GENESIS – Networking Learning Report

LTTS
GLOBAL
ENGINEERING
ACADEMY

L&T Technology Services

Details

Ver. Rel. No.	Release Date	Prepared. By	Reviewed By	To be Approved	Remarks/Revision Details
1.0	16/12/2020	Lakshmi N		Srinivas K	
1.1	17/12/2020	Lakshmi N		Srinivas K	
1.2	18/12/2020	Lakshmi N		Srinivas K	
1.3	19/12/2020	Lakshmi N		Srinivas K	

Table of Contents

List of Figures

1 NETWORK

- A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

1.1 TYPES AND TOPOLOGIES:

- Network topology describes the layout or appearance of network devices such as computers, cables and other components.
- Components within a data communication network are interconnected both physically and logically.
- The physical topology describes the way in which a network physically laid out and logical topology describes how data flow through the network.

1.1.1 BUS TOPOLOGY:

- Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. Bi-directional feature is not available in bus topology.
- When the computer sends a signal to the cable, all the computers receive the information but the computer whose address matches with the signal accepts the data.

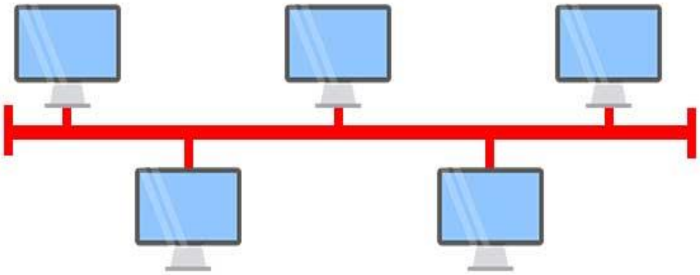


Figure 1: Bus Topology

- **Advantages:**
  - The bus topology is easy to understand and install.
  - The cabling cost is low.
  - The bus topology is easy to expand.

- **Disadvantages:**
  - Only one computer can transmit data at one time and others have to wait till their turn comes.
  - If the cable breaks or loose connection then it can bring down the whole network.
  - The speed of bus topology is slow because only one computer can send a message at a time.

1.1.2 MESH TOPOLOGY:

- In mesh topology, every device is connected to another device via separate channels. These channels are known as links.

- If N no: of devices are connected to each other, then total number of ports required by each device is N-1 and total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2

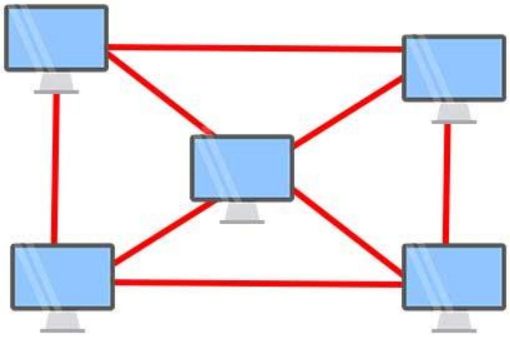


Figure 2: Mesh Topology

- **Advantages:**
  - It provides security and privacy.
  - The failure of a single computer does not bring down the whole network.
- **Disadvantages:**
  - Cabling cost is more.
  - The hardware cost to connect each device is expensive

1.1.3 STAR TOPOLOGY:

- In a star topology, all the devices are connected to a central device known as hub. This device will then control all the data traffic flow within the entire network.

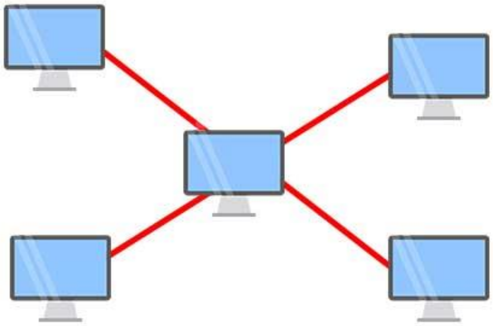


Figure 3: Star Topology

- **Advantages:**
    - Relatively easy to set up and maintain – Just connect or disconnect devices from the central hub.
    - A broken node will not affect the rest of the network.
- **Disadvantages**
    - The network performance and the number of connections are limited by the central device.
    - A good central hub or router can be very costly.
    - Single point of failure. If the central node goes down, the entire network collapses.

1.1.4 RING TOPOLOGY:

- A ring topology can be best described as devices connected in a closed loop daisy chain.
- Data transmission in a ring network is usually unidirectional.

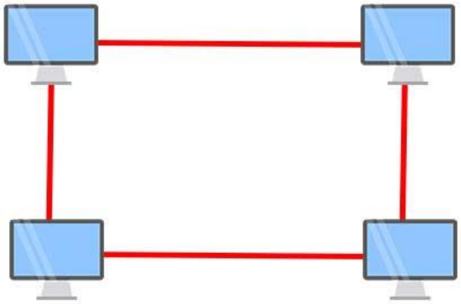


Figure 4: Ring Topology

- **Advantages:**
  - Ring networks can span over a longer physical distance, as the nodes will regenerate the message as it is being passed across.
  - Adding more nodes will not slow down the entire network, as only nodes that have the token can transmit data.
  - Relatively affordable and easy to build or expand a ring network, as it is essentially just putting the devices into a closed daisy chain.
- **Disadvantages:**
  - Depending on how the ring network is configured, a single break in the network can technically still function normally. But with 2 broken nodes, the ring network will essentially collapse into 2 separate halves.
  - It is an absolute pain to add or remove a node, as it will affect the rest of the network.

1.1.5 HYBRID TOPOLOGY:

- A hybrid network is simply one that adopts two or more different topologies.

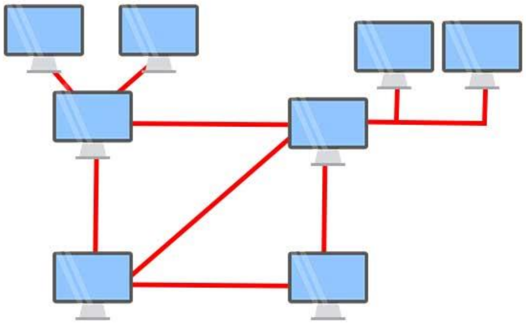


Figure 5: Hybrid Topology

- **Advantages:**
  - Flexible design.
  - Scalable. Expand as the organization needs, and shrink if needed.
- **Disadvantages:**
  - Complex in design. The network engineer has to know various topologies and network gimmicks.
  - May not be the most cost-effective, as it may involve the use of many different networking devices.

1.1.6 TREE TOPOLOGY:

- In a tree topology, there is “top level node” followed by several “sub-level nodes” and “sub-sub-level nodes”, effectively forming a hierarchy.

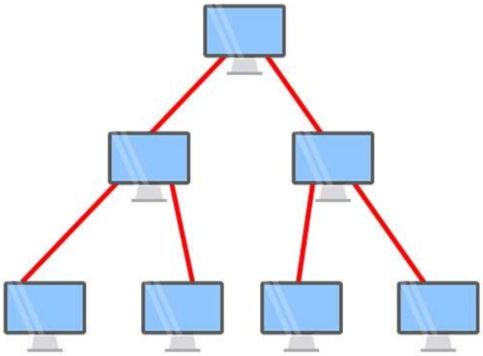


Figure 6: Tree Topology

- **Advantages:**
  - Good for large networks that are divided into groups.
  - Easier to manage as the network is divided into segments.
  - Quite robust when configured properly. If a sub-network breaks, it will not affect the rest of the network.
- **Disadvantages:**
  - Costly to build, as it involves a lot of network equipment and cables.
  - Depending on how the tree network is built again – If the “top level node” or central hub goes down, the entire network can be crippled.

2 WIRED AND WIRELESS NETWORKS

2.1 PAN

- A personal area network (PAN) is a computer network organized around an individual for personal use only. They typically involve a computer, phone, printer, tablet, or some other device like a PDA.
- It typically ranges within 10m and WLAN ranges from10m to 100m.
- PAN supports 250 kbps in zigbee, from kbps to 24 Mbps in Bluetooth case.

2.2 LAN

- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home.
- A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
- It ranges from 10 to 100m and more in case of wireless LAN.
- LAN supports 10, 100 and 1000 Mbps.
- Wired LAN devices are connected using Ethernet cables.

2.3 WLAN

- WLAN is a local area network (LAN) that doesn’t rely on wired ethernet connections.
- A wireless local area network (WLAN) is a wireless distribution method for two or more devices.
- WLAN supports 54 Mbps or above.
- WLANs use high-frequency radio waves and often include an access point to the Internet.
- A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

2.4 WAN

- A wide area network spans a large geographic area such as a city, state, or country.
- It can be private to connect parts of a business, or it can be public to connect smaller networks.
- It ranges more than 1,00,000 kms.
- It runs on bandwidths of 20 Mbps, 50 Mbps, or 100 Mbps.

2.5 MAN

- A metropolitan area network (MAN) is similar to a local area network (LAN) but spans an entire city or campus, or some other municipal or organizational territory.
- MANs are formed by connecting multiple LANs.
- It serves geographical area of 5-50kms in range.
- Thus, MANs are larger than LANs, but smaller than wide area networks (WAN) that cover dispersed geographical areas, sometimes directly connecting users around the world.
- It supports a speed of 5-10 Mbps.

2.6 WIFI

- Wi-Fi is a wireless networking protocol that devices use to communicate without direct cable connections. It is an industry term that represents a type of wireless local area network (LAN) protocol based on the 802.11 IEEE network standard.
- The 802.11a will transmit data at a frequency level of 5GHz – transmits a maximum of 54Mbps.
- The 802.11b will transmit data at a frequency level of 2.4GHz – transmits a maximum of 11 Mbps.
- The 802.11g will transmit data at 2.4GHz – transmits a maximum of 54 Mbps.
- The main requirement for Wi-Fi is a device that receives and transmits a wireless signal, usually a router, but sometimes a phone or computer.

2.7 WIMAX

- Worldwide Interoperability for Microwave Access is a technology standard for long-range wireless networking for both mobile and fixed connections.
- A single WiMAX tower can provide coverage to a very large areas big as 3,000 square miles i.e., 8,000 square km.
- WiMAX should be able to handle up to 70 megabits per second.

3 COMPONENTS

3.1 ROUTER

- Routers connect computers and other devices to the Internet. A router acts as a dispatcher, choosing the best route for your information to travel.
- The IP address assigned to the WAN or internet connection is a public IP address. The IP address assigned to the local network connection is a private IP address. The private IP address assigned to a router is usually the default gateway for the various devices on the network.
- A router operates on the Network layer (layer 3) of the OSI model and uses routing tables to understand where traffic is coming from and where it should go.
- A router will typically include a 4 to 8 port Ethernet switch (or hub) and a Network Address Translator (NAT). In addition, they usually include a Dynamic Host Configuration Protocol (DHCP) server, Domain Name Service (DNS) proxy server and a hardware firewall to protect the LAN from malicious intrusion from the Internet.
- All routers have a WAN Port that connects to a DSL or cable modem for broadband Internet service and the integrated switch allows users to easily create a LAN. This allows all the PCs on the LAN to have access to the Internet and Windows file and printer sharing services.

3.2 SWITCH

- In networks the switch is the device that filters and forwards packets between LAN segments.
- Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol.
- LANs that use switches to join segments are called switched LANs or, for Ethernet networks, switched Ethernet LANs.

3.3 HUB

- A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN.
- The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
- In a hub, a frame is broadcasted to every one of its ports.
- The hub has no way of distinguishing which port a frame should be sent to.
- Passing it along to every port ensures that it will reach its intended destination.
- This place a lot of traffic on the network and can lead to poor network response times.

3.4 BRIDGE

- A bridge is a network device that connects multiple LANs (Local Area Networks) together to form a larger LAN. The process of aggregating networks is called network bridging.
- A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
    - If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
    - If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

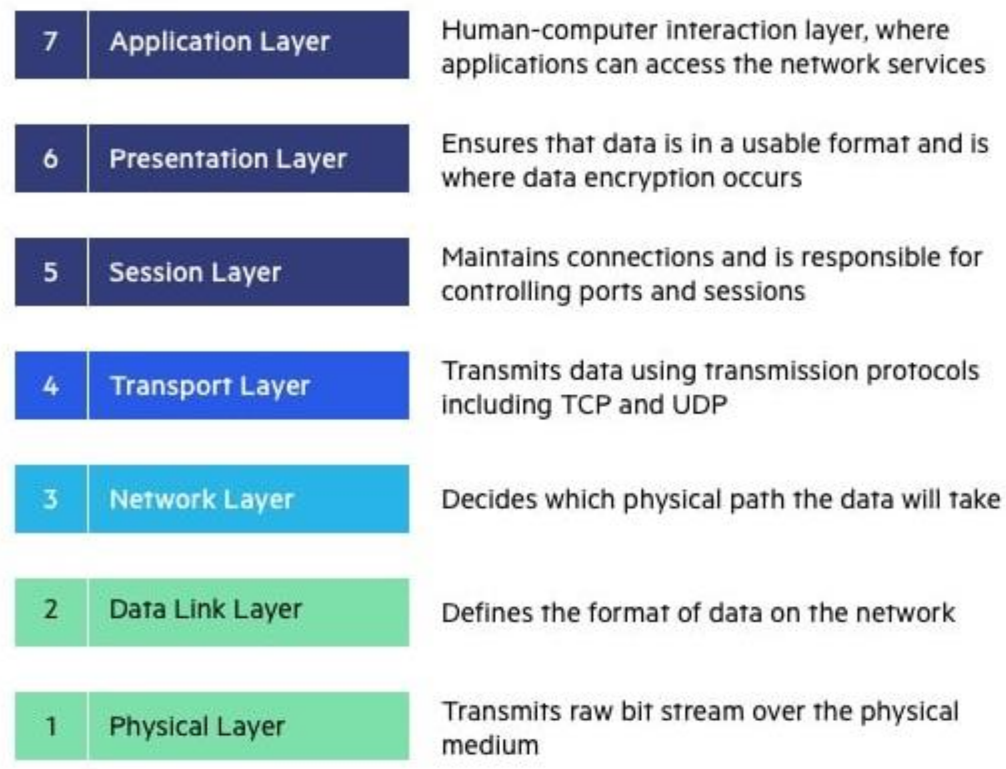
3.5 GATEWAY

- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

3.6 ACCESS POINTS

- An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.
- An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

4 OSI MODEL

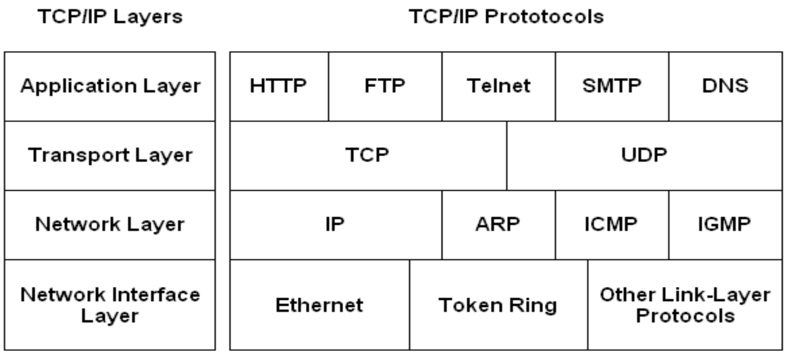


7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Figure 7: OSI Model

5 TCP PROTOCOL

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



TCP/IP Layers	TCP/IP Prototocols				
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		

Figure 8: TCP Protocol

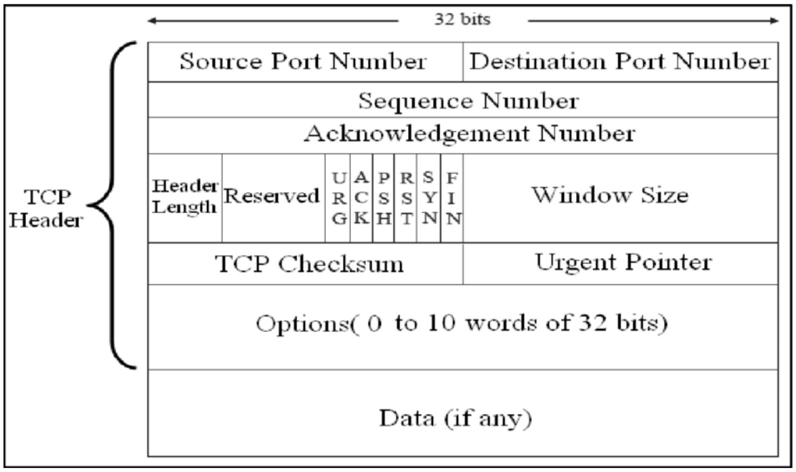


Figure 9: TCP Header

6 UDP PROTOCOL

- The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network.
- The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. Hence it enables a faster transmission.
- It provides an unreliable connection delivery service. It does not provide any services of IP except that it provides process-to-process communication.
- The UDP message can be lost, delayed, duplicated, or can be out of order.

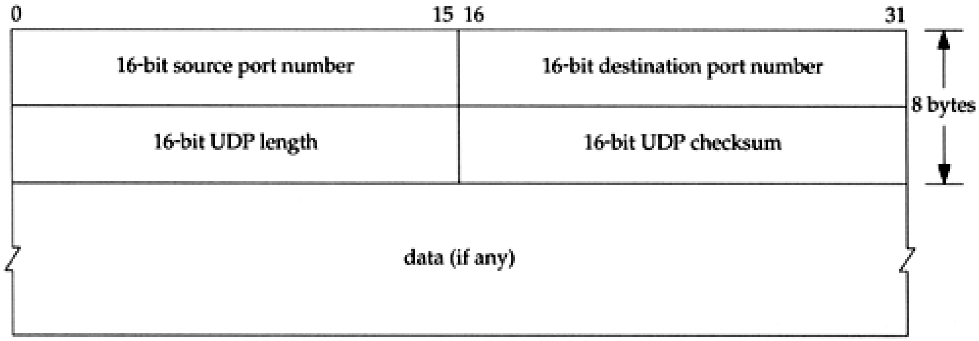


Figure 10: UDP Header

7 IP PROTOCOL

- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets.
- IP information is attached to each packet, and this information helps routers to send packets to the right place.
- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

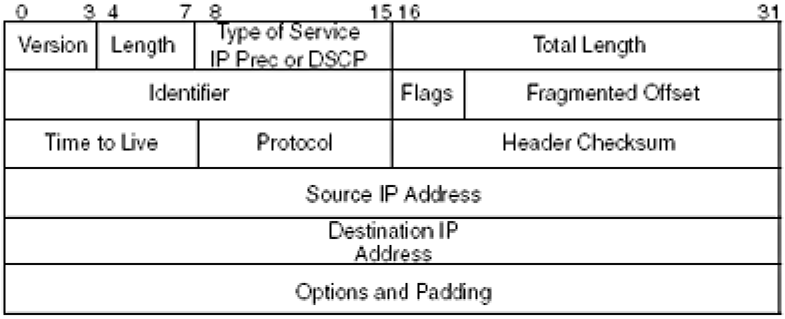


Figure 11: IP Header

8 L2 PROTOCOLS

8.1 ARP

- ARP stands for Address Resolution Protocol.
- ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address.
- The host or the router sends an ARP query packet - query is broadcast over the network
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The response packet contains the recipient's IP and physical addresses
- An ARP packet is encapsulated directly into a data link frame.
- The type field indicates that the data carried by the frame are an ARP packet.

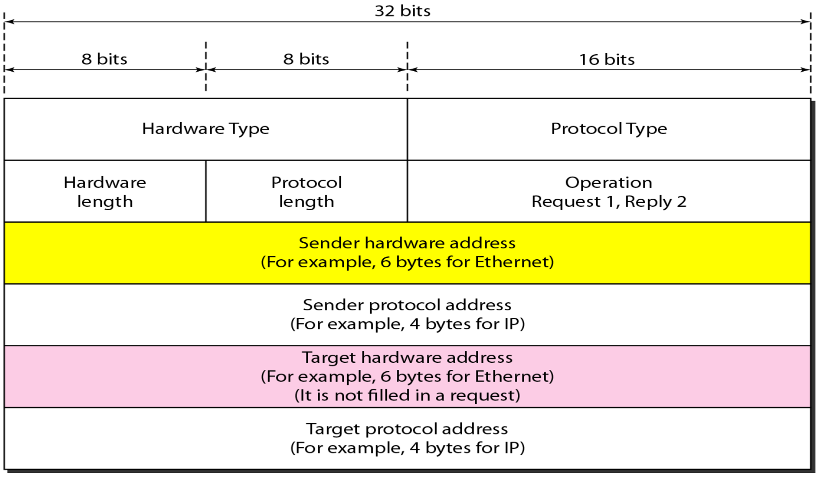

32 bits
8 bits
8 bits
16 bits
Hardware Type
Protocol Type
Hardware length
Protocol length
Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)
Sender protocol address (For example, 4 bytes for IP)
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)
Target protocol address (For example, 4 bytes for IP)

Figure 12: ARP Packet Format

8.2 RARP

- RARP stands for Reverse Address Resolution Protocol.
- It is used when a host knows its physical address, but needs to know its logical address – no enough IP addresses to assign to each station it needs to assign IP addresses on demand.
- It uses the physical address to get the logical address by using the RARP protocol.
- A RARP request is created and broadcast on the local network.
- Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

8.3 DHCP

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- DHCP provides static and dynamic address allocation that can be manual or automatic.
- A DHCP server has a database that statically binds physical addresses to IP addresses known as static allocation.
- DHCP has a second database with a pool of available IP addresses known as dynamic allocation.
- When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

8.4 ICMP

- The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.
- ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.
- ICMP messages are divided into two broad categories: error-reporting messages and query messages.
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages help a host or a network manager get specific information from a router or another host.

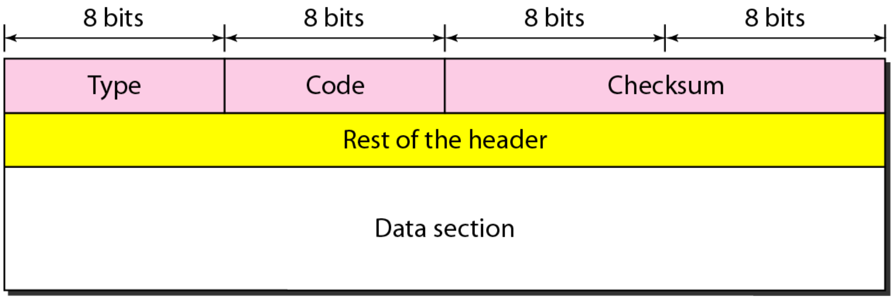


Figure 13: ICMP Message Format

9 L3 PROTOCOLS

9.1 BGP

- Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISPs.
- The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- In BGP protocol, the path between source and destination (actually list of autonomous systems) is represented as a list of attributes. Each attribute gives some information about the path.
- To create a reliable environment, BGP uses the services of TCP.

9.2 EIGRP

- Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer-3 devices to deliver the packet.
- EIGRP works on network layer protocol of OSI model and uses the protocol number 88.
- It uses some messages to communicate with the neighbor devices that operates EIGRP. These are :-
    - Hello message
    - NULL update
    - Full Update
    - Partial update
    - Query message
    - Reply message
    - Acknowledgement message

9.3 RIP PROTOCOL

- Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.
- The metric used by RIP is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a **hop count**.

- Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
- In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen.
- It broadcasts the routing updates to the entire network that creates a lot of traffic.

9.4 OSPF

- Open shortest path first (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm.
- OSPF divides an autonomous system into areas which is a collection of networks, hosts, and routers all contained within an autonomous system.
- The OSPF protocol assign a cost, called the metric, to each route. The metric can be based on a type of service like minimum delay, maximum throughput, and so on.
- In OSPF terminology, a connection is called a link.
- OSPF is the first widely deployed routing protocol. It can converge with a network in a few seconds and it is one of the protocols that can provide loop-free paths.

10 IPv4

- IP stands for Internet Protocol and v4 stands for version 4.
- IP version four addresses are 32-bit integers which will be expressed in hexadecimal notation.
- **Parts of IPv4:**
  - Network part:
    The network part indicates the distinctive variety that's appointed to the network. The network part conjointly identifies the category of the network that's assigned.
  - Host Part:
    The host part uniquely identifies the machine on your network. This a part of the IPv4 address is assigned to every host. For each host on the network, the network part is the same, however, the host half must vary.
  - Subnet number:
    Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

- **Characteristics of IPv4:**

  - IPv4 uses 32-bit addressing which allows a total of 4,294,967,296 (2^32) addresses.
  - Some addresses are reserved for public and private networks.
  - An IP address consists of four octets which are separated by a period, which is also known as *dotted-decimal notation.*
  - In the total no: of host IP addresses, the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

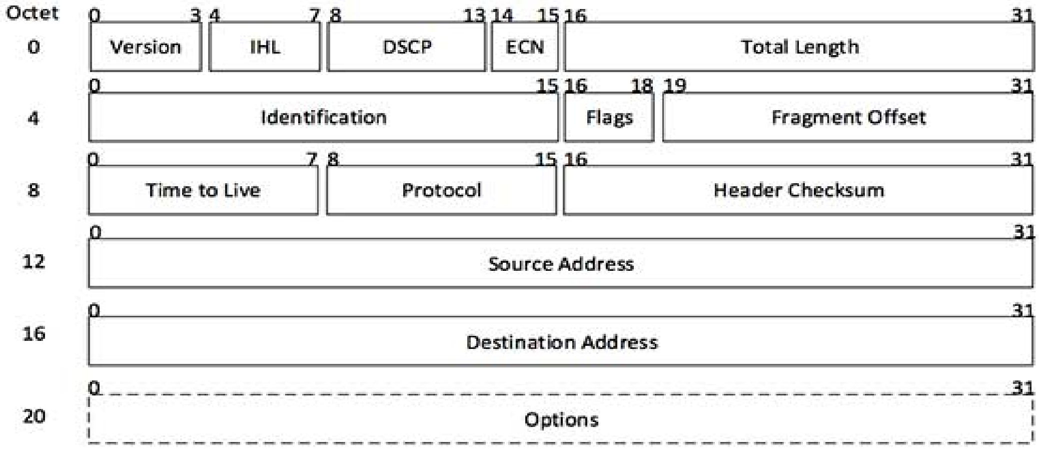


Figure 14: IP Header

10.1 CLASSFUL ADDRESSING

- The 32 bit IP address is divided into five sub-classes.

- **Class A:**
  - In Class A, an IP address is assigned to those networks that contain a large number of hosts.
  - The network ID is 8 bits long and the host ID is 24 bits long.
  - In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID.

- **Class B:**
  - In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.
  - The Network ID is 16 bits long.
  - The Host ID is 16 bits long**.**

- In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID.

- **Class C:**
  - In Class C, an IP address is assigned to only small-sized networks.
  - The Network ID is 24 bits long.
  - The host ID is 8 bits long.
  - In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID.

- **Class D:**
  - In Class D, an IP address is reserved for multicast addresses.
  - It does not possess subnetting.
  - The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.

- **Class E:**
  - In Class E, an IP address is used for the future use or for the research and development purposes.
  - It does not possess any subnetting and higher order bits of the first octet is always set to 1111.

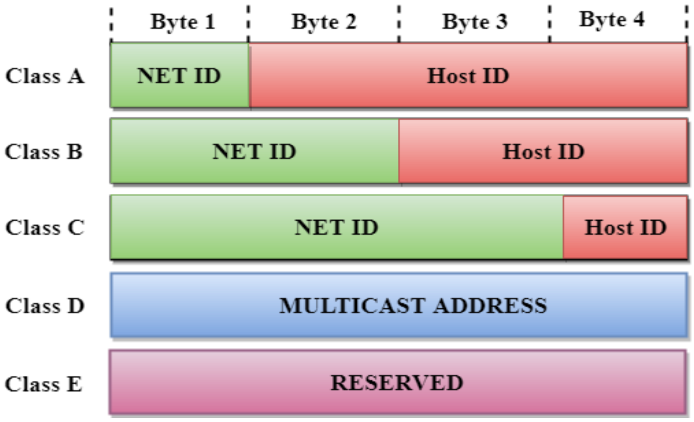


Figure 15: Classful Addressing

10.2 SUBNETTING

- Subnetting is the practice of dividing a network into two or more smaller networks to increase the routing efficiency and the security of the network and thereby reducing the size of the broadcast domain.
- Applying the subnet mask to an IP address splits the address into two parts, an extended network address and a host address.

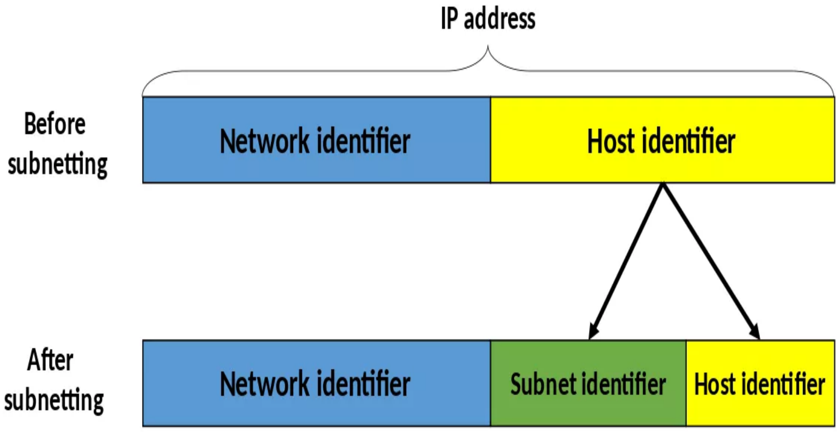


Figure 16: Subnetting

- **Example: Designing of 3 networks in class B using subnetting**.
  - IP Address: 132.108.6.0/16
  - 2^2 = 4 networks can be generated by borrowing 2 bits from the host field.
  - Therefore, the no: of host bits are reduced to 16-2 =14 bits.
  - Network has now 16+2=18 bits.
  - The total no: of network addresses become 2^18 and total host addresses become 2^14.

11 IPv6

- IPv6 was developed to deal with the problem of IP v4 exhaustion.
- IPv6 is 128-bits address having an address space of 2^128, which is bigger than IPv4.
- In IPv6 Colon-Hexa representation is used.
- There are 8 groups and each group represents 2 Bytes.
- In IPv6 representation, we have three addressing methods
  - Unicast
  - Multicast
  - Anycast
- **Unicast Address:** Unicast Address identifies a single network interface. A packet sent to unicast address is delivered to the interface identified by that address.
- **Multicast Address:** Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.
- **Anycast Address:** Anycast Address is assigned to a group of interfaces.

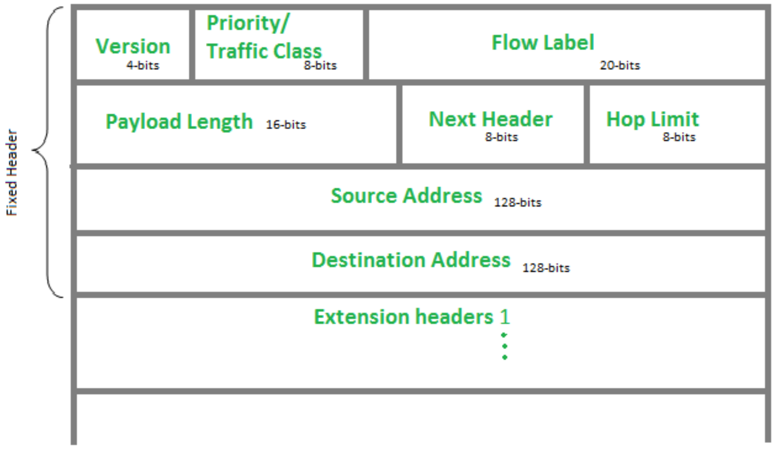


Figure 17: IPv6 Header

12 CISCO PACKET TRACER OUTPUT

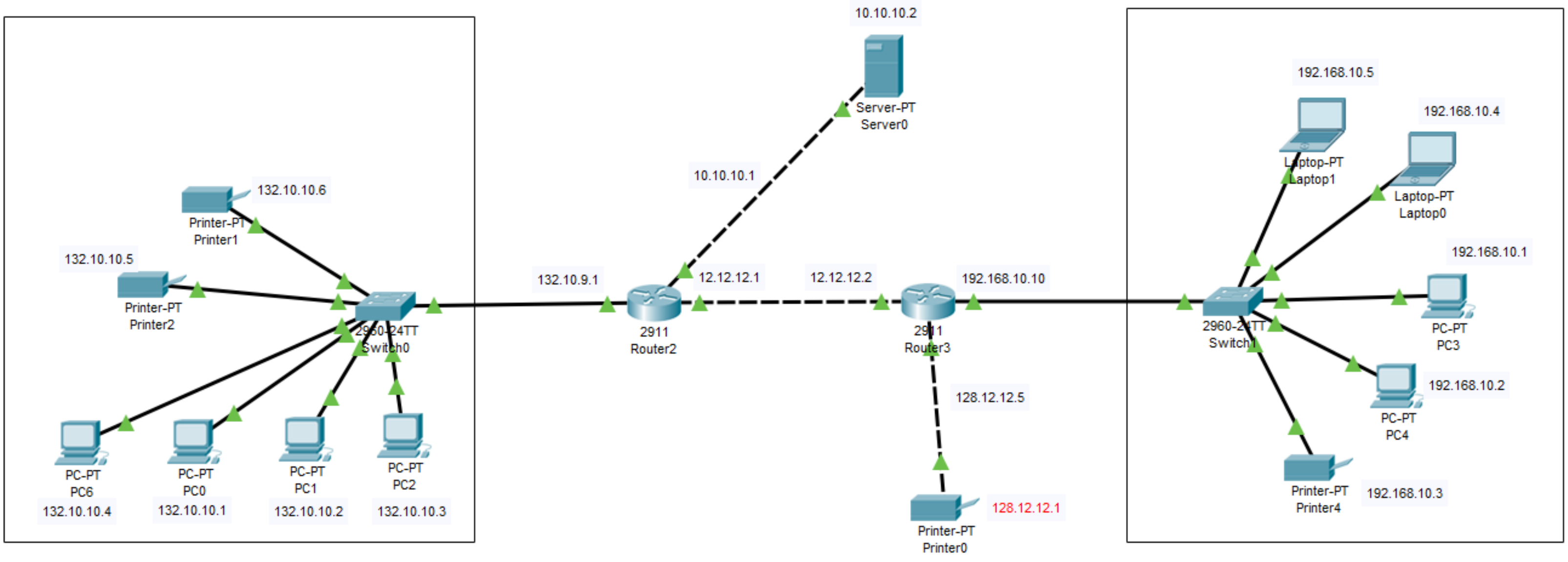
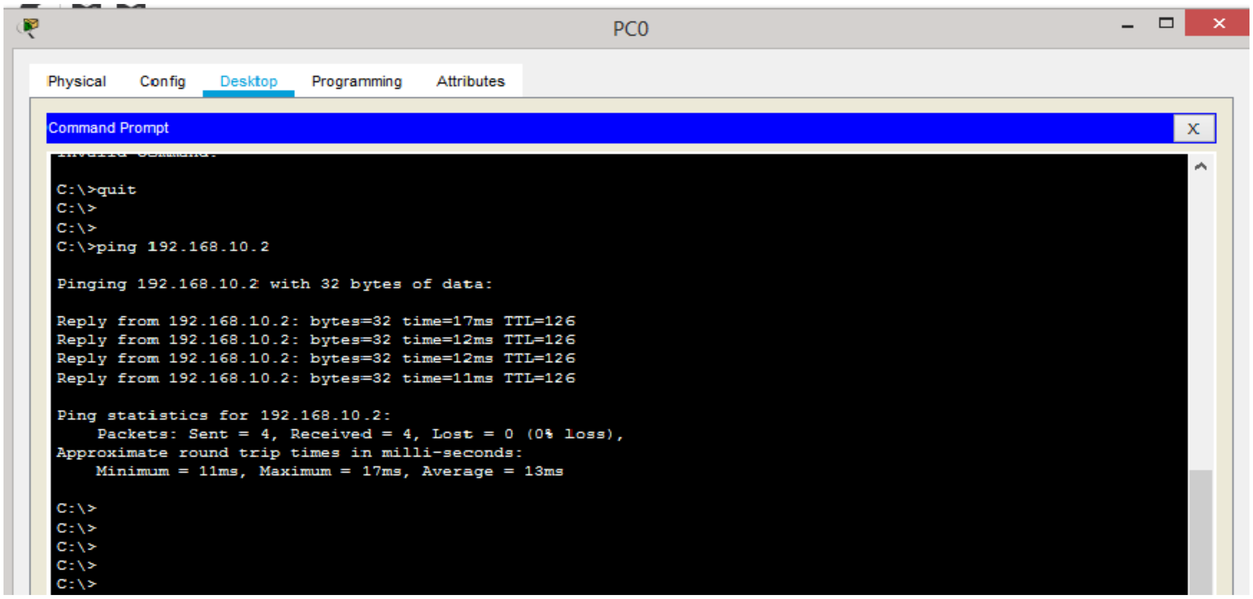


Figure 18: Network in Cisco Packet Tracer

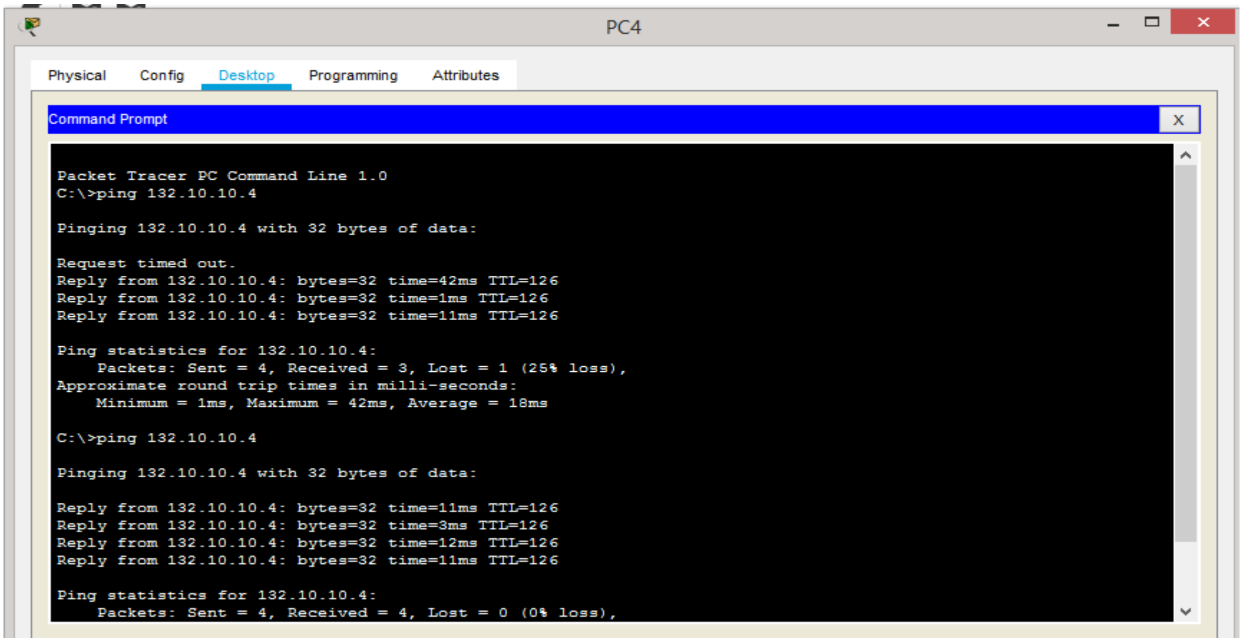
12.1 Ping output from PC0 (132.10.10.1) to PC4 (192.168.10.2)



```
Invalid Command.

C:\>quit
C:\>
C:\>
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=17ms TTL=126
Reply from 192.168.10.2: bytes=32 time=12ms TTL=126
Reply from 192.168.10.2: bytes=32 time=12ms TTL=126
Reply from 192.168.10.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 17ms, Average = 13ms

C:\>
C:\>
C:\>
C:\>
C:\>
```

Figure 19: Ping Output - 1

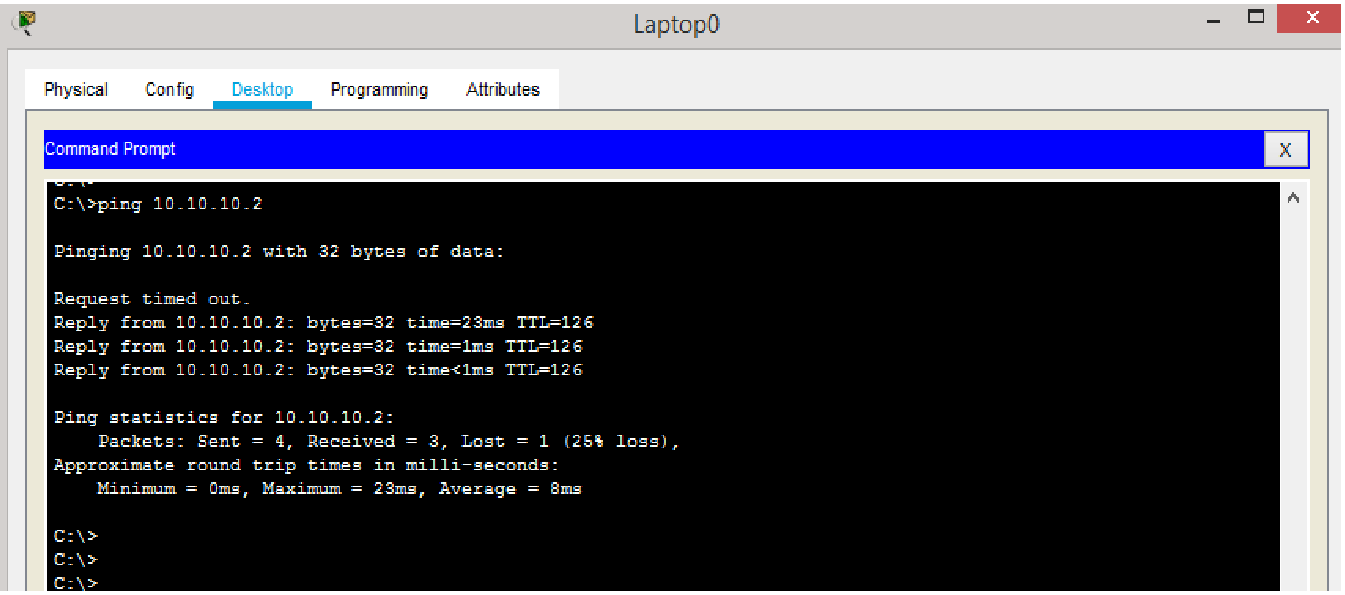
12.2 Ping output from PC4 (192.168.10.2) to PC6 (132.10.10.4)



```
Packet Tracer PC Command Line 1.0
C:\>ping 132.10.10.4

Pinging 132.10.10.4 with 32 bytes of data:

Request timed out.
Reply from 132.10.10.4: bytes=32 time=42ms TTL=126
Reply from 132.10.10.4: bytes=32 time=1ms TTL=126
Reply from 132.10.10.4: bytes=32 time=11ms TTL=126

Ping statistics for 132.10.10.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 42ms, Average = 18ms

C:\>ping 132.10.10.4

Pinging 132.10.10.4 with 32 bytes of data:

Reply from 132.10.10.4: bytes=32 time=11ms TTL=126
Reply from 132.10.10.4: bytes=32 time=3ms TTL=126
Reply from 132.10.10.4: bytes=32 time=12ms TTL=126
Reply from 132.10.10.4: bytes=32 time=11ms TTL=126

Ping statistics for 132.10.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 20: Ping Output – 2

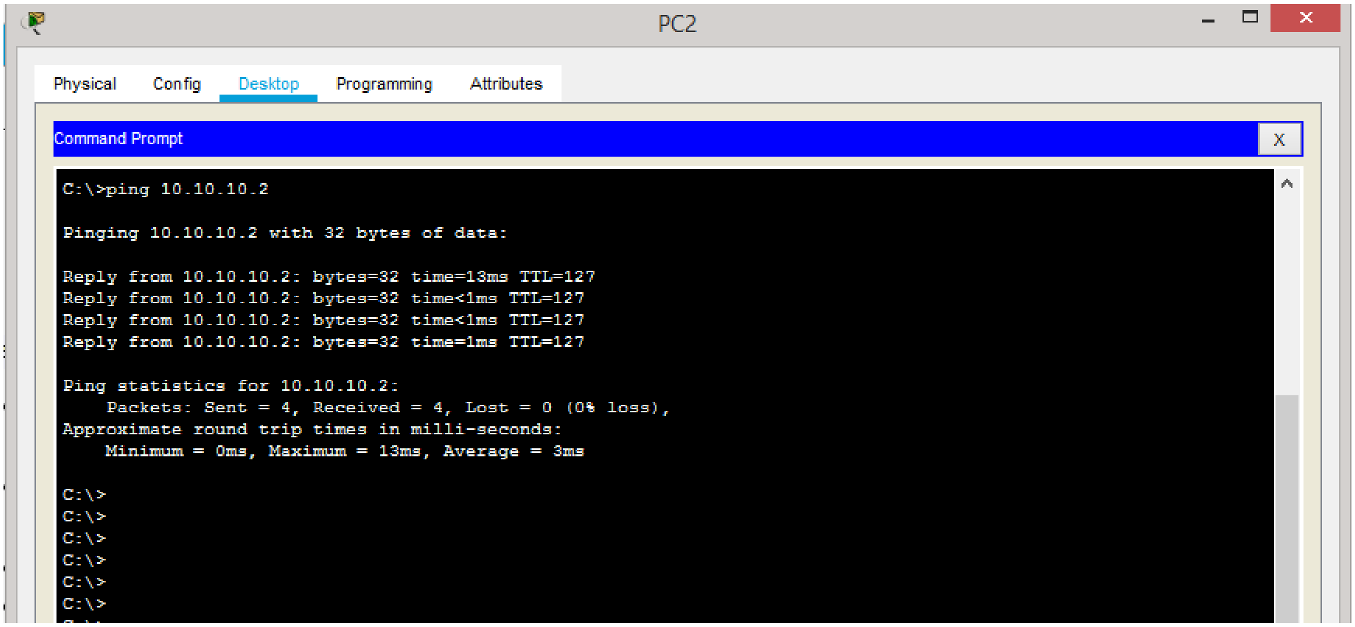
12.3 Ping output from Laptop0 (192.168.10.4) to server (10.10.10.2)



```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.2: bytes=32 time=23ms TTL=126
Reply from 10.10.10.2: bytes=32 time=1ms TTL=126
Reply from 10.10.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 23ms, Average = 8ms

C:\>
C:\>
C:\>
```

Figure 21: Ping Output - 3

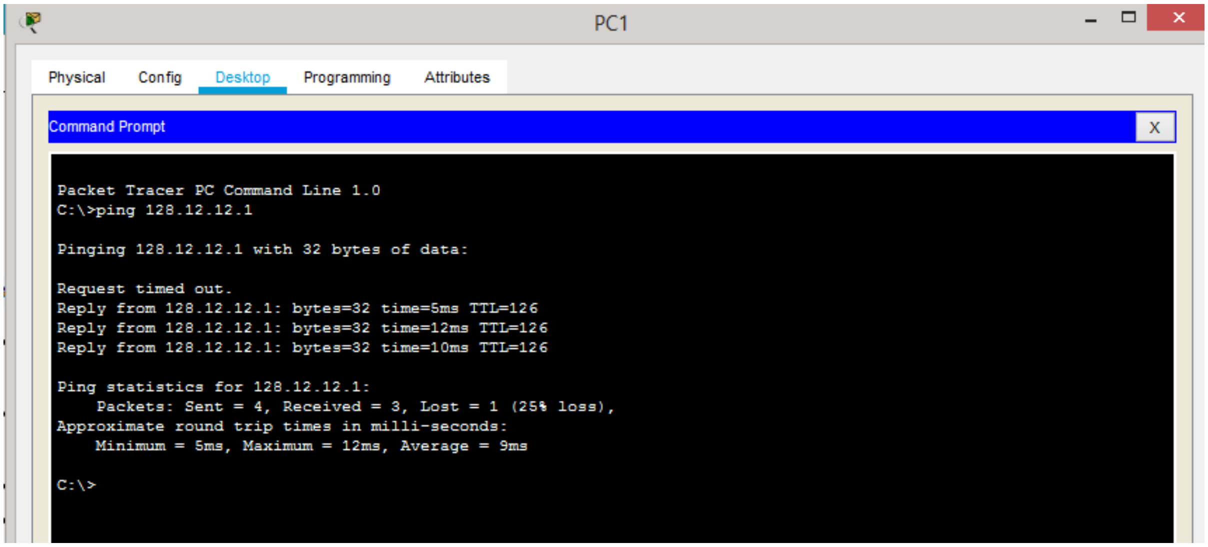
12.4 Ping output from PC2 (132.10.10.3) to server (10.10.10.2)



```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=13ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Figure 22: Ping Output - 4

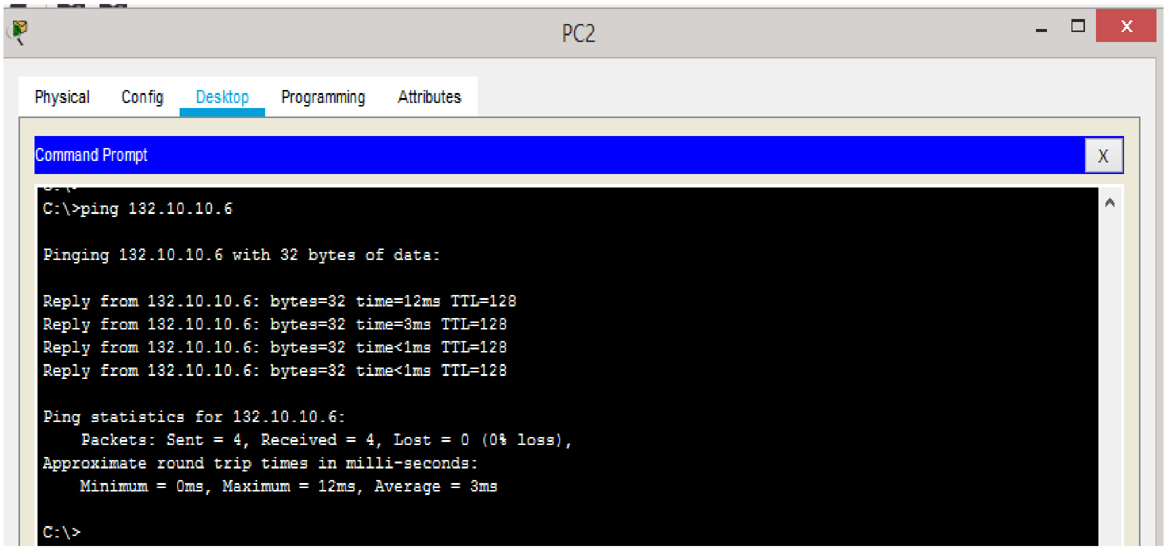
12.5 Ping output from PC1 (132.10.10.2) to Printer0 (128.12.12.1)



```
Packet Tracer PC Command Line 1.0
C:\>ping 128.12.12.1

Pinging 128.12.12.1 with 32 bytes of data:

Request timed out.
Reply from 128.12.12.1: bytes=32 time=5ms TTL=126
Reply from 128.12.12.1: bytes=32 time=12ms TTL=126
Reply from 128.12.12.1: bytes=32 time=10ms TTL=126

Ping statistics for 128.12.12.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 12ms, Average = 9ms

C:\>
```

Figure 23: Ping Output - 5

12.6 Ping output from PC2 (132.10.10.3) to Printer1 (132.10.10.6)



```
C:\>ping 132.10.10.6

Pinging 132.10.10.6 with 32 bytes of data:

Reply from 132.10.10.6: bytes=32 time=12ms TTL=128
Reply from 132.10.10.6: bytes=32 time=3ms TTL=128
Reply from 132.10.10.6: bytes=32 time<1ms TTL=128
Reply from 132.10.10.6: bytes=32 time<1ms TTL=128

Ping statistics for 132.10.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

Figure 24: Ping output - 6

13 REFERENCES

[1] Types of Network Topology - GeeksforGeeks

[2] 7 Types of Computer Network Topology (With Diagrams) (red-dot-geek.com)

[3] Uses of Bridges in Computer Network (tutorialspoint.com)

[4] IPv4 Address: Structure, Classes and Types - Video & Lesson Transcript | Study.com

[5] https://www.javatpoint.com/rip-protocol

[6] https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

[7] https://www.cbtnuggets.com/blog/technology/networking/networking-basics- what-is-ipv4-subnettingrg/how-address-resolution-protocol-arp-works

[8] https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works