Terna Engineering College

Computer Engineering Department
Program: Sem V

Course: Computer Network Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No. 07

A.1 Objective:

Design a LAN and establish connection to other networks and understand the basic working of PING (ICMP) and ARP (DLL).

A.2 Prerequisite:

- Knowledge about LAN, MAN and WAN and NW Elements.
- Linux NW Commands
- HW and IP Address concepts.
- Concept of Analysis, Design, Simulation and Modelling
- Cisco Packet tracer as simulation tool

A.3 Outcome:

After successful completion of this experiment students will be able to

- Ability to select the proper NW Elements required to design NWs.
- Design different LANs.
- Connect the LANs through the routers by addressing the proper addresses.
- To Design an environment to learn various commands and Protocols used by various layers of networking.
- Simulate the designed NW using PING, ICMP and ARP.

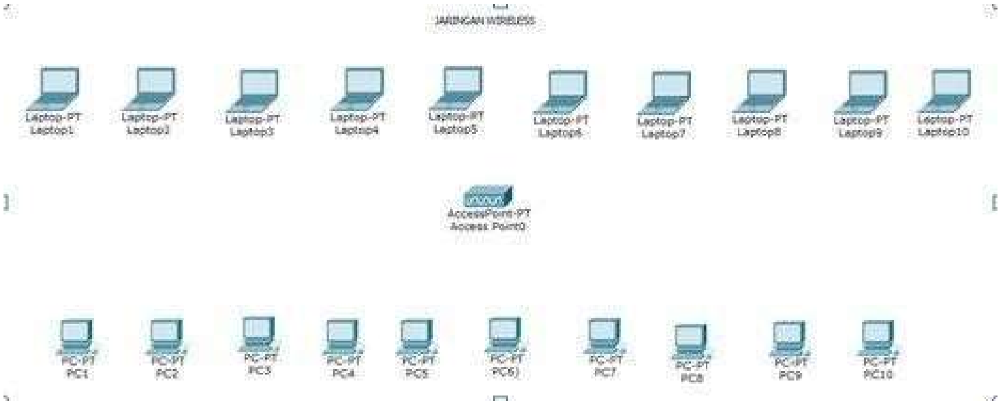
A.4 Theory/Tutorial:

1. Steps to create LAN

Cisco Packet Tracer is an application designed to be able to simulate a network before actually doing the network development, and also can be used for simulation research in a network.

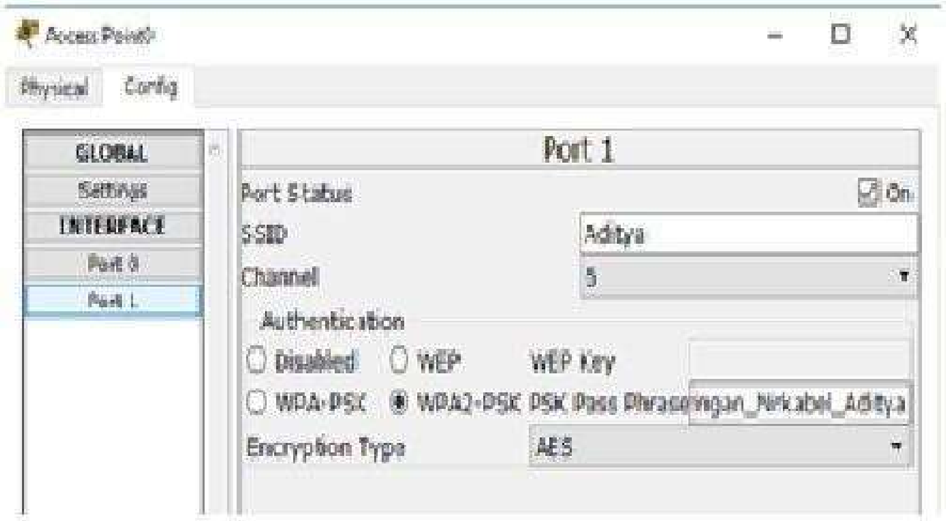
1. Work Steps
   • Create a network using an Access Point consisting of 10 PCs and 10 Laptops
   • Create a WPA2-PSK security system on the Access Point with the SSID as we want and the Network password.

1. make the network as follows.



1. Then create SSID and Password in Access Point.

- Clicked 2 times on AP.
- After that choose Config tab ◊ select Port 1 ◊ fill in SSID and Password.



Port 1

Port Status ☑ On

SSID Aditya

Channel 5

Authentication

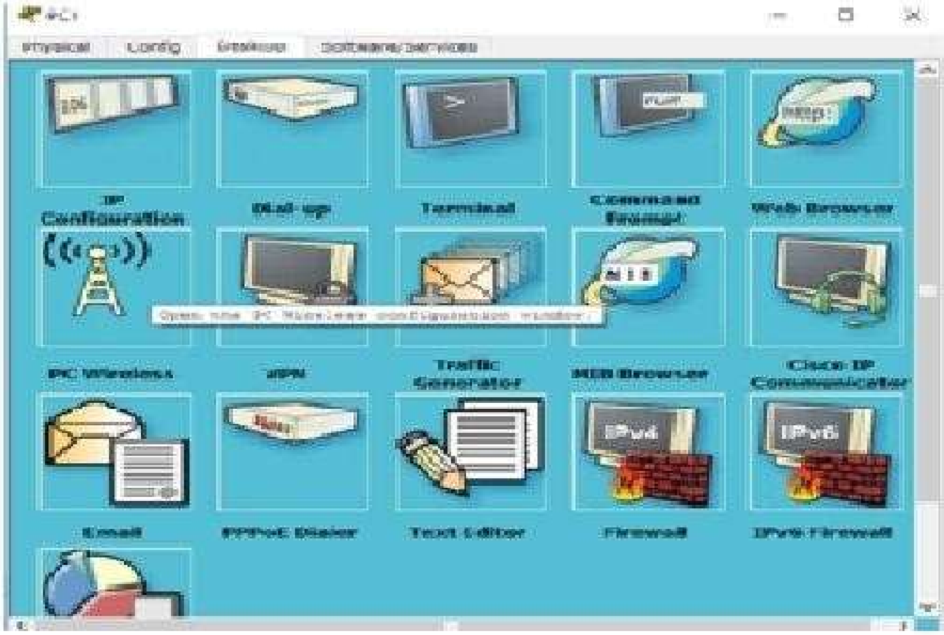
○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase ingan_Nirkabel_Aditya

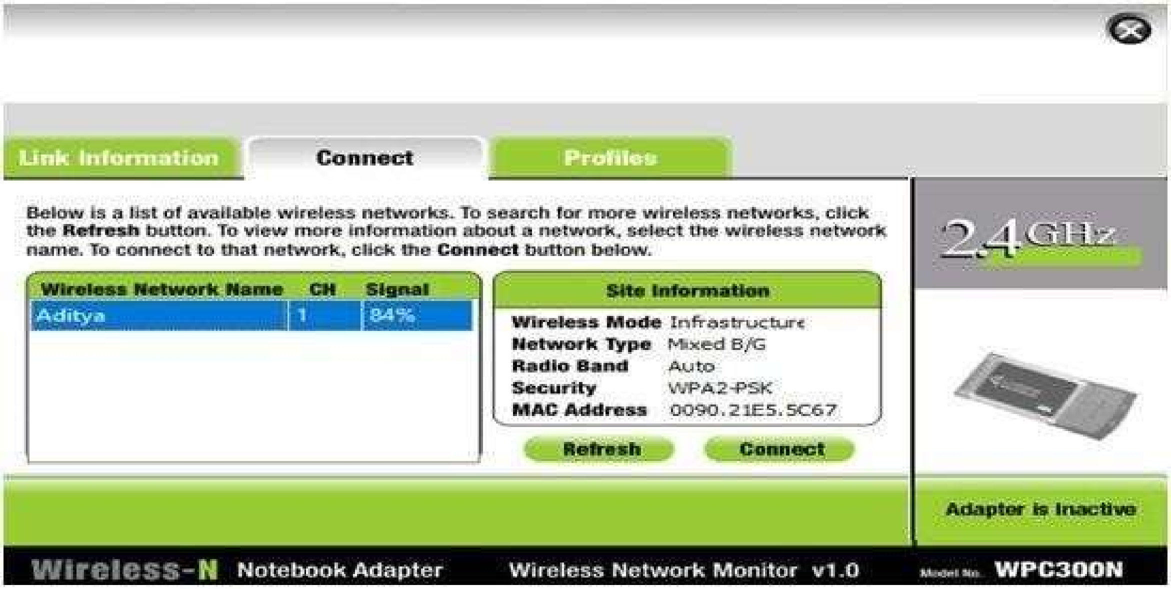
Encryption Type AES

1. After that, connect PC and Laptop to AP.

- Clicked 2 times on PC / Laptop.
- Then choose Desktop tab ◊ choose PC Wireless



- After that, choose the Connect tab ◊ choose the name of the AP you want to connect ◊ pressing Connect



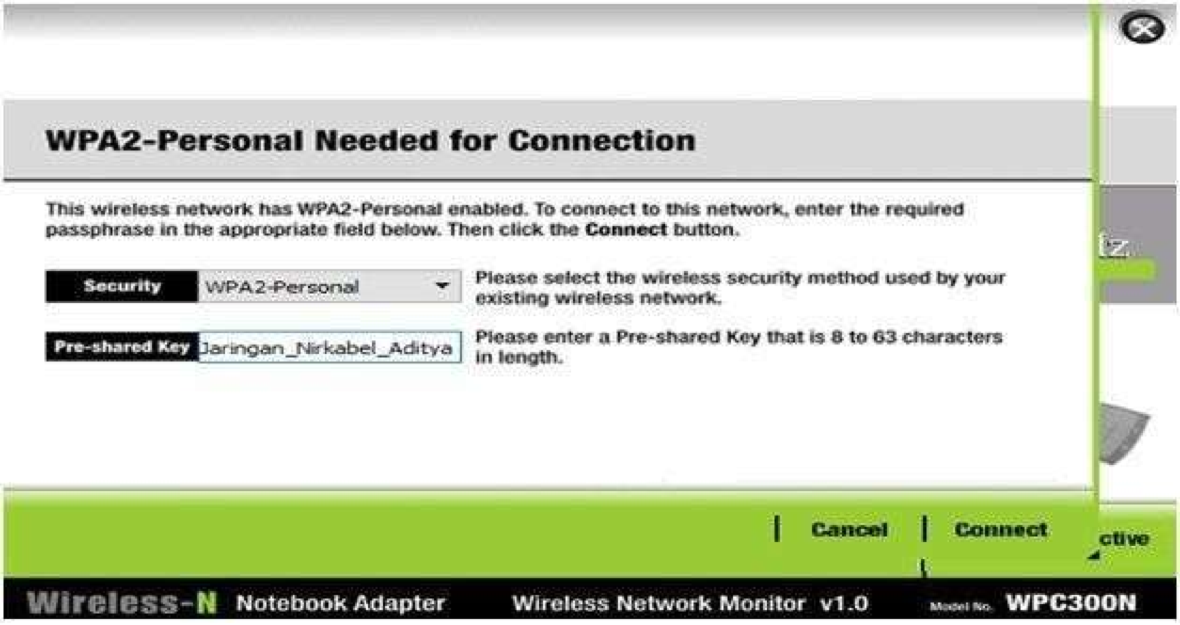
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Aditya	1	84%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G
Radio Band	Auto
Security	WPA2-PSK
MAC Address	0090.21E5.5C67

- After that fill in the AP password.

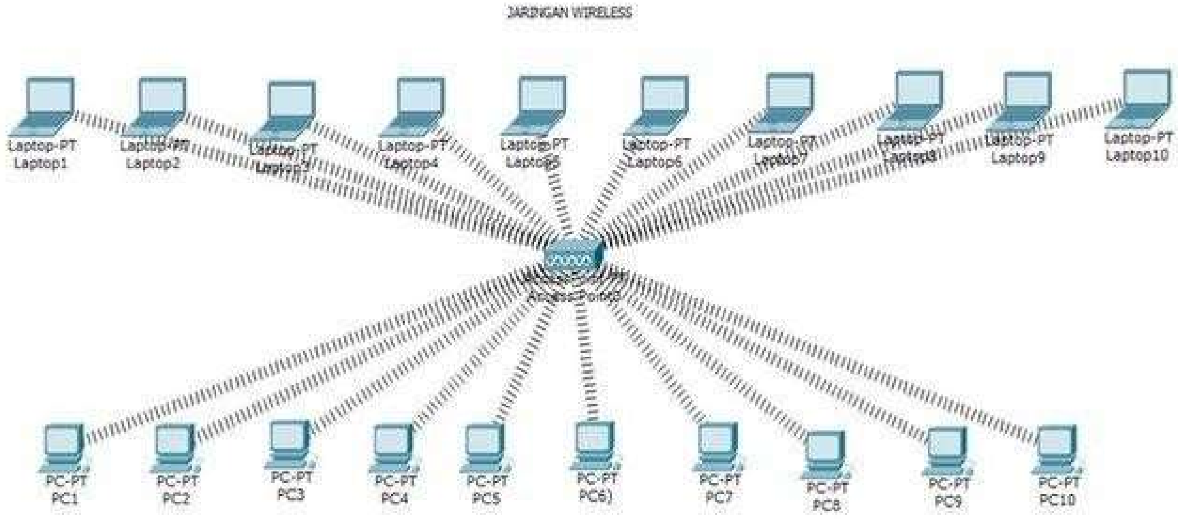


WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

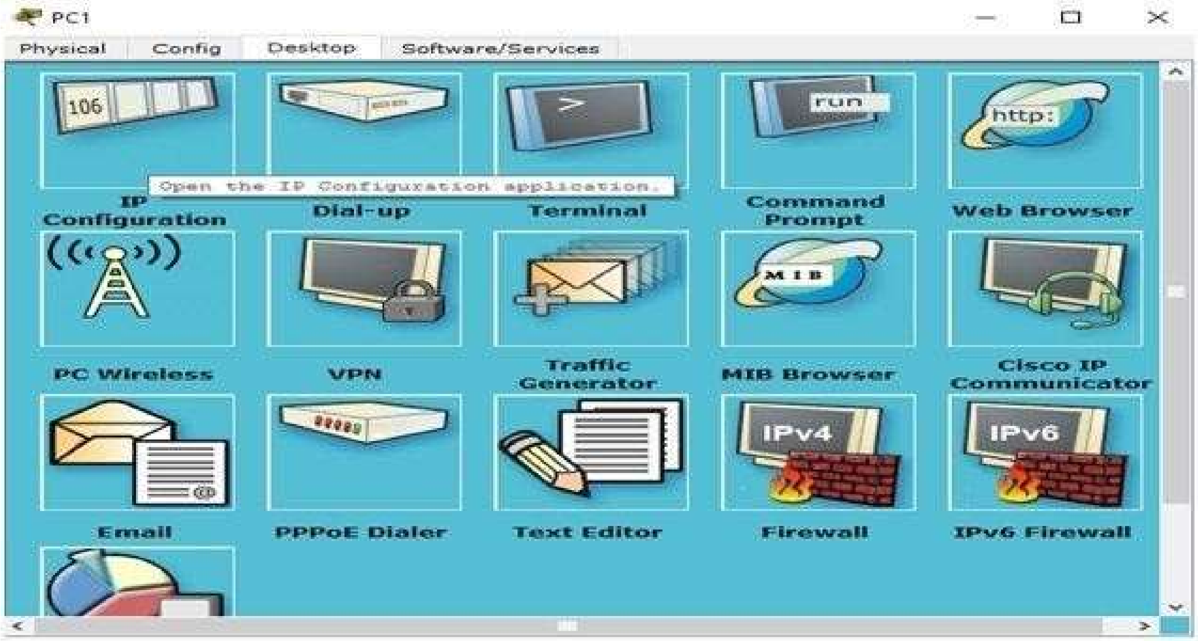
Security	WPA2-Personal	Please select the wireless security method used by your existing wireless network.
Pre-shared Key	Jaringan_Nirkabel_Aditya	Please enter a Pre-shared Key that is 8 to 63 characters in length.

- When completed, then PC and Laptop are connected to AP.

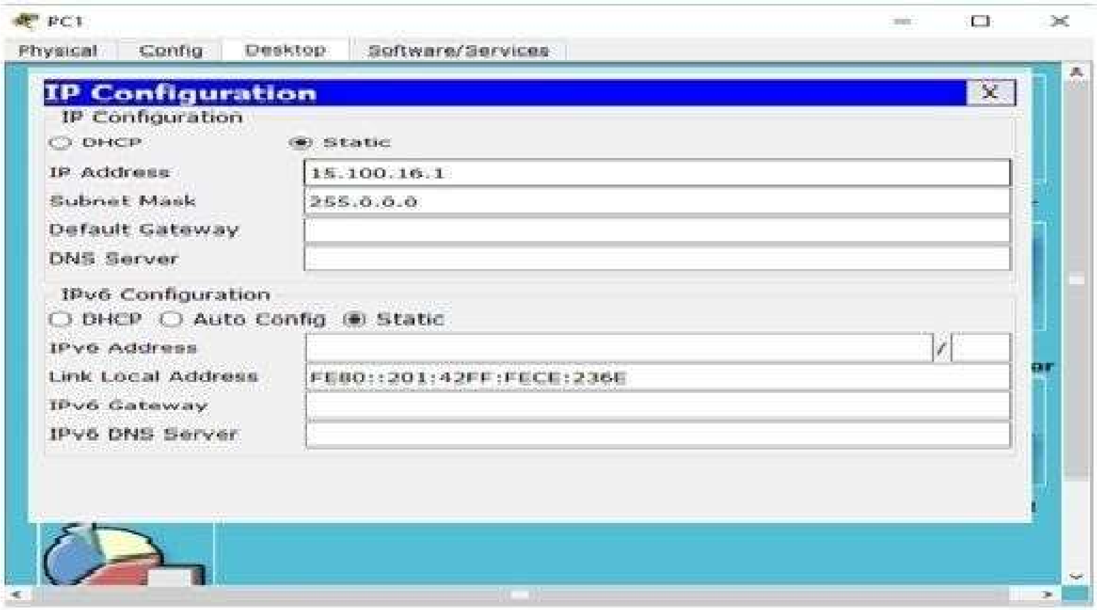


- After that fill the IP Address for PC and laptop.
  o Clicking 2 times on PC / laptop.

o Then select Desktop tab ◊ choose IP Configuration.



- Then choose Static radio button ◊ fill in IP Address.



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 15.100.16.1

Subnet Mask 255.0.0.0

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::201:42FF:FECE:236E

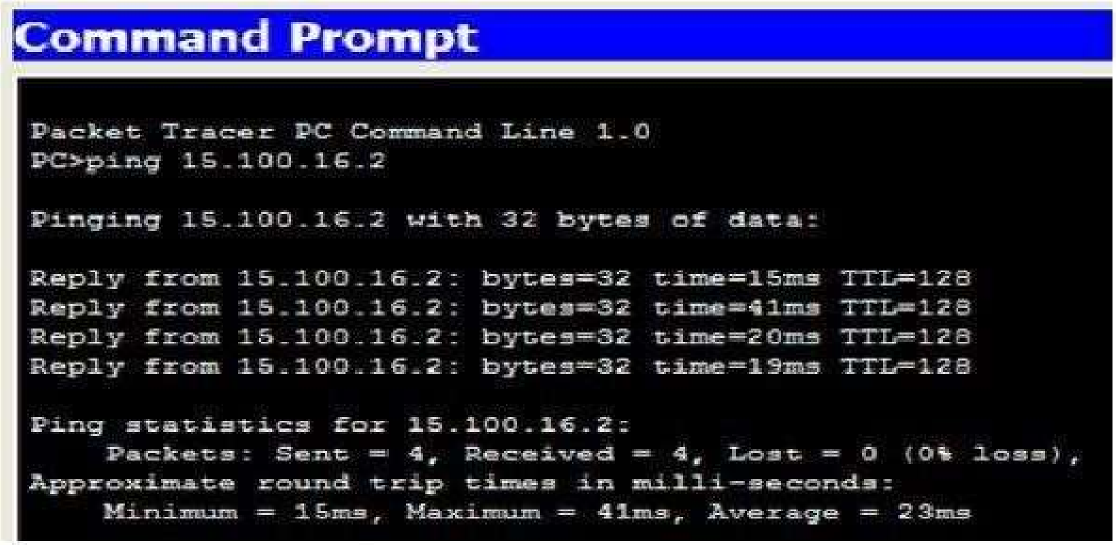
IPv6 Gateway

IPv6 DNS Server

- After that, perform PING to find out if PC / laptop is connected.

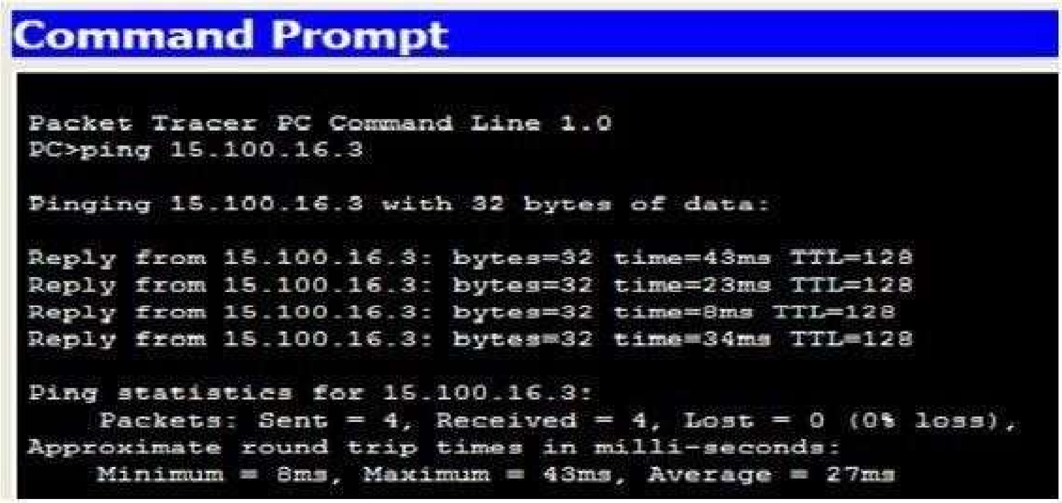
o PC – PC

PC 1 – PC 2



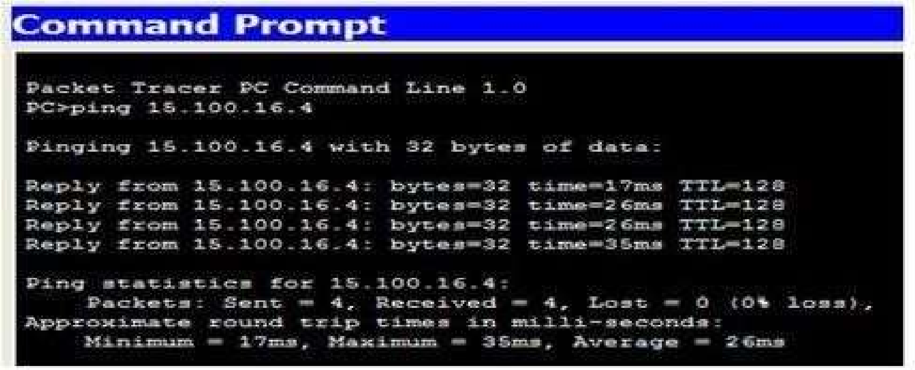
```
Packet Tracer PC Command Line 1.0
PC>ping 15.100.16.2

Pinging 15.100.16.2 with 32 bytes of data:

Reply from 15.100.16.2: bytes=32 time=15ms TTL=128
Reply from 15.100.16.2: bytes=32 time=41ms TTL=128
Reply from 15.100.16.2: bytes=32 time=20ms TTL=128
Reply from 15.100.16.2: bytes=32 time=19ms TTL=128

Ping statistics for 15.100.16.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 41ms, Average = 23ms
```

PC 2 - PC 3



```
Packet Tracer PC Command Line 1.0
PC>ping 15.100.16.3

Pinging 15.100.16.3 with 32 bytes of data:

Reply from 15.100.16.3: bytes=32 time=43ms TTL=128
Reply from 15.100.16.3: bytes=32 time=23ms TTL=128
Reply from 15.100.16.3: bytes=32 time=8ms TTL=128
Reply from 15.100.16.3: bytes=32 time=34ms TTL=128

Ping statistics for 15.100.16.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 43ms, Average = 27ms
```

PC 3 - PC 4



```
Packet Tracer PC Command Line 1.0
PC>ping 15.100.16.4

Pinging 15.100.16.4 with 32 bytes of data:

Reply from 15.100.16.4: bytes=32 time=17ms TTL=128
Reply from 15.100.16.4: bytes=32 time=26ms TTL=128
Reply from 15.100.16.4: bytes=32 time=26ms TTL=128
Reply from 15.100.16.4: bytes=32 time=35ms TTL=128

Ping statistics for 15.100.16.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 35ms, Average = 26ms
```

PC 4 - PC 5

ARP(Address Resolution Protocol):

Most of the computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address) i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into picture, its functionality is to translate IP address to physical address. The acronym ARP stands for **Address Resolution Protocol** which is one of the most important protocol of the Data Link Layer.

Imagine a device wants to communicate with the other over the internet. What ARP does? Is it broadcast a packet to all the devices of the source network?
The devices of the network peel the header of the data link layer from the protocol data unit (PDU) called frame and transfers the packet to the network layer (layer 3 of OSI) where the network ID of the packet is validated with the destination IP's network ID of the packet and if it's equal then it
responds to the source with the MAC address of the destination, else the packet reaches the gateway of the network and broadcasts packet to the devices it is connected with and validates their network ID
The above process continues till the second last network device in the path to reach the destination where it gets validated and ARP in turn responds with the destination MAC address.

PING:

The PING utility is a system administrator's tool that is used to see if a computer is operating and also to see if network connections are intact. Ping uses the Internet Control Message

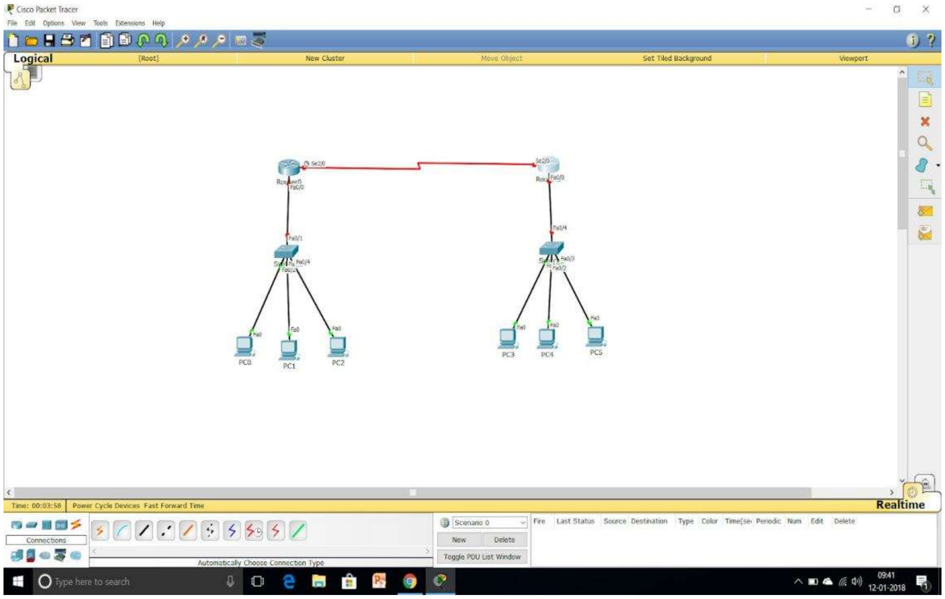
Protocol (ICMP) Echo function. A small packet is sent through the network to a particular IP address. This packet contains 64 bytes - 56 data bytes and 8 bytes of protocol reader information. The computer that sent the packet then waits and listens for a return packet. If the connections are good and the target computer is up, a good return packet will be received. PING can also tell the user the number of hops that lie between two computers and the amount of time it takes for a packet to make the complete trip. Additionally, an administrator can use Ping to test out name resolution. If the packet bounces back when sent to the IP address but not when sent to the name, then the system is having a problem matching the name to the IP address.

SN O.	NAME OF THE DEVICE	INTERFACE	IP ADDRESS	Subnet Mask	Default Gateway
1.	Router 0	fa0/0	192.168.1.1	255.255.255.0	--------
2.	Router 0	Fa0/1	10.0.0.1	255.0.0.0	--------
3.	Router 1	fa0/0	192.168.2.1	255.255.255.0	--------
4.	Router 1	Fa0/1	10.0.0.2	255.0.0.0	--------
5.	PC0	fa0/0	192.168.1.2	255.255.255.0	192.168.1.1
6.	PC1	fa0/0	192.168.1.3	255.255.255.0	192.168.1.1
7.	PC2	fa0/0	192.168.1.4	255.255.255.0	192.168.1.1
8.	PC0	fa0/0	192.168.2.1	255.255.255.0	192.168.2.1
9.	PC1	fa0/0	192.168.2.1	255.255.255.0	192.168.2.1
10.	PC2	fa0/0	192.168.2.1	255.255.255.0	192.168.2.1

2. **LAN To be developed using the above steps.**

   Interface Configuration table:

A6 Design:



References:

- https://youtu.be/FnH1XUQsoD8
- https://youtu.be/ihKtFQEikFA

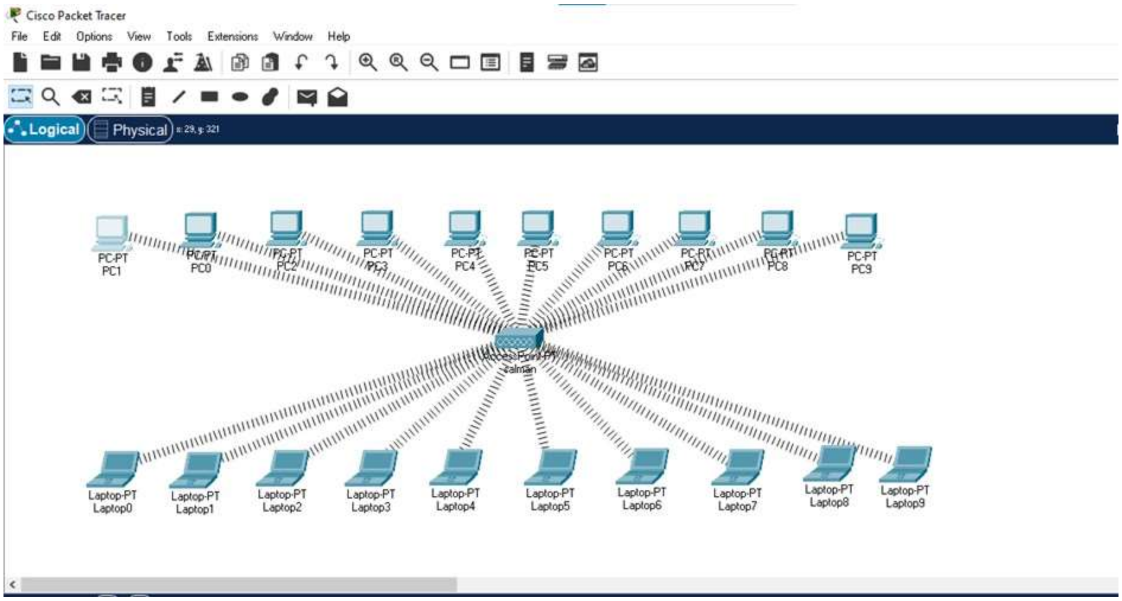
PART B

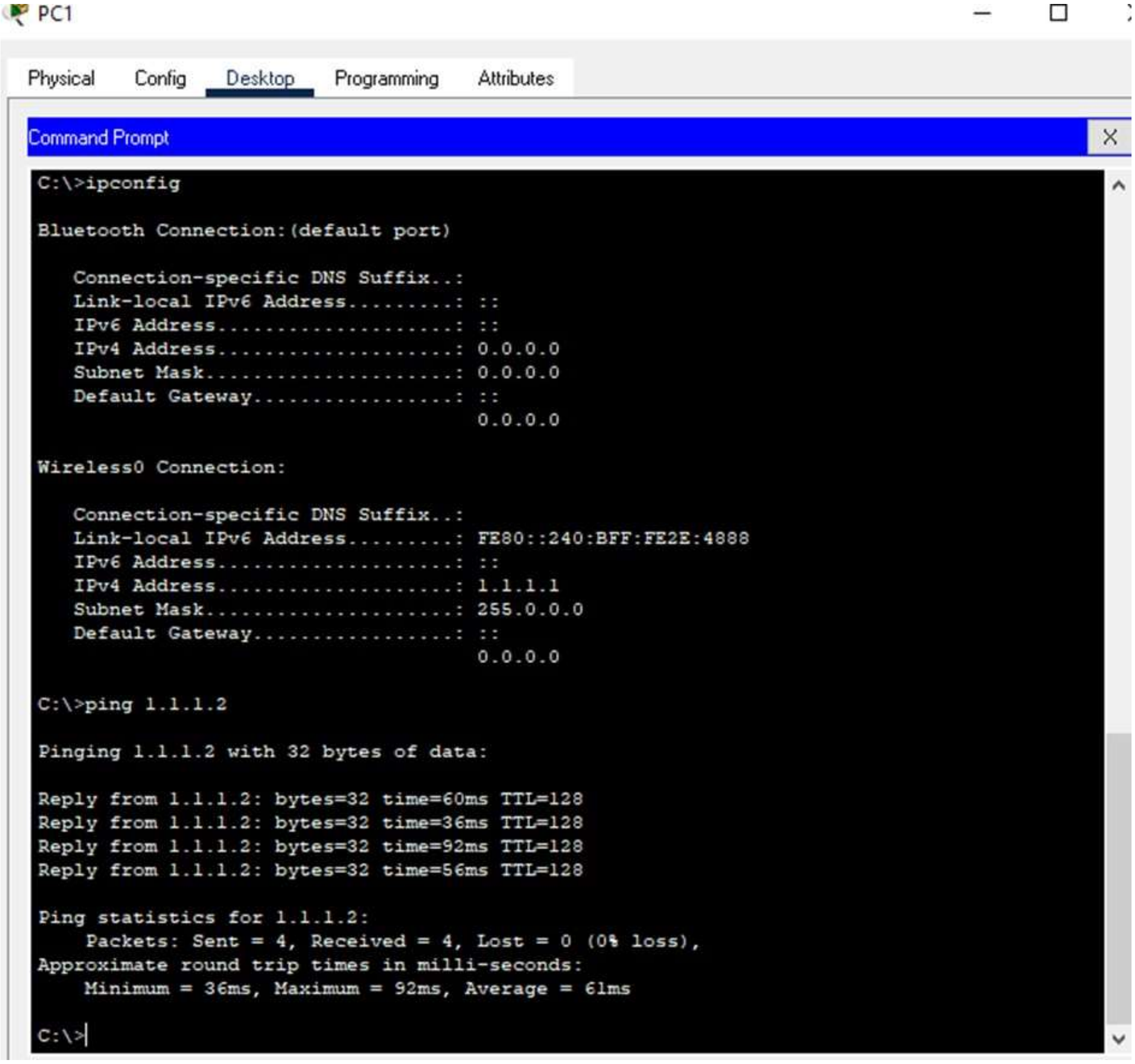
(PART B : TO BE COMPLETED BY STUDENTS)

Roll No.: A11	Name: Khan Mohammad TAQI
Class : T.E. A	Batch : A1
Date of Experiment:	Date of Submission:
Grade :	

B.1 Document created by the student:

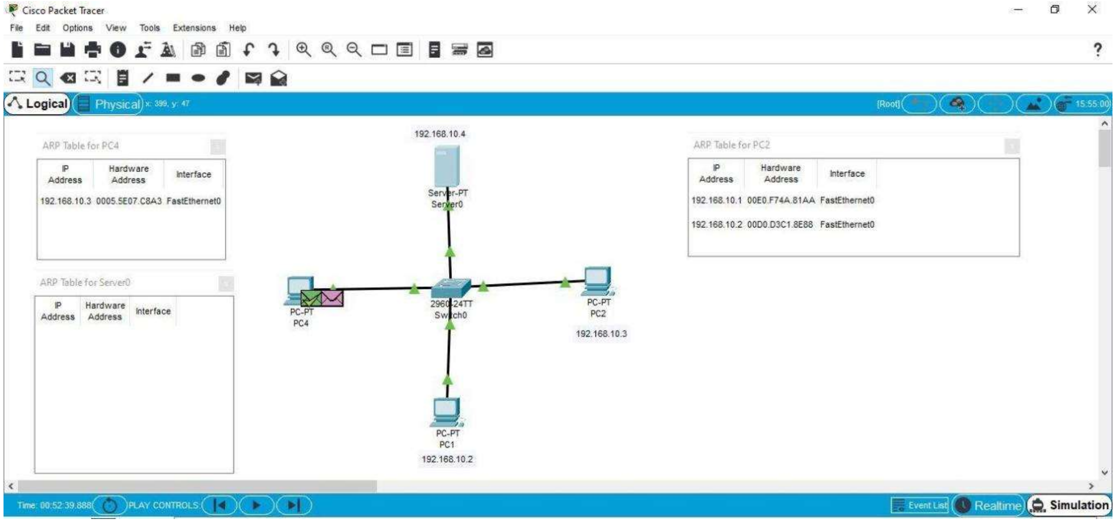
1. **LAN:**





```
C:\>ipconfig

Bluetooth Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

Wireless0 Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::240:BFF:FE2E:4888
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.1.1
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.1.2

Pinging 1.1.1.2 with 32 bytes of data:

Reply from 1.1.1.2: bytes=32 time=60ms TTL=128
Reply from 1.1.1.2: bytes=32 time=36ms TTL=128
Reply from 1.1.1.2: bytes=32 time=92ms TTL=128
Reply from 1.1.1.2: bytes=32 time=56ms TTL=128

Ping statistics for 1.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 92ms, Average = 61ms

C:\>
```

2. ARP(Address Resolution Protocol):



ARP Table for PC4

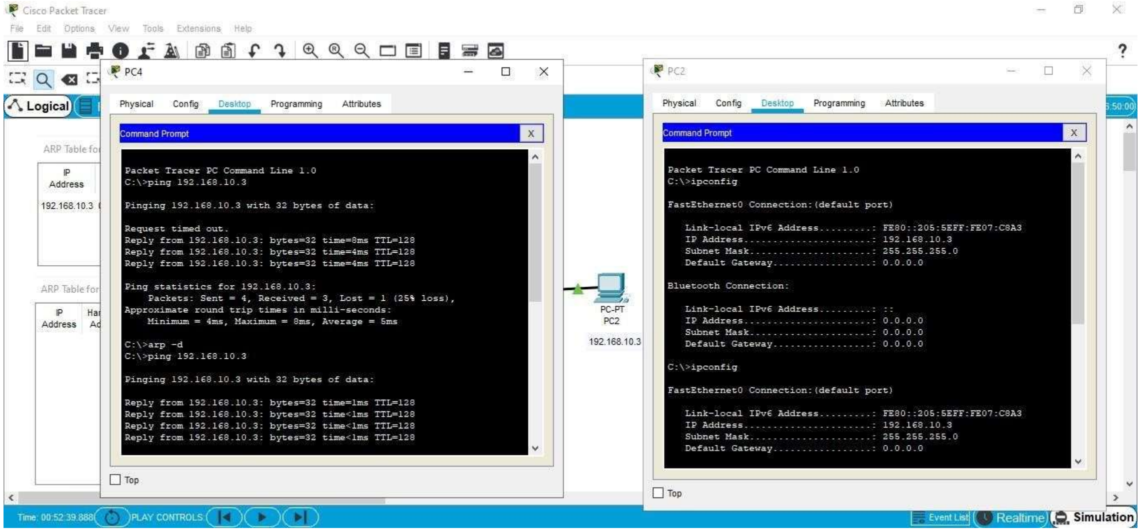
IP Address	Hardware Address	Interface
192.168.10.3	0005.5E07.C8A3	FastEthernet0

ARP Table for Server0

IP Address	Hardware Address	Interface

ARP Table for PC2

IP Address	Hardware Address	Interface
192.168.10.1	00E0.F74A.81AA	FastEthernet0
192.168.10.2	00D0.D3C1.8E88	FastEthernet0



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.3: bytes=32 time=8ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128
Reply from 192.168.10.3: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -d
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time=1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
```

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::205:5EFF:FE07:C8A3
   IP Address......................: 192.168.10.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0

Bluetooth Connection:

   Link-local IPv6 Address.........: ::
   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::205:5EFF:FE07:C8A3
   IP Address......................: 192.168.10.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
```

B.3 Observations and learning:

ARP-Ping IP checks whether an IP address is used by another device on a LAN by sending an ARP packet. Before configuring an IP address for a device, send an ARP Request packet to this IP address to check whether the IP address is in use. ARP is necessary because the software address (IP address) of the host or computer connected to the network needs to be translated to a hardware address (MAC address). Without ARP, a host would not be able to figure out the hardware address of another host.

B.4 Conclusion:

PING and ARP are vital components of network communication, with PING focusing on network diagnostics and ARP facilitating local communication by mapping IP addresses to MAC addresses. Understanding the roles of these protocols is essential for network administrators and troubleshooting network- related issues.

B.5 Question of Curiosity:

1. What is CISCO Packet tracer? How can one make use of it by learning CN?

Answer: Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is widely used in networking education and training programs to help students and professionals learn and practice networking concepts and configurations. Here's how you can make use of Cisco Packet Tracer for learning computer networking (CN):

1. Network Simulation:

- Cisco Packet Tracer allows you to create and simulate network topologies, including routers, switches, hubs, PCs, servers, and various networking devices
- You can design complex network scenarios and configure devices as you would be a real network, making it a valuable tool for hands-on practice.

2. Experimentation:

- It provides a safe environment to experiment with networking configurations without the risk of disrupting real networks.
- You can configure routing protocols, set up VLANs, create access control lists (ACLs), and perform other network-related tasks.

3. Learning Resources:

- Cisco Packet Tracer comes with a variety of pre-built labs and exercises, allowing you to practice specific networking concepts and scenarios.
- Many educational institutions and training programs provide Packet Tracer labs and resources as part of their networking courses.

4. Visualization:

- Packet Tracer offers a visual representation of how data packets flow through a network, helping learners understand the process of packet forwarding and routing.
- You can see how packets move between devices and troubleshoot connectivity issues visually.

5. Assessments:

- Instructors can use Packet Tracer for creating assessments and quizzes to evaluate students' understanding of networking concepts.
- It provides a way to grade students based on their configuration and troubleshooting skills.

6. Realistic Scenarios:

- You can create realistic network scenarios, including WAN (Wide Area Network) connections, LAN (Local Area Network) setups, and even incorporate IoT (Internet of Things) devices to practice various networking scenarios.

2. What are all the NW elements you will use in the CISCO Packet Tracer?

Answer: Cisco Packet Tracer is a comprehensive network simulation tool that includes a wide range of network elements or components that you can use to build and simulate various network topologies and scenarios. Here are some of the key network elements you will find in Cisco Packet Tracer:

1. Routers: Cisco Packet Tracer provides a variety of router models that allow you to configure and simulate routing protocols, create network segments, and interconnect multiple networks.

2. Switches: You can use switches to connect devices within a local network segment, set up VLANs (Virtual LANs), and manage traffic within the same subnet.

3. Hubs: Hubs are basic network devices used to connect devices within a network segment. Unlike switches, hubs broadcast data to all connected devices.

4. End Devices: This category includes various end-user devices such as PCs, laptops, servers, smartphones, and tablets. You can configure these devices to generate and receive network traffic.

5. Wireless Devices: Packet Tracer includes wireless routers, access points, and wireless clients for simulating wireless LANs (Wi-Fi networks).

6. Firewalls: You can configure firewall devices to control and monitor traffic flow between different network segments, adding a layer of security to your simulations.

7. Modems: Modems can be used to simulate broadband and dial-up connections to the internet or other networks.

8. VoIP Phones: Packet Tracer supports Voice over IP (VoIP) phone devices, allowing you to simulate voice communication over IP networks.

9. IoT Devices: You can add Internet of Things (IoT) devices like sensors and actuators to simulate IoT networks and interactions.

10. Cloud and Server Devices: These devices represent cloud services and server infrastructure. You can configure them to host web services, applications, and other network resources.
11. WAN Emulation: Packet Tracer includes WAN (Wide Area Network) emulation features to simulate connections between remote locations, such as leased lines, Frame Relay, and more.
12. Cabling and Connectors: You can connect devices with various types of cables (Ethernet, serial, console) and connectors. Packet Tracer also simulates cable lengths and signal loss.
13. Packet Generators: These tools allow you to generate custom network traffic and analyze packet flow within your simulated network.
14. Protocol Analyzers: Packet Tracer includes built-in protocol analyzers for monitoring and troubleshooting network traffic.
15. Network Services: You can configure DHCP servers, DNS servers, and other network services to provide essential network functionality.
16. Security Devices: Besides firewalls, you can set up security appliances like intrusion detection systems (IDS) and intrusion prevention systems (IPS) to enhance network security.
17. Virtualization: Packet Tracer supports virtualization technologies, allowing you to create and manage virtual machines within your network.

3. Define the following and provide the example for each
    a. IP address
    b. DNS
    c. Subnet mask
    d. Gateway
    e. RIP

Answer: a. IP address: An IP (Internet Protocol) address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two primary functions:
1. Host Identification: An IP address identifies a specific device, such as a computer, server, router, or any other networked device, within a network or on the internet. It is similar to a postal address that helps in routing data packets to the correct destination.
2. Location Addressing: IP addresses also play a crucial role in determining the location or network segment to which a device belongs. This information is essential for the routing of data packets across networks and the internet.
There are two versions of IP addresses in common use:
1. IPv4 (Internet Protocol version 4)
2. IPv6 (Internet Protocol version 6)

- **Example :** 192.168.0.1
  172.16.254.100
  10.0.0.2
  203.0.113.45

b. DNS: DNS stands for Domain Name System. It is a fundamental and a critical component of the internet and computer networking. DNS serves as a decentralized naming system that translates human-readable domain names into numerical IP (Internet Protocol) addresses that computers and networking devices use to identify each other on the internet.

- **Example :** www.amazon.com

c. Subnet mask: A subnet mask is a 32-bit numerical value used in Internet Protocol (IP) networking to divide an IP address into network and host portions. It is used to identify which part of an IP address corresponds to the network identifier and which part represents the host identifier within a particular subnet. Subnet masks are essential for routing and organizing IP networks.

- **Example :** A common subnet mask for simple home networks is 255.255. 255.0

d. Gateway: A gateway, in the context of networking, is a network device or a software component that serves as an entry and exit point for data traffic between different networks or network segments. Its primary function is to facilitate communication between devices or networks that use different communication protocols or have distinct addressing schemes. Gateways play a crucial role in enabling data exchange between networks with varying characteristics.

- **Example :** A router can act as a gateway in a single network. In similar ways, Switches, Servers, Firewalls, etc.

e. RIP: RIP, which stands for Routing Information Protocol, is one of the oldest and most basic interior gateway protocols used in computer networking. RIP is designed for routing within small to medium-sized networks, particularly those using the Internet Protocol (IP). It falls into the category of distance-vector routing protocols and is used to determine the best path for data to travel from one network node to another within an autonomous system (AS).

- **Example :** Consider that router R1 wants to send a packet to the router R8. If you observe the figure below then you can see that there are 3 routes from router R1 to R8 i.e., via R2, R4, and R5. The hop count value of route 1 is 3, the hop count value of route 2 is 2 and the hop count value of route 3 is 4.

4. What is Ping? It belongs to which protocol family.

Answer: PING, which stands for Packet Internet Groper, is a network utility tool used to test the reachability of a host (a device or a computer) on an Internet Protocol (IP) network. It also measures the round-trip time it takes for a packet of data to travel from the source to the destination and back. Ping is part of the ICMP (Internet Control Message Protocol) protocol family.

5. ARP requests are always broadcast why?

Answer: ARP (Address Resolution Protocol) requests are broadcast because they serve the specific purpose of discovering the MAC (Media Access Control) address associated with an IP (Internet Protocol) address within the same local network segment. Broadcast ARP requests are necessary due to the following reasons:

- Unknown MAC Addresses
- Local Network Scope
- Address Resolution Process
- Target Device Response
- Caching
- Efficiency in Local Communication

6. What does an ARP reply carry?

Answer: An ARP (Address Resolution Protocol) reply carries essential information required for mapping an IP (Internet Protocol) address to its corresponding MAC (Media Access Control) address within a local network segment. When a device receives an ARP request and determines that it matches its own IP address, it responds with an ARP reply packet. Here's what an ARP reply typically carries:

1. Sender MAC Address: The ARP reply packet includes the MAC address of the device sending the reply. This field identifies the sender's data link layer (Layer 2) address, allowing the requesting device to learn the MAC address of the device it wants to communicate with.

2. Sender IP Address: The ARP reply packet also contains the IP address of the device sending the reply. This field helps the requesting device correlate the received MAC address with the corresponding IP address.

3. Target MAC Address: In an ARP reply, this field typically contains the MAC address of the sender, as this is the information the requesting device is seeking—the MAC address corresponding to a specific IP address.

4. Target IP Address: The target IP address field in the ARP reply packet contains the IP address for which the ARP request was initially made. It matches the IP address for which the requesting device sought a MAC address.

5. Ethernet Frame Format: ARP replies are encapsulated in Ethernet frames when used in Ethernet-based networks. Therefore, an ARP reply packet includes the standard Ethernet frame header, including destination and source MAC addresses, an Ethernet frame type/length field, and an optional Frame Check Sequence (FCS) for error checking.

6. Packet Length: Some ARP reply packets include information about the packet length or size, typically specified in the Ethernet frame type/length field.

7. What is RARP? How is it different from ARP?

Answer: RARP, or Reverse ARP (Address Resolution Protocol), is a network protocol used for a specific and somewhat obsolete purpose, while ARP (Address Resolution Protocol) serves a different but more commonly used function. Here's an explanation of RARP and the key differences between RARP and ARP:

- **RARP (Reverse ARP):**

1. Purpose: RARP is used to discover the IP address associated with a known MAC (Media Access Control) address. In other words, it performs the reverse of what ARP does. Instead of mapping an IP address to a MAC address (as ARP does), RARP maps a MAC address to an IP address.

2. Usage: RARP was primarily used in older computer networks, particularly diskless workstations and early booting systems, to obtain their IP addresses from a central server or RARP server. This was essential for these systems because they needed an IP address to communicate on the network.

3. Operation: When a device with a known MAC address needs to discover its IP address, it sends a RARP request packet to the RARP server on the local network segment. The RARP server responds with a RARP reply packet containing the IP address associated with the MAC address.

4. Legacy: RARP has largely been replaced by other mechanisms like BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol), which offer more flexibility and functionality for IP address assignment, including the allocation of additional configuration information beyond just the IP address.

- **ARP (Address Resolution Protocol):**

1. Purpose: ARP is used to discover the MAC address associated with a known IP address. It allows devices on a local network segment to map IP addresses to MAC addresses so that they can communicate with each other within the same subnet.

2. Usage: ARP is an integral part of IP networking and is used by devices in local network segments to perform address resolution, enabling them to send data packets to the correct MAC address based on the destination IP address.

3. Operation: When a device needs to find the MAC address corresponding to a specific IP address within its local network, it sends an ARP request packet to the broadcast address of the local network. The device with the matching IP address responds with an ARP reply packet containing its MAC address.

4. Continued Use: ARP remains a fundamental protocol for local network communication and is still widely used today, especially in Ethernet-based LANs.

In summary, RARP and ARP serve opposite purposes when it comes to address resolution. RARP finds the IP address for a known MAC address, primarily for booting purposes, while ARP finds the MAC address for a known IP address, enabling devices to communicate within a local network segment.

****