

Networking Overview

Contents



OVERVIEW OF
REFERENCE MODEL
(OSI, TCP/IP)



OVERVIEW OF IPV4
AND IPV6
ADDRESSING



SWITCHING AND
ROUTING BASICS



OVERVIEW OF SDN
AND OPEN FLOW



WINDOWS AND
LINUX NETWORKING
BASICS

OSI Reference Model



International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.



Open Systems Interconnection (OSI) reference model is the result of this effort.



In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.



The Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.

Contd..



The OSI model is now considered the primary Architectural model for inter-computer communications.



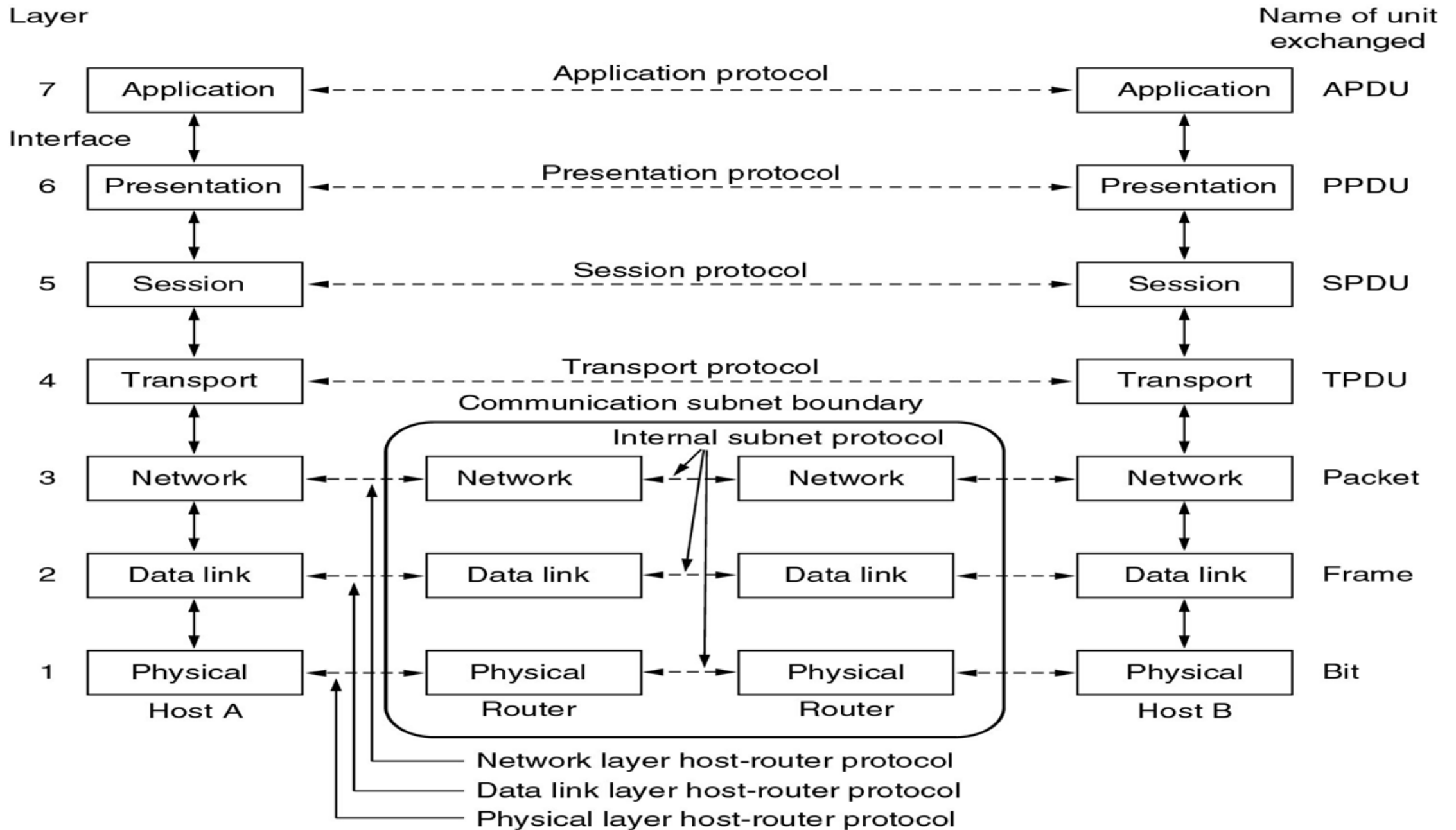
The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.



The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .



•This separation into smaller more manageable functions is known as layering.



Physical Layer



It is the lowest layer of OSI model



It provides physical interface for transmission of information.



It defines rules by which bits are passed from one system to another on a physical communication medium.



It Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.



Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.



The Physical layer is essential for ensuring the reliable transmission of data over the network

Data Link Layer

Data link layer attempts to provide reliable communication over the physical layer interface.

Breaks the outgoing data into frames and reassemble the received frames.

Create and detect frame boundaries.

Handle errors by implementing an acknowledgement and retransmission scheme.

Implement flow control.

Supports points-to-point as well as broadcast communication.

Supports simplex, half-duplex or full-duplex communication

Network Layer



This is the third layer of OSI Model.



Implements routing of frames (packets) through the network.



Defines the most optimum path the packet should take from the source to the destination



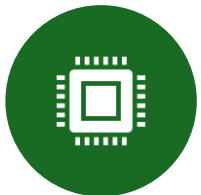
Defines logical addressing so that any endpoint can be identified.



Handles congestion in the network.



Facilitates interconnection between heterogeneous networks (Internetworking).



The network layer also defines how to fragment a packet into smaller packets to accommodate different media

Transport Layer



The Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.



Ensures that the data units are delivered error free.



Ensures that data units are delivered in sequence.



Ensures that there is no loss or duplication of data units.



Provides connectionless or connection oriented service.



Provides for the connection management.



Multiplex multiple connection over a single channel.

Session Layer



Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.



This layer requests for a logical connection to be established on an end-user's request.



Any necessary log-on or password validation is also handled by this layer.



Session layer is also responsible for terminating the connection.



This layer provides services like dialogue discipline which can be full duplex or half duplex.



Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Presentation Layer

- ✓ **Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.**
- ✓ **Also handles data compression and data encryption (cryptography).**

Features:

- Data encryption and decryption
 - Data compression
 - Data formatting
 - Data translation
 - Protocol conversion
 - Verify Data integrity
- ✓ Presentation layer ensures that data sent from one system can be understood by another system by handling data translation, compression, encryption, decryption, and formatting.

Application Layer

Application layer interacts with application programs and is the highest level of OSI model.

Application layer contains management functions to support distributed applications.

Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

Main Features:

Provides a user interface that allows users to interact with network services.

Provides network services to user applications, such as email, file transfer, and remote login.

Translate between different communication protocols, so that systems using different protocols can communicate with each other.

Data formatting

Inter-process communication:.

Provides services that allow users to share network resources, such as printers and file servers.

TCP/IP Reference Model



TCP/IP means Transmission Control Protocol and Internet Protocol.



The Defense Advanced Research Projects Agency ([DARPA](#)), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET, a wide area network that preceded the internet.



It is the network model used in the current Internet architecture as well.



The TCP/IP reference model is a simpler and more flexible model than the OSI model, and is widely used in modern networking.



It is the basis for the Internet Protocol suite and is the protocol stack used for communication over the internet.

TCP/IP Layers

TCP/IP Protocols

| | | | | | |
|-------------------------|----------|------------|--------|----------------------------|------|
| Application Layer | HTTP | FTP | Telnet | SMTP | DNS |
| Transport Layer | TCP | | UDP | | |
| Network Layer | IP | | ARP | ICMP | IGMP |
| Network Interface Layer | Ethernet | Token Ring | | Other Link-Layer Protocols | |

The TCP/IP Protocol Framework

Network Interface Layer

- **Physical addressing:** The Network Interface layer adds a physical address to the data packet, allowing it to be sent over the physical network.
- **Framing:** The Network Interface layer divides the data packet into smaller units called frames, which are transmitted over the network.
- **Error detection and correction:** The Network Interface layer includes error detection and correction mechanisms to ensure that the data transmitted over the network is accurate.
- **Flow control:** The Network Interface layer includes flow control mechanisms to manage the transmission of data between devices.
- **Access control:** The Network Interface layer provides access control to the physical network, allowing devices to share the network resources.
- **Media access management:** The Network Interface layer manages the access to the physical media, such as a shared Ethernet cable, to avoid collisions between data packets.

Protocols

- Ethernet - for wired networks, Wi-Fi (802.11) - for wireless networks
- Point-to-Point Protocol (PPP) - for point-to-point connections, • Serial Line Internet Protocol (SLIP) - for serial connections

Network/Internet Layer

- The Internet layer is responsible for logical transmission of data packets over the internet. It can be compared to the network layer of the OSI model.
- The main functions of the internet layer are:
- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- It reassembles the out-of-order packets when they reach the destination.
- It handles the error in transmission of data packets and fragmentation of data packets.

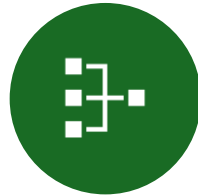
The protocols used in this layer are:

- **Internet Protocol, IP:** It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called datagrams that travel over different routes across multiple nodes.
- **Address Resolution Protocol, ARP:** This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.
- **Internet Control Message Protocol, ICMP:** It monitors sending the queries as well as the error messages.
- **Internet Group Message Protocol, IGMP:** It allows the transmission of a message to a group of recipients simultaneously.

Transport Layer



The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host. It corresponds to the transport layer of the OSI model.



The functions of the transport layer are:



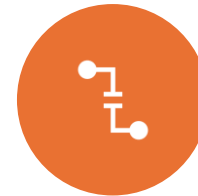
It facilitates the communicating hosts to carry on a conversation.



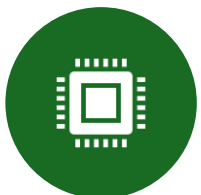
It provides an interface for the users to the underlying network.



It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.



The protocols used in this layer are:



Transmission Control Protocol, TCP: a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data, with mechanisms for flow control and congestion control.



User Datagram Protocol, UDP: It is a message-oriented protocol that provides a simple unreliable, connectionless, unacknowledged service. It is suitable for applications that do not require TCP's sequencing, error control or flow control. It is used for transmitting a small amount of data where the speed of delivery is more important than the accuracy of delivery.

Application Layer



It provides the interface between the applications we use to communicate and the underlying network over which our messages are transmitted.



Application layer protocols are used to exchange data between programs running on the source and destination hosts.



There are many Application layer protocols and new protocols are always being developed.



The functions of the application layer are:



It facilitates the user to use the services of the network.



It is used to develop network-based applications.



It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.



It is also concerned with error handling and recovery of the message as a whole.

Contd..



Hyper Text Transfer Protocol, HTTP: It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.



File Transfer Protocol, FTP: It is a client-server based protocol for transfer of files between client and server over the network.



Simple Mail Transfer Protocol, SMTP: It lays down the rules and semantics for sending and receiving electronic mails (e-mails).



Domain Name System, DNS: It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.



TELNET: It provides bi-directional text-oriented services for remote login to the hosts over the network.



Simple Network Management Protocol, SNMP: It is for managing, monitoring the network and for organizing information about the networked devices.

Difference between OSI and TCP/IP

| OSI MODEL | TCP/IP MODEL |
|---|--|
| 1. 7 layers present in the architecture. | Only 4 layers are present. |
| 2. Not practically implemented yet. | Practical Model. |
| 3. Layering aspects, functions of each layer and division of responsibilities are specifically presented by this model. | Division of responsibilities on each layer is not so specific. |
| 4. The concept of services, interfaces and protocols are well explained. | No clear distinction between the three |
| 5. Model was devised first and protocols were latter fitted to appropriate layers. | The protocols came first and model was just explanation of protocols based on 4 layers. |
| 6. Widely used as a standard reference model in the design of computer networks. | Not considered as a design standard due to the failure in distinguishing services, interfaces and protocols. |
| 7. Connectionless and connection oriented services are there in Network layer but only connection oriented services in Transport layer. | Connectionless and connection oriented services in transport layer but only connectionless service in Network layer. |
| 8. This is a protocol independent model. | This is a protocol specific model. |

IPv4 Address

- An IP address is a unique address that identifies a device on the internet or a local network.
 - IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
 - *An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet*
 - The IPv4 addresses are unique and universal.
 - The address space of IPv4 is 2^{32} or 4,294,967,296
 - IP address: 32-bit identifier for host, router *interface*
 - *interface*: connection between host, router and physical link
- router's typically have multiple interfaces
- host may have multiple interfaces
- IP addresses associated with interface, not host, or router.
- The **IP address** space is managed globally by the Internet **Assigned** Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for **assignment** to end users and local Internet registries, such as Internet service providers

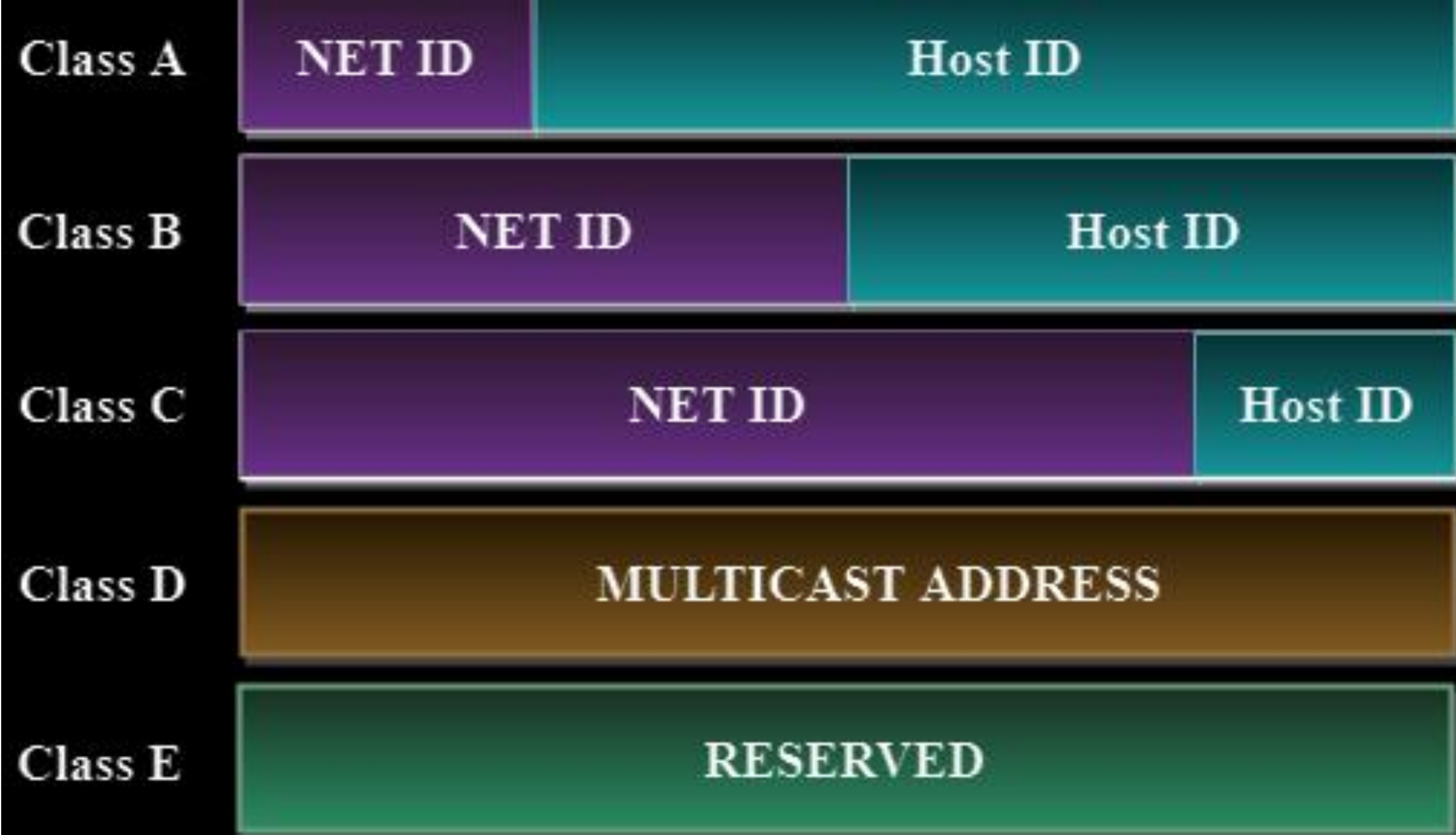
Contd..

IP address has two parts:

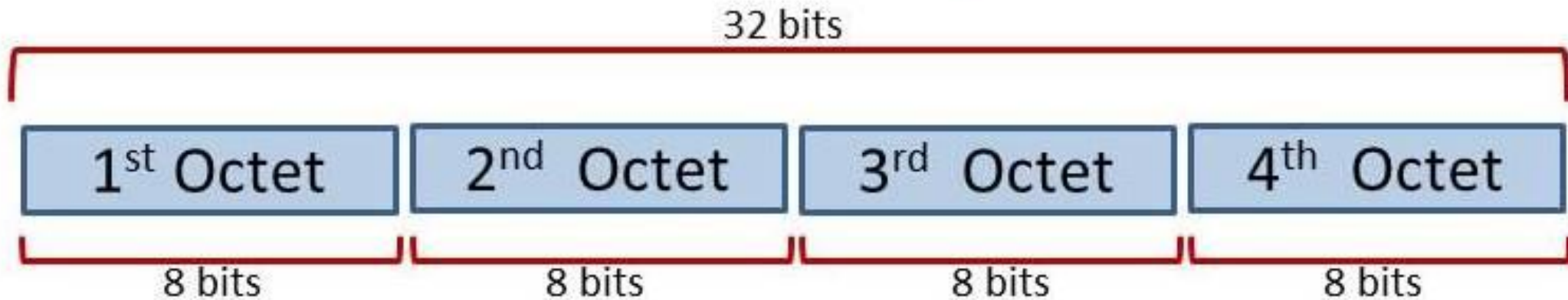
- The network prefix identifies a network and the host number identifies a specific host (actually, interface on the network)
- network part** :high order bits
- host part** :low order bits

Within the IPv4 address range , there are three types of addresses:

- **Network Address** - The address by which we refer to the network.
- **Broadcast Address** - A special address used to send data to all hosts in the network.
- **Host Address** - The addresses assigned to the end devices in the network.



IP Version 4 Addressing Structure



| Classes of IP | 1 st Octet range | Default Subnet Mask |
|---------------|-----------------------------|---------------------|
| Class A | 0-127 | 255.0.0.0 |
| Class B | 128-191 | 255.255.0.0 |
| Class C | 192-223 | 255.255.255.0 |
| Class D | 224-239 | ----- |
| Class E | 240-255 | ----- |

IPv4 Class Ranges

| Class | High order bits | Start ip address | End ip address |
|--------------|-----------------|------------------|-----------------|
| A | 0 | 0.0.0.0 | 127.255.255.255 |
| B | 10 | 128.0.0.0 | 191.255.255.255 |
| C | 110 | 192.0.0.0 | 223.255.255.255 |
| Multicast | 1110 | 224.0.0.0 | 239.255.255.255 |
| Experimental | 1111 | 240.0.0.0 | 255.255.255.255 |

| Classes of IP address | Default Subnet Mask | CIDR Notation | Host bits | Number host per network |
|-----------------------|---------------------|---------------|-----------|-------------------------|
| Class A | 255.0.0.0 | /8 | 24 | $2^{24}-2=1,67,77,214$ |
| Class B | 255.255.0.0 | /16 | 16 | $2^{16}-2=65,534$ |
| Class C | 255.255.255.0 | /24 | 8 | $2^8-2=254$ |

| Private IP | Public IP |
|---|---|
| Used with LAN or Network | Used on Public Network |
| Not recognized over Internet | Recognized over Internet |
| Assigned by LAN administrator | Assigned by Service provider / IANA |
| Unique only in LAN | Unique Globally |
| Free of charge | Cost associated with using Public IP |
| Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255 | Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255 |

IPv6 address

- IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.
- Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network. Packet switching involves the sending and receiving of data in packets between two nodes in a network.
- The most important feature of IPv6 is a much larger address space than in IPv4. IPv6 addresses are 128 bits long, compared to only 32 bits previously.
- While the IPv4 address space contains only about **4.3 billion addresses**, IPv6 supports approximately 340 undecillion (3.4×10^{38}) unique addresses, deemed enough for the foreseeable future.
- **This number is 340,282,366,920,938,463,463,374,607,431,768,211,456, which is normally expressed in scientific notation as about 3.4×10^{38} addresses. That's about 340 trillion, *trillion*, **trillion** addresses.**

IPv6 Address Notation

My IP Address is:

IPv6: ? 2404:7c00:48:f4bd:516c:a401:a592:dd94

IPv4: ? 43.245.86.73

- IPv6 addresses are denoted by eight groups of hexadecimal quartets separated by colons in between them.

Following is an example of a valid IPv6 address:

2001:cdba:0000:0000:0000:0000:3257:9652

Any four-digit group of zeroes within an IPv6 address may be reduced to a single zero or altogether omitted. Therefore, the following IPv6 addresses are similar and equally valid:

2001:cdba:0000:0000:0000:0000:3257:9652

2001:cdba:0:0:0:0:3257:9652

2001:cdba::3257:9652

Categories of IPv6 Address

- **Unicast address** The unicast address specifies a single interface. A packet sent to a unicast address destination travels from one host to the destination host.
- The two regular types of unicast addresses include:
- **Link-local address:** Link-local addresses are designed for use on a single local link (local network). Link-local addresses are automatically configured on all interfaces. The prefix used for a link-local address is fe80::/10. Routers do not forward packets with a destination or source address containing a link-local address.
- **Global address:** Global addresses are designed for use on any network. The prefix used for a global address begins with binary 001.



Anycast address: An anycast address specifies a set of interfaces, possibly at different locations, that all share a single address. A packet sent to an anycast address goes only to the nearest member of the anycast group..



Multicast address: The multicast address specifies a set of interfaces, possibly at multiple locations. The prefix used for a multicast address is ff. If a packet is sent to a multicast address, one copy of the packet is delivered to each member of the group.

Special IPv6 Addresses

Down

| IPv6 Address | Description |
|------------------------|--|
| <code>::/0</code> | <ul style="list-style-type: none">• All networks and used when specifying a default static route.• It is equivalent to the IPv4 quad-zero (0.0.0.0) |
| <code>::/128</code> | <ul style="list-style-type: none">• Unspecified address and is initially assigned to a host when it first resolves its local link address |
| <code>::1/128</code> | <ul style="list-style-type: none">• Loopback address of local host• Equivalent to 127.0.0.1 in IPv4 |
| <code>FE80::/10</code> | <ul style="list-style-type: none">• Link-local unicast address• Similar to the Windows autoconfiguration IP address of 169.254.x.x |
| <code>FF00::/8</code> | <ul style="list-style-type: none">• Multicast addresses |
| All other addresses | <ul style="list-style-type: none">• Global unicast address |

Difference between IPv4 and IPv6

- The major difference in the IPv4 and IPv6 addressing is the appearance of the IP addresses. IPv4 uses four one-byte decimal numbers separated by a dot (e.g., 192.168.0.1). On the other hand, IPv6 uses hexadecimal numbers separated by colons (e.g., fe80::d4a8:4521:d2d8:d8f4b11).
- IPv4 and IPv6 are numeric and alphanumeric addressing methods respectively.
- The length of IPv4 address is 32-bit while length of IPv6 is 128-bit.
- IPv4 and IPv6 offer 12- and eight-headers fields respectively.
- Broadcasting feature is supported only by IPv4, not IPv6.
- The checksum field is absent in IPv6 and present in IPv4.
- The concept of virtual length subnet masking is applicable only to IPv4.
- For mapping MAC addresses, IPv4 uses ARP while IPv6 makes use of NDP(Neighbour Discovery Protocol)
- IPv4 supports manual and DHCP address configurations, and IPv6 supports auto and renumbering address configuration
- IPv4 can generate address space up to 4.29 billion whereas IPv6 can generate up to 3.4×10^{38} of address space.

Switching



The mechanism for exchange of information between different computer networks and network segments is called switching



In large networks there might be multiple paths linking sender and receiver.



Information may be switched as it travels through various communication channels.



There are three typical switching techniques available for digital traffic.



Circuit Switching



Message Switching



Packet Switching

Circuit switching is a technique that directly connects the sender and the receiver in an unbroken path.

Circuit switching was designed in 1878 in order to send telephone calls down a dedicated channel.

This channel remains open and in use throughout the whole call and cannot be used by any other data or phone calls

There are three phases in circuit switching:

Circuit Establish

Data Transfer

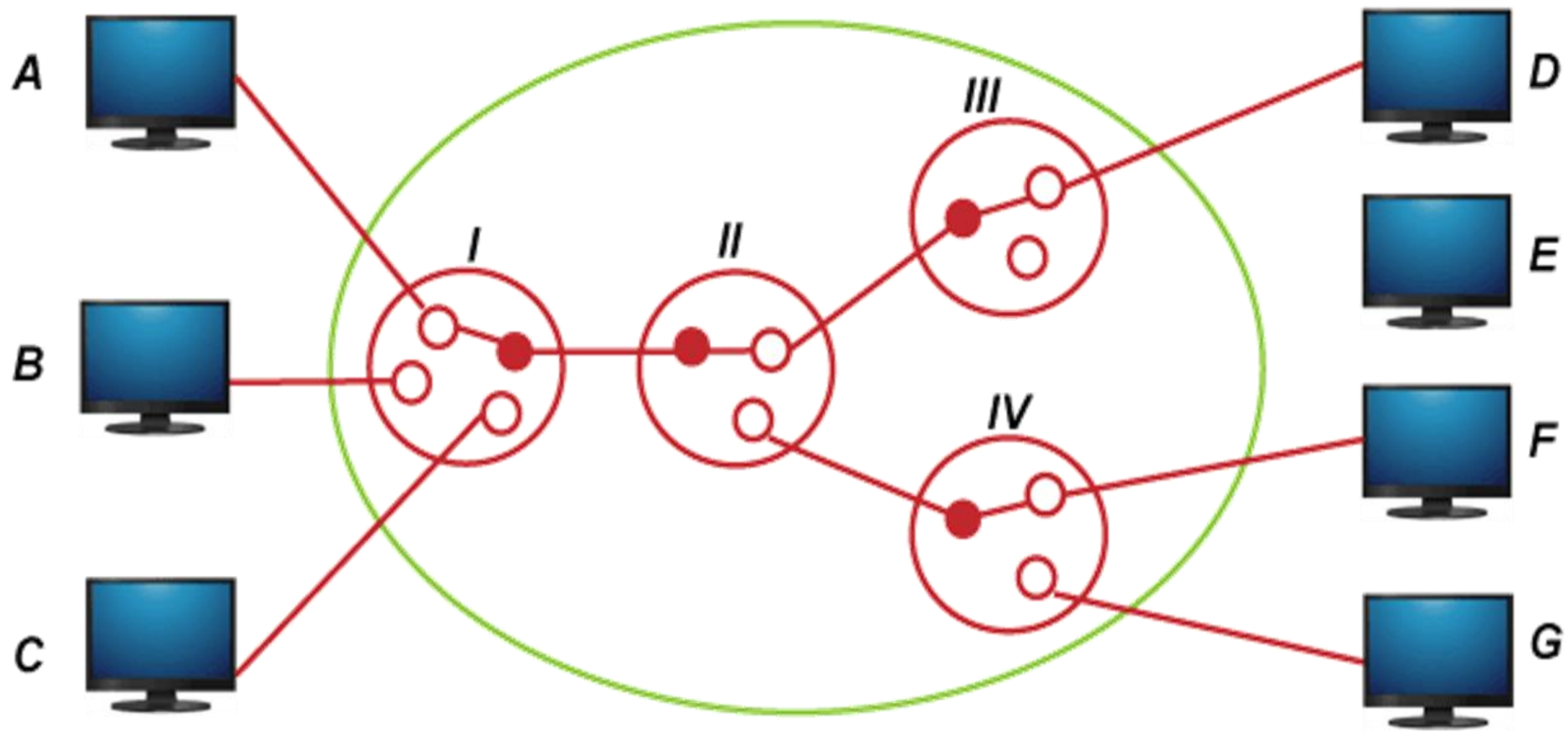
Circuit Disconnect

In telephone communication system, the normal voice call is the example of Circuit Switching.

Circuit switching is pass through three phases, that are circuit establishment, data transfer and circuit disconnect

With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.

Routing decisions must be made when the circuit is first established, but there are no decisions made after that time.



Circuit Switched Network

Message Switching



- Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced.



- In message switching, end-users communicate by sending and receiving *messages* that included the entire data to be shared.



- With message switching there is no need to establish a dedicated path between two stations.



- When a station sends a message, the destination address is appended to the message.



- The message is then transmitted through the network, in its entirety, from node to node.



- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.

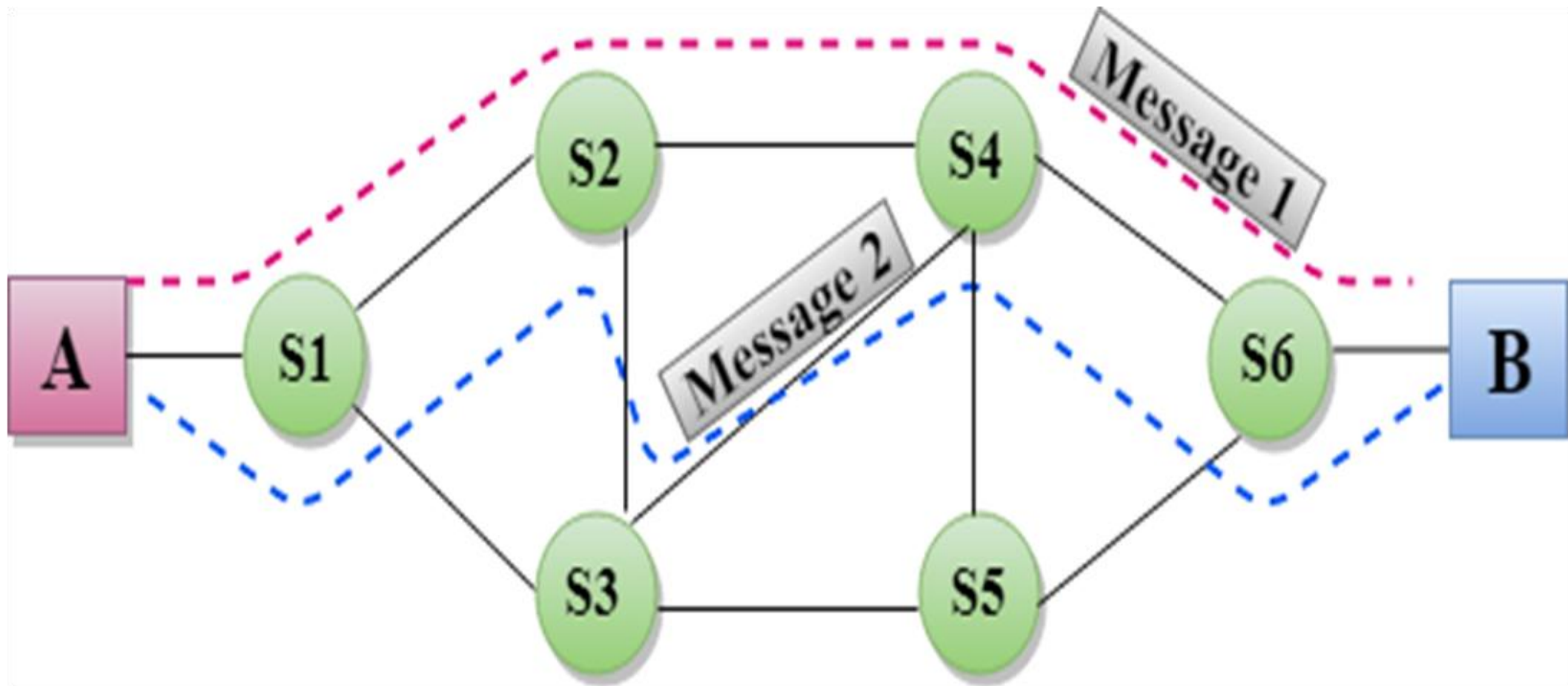


- This type of network is called a store-and-forward network.



- Message switching treats each message as an independent entity.

Contd.



Packet Switching

In packet switching, a message is broken into individual chunks called packets and packets are given a unique number to identify their order at the receiving end.

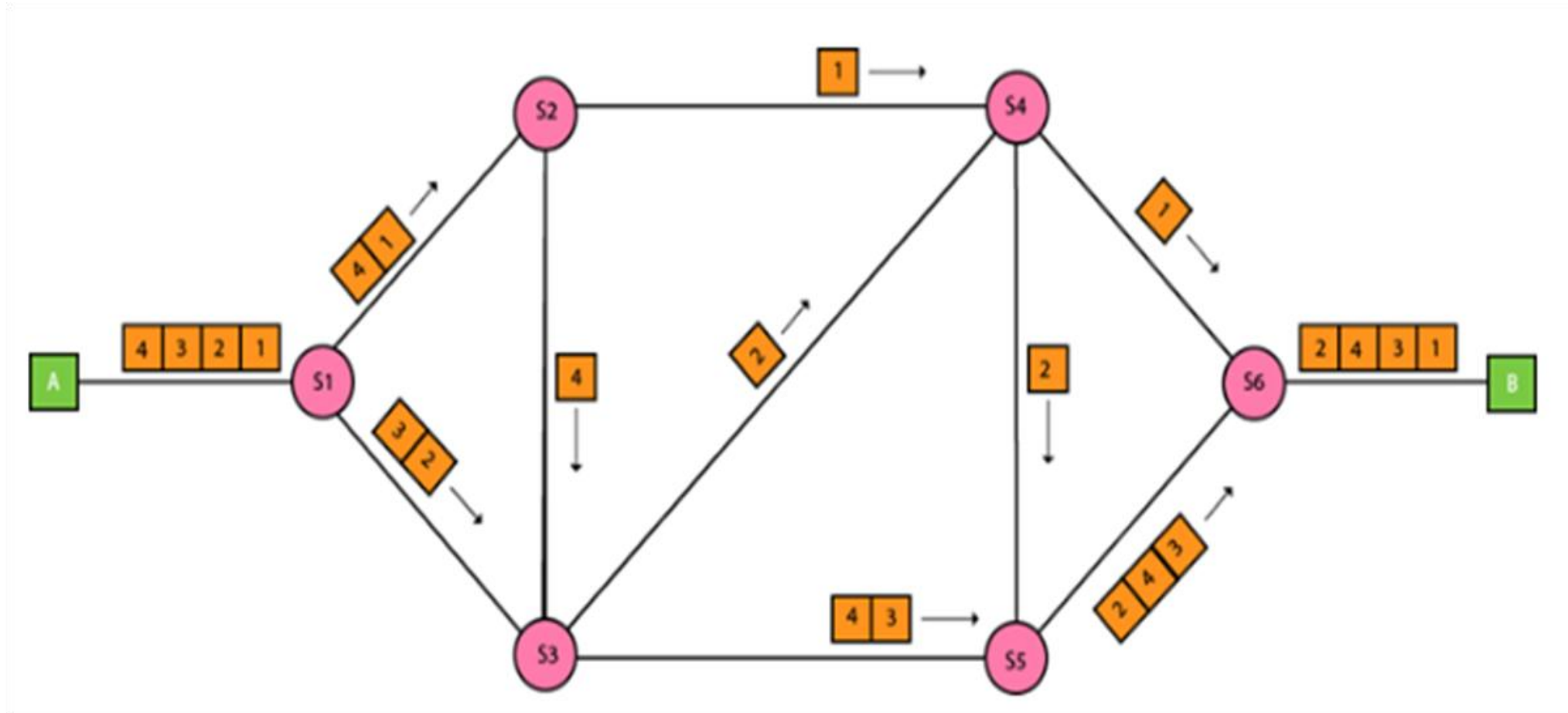
Every packet contains some information in its headers such as source address, destination address and sequence number.

Packets will travel across the network, taking the shortest path as possible.

All the packets are reassembled at the receiving end in correct order.

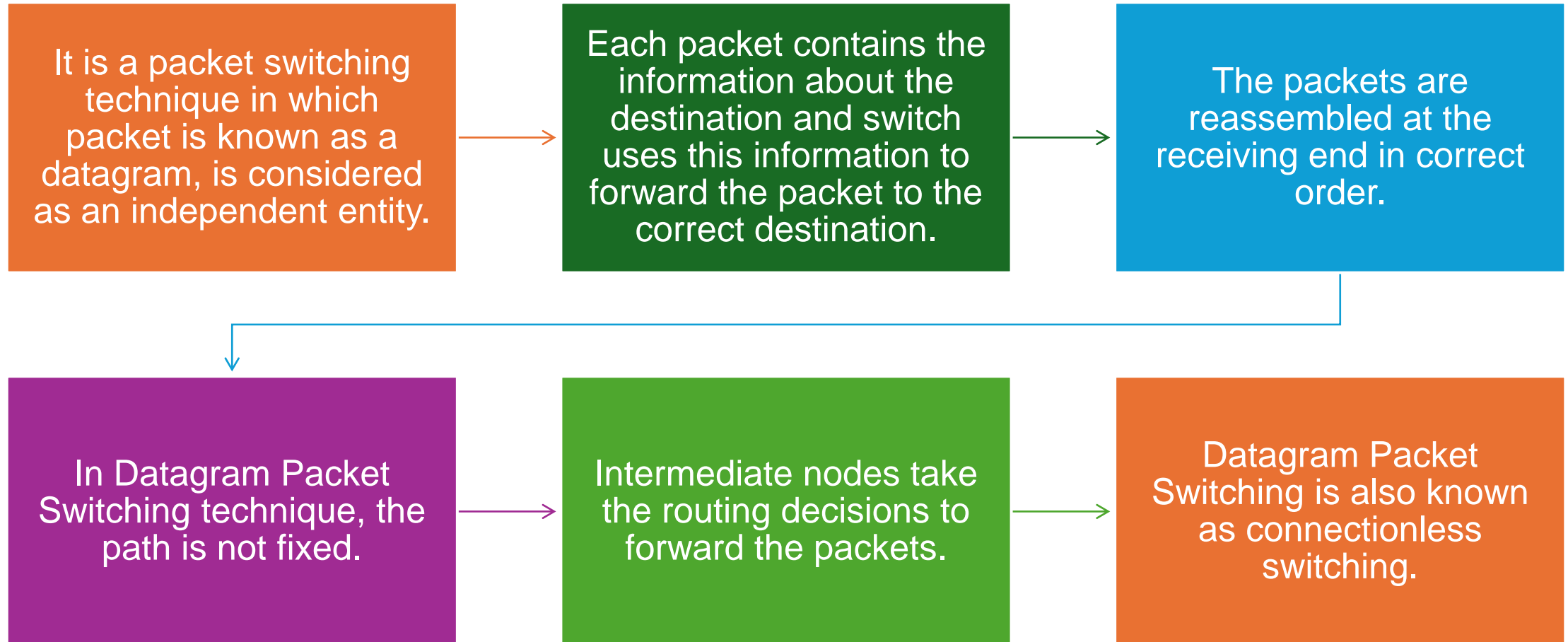
If any packet is missing or corrupted, then the message will be sent to resend the message.

If the correct order of the packets is reached, then the acknowledgment message will be sent.



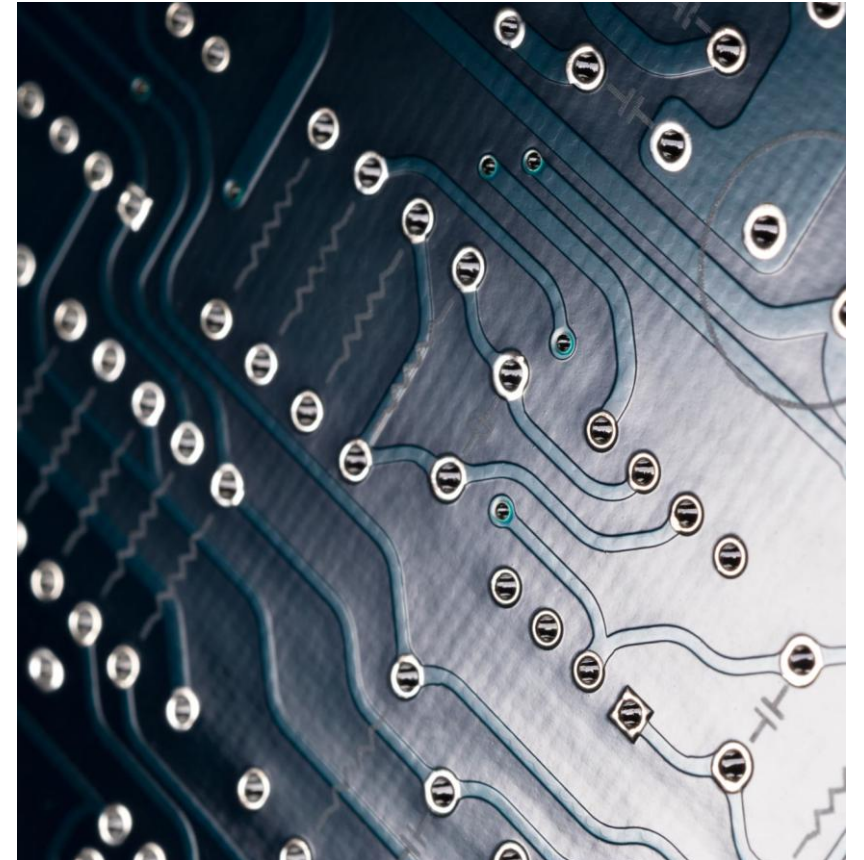
Packet Switching

Datagram Packet Switching



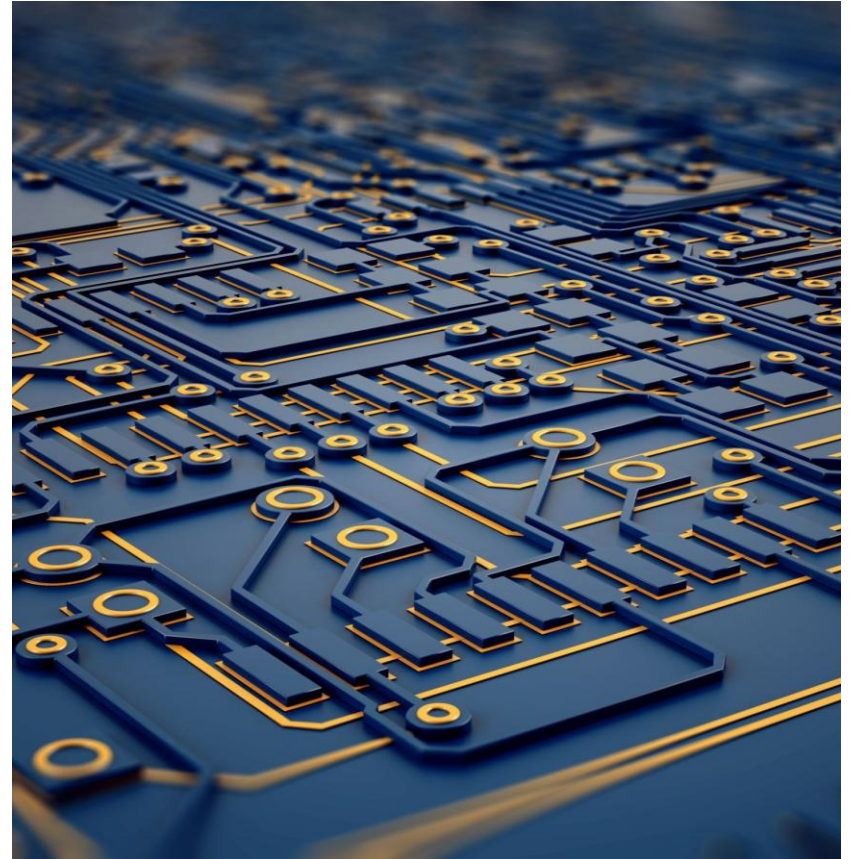
Virtual Circuit Packet Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.
- Virtual circuits imply acknowledgements, flow control, and error control, so these circuits are reliable



Advantages of Packet Switching

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.



| Circuit Switching | Message Switching | Packet Switching |
|---|---|--|
| There is physical connection b/w transmitter and receiver | No physical path is set in advance b/w transmitter and receiver | No physical path is established b/w transmitter and receiver |
| All the packet uses same path | Packet are stored and forward | Packet travels independently |
| Need an end to end path before the data transmission | No need of end to end path before data transmission | No need of end to end path before data transmission |
| Reserves the entire bandwidth in advance | Does not reserve the bandwidth in advance | Does not reserve the bandwidth in advance |
| Waste of bandwidth is possible | No waste of bandwidth | No waste of bandwidth |
| It cannot support store and forward transmission | It support store and forward transmission | It support store and forward transmission |
| Not suitable for handling interactive traffic | Suitable for handling interactive traffic | Suitable for handling interactive traffic |

Comparison of Datagram & VC networks

| Circuit switching | Datagram packet switching | Virtual-circuit packet switching |
|---|--|---|
| Dedicated transmission path | No dedicated path | No dedicated path |
| Continuous transmission of data | Transmission of packets | Transmission of packets |
| Fast enough for interactive | Fast enough for interactive | Fast enough for interactive |
| Messages are not stored | Packets may be stored until delivered | Packets stored until delivered |
| The path is established for entire conversation | Route established for each packet | Route established for entire conversation |
| Call setup delay; negligible transmission delay | Packet transmission delay | Call setup delay; packet transmission delay |
| Busy signal if called party busy | Sender may be notified if packet not delivered | Sender notified of connection denial |

Router



- A router is a device that connects two or more IP networks or sub networks
- Routers are networking devices operating at layer 3 or a **network layer** of the **OSI model**
- They are responsible for receiving, analysing, and forwarding data packets among the connected **computer networks**
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.
- A router looks at the destination address in the IP packet, and decides how to forward it.

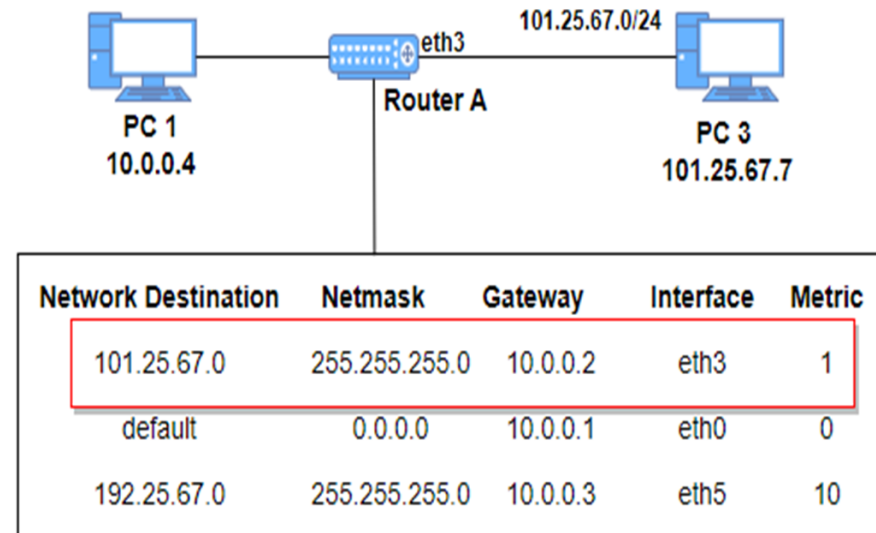


Routing

- Routing is the process of forwarding packets from one network to the destination address in another network.
- **Routing** is the process of selecting a path for traffic in a network or between or across multiple networks

Routing Table

- A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.
- All IP-enabled devices, including routers and switches, use routing table
- Routing table contains the information necessary to forward a packet along the best path toward its destination.
- Each packet contains information about its origin and destination.
- Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network.



Forwarding Table

- Each router/host has a forwarding table, indicating the path or the next hop for a given destination host or a network
- The router/host tries to match the destination address of a packet against entries in the forwarding table
- If there is a match, the router forwards it to the corresponding gateway router or directly to the destination host
- Default route is taken if no other entry matches the destination address

The Forwarding Table

| Destination | Next-Hop | Interface |
|------------------|--------------------|-----------|
| 10.40.0.0/16 | 192.248.40.60 | Ethernet0 |
| 192.248.0.140/30 | Directly connected | Serial1 |
| 192.248.40.0/26 | Directly connected | Ethernet0 |
| 192.248.0.0/17 | 192.248.0.141 | Serial1 |
| 203.94.73.202/32 | 192.248.40.3 | Ethernet0 |
| 203.115.6.132/30 | Directly connected | Serial0 |
| Default | 203.115.6.133 | Serial0 |

Typical forwarding table on a simple edge router

IP Routing

- Forwarding table entry (the path) is created by the administrator (static) or received from a routing protocol (dynamic)
- More than one routing protocol may run on a router – Each routing protocol builds its own routing table (Local RIB)
- Several alternative paths may exist – Best path selected for the router's Global routing table (RIB)
- Decisions are updated periodically or as topology changes (event driven)
- Decisions are based on: – Topology, policies and metrics (hop count, filtering, delay, bandwidth, etc.)

Routing Protocols

- A **routing protocol** specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.

Every network routing protocol performs three basic functions:

- *discovery* – identify other routers on the network
- *route management* – keep track of all the possible destinations (for network messages) along with some data describing the pathway of each
- *path determination* – make dynamic decisions for where to send each network message

Routing Algorithm

- Routing is the process of transferring the packets from one network to another network and delivering the packets to the hosts.
- Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently
- The traffic is routed to all the networks in the internetwork by the routers. In the routing process a router must know following things:
 - Destination device address.
 - Neighbor routers for learning about remote networks.
 - Possible routes to all remote networks.
 - The best route with the shortest path to each remote network.
 - How the routing information can be verified and maintained

Static Routing

- Static routing is a process in which we have to manually add routes in routing table.
- **Static routing** does not involve any change in routing table unless the network administrator changes or modify them manually.
- Static routing algorithms function well where the network traffic is predictable.
- This is simple to design and easy to implement. There is no requirement of complex routing protocols.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology

Dynamic Routing

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

A dynamic protocol have following features:

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

Contd.

Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

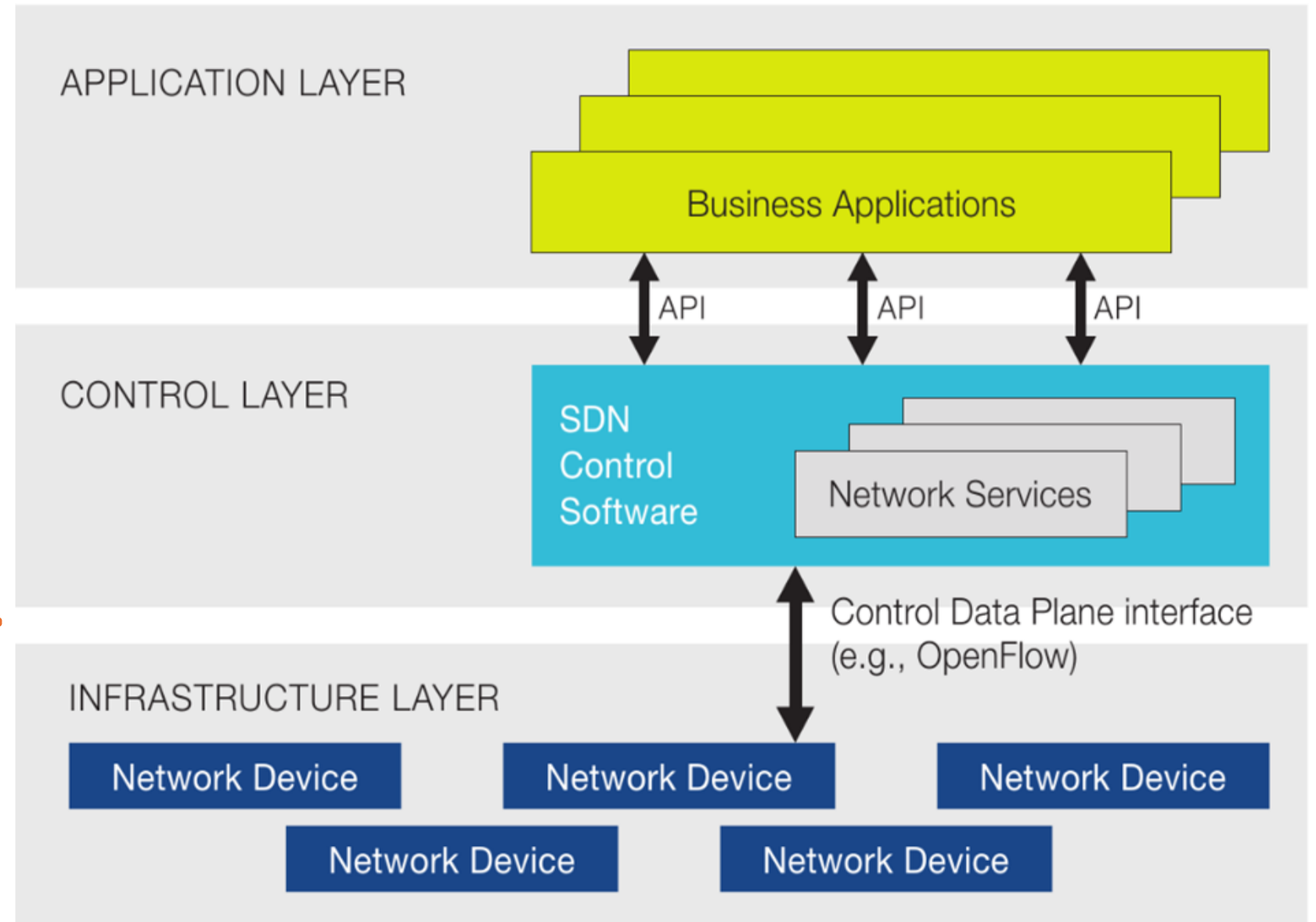
• Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing

SDN and Open Flow

- Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.
- Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications.
- This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.
- The OpenFlow protocol is a foundational element for building SDN solutions.
- OpenFlow is a network communication protocol used between controllers and forwarders in an SDN architecture
- OpenFlow introduces the concept of flow table, based on which forwarders forwards data packets.

Architecture of SDN










SDN Applications:

- SDN Applications are programs that communicate behaviors and needed resources with the SDN Controller via application programming interfaces (APIs).
- In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes.
- These applications could include networking management, analytics, or business applications used to run large data centers.
- For example, an analytics application might be built to recognize suspicious network activity for security purposes.








SDN Controller:

- The SDN Controller is a logical entity that receives instructions or requirements from the SDN Application layer and relays them to the networking components.
- The controller also extracts information about the network from the hardware devices and communicates back to the SDN Applications with an abstract view of the network, including statistics and events about what is happening.

- 
- **SDN Networking Devices:** The SDN networking devices control the forwarding and data processing capabilities for the network.
 - This includes forwarding and processing of the data path.
 - The SDN architecture APIs are often referred to as northbound and southbound interfaces, defining the communication between the applications, controllers, and networking systems.
 - A Northbound interface is defined as the connection between the controller and applications, whereas the Southbound interface is the connection between the controller and the physical networking hardware.
 - Because SDN is a virtualized architecture, these elements do not have to be physically located in the same place
- 
- 
- 
- 

Open Flow

- OpenFlow is considered the first software-defined networking (SDN) standard.
- The OpenFlow protocol is a network protocol closely associated with Software-Defined Networking (SDN).
- SDN is a network architecture that allows network administrators to control traffic from a centralized Controller. A Controller is an application that manages flow control in an SDN environment.
- The OpenFlow protocol allows a server to instruct network switches where to send data packets.
- It is an open communications protocol in SDNs that enables the SDN Controller to interact with the forwarding plane (switches, routers, etc.) and adapt the network to be responsive to real-time traffic and business requirements.

- 
- In a non-OpenFlow or legacy switch, packet forwarding (the data path) and route determination (the control path) occur on the same device.
 - A switch using the OpenFlow protocol separates the data path from the control path.
 - The OpenFlow protocol is used on the control plane (which is centralized on the SDN Controller) to communicate with the data plane (which is distributed among the network nodes) in an SDN network.
 - Using the OpenFlow specifications, a switch can be configured to operate with similar results to a legacy switch, without having to manually re-configure the switch if the network changes.
- 
- 
- 
- 

Advantages of SDN

CENTRALIZED CONTROL FOR SIMPLIFIED MANAGEMENT.



```
graph TD; A[CENTRALIZED CONTROL FOR SIMPLIFIED MANAGEMENT.] --> B[DYNAMIC ADAPTABILITY TO CHANGING TRAFFIC PATTERNS.]; B --> C[IMPROVED SCALABILITY FOR EASY NETWORK EXPANSION.]; C --> D[ENHANCED SECURITY THROUGH CENTRALIZED POLICY ENFORCEMENT.]; D --> E[FACILITATION OF INNOVATION WITH PROGRAMMABILITY AND AUTOMATION.];
```

DYNAMIC ADAPTABILITY TO CHANGING TRAFFIC PATTERNS.

IMPROVED SCALABILITY FOR EASY NETWORK EXPANSION.

ENHANCED SECURITY THROUGH CENTRALIZED POLICY ENFORCEMENT.

FACILITATION OF INNOVATION WITH PROGRAMMABILITY AND AUTOMATION.

Basics in Computer Networking

- **Network:** A collection of interconnected computers and devices that can communicate with each other.
- **Nodes:** Devices connected to a network, including computers, servers, printers, routers, switches, etc.
- **Protocol:** Rules and standards governing how data is transmitted over a network. Examples include TCP/IP, HTTP, and FTP.
- **Topology:** The physical and logical arrangement of nodes in a network. Common topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** Networks provided by service providers, allowing users to lease network capacity and functionality. Examples include wireless communications and data carriers.
- **IP Address:** Unique numerical identifiers assigned to devices on a network, used for identification and communication.
- **DNS (Domain Name System):** A protocol translating human-readable domain names (like www.google.com) into IP addresses computers can understand.
- **Firewall:** A security device or software that monitors and controls network traffic, protecting against unauthorized access and security threat

Windows and Linux Networking Basics

In Windows, networking refers to the process of connecting devices and sharing resources like files, printers, and internet access.

Fundamental steps to set up and manage network connections on a Windows and Linux computer

Check Hardware: Ensure network hardware (Ethernet or Wi-Fi adapters) is installed and functional.

Enable Network Adapter: Activate the network adapter using command-line tools or network settings.

Scan for Networks: Use a network manager tool to scan for available networks.

Connect: Select the desired network and provide credentials if required.

Configure Settings: Optionally adjust network settings using command-line tools or configuration files.

Verify Connection: Confirm internet access by using web browsers or network-dependent applications.

Manage Profiles: Utilize network profiles to customize settings for different environments.

Troubleshoot: Use built-in tools to diagnose and resolve any connectivity issues.