./

GENESIS – Networking

Learning Report



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be Approved** | **Remarks/Revision Details** |
| 1. | 24/03/2020 | Abhishek Guria |  | Srinivas K |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Details**

Contents

[Contents 3](#_Toc59439644)

[1. Networking: 5](#_Toc59439645)

[**1.1** **Types of Networking:** **Error! Bookmark not defined.**](#_Toc59439646)

[Local Area Network (LAN): Error! Bookmark not defined.](#_Toc59439647)

[Wide Area Network (WAN): Error! Bookmark not defined.](#_Toc59439648)

[Metropolitan Area Network (MAN): Error! Bookmark not defined.](#_Toc59439649)

[Personal Area Network (PAN): Error! Bookmark not defined.](#_Toc59439650)

[**1.2** **Network Topologies:** 6](#_Toc59439651)

[Bus Topology: 7](#_Toc59439652)

[Mesh Topology: 8](#_Toc59439653)

[Star Topology: 8](#_Toc59439654)

[Ring Topology: 9](#_Toc59439655)

[Tree Topology: 10](#_Toc59439656)

[2 Wired Networks: 11](#_Toc59439657)

[3 Wireless Networking: 11](#_Toc59439658)

[4 Terminologies: 12](#_Toc59439659)

[**Hub:** 12](#_Toc59439660)

[**Switch:** 12](#_Toc59439661)

[**Router:** 13](#_Toc59439662)

[**Bridge:** 13](#_Toc59439663)

[**Gateway:** 13](#_Toc59439664)

[**Access Point:** 13](#_Toc59439665)

[5 OSI Layer: 13](#_Toc59439666)

[**Physical Layer:** 14](#_Toc59439667)

[**Data Link Layer:** 14](#_Toc59439668)

[**Network Layer:** 15](#_Toc59439669)

[**Transport Layer:** 15](#_Toc59439670)

[**Session Layer:** 16](#_Toc59439671)

[**Presentation Layer:** 16](#_Toc59439672)

[**Application Layer:** 17](#_Toc59439673)

[6 TCP: 17](#_Toc59439674)

[**Characteristics of TCP protocol:** 17](#_Toc59439675)

[**Connection in TCP** 18](#_Toc59439676)

[7 UDP: 19](#_Toc59439677)

[**Connection in UDP:** 20](#_Toc59439678)

[8 IPv4: 20](#_Toc59439679)

[**IP Subnetting:** 21](#_Toc59439680)

[9 IPv6: 22](#_Toc59439681)

[10 Layer 2 and Layer 3 Protocols: 23](#_Toc59439682)

[**Border Gateway Protocol (BGP) (Layer 3):** 23](#_Toc59439683)

[**Open Shortest Path First (OSPF) Protocol (Layer 2):** 24](#_Toc59439684)

[CISCO PACKET TRACER 25](#_Toc59439685)

[Implementing Simple University Network 25](#_Toc59439686)

[11 Reference: 26](#_Toc59439687)

1. **NETWORKING:**

Q. WHAT IS NETWORK?

A network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams in order to share resources or allow communication is known as network.

also, there are many types of network.

A very common types of networks are:-

1. Local area Network (LAN)

* It is network in which only there are computers of one organization connected within Well-defined area.
* provide the highest speed connections among computers, but sacrifice the ability to span long distances.
* delay across a LAN can be as short as a few tenths of a millisecond or as long as 10 milliseconds
* Mostly these networks are of college campuses.
* Speed = between 1 Gbps and 10 Gbps.

1. Wide Area Network (WAN)

* This is generally for large areas mainly used to connect a large number of LAN’s and MAN’s.
* Uses switched connections to link remote location computers.
* Delays across a WAN can vary from
* a few milliseconds to several tenths of a second.
* Speed = High speed (1000 Mbps) Less speed (150 Mbps).

1. Metropolitan Area Network (MAN):

* The name itself shows it ability to cover up to a hundred kilometers.
* Speed= 5 to 10 Mbps.

1. Personal Area Network (PAN)

* Network which is for personal use
* Can be use between personal devices and for Internet.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network covers an area of 30feet.

## **NETWORK TOPOLOGIES:**

Topology refers to layout of a computer network, there are two types of topology physical and logical topology.

Physical topology is geometrical representation of all nodes in the network.

1. BASED ON LAN TOPOLOGIES
2. MESH
3. STAR
4. BUS
5. RING
6. HYBRID

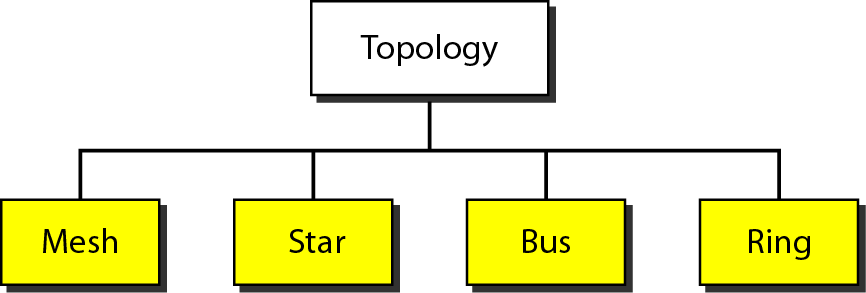


Figure 1.5 Topology

### BUS TOPOLOGY:

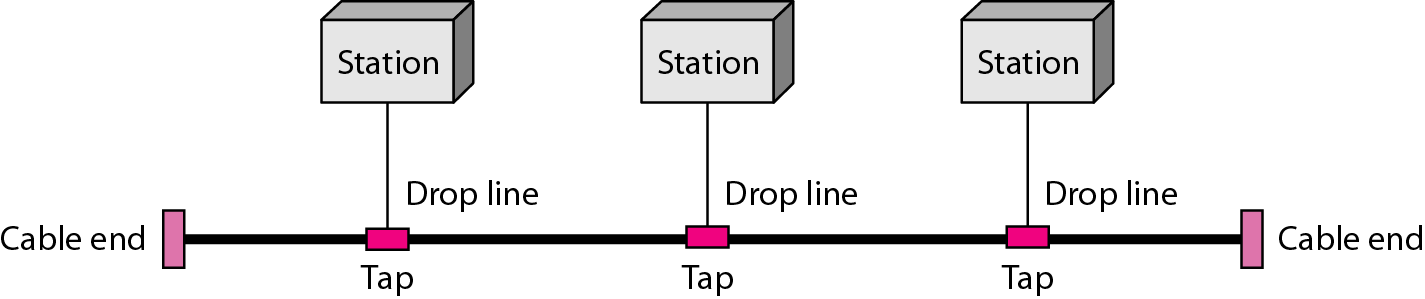


Figure 1.1 Bus Topology

* The bus topology is linear. Data is transmitted from one node to the next through the length of the LAN physical medium.
* The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard network.
* In this One long cable acts as a backbone to link all the devices in a network.
* There is no bi-directional feature in bus topology.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Low cost cable, as hubs are not used installation cost is low. | Extensive cabling |
| Failure in one node doesn’t affect another node | Signal Interference, if two nodes send the message simultaneously, then the signals of both the node collide with each other. |

### MESH TOPOLOGY:

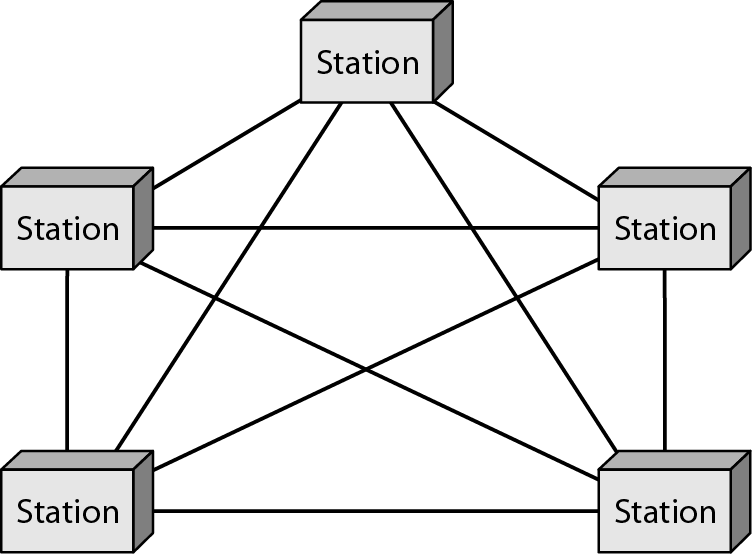


Figure 1.2 Mesh Topology

* In Mesh Topology computers are interconnected with each other through various redundant connections.
* There exist multiple paths from one computer to another computer.
* Number of cables in mesh topology is = (n\*(n-1))/2, where n is the number of nodes.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| This topology is very reliable will not affect the communication between connected nodes. | Costly, as it contains large number of routers and cables. |
| Communication is fast between the nodes. | These topologies are very large and very difficult to maintain and manage. |

### STAR TOPOLOGY:

* Either coaxial or RJ-45 is used depends on type of network card installed in computer.
* Star topologies are often made up of multiple bus and ring topologies.

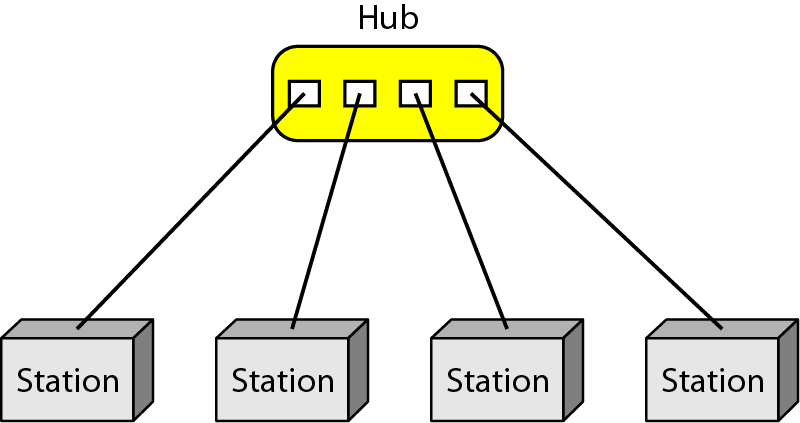


Figure 1.3 Star Topology

* In star topology all the nodes are connected to the hub.
* Coaxial cables or RJ-45 are used to connect the computers.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Easily Expandable, as new ports can be added can be added to the open ports of the hub. | Cable routing becomes difficult when a significant amount of routing is required |
| If one computer on the network fails, the rest of the network continues to function normally. | f the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network. |

### RING TOPOLOGY:

* Ring is similar to bus, except that the end nodes are attached to form a closed loop, and data transmission only flows in one direction.

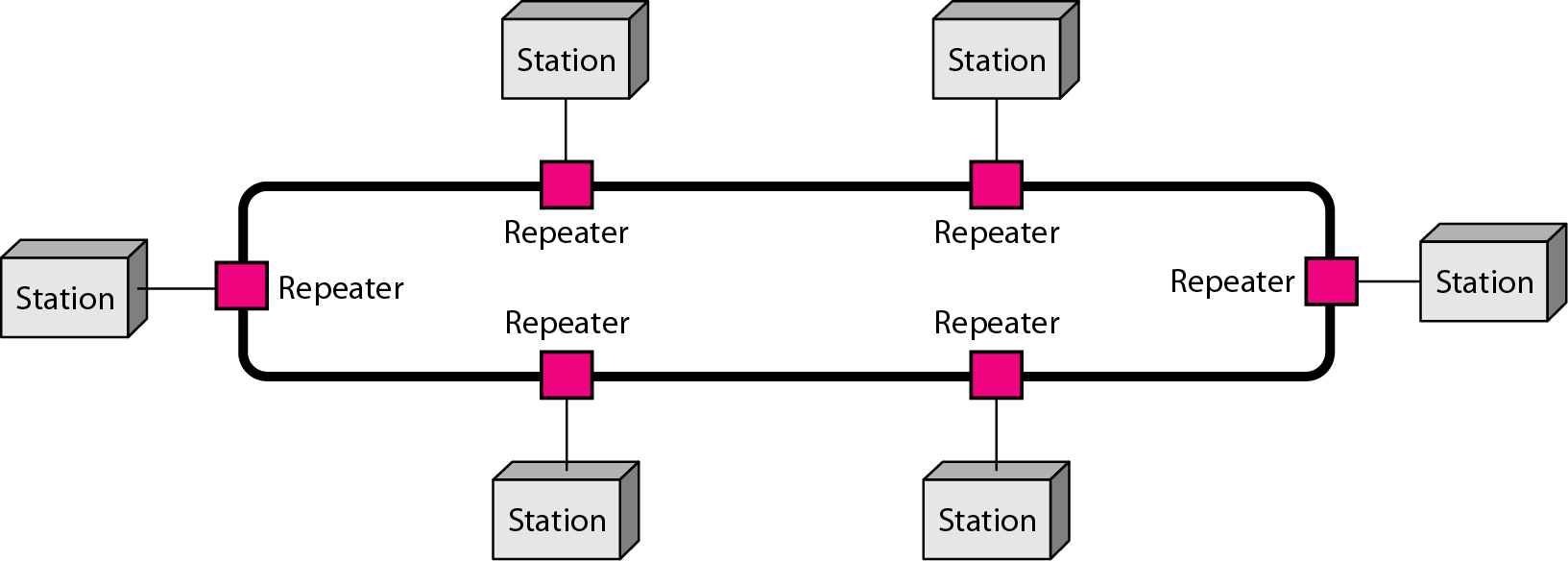


Figure 1.4 Ring Topology

* In Ring Topology data flows in one direction, it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* Access method of the ring topology is token passing

Token passing**:** It is a network access method in which token is passed from one node to another node.

Token**:** It is a frame that circulates around the network.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| This type of topology combines the benefits of different types of topologies in one topology. Can be modified as per requirement. It is extremely flexible and reliable. | Design of a hybrid network is very complex. 2. There is change hardware to connect topology with another topology. |
| Error detecting and troubleshooting is easy. Handles large volume of traffic. | Usually hybrid architectures are usually larger in scales so they require a lot of cables in installation process. |

### HYBRID TOPOLOGY:

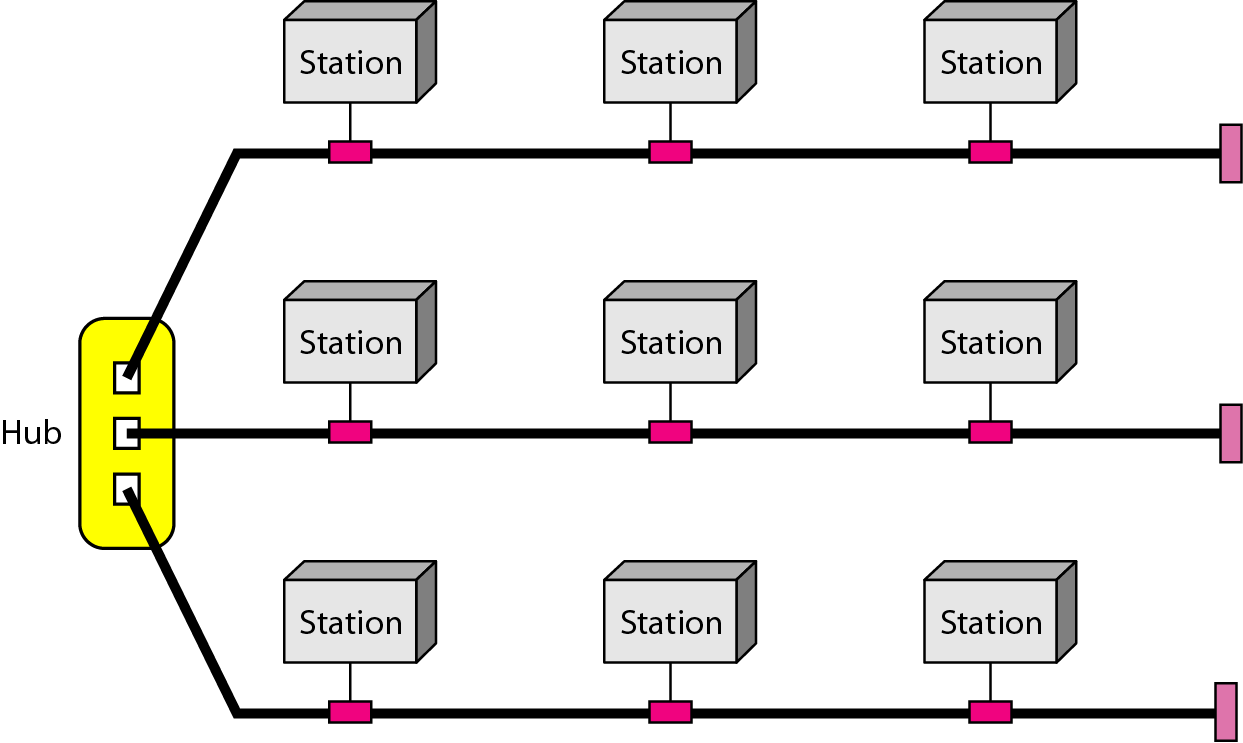


Figure 1.5 hybrid Topology

* It combines the characteristics of bus topology and ring topology.
* Here the computers are connected in hierarchical fashion.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Easily Expandable | Devices required for broadband transmission are very costly. |
| Error detection and error correction are very easy in a tree topology | Tree mainly relies on main cable and the main cable will damage the overall network |

# WIRED NETWORKS:

Wired communication refers to the transmission of the data over wire-based technology, it may include connection of two or more computers, printers, scanners, keypad and devices linked by Ethernet cables.

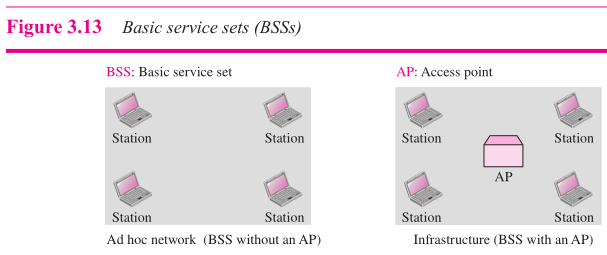
Some of the Ethernet standards are:

* 802.3 – It is a 10BASE5 thick coax, which has data rate of 10Mbps and operates on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) process
* 802.3a – It is a 10BASE2 thin coax, which has data rate of 10Mbps.
* 802.3i – It is a 10BASET twisted pair cable, which has data rate of 10Mbps.
* 802.3u – It is a 100BASET twisted pair cable, which has data rate of 100Mbps.

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| Bandwidth is very high and that interference is very limited through direct connections | Data transmission over this distance may be slow or nonexistent. |
| Easily Expandable | Devices required for broadband transmission are very costly. |
| Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. | It must be rewired every time it is moved. |

# WIRELESS NETWORKING:

Wireless Networking is a network that uses electromagnetic waves traveling through free space to connect stations or devices. It enables data to be shared between two devices without any physical connection between them.

****

Some wireless Networking standards are:

* 802.4- This standard specifies the Token-bus media access control method. It is one of two token passing access methods. IEEE 802.4 is based on a physical bus or tree topology.
* 802.5- This is the second of the token passing access control methods. Token-ring is most commonly used in a network structure following both a logical and physical ring topology. The right to transmit is controlled by a token.
* 802.11n- This standard works on both the 2.4 GHZ and 5 GHZ bands, its net data ranges from 54Mbits/s to 600Mbits/s.

# COMPONENTS:

## **HUB:**

* A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
* A hub has many ports, a computer which wants to be connected to the network is connected to one of these ports, when the data frame arrives it broadcast to every other port connected to the hub, without considering its destination.
* Types of hub are given below.

**ACTIVE HUB:** It checks the data to be sent and decides which packet to send first.

**PASSIVE HUB:** It is capable of determining the bugs and faulty hardware.

**INTELLIGENT HUB:** These hubs have some kinds of management software that help to analyze the problem in the network and resolve them.

## **SWITCH:**

* A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.
* Like hub switch also has many ports, but when the data frame arrives the switch checks the destination address and sends the data to the corresponding device, this supports both unicast and multicast communication.
* A switch works at the data link layer of the OSI model.
* The speed of switch is 10/100 Mbps, 1 Gbps, and 10 Gbps.
* transmission mode is full-duplex.
* It reduces unnecessary traffic and keeps MAC address of devices connected to it. Not used to exchange the data outside the network and cannot read IP addresses

**DIFFERENCE BETWEEN HUB AND SWITCH**

|  |  |
| --- | --- |
| Hub | Switch |
| Operates in physical layer of OSI model | Operates in Data Link layer of OSI model |
| It broadcasts messages | It supports unicast, multicast and broadcast |
| Half Duplex transmission mode | Full Duplex transmission mode |

## **ROUTER:**

* Routers are networking devices that operate in network layer of the OSI model.
* They are responsible for receiving, analyzing, 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.
* uses protocols such as ICMP to communicate between two or more networks.
* Router can be used in both Local Area Networks and Wide Area Networks. In router to transmit data, it uses IP address in IP address mentioned in the destination field of the IP packet.

## **BRIDGE:**

* Bridge is a network device that connects multiple local area networks (LAN) together to form a larger LAN,
* The process of grouping networks is called network bridging. Bridges operate in data link layer of the OSI model.
* There Two types of Bridges:

1. Transparent Bridges
2. Source Routing Bridges

## **GATEWAY:**

* A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
* Gateway operates at level 3 in the network layer of the OSI model, it acts as entry and exit point for a network.
* They are generally more complex than switch or router.

## **ACCESS POINT:**

* Access Point (AP) is 802.11 wireless implementations, it is the interface between wired and wireless network, that all the wireless clients associate to and exchange data with.
* They are hardwired to other devices which are broadband
* Typically they provide wireless access to the internet but some does not they specified for confidential network access.
* Most of the access points have built in routers which let wireless to connect to a network.

# OSI LAYER:

* It is considered as basic structure for networking. It’s based on the concept of splitting of communication system into seven abstract layers each one depends on last one

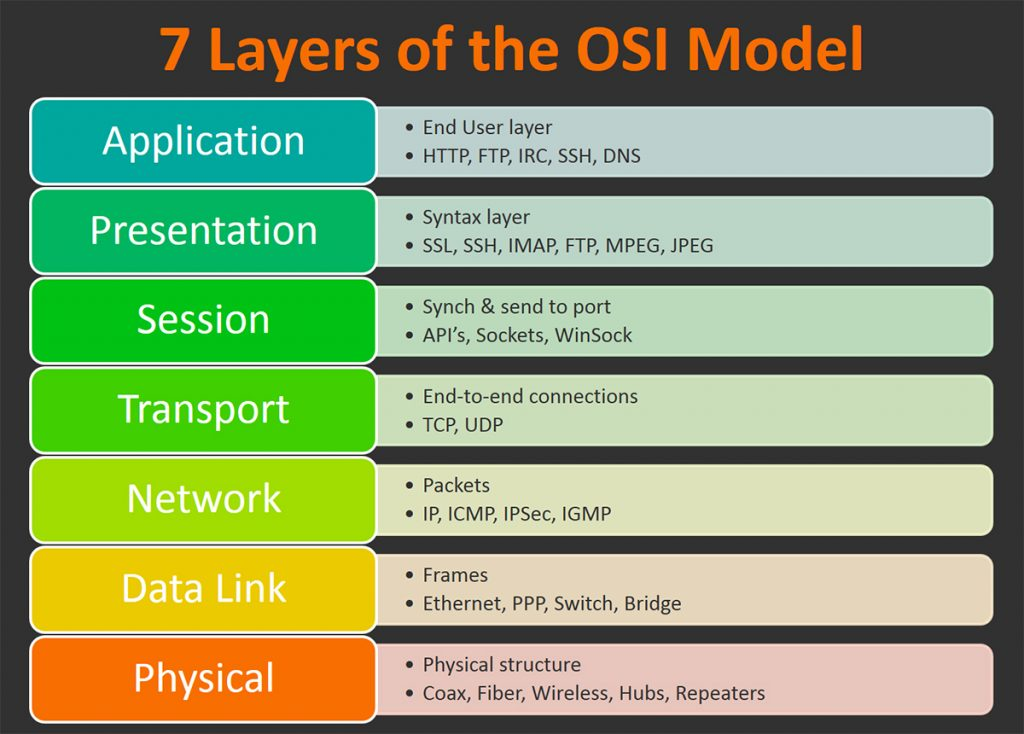


Figure:- OSI Layers

* The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.

## **PHYSICAL LAYER:**

Physical Layer is responsible for movements of individual bits from one node to the next.

* Physical characteristics of interfaces & medium, type of transmission medium.
* Representation of bits.
* Data rate.
* Synchronization of bits.
* Line configuration.

## **DATA LINK LAYER:**

Data link layer is responsible for moving frames from one node to the next**.**

* Framing.
* Physical addressing.
* Flow control.
* Error control.
* Access control.

## **NETWORK LAYER:**

Network layer is responsible for the delivery of individual packets from the source host to the destination host.

## **s LAYER:**

Transport layer is responsible for the delivery of a message from one process to another.

* service-point addressing.
* Segmentation and reassembly.
* Connection control.
* Flow control.
* Error control.

## **SESSION LAYER:**

The session layer is responsible for dialog control and synchronization.

* Dialog control.
* Synchronization

## **PRESENTATION LAYER:**

The Presentation layer is responsible for translation, compression, and encryption**.**

* + Concerned with syntax and semantics of the information.
  + Translation.
  + Encryption.
  + Compression.

## **APPLICATION LAYER:**

The Application layer is responsible for providing services to the user.

* + Network virtual terminal.
  + File transfer, access, and management.
  + Mail services.
  + Directory Services

# TCP:

TCP is a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network. It is the most common protocol in networks that use the Internet Protocol (IP), together they are referred as TCP/IP.

TCP takes the message from application/server and divides them into packets, which can then be forwarded by the devices in the network – switches, routers, security gateways – to the destination. TCP numbers each packet and reassembles them prior to handing them off to the application/server recipient. As it connection oriented it ensures that the connection is mentioned between the sender and reviver till the message is complete.

## **CHARACTERISTICS OF TCP PROTOCOL:**

* TCP provides error-checking and recovery mechanism
* TCP provides flow control and quality of service.
* TCP provides end-to-end communication.
* TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

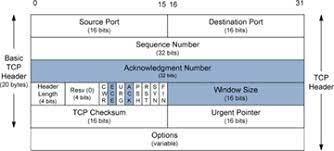


Figure TCP Datagram

**Source Port Address:**

It is a 16-bit field that holds the address of the sender application.

**Destination Port Address:**

It is a 16-bit field that holds the address of the receiver application.

**Sequence Number:**

It is 32-bit field that holds the sequence number, it is used to reassemble the message at the receiving end if the segments are received out of order.

**Acknowledgement Number-**

It is 32-bit field that holds the acknowledgement number, it acknowledges the pervious bytes being received successfully.

**Header Length (HLEN):**

It is 4-bit field that indicates the length of the TCP header.

**Control flags:**

It contains 6 1-bit control bits, that control the connection termination, establishment, flow control, mode of transfer, connection abortion etc.

**Window size:**

Tells the window size of the sending TCP bytes.

**Checksum:**

It contains the checksum for error control.

**Urgent pointer:**

This point to data that is urgently required to reach the processor.

## **CONNECTION IN TCP**

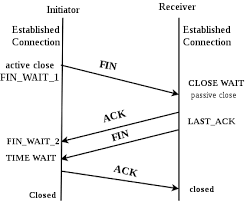


Figure:- Connections in TCP

* TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.
* TCP/IP suite of conventions is classified as stateless, which suggests each client request is considered new since it is irrelevant to past requests. Being stateless liberates up network paths so they can be utilized continuously.
* TCP/IP model differs from the seven-layer Open System Interconnection (OSI) model designed after it.

# UDP:

* It is connectionless and unreliable in Transport Layer protocol. It is mainly used in computer gaming, voice or video communication and live communication, it doesn’t provide error checking and saves the Bandwidth.
* It is more efficient in terms of both latency and bandwidth.
* It is located between application layer and IP layer, and serves as intermediate function between both of them.
* There is no error checking in UDP. This helps in saving bandwidth.

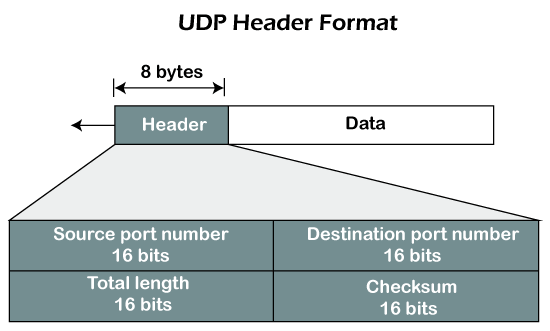


Figure 7.1 UDP Header Format

**Source Port:**

It is the 16-bit field used to identify the port number of the source.

**Destination Port:**

It is the 16-bit field used to identify the port number of the destination.

**Length:**

It is the 16-bit field that contains the length of the UDP including the header.

**Checksum:**

It is the 16-bit field that contains the one’s compliment of the UDP header.

## **CONNECTION IN UDP:**

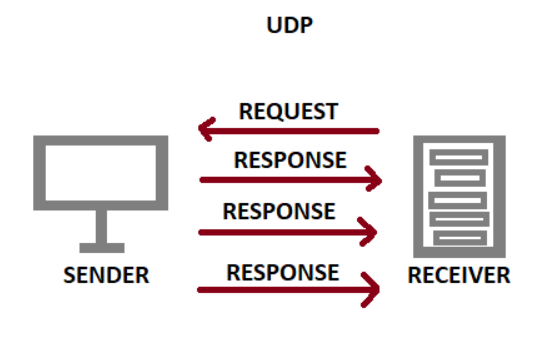


Figure Connections in UDP

* UDP doesn’t follow three-way handshake before transmission.
* In UDP there is no end to end connection.
* First the receiver sends request to the sender to send the data.
* When the sender receives the starts to send the data.
* Receiver doesn’t acknowledge to the data received.

1. **L2 PROTOCOLS:**
2. **L3 PROTOCOLS:-**

OSPF PROTOCOL:

* The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.
* The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors.
* The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm.
* Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.
* The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet quality of service requirements.
* The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.
* Each OSPF router distributes information about its local state (usable interfaces and reachable neighbors, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. Each router uses the received messages to build up an identical database that describes the topology of the AS.

# IPv4:

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a Device d (for example, a computer or a router) to the Internet. The address space of IPv4 is 232 or 4,294,967,296.

**CHARACTERISTICS OF IPV4:**

* IPv4 could be a numeric address, and its bits are separated by a dot.
* It has unicast, broadcast, and multicast style of addresses.
* The numbers of header fields are twelve and the length of the header filed is twenty.
* IPv4 uses the Post Address Resolution Protocol to map to mac address.

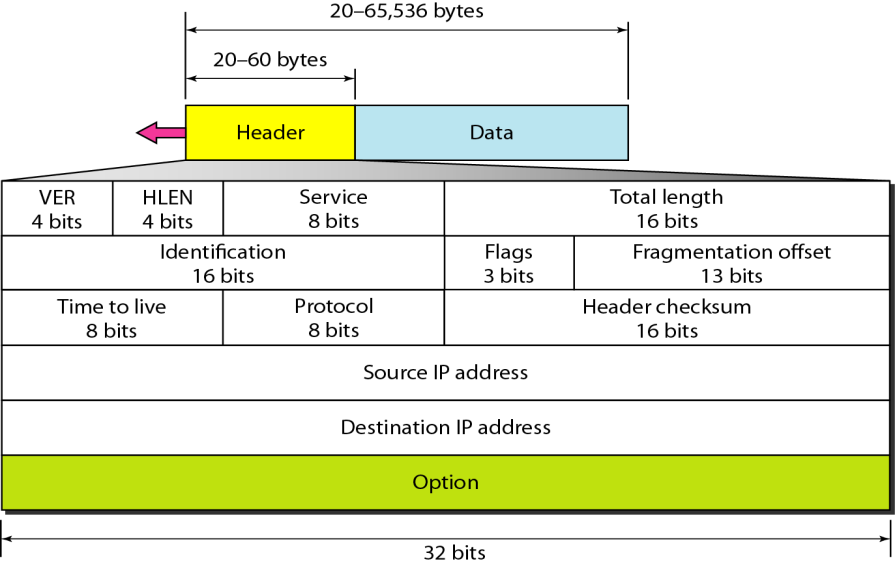


Figure 8.1 IPv4 Header Format

**Classes in IPv4:**

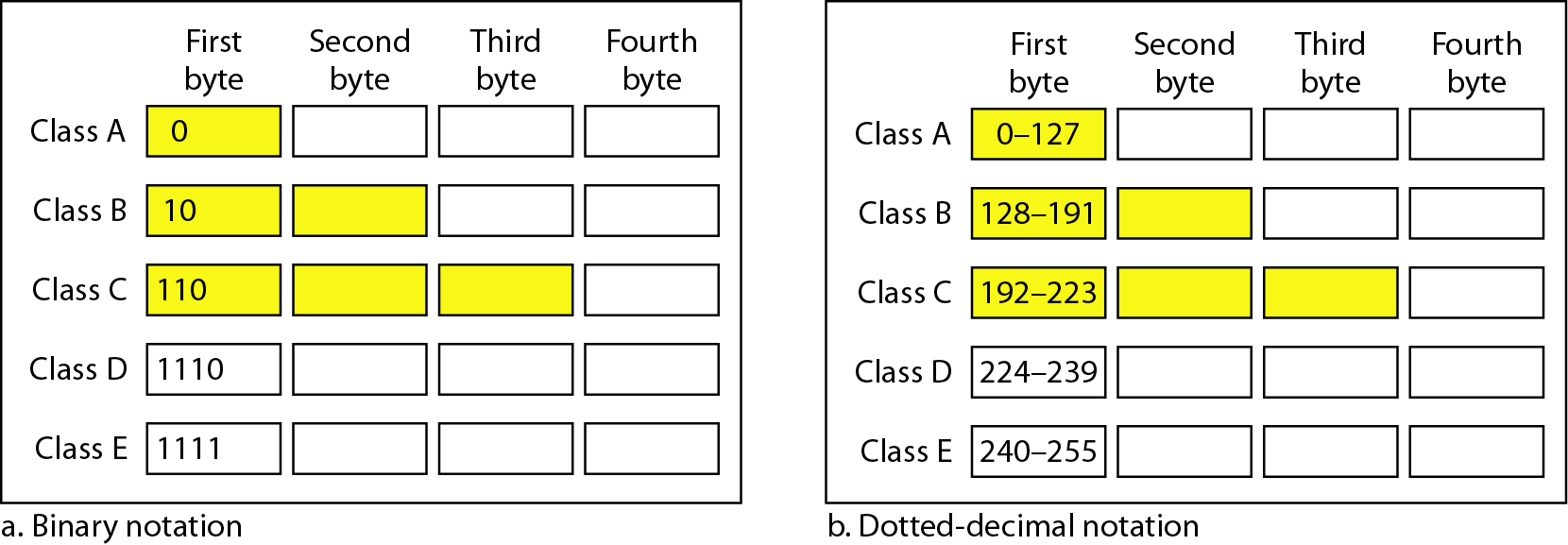
****

Figure 8.2 Classes in IPv4

## **IP SUBNETTING:**

Design for 6 Networks in Class C using IP Subnetting

* Class C address – 212.212.212.1/24
* Finding ‘n’ value for 6 networks => 2 ^ n = 8; n= 3 for 6 networks.
* CIDR for the given example is => 24 + 3 = 27.
* Class C address after CIDR updating is – 212.212.212.1/27
* Subnet mask is 255.255.255.224
* Number of addresses available are => 2 ^ 5 = 32.
* Out of 2 first address is Network Id and last address is Broadcast address.
* Number of Host Id’s available is = 32-2 = 30 per network.
* Host Id’s for respective networks

1. Network 1 = 212.212.212.0 – 212.212.212.31
2. Network 2 = 212.212.212.32 – 212.212.212.63
3. Network 3 = 212.212.212.64 – 212.212.212.95
4. Network 4 = 212.212.212.96 – 212.212.212.127
5. Network 5 = 212.212.212.128 – 212.212.212.159
6. Network 6 = 212.212.212.160 – 212.212.212.191

# IPv6:

IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4.IPv6 use Colon-Hex representation. There are 8 groups and each group represent 2 Bytes.

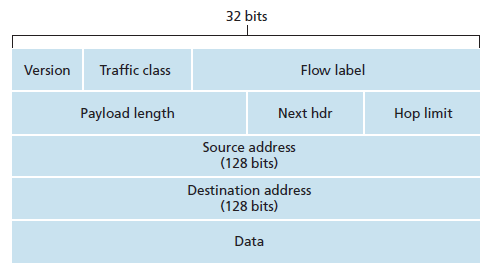


Figure 9.1 IPv6 Datagram

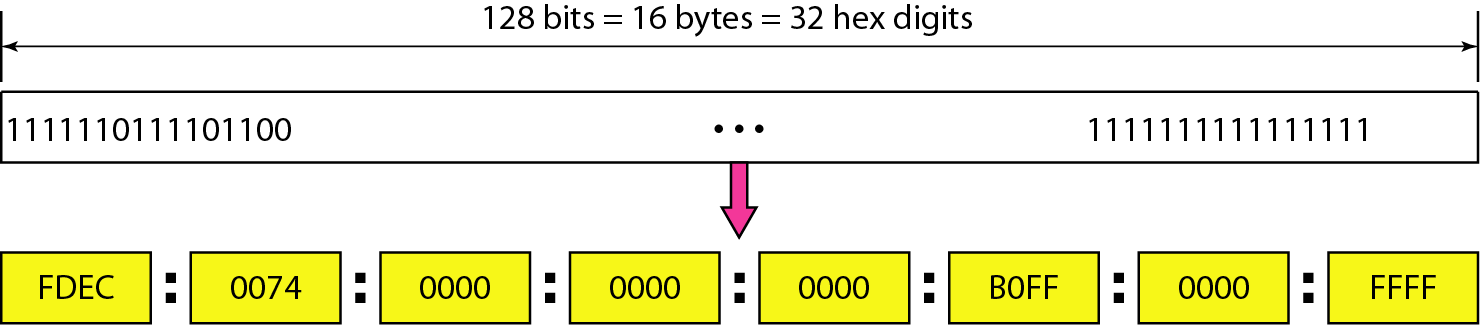


Figure 9.2 IPv6 Address Format

IPv6 can be abbreviated, leading zeros in IPv6 can usually be left out, and this would shorten the address.

**Example:**

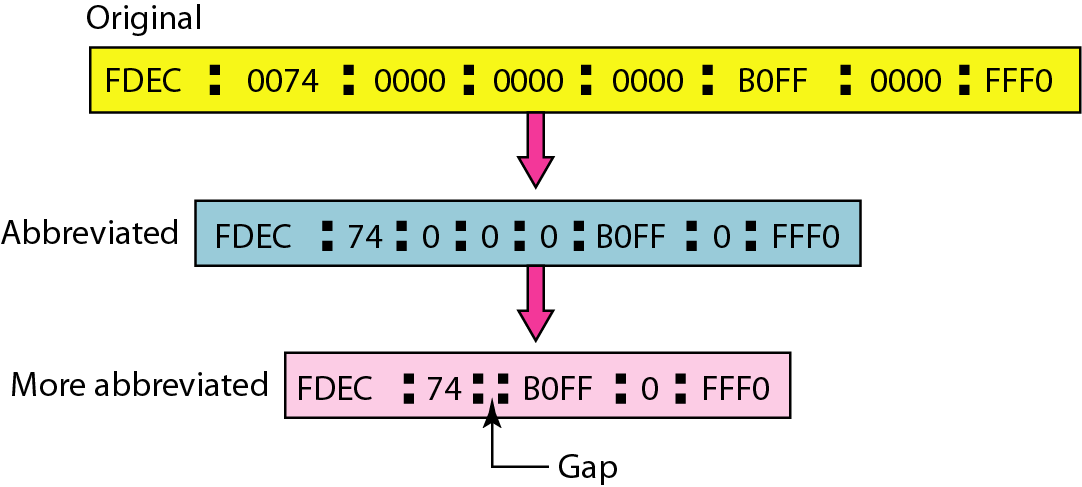


Figure 9.3 Abbreviation of IPv6 address

# LAYER 2 AND LAYER 3 PROTOCOLS:

## **BORDER GATEWAY PROTOCOL (BGP) (LAYER 3):**

BGP is a gateway protocol designed to exchange routing information between AS (autonomous systems). BGP’s main function is to exchange network information with other BGP systems. It constructs an autonomous systems graph based on the information exchanged between BGP routers.

**Characteristics of Border Gateway Protocol (BGP):**

* Bandwidth is conserved in BGP.
* It supports TCP
* It also supports security.
* It supports Next-Hop Paradigm.
* It includes path information, along with present and next destination address pair.
* It provides communication between two autonomous systems.

## **OPEN SHORTEST PATH FIRST (OSPF) PROTOCOL (LAYER 2):**

OSPF is a link state protocol that is used to find the shortest path between the destination and source router using its own Shortest Path First. OSPF uses multicast address for normal communication.

**OSPF Terms-**

* **Router priority:** It is an 8-bit value assigned to a router operating OSPF.
* **Router I’d:** It is highest active IP address present on the router.
* **Designated Router (DR):** It distributes the LSAs to all the other routers.
* **Backup Designated Router (BDR):** It is backup to DR in a broadcast network, when DR goes down BDR takes over as DR and performs its functions.

ADDRESS RESOLUTION PROTOCOL(ARP):

* Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.
* There are four types of ARP.

1. Proxy ARP
2. Gratuitous ARP
3. Reverse ARP
4. Inverse Arp

* The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address.
* The address resolution procedure is completed when the client receives a response from the server containing the required address.
* The Ethernet address is a link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the link addresses of individual nodes which are to be used.
* The address resolution protocol (ARP) is therefore used to translate between the two types of address. The ARP client and server processes operate on all computers using IP over Ethernet. The processes are normally implemented as part of the software driver that drives the network interface card.
* To reduce the number of address resolution requests, a client normally caches resolved addresses for a (short) period. The ARP cache is of a finite size and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The ARP cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers which are not currently running.
* If a host changes the MAC address it is using, this can be detected by other hosts when the cache entry is deleted, and a fresh ARP message is sent to establish the new association. The use of gratuitous ARP (e.g. triggered when the new NIC interface is enabled with an IP address) provides a more rapid update of this information.
* The use of ARP when a computer tries to contact a remote computer on the same LAN (known as "sysa") using the "ping" program. It is assumed that no previous IP datagrams have been received form this computer, and therefore ARP must first be used to identify the MAC address of the remote computer.

# 

# CISCO PACKET TRACER

# 

# Implementing Simple University Network

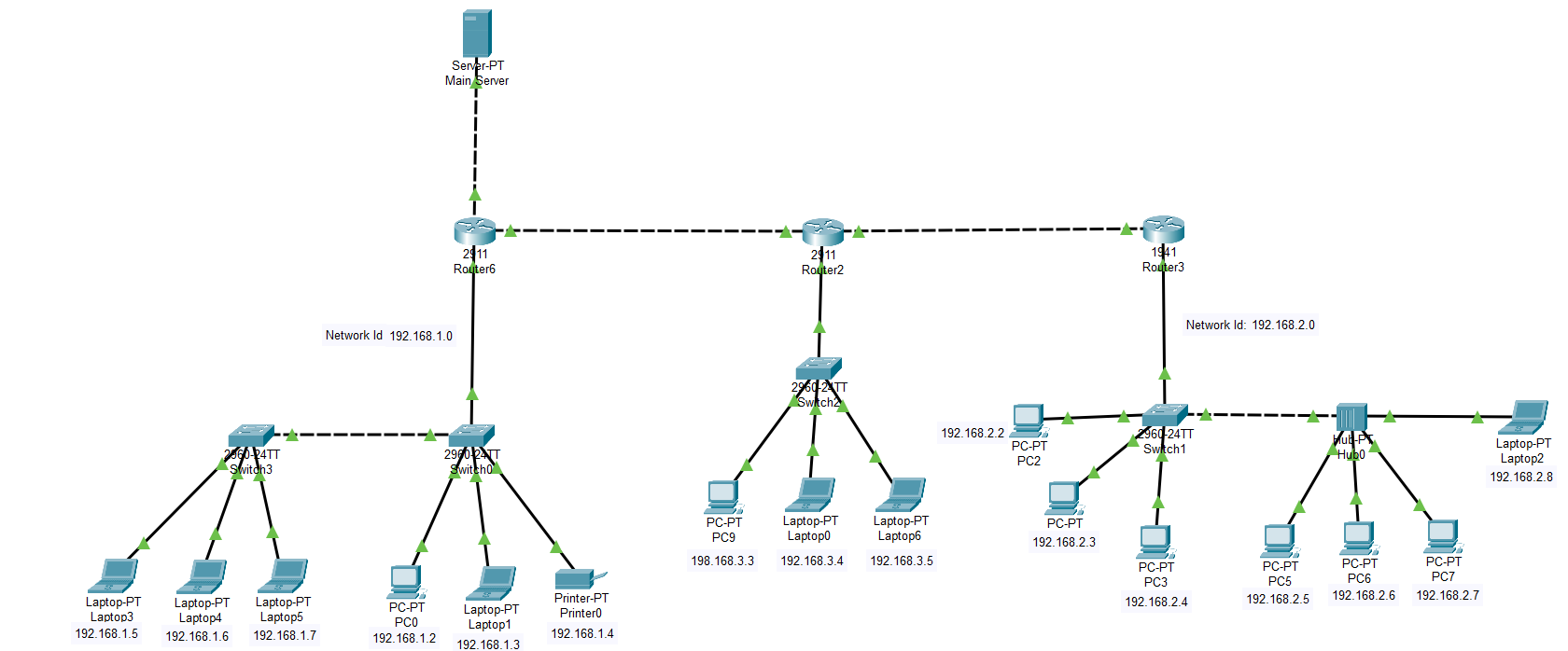


Figure :- Simple University Network

In the above diagram Simple University Network is implemented using one main server, three routers, 4 switch, one hub, one printer and 15 end devices.

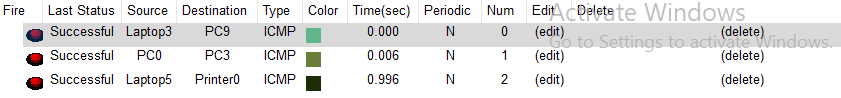


Figure 11.2 Successful Packet Transfer

In the above diagram it shows the successful packet transfer between two different networks of different classes.

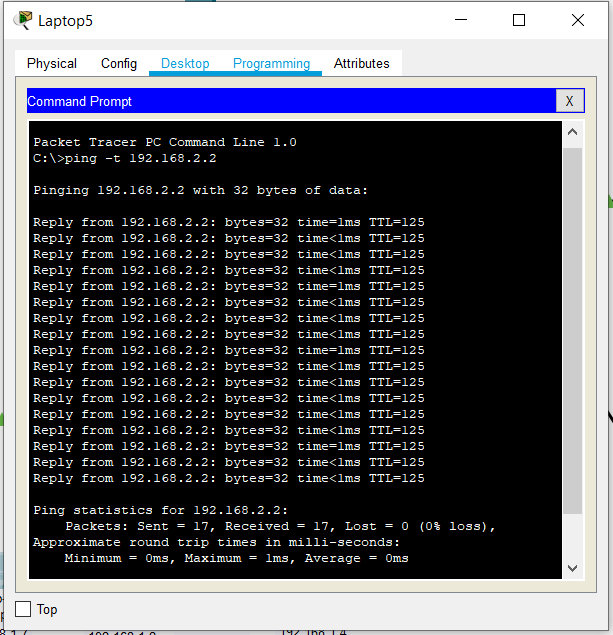


Figure 11.3 Ping between different networks

# Reference:

[1] <https://fcit.usf.edu/network/chap1/chap1.htm>

[2] <https://www.javatpoint.com/types-of-computer-network>

[3] <https://icograms.com/usage-network-diagram.php>

[4] <https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network>

[5] <https://en.wikipedia.org/wiki/IEEE_802.11#802.11n>

[6] <https://networkencyclopedia.com/wireless-networking/>

[7] <https://www.geeksforgeeks.org/what-is-ipv4/>

[8] <https://www.geeksforgeeks.org/internet-protocol-version-6-ipv6/>

[9] <https://www.geeksforgeeks.org/user-datagram-protocol-udp/>

[10] <https://www.imperva.com/blog/bgp-routing-explained/>