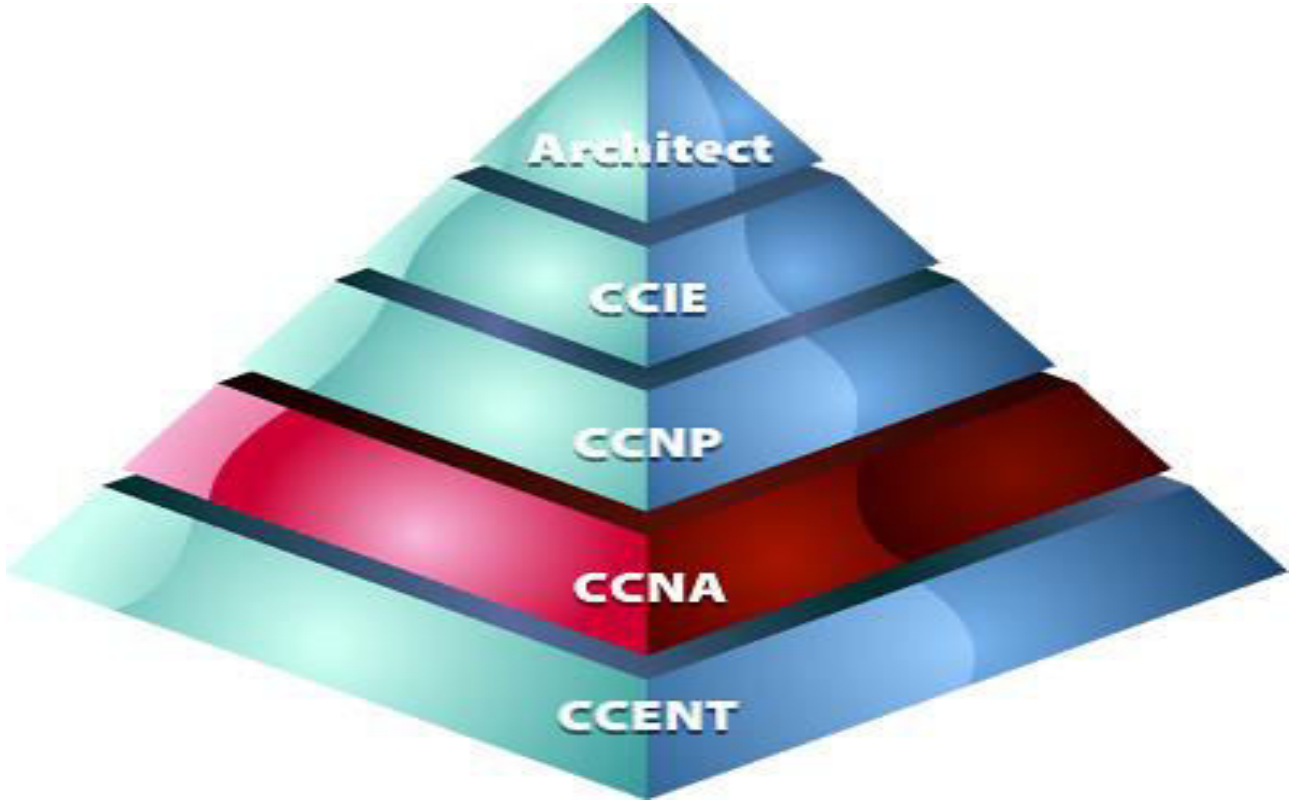
Cisco Certified Network Associate (CCNA)

- Cisco certifications are globally respected IT certification programs for Wide Area Networking (Internetworking).
- Cisco has five levels of certification:
  - CCENT (Cisco Certified Entry Networking Technician)
  - CCNA (Cisco Certified Network Associate)
  - CCNP (Cisco Certified Network Professional)
  - CCIE (Cisco Certified Inter networking Expert)
  - CCAr (Cisco Certified Architect)



There are 2 tracks for CCNA examination :

- **Two paper track**
  - **ICND 1 (100-101) (On passing this exam the candidate is CCENT)**
  - **ICND 2 (200-101) (On passing both exams the candidate is CCNA)**

Cisco Certified Entry Networking Technician (CCENT)

Interconnecting Cisco Network Devices (ICND)

OR

- **One paper track**
  - **CCNA (200-120) (On passing this exam the candidate is CCNA)**

- **Cisco Certified Network Associate R&S exam is the associate level exam into Wide Area Networking.**

Exam Number	**:**	**200-125 CCNA V3**
Duration	**:**	**90 Minutes**
Number of questions	**:**	**50-60 questions**
Passing Mark	**:**	**825 / 1000**
Available Languages	**:**	**English**
Exam Questions	**:**	**Multiple-choice single answer**
		Multiple-choice multiple answer
		Drag-and-drop
		Simulations (Simlet)
		Scenario Based (Testlet)

Basics of Networking

Network:

- Interconnection of two or more devices is called as a network.
- The communication between two or more interconnected devices is called networking.
- An internetwork is a connection of two or more networks.
- Internetworking means communication between different networks.

Types of Networks

- **LAN**

Local Area Networks are used to connect networking devices that are in a very close geographic area such as a floor of a building, a building itself or within a campus.

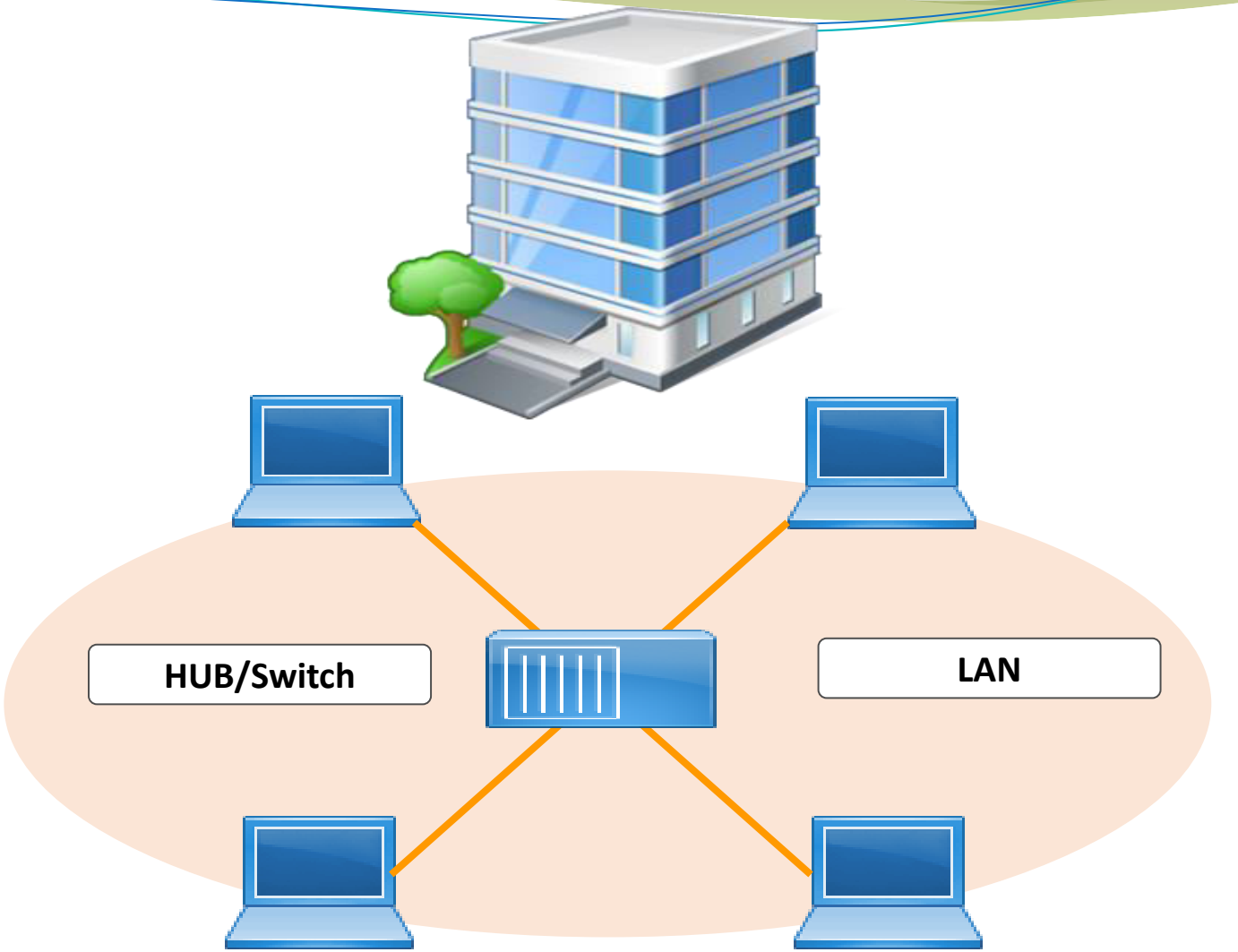
- **MAN**

Metropolitan Area Network are used to connect networking devices that may span around the entire city.

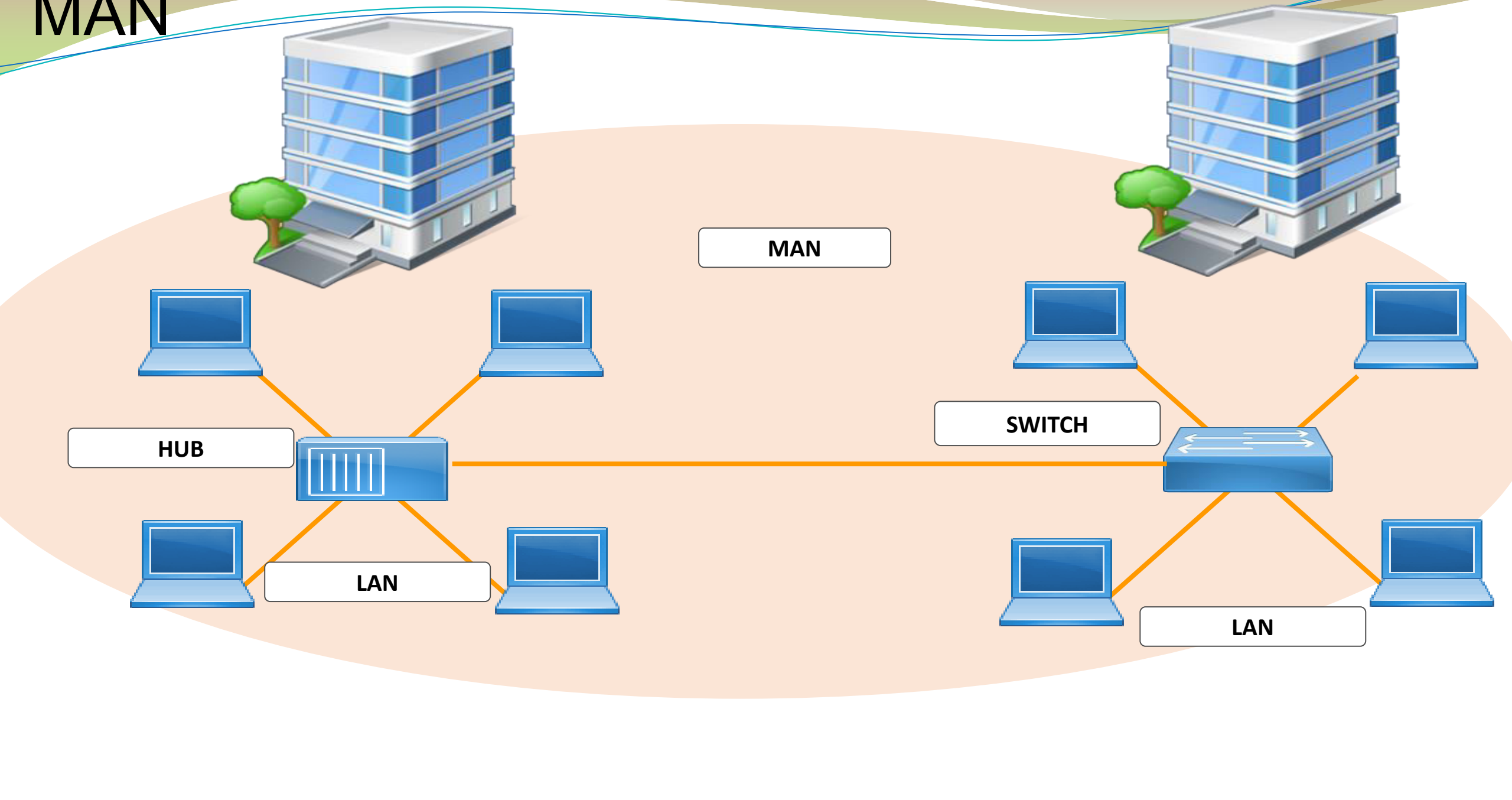
- **WAN**

Wide Area Networks which connects two or more LANs present at different geographical locations.

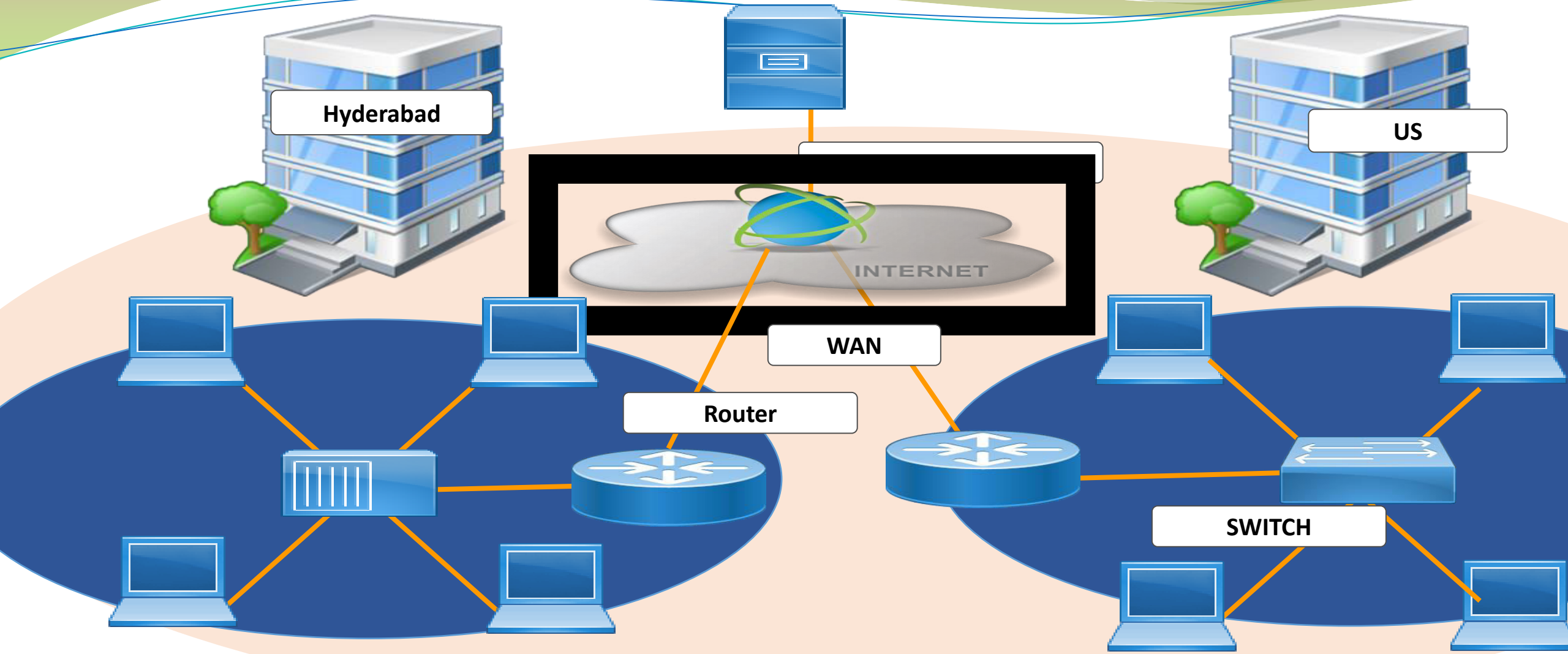
LAN



MAN



WAN

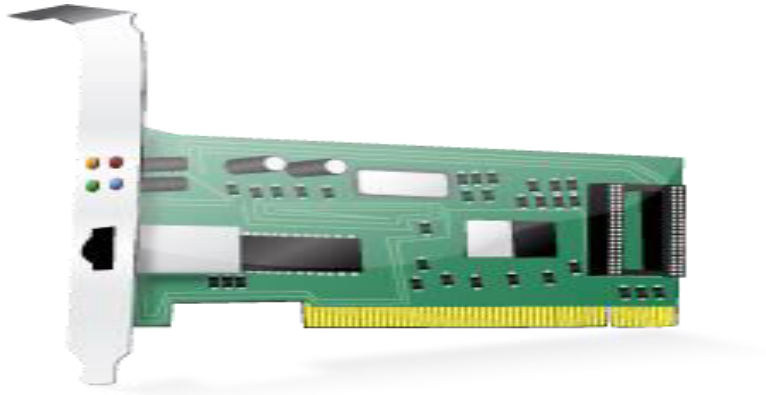


Basic requirements to form a network

- NIC (Network interface card) also called as LAN card
- Media
- Networking devices (Hub, Switch, Router etc.)
- Protocols
- Logical Address (IP address)

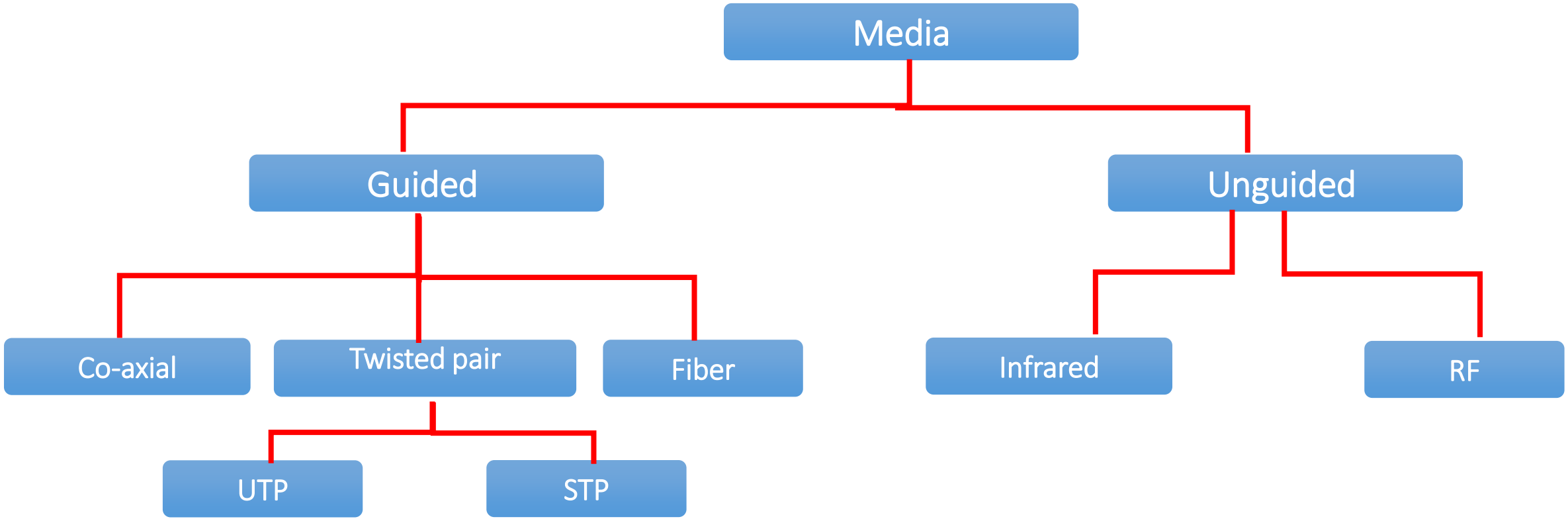
NIC(Network Interface Card)

- NIC is the interface between the computer and the network
- It is also known as the Lan card or Ethernet card
- Ethernet cards have a unique 48 bit address called as MAC (Media access control) address
  - MAC address is also called as Physical address or hardware address
  - The 48 bit MAC address is represented as 12 Hexa-decimal digits
  - Example: 0016.D3FC.603F
- Network cards are available in different speeds
  - Ethernet (10 Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1000 Mbps)



Media

- The purpose of the media is to transport bits from one machine to another.



Media

UTP Cable

Co-axial cable

Fiber optic

Types of Twisted Pair cables

Category	DTR	Purpose	Connector
CAT 1	1 Mbps	Telephone Lines	RJ 11
CAT 2	4 Mbps		RJ 11
CAT 3	10 Mbps	Ethernet	RJ 45
CAT 4	16 Mbps		RJ 45
CAT 5	100 Mbps	Fast Ethernet	RJ 45
CAT 5e	500 Mbps		RJ 45
CAT 6	1000 Mbps	Gigabit Ethernet	RJ 45

Topology

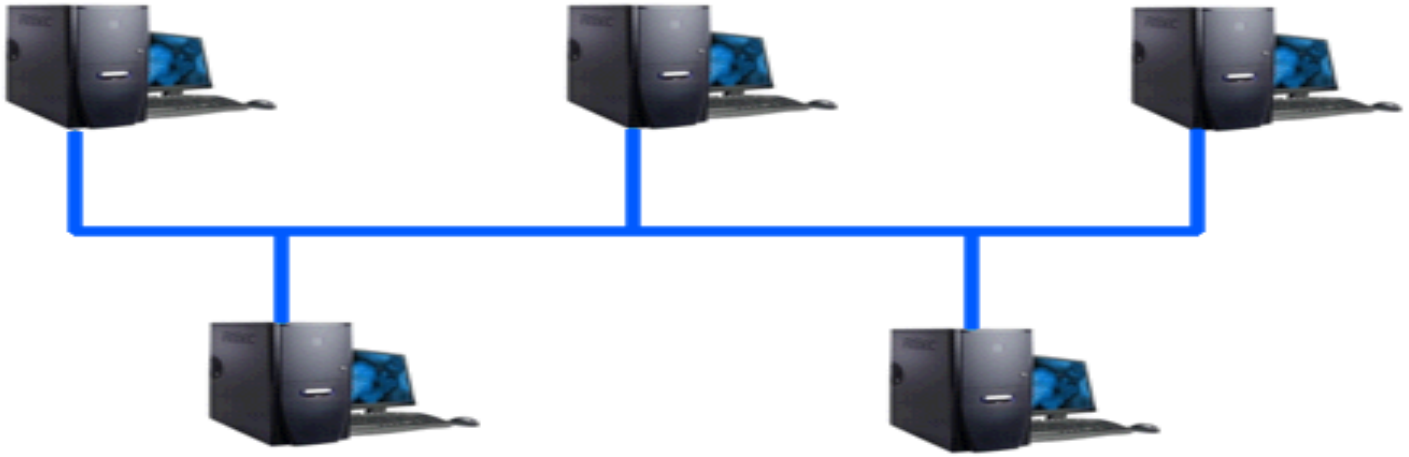
Topology is a physical layout of the systems connected in a network.

Different types of topology are:

- **Bus**
- **Ring**
- **Mesh**
- **Star**

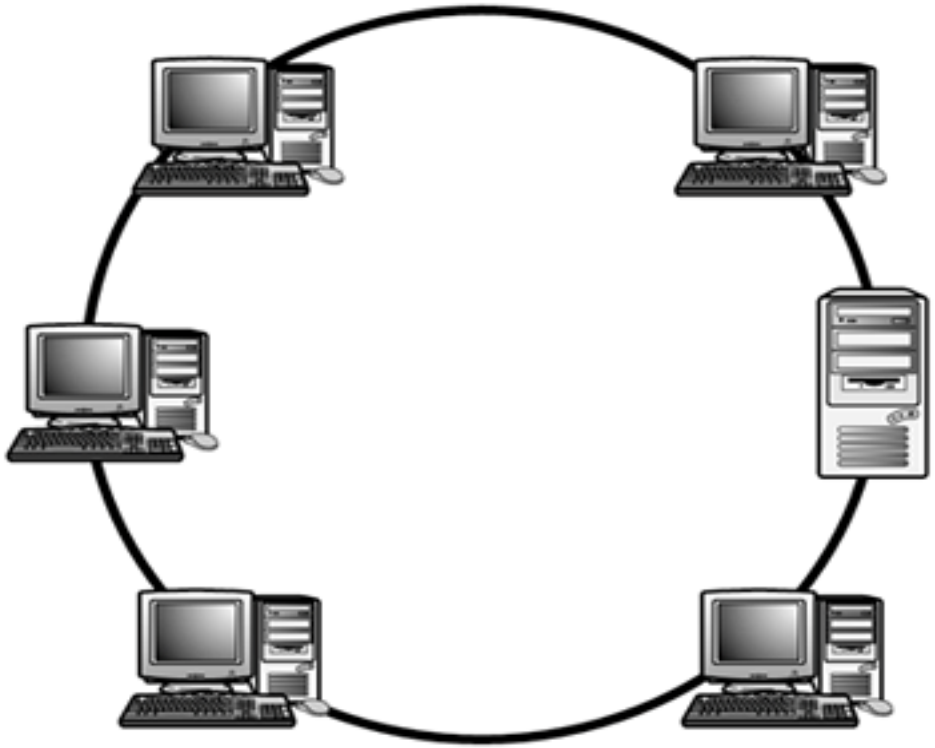
Bus Topology

- In bus topology all devices are connected to a single cable or backbone.
- It supports half duplex communication.
- A break at any point along the backbone will result in total network failure.



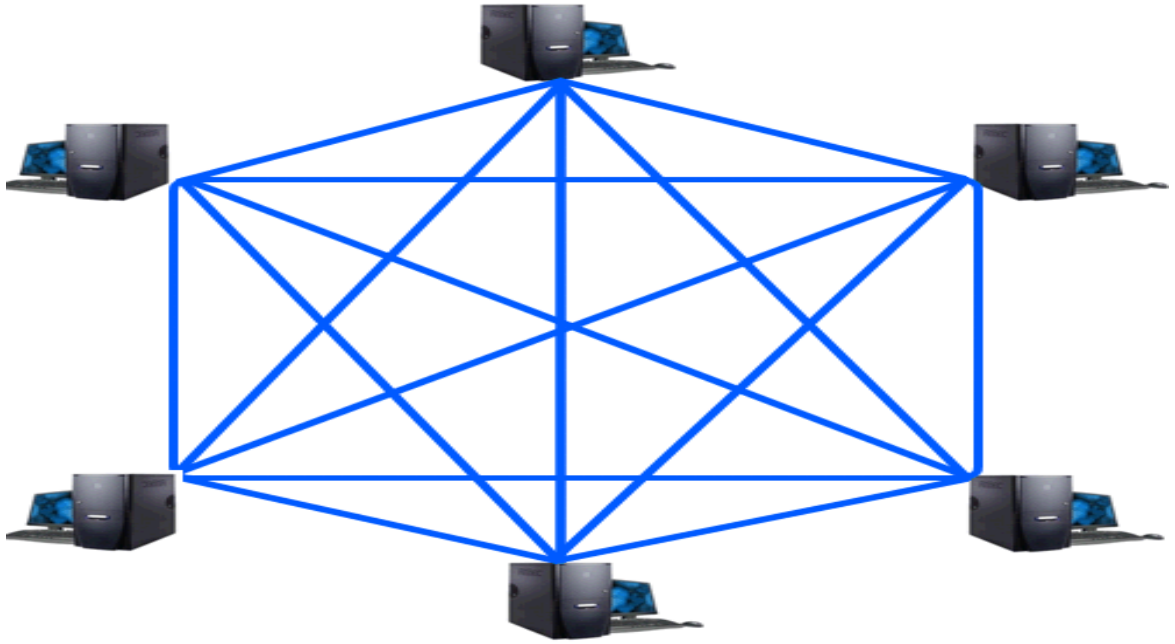
Ring Topology

- In ring topology each computer or device is connected to its neighbor forming a loop.
- Failure of a single device or a break anywhere in the cable causes the full network to stop communicating



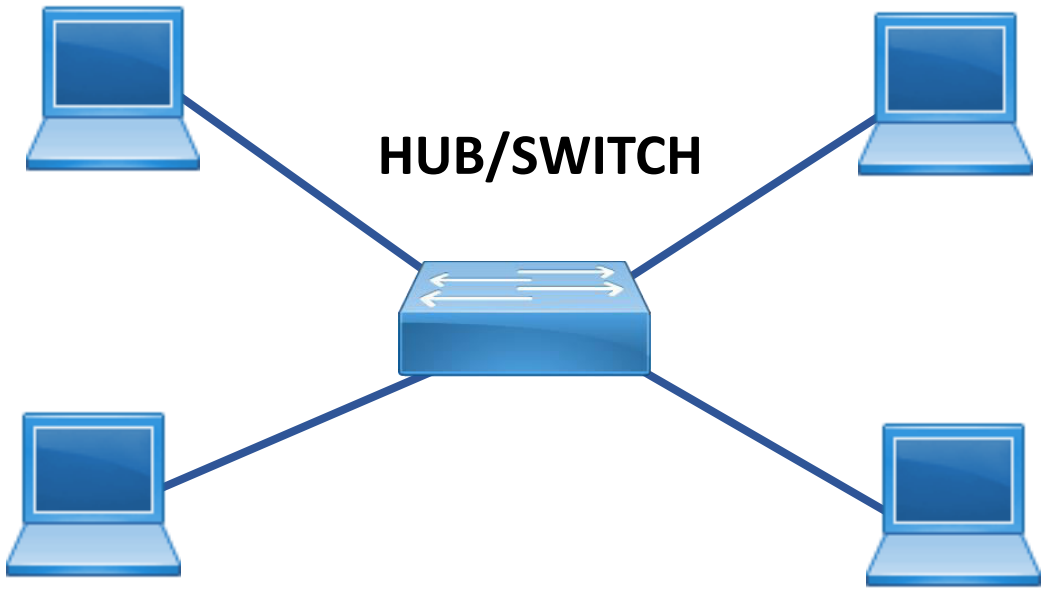
Mesh Topology

- In mesh topology each device is directly connected to all other devices
- The disadvantage is the number of NIC's required on each device and the complex cabling.



Star Topology

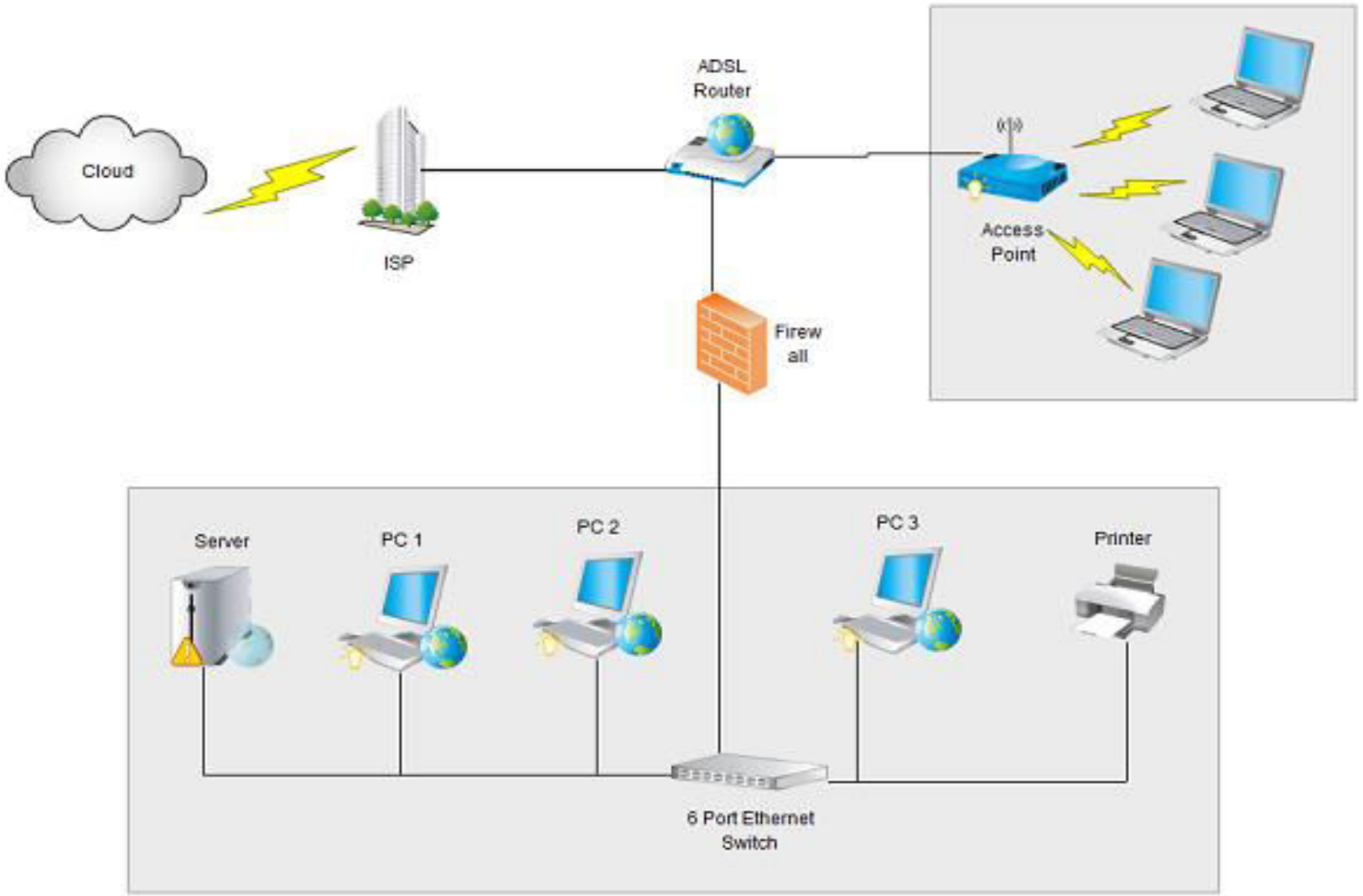
- The most commonly used topology
- It consist of one centralized device which can be either a switch or a hub.
- The devices connect to the various ports on the centralized devices.

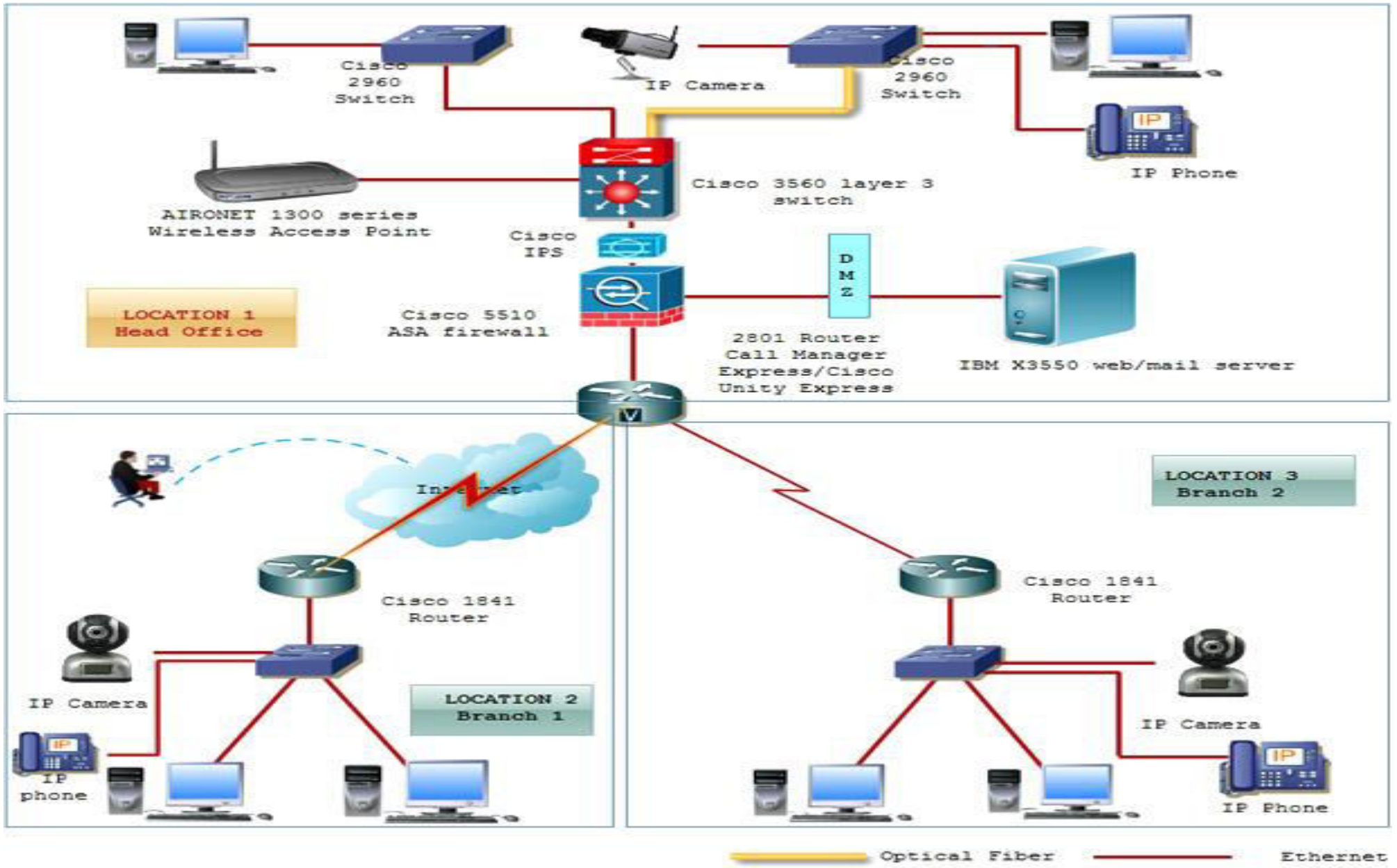


Networking device

The various types of networking devices are:

- **Hub**
- **Switch**
- **Router**
- **Firewalls**
- **Access Points**
- **Wireless Controllers**
- **Load Balancers**


Cloud
ISP
ADSL
Router
Access
Point
Firew
all
Server
PC 1
PC 2
PC 3
Printer
6 Port Ethernet
Switch


Cisco
2960
Switch
IP Camera
Cisco
2960
Switch
IP Phone
AIRONET 1300 series
Wireless Access Point
Cisco 3560 layer 3
switch
Cisco
IPS
D
M
Z
LOCATION 1
Head Office
Cisco 5510
ASA firewall
2801 Router
Call Manager
Express/Cisco
Unity Express
IBM X3550 web/mail server
Internet
LOCATION 3
Branch 2
Cisco 1841
Router
Cisco 1841
Router
IP Camera
LOCATION 2
Branch 1
IP Camera
IP
phone
IP Phone
Optical Fiber
Ethernet

Hub / Repeater

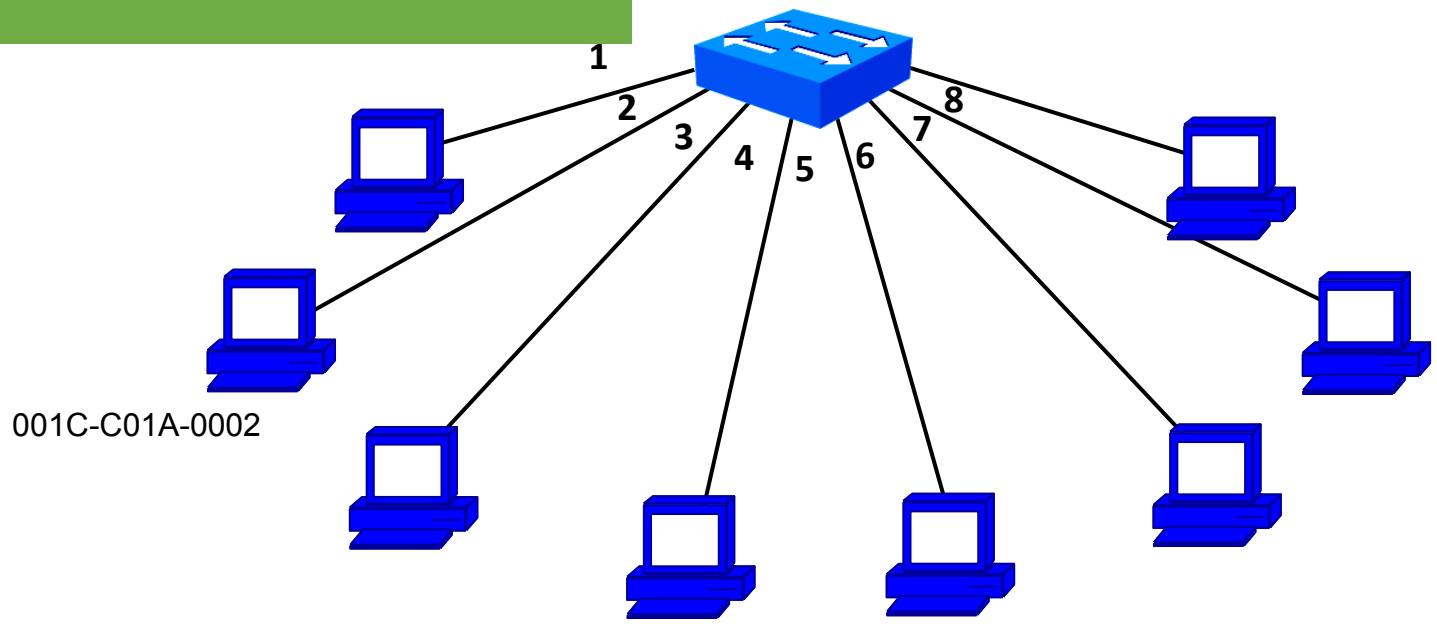
- **It is not an Intelligent Device.**
- **It works with bits.**
- **Uses broadcast for communication.**
- **Bandwidth is shared.**
- **Half-duplex communication.**

Switch

- It is an Intelligent device.
- It maintains MAC address table (hardware address).
- Each port of the switch has fixed bandwidth.
- It works with Flooding and Unicast.
- Supports full duplex communication

Source MAC
001C.C01A.0002
Destination MAC
001C.C01A.0004

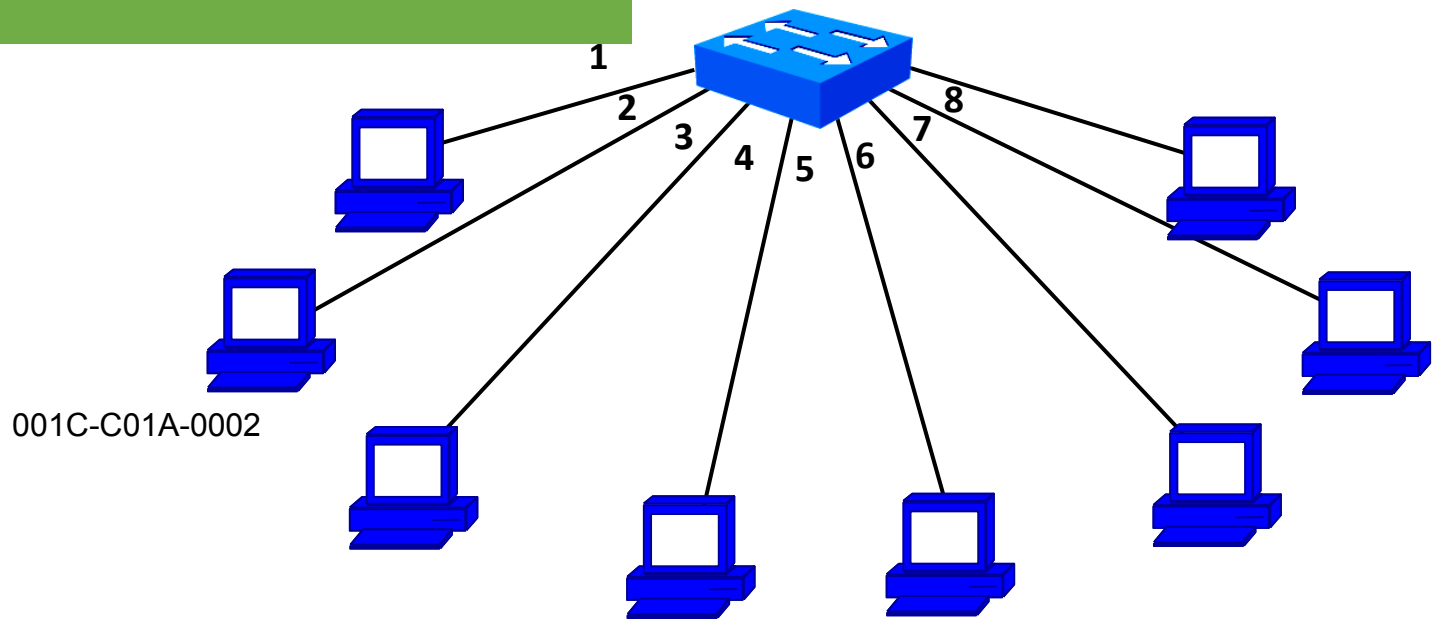
DATA



MAC ADDRESS TABLE	
PORT	MAC-ADDRESS
Fa0/1	
Fa0/2	001C-C01A-0002
Fa0/3	
Fa0/4	
Fa0/5	
Fa0/6	
Fa0/7	
Fa0/8	

Source MAC
001C.C01A.0002
Destination MAC
001C.C01A.0004

DATA



PORT	MAC-ADDRESS
Fa0/1	
Fa0/2	001C-C01A-0002
Fa0/3	
Fa0/4	001C-C01A-0004
Fa0/5	
Fa0/6	
Fa0/7	
Fa0/8	

MAC Address Table in Switch

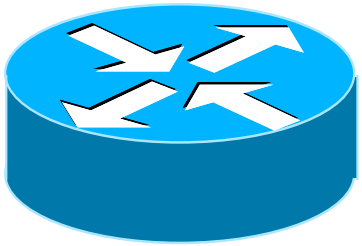
```
Switch#show mac-add
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   1    0007.8580.7456    DYNAMIC     Fa0/1
   1    000d.6516.d692    DYNAMIC     Fa0/3
   1    000d.bcef.ae82    DYNAMIC     Fa0/4
   1    000e.83f6.32da    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 4
Switch#
```

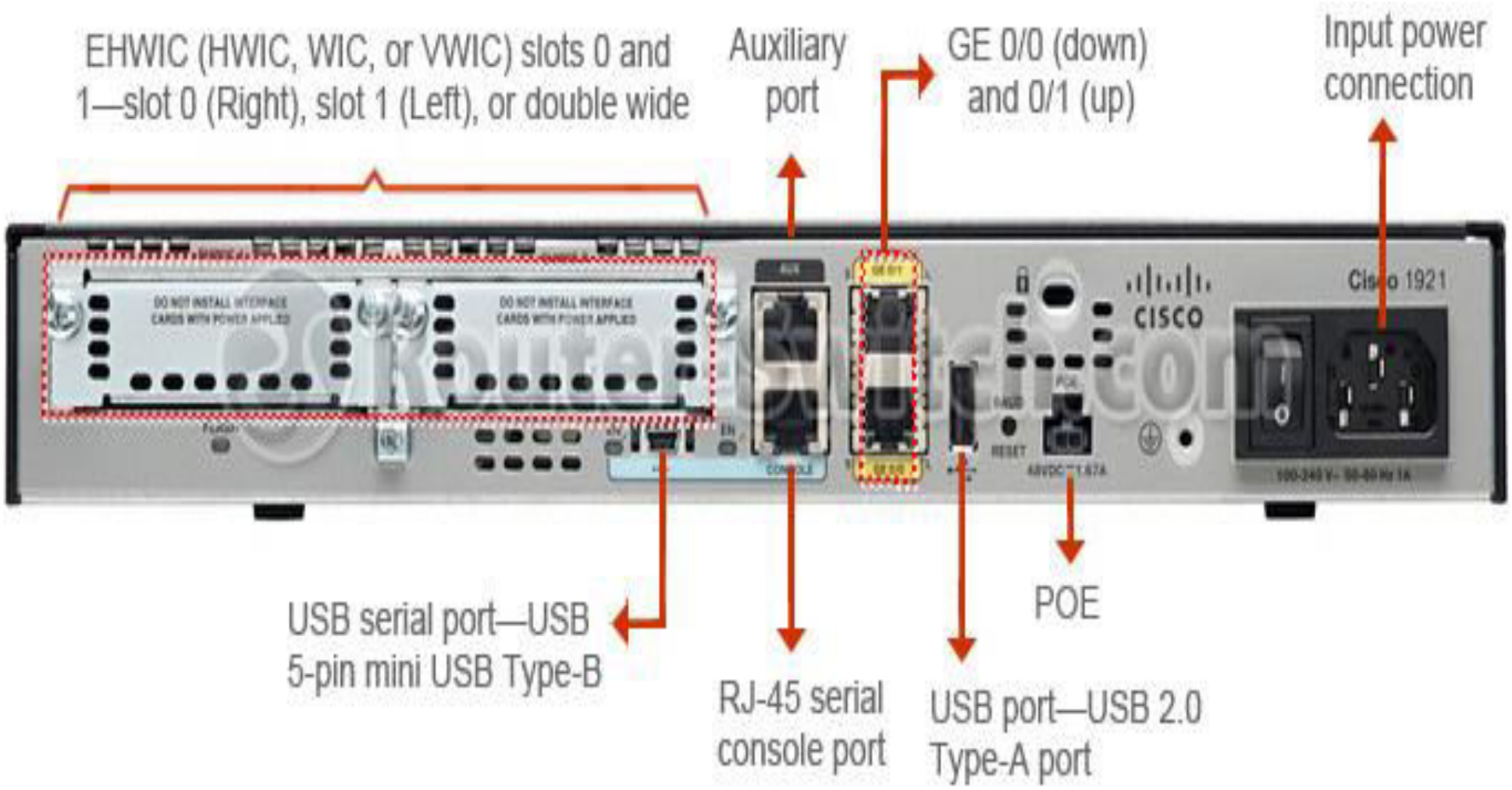
Router

- It is an Intelligent device
- It works with Logical Addressing (i.e. IP, IPX, AppleTalk)
- It works with Fixed bandwidth

Symbolic Representation:



Router


EHWIC (HWIC, WIC, or VWIC) slots 0 and 1—slot 0 (Right), slot 1 (Left), or double wide
Auxiliary port
GE 0/0 (down) and 0/1 (up)
Input power connection
USB serial port—USB 5-pin mini USB Type-B
RJ-45 serial console port
USB port—USB 2.0 Type-A port
POE

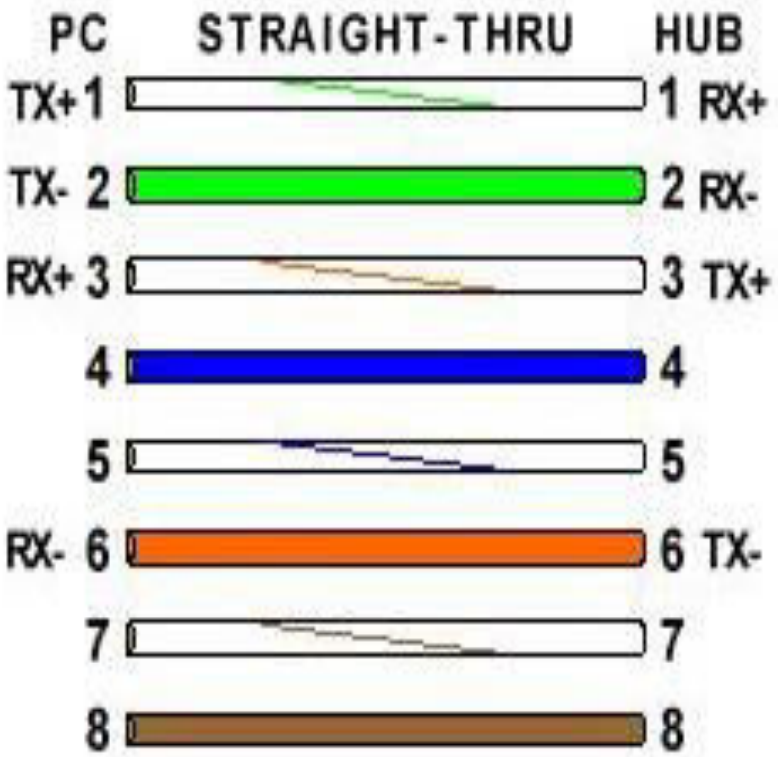
Cables used to Connect

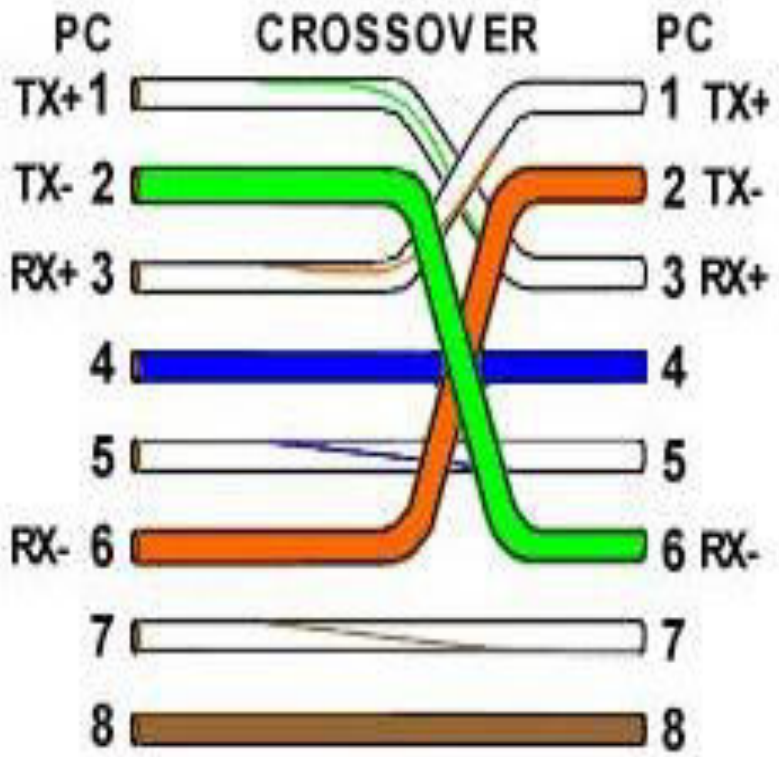
Straight Cable: Usually use straight cable to connect different type of devices.

Cross Cable: usually used to connect same type of devices

	PC	HUB	Bridge	Switch	Router
PC	Cross Cable	Straight	Cross Cable	Straight	Cross Cable
HUB	Straight	Cross Cable	Straight	Cross	Straight
Bridge	Cross Cable	Straight	Cross Cable	Straight	Cross Cable
Switch	Straight	Cross	Straight	Cross Cable	Straight
Router	Cross Cable	Straight	Cross Cable	Straight	Cross Cable

Colour Code for Straight & Cross Cables

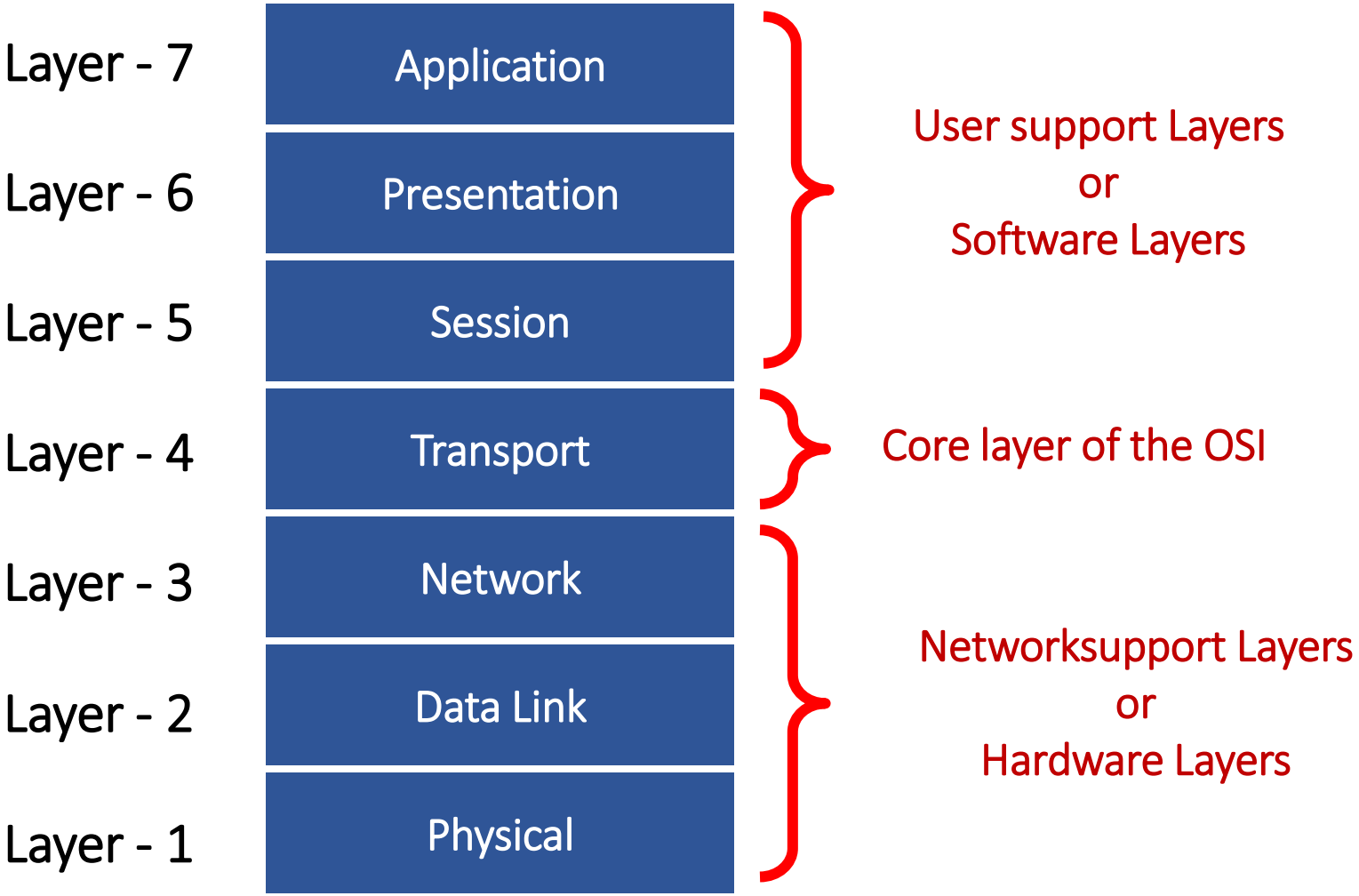




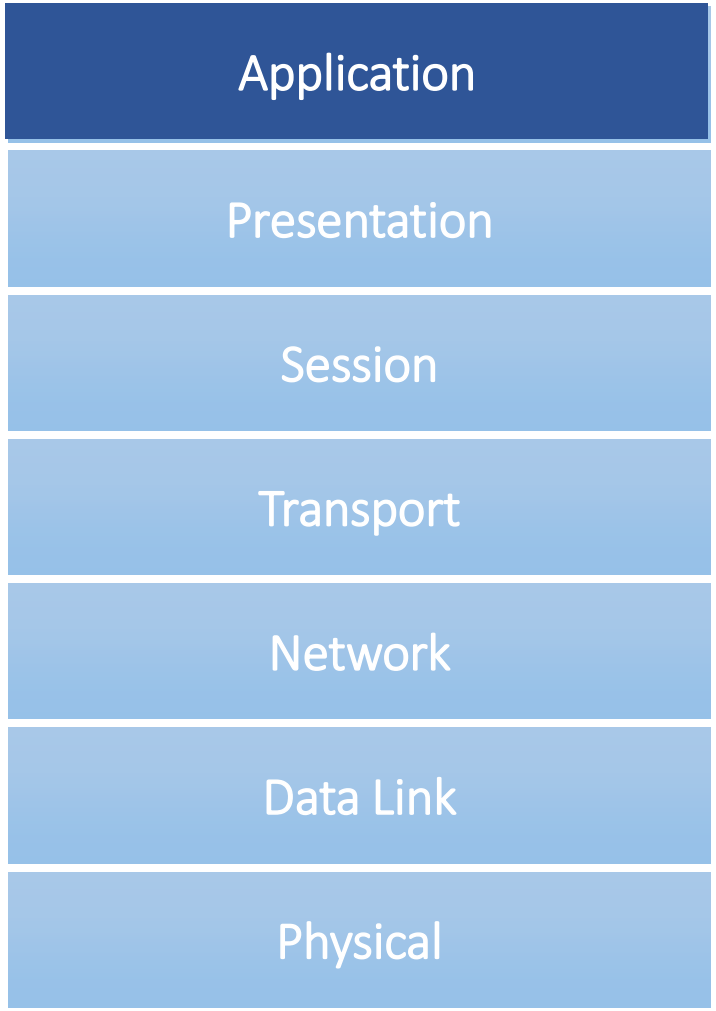
Open System Interconnect(OSI)

- **OSI was developed by the International Organization for Standardization (ISO) and introduced in 1984.**
- **It is a layered architecture (consists of seven layers).**
- **Each layer defines a set of functions which takes part in data communication.**

OSI Model Layers



Application Layer



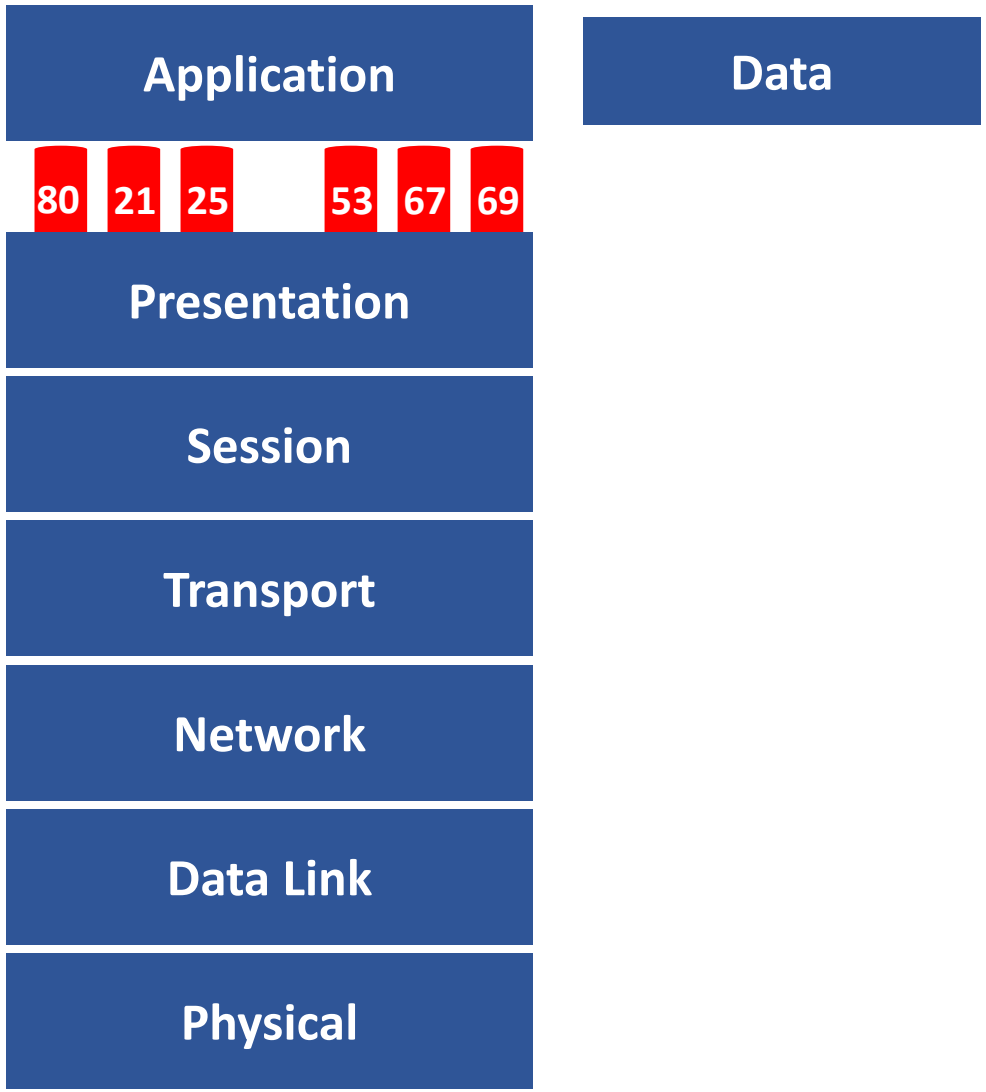
Application Layer : is responsible for providing an interface for the users to interact with application services or Networking Services .

Ex: Web browser(HTTP), Telnet etc.

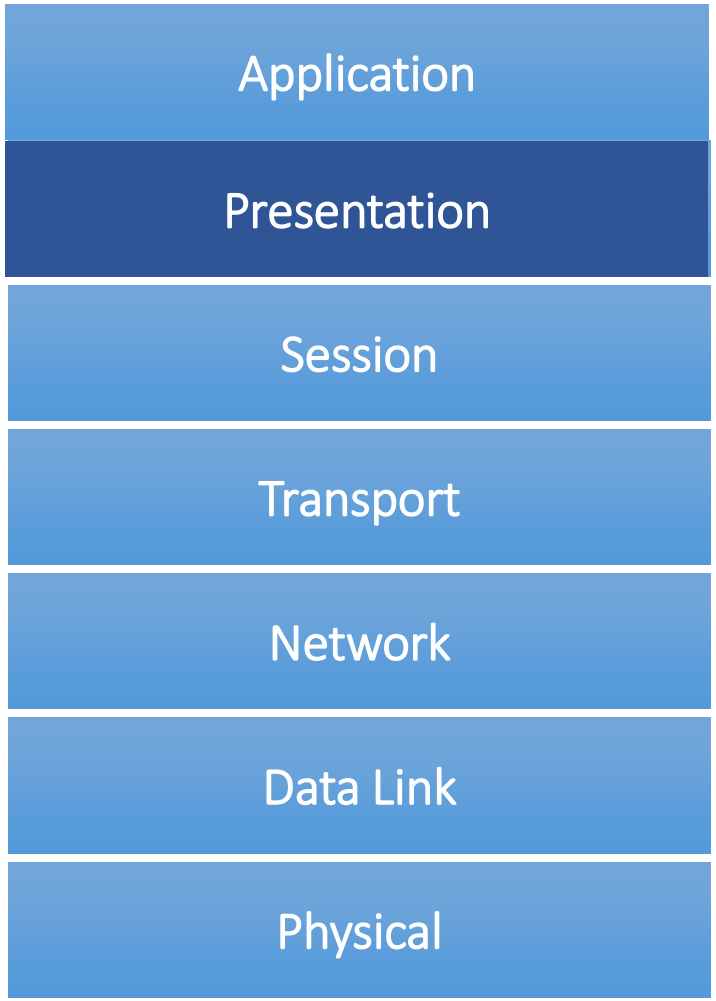
Examples of Networking Services

Service	Port No.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

Data flow from Application Layer



Presentation Layer



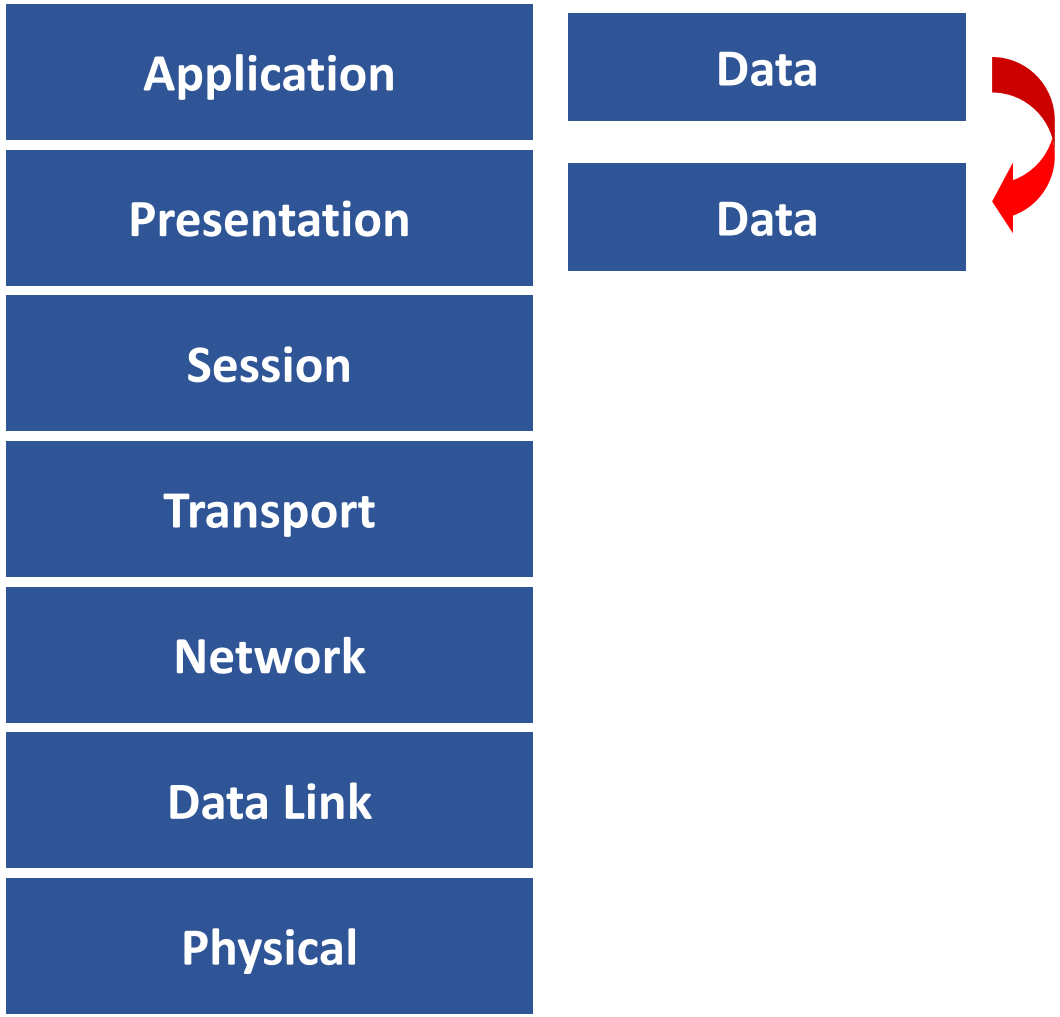
Presentation Layer : It is responsible for defining a standard format to the data.

It deals with data presentation.

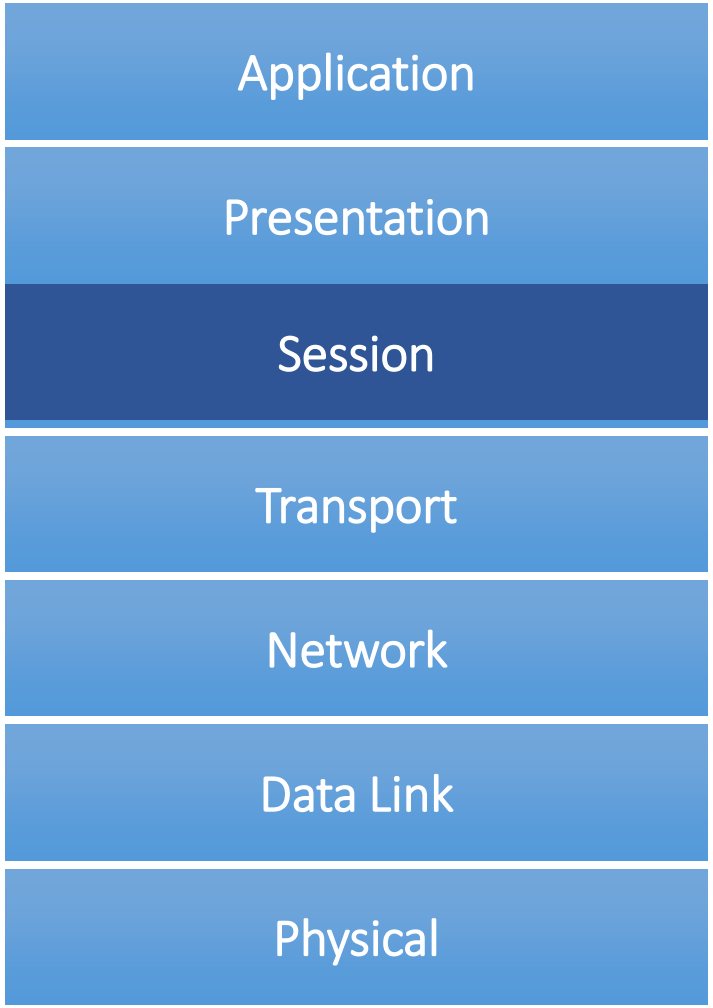
The major functions described at this layer are..

- **Encoding – Decoding**
  - **Ex : ASCII, EBCDIC (Text)**
  - **JPEG,GIF,TIFF (Graphics)**
  - **MIDI,WAV (Voice)**
  - **MPEG,DAT,AVI (Video)**
- **Encryption – Decryption**
- **Compression – Decompression**

Data flow from Presentation Layer



Session Layer



Session Layer : It is responsible for establishing, maintaining and terminating the sessions.

Session ID is used to identify a session or interaction.

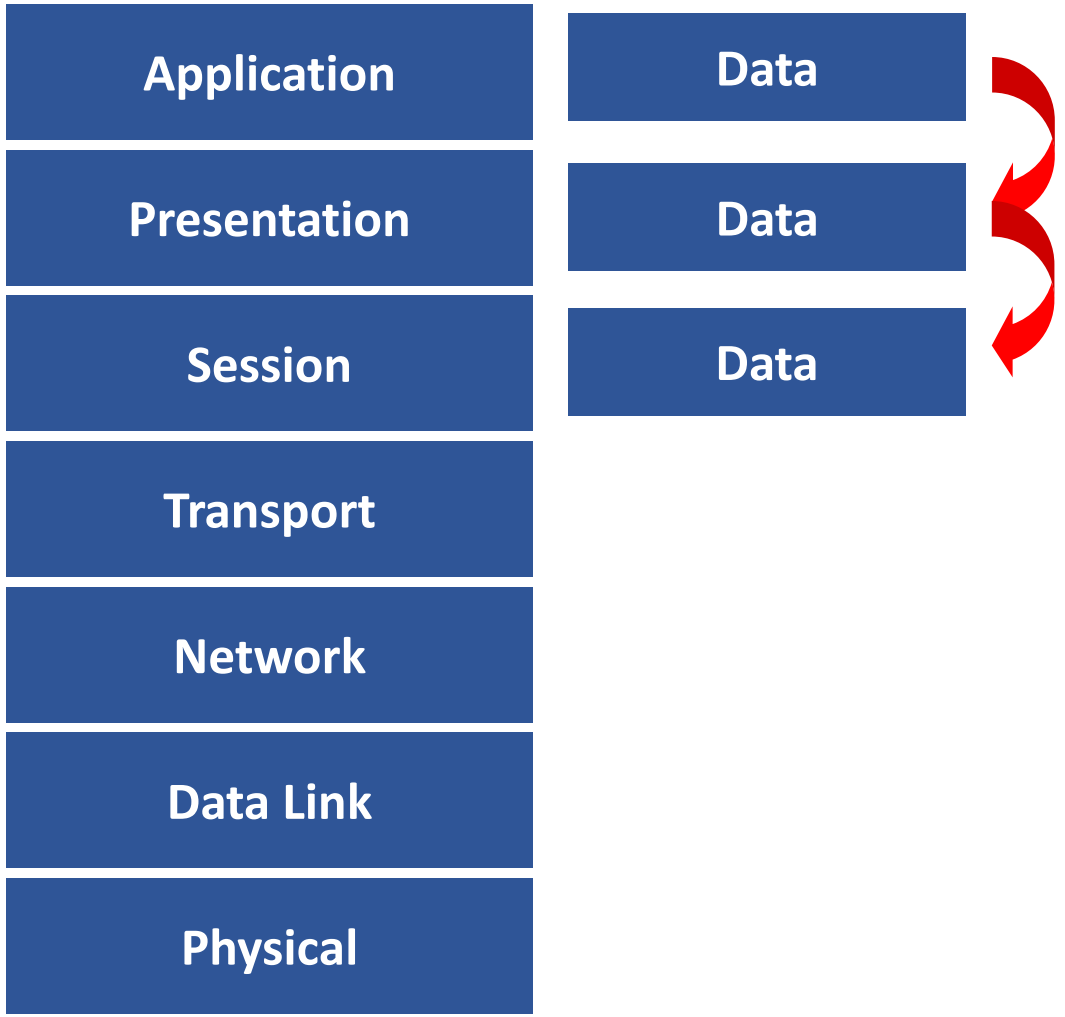
Ex :

RPC Remote Procedural Call

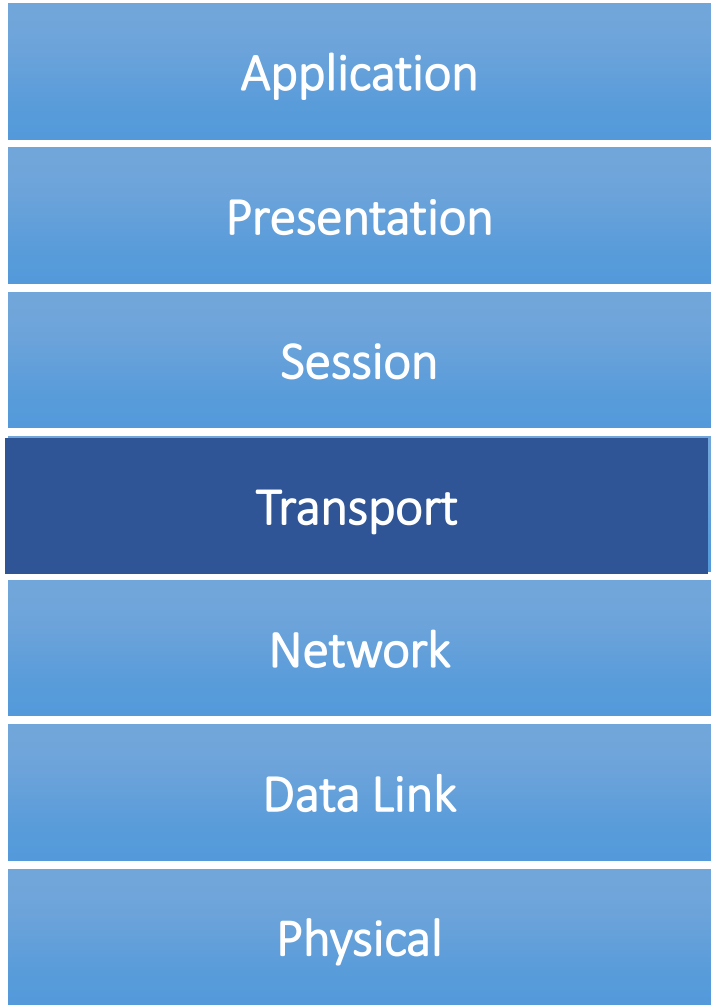
SQL Structured Query Language

ASP AppleTalk Session protocol

Data flow from Session Layer



Transport Layer



Transport Layer : It provides data delivery mechanism between the applications in the network.
The major functions described at the Transport Layer are.

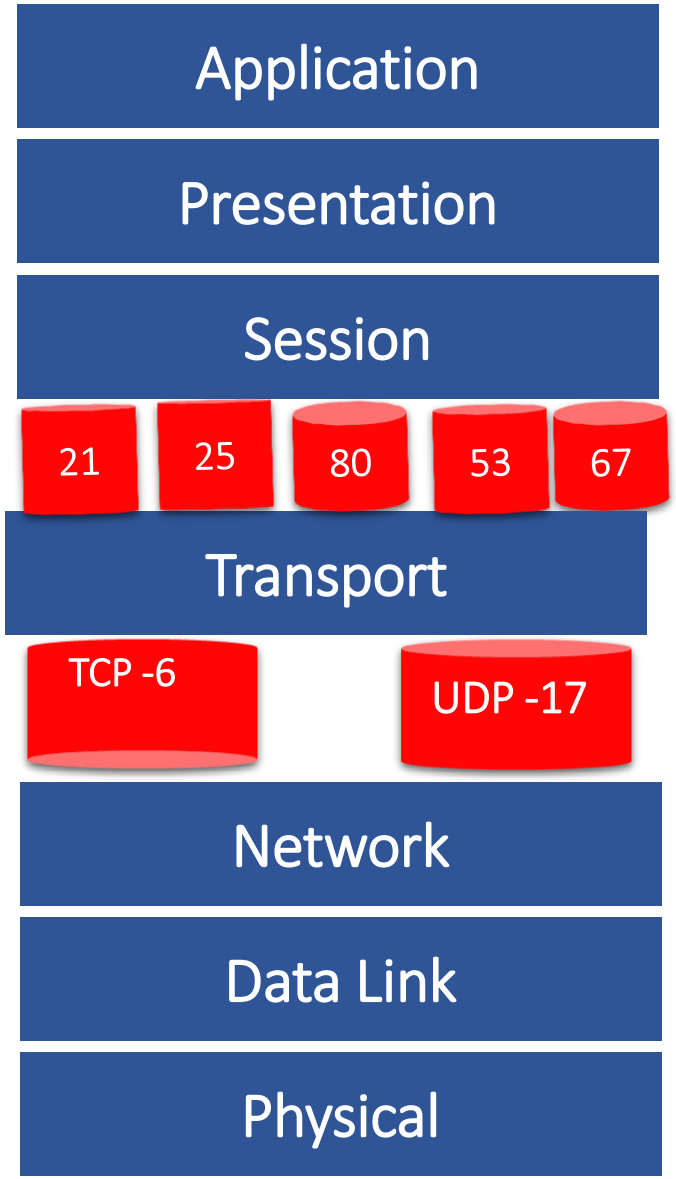
- **Identifying Service**
- **Multiplexing & De-multiplexing**
- **Segmentation**
- **Sequencing & Reassembling**
- **Error Correction**
- **Flow Control**

Identifying a Service

- Identification of Services is done using port Numbers.
- Port is a logical communication Channel

Total No. Ports	0 – 65535
Reserved Ports	1 - 49151
Open Ports	49152 – 65535

Multiplexing & De-multiplexing



Multiplexing and De-multiplexing are the two very important functions that are performed by Transport Layer.

Transport layer at the sender side receives data from different Applications , encapsulates every packet with a Transport Layer header and pass it on to the underlying Network Layer. This job of transport layer is known as Multiplexing.

At the receiver's side, the transport layer will do De-Multiplexing

Eg: Suppose you are sitting in front of your computer, and you are downloading web pages while running one FTP session and two Telnet sessions.

You therefore have four network application processes running – two Telnet processes, one FTP process, and one HTTP process. When the transport layer in your computer receives data from the network layer below, it needs to direct the received data to one of these four processes. Let’s now examine how this is done

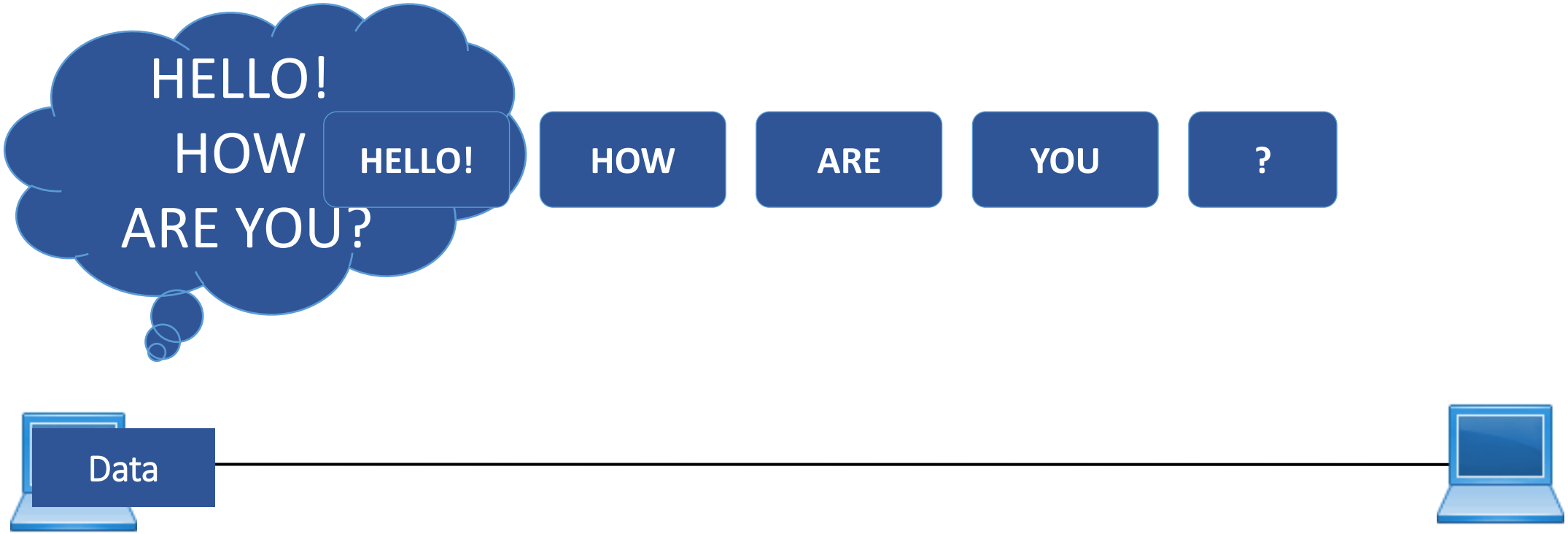
Transport Layer Protocols

- The protocols which takes care of Data Transportation at Transport layer are TCP and UDP

TCP	UDP
Transmission Control Protocol Connection Oriented Supports Acknowledgements Reliable communication Slower data Transportation Protocol No is 6 Ex: HTTP, FTP, SMTP	User Datagram Protocol Connection Less No support for Acknowledgements Unreliable communication Faster data Transportation Protocol No is 17 Ex: DNS, DHCP, TFTP

Segmentation , Sequencing & Reassembling

Segmentation and Reassembling : A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.



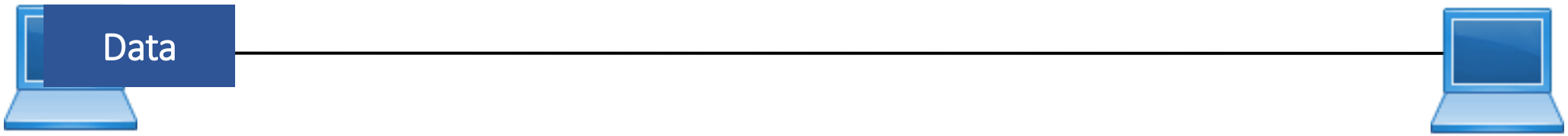
HELLO!
1/5

HOW
2/5

ARE
3/5

YOU
4/5

?
5/5



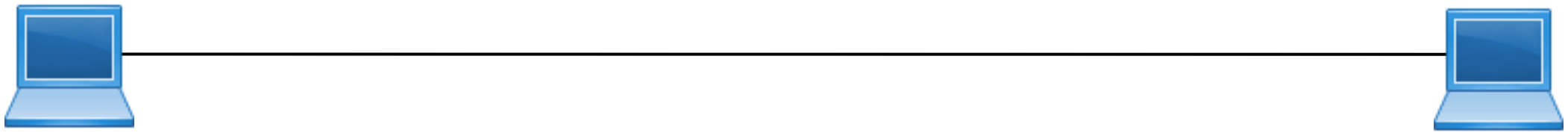
HOW
2/5

?
5/5

ARE
3/5

HELLO!
1/5

YOU
4/5



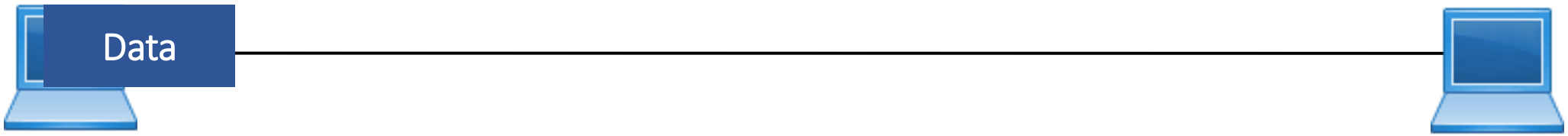
HELLO!
1/5

HOW
2/5

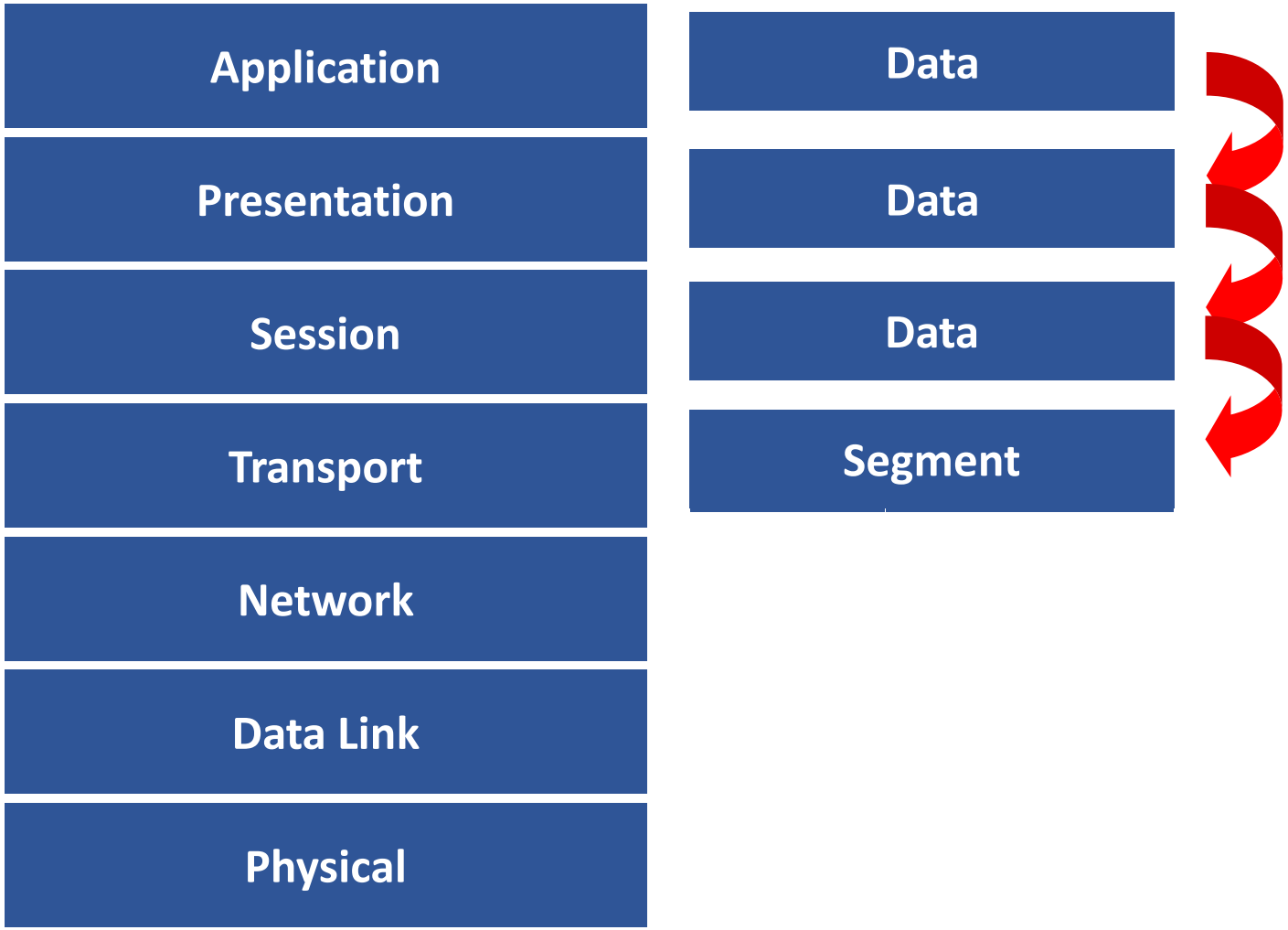
ARE
3/5

YOU
4/5

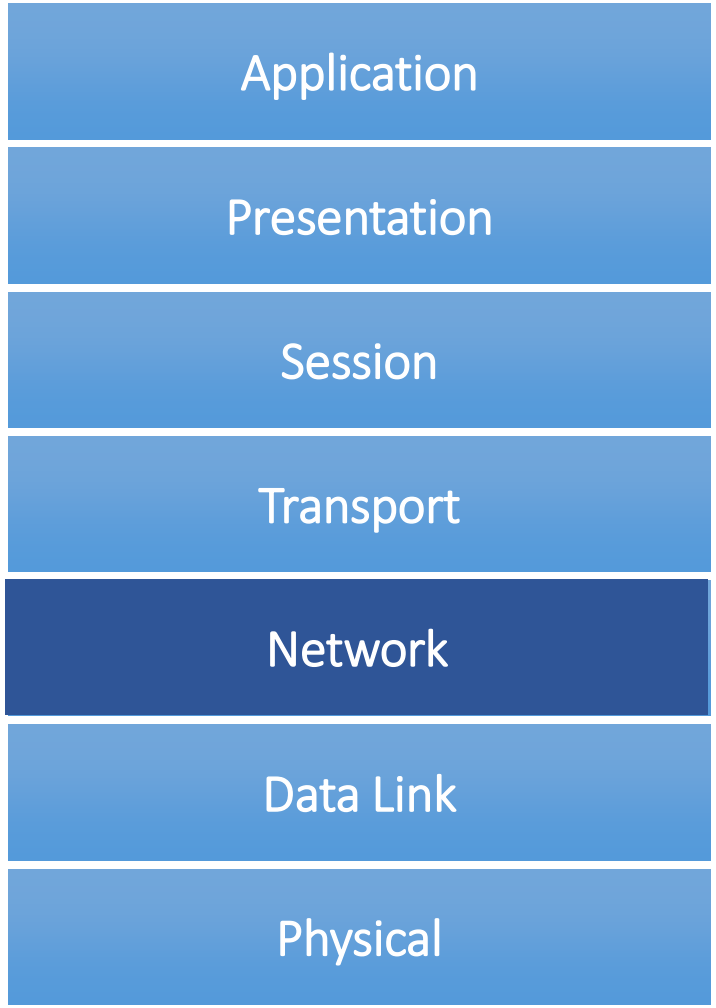
?
5/5



Data flow from Transport Layer



Network Layer



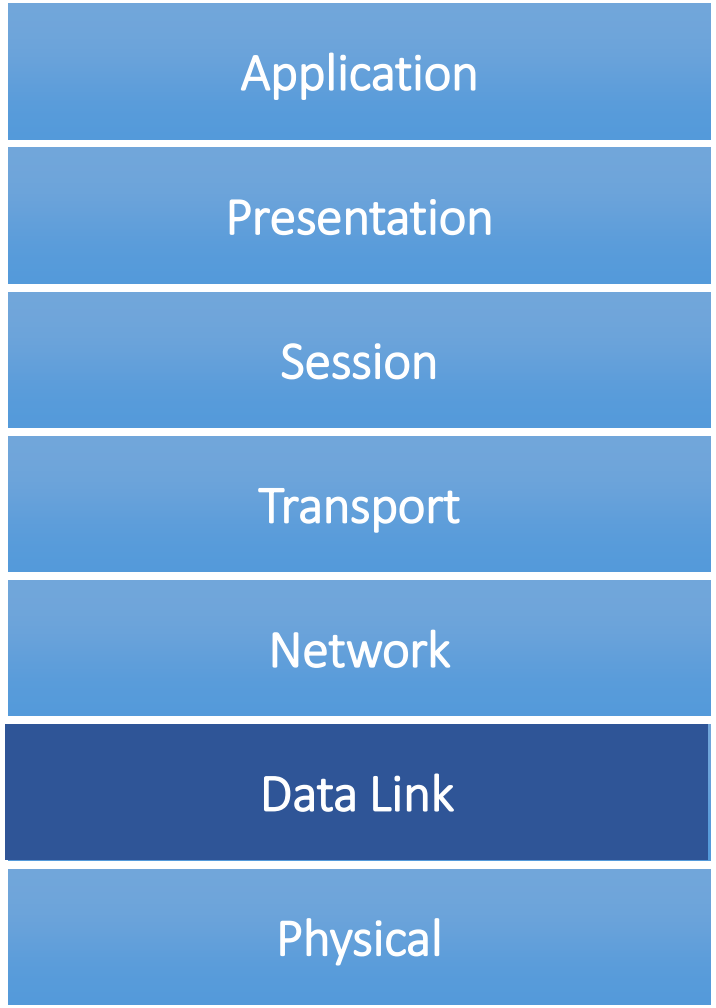
Network Layer : It provides Logical addressing & Path determination (Routing)
The protocols that work in this layer are:
Routed Protocols :
IP, IPX, AppleTalk.. Etc
Routed protocols used to carry user data between hosts.
Routing Protocols :
RIP, OSPF.. Etc
Routing protocols performs Path determination (Routing).

Data flow from Network Layer

Device that works at Network Layer is Router

Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data Link	
Physical	

Datalink Layer



Datalink Layer

It has 2 sub layers

•MAC (Media Access Control) It provides reliable transit of data across a physical link.

It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check)

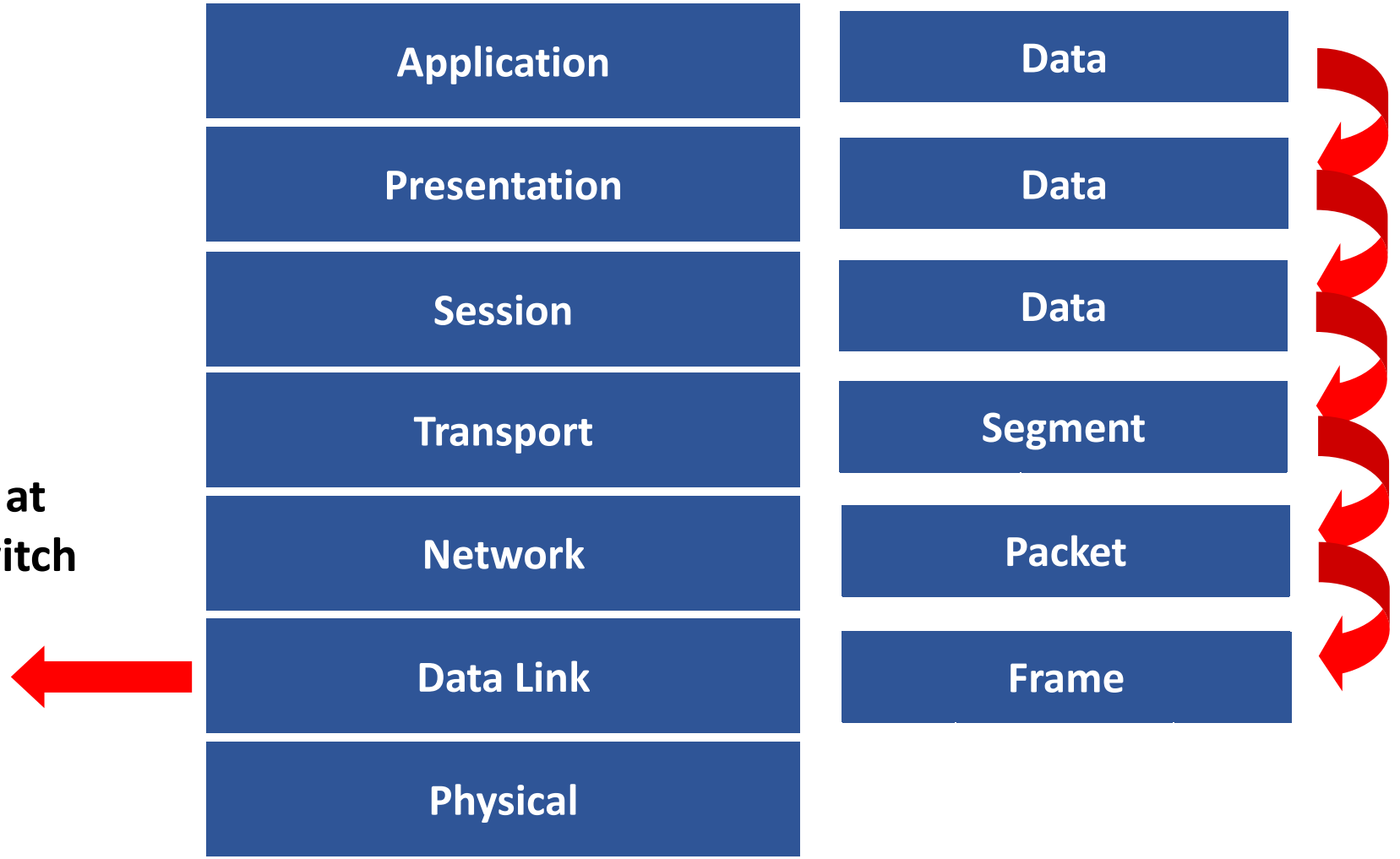
Ex: Ethernet, Token ring…etc

•LLC (Logical Link Control)

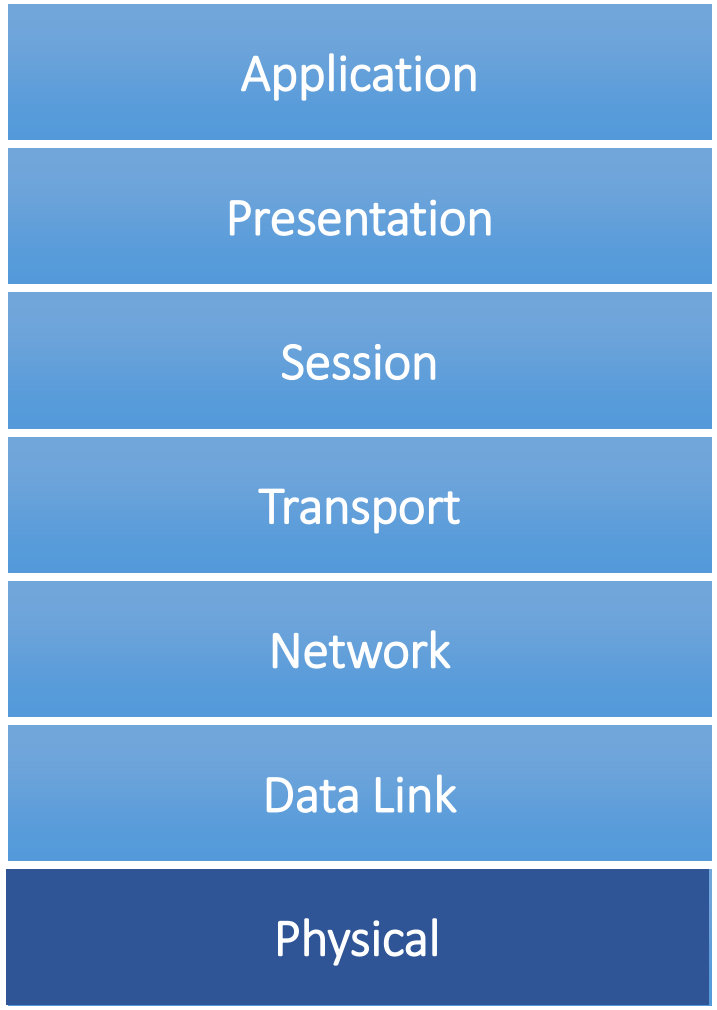
It provides communication with Network layer.

Data flow from Data link Layer

Devices that work at Data link layer is Switch



Physical Layer



Physical Layer : It defines the electrical, Mechanical & functional specifications for communication between the Network devices.

The functions described at this layer are

Encoding/decoding:

It is the process of converting the binary data into signals based on the type of the media.

Copper media : Electrical signals of different voltages

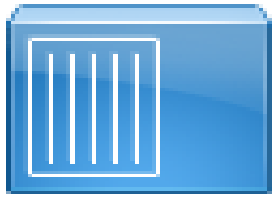
Fiber media: Light pulses of different wavelengths

Wireless media: Radio frequency waves

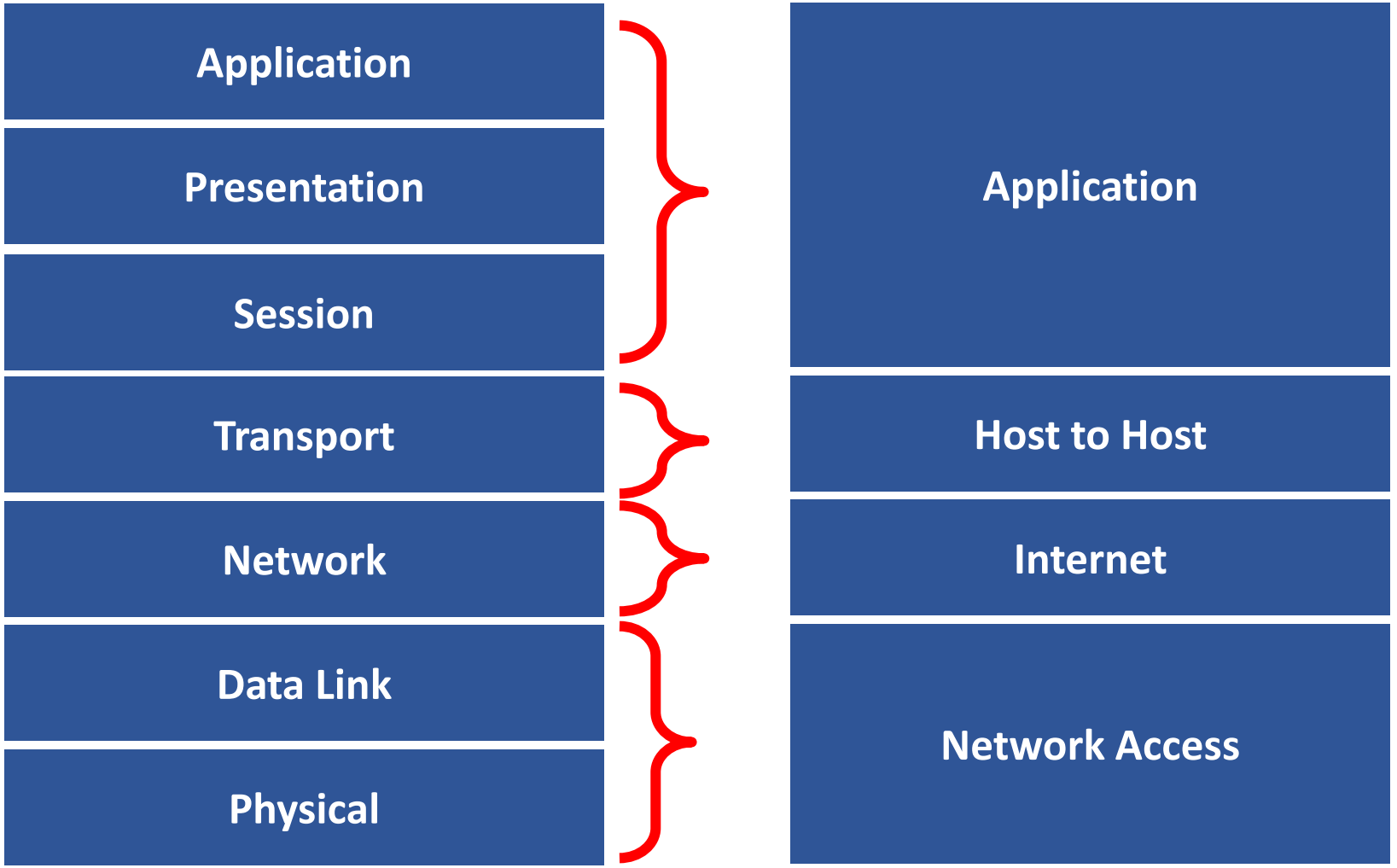
Data flow from Physical Layer

Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bits

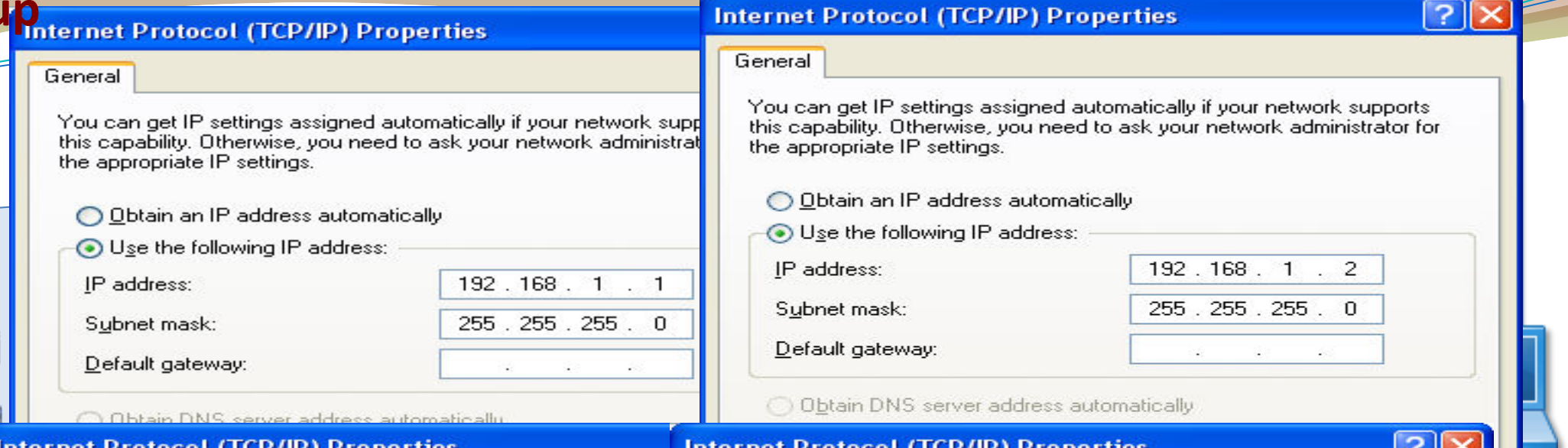
Devices that work at physical layer are Hub , Repeater



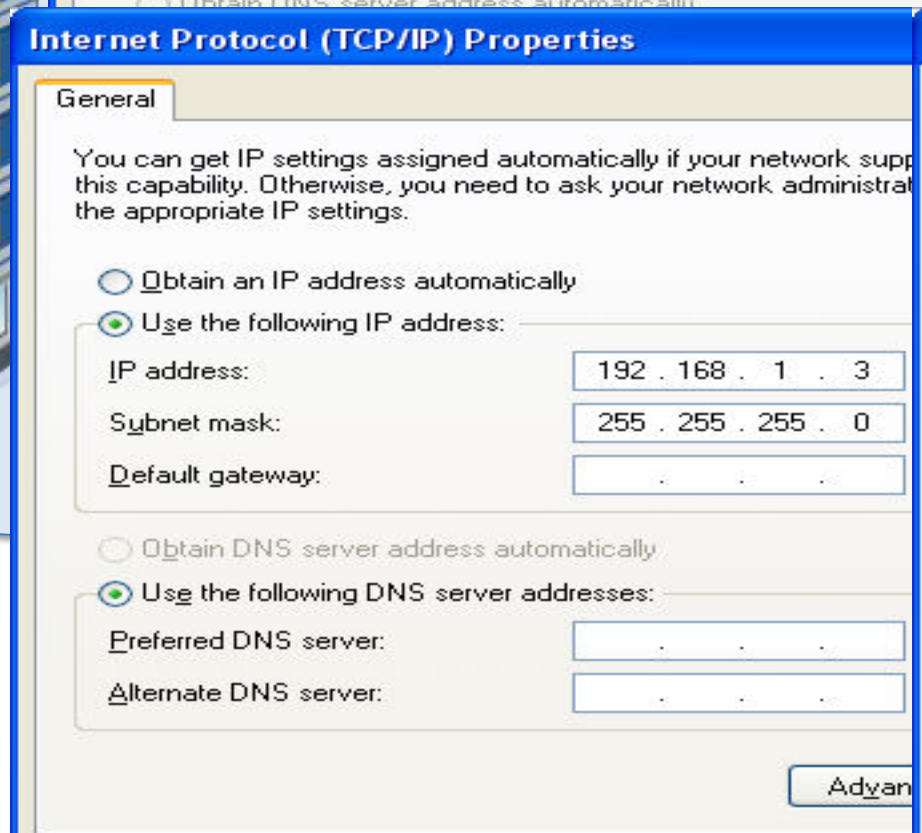
Comparison between OSI & TCP/IP Model

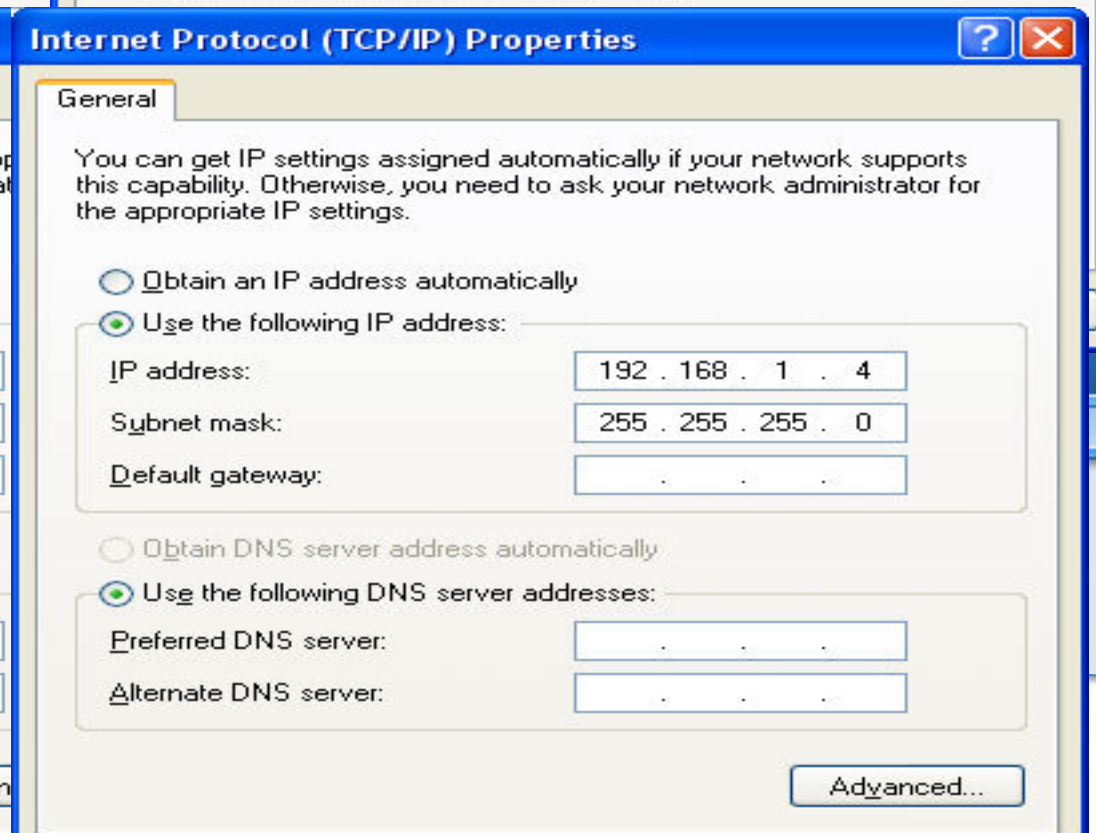


LAN Setup


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supp
this capability. Otherwise, you need to ask your network administrat
the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway:

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supp
this capability. Otherwise, you need to ask your network administrat
the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 3
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advan


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 4
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...

IP Addressing

IP Address

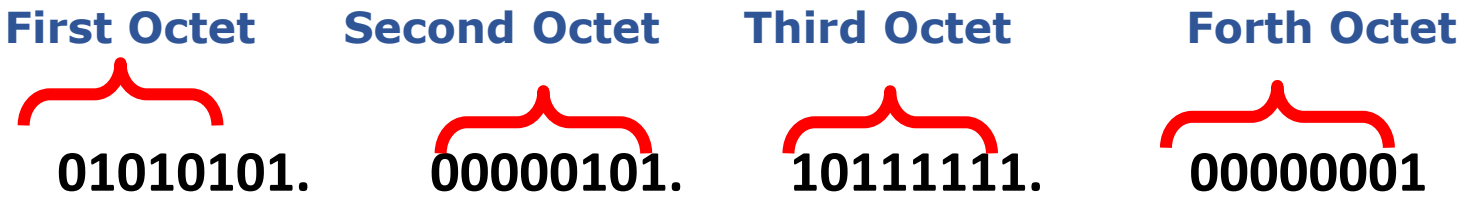
- IP Address is a Logical Address
- It is a Network Layer address (Layer 3)
- Two Versions of IP:
  - IP version 4 is a 32 bit address
  - IP version 6 is a 128 bit address

IP version 4

- Bit is represent by 0 or 1 (i.e. Binary)
- IP address in binary form (32 bits):

01010101000001011011111100000001

- 32 bits are divided into 4 Octets:



- IP address in decimal form:

85.5.191.1

IPv4 address range

Taking Example for First Octet :
Total 8 bits, Value will be 0's and 1's
i.e. 2^8 = 256 combination

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
0	0	0	0	0	0	0	0	=	0
0	0	0	0	0	0	0	1	=	1
0	0	0	0	0	0	1	0	=	2
0	0	0	0	0	0	1	1	=	3
0	0	0	0	0	1	0	0	=	4
1	1	1	1	1	1	1	1	=	255

Total IP Address Range
0 . 0 . 0 . 0
to
255.255.255.255

Binary to Decimal

128	64	32	16	8	4	2	1	Answer
1	1	0	0	0	0	0	0	192
0	0	0	0	1	0	1	0	10
1	0	1	0	1	0	0	0	168
1	0	1	0	1	1	0	0	172
0	0	0	1	0	0	0	0	16

Decimal to Binary

Decimal	128	64	32	16	8	4	2	1
18	0	0	0	1	0	0	1	0
152	1	0	0	1	1	0	0	0
200	1	1	0	0	1	0	0	0
15	0	0	0	0	1	1	1	1
240	1	1	1	1	0	0	0	0

IP Address Classification

IP address are divided into 5 Classes

- **CLASS A**
- **CLASS B**
- **CLASS C**

Used in LAN & WAN

- **CLASS D** — Reserved for Multicasting
- **CLASS E** — Reserved for Research & Development

Priority Bit

- Priority Bit is used for IP Address classification.
- Most significant bit(s) from the first octet are selected for Priority Bit(s).
- Class A priority bit is 0
- Class B priority bits are 10
- Class C priority bits are 110
- Class D priority bits are 1110
- Class E priority bits are 1111

Class A Range

- In Class A : First bit of the first octet is reserved as priority bit, bit value is zero.
- 0xxxxxxx. xxxxxxxx. xxxxxxxx. Xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
0	0	0	0	0	0	0	0	=	0
0	0	0	0	0	0	0	1	=	1
0	0	0	0	0	0	1	0	=	2
0	0	0	0	0	0	1	1	=	3
0	0	0	0	0	1	0	0	=	4
0	1	1	1	1	1	1	1	=	127

Class A Range
0 . 0 . 0 . 0 to
127 . 255 . 255 .255

Class B Range

- In Class B : First two bits of the first octet are reserved as priority bits, bit value as 10.
- 10xxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	0	0	0	0	0	0	0	=	128
1	0	0	0	0	0	0	1	=	129
1	0	0	0	0	0	1	0	=	130
1	0	0	0	0	0	1	1	=	131
1	0	0	0	0	1	0	0	=	132
1	0	1	1	1	1	1	1	=	191

Class B Range
128 . 0 . 0 . 0 to
191 . 255 . 255 .255

Class C Range

- In Class C : First three bits of the first octet are reserved as priority bits, bit value as 110.
- 110xxxxx. xxxxxxxx. xxxxxxxx. Xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	0	0	0	0	0	0	=	192
1	1	0	0	0	0	0	1	=	193
1	1	0	0	0	0	1	0	=	194
1	1	0	0	0	0	1	1	=	195
1	1	0	0	0	1	0	0	=	196
1	1	0	1	1	1	1	1	=	223

Class C Range
192 . 0 . 0 . 0 to
223 . 255 . 255 .255

Class D Range

- In Class D : First four bits of the first octet are reserved as priority bits, bit value as 1110.
- 1110xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	1	0	0	0	0	0	=	224
1	1	1	0	0	0	0	1	=	225
1	1	1	0	0	0	1	0	=	226
1	1	1	0	0	0	1	1	=	227
1	1	1	0	0	1	0	0	=	228
1	1	1	0	1	1	1	1	=	239

Class D Range
224 . 0 . 0 . 0 to
239 . 255 . 255 .255

Class E Range

- In Class E : First four bits of the first octet are reserved as priority bits, bit value as 1111.
- 1111xxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
1	1	1	1	0	0	0	0	=	240
1	1	1	1	0	0	0	1	=	241
1	1	1	1	0	0	1	0	=	242
1	1	1	1	0	0	1	1	=	243
1	1	1	1	0	1	0	0	=	244
1	1	1	1	1	1	1	1	=	255

Class E Range
240 . 0 . 0 . 0 to
255 . 255 . 255 .255

Ranges

Class A Range
0 . 0 . 0 . 0 to
127.255.255.255

Class B Range
128 . 0 . 0 . 0 to
191.255.255.255

Class C Range
192 . 0 . 0 . 0 to
223 . 255 . 255 .255

Class D Range
224 . 0 . 0 . 0 to
239 . 255 . 255 .255

Class E Range
240 . 0 . 0 . 0 to
255 . 255 . 255 .255

Identifying Class

IP Address	Class
10.1.100.1	A
150.17.2.200	B
192.1.1.1	C
224.0.0.10	D
120.200.1.1	A

Octet Format

- IP address is divided into Network & Host Portion
  - CLASS A is written as N.H.H.H
  - CLASS B is written as N.N.H.H
  - CLASS C is written as N.N.N.H

CLASS A – No. Networks & Hosts

- Class A Octet Format is N.H.H.H

  Network bits : 8 Host bits : 24

- No. of Networks

  = $2^{\text{no of network bits– Priority bit}}$

  = 2^{8-1} (-1 is Priority Bit for Class A)

  = 2^{7}

  = 128 – 2 (-2 is for 0 & 127 Network)

  = 126 Networks

- No. of Host

  = $2^{\text{no of host bits}} - 2$

  = 2^{24} – 2 (-2 is for Network ID & Broadcast ID)

  = 16777216 - 2

  = 16777214 Hosts/Network

CLASS B – No. Networks & Hosts

- Class B Octet Format is N.N.H.H

  Network bits : 16 Host bits : 16

- No. of Networks

  = $2^{\text{no of network bits– Priority bit}}$

  = 2^{16-2} (-2 is Priority Bit for Class B)

  = 2^{14}

  = 16384 Networks

- No. of Host

  = $2^{\text{no of host bits}} - 2$

  = $2^{16} – 2$ (-2 is for Network ID & Broadcast ID)

  = 65536 - 2

  = 65534 Hosts/Network

CLASS C – No. Networks & Hosts

- Class C Octet Format is N.N.N.H

  Network bits : 24 Host bits : 8

- No. of Networks

  = $2^{\text{no of network bits– Priority bit}}$

  = 2^{24-3} (-3 is Priority Bit for Class C)

  = 2^{21}

  = 2097152 Networks

- No. of Host

  = $2^{\text{no of host bits}} - 2$

  = $2^{8} - 2$ (-2 is for Network ID & Broadcast ID)

  = 256 - 2

  = 254 Hosts/Network

Network & Broadcast Address

- Network address: This is the address that identifies the subnet of a host.
- Broadcast address: An IP Address that allows information to be sent to all machines on a given subnet rather than a specific machine.
- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

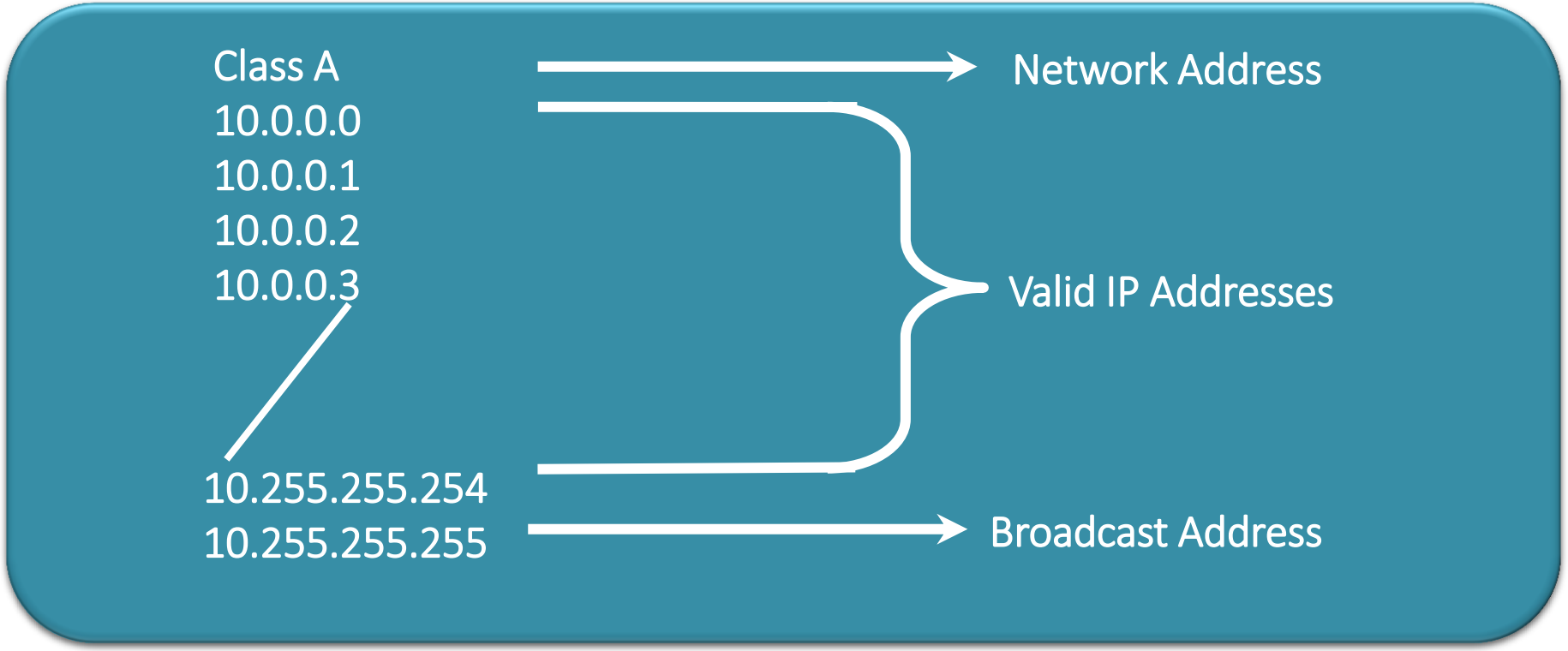
Example - Class A

- **Class A : N.H.H.H**
  - **Network Address :**

0xxxxxxx.00000000.00000000.00000000

  - **Broadcast Address :**

0xxxxxxx.11111111.11111111.11111111



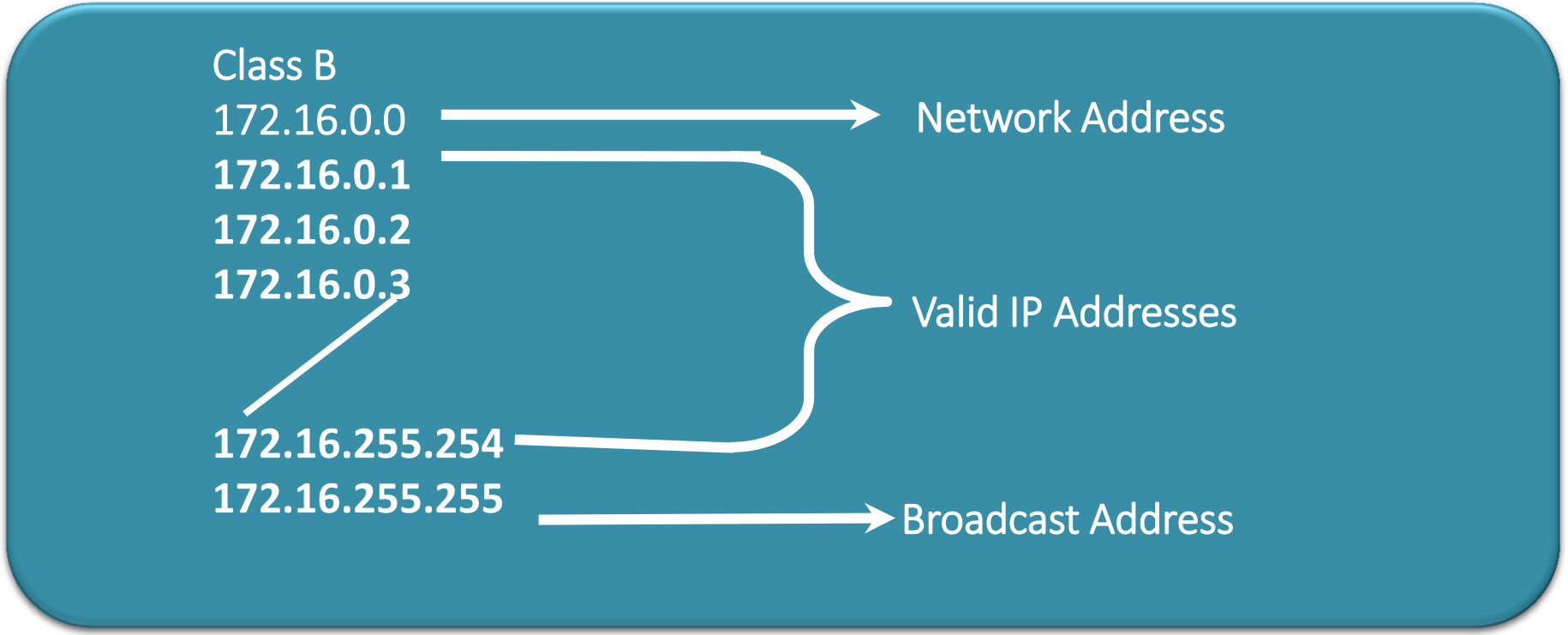
Example - Class B

- **Class B : N.N.H.H**
  - **Network Address :**

10xxxxxx.xxxxxxxx.00000000.00000000

  - **Broadcast Address :**

10xxxxxx.xxxxxxxx.11111111.11111111



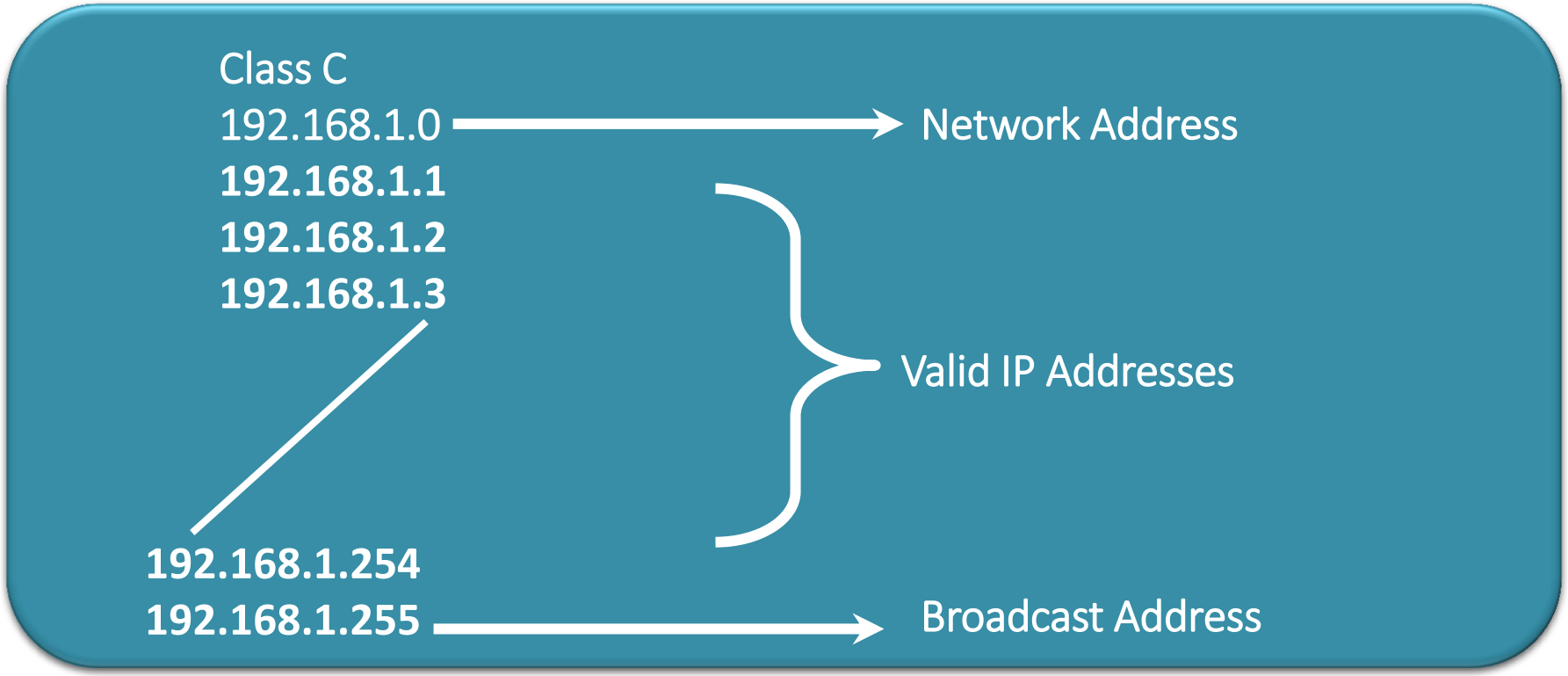
Example - Class C

- **Class C : N.N.N.H**
  - **Network Address :**

110xxxxx.xxxxxxxx.xxxxxxxx.00000000

  - **Broadcast Address :**

110xxxxx.xxxxxxxx.xxxxxxxx.11111111



Private IP Address

- **There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.**
- **These addresses are not Routable (or) valid on Internet.**

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

Subnet Mask

- Subnet Mask differentiates the Network and Host portions of an IP address
- Represented with all 1's in the network portion and with all 0's in the host portion.

Default Subnet Mask

- Class A : N.H.H.H
  11111111.00000000.00000000.00000000
  Default Subnet Mask for Class A is 255.0.0.0

- Class B : N.N.H.H
  11111111.11111111.00000000.00000000
  Default Subnet Mask for Class B is 255.255.0.0

- Class C : N.N.N.H
  11111111.11111111.11111111.00000000
  Default Subnet Mask for Class C is 255.255.255.0

Default subnet mask

IP Address	Default subnet mask
17.1.1.1	255.0.0.0
202.1.0.18	255.255.255.0
190.10.1.1	255.255.0.0
102.10.1.10	255.0.0.0
192.0.0.1	255.255.255.0

How Subnet Mask Works ?

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
ANDING PROCESS :
192.168.1.1 = 11000000.10101000.00000001.00000001
255.255.255.0 = 11111111.11111111.11111111.00000000
==========
192.168.1.0 = 11000000.10101000.00000001.00000000

==========

The output of an AND table is 1 if both its inputs are 1.

For all other possible inputs the output is 0.

Subnetting

Subnetting

- Creating Multiple independent Networks from a single Network
- Converting Host bits into Network bits
  (i.e. converting 0's into 1's)
- Subnetting can be performed in two ways
- FLSM (Fixed Length Subnet Mask)
- VLSM (Variable Length Subnet Mask)
- Subnetting can be done based on requirement
- Number of Networks Required?
- Number of Hosts Required?

Note:- It is very Useful for Internet Service Providers (ISP), Large Organizations /Companies etc.,

Requirement of Networks

- A corporate network has 200 PC's
- Which class of IP Address is preferred for the network ?

  Answer : class C
- There are 4 departments with 50 pc's each

Marketing	→	192.168.1.1 to 192.168.1.50
Sales	→	192.168.1.51 to 192.168.1.100
Finance	→	192.168.1.101 to 192.168.1.150
IT	→	192.168.1.151 to 192.168.1.200

- **Administrators requirement :**
- **Inter-department communication should not be there**

Solution :

- **Allocate different Networks to each Department**

i.e.,

Marketing	⟹	**192.168.1.1 to 192.168.1.50**
Sales	⟹	**192.168.2.1 to 192.168.2.50**
Finance	⟹	**192.168.3.1 to 192.168.3.50**
IT	⟹	**192.168.4.1 to 192.168.4.50**

Main Aim of Subnetting

- Problem with the previous scenario is
- Wastage of IP addresses, if it is Public IP addresses (Approx. 800)
- To reduce the wastage of IP addresses, we have Subnetting
  - Requirement of Networks

Requirement of Subnets – 4 no's ?

Class C : 192.168.1.0

255.255.255.0

Subnets required : 4 no's

= $2^n \geq$ Req. of Subnet

= $2^n \geq 4$

= $2^2 \geq 4$

= 4 subnets

Customized subnet mask =

255. 255. 255. 0

11111111. 11111111. 11111111. 00000000

. 11000000

255. 255. 255. 192

Calculation of Hosts / subnet

= $2^h - 2$ (-2 is for Network ID & Broadcast ID)

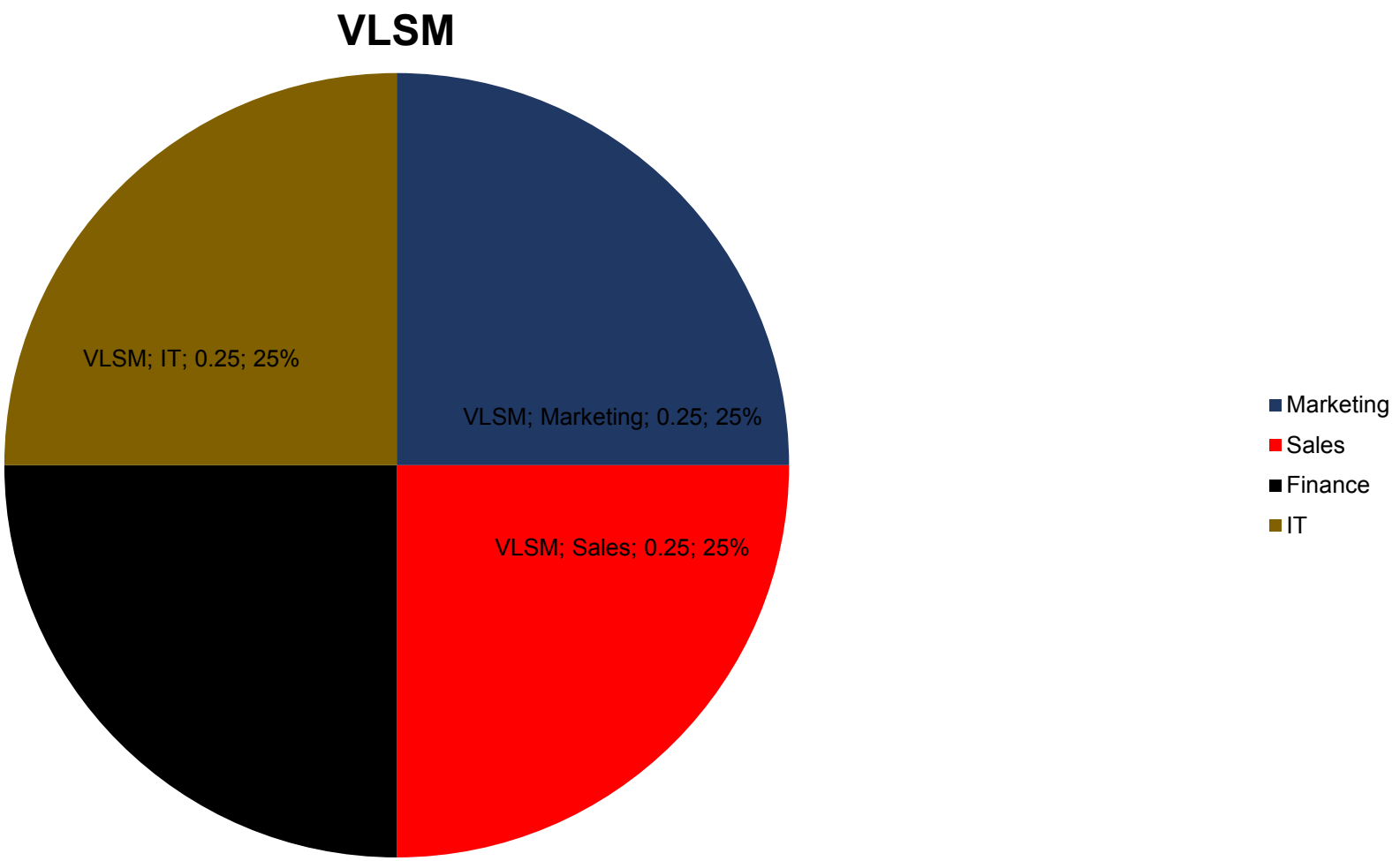
= $2^6 - 2$

= 64 – 2

= 62 Hosts/subnet

Subnet Range	
Network ID	Broadcast ID
192.168.1.1	192.168.1.63
192.168.1.64	192.168.1.127
192.168.1.128	192.168.1.191
192.168.1.192	192.168.1.255

FLSM


VLSM
VLSM; IT; 0.25; 25%
VLSM; Marketing; 0.25; 25%
VLSM; Sales; 0.25; 25%
Marketing
Sales
Finance
IT

VLSM

- Subnetting a subnet is called as Variable Length Subnet Mask
- VLSMs provide the capability to include more than one subnet mask within a major network

Requirement of Hosts

- In corporate network there are 4 departments and their requirement as follows,

Marketing	→	10
Sales	→	50
Finance	→	25
IT	→	100

Arrange them in Descending Order

IT	100
Sales	50
Finance	25
Marketing	10

Requirement of Hosts

Class C : 192.168.1.0

255.255.255.0

Hosts required : 100 , 50 , 25 and 10

First , we calculate for IT = 100 Hosts

$2^h - 2 \geq$ Req. of Hosts

$= 2^h - 2 \geq 100$

$= 2^7 - 2 \geq 100$

$= 128 - 2 = 126$ hosts/subnet

Customized subnet mask =

255. 255. 255. 0

11111111. 11111111. 11111111. 00000000

. 10000000

255. 255. 255. 128

Calculation of subnets

= 2^n

= 2^1

= 2

= 2 Hosts/subnet

Subnet Range

Network ID	Broadcast ID	
192.168.1.0	192.168.1.127	I T
192.168.1.128	192.168.1.255	

Now , Available network is 192.168.1.128 to 192.168.1.255

Next, we calculate for Sales = 50 Hosts

$2^h - 2 \geq$ Req. of Hosts

$= 2^h - 2 \geq 50$

$= 2^6 - 2 \geq 50$

$= 64 - 2 = 62$ hosts/subnet

Customized subnet mask =

255. 255. 255. 128

11111111. 11111111. 11111111. 10000000

. 11000000

255. 255. 255. 192

Calculation of subnets

= 2^n

= 2^1

= 2

= 2 Hosts/subnet

Subnet Range		
Network ID	Broadcast ID	
192.168.1.128	to 192.168.1.191	SALES
192.168.1.192	to 192.168.1.255	

- **Similarly, we can calculate for Finance = 25 Hosts**

Using 192.168.1.192 to 192.168.1.255

Subnet Mask 255.255.255.192

$2^h - 2 \geq$ Req. of Hosts

$= 2^h - 2 \geq 25$

$= 2^5 - 2 \geq 25$

$= 32 - 2 = 30$ hosts/subnet

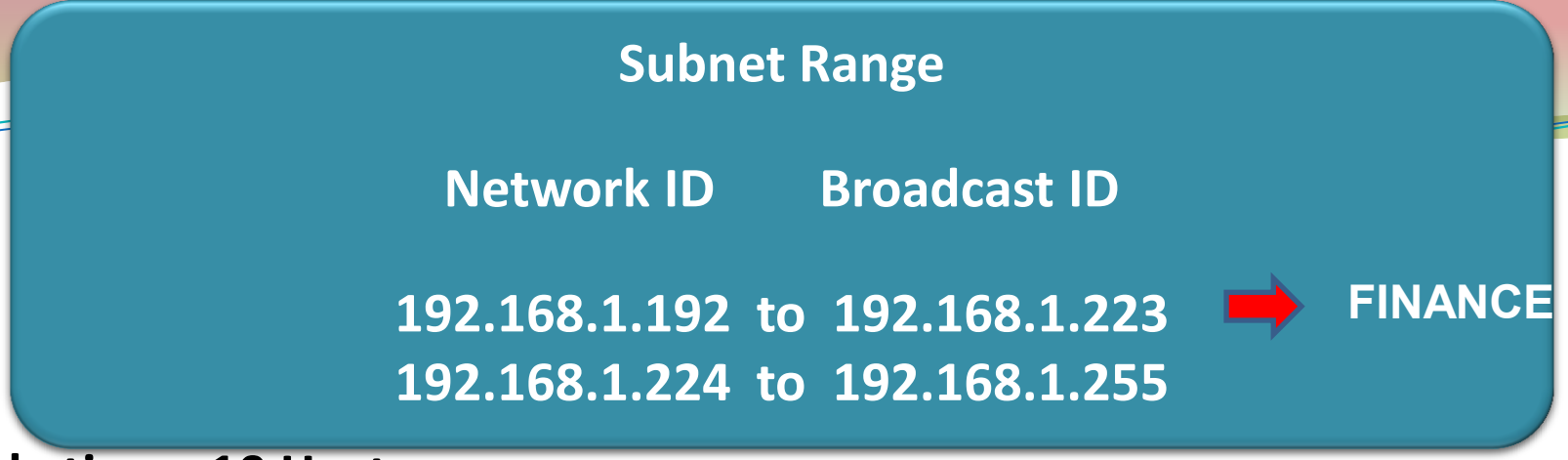
Customized subnet mask =

255. 255. 255. 192

11111111. 11111111. 11111111. 11000000

. 11100000

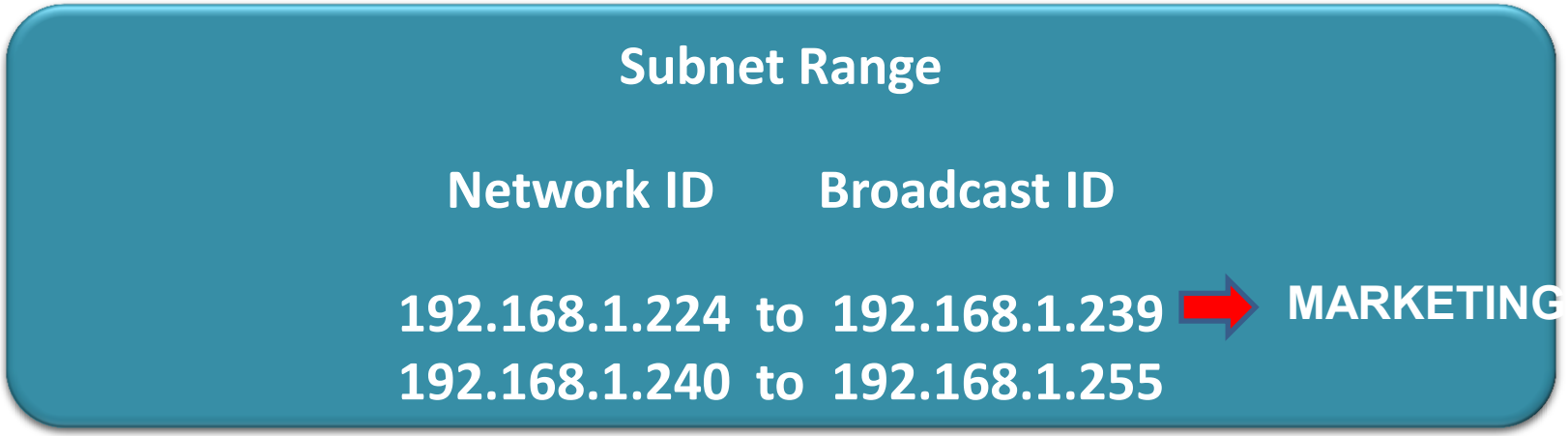
255. 255. 255. 224



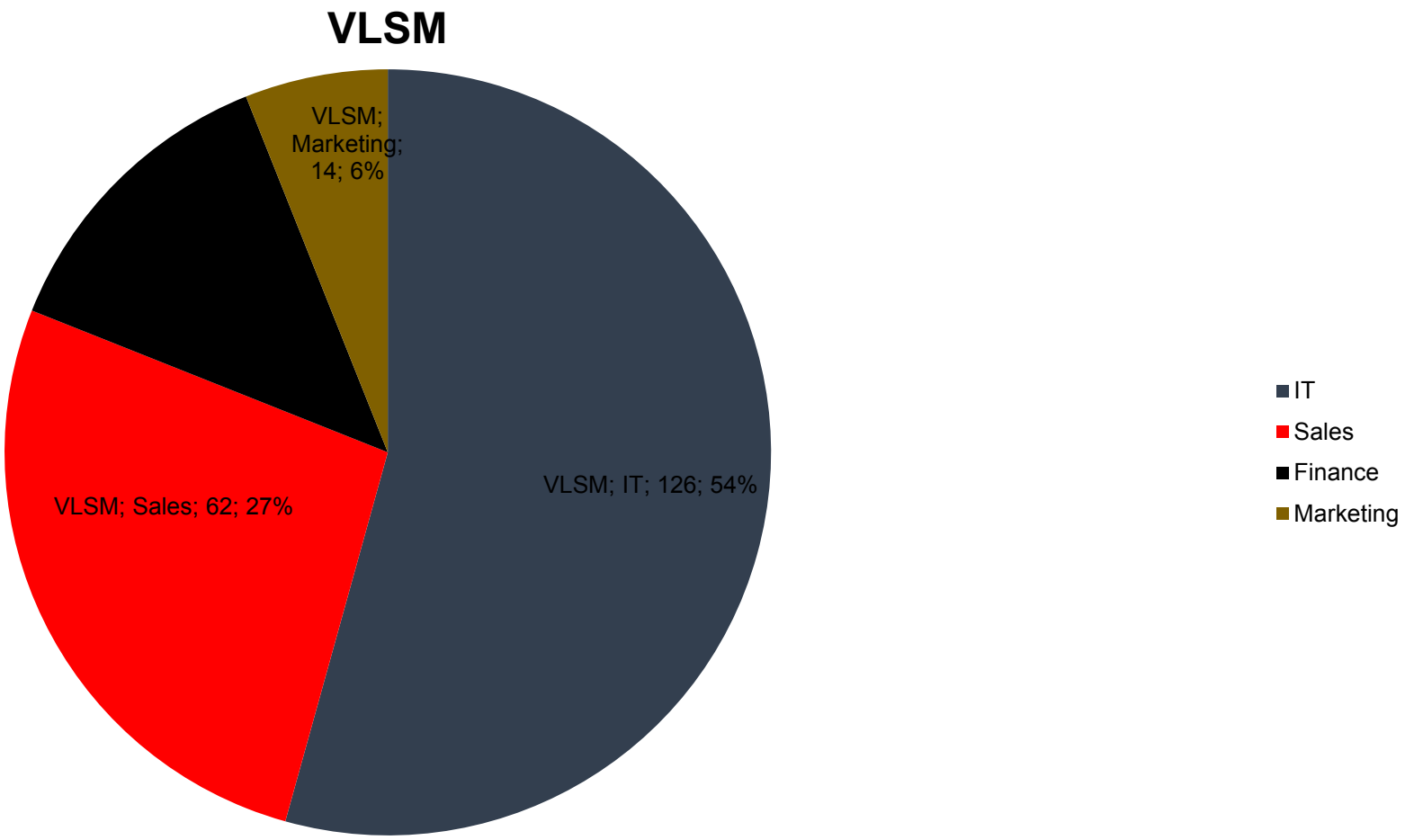
•For Marketing = 10 Hosts

Using 192.168.1.224 to 192.168.1.255 with Subnetmask 255.255.255.224

•If we calculate, then we will get customized subnet mask 255.255.255.240 and Range as follows



VLSM


VLSM
VLSM; Marketing; 14; 6%
VLSM; Sales; 62; 27%
VLSM; IT; 126; 54%
IT
Sales
Finance
Marketing

Power table

POWER TABLE

2^5 = [illegible]	2^{10} = [illegible]	2^{20} = [illegible]	2^{30} = [illegible]

Some Important Values

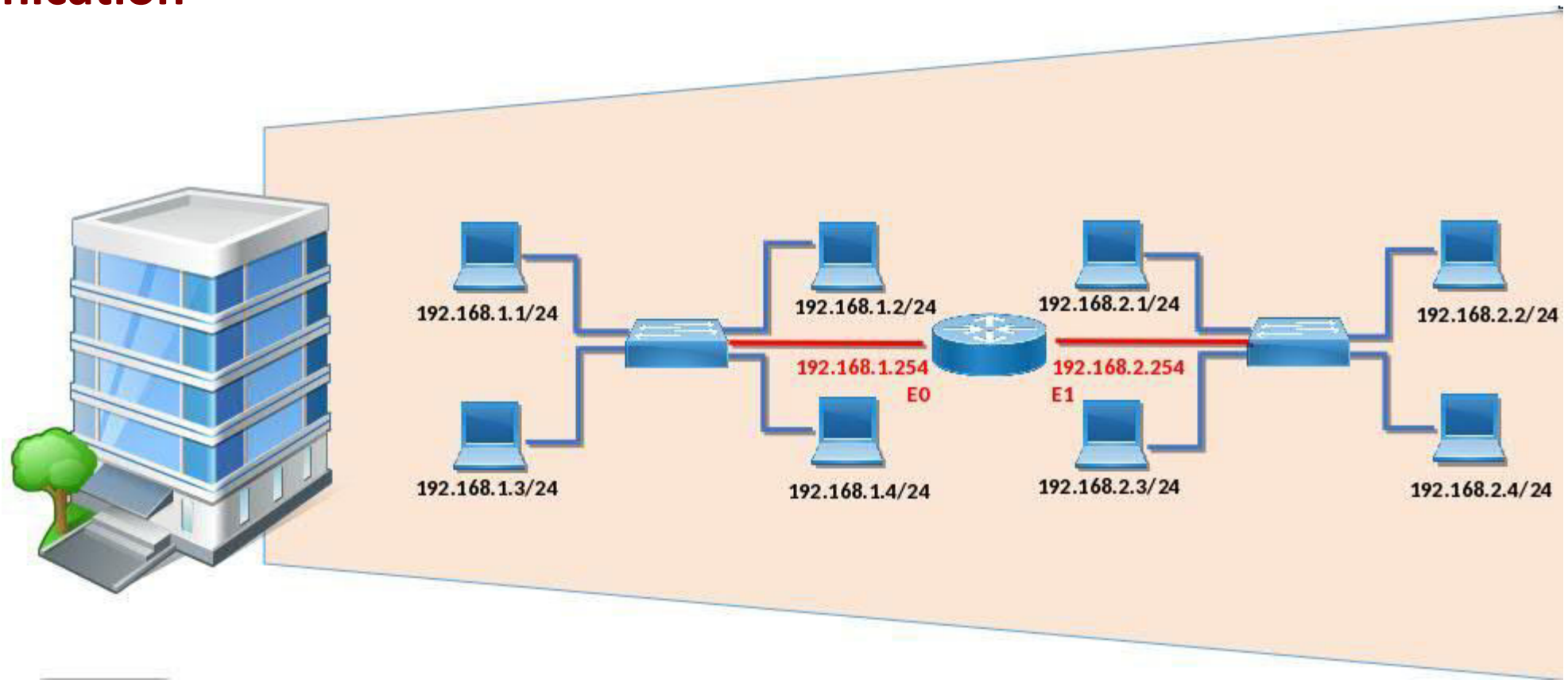
VALUES IN SUBNET MASK		
Bit	Value	Mask
1	128	10000000
2	192	11000000
3	224	11100000
4	240	11110000
5	248	11111000
6	252	11111100
7	254	11111110
8	255	11111111

Slash notation

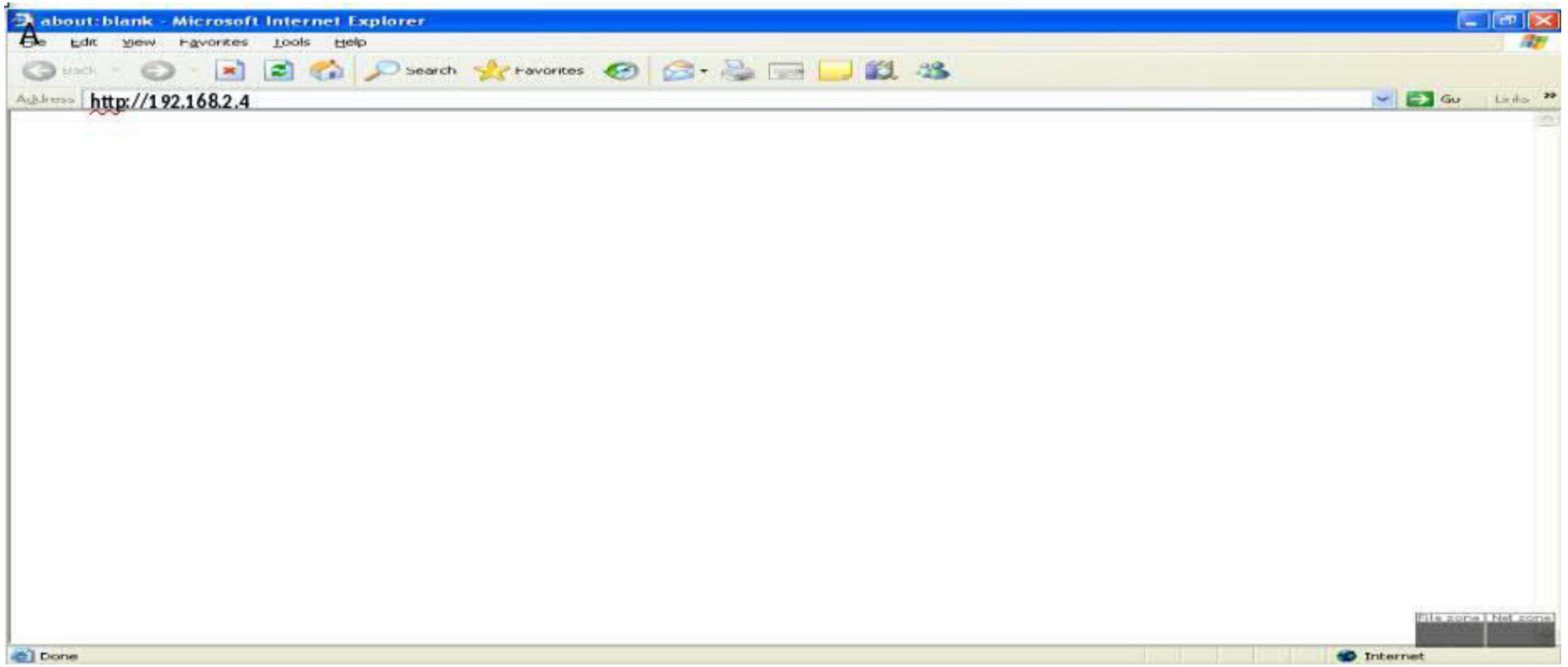
Slash notation	subnet mask
/8	255.0.0.0
/12	255.240.0.0
/16	255.255.0.0
/22	255.255.252.0
/24	255.255.255.0

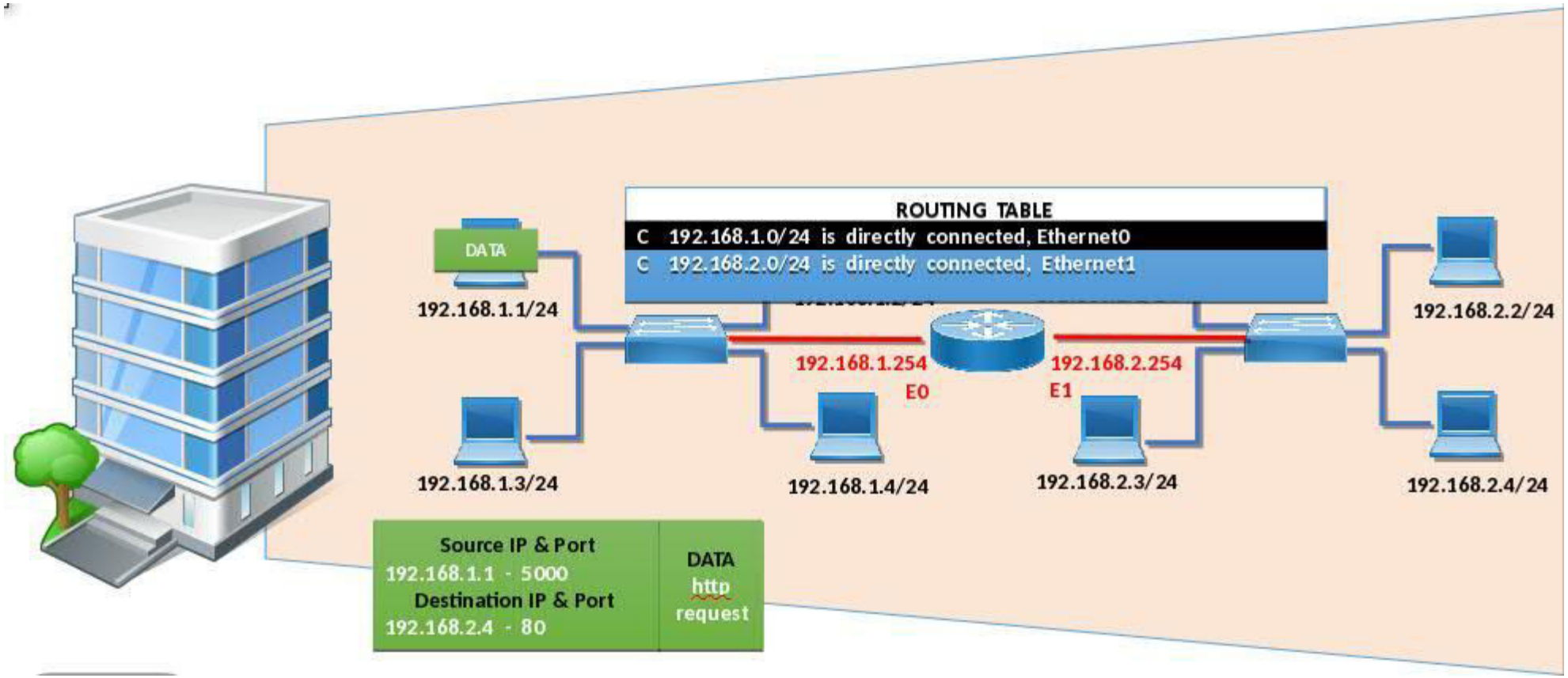
Different Network Communication

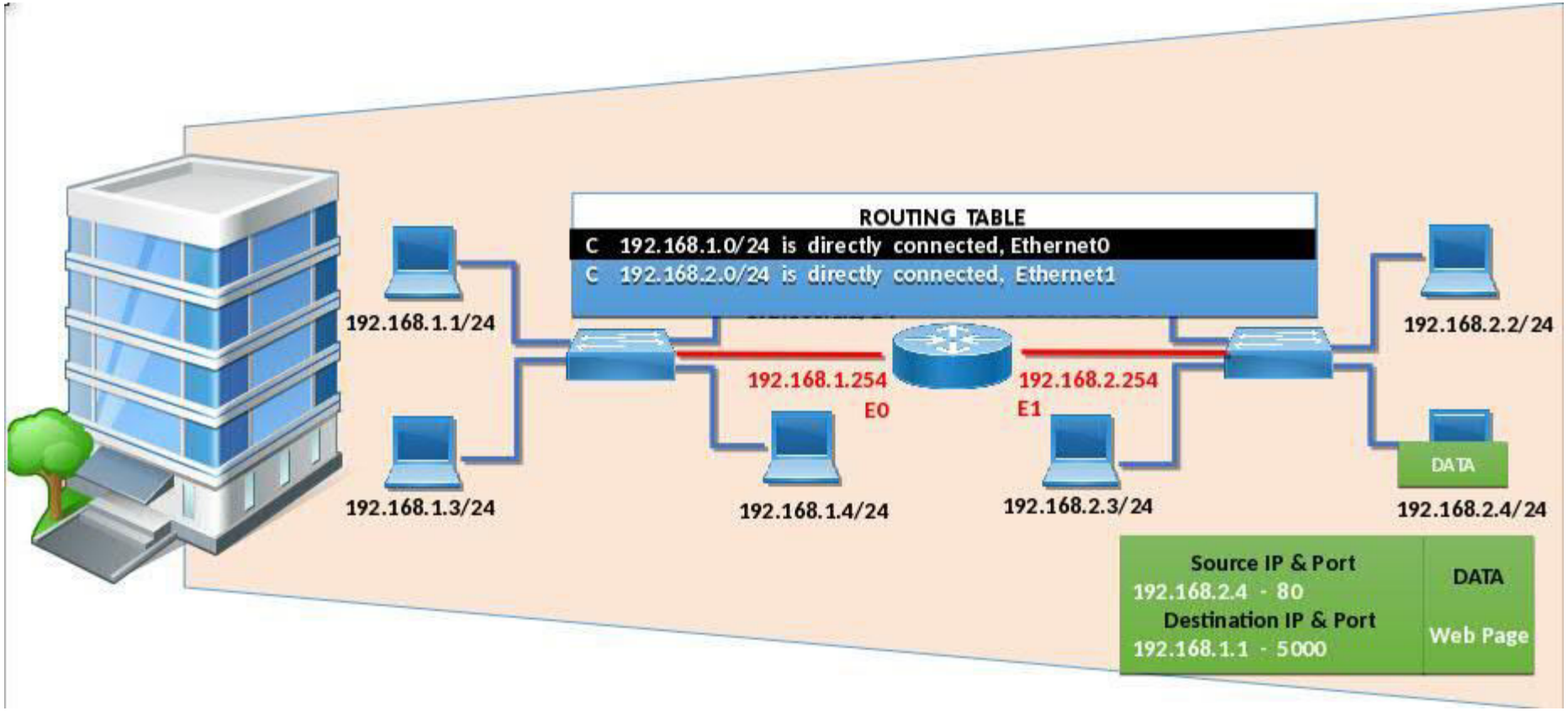
LAN - Different Network Communication



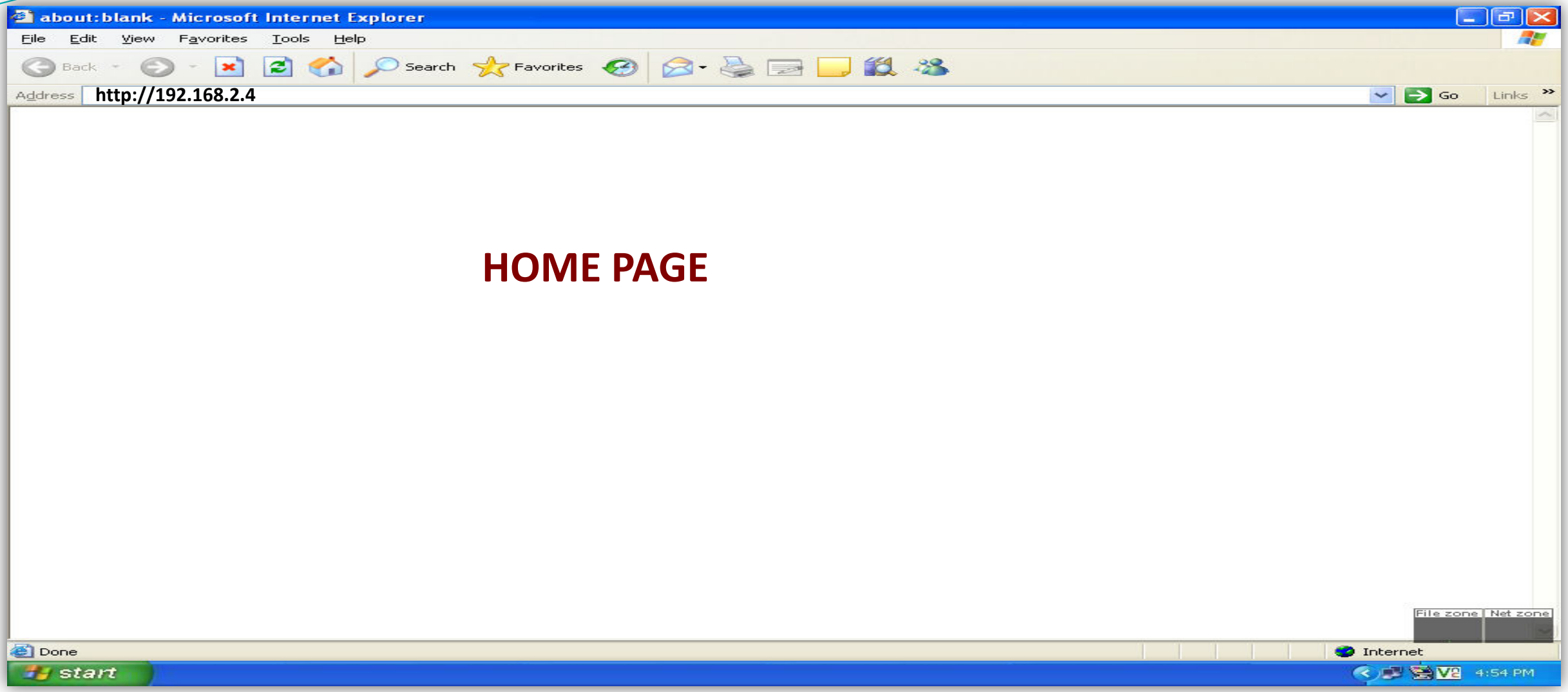
LAN - Different Network Communication


about:blank - Microsoft Internet Explorer
Edit View Favorites Tools Help
Search
Favorites
http://192.168.2.4
Done
Internet


ROUTING TABLE
C 192.168.1.0/24 is directly connected, Ethernet0
C 192.168.2.0/24 is directly connected, Ethernet1
DATA
192.168.1.1/24
192.168.1.3/24
192.168.1.4/24
192.168.1.254
E0
192.168.2.254
E1
192.168.2.3/24
192.168.2.2/24
192.168.2.4/24
Source IP & Port
192.168.1.1 - 5000
Destination IP & Port
192.168.2.4 - 80
DATA
http
request


ROUTING TABLE
C 192.168.1.0/24 is directly connected, Ethernet0
C 192.168.2.0/24 is directly connected, Ethernet1
192.168.1.1/24
192.168.1.3/24
192.168.1.254
E0
192.168.1.4/24
192.168.2.254
E1
192.168.2.3/24
192.168.2.2/24
DATA
192.168.2.4/24
Source IP & Port
192.168.2.4 - 80
Destination IP & Port
192.168.1.1 - 5000
DATA
Web Page

LAN - Different Network Communication



Introduction to Routers

Router

- Router is an internetworking device.
- It enables communication between two or more different logical networks.
- It is a Network Layer (layer 3) device.
- It comes from the word “ROUTE”. Hence it is also a device that finds the best route (path) for networks.
- The IP of Router is the default gateway for all devices in LAN.

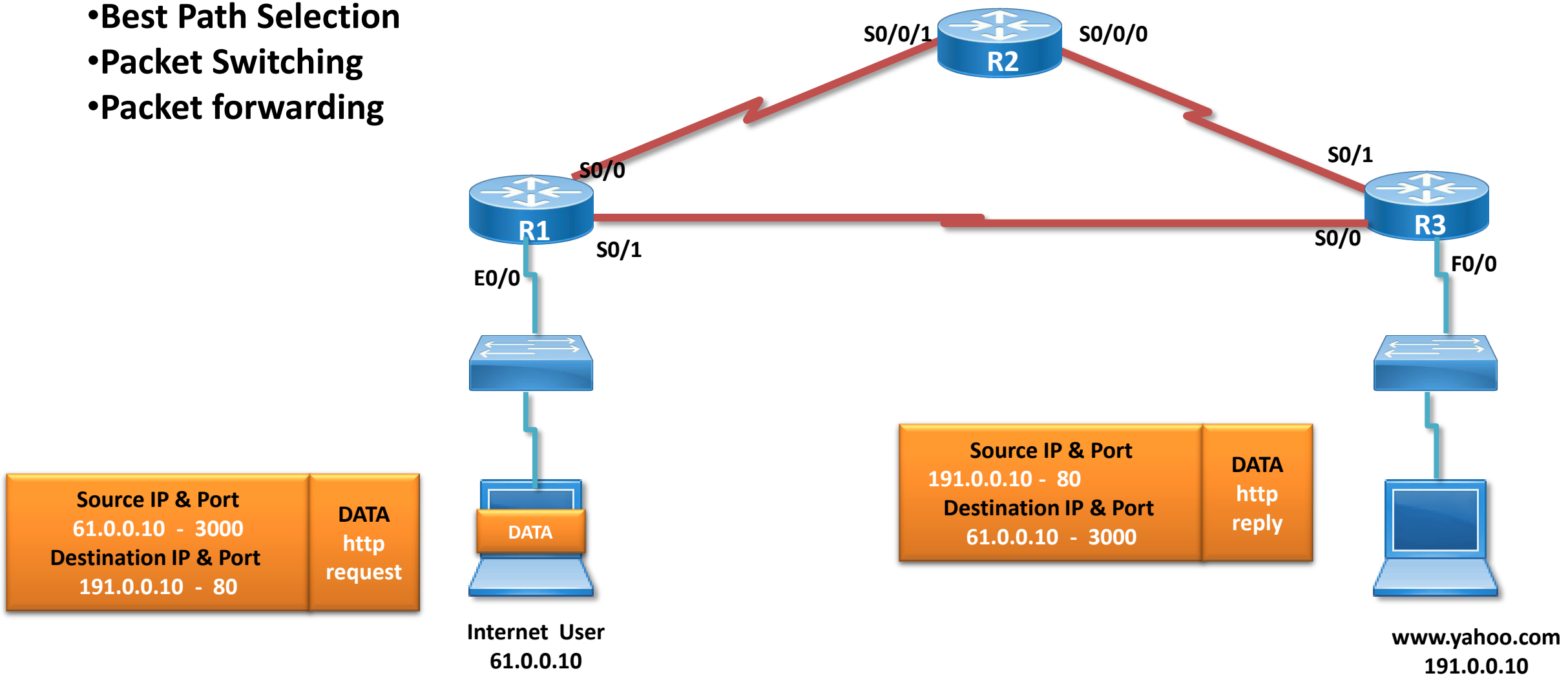
Type of Routers

There are two type of Routers

- Hardware Routers:
  - Cisco, Juniper, Multicom, HP, Dlink, Maipu and many more…
- Software Routers:
  - Microsoft Server, Linux Server

Functions of a Router

- Inter-network Communication
- Best Path Selection
- Packet Switching
- Packet forwarding



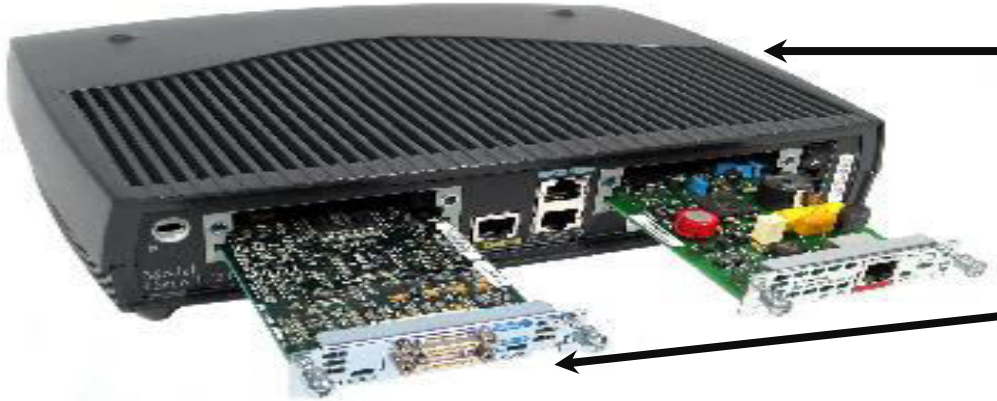
External Components of a Router

Types of Hardware Routers

- Fixed Router
- Modular Router

Fixed Router

Modular Router

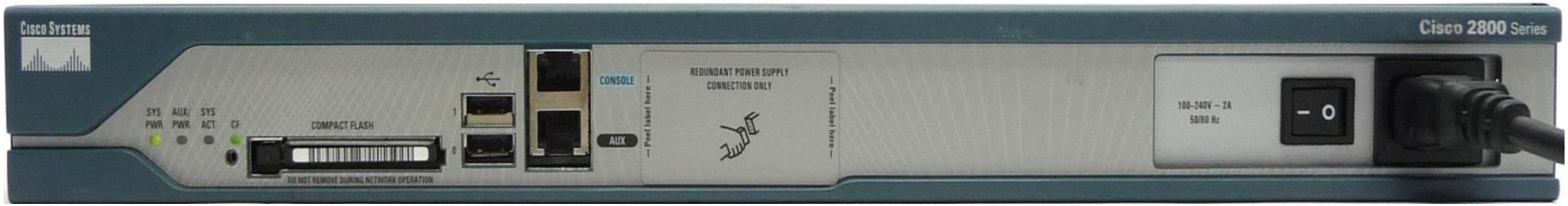


Cisco 1700 Modular Router

WIC – Wan Interface Card

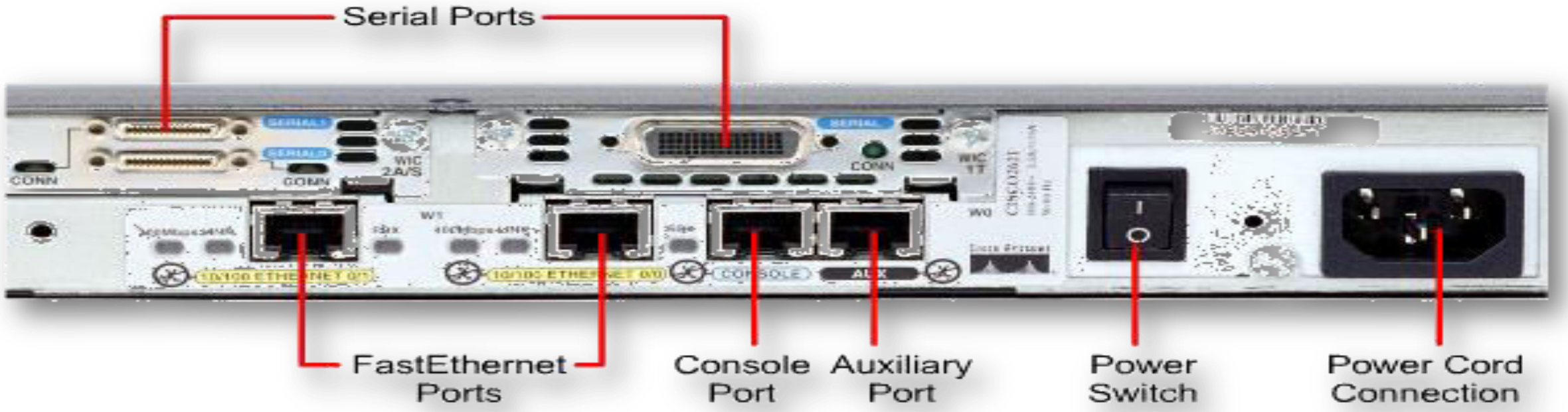
Cisco 2600 Modular Router

2800 Series


Cisco Systems
Cisco 2800 Series
SYS PWR
AUX/ PWR
SYS ACT
CF
COMPACT FLASH
DO NOT REMOVE DURING NETWORK OPERATION
CONSOLE
AUX
REDUNDANT POWER SUPPLY
CONNECTION ONLY
Peel label here
100-240V ~ 2A
50/60 Hz

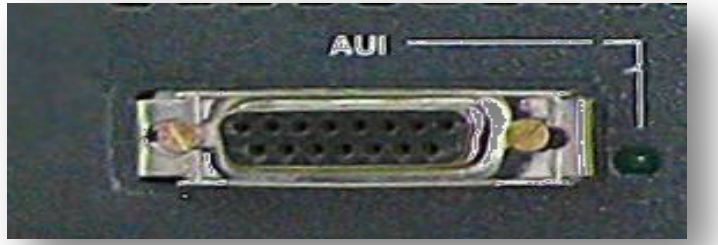

HWIC 3
HWIC 1
DO NOT INSTALL INTERFACE CARDS WITH POWER APPLIED
SEE MANUAL BEFORE INSTALLATION
B1
B2
NT1
ISDN BRI U
WIC 1B-U V2
LP
AL
CD
T1 DSU/CSU
LOOP BACK
WIC 1DSU-T1 V2
SN:FTX1128A649
COM7C00ARA
CISCO2811
A= ACT
S= SPEED
F= FDX
L= LINK
FE 0/1
FE 0/0
PVDM1
PVDM0
AIM1
AIM0


AUI
SERIAL 0
SERIAL 1
CONSOLE
AUX
Input :100-240VAC
Freq : 50/60 HZ
Current : 1.2-0.6 A
Watts : 40 W
Safety Warning : See instructions for use
Cisco 2501


Serial Ports
FastEthernet Ports
Console Port
Auxiliary Port
Power Switch
Power Cord Connection

Attachment Unit Interface

- Attachment Unit Interface (AUI) is used to connect the Router to the LAN.
- It is also called as the Ethernet interface.
- AUI is an DB 15 pin female interface.
- Transceiver is used to connect AUI port to LAN HUB / Switch.
- Transceiver converts DB-15 signal to RJ-45.



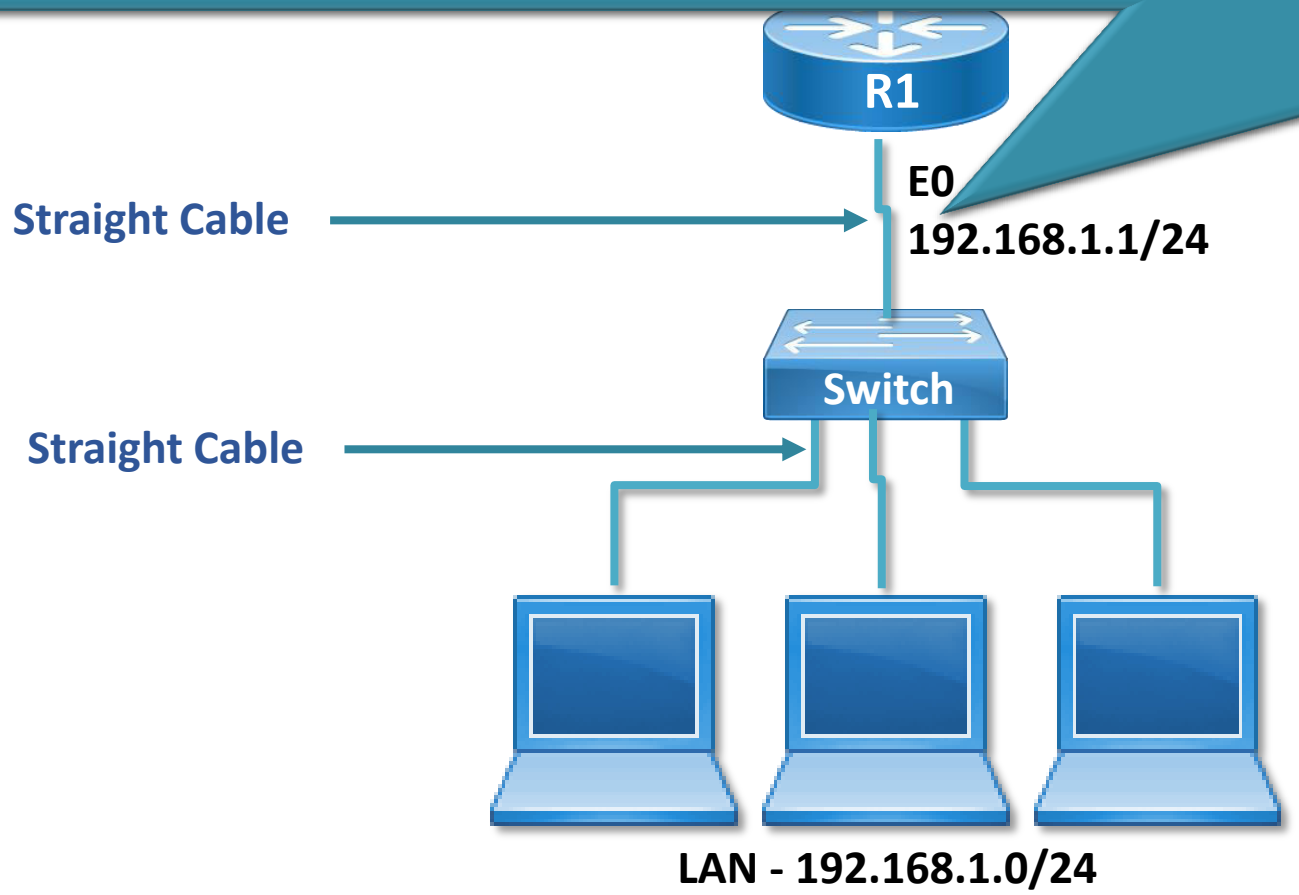
Transceiver

Other LAN Interfaces - RJ-45 ports

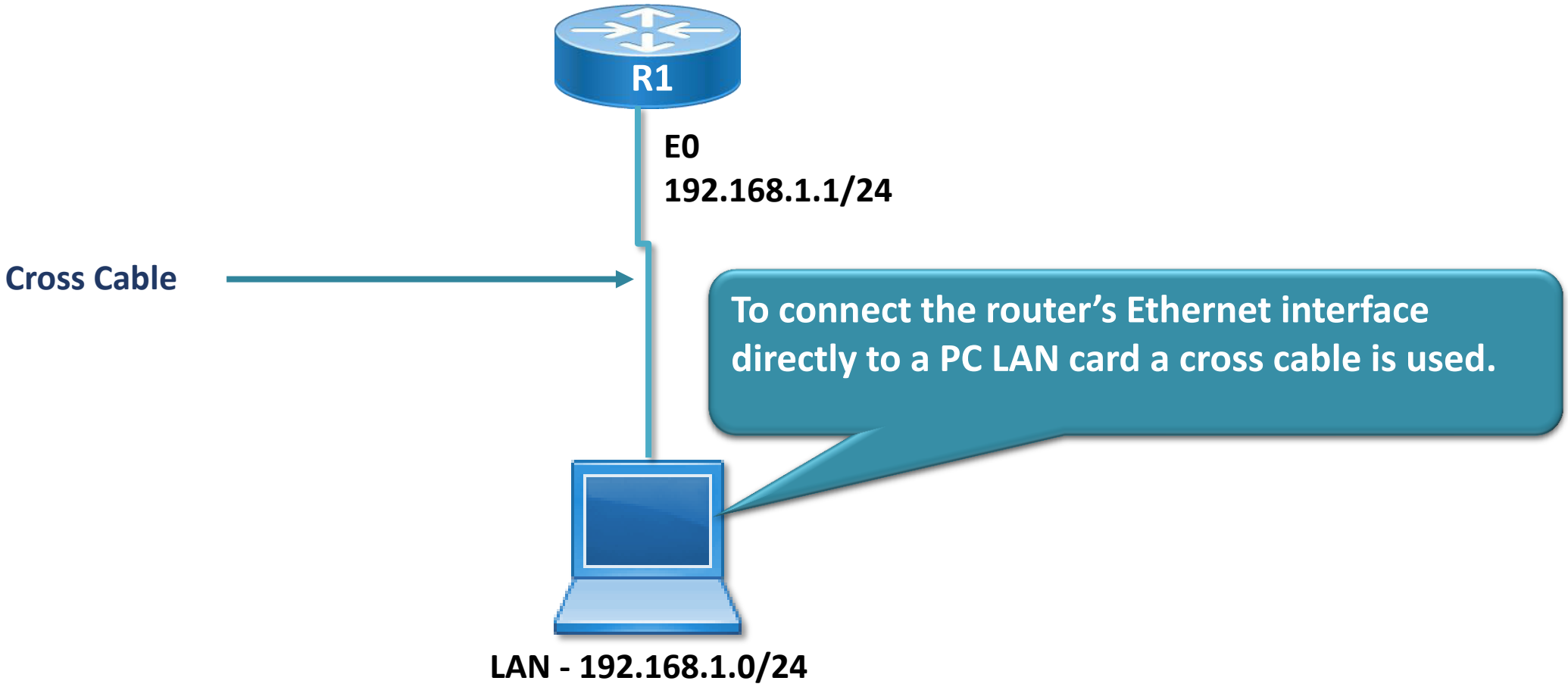
- Routers have RJ-45 ports to connect the Router to the LAN.
- The speed of the RJ-45 ports can be
  - 10 Mbps Ethernet
  - 10/100 Mbps Fast Ethernet
  - 10/100/1000 Mbps Gigabit Ethernet

LAN Connectivity

An IP address has to be assigned to this interface. It should be in the same network as that of the LAN. This IP address is the default gateway address for all LAN systems.



LAN Connectivity



Serial Port

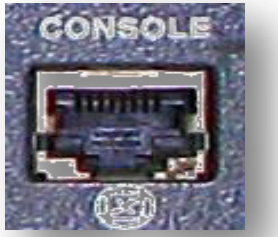
- Serial port is used for WAN Connectivity.
- Serial port are available as
  - 60 pin female connectors.
  - Smart Serial 26 pin female connectors.
- V.35 cable is used to connect the serial port of the router to the leased line modem (CSU/DSU).

HWIC

Gigabit Ethernet High-Speed WAN Interface Card (HWIC) brings Gigabit Ethernet connectivity to Cisco Integrated Services Routers routers to accelerate applications such as Metro Ethernet access, inter-VLAN routing, and high-speed connectivity to LAN switches

Console Port

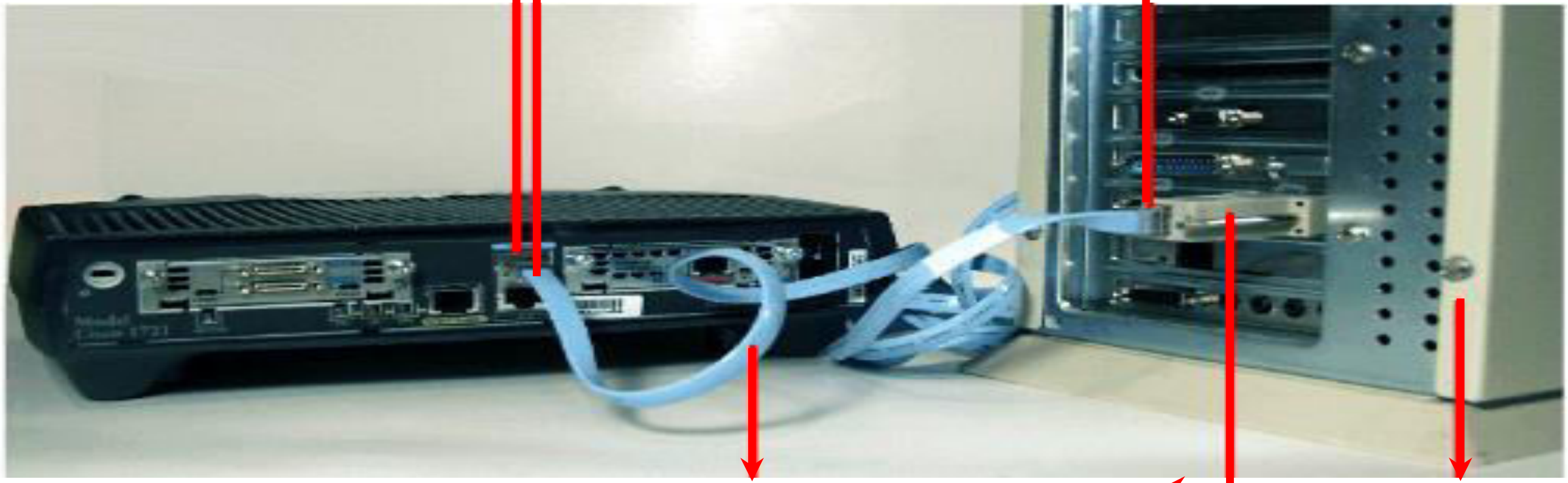
- It is a local administrative port.
- It is a RJ-45 Port.
- It is used for initial configuration and advance troubleshooting.
- Note : It is the most important and sensitive port on the Router.



DB-9 Convertor

Console cable

Console Connectivity



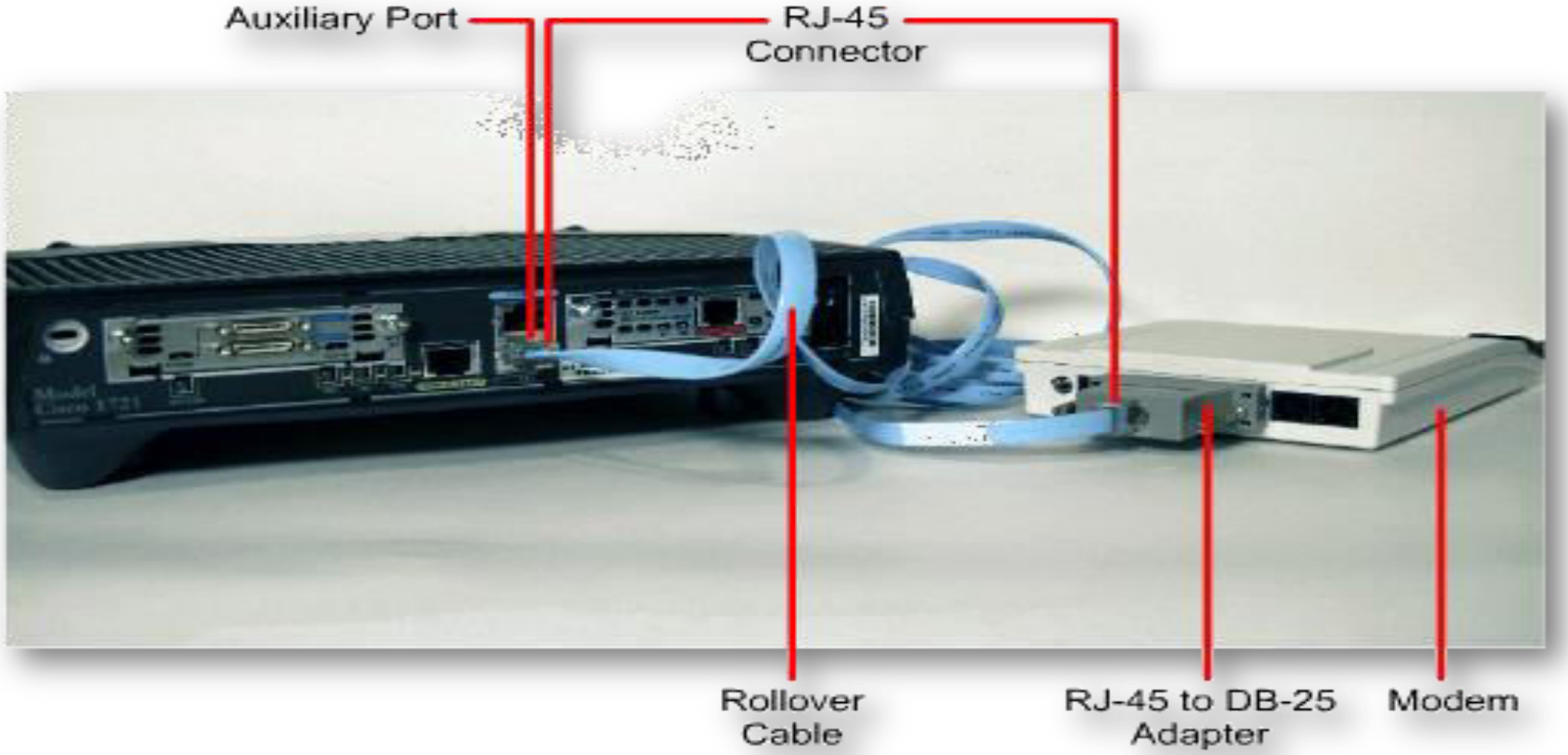
Auxiliary Port

- It is a remote administrative port.
- Used for remote administration / configuration.
- Its an RJ-45 port.
- A console / rollover cable is used to connect the auxiliary port to a dial-up modem.

Roll over Cable

One End	Other End
Orange-white	Brown
Orange	Brown-white
Green-white	Green
Blue	Blue-white
Blue-white	Blue
Green	Green-white
Brown-white	Orange
Brown	Orange-white

Auxiliary Connectivity



Interfaces of a Router

- LAN Interface
  - Attachment Unit Interface (AUI) 10 Mbps
  - RJ 45 Ethernet / FastEthernet / GigabitEthernet
- WAN Interface
  - Normal Serial Interface
  - Smart Serial Interface
- Administrative Interface
  - Console
  - Auxiliary

Internal Components of a Router

Internal Components of Router

- ROM (Read only Memory)
  - It contains a bootstrap program which searches and loads the operating system.
  - It is similar to the BIOS of a PC.
  - It also contains a ROMMON for advance troubleshooting.

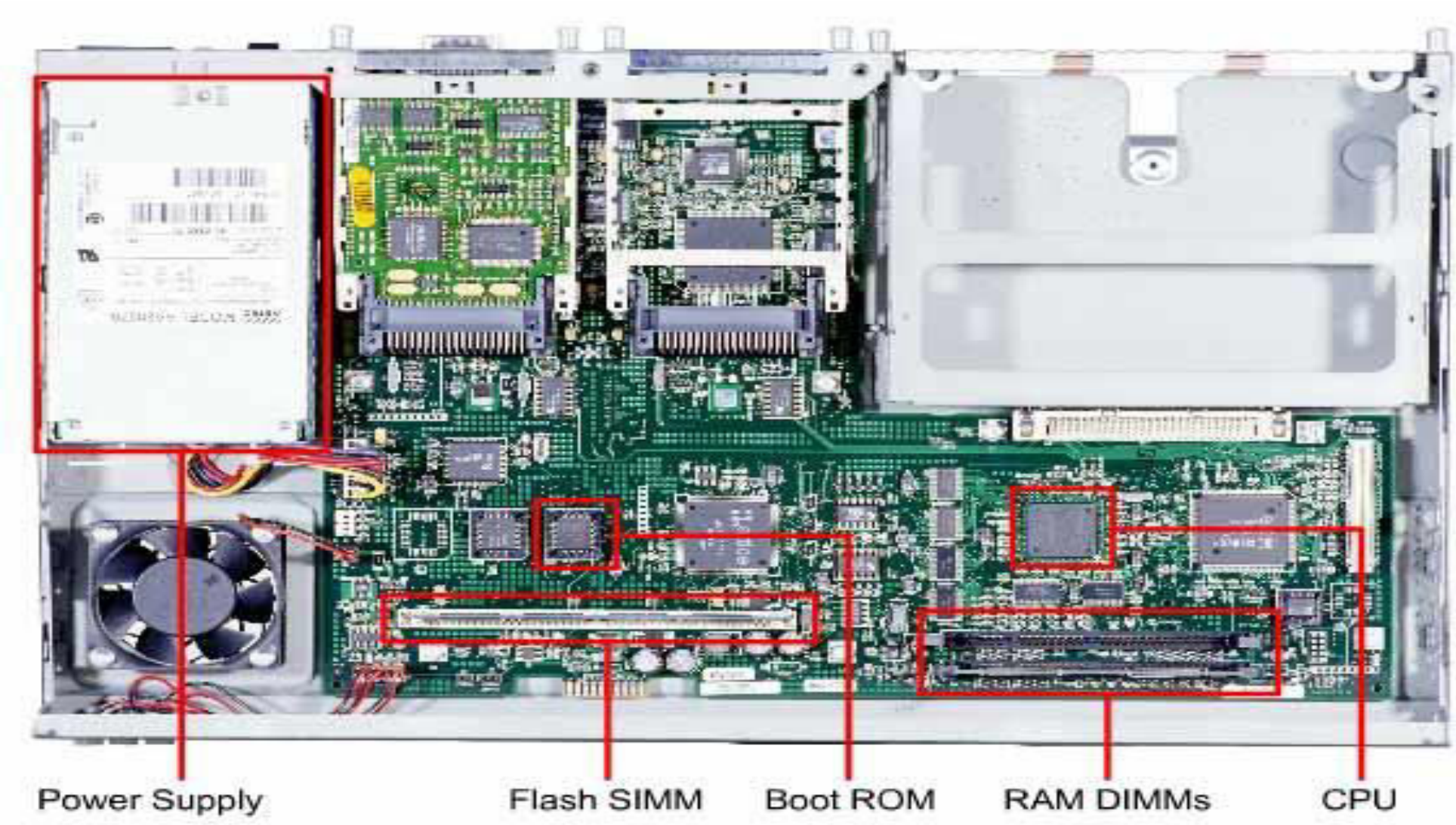
- Flash memory
  - The Internetwork Operating System (IOS) is stored here.
  - IOS is a Cisco proprietary operating system.

Internal Components of Router

- NVRAM (Non Volatile Random Access Memory)
  - NVRAM is similar to a hard disk.
  - It is also known as permanent storage.
  - The startup configuration is stored here.

- RAM (Random Access Memory)
  - It is also called as the main memory.
  - It is a temporary storage.
  - The running configuration is stored here.

Internal Components of Router

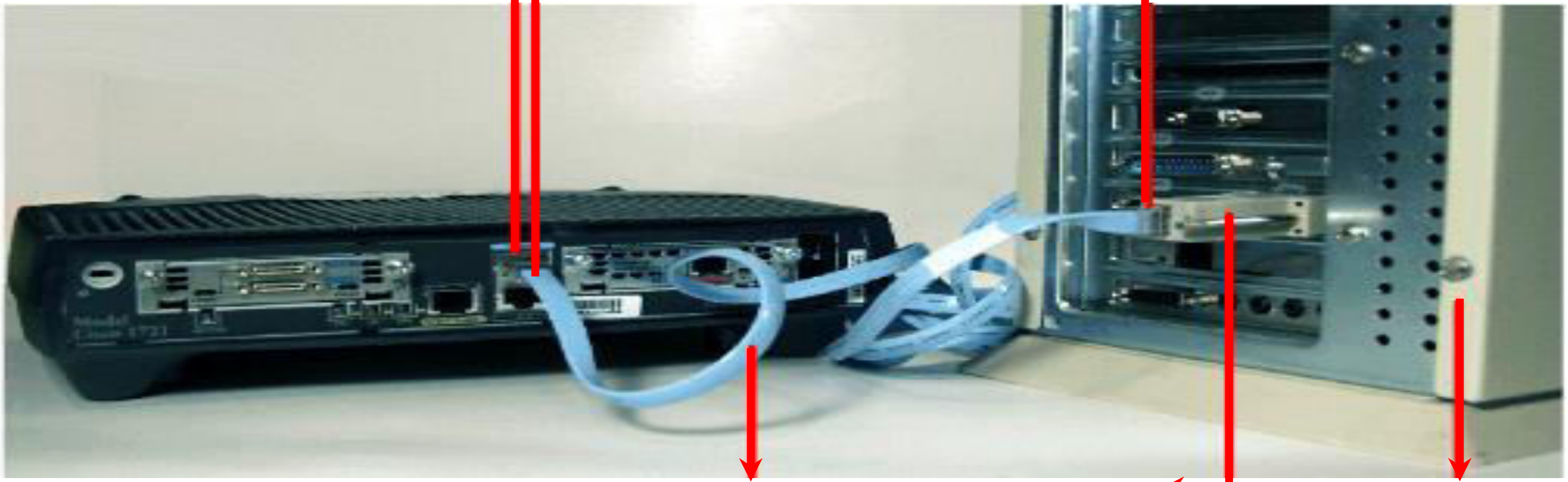


BOOT Sequence

Power On Self Test – checks the hardware	POST
ROM loads Bootstrap program and searches for the IOS	ROM
IOS from Flash is loaded	FLASH
The startup configuration is loaded from the NVRAM	NVRAM
Boot process is completed as everything is loaded into the RAM	RAM

Initial Configuration

Console Connectivity



Console Connectivity

- Cisco Routers & Switches does not have any default IP address or Configuration, hence require to use the Console port for Initial Configuration.
- Require physical connection between the Cisco Router/Switch and PC via console cable.

Emulation Software

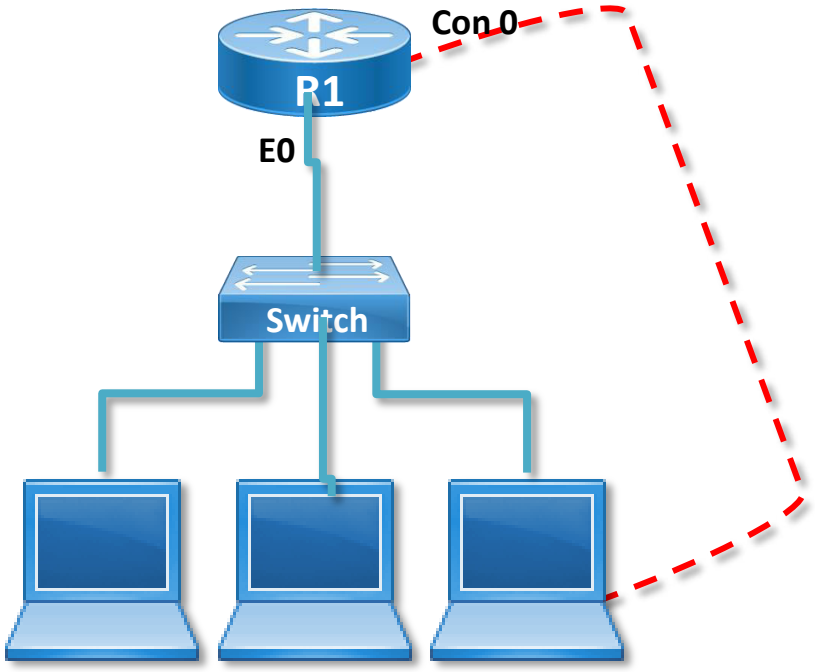
WINDOWS

- **Hyper-terminal / Putty / Teraterm**

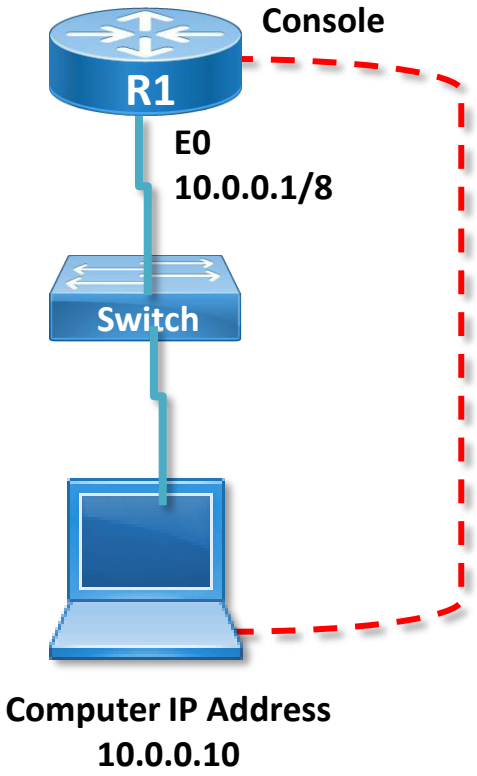
LINUX

- **Minicom -s**

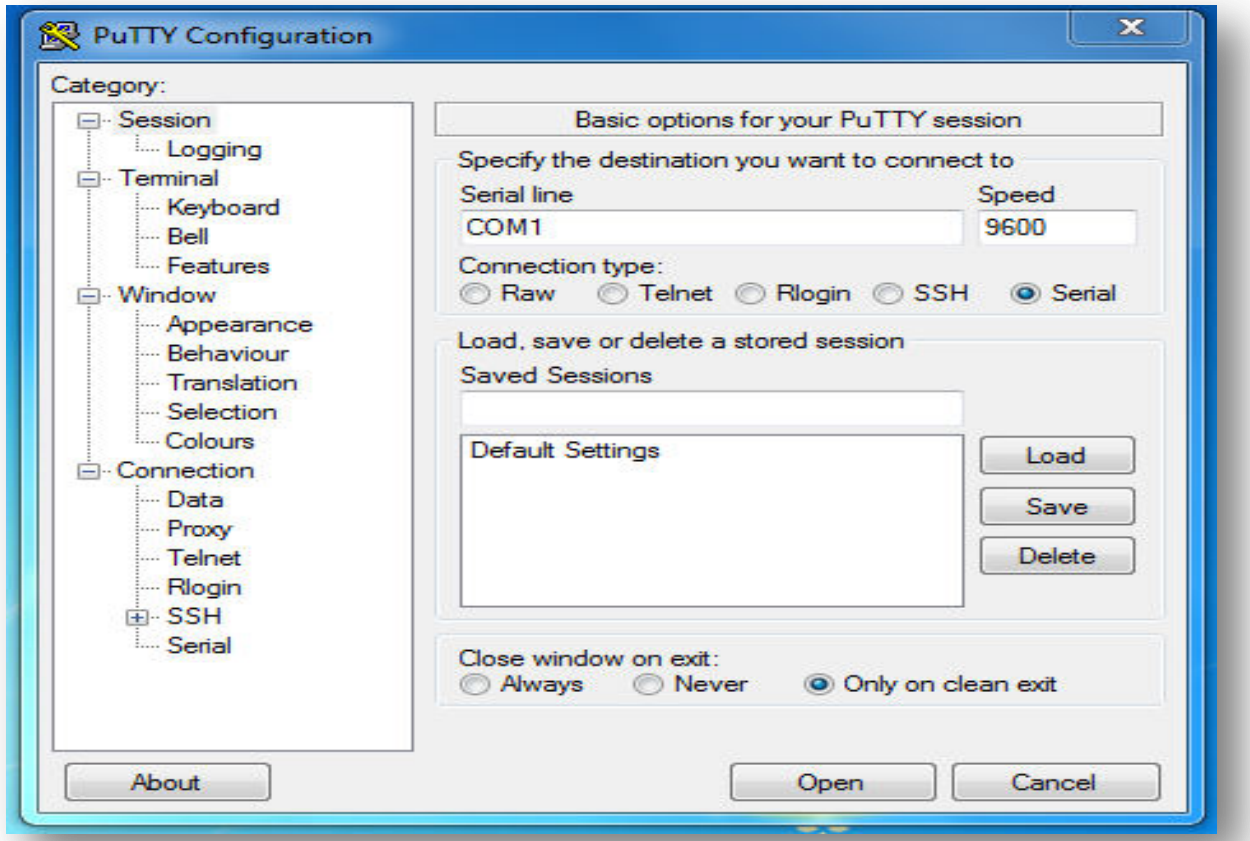
Initial Configuration



Accessing Router



- Accessing router via console from Microsoft Windows Computer
- Start a terminal emulator application, such as PUTTY.exe
- Select Serial option and set speed to 9600
- Click Open



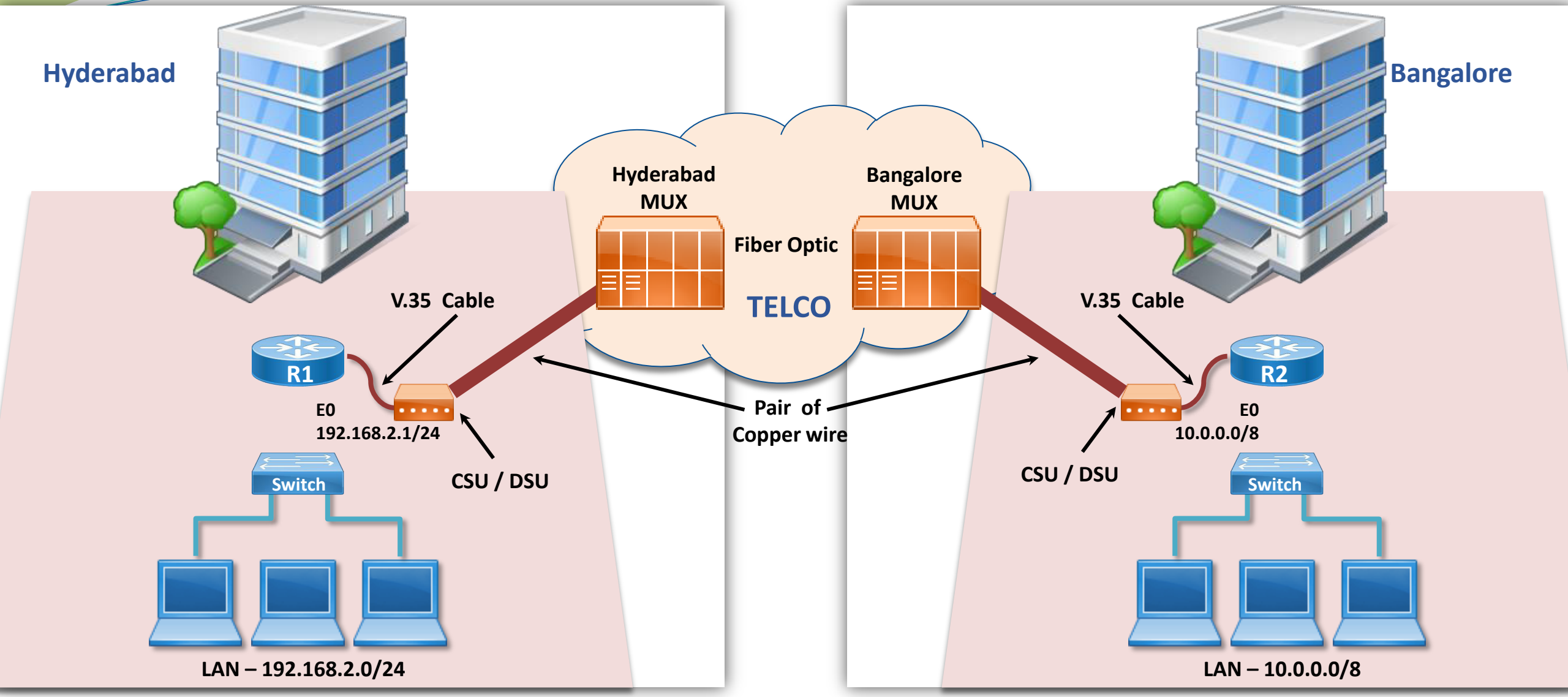
WAN Technologies

Types of WAN Technologies

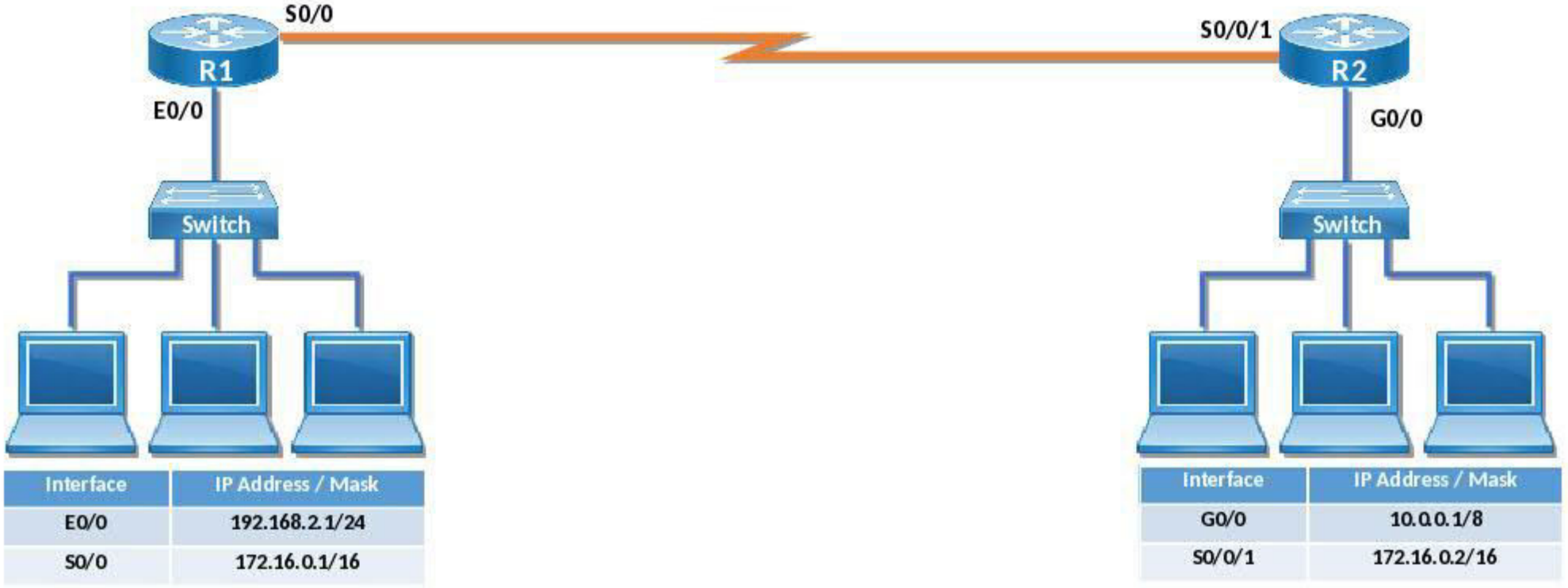
- Dedicated service
  - Leased Line
    - MLLN (Managed Leased Line Networks)
- Circuit switching
  - PSTN (Public Switched Telephone Networks)
  - ISDN (Integrated Services Digital Networks)
- Packet Switching
  - Frame-relay
  - MPLS (Multi Protocol Label Switching)
  - ATM (Asynchronous Transfer Mode)
- Broadband
  - DSL
  - Cable Internet
- VSAT
- MOBILE - 3G/4G

WAN Connectivity

Wan Connectivity



Wan Connectivity Representation



Interface	IP Address / Mask
E0/0	192.168.2.1/24
S0/0	172.16.0.1/16

Interface	IP Address / Mask
G0/0	10.0.0.1/8
S0/0/1	172.16.0.2/16

Device Classification

DCE	DTE
lData Communication Equipment lGenerate clocking (i.e. Speed) lMaster lExample of DCE:- CSU/DSU	lData Termination Equipment lAccept clocking (i.e. Speed) lSlave lExample of DTE:- Router

Serial - back to back cable

- When the distance between two Routers is short, a special V.35 Back to Back Cable is used to replace the copper wire, CSU/DSU and MUX.
- For data communication using back to back Serial cable, one end has to be a DCE and the other has to be a DTE.

ROUTER 1

ROUTER 2

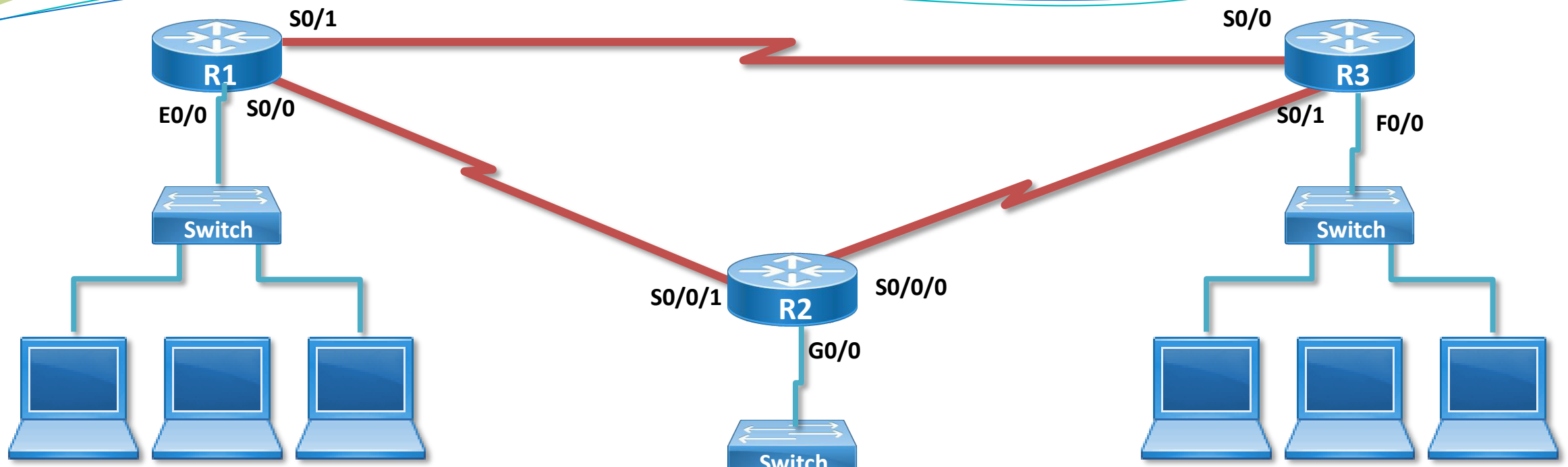
Encapsulation

- Encapsulation is the process of adding a new Header or Trailer to data.
- The header and trailer contains information which is needed for proper transportation of the data.
- There are different types of WAN Encapsulation:
  - PPP
  - HDLC
  - Frame Relay

Wan Encapsulation

PPP	HDLC
Point to Point Protocol Open Standard Protocol Supports Authentication Supports Compression	High level Data link Control Vendor proprietary Protocol No Support for Authentication No Support for Compression

Wan Interface Configuration



Interface	IP Address / Mask
E0/0	192.168.2.1/24
S0/0	172.16.0.1/16
S0/1	172.18.0.2/16

Interface	IP Address / Mask
G0/0	10.0.0.1/8

Interface	IP Address / Mask
F0/0	192.168.3.1/24
S0/0	172.18.0.1/16
S0/1	172.17.0.2/16

Serial Interface Configuration

To check DCE/DTE

- Router# Show controllers Serial < no. >

Serial Interface Configuration

- Router(config)# interface Serial <no.>
- Router(config-if)# ip address < ip > < Subnet mask >
- Router(config-if)# no shutdown
- Router(config-if)# clock rate < bandwidth >
- Router(config-if)# encapsulation < HDLC/PPP >

Verification

- Router# Show interface Serial <no. >

WAN Interface Configuration

The first step to establish the WAN connection is to configure the Serial (WAN) interface.

By default the serial interface on the Router does not have IP address, encapsulation is HDLC and the interface is in shutdown state.

Check for DTE or DCE interface, so that the clock rate can be configured on the DCE interface.

Syntax: Router# show controllers serial

Output:
KEY# show controllers serial 0/0

Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected
idb at 0x8096C8CC, driver data structure at 0x80971DD0
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
---More ---

The following are the commands to assign IP, encapsulation & enable the serial port:

Syntax:

Router(config)# interface serial <no>

Router(config-if)# ip address <ip> <mask>

Router(config-if)# encapsulation <ppp> or <hdlc>

Router(config-if)# clockrate <clockrate vlaue> ---- Clock rate has to be given in DCE routers

Router(config-if)# no shutdown

Check the serial interface connectivity

Syntax:

Router# show interface serial <no>

Output:

Router# show interface serial 0/0

Serial0/0 is up, line protocol is up

Hardware is PowerQUICC Serial
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:02, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/2/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1047 packets input, 68589 bytes, 0 no buffer
Received 584 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
1021 packets output, 69756 bytes, 0 underruns
0 output errors, 0 collisions, 13 interface resets
0 output buffer failures, 0 output buffers swapped out
28 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

From the output, the first line indicates the status of the Serial interface, there are 4 different states:

1. Serial 0/0 is up , line protocol is up

(Layer 1 & Layer 2 Connectivity and configuration is fine)

2. Serial 0/0 is administratively down, line protocol is down

('No Shutdown' has to be given on the local Router's Serial interface)

3. Serial 0/0 is up, line protocol is down

(Encapsulation mismatch or clock rate has not been given on the DCE interface or Lease Line problem)

4. Serial 0/0 is down, line protocol is down

(Problem with the v.35 cable, CSU/DSU or 'no shutdown' has not been given on the remote Router)

Note: Unless both serial & line protocol is up Interface will not work(transfer the data)

Router# show flash
System flash directory:
File Length Name/status
1 3420472 c2600-i-mz_120-9.bin
[3420536 bytes used, 4968072 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)

Router# show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), **Version 12.0(9),** RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 24-Jan-00 22:33 by bettyl
Image text-base: 0x80008088, data-base: 0x805FF878
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Router uptime is 46 minutes
System restarted by reload
System image file is "**flash:c2600-i-mz_120-9.bin"**
Cisco 2610 (MPC860) processor (revision 0x203) with **28672K/4096K** bytes of memory.
Processor board ID JAD041806FJ (1957657516)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 **Ethernet/IEEE 802.3 interface(s)**
2 **Serial(sync/async) network interface(s)**
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Using IOS context sensitive help (?)

The “?” provides context sensitive help, it provides the command syntax or the commands supported in the various IOS modes.

Example 1:

Router>?
Exec commands:

<1-99>	Session number to resume
access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
lock	Lock the terminal
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)

--More--

Example 2:

```
Router(config)# interface ?
Async                 Async interface
BVI                         Bridge-Group Virtual Interface
Dialer                Dialer interface
Ethernet              IEEE 802.3
Group-Async           Async Group interface
Loopback              Loopback interface
Multilink             Multilink-group interface
Null                        Null interface
Serial                Serial
Tunnel                Tunnel interface
```

Similarly the context sensitive help can be used in all IOS modes and commands.
Command line editing:

Tab -> for command completion
Ctrl + a -> to beginning of the command
Ctrl + e -> to end of the command
Esc + b -> back by one word
Esc + f -> forward by one word

Wrong command notification:

```
Router# comfigure terminal
^
% Invalid input detected at '^' marker.

Router#
```

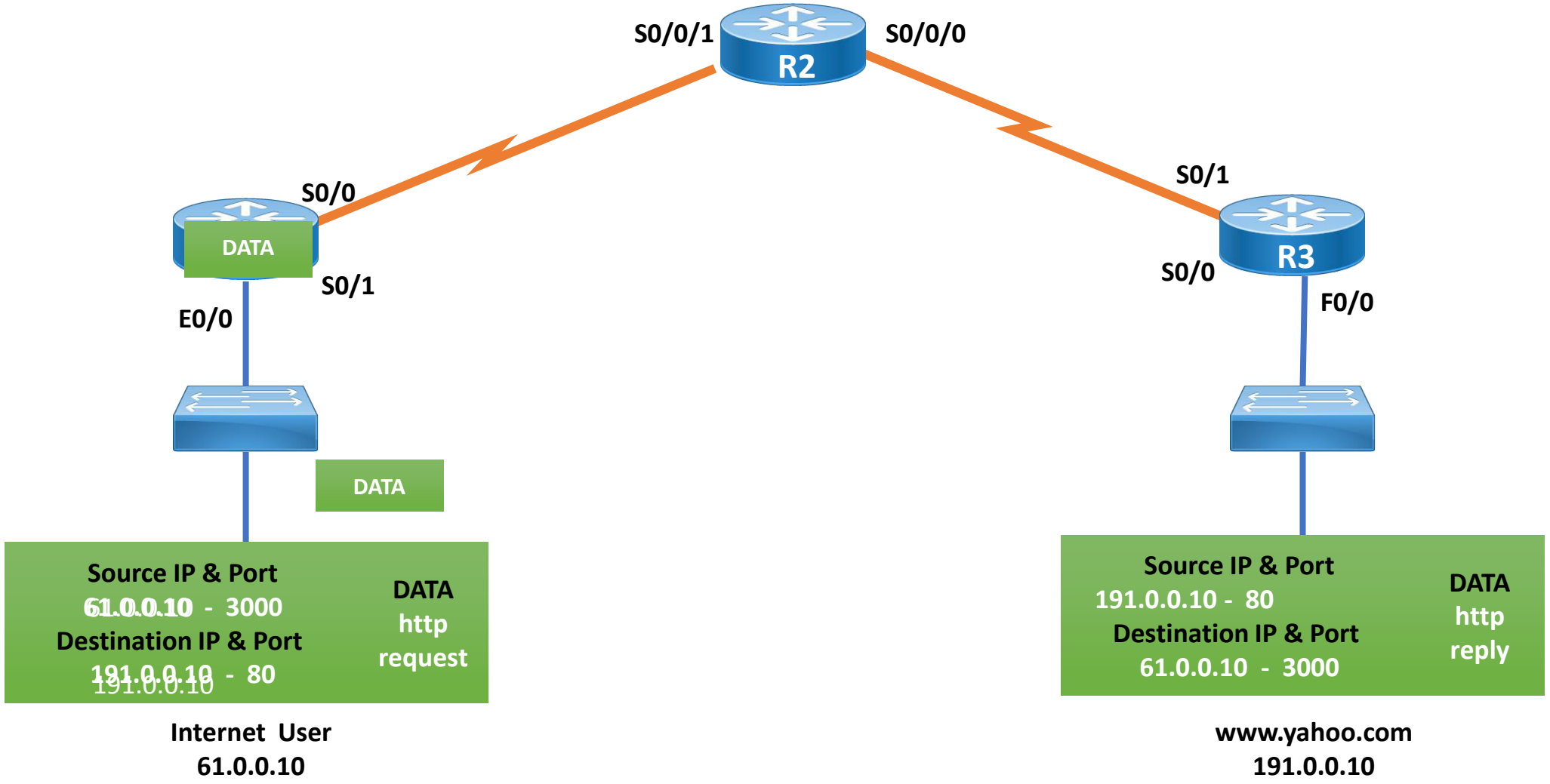
Command line errors occur primarily from typing mistakes.

IP Routing

IP Routing

- Routing is the process of moving IP packets from one network to another network.
- Routing involves two basic activities:
  - Determining best paths.
  - Forwarding packets through these paths.

IP Routing


S0/0/1
R2
S0/0/0
S0/0
DATA
S0/1
S0/1
R3
S0/0
E0/0
F0/0
DATA
Source IP & Port
61.0.0.10 - 3000
Destination IP & Port
191.0.0.10 - 80
DATA
http
request
Source IP & Port
191.0.0.10 - 80
Destination IP & Port
61.0.0.10 - 3000
DATA
http
reply
Internet User
61.0.0.10
www.yahoo.com
191.0.0.10

Routing Network Diagram

E0/0	192.168.2.1/24
S0/0	172.16.0.1/16

G0/0	10.0.0.1/8
S0/0/1	172.16.0.2/16

Conditions for Routing

- The Head office router's Ethernet interface should be in the same network as the Head office LAN and similarly on Branch office side, the router's Ethernet interface should belong to the same network as the branch office LAN.
- The serial interface between the head office and the branch office should be in same network.
- Head office LAN and Branch office LAN should be in different network.
- All interfaces of a Router should be in different network.

Types of Routing

- Static Routing
- Default Routing
- Dynamic Routing

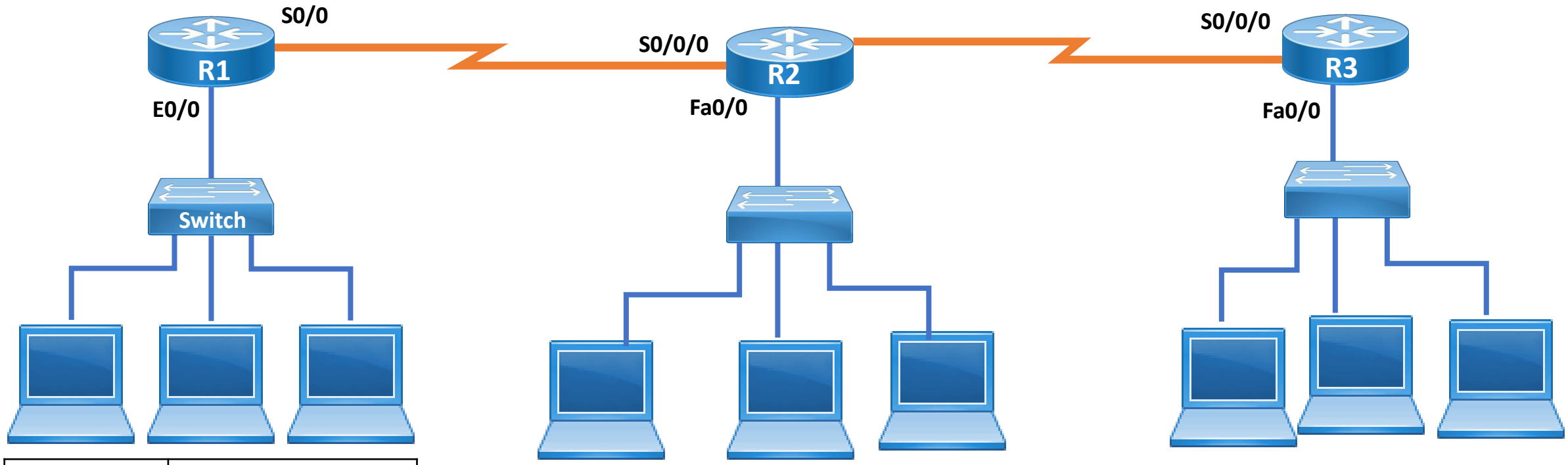
Static Routing

Static Routing

- **Static routes are configured, maintained and updated by network administrator manually.**
- **Administrator should know the destination IP network for configuration.**
- **Administrative distance for Static Route is 1.**

Administrative Distance (AD) is the “reliability” of the routing protocol. AD range is 0-255, lesser the administrative distance, higher the priority

Routing Network Diagram



Interface	IP Address / Mask
E0/0	192.168.1.1/24
S0/0	10.0.0.1/30

nterface	IP Address / Mask
fa0/0	192.168.2.1/24
S0/0/0	10.0.0.2/30
S0/0/1	11.0.0.1/30

Interface	IP Address / Mask
fa0/0	192.168.3.1/24
S0/0	11.0.0.2/30

Static Route Configuration

Static Route configuration

- Router(config)# ip route < Destination network ID > < Destination Subnet mask > < Exit Interface type > < Exit interface no. >

Or

- Router(config)# ip route < Destination network ID > < Destination Subnet mask > < Next Hop IP address >

Verification

- Router# Show ip route

Advantages and Disadvantages of Static routing

Advantages	Disadvantages
Secured	No Automatic Updates
Reliable	Need of Destination network ID for the configuration
Faster	Administrative work is more
No wastage of bandwidth	Used in Small networks

To verify the routing table:

Output:
IND# show ip route

Default gateway is not set

Host Gateway Last Use Total Uses Interface
ICMP redirect cache is empty

The above output implies that IP Routing process is disabled. To enable IP Routing use the following
command in Global Configuration Mode:

Command:

Router(config)# ip routing

To verify the routing table after routing is enabled.

Output:

IND# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR

Gateway of last resort is not set
C 172.16.0.0/16 is directly connected, Serial0/1
C 10.0.0.0/8 is directly connected, Ethernet0/1

Once routing is enabled the directly connected networks are automatically added into the routing table. “C" represents directly connected networks. The IP Network was learnt through the local Interface of the router.

To configure static routing use the following syntax:

Syntax:

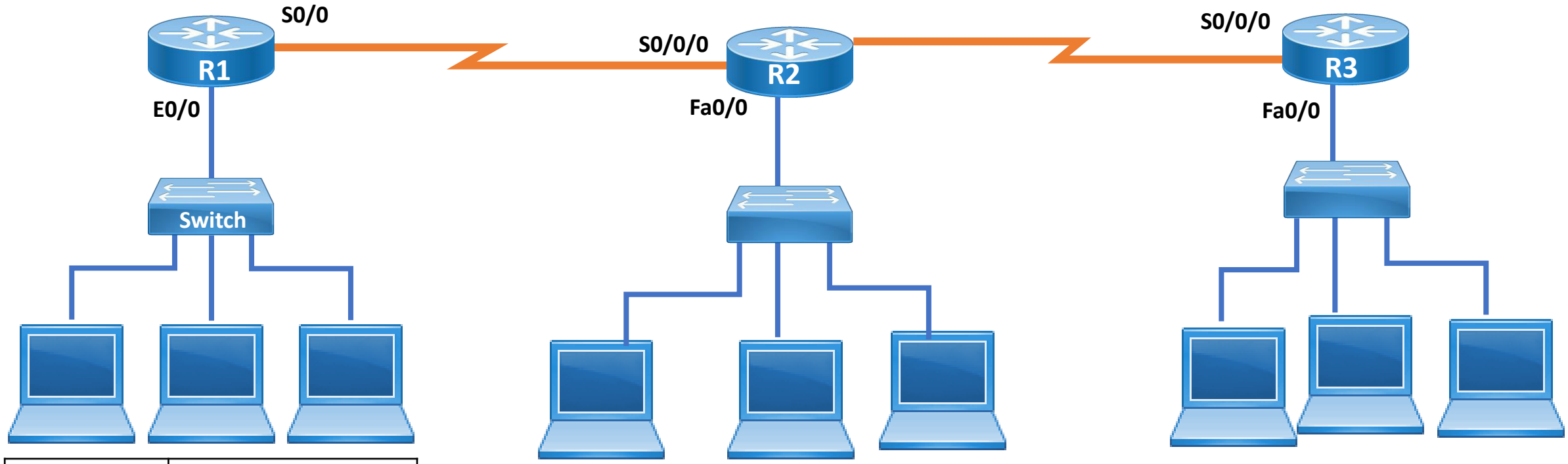
Router(config)# ip route <Destination Network ID> <Destination subnet mask>
<Next hop IP-address>

OR

Router(config)# ip route <Destination Network ID> <Destination subnet mask>
<Exit Interface type> <Interface No.>

Dest N/W ID = Network ID (of remote network)
Dest subnet mask = Subnet mask (of remote network)
Next hop ip address = IP Address of the Next Router(directly connected)
Exit interface type & Number = outgoing interface type and number

Routing Network Diagram



Interface	IP Address / Mask
E0/0	192.168.1.1/24
S0/0	10.0.0.1/30

nterface	IP Address / Mask
fa0/0	192.168.2.1/24
S0/0/0	10.0.0.2/30
S0/0/1	11.0.0.1/30

Interface	IP Address / Mask
fa0/0	192.168.3.1/24
S0/0	11.0.0.2/30

To view the routing table for verification of Static Route

Syntax:
Router# show ip route

Output:
Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B – BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR

Gateway of last resort is not set
C 192.168.2.0/24 is directly connected, fastEthernet0/0
C 11.0.0.0/8 is directly connected, Serial0/0/1
C 10.0.0.0/8 is directly connected, Serial0/0/0
S 192.168.1.0/24 [1/0] via 10.0.0.1
S 192.168.3.0/24 [1/0] via 11.0.0.2

“S” represents Static route. The IP Network was defined through the Static routing command.

Syntax:
Router# ping <IP of destination PC>

Output:
Router# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/79/91 ms

To enable the log messages on Telnet session, give the following command. (By default log messages can be
seen only on Console connectivity - Hyper-terminal/Putty)

Router# terminal monitor

To view log messages for any changes in the routing table, use the following command:
Router# debug ip routing

To view the source and destination of the packet, use the following command:
Router# debug ip packet

Dynamic Routing

Advantages of Dynamic routing

- Changes in the network topology are updated dynamically
- Only the directly connected network information is required for the configuration
- Administrative work is reduced
- Used for medium and large Networks

Types of Dynamic Routing Protocols

- Distance vector
  - RIP (Routing Information Protocol)
  - IGRP (Interior gateway routing protocol)

- Advanced distance vector
  - EIGRP(Enhanced Interior gateway routing protocol)

- Link-state
  - OSPF (open shortest path first)
  - IS-IS (intermediate system to intermediate system)

RIP

Routing Information Protocol

- Distance vector protocol
- It is open standard protocol
- Uses Bellmen-ford Algorithm
- Classfull routing protocol
- Updates are periodically broadcasted using IP address 255.255.255.255
- Complete routing table sent as an update
- Each Update can contain maximum of 25 routes
- Administrative Distance is 120
- Metric is Hop count
- Maximum hop count supported is 15
- Load balancing on 4 equal paths by default (maximum 16 equal paths)
- Also known as “Routing by Rumor”

RIP Timers

- **Update Timer : 30 sec**
  - **Time between two consecutive updates**
- **Invalid Timer : 180 sec**
  - **Time a router waits to hear an update from the neighbor**
  - **The route is marked as unreachable if there is no update for this time period**
- **Flush Timer : 240 sec**
  - **Time after which the invalid route is removed from the routing table**

Disadvantages of RIP

- More Bandwidth is utilized for sending the updates.
- Does not consider the bandwidth in metric calculations, uses only hop count
- Slow convergence
- Formation of routing loops

Routing loops

- Routing loops are formed due to the default behavior of RIP
- Complete routing tables are exchanged
- Slow convergence
- No verification of updates received

Routing loop avoidance

Built in Mechanisms to avoid switching loops

- Split Horizon

  A route learnt through an interface is never advertised back out of that same interface

- Route poisoning

  The route is marked as 16 hops

  It is a mechanism to inform regarding unreachable route to neighbor

- Poison reverse

  Violating split horizon rule, sending the update through an interface from where it is being received, only in a case when network is unreachable (16hops)

- Hold down timer : 180 sec

  The router does not accept any update for the invalid route for this time period

- Flash update (Triggered update)

  Change in the network typologies causes the router to send the update immediately without waiting for the update timer to get over

Comparison between RIPv1 and RIPv2

RIP v1	RIP v2
lClassfull routing protocol lDoes not advertise subnet mask information in routing update lIt works with broadcasting (255.255.255.255) •It does not support Authentication	lClassless routing protocol l Advertises the subnet mask information in routing update lIt works with multicasting (224.0.0.9) •It supports Authentication

RIP configuration

RIP configuration

```
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network < Network ID >
```

Verification

```
Router# Show ip route
```

To check the logs

```
Router# debug ip rip
Router# terminal monitor
```

EIGRP

Enhanced Interior Gateway Routing Protocol

- Advance Distance vector routing protocol
- It is open standard protocol, was Cisco proprietary
- Uses DUAL (Diffusion Update Algorithm)
- Classless routing protocol
- Updates are sent through Multicast IP address (224.0.0.10)
- Incremental Updates and Triggered updates
- Administrative distance is 90
- Metric : Composite Metric
  - Bandwidth, delay, load, reliability and MTU
  - Bandwidth and delay is used by default

EIGRP

- Maximum hop count supported is 255 (Default is 100)
- Hello packets are sent every 5 seconds
- Supports multiple Routed Protocols - IP, IPX and Apple Talk protocols
- Support equal and unequal cost load balancing (default 4 paths and maximum 16 equal or unequal path)
- Fast Convergence to topology changes

EIGRP Tables

- Neighbor Table
  - Contains information about directly connected neighbors.

- Topology Table
  - Contains entries for all destinations, along with the feasible distance and the advertised distance.
  - Contains the successors.
  - Contains feasible successor if any.

- Routing Table
  - Entries with the best path for each destination from the Topology table are moved into the Routing Table

EIGRP Terminology

- **Feasible Distance FD :**
  - **Feasible distance (FD) is the metric of the best route to a destination, including the local link distance.**
  - **Feasible distance = advertised distance + local link distance (of the best path)**

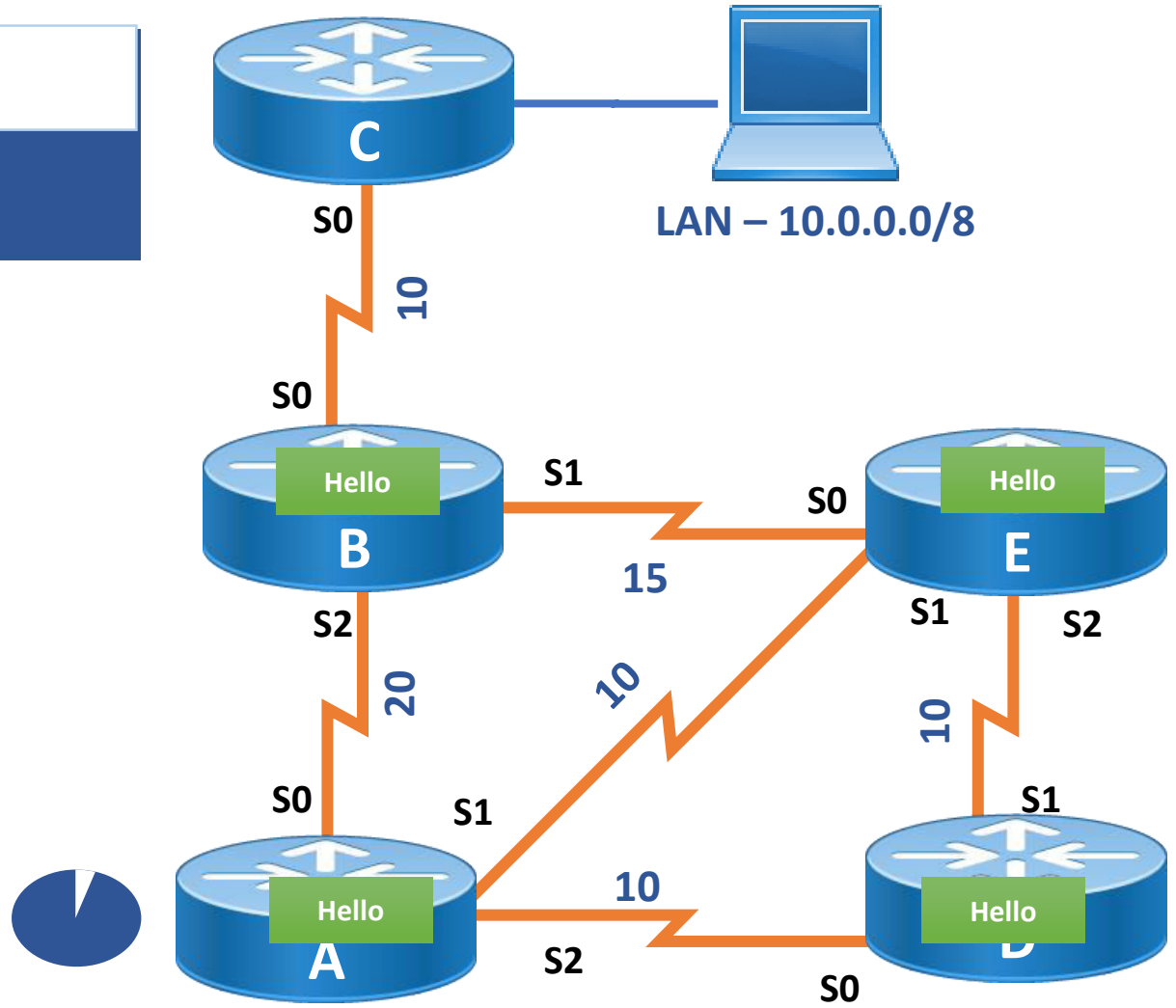
- **Advertised Distance AD:**
  - **The distance of a route as advertised by the neighbor. It does not include the local link distance.**

- **Successor :**
  - **The neighbor with best distance to the destination.**

- **Feasible Successor :**
  - **The neighbor with second best distance to the destination, which meets this criteria: advertised distance should be less than the feasible distance (AD <FD)**

EIGRP - Neighbor Table

NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1



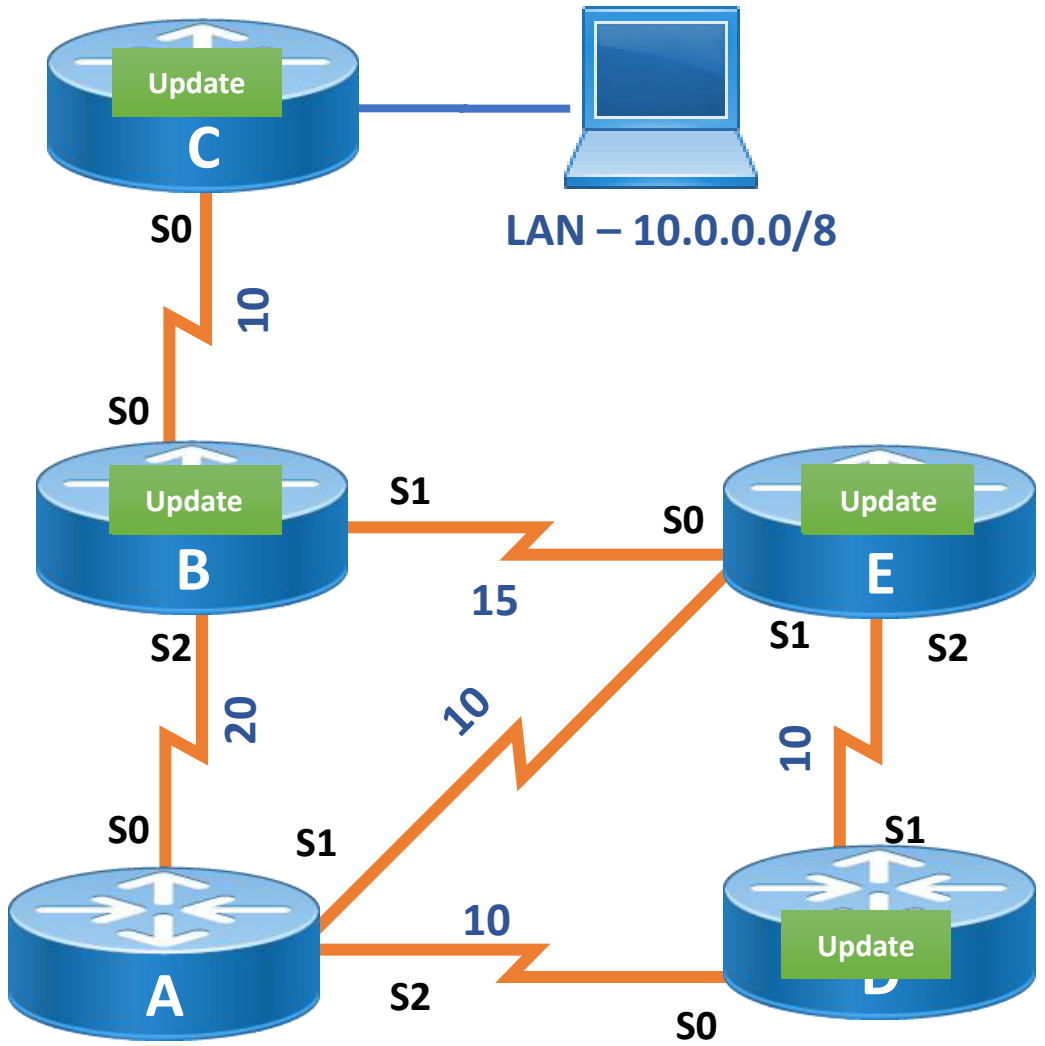
EIGRP - Topology Table

NEIGHBOR TABLE (Router A)

Neighbor	Interface
B	S0
D	S2
E	S1

TOPOLOGY TABLE (Router A)

Network	Neighbor	TD		AD	FD
10.0.0.0/8	via B	30	30	S 10	
	via E	35		FS 25	
	via D	45		35	



EIGRP - Routing Table

NEIGHBOR TABLE (Router A)

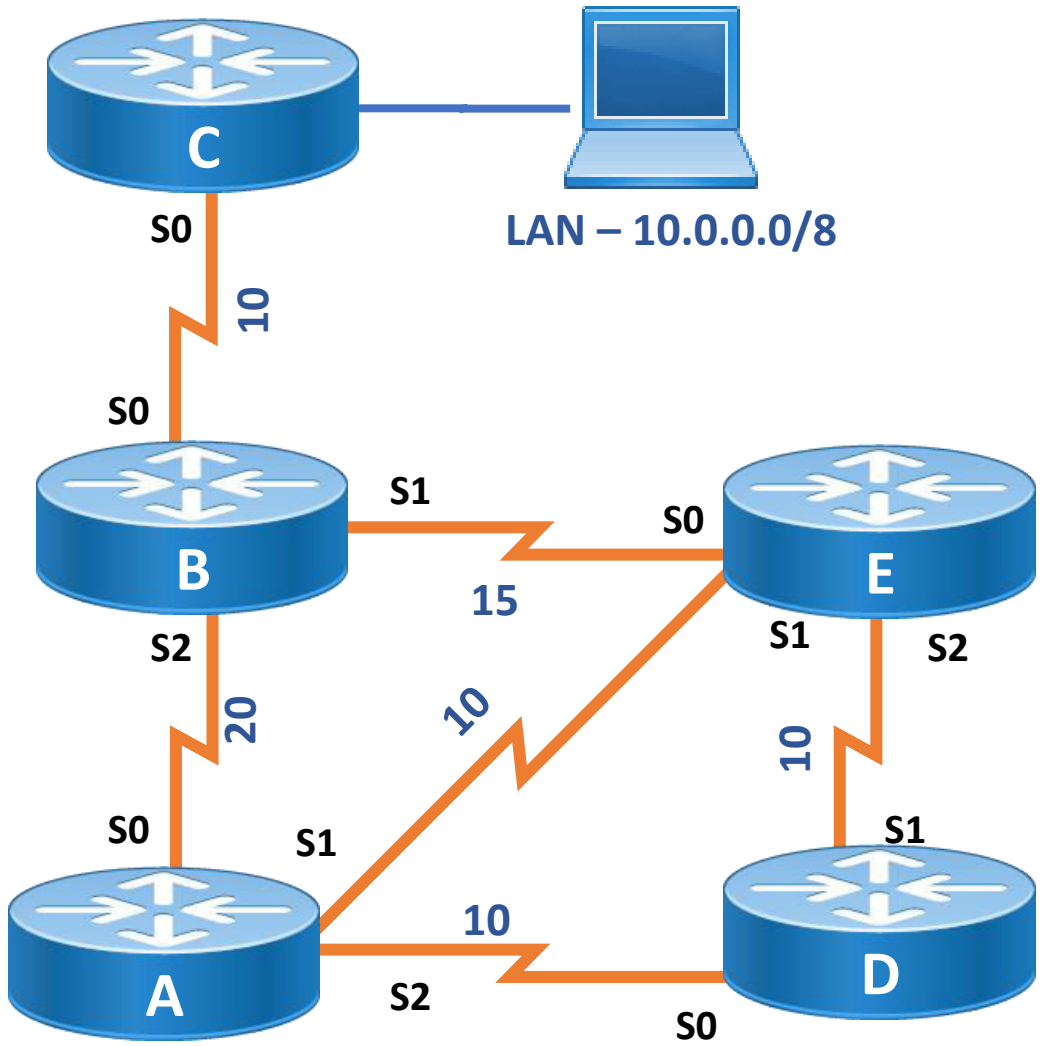
Neighbor	Interface
B	S0
D	S2
E	S1

TOPOLOGY TABLE (Router A)

Network	Neighbor	TD		AD	FD
10.0.0.0/8	via B	30	30 S	10	
	via E	35	FS	25	
	via D	45		35	

ROUTING TABLE (Router A)

D 10.0.0.0/8 [90/30] via B, 01:36, Serial0



Autonomous System

- An autonomous system is a collection of networks or routers under a common administrative policy
- Autonomous systems are identified using numbers
- Autonomous system number ranges from 0 - 65535
  - Public : 1 – 64511
  - Private : 64512 – 65535

Eigrp configuration and Verification Syntax

EIGRP configuration

- Router(config)# ip routing
- Router(config)# router eigrp <As no. >
- Router(config-router)# network < Network ID >

Verification

To check Routing Table

- Router # show ip route

To check Neighbor Table

- Router # show ip eigrp neighbor

To check Topology Table

- Router # show ip eigrp topology

To configure EIGRP routing protocol

Use the following command to enable EIGRP and advertise directly connected networks.

Syntax:
Router(config)# router eigrp <autonomous system no>
(The Autonomous system number is between 1 – 65535)

Router(config-router)# network <network ID>

To verify, the following commands can be give on Routers

Show commands:

Jammu#show ip route
Jammu#show ip protocols

Jammu#show ip eigrp neighbor
Jammu#show ip eigrp topology
Jammu#show ip eigrp neighbor detail

Neighbor Table: As its name suggests this table consists of information of neighbor routers whose information is collected using Hellos. It consists of all directed neighbors. (Neighbors should be in same AS). The show ip eigrp neighbor command lists the information about neighbors.

```
Router_B#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address                 Interface       Hold Uptime    SRTT   RTO  Q  Seq
                                            (sec)          (ms)       Cnt Num
0   20.0.0.1                Se0/0           12   01:58:22  40     1000 0   1

Router_B#
```

H: Handle: Order in which neighbor adjacency is formed. The first router will have ‘0’ the following one will have ‘1’ and so on.
Address: IP address of the neighbor
Interface: Interface of the neighbor connected
Hold Time: Timer how long to hold a neighbor if a hello is not received. By default it is 15 seconds.
Uptime: Since when the neighbor is up
SRTT: Smooth Round Trip Time: Time taken for a packet to reach the neighbor and **get an acknowledgment back. This time is in milliseconds.**
RTO: Retransmission Timeout: Time taken to wait before router retransmits a packet to the neighbor
Q Cnt: Queue Count: Number of packets that are waiting to be transmitted (Update, Reply, Query). Any number greater than 0, signifies some congestion in the network.
Seq Number: Sequence Number: It is the sequence number of the last packet received from neighbor.

Topology Table: This table contain a lot of information i.e. All the paths to destination learnt by the EIGRP neighbors. The command “show ip eigrp topology” shows the topology table.

```
Router_B#show ip eigrp topology
IP-EIGRP Topology Table for AS 10

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 20.0.0.0/8, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 10.0.0.0/8, 1 successors, FD is 2172416
         via 20.0.0.1 (2172416/28160), Serial0/0
Router_B#
```

FD: Feasible Distance: metric to a destination

2172416 / 28160: In the output 2172416 is the feasible distance and 28160 is the advertised distance.

Advertised distance is the distance from your neighbor to destination.

Feasible distance is the total distance from you till the destination.

P: Passive: means the router is not looking for the route actively, thus it means it is in good situation.

The status of ‘Active’ means some instability in network.

Routing Table: This is the table that has the best possible route to a destination. The command "show ip route" shows all routes. To specifically see the EIGRP route in routing table "show ip route eigrp" command is used.

```
Router B#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    10.0.0.0/8 [90/2172416] via 20.0.0.1, 00:38:20, Serial0/0
C    20.0.0.0/8 is directly connected, Serial0/0
Router B#
```

```
Router B#show ip route eigrp
D    10.0.0.0/8 [90/2172416] via 20.0.0.1, 00:38:04, Serial0/0
```

D: Shows this is an EIGRP learnt route

90/ 2172416: Here 90, is the Administrative Distance of EIGRP. 2172416 is the metric

.

Via 20.0.0.1: the neighbor that advertised the route

00:38:04: Time since the route was learnt

Serial 0/0: The outbound interface going towards the destination.

Routing Protocol Classification

IGP

- Interior Gateway Protocol
- Routing protocols used within an Autonomous system
- Ex: RIP, IGRP, EIGRP, OSPF, IS-IS

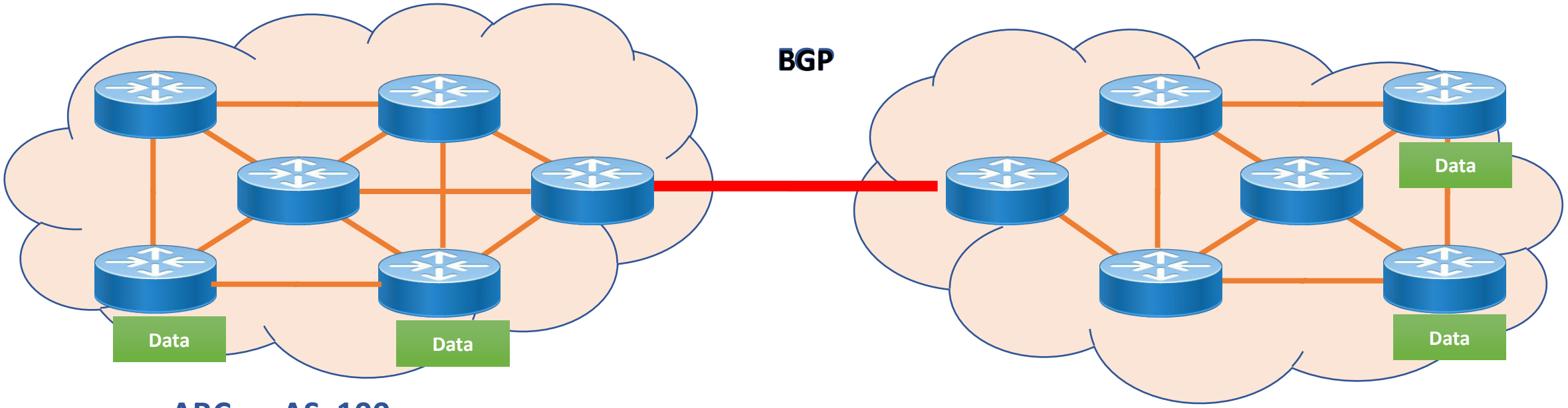
EGP

- Exterior Gateway Protocol
- Routing protocol used between different Autonomous systems
- Ex: Border Gateway Protocol is extensively used as EGP

IGP and EGP

RIP, OSPF, IGRP, EIGRP

RIP, OSPF, IGRP, EIGRP



ABC - AS 100

XYZ - AS 200

- IGPs operate within an autonomous system
- EGPs connect different autonomous systems

Summarization

- Route summarization takes a set of contiguous networks or subnets and groups them together using a shorter subnet mask.
- The advantages of summarization are that it reduces the number of entries in the route table.

EIGRP summarization

- EIGRP supports summarization at any location in the internetwork.
- By default EIGRP has auto-summarization enabled.
- Summarize the routes that are advertised through classfull network boundaries.

To disable auto-summarization

```
Router(config)#  router eigrp <As. no.>
Router(config-router)#  no auto-summary
```

EIGRP Passive interface

- The interface can be configured as passive , for stopping the hellos and Updates.
- The passive interface cannot send any hellos over the interface , but it can receive hellos.

To configure passive interface

```
Router(config)#  router eigrp <As. no.>
Router(config-router)#  passive-interface <interface type> <no.>
```

OSPF

Open Shortest Path First

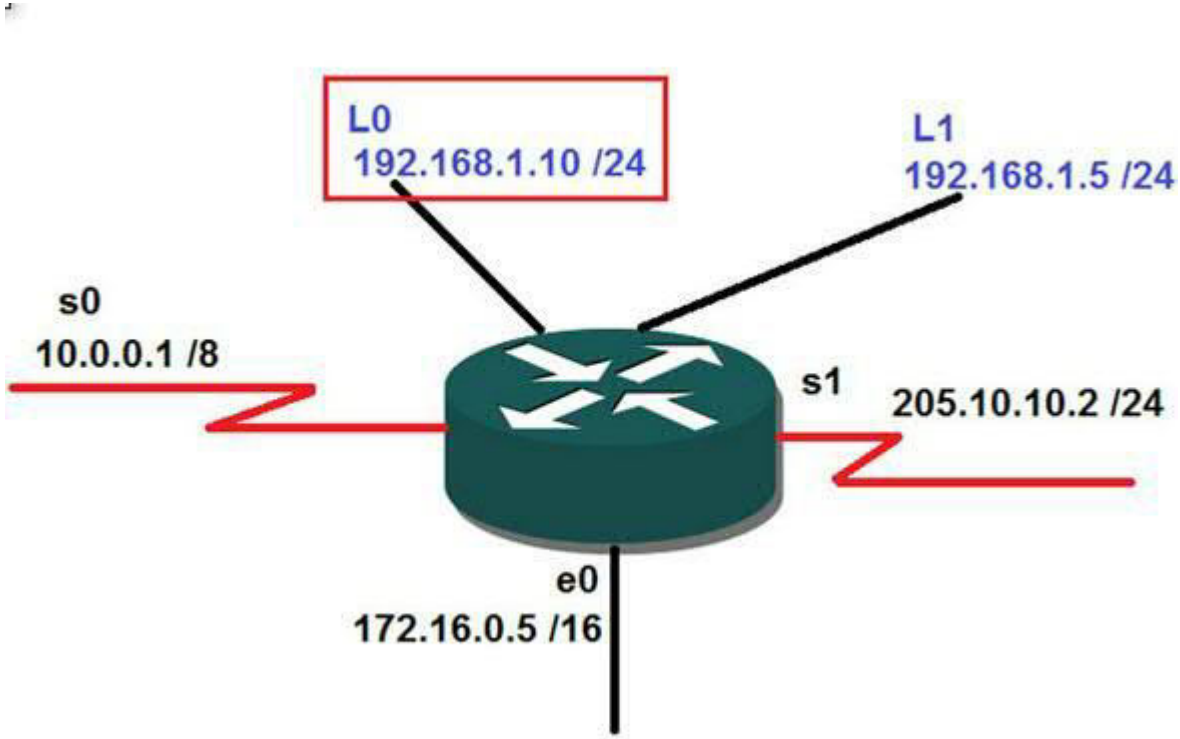
- Link State Protocol
- Open standard
- Classless routing protocol
- Uses Dijkstra (Shortest Path First (SPF)) Algorithm
- Updates are sent through Multicast IP address 224.0.0.5 and 224.0.0.6
- Supports Triggered Updates and incremental updates
- Administrative distance is 110
- Metric = Cost = 10^8/Bandwidth in bps (CISCO)

OSPF (contd..)

- Hello packets are sent every 10 seconds, Dead interval 40 sec
- OSPF sends updates (LSAs) when there is a change to one of its links
- LSAs are additionally refreshed every 30 minutes.
- Unlimited Hop Count
- Designed to scale and support large / Enterprise networks
- Hierarchical network design using Areas
- One area has to be designated as Area 0
- Area 0 is called the Backbone Area

Router ID

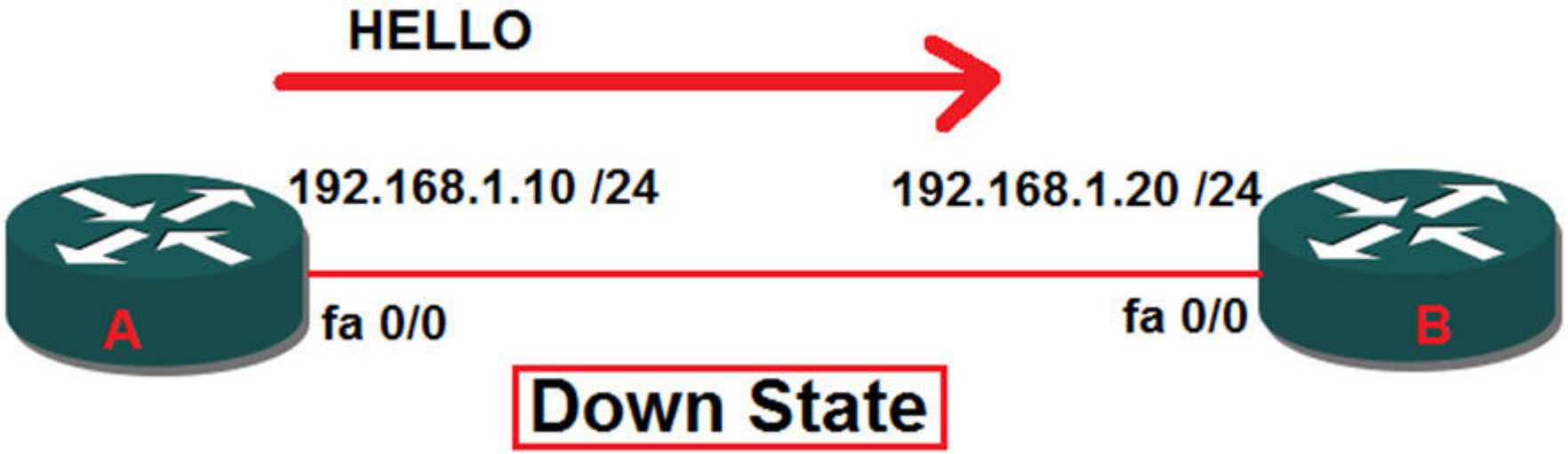
- Router ID is used to identify the Router.
- The highest IP assigned to an active physical interface is the Router ID.
- If logical interface is configured then the highest IP assigned to a logical interface (loopback) is the Router ID.



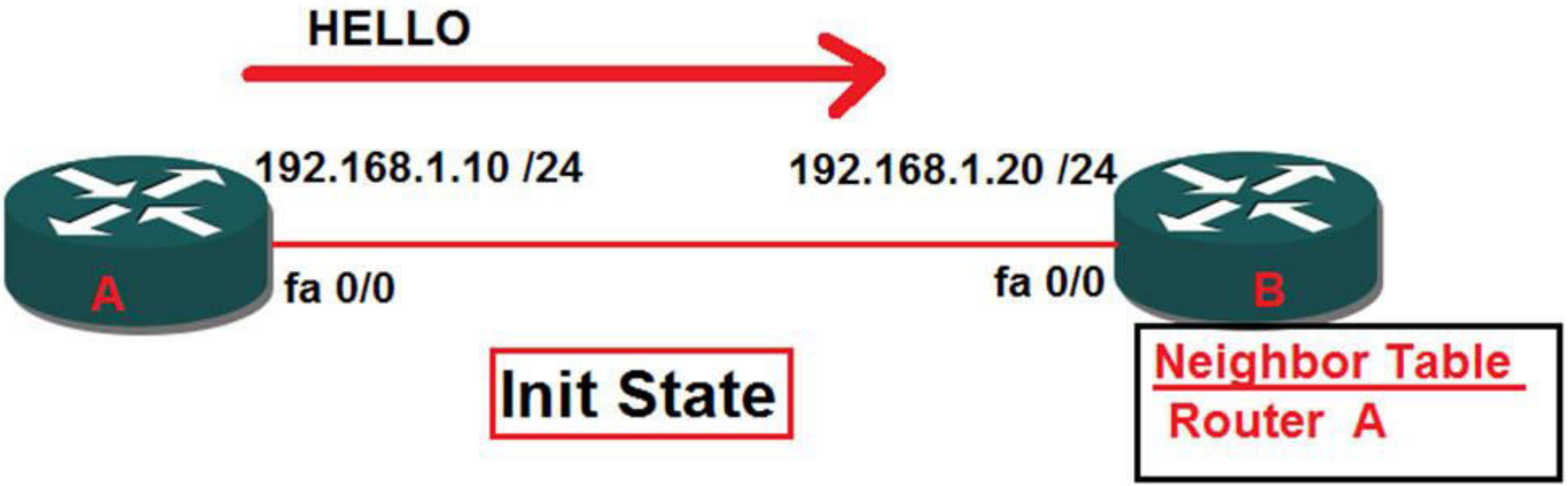
OSPF Neighbor States

The neighbor formation process in OSPF occurs in 7 stages:

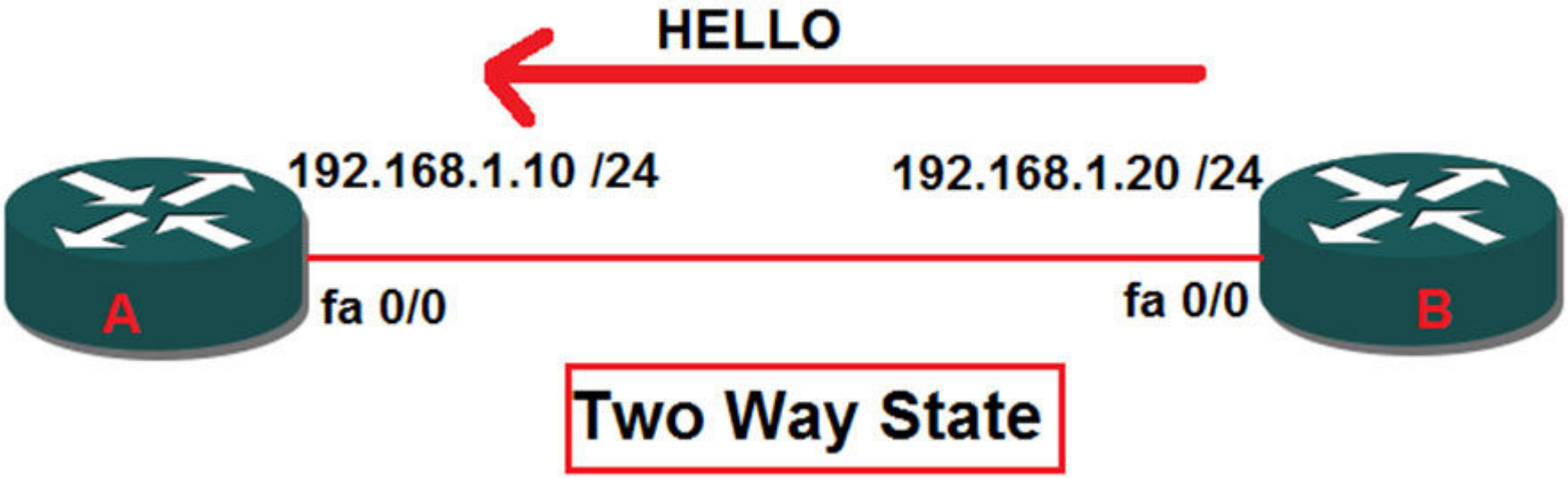
1. DOWN State: After OSPF is configured, Router A will send HELLO Packets and as Router A does not know about any other routers it is in DOWN State



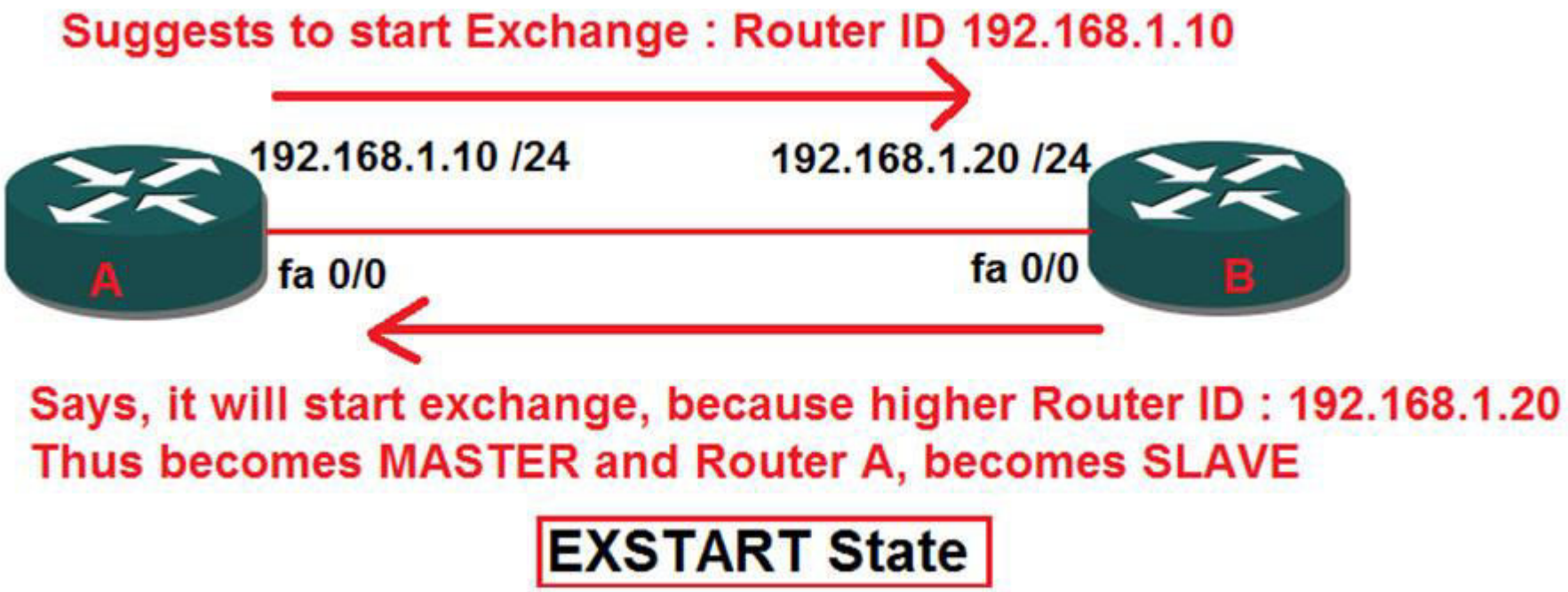
2. INIT State: Router B receives the HELLO and adds it to its neighbor table and is not in INIT state.



3. 2-WAY State: Router B, will send a unicast as response to Router A. As Router A receives the packet, it sees its name in the HELLO packet as a neighbor and here we are in 2-WAY State.



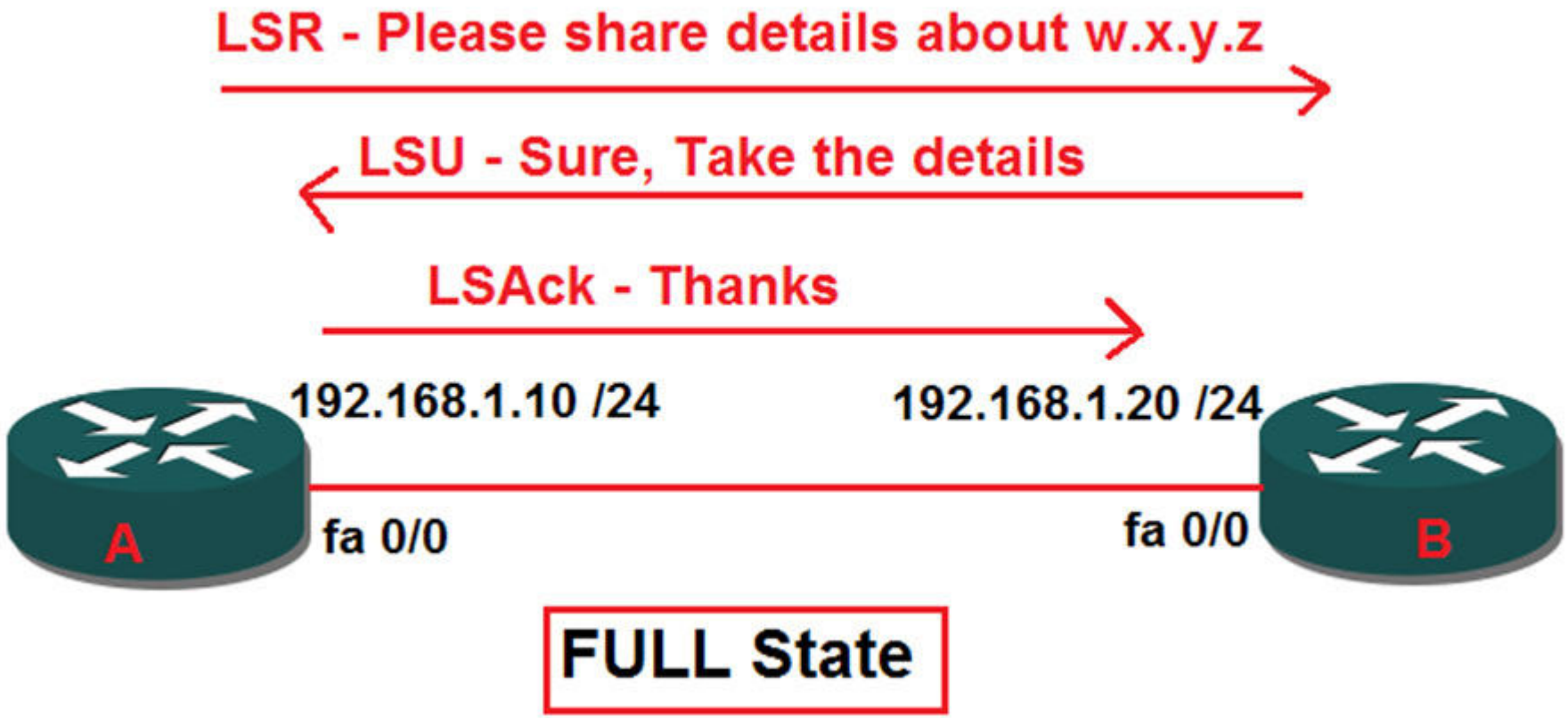
4. Exstart State: In case of multi-access network, a DR (Designated Router) and BDR (Backup Designated Router) need to be elected by OSPF. In Exstart State DBs are Synced and Master and Slave role is decided. Higher Router ID becomes Master and Starts Exchange.



5. Exchange State: In this the LSDBs are synchronized and exchanged. The Master sends it first and both populate the networks that they don’t know.

6. Loading State: Here LSAcks are sent for acknowledging the DBDs. While comparing if a neighbor has newer information it is requested using LSR. While LSR is being sent the device is in LOADING State. The other routers send the info in LSU.

7. Full State: When the requested info is provided using LSU and when the LSAck is received to Finish. We are considered to be in FULL State.



OSPF Terminology

- Neighbor
  - Routers that share a common link become neighbors.
  - Neighbors are discovered by Hello Packets.
  - To become neighbors the following should match
    - Area ID
    - Network ID and Subnet Mask
    - Hello and Dead Intervals
    - Authentication

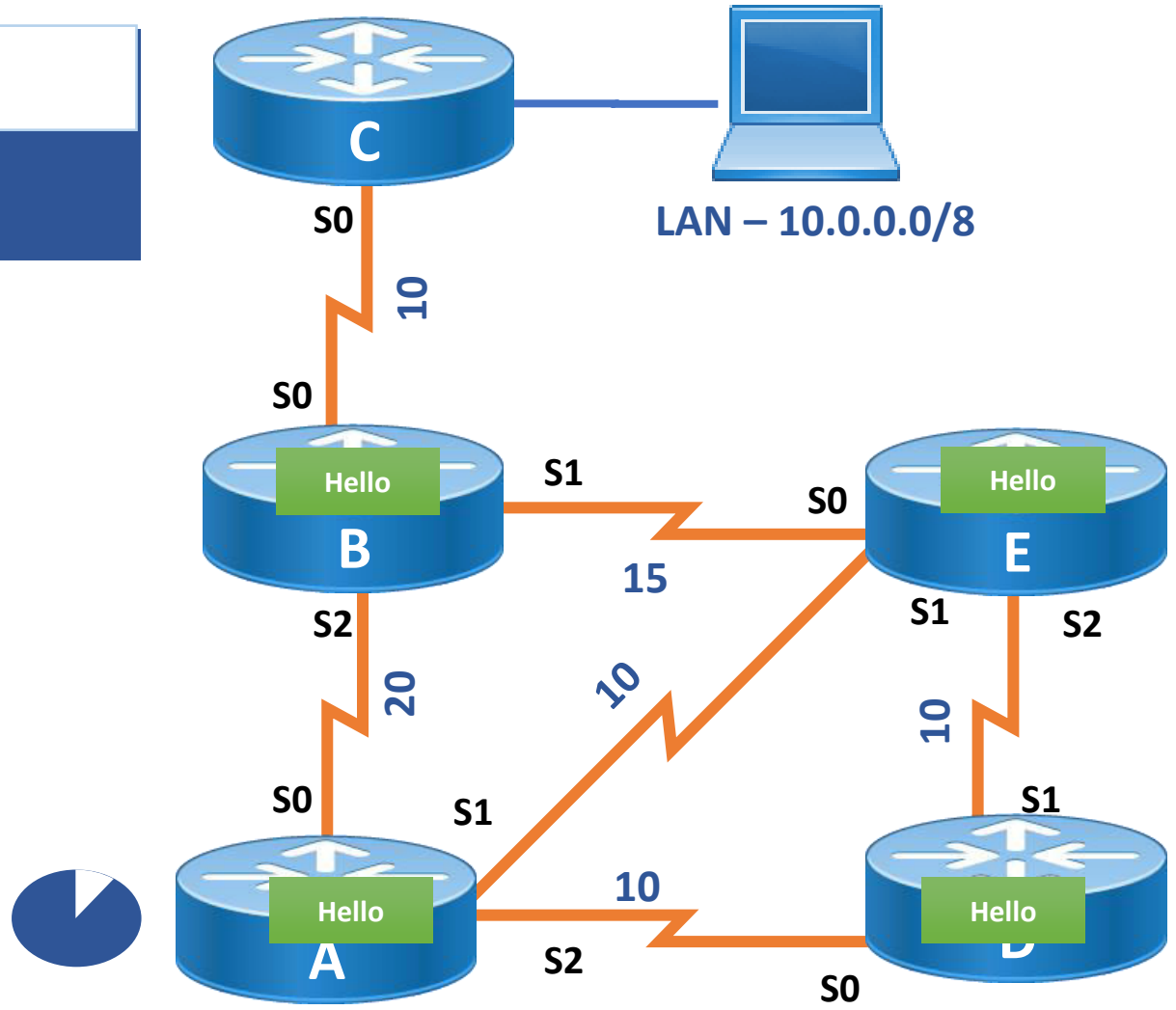
- Adjacencies
  - Adjacencies are formed once neighbor relation is established.
  - In Adjacencies the database details are exchanged.

OSPF Tables

- It maintains three tables :
- Neighbor Table
  - Neighbor table contains information about the directly connected OSPF neighbors forming adjacency.
- Database Table
  - Database table contains information about the entire view of the topology with respect to each router.
- Routing Table
  - Routing table contains information about the best path calculated by the shortest path first algorithm in the database table.

OSPF - Neighbor Table

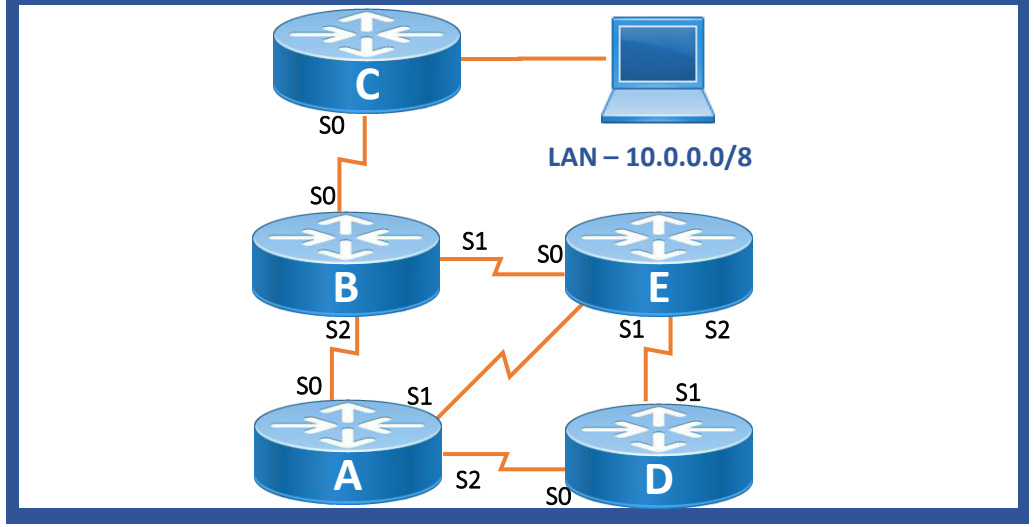
NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1

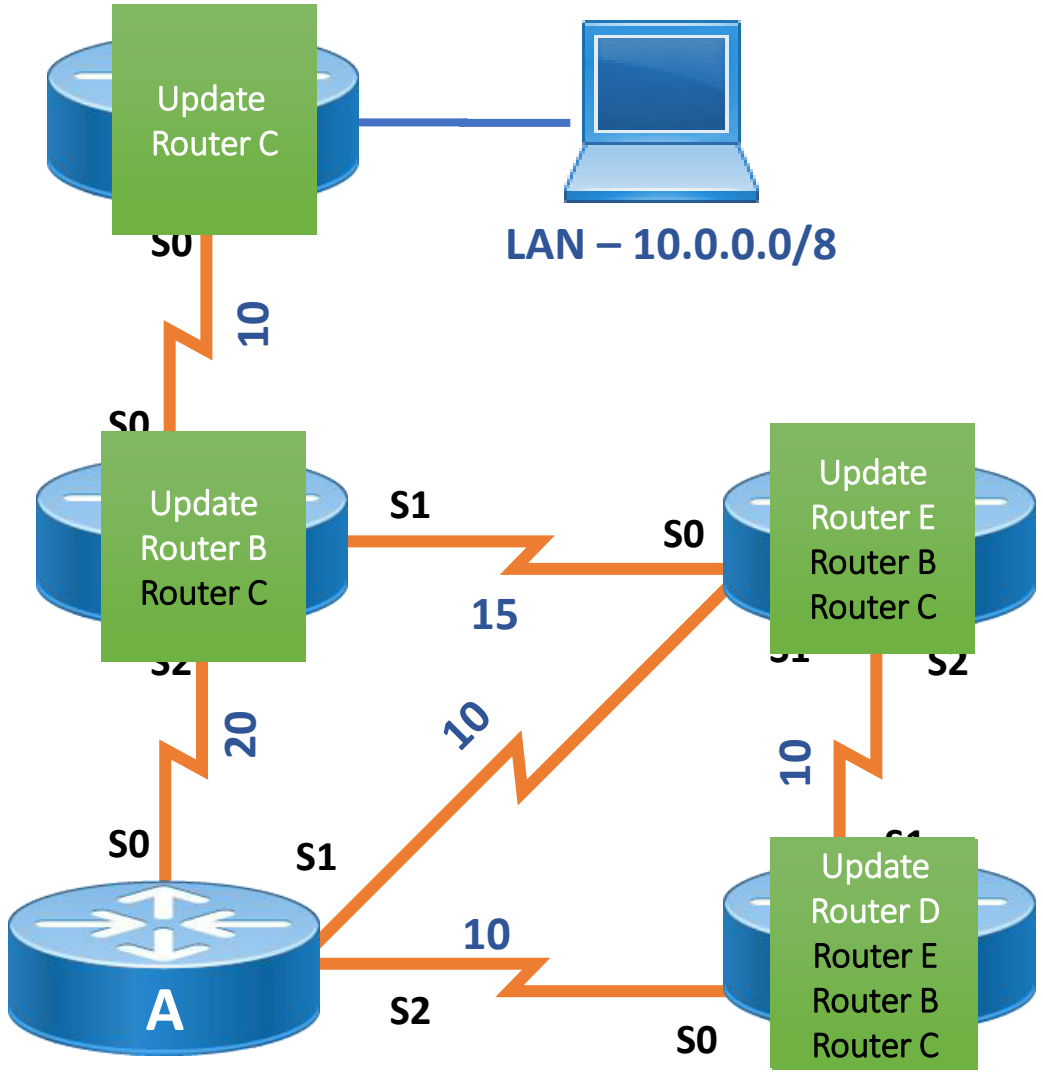


OSPF - Database Table

NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1

DATABASE TABLE (Router A)

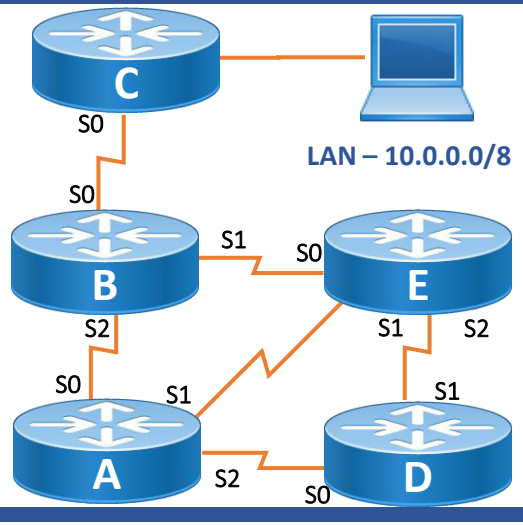




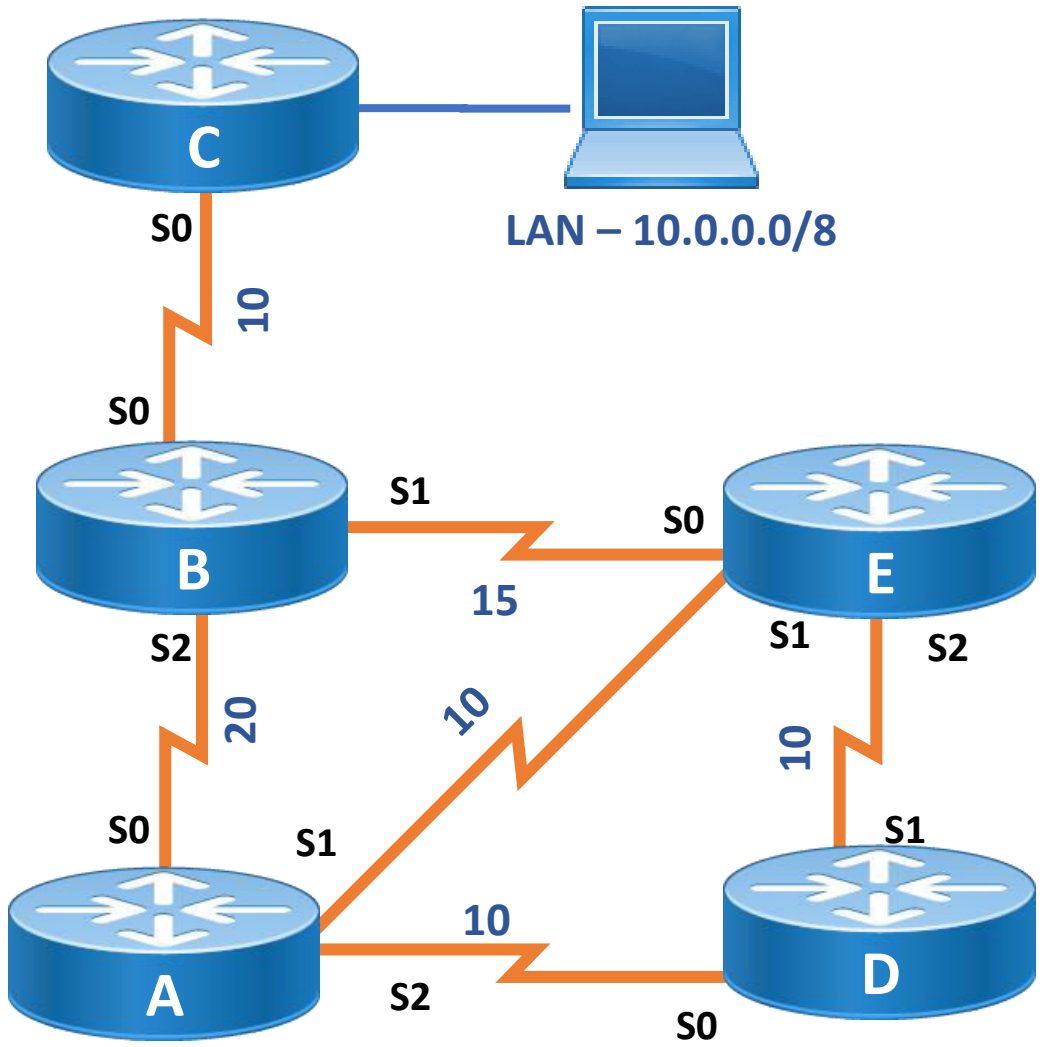
OSPF - Database Table

NEIGHBOR TABLE (Router A)	
Neighbor	Interface
B	S0
D	S2
E	S1

DATABASE TABLE (Router A)



ROUTING TABLE (Router A)
O 10.0.0.0/8 [110/30] via B, 01:36, Serial0



Wild Card Mask

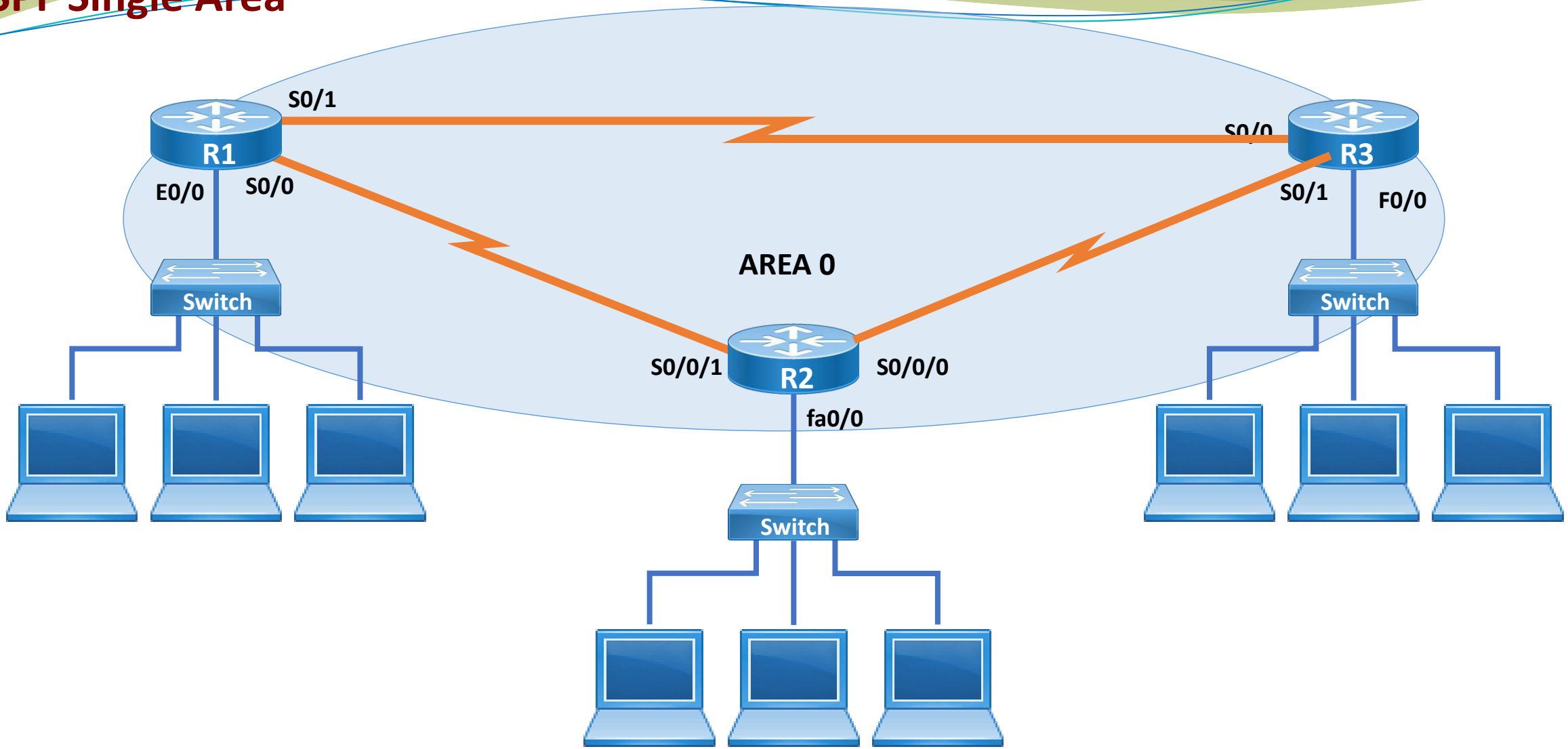
- A wild card mask can be calculated using the formula :

```
        Global Subnet Mask
  –     Subnet Mask
        --------------------------------
        Wild Card Mask
```

E.g.

```
        255.255.255.255          255.255.255.255
  –     255.255.255.   0    –     255.255.255.240
        ----------------         ----------------
         0.   0.   0.255           0.   0.   0.  15
```

OSPF Single Area



OSPF configuration and Verification syntax

OSPF configuration

- Router(config)# ip routing
- Router(config)# router ospf < Process ID >
- Router(config-router)# network < Network ID > <Wildcard mask > area <area ID >

Verification

To check Routing Table

- Router # show ip route

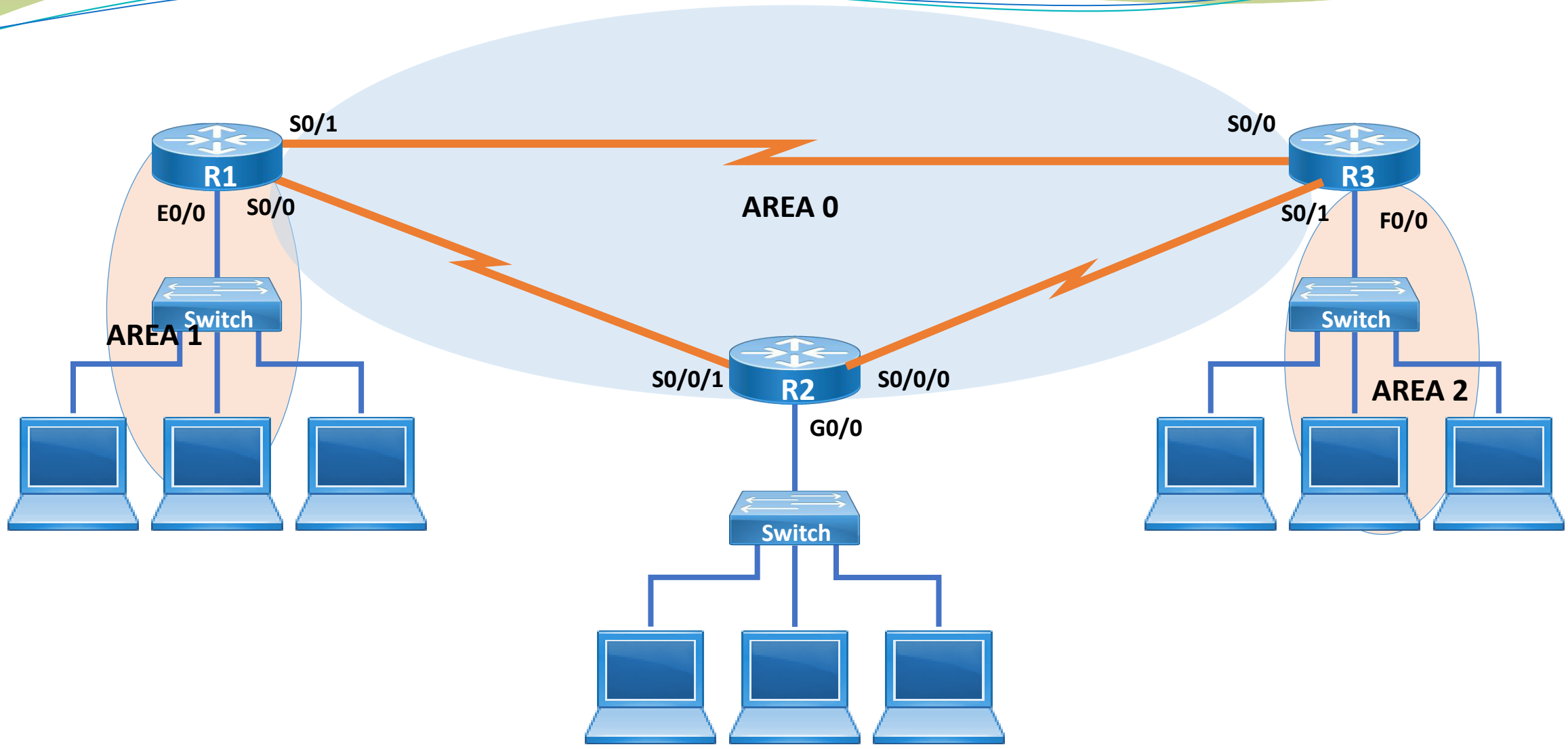
To check Neighbor Table

- Router # show ip ospf neighbor

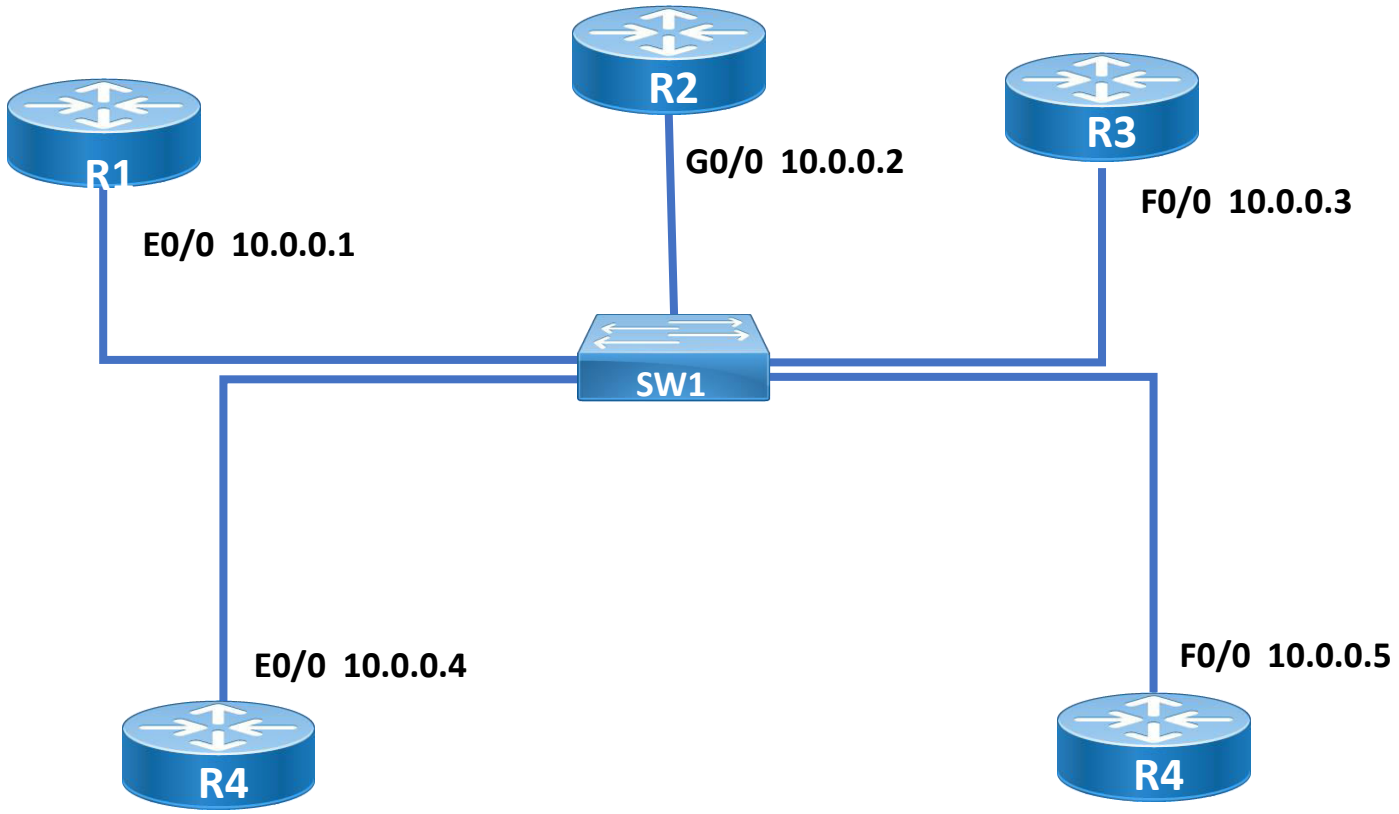
To check Database Table

- Router # show ip ospf database

Multi Area


S0/1
S0/0
R1
R3
E0/0
S0/0
AREA 0
S0/1
F0/0
Switch
Switch
AREA 1
S0/0/1
R2
S0/0/0
AREA 2
G0/0
Switch

OSPF in LAN


R1
R2
R3
G0/0 10.0.0.2
E0/0 10.0.0.1
F0/0 10.0.0.3
SW1
E0/0 10.0.0.4
F0/0 10.0.0.5
R4
R4

DR and BDR

- Designated Router (DR)
  - Designated Router is elected when ever OSPF routers are connected to the same multi-access networks.
  - This is done to reduce the number of adjacencies formed.
  - If there is a change in topology the initial router will only update the DR and BDR and no other router. The DR in turn will update the remaining routers.
- Backup Designated Router (BDR)
  - This is a backup to the DR and will only receive updates but will not update the other routers.
  - If the DR goes down then the BDR will act as the DR.

DR and BDR Elections

- DR and BDR Election is done by the Hello Packets
- The router with the highest OSPF priority will become the DR and the router with the second highest priority will become BDR
- On all routers the default priority is 1
- In that case, the router with the highest Router ID will become the DR and the Router with the second highest ID will become the BDR
- Multicast address used for updating
  - Other routers to DR → 224.0.0.6
  - DR to other routers → 224.0.0.5

DR and BDR

To check DR/BDR status

To check DR/BDR Status

- Router # show ip ospf neighbor

To check the self status

- Router # show ip ospf interface ethernet < no. >

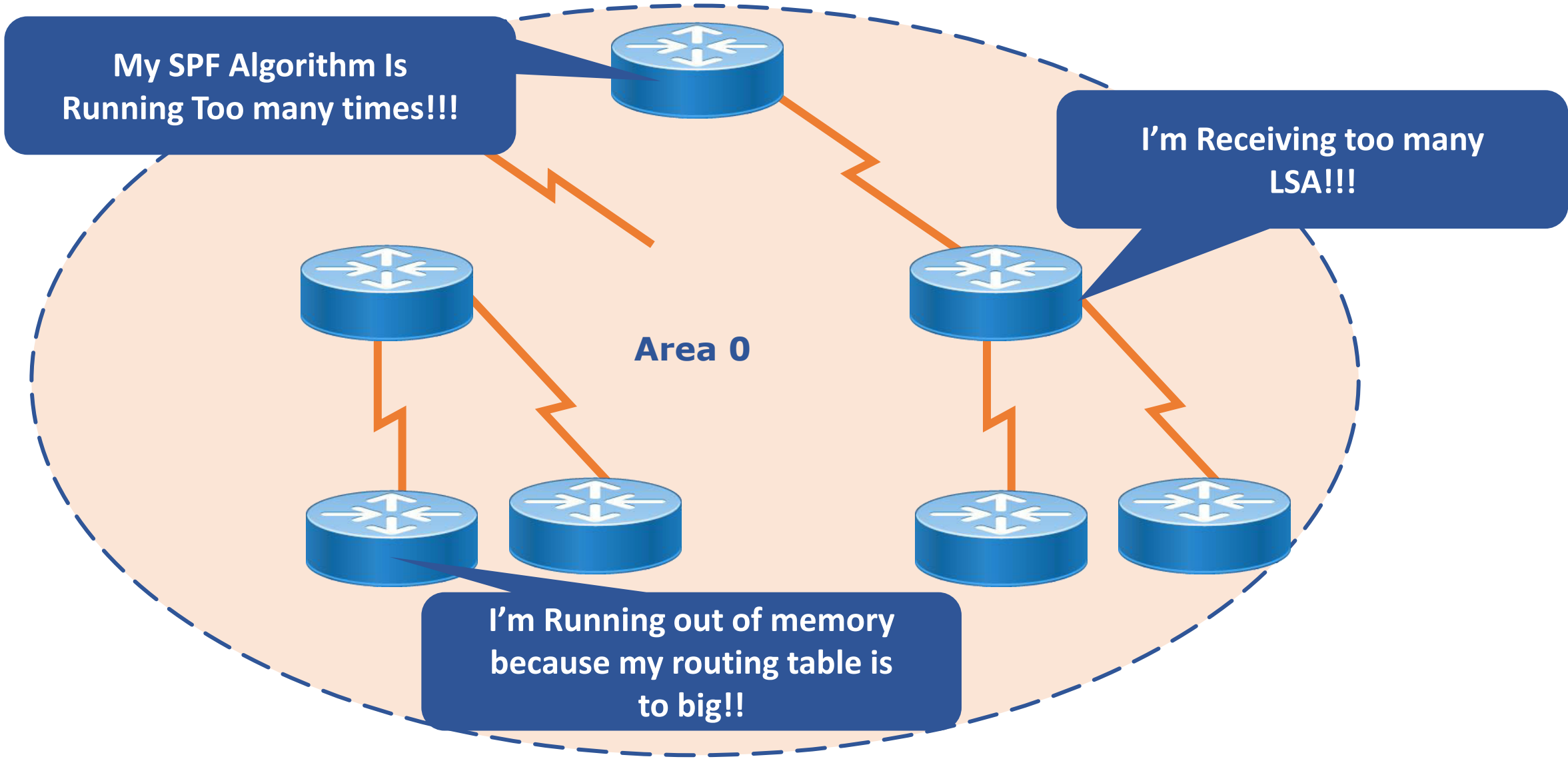
To change the priority

- Router(config) # interface ethernet < no. >
- Router(config-if) # ip ospf priority < priority >

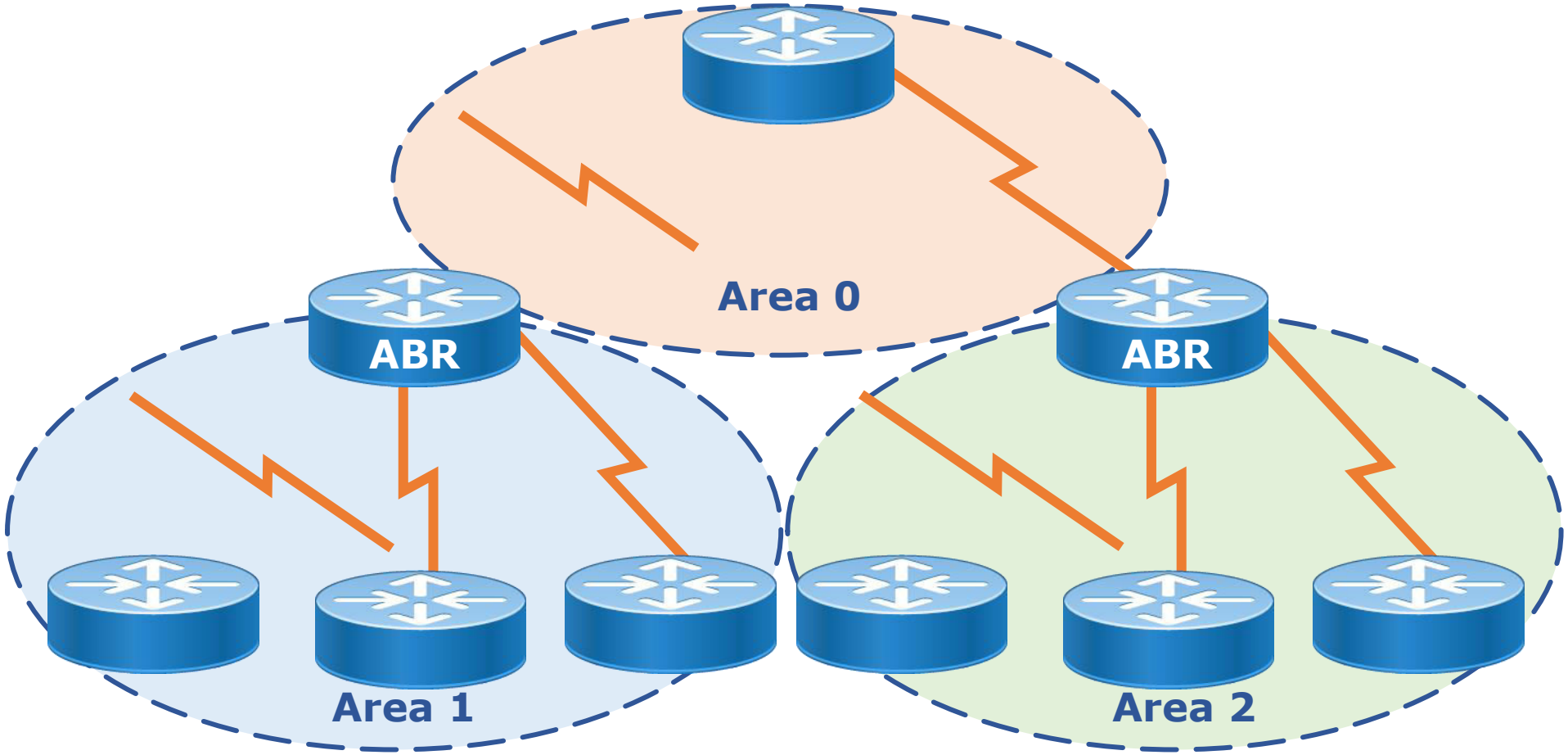
For Election process

- Router # clear ip ospf process

OSPF Multi Area



Issue of Maintaining of large OSPF network



ABR and ASBR

- **ABR (Area Border Router)**
  An OSPF Router with interfaces connected to the backbone area and to other area
- **ASBR (Autonomous System Border Router)**
  A router that exchanges routing information with routers belonging other AS (Autonomous System)

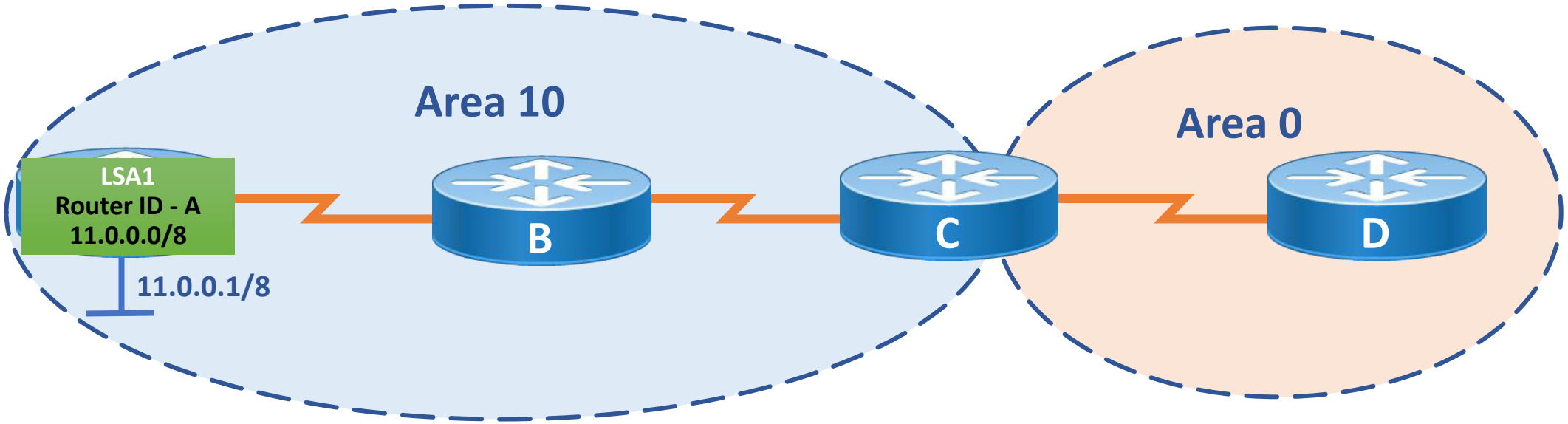
Types of LSAs

1	Router LSAs
2	Network LSAs
3	Summary LSAs

LSA Type - 1

- One Router LSA (type 1) for every router in an area
  - Includes list of directly attached links
  - Each link identified by IP prefix and link type
- Identified by the router ID of the originating router
- Floods within its area only; does not cross the ABR

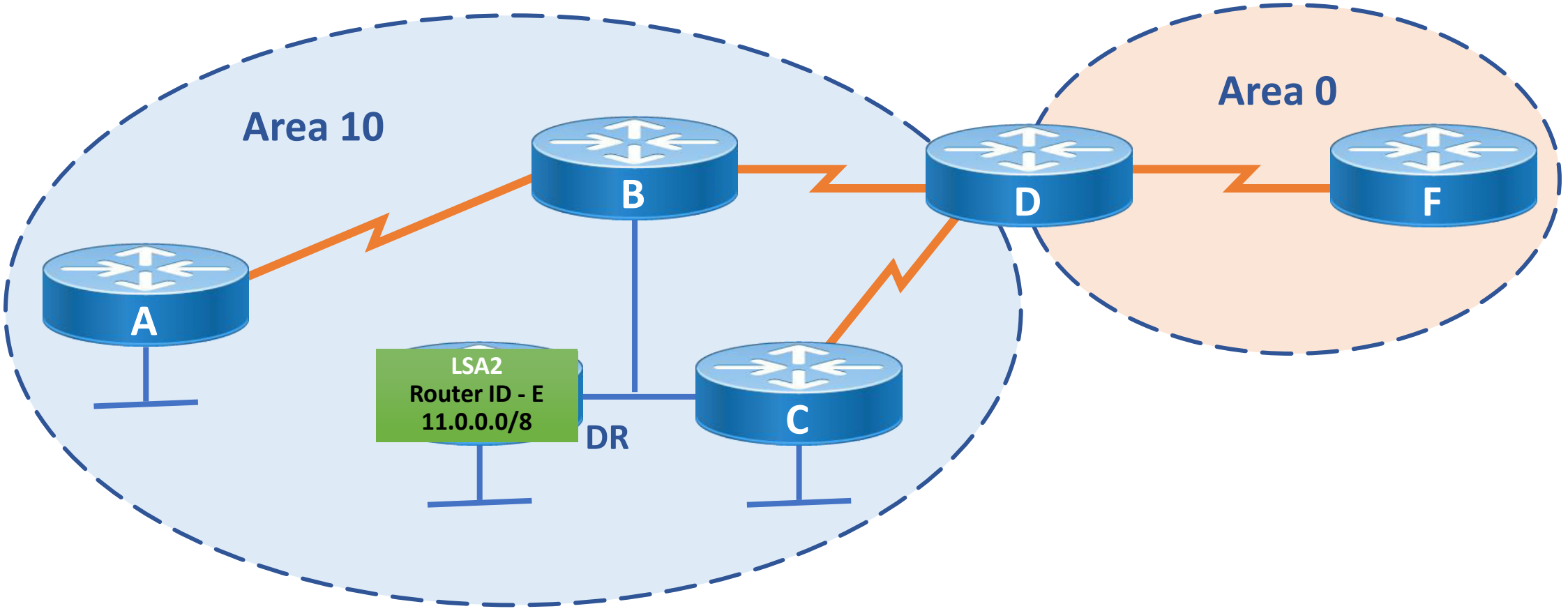
LSA Type - 1



LSA Type - 2

- One Network (type 2) LSA for each transit broadcast or NBMA network in an area
  Includes Network ID, subnet mask and list of attached routers on that transit link
- Advertised by the DR of the transit network
- Floods within its area only; does not cross ABR

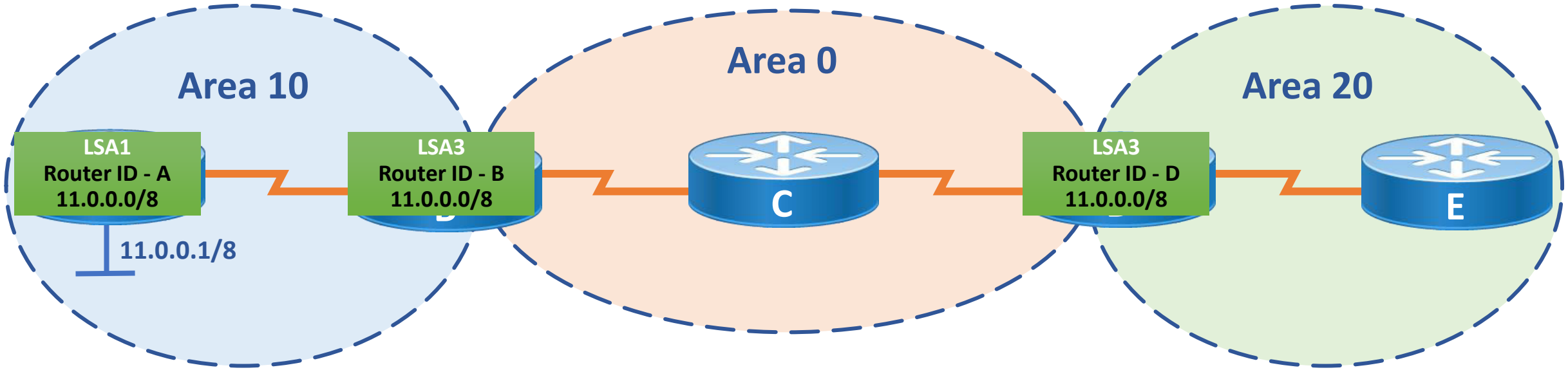
LSA Type - 2



LSA Type - 3

- Type 3 LSAs are used to flood network information to areas outside the originating area (inter-area)
contains network ID and subnet mask
- Advertised by the ABR of originating area
- Regenerated by subsequent ABRs to flood throughout the autonomous system.
- By default, routes are not summarized and there is one type 3 LSA for every subnet

LSA Type - 3


Area 10
Area 0
Area 20
LSA1
Router ID - A
11.0.0.0/8
11.0.0.1/8
LSA3
Router ID - B
11.0.0.0/8
C
LSA3
Router ID - D
11.0.0.0/8
E

Disadvantages of OSPF

- Consumes More Memory and CPU processing time
- Complex configuration