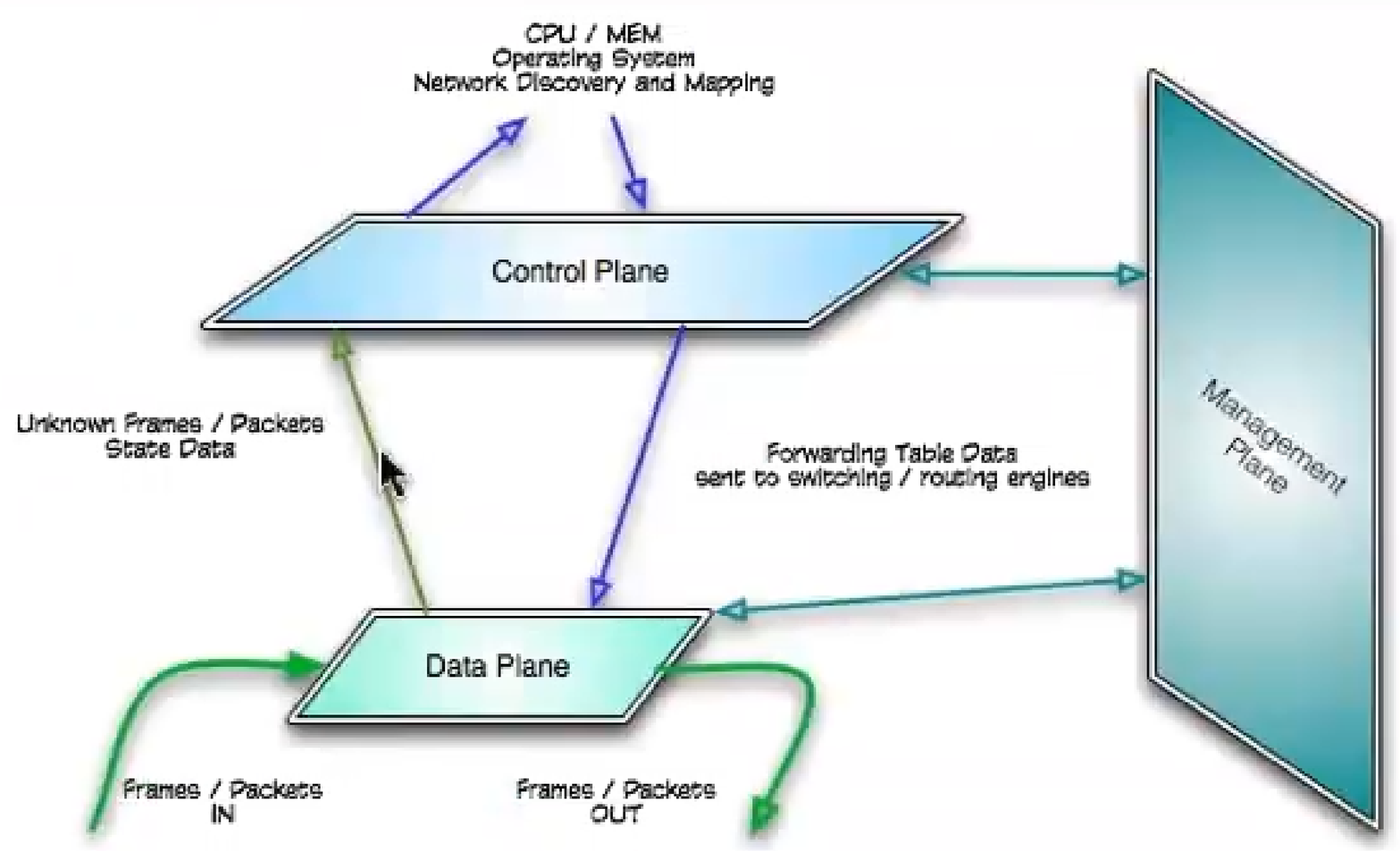
# Data plane, Control Plane and Management Plane

Data plane — all the functions and processes that forward packets/frames from one interface to another

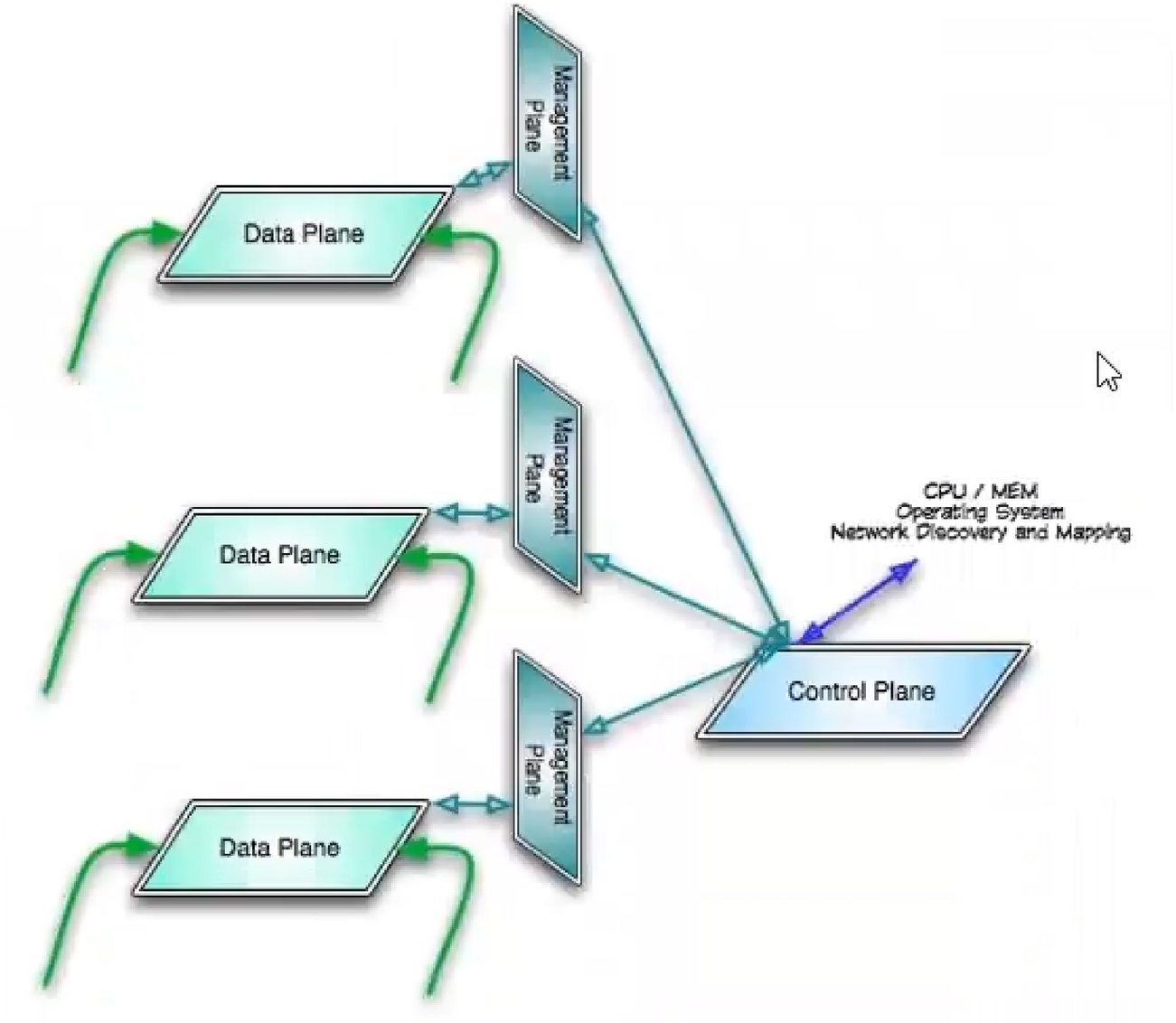
Control plane — all the functions and processes that determine which path to use (such as LDP, Routing protocols, etc.)

Management plane — all the functions you use to control and monitor devices.

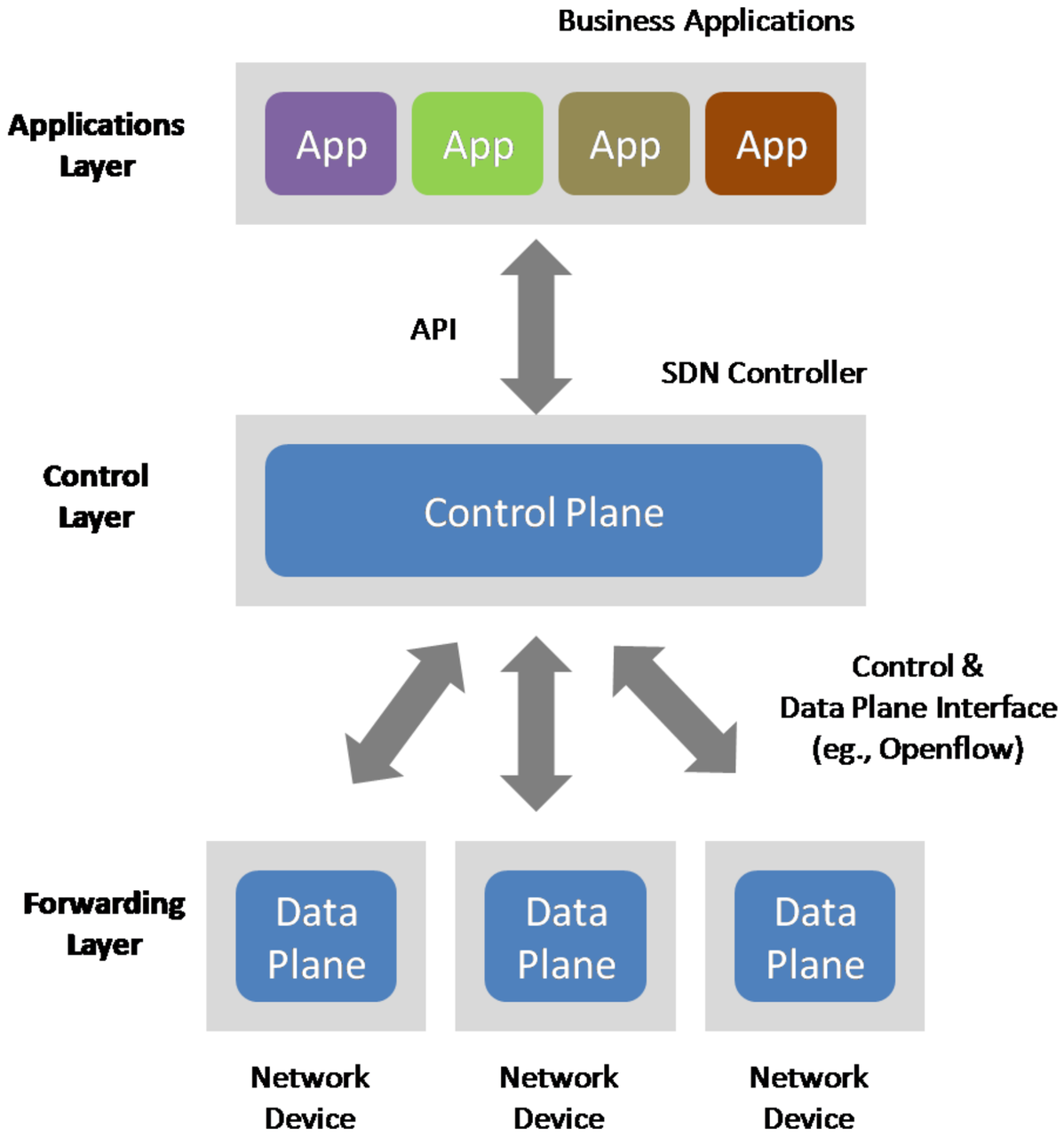
# Legacy Network



# Controller Based Network

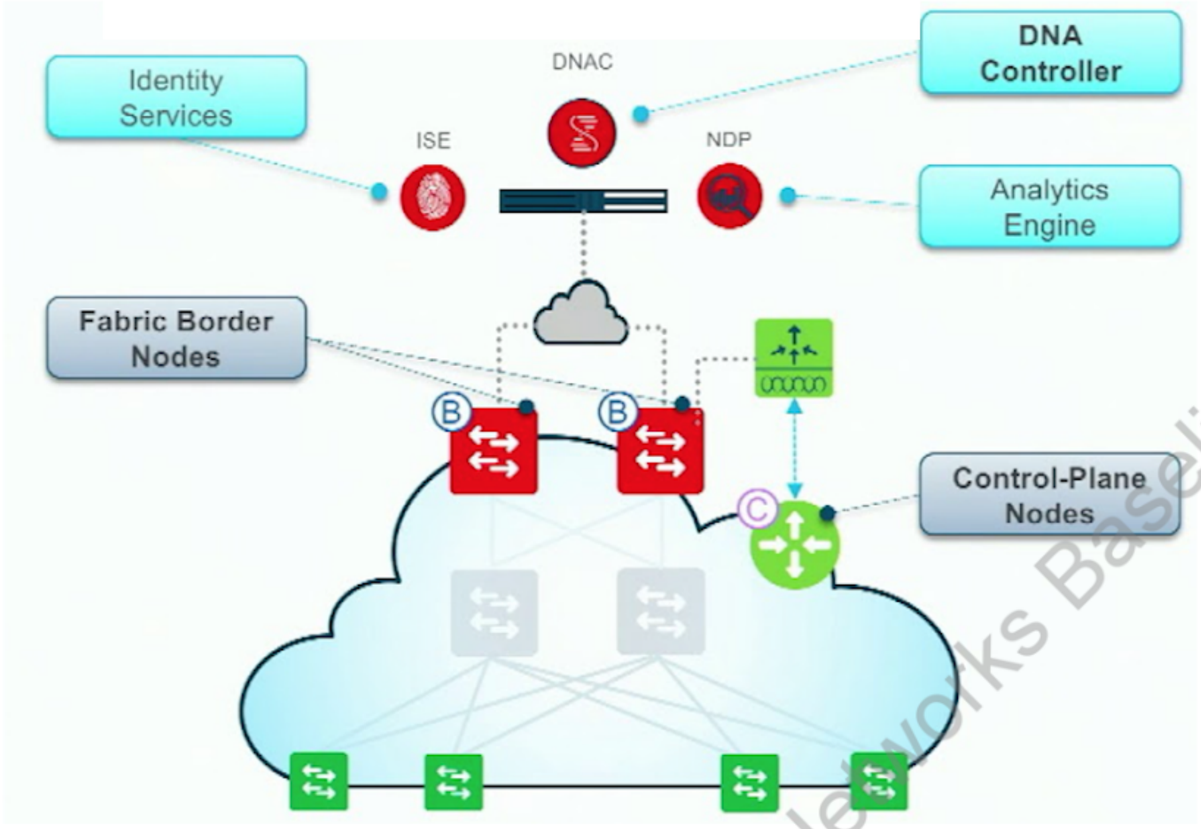


# Software Defined Networks Architecture

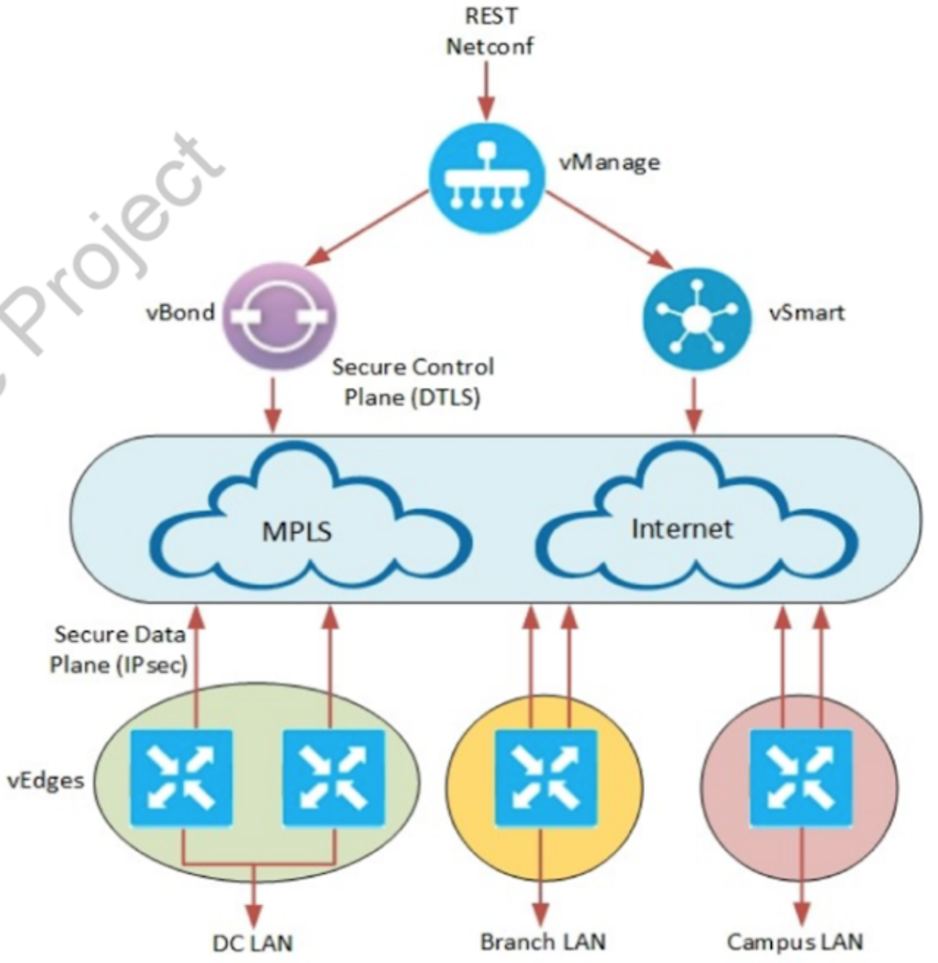


1) SDN - Software Defined Network
2) Northbound interface and Southbound interface
3) API - Application program interface
4) API is a medium for two applications to communicate to each other
5) Northbound interface use REST API (Representational State Transfer API) to communicate to SDN Controller
6) Southbound interface use - Openflow, Netconf protocols to communicate to SDN Controller
7) RestAPI is one of the type in API
8) JSON is a languge RestAPI use to communicate between two applications
9) Actions we can perform using API is CRUD - Create, Read, Update, Delete
10) Network Automation tools - Ansible, Puppet, CEF

# Cisco SD-Access and Cisco Viptela SDWAN network Architecture




Cisco SD-Access




Cisco Viptela SD-WAN

1) WAN is collection of LAN
2) SDWAN is a technology and Cisco has named its SDWAN technology as Viptela
3) SDWAN is used to mange devices at WAN
4) SDWAN is used for automation at WAN side
5) SDWAN terms: V-manage, V-smart, V-bond, V-edge
6) SD-Access is a technology used to manage device at LAN
7) SD-Access is used for automation at LAN side
8) SD-Access terms - DNAC: Dynamic network analysis controller, ISE: Identity service engine, NDPE: Neighbor Discovery Protocol Engine