**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SCHOOL OF COMPUTING**

**SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**

**(DEEMED TO BE UNIVERSITY)**

**CATEGORY - 1 UNIVERSITY BY UGC**

**Accredited “A++” by NAAC I Approved by AICTE**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119**

**Cisco AICTE Virtual Internship Program 2024**

A Cisco AICTE Virtual Internship project report on Networking submitted in partial

fulfillment of the requirements for the AICTE-CISCO virtual Internship in Networking

Program 2024

Submitted By : DASARI NAGENDRA

**AICTE STUDENT ID**  : STU662cf8267f4ee1714223142

**Student ID (Enrolment number)** : 42110251

**Email** : [muralidora504@gmail.com](mailto:muralidora504@gmail.com)

**Contact Info** : 8555874504

**NetPath Illuminator: The Network Odyssey**





**The objective of the " NetPath Illuminator" project is to integrate practical networking lab experiences with the creation of an innovative tool that allows students to explore the packet flow through various network devices and topologies as well as, if possible, extend the vision to create a tool which can provide the Real-Time Packet Journey as well as allow users to query the network events.**

**This tool aims to create a real-time graphical representation of how data packets travel from their source to destination, navigating through the layers of a network, and highlighting the interactions with switches, routers, and across different subnet boundaries.**

**The project will synthesize the learning objectives from the seven networking labs/Levels into the development of a comprehensive system. Students will be able to input their network configurations and observe the dynamic journey of packets as they cross various network segments.**

**Project Description:**

1. **Networking Fundamentals Integration: Students will use knowledge gained from Level 1 to 8 to simulate network environments and visualize the packet flow in those scenarios. The concepts of ARP, MAC (Media Access Control) tables, Switching, IP routing, Routing tables, Static routing and Dynamic routing protocols will all contribute to the representation of packets as they traverse the network.**
2. **Packet Sniffer – Students can use the packet sniffer which is an inbuilt tool in Packet Capture (tutorial available at**

**https://**[**www.youtube.com/watch?v=gsCSKQAVT2M**](http://www.youtube.com/watch?v=gsCSKQAVT2M) **) or a tool like Wireshark to dump packet captures in various Levels in the pcap format.**

1. **Visualization Component: Students can put the packet captures into a database. Additionally, they can design a basic visualization system that graphically displays the packet flow at each Level. It should highlight the path packets take, including intermediate devices they traverse, any routing decisions made, and the final delivery to the destination.**

**Expansion beyond this project's parameters: Students can augment the project by developing an AI-powered packet analyzer. They would train their models using the captured packets. Students can draw inspiration from open-source projects such as Packet Buddy or Packet RAPTOR and incorporate their unique models.**

**Levels:**

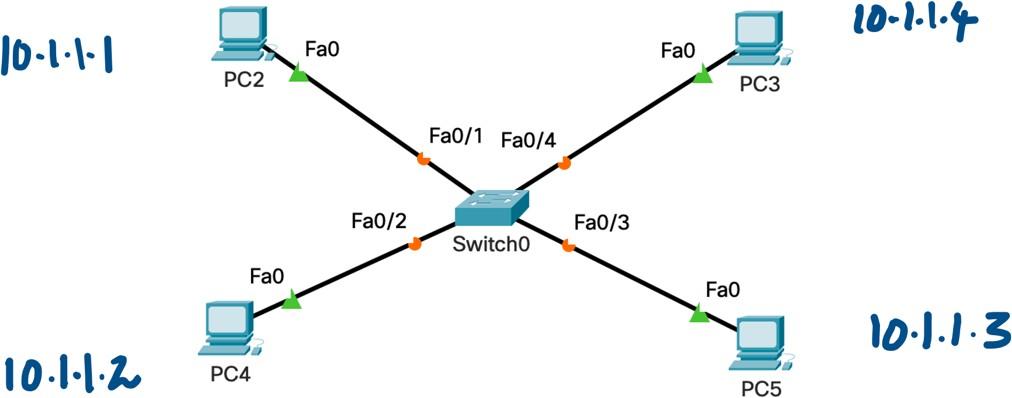
* **Level-1: The objective is to establish a connection between two PCs and assign specific IP addresses to them. The main task is to examine the communication process using the "ping" command. Additionally, we will explore the purpose of Address Resolution Protocol (ARP) and understand why both MAC and IP addresses are necessary. We will also learn about ARP tables and how to view them.**

****

**(Hint: If you are using Cisco Packet Tracer, you can experiment with commands such as "arp -d" and "arp -a" on the computers. These**

**commands allow you to manage the Address Resolution Protocol (ARP) cache. By using "arp -d", you can delete entries from the ARP cache, and with "arp -a", you can view the contents of the ARP cache, which provides information about the IP-to-MAC address mappings.)**

* **Level-2: The objective is to establish a connection between multiple computers using a switch and assign unique IP addresses to each computer. The Level involves performing "ping" tests between neighboring computers to verify connectivity. Also, we will explore the MAC table in the switch and understand its fundamental functionalities such as learning, flooding, and forwarding. Furthermore, we will experiment with basic configuration and view commands on the switch to familiarize ourselves with its operation.**



**The command "show mac address-table" provides a view of the MAC address table entries stored on the switch. It reveals details such as MAC addresses associated with each port, VLAN assignments (where applicable), and the aging time designated for each entry.**

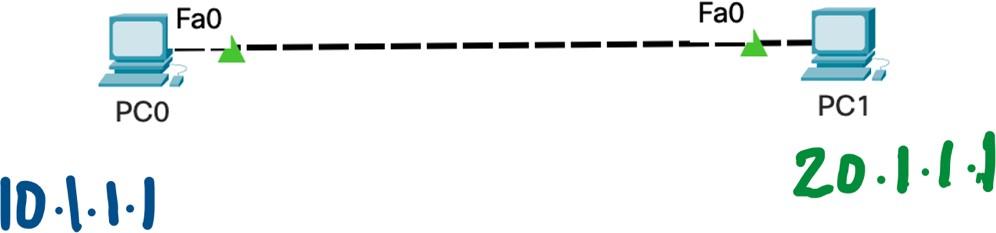
**Additionally, students can delve deeper into the significance of VLANs, their configuration process, and the function of aging timers in network management.**

**To explore different command modes and configurations in Cisco IOS, you can begin with:**

* **User EXEC mode: Accessible upon login, limited to basic commands like 'show' and 'ping'.**
* **Privileged EXEC mode: Entered using 'enable', allows configuration changes and detailed troubleshooting.**
* **Global Configuration mode: Accessed with 'configure terminal', used for device-wide settings such as the switch's name ('hostname Switch1').**
* **Interface Configuration mode: Accessed with 'interface interface\_name', used to configure specific interfaces on the switch ('interface FastEthernet0/1').**
* **Show Commands: Examples include 'show running-config' to display the current configuration of the switch.**
* **Troubleshooting Commands: Such as 'ping' to test connectivity.**

**These commands and modes are essential for configuring, monitoring, and troubleshooting Cisco devices effectively.**

* + **Level-3: In this Level, two computers are connected directly to each other using a wire, and different IP addresses are assigned to them with separate subnets. When attempting to ping one PC from the other, the ping operation fails. The objective is to investigate the reason behind this failed ping, despite the direct connection between the computers.**

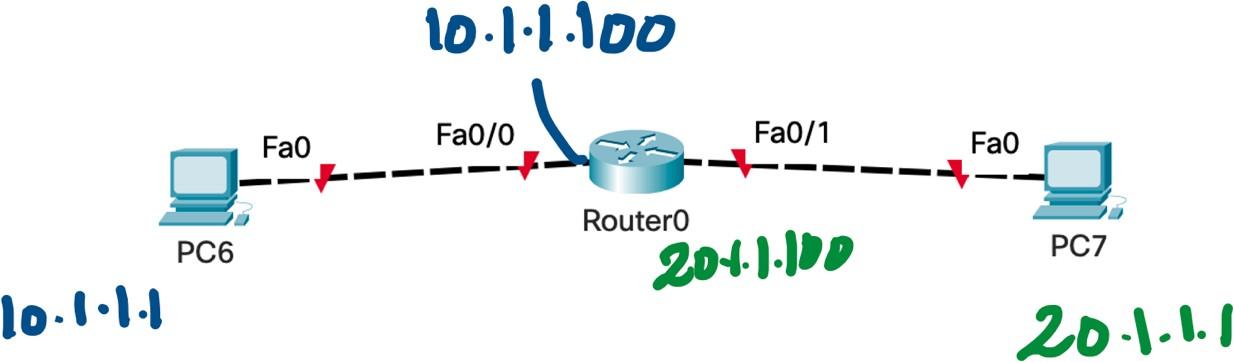


**More Information: We observe that the ARP resolution is not occurring, leading to the failure of the ping. The Address Resolution Protocol (ARP) is responsible for mapping IP addresses to MAC addresses. In this case, since the computers are on different subnets, they are not in the same broadcast domain. As a result, the ARP messages from one PC cannot reach the other PC, preventing the MAC address resolution and subsequent successful communication.**

**This situation highlights the need for routers. Routers are devices that operate at the network layer (Layer 3) of the OSI model and facilitate**

**communication between different subnets or networks. By connecting the two computers through a router, it can perform the necessary routing functions, including ARP resolution between subnets. This enables successful communication between devices on different subnets by forwarding packets between them.**

* + **Level-4: In this Level, the objective is to establish a connection between two computers using a router. The computers are configured to have different IP addresses. The Level involves performing a ping test from one computer to the other. Additionally, we will examine the routing table and route entries using commands such as "show ip route" and "show ip inter brief". This will allow us to understand how routing works and observe the routing entries.**



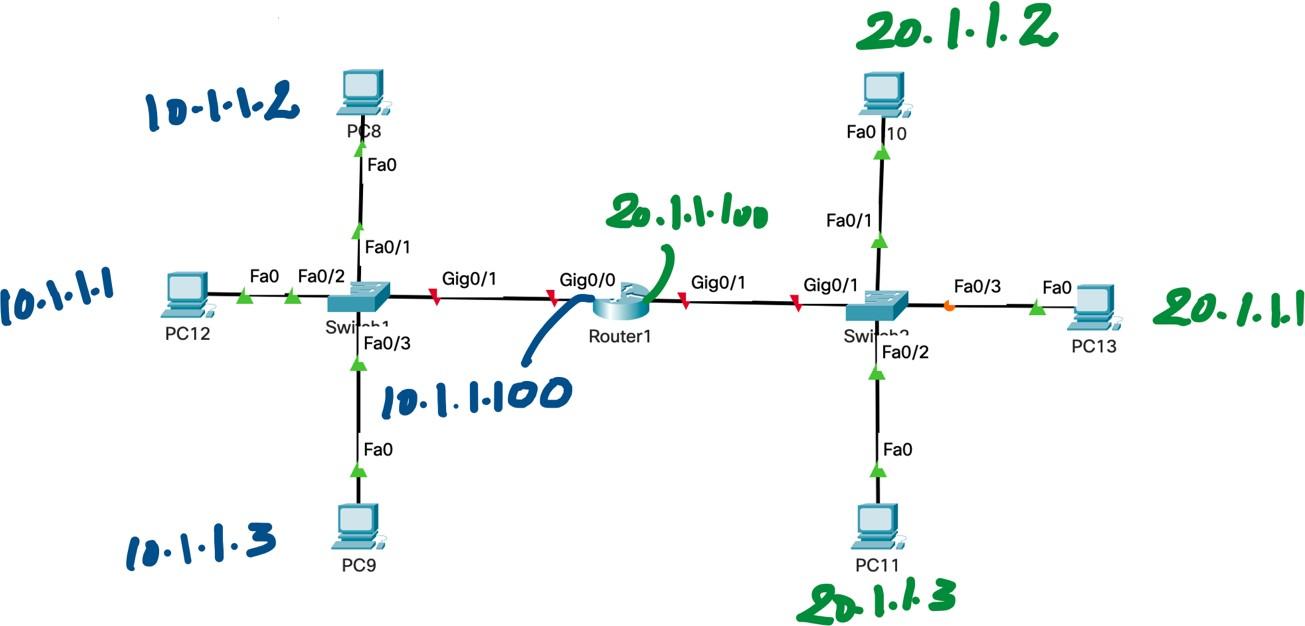
**It is also important to understand the concept of a default gateway and its significance in networking. The default gateway refers to the IP address of the router that serves as the exit point for traffic from a local network to other networks. The need for a default gateway arises when a device within a network needs to communicate with devices outside of its immediate network or subnet. When a device receives a packet destined for an external network, it checks its routing table to determine if it has a specific route for that destination. If there is no specific route available, the device forwards the packet to the default gateway.**

**The default gateway acts as the intermediary, forwarding packets from the local network to external networks, such as the internet. It serves as the entry and exit point for traffic going in and out of the**

**local network, enabling communication with devices located in different networks or subnets.**

**In summary, the default gateway plays a crucial role in enabling network connectivity beyond the local network. It facilitates the routing of packets to external networks, allowing devices to communicate with resources outside of their immediate network.**

* + **Level-5: The objective is to establish connectivity between multiple computers by utilizing two separate networks, a router, and a switch. The setup involves connecting the computers to the switch, which in turn is connected to the router, thereby enabling communication between the two networks.**

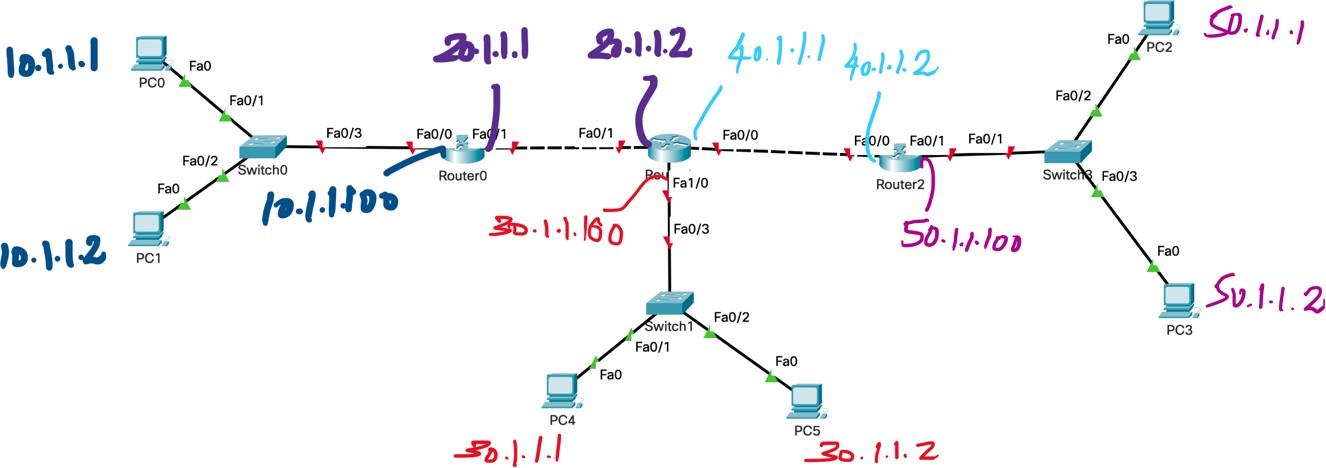
**The Level focuses on understanding how ping operations work between the two networks. By initiating ping commands from computers in one network to computers in the other network, we can examine the functionality of inter-network communication.**

**Additionally, we will explore the routing table in the router, which contains information about network routes and helps determine the best path for forwarding packets between the networks. The ARP table, which maintains IP-to-MAC address mappings, will also be examined to observe how address resolution occurs across the networks.**

**Furthermore, we will investigate the MAC table within the switch. The MAC table stores MAC addresses and associated ports, allowing the switch to efficiently forward frames to the correct destination.**

**By examining the routing table, ARP table, and MAC table, we can gain insights into the network's routing and switching operations, addressing resolution, and how the switch manages and forwards traffic between the connected networks.**

* + **Level-6: The objective is to establish connectivity between different networks using routers. We will configure static routes to connect multiple networks. By utilizing the appropriate router commands, we can configure static routes and examine their configuration using the "show ip route" command.**



**Static routes are manually defined routes that specify the network destinations and next-hop routers to reach those destinations. By configuring static routes, we can direct traffic from one network to another through specific routers.**

**We will explore the routing information base (RIB) within the routers. The RIB is a database that contains routing information, including static routes, dynamic routes, and administrative distance values. It helps the router determine the best path for forwarding packets based on the destination IP address.**

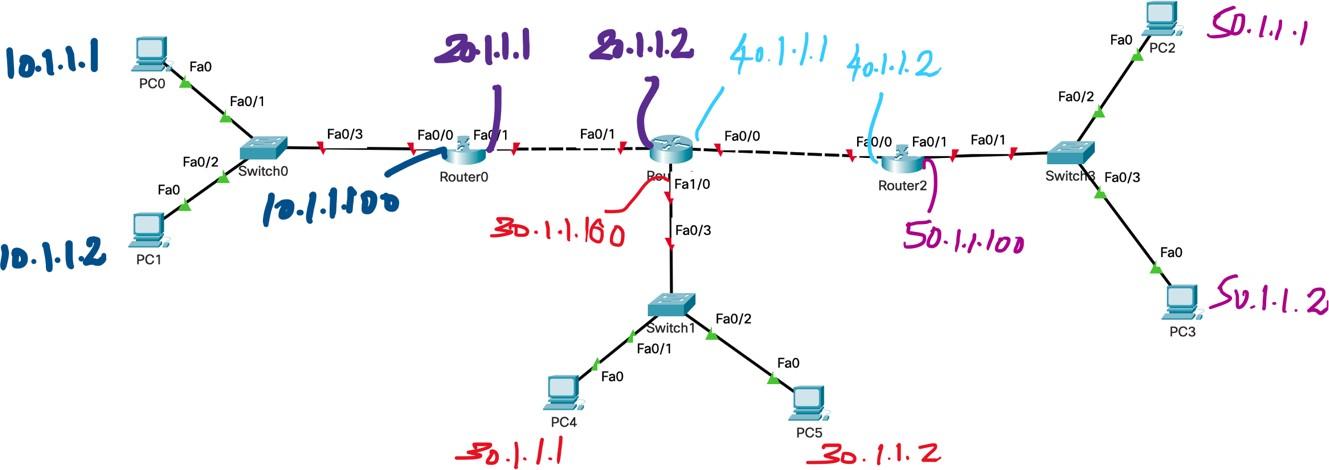
**By using the "show ip route" command, we can view the contents of the RIB and observe the configured static routes. This command**

**provides valuable information about the routing table, including network prefixes, next-hop routers, and administrative distances.**

**Understanding the RIB and how routers work is crucial for comprehending the decision-making process involved in routing packets. Routers analyze the destination IP addresses of incoming packets, consult the RIB, and use various routing protocols or static route configurations to determine the best path for forwarding the packets toward their destinations.**

**By configuring static routes, examining the RIB, and studying the router's operation, we can gain insights into how routers handle packet forwarding and how network connectivity is established between different networks**

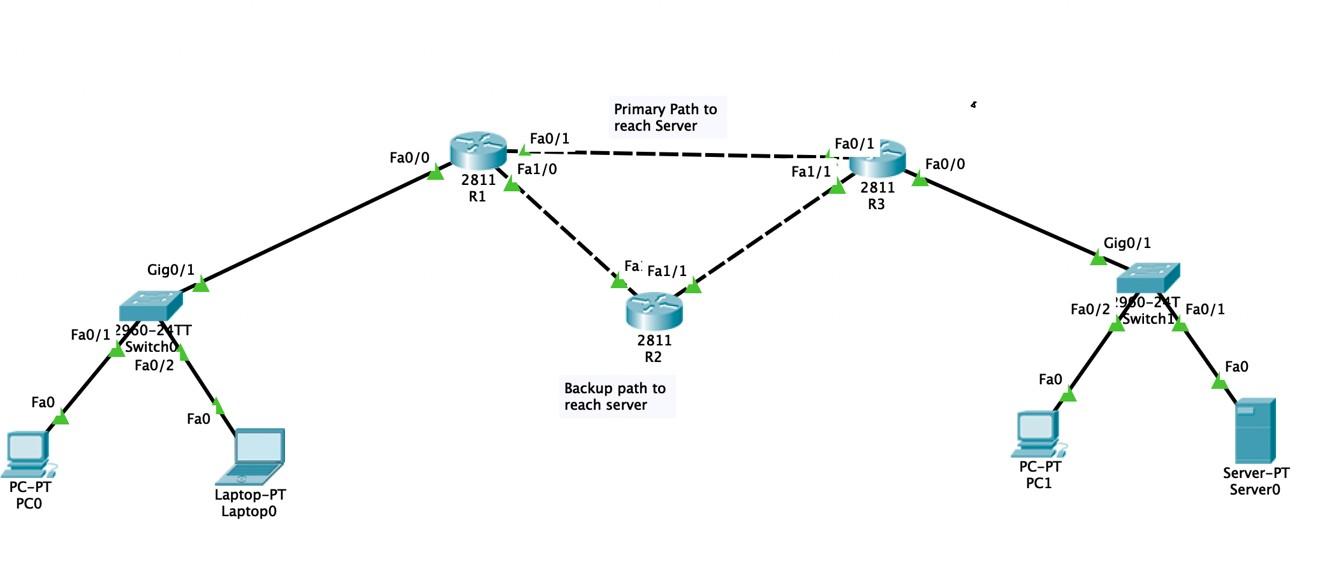
* + **Level-7: The objective is to establish connectivity between multiple networks using routers. We will configure a dynamic routing protocol, such as OSPF (Open Shortest Path First), on each router in the Level. The focus will be on understanding how OSPF operates and how it builds the routing table.**



**We will utilize OSPF-specific show commands to examine how OSPF works. These commands provide insights into OSPF's behavior, including the OSPF Neighbour relationships, the states of OSPF interfaces, and the OSPF routing table. By using the show ip route command, we can check the resulting IP route table, which contains information about OSPF-learned routes and their associated next hops.**

**By configuring OSPF, analyzing the OSPF show commands, examining the IP route table, and reviewing the show ip int brief table, we can gain a deeper understanding of how OSPF facilitates efficient routing within a network and how it dynamically builds the routing table to determine the best paths for packet forwarding.**

**Level-8: To establish network connectivity between multiple networks using routers by configuring OSPF (Open Shortest Path First) on each router. In this level, one needs to have Primary and Backup path (with one extra hop or one can even configure higher cost) to reach the server. With these two paths, one needs to capture the packets to reach to the server and observe the packet flow. Then one needs to shutdown the link Fa0/1 at R1 so that Primary path goes down. Then observe in the packet path. How OSPF dynamically reroutes packets after convergence.**



**Deliverables:**

* + - **Students must simulate all the above network Levels and do capture the commands mentioned.**
    - **Students must utilize a packet sniffer or Wireshark to intercept the packets at each node during every Level Students should analyze the packets captured from different devices (nodes), students can extract relevant information from the packet headers, particularly noting changes occurring in the Ethernet and IP headers. This data will enable them to create a flow diagram illustrating the path of the packet flow from their device (host) to the external network.**
    - **Students are free to select any flowchart creation tool to depict the packet path.**

**(NOTE: Projects are in the GitHub** [**LINK**](https://github.com/nagendra-dasari-2004) **)**

**Assessment Criteria: Upon completion of the above projects, students are expected to -**

* + **Explain the distinction between MAC learning and IP networking**
  + **Differences between Layer 2 and Layer 3 networks.**
  + **Explain the function of subnetting and the workings of the Address Resolution Protocol (ARP).**
  + **Explain the role of a default gateway, the process required for packets to move between subnets, and the initial steps for troubleshooting connectivity issues.**
  + **Should be able to differentiate between a router and a switch in more practical manner.**
  + **Should be able to articulate the purpose of static routing and the method by which network connectivity is established across different networks.**
  + **What does Routing Information Base (RIB) mean**
  + **One should be able to define what a routing protocol is, the differences between static and dynamic routing protocols, and provide an example of a dynamic routing protocol.**
  + **Explain how the ping function works? Additionally, elaborate on the significance of the ICMP protocol? Develop a ping program using C/C++. Implementing a basic ping program involves using sockets to send ICMP (Internet Control Message Protocol) echo requests and handle ICMP echo replies.**
  + **Explain the basic flow of packet from PC to a web server located outside the campus.**

**By completing the "NetPath Illuminator" project, students will gain a practical understanding of networking concepts, apply their theoretical knowledge to a real-world application.**

**(NOTE: Assignment solution are placed down)**

**1.Explain the distinction between MAC learning and IP networking**

| **S.NO** | **MAC Address** | **IP Address** |
| --- | --- | --- |
| 1. | MAC Address stands for Media Access Control Address. | IP Address stands for Internet Protocol Address. |
| 2. | MAC Address is a six byte hexadecimal address. | IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address. |
| 3. | A device attached with MAC Address can retrieve by ARP protocol. | A device attached with IP Address can retrieve by RARP protocol. |
| 4. | [NIC](https://www.geeksforgeeks.org/nic-full-form/) Card’s Manufacturer provides the MAC Address. | Internet Service Provider provides IP Address. |
| 5. | MAC Address is used to ensure the physical address of a computer. | IP Address is the logical address of the computer. |
| 6. | MAC Address operates in the data link layer. | IP Address operates in the network layer. |
| 7. | MAC Address helps in simply identifying the device. | IP Address identifies the connection of the device on the network. |
| 8. | MAC Address of computer cannot be changed with time and environment. | IP Address modifies with the time and environment. |
| 9. | MAC Addresses can’t be found easily by a third party. | IP Addresses can be found by a third party. |
| 10. | It is a 48-bit address that contains 6 groups of 2 hexadecimal digits, separated by either hyphens (-) or colons(.).  Example:  00:FF:FF:AB:BB:AA  or  00-FF-FF-AB-BB-AA | IPv4 uses 32-bit addresses in dotted notations, whereas IPv6 uses 128-bit addresses in hexadecimal notations.  Example:  IPv4 192.168.1.1  IPv6  FFFF:F200:3204:0B00 |
| 11. | No classes are used for MAC addressing. | IPv4 uses A, B, C, D, and E classes for IP addressing. |
| 12. | MAC Address sharing is not allowed. | In IP address multiple client devices can share the IP address. |
| 13. | MAC address help to solve IP address issue. | IP addresses never able to solve MAC address issues. |
| 14. | MAC addresses can be used for broadcasting. | The IP address can be used for broadcasting or multicasting. |
| 15. | MAC address is hardware oriented. | IP address is software oriented. |
| 16. | While communication, Switch needs MAC address to forward data. | While communication, Router need IP address to forward data. |

**2.Differences between Layer 2 and Layer 3 networks.**

*Layer 2*, known as the Data Link Layer, provides node-to-node data transfer with MAC address identification. All nodes on a layer 2 network are visible to one another. Ethernet switches are a common layer 2 example.

*Layer 3*, known as the Network Layer routes data packets to specific nodes identified by IP addresses. Visibility amongst nodes is point-to-point. As its function suggests, routers are a common layer 3 example.

Both have merits for different applications.

Layer 2 is beneficial for remote support. Enabling both the full functionality of most industrial protocols that sit atop ethernet *and* the ability to search for active IP nodes puts the programmer next to the machine, albeit virtually. There is no functional difference in this example between a layer 2 network and an ethernet cord.

Layer 3 provides a more scalable network infrastructure, like that used in a globally distributed system of machines connected to a central cloud for data analytics. Because data packets are *routed,* layer 3 enables 1-1 NAT and VLAN, among other traditional networking strategies. As distributed networks scale, layer 3 becomes more practical for managing connections.

**3.Explain the function of subnetting and the workings of the Address Resolution Protocol (ARP).**

An IP address is the *logical* addressing scheme for nodes on a network. IP Addresses exist at the Network layer of the OSI Model and help facilitate the L3 goal of “*end to end*” delivery.

A MAC address is the *physical* addressing scheme for individual NIC cards on each node of a network. MAC addresses exist at the Data Link layer of the OSI Model and help facilitate the L2 goal of “*hop to hop*” delivery.

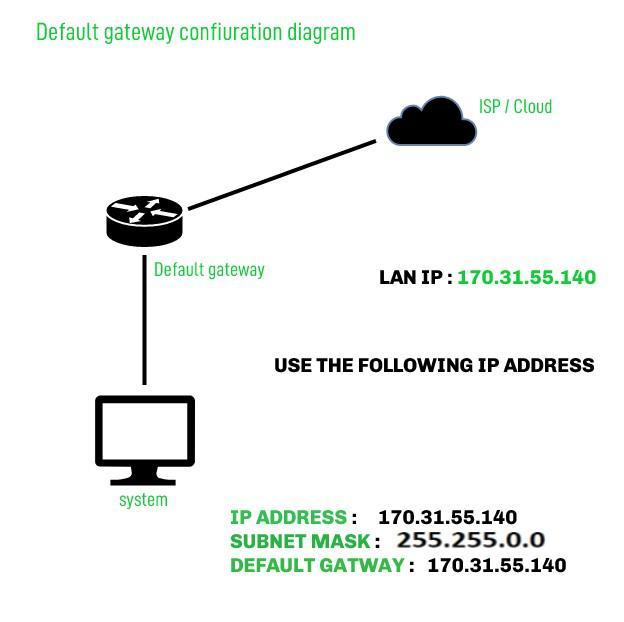
**4.Explain the role of a default gateway, the process required for packets to move between subnets, and the initial steps for troubleshooting connectivity issues.**

**Default Gateway:**

* The default gateway is the node that forwards the packet from the source to other networks when there is no routing information about the destination i.e. host (or router) does not know where the destination is present.
* A default gateway is a route to which information is passed when the device does not know where the destination is present.
* It is used when there is no routing information available about the destination.
* It is a node that allows the communication of computers on different networks.
* ‘Default’ here means the default route which is to be taken when the host does not know where the destination is.
* It is most commonly used for webpage access.
* This is an important part of networking for routing the data and finding the corresponding destination which is in another network.

**When Default Gateway is Used:**

When the source wants to reach a destination which is outside its network then, the source uses the default gateway to forward the data and locate the destination’s network so that data should reach its intended destination. The default gateways are used when the host doesn’t know about the destination’s network i.e. the network in which the destination is present or when the route information is not available for any destination then it goes to the default gateway so that it can identify in which network the destination is and can forward the data through that route. The default gateway is an important device for the data forwarding and routing of the data on the other network. It helps in the communication of one network computer with the other network computer.



**How to Find Your Default Gateway:**

**1. In Windows:**

1. In Windows, we can get our default gateway with Command Prompt.
2. To access the command prompt click on start and search for “**CMD**” and open.
3. In the command prompt window type “**ipconfig**” command and press enter and you can see the Default Gateway in the information generated by the command with the machine’s IP address listed.

**2. In Linux:**

* Open the terminal and use the command “**ip route | grep default**“. It will locate the default gateway.

**5.Should be able to differentiate between a router and a switch in more practical manner**

**Router:**

The router is a networking device that works at the network layer i.e., a third layer of the ISO-OSI model, and is the multiport device. It establishes a simple connection between the networks to provide the data flow between the networks. Router transfers data in the form of packets is used in LAN as well as MAN.

It works on network layer 3 and is used in LANs, MANs, and WANs. It stores IP addresses and maintains addresses on its own.

**Switch:**

It is a point-to-point communication device. Basically, it is a kind of bridge that provides better connections. It is a kind of device that sets up and stops the connections according to the requirements needed at that time. It comes up with many features such as flooding, filtering, and frame transmission.

| **Router** | **Switch** |
| --- | --- |
| The main objective of router is to connect various networks simultaneously. | While the main objective of switch is to connect various devices simultaneously. |
| It works in network layer | While it works in data link layer |
| Router is used by LAN as well as MAN | While switch is used by only LAN. |
| Through the router, data is sent in the form of packets. | While through switch data is sent in the form of  frame. |
| There is less collision taking place in the router. | While there is no collision taking place in full duplex switch. |
| Router is compatible with NAT | While it is not compatible with NAT. |
| Router is a relatively much more expensive device than switch. | Switch is an expensive device than hub. but cheaper than router. |
| maximum speed for wireless is 1-10 Mbps and maximum speed for wired connections is 100 Mbps. | Maximum speed is 10Mbps to 100Mbps. |
| Router needs at least two networks to connect. | Switch needs at least single network is to connect. |
| The types of routing are Adaptive and Non-Adaptive . | The types of switching are: Circuit, Packets and Message Switching. |

**6.Should be able to articulate the purpose of static routing and the method by which network connectivity is established across different networks.**

Static routing is a routing protocol that helps to keep your network organized and to optimize routing performance. It enables the router to assign a specific path to each network segment and to keep track of network changes. This helps to improve network stability and continuity. This adds security because a single administrator can only authorize routing to particular networks.

**Steps to Configure and Verify Two Router Connections in Cisco Packet Tracer :**

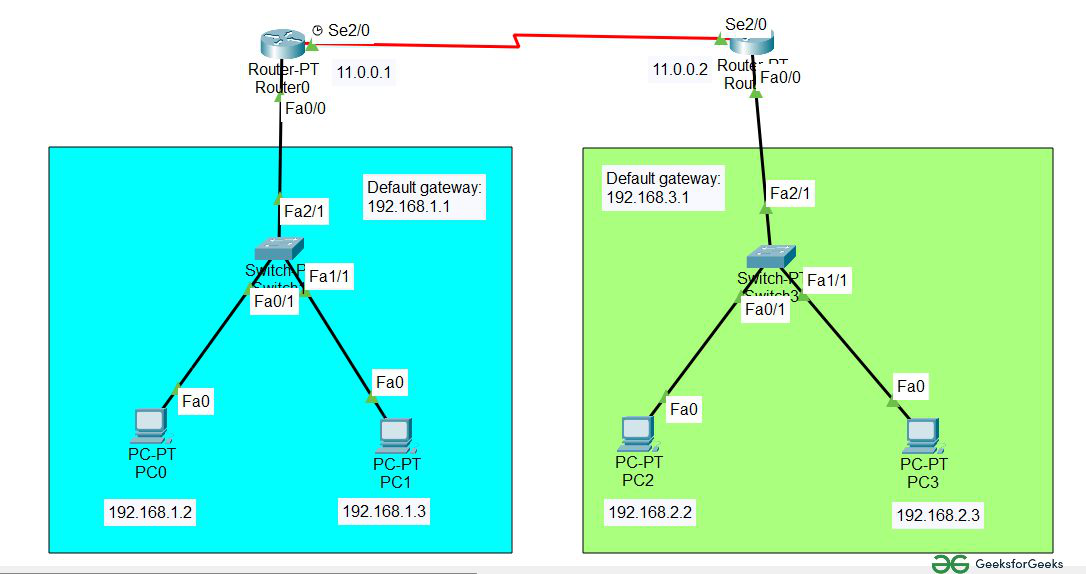
**Step 1**: First, open the cisco packet tracer desktop and select the devices given below:

| **S.NO** | **Device** | **Model Name** | **Qty.** |
| --- | --- | --- | --- |
| **1.** | PC | PC | 4 |
| **2.** | Switch | PT-Switch | 2 |
| **3.** | Router | PT-Router | 2 |

**IP Addressing Table For PCs:**

| **S.NO** | **Device** | **IPv4 Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| **1.** | pc0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| **2.** | pc1 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| **3.** | pc2 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |
| **4.** | pc3 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 |

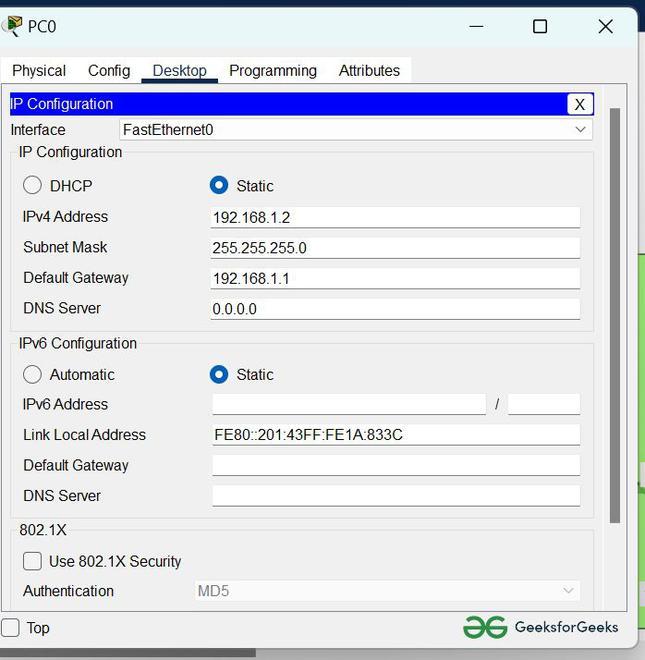
* Then, create a network topology as shown below the image.
* Use an Automatic connecting cable to connect the devices with others.

**

*Correction: Default Gateway in 2nd network is 192.168.2.1*

**Step 2:**Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing table given above.

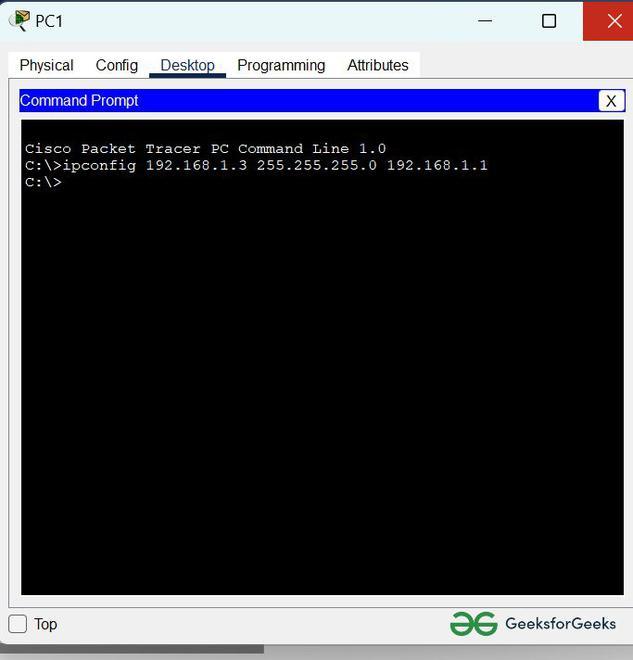
* To assign an IP address in PC0, click on PC0.
* Then, go to desktop and then IP configuration and there you will IPv4 configuration.
* Fill IPv4 address and subnet mask.



**Step 3:** Assigning IP address using the ipconfig command.

* We can also assign an IP address with the help of a command.
* Go to the command terminal of the PC.
* Then, type ipconfig <IPv4 address><subnet mask><default gateway>(if needed)

*Example: ipconfig 192.168.1.3  255.255.255.0 192.168.1.1*

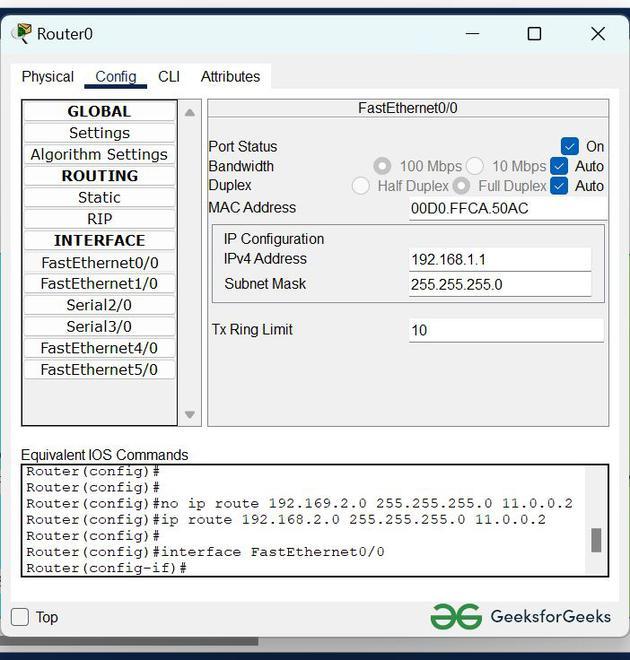


* Repeat the same procedure with other PCs to configure them thoroughly.

**Step 4:** Configure router with IP address and subnet mask.

| **S.NO** | **Device** | **Interface** | **IPv4 Addressing** | **Subnet Mask** |
| --- | --- | --- | --- | --- |
| **1.** | router0 | FastEthernet0/0 | 192.168.1.1 | 255.255.255.0 |
| Serial2/0 | 11.0.0.1 | 255.255.255.0 |
| **2.** | router1 | FastEthernet0/0 | 192.168.2.1 | 255.255.255.0 |
| Serial2/0 | 11.0.0.2 | 255.255.255.0 |

* To assign an IP address in router0, click on router0.
* Then, go to config and then Interfaces.
* Then, configure the IP address in FastEthernet and serial ports according to IP addressing Table.
* Fill IPv4 address and subnet mask.



* Repeat the same procedure with other routers to configure them thoroughly.

**Step 5:** After configuring all of the devices we need to assign the routes to the routers.

To assign static routes to the particular router:

* First, click on router0 then Go to CLI.
* Then type the commands and IP information given below.

*CLI command : ip route <network id> <subnet mask><next hop>*

Static Routes for Router0 are given below:

*Router(config)#ip route 192.168.2.0 255.255.255.0 11.0.0.2*

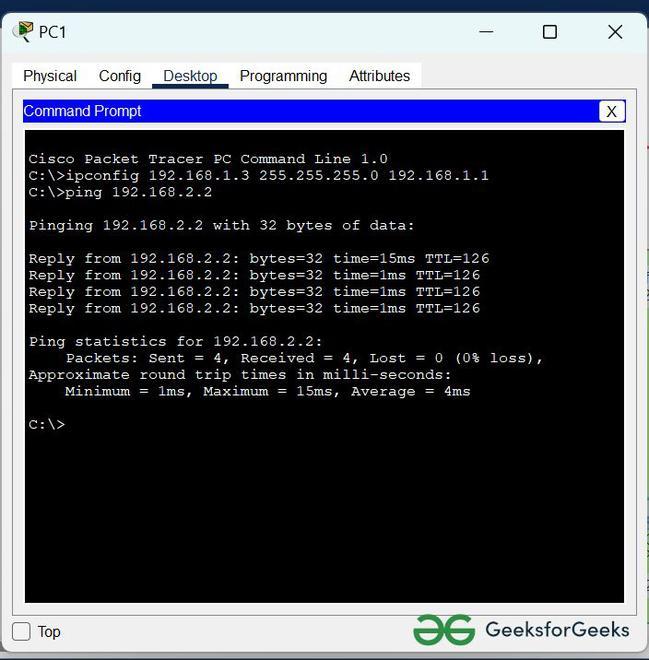
Static Routes for Router1 are given below:

*Router(config)#ip route 192.168.1.0 255.255.255.0 11.0.0.1*

**Step 6:** Verifying the network by pinging the IP address of any PC. We will use the ping command to do so.

* First, click on PC1 then Go to the command prompt
* Then type ping <IP address of targeted node>
* As we can see in the below image we are getting replies which means the connection is working very fine

*Example : ping 192.168.2.2*



**7.What does Routing Information Base (RIB) mean**

The entire set of BGP routes learned and advertised by a BGP router make up its BGP Routing Information Base (RIB). Conceptually the BGP RIB can be divided into 3 parts:

* RIB-IN
* LOC-RIB
* RIB-OUT

The RIB-IN (or Adj-RIBs-In as defined in RFC 4271) holds the BGP routes that were received from peers and that the router decided to keep (store in its memory).

The LOC-RIB contains modified versions of the BGP routes in the RIB-IN. The path attributes of a RIB-IN route can be modified using BGP import policies. All of the LOC-RIB routes for the same NLRI are compared in a procedure called the BGP decision process that results in the selection of the best path for each NLRI. The best paths in the LOC-RIB are the ones that are actually ‛usable’ by the local router for forwarding, filtering, auto-discovery, and so on.

The RIB-OUT (or Adj-RIBs-Out as defined in RFC 4271) holds the BGP routes that were advertised to peers. Normally a BGP route is not advertised to a peer (in the RIB-OUT) unless it is ‛used’ locally but there are exceptions. BGP export policies modify the path attributes of a LOC-RIB route to create the path attributes of the RIB-OUT route. A particular LOC-RIB route can be advertised with different path attribute values to different peers so there can exist a 1:N relationship between LOC-RIB and RIB-OUT routes.

**8.One should be able to define what a routing protocol is, the differences between static and dynamic routing protocols, and provide an example of a dynamic routing protocol.**

| **Features** | **Static Routing** | **Dynamic Routing** |
| --- | --- | --- |
| **Definition** | It happens when a router utilizes a manually specified routing entry rather than information from dynamic routing traffic. | It is a method in which a router may transmit data via a different route or to a specific  destination based on the current state of the network's communication circuits. |
| **Configuration Technique** | The routing tables are manually updated in static routing. | The tables are automatically updated in dynamic routing. |
| **Routes** | Routes are specified by the administrative. | The routes are updated according to the modifications in the network. |
| **Routing Algorithms** | It doesn't utilize any complicated routing algorithms. | It utilizes complicated routing algorithms. |
| **Link Affect** | When a link fails in static routing, it interrupts the other routing path. | The link failure doesn't affect rerouting in dynamic routing. |
| **Bandwidth** | It needs less bandwidth. | It needs more bandwidth. |
| **Security** | It offers high security. | It offers less security. |
| **Network Infrastructure** | Its network infrastructure is minimal. | Its network infrastructure is large. |
| **Routing Protocols** | It doesn't utilize any protocol. | It employs protocols such as eigrp, arp, and others to calculate the routing process. |
| **Additional Resources** | It doesn't need any extra resources. | It needs extra resources to hold the information. |
| **Implementation** | It is implemented in small networks. | It is implemented in large networks. |
| **Routing table building** | Routing locations are hand-typed in static routing. | In dynamic routing, locations are dynamically filled in the table. |

**9.Explain how the ping function works? Additionally, elaborate on the significance of the ICMP protocol? Develop a ping program using C/C++. Implementing a basic ping program involves using sockets to send ICMP (Internet Control Message Protocol) echo requests and handle ICMP echo replies.**

Ping is a necessity for debugging the Internet. Ping is a basic Internet tool that allows a user to verify that a particular IP address exists and can accept requests., with other facilities.

Ping sends out ICMP packets by opening a RAW Socket, which is separate from TCP and UDP. Since IP does not have any inbuilt mechanism for sending error and control messages. It depends on Internet control message protocol (ICMP) to provide error control. It is used for reporting errors and management queries.

// C program to Implement Ping

#include& lt; stdio.h & gt;

#include& lt; sys / types.h & gt;

#include& lt; sys / socket.h & gt;

#include& lt; netinet / in.h & gt;

#include& lt; arpa / inet.h & gt;

#include& lt; netdb.h & gt;

#include& lt; unistd.h & gt;

#include& lt; string.h & gt;

#include& lt; stdlib.h & gt;

#include& lt; netinet / ip\_icmp.h & gt;

#include& lt; time.h & gt;

#include& lt; fcntl.h & gt;

#include& lt; signal.h & gt;

#include& lt; time.h & gt;

#define PING\_PKT\_S 64

#define PORT\_NO 0

#define PING\_SLEEP\_RATE 1000000 x

#define RECV\_TIMEOUT 1

int pingloop = 1;

struct ping\_pkt {

struct icmphdr hdr;

char msg[PING\_PKT\_S - sizeof(struct icmphdr)];

};

unsigned short checksum(void\* b, int len)

{

unsigned short\* buf = b;

unsigned int sum = 0;

unsigned short result;

for (sum = 0; len & gt; 1; len -= 2)

sum += \*buf++;

if (len == 1)

sum += \*(unsigned char\*)buf;

sum = (sum & gt; > 16) + (sum & amp; 0xFFFF);

sum += (sum & gt; > 16);

result = ~sum;

return result;

}

void intHandler(int dummy) { pingloop = 0; }

char\* dns\_lookup(char\* addr\_host,

struct sockaddr\_in\* addr\_con)

{

printf("\nResolving DNS..\n & quot;);

struct hostent\* host\_entity;

char\* ip = (char\*)malloc(NI\_MAXHOST \* sizeof(char));

int i;

if ((host\_entity = gethostbyname(addr\_host)) == NULL) {

// No ip found for hostname

return NULL;

}

strcpy(ip,

inet\_ntoa(\*(struct in\_addr\*)host\_entity - >

h\_addr));

(\*addr\_con).sin\_family = host\_entity - >

h\_addrtype;

(\*addr\_con).sin\_port = htons(PORT\_NO);

(\*addr\_con).sin\_addr.s\_addr = \*(long\*)host\_entity - >

h\_addr;

return ip;

}

char\* reverse\_dns\_lookup(char\* ip\_addr)

{

struct sockaddr\_in temp\_addr;

socklen\_t len;

char buf[NI\_MAXHOST], \*ret\_buf;

temp\_addr.sin\_family = AF\_INET;

temp\_addr.sin\_addr.s\_addr = inet\_addr(ip\_addr);

len = sizeof(struct sockaddr\_in);

if (getnameinfo((struct sockaddr\*)&

temp\_addr, len, buf, sizeof(buf), NULL,

0, NI\_NAMEREQD)) {

printf(

"

Could not resolve reverse lookup of hostname\n

& quot;);

return NULL;

}

ret\_buf

= (char\*)malloc((strlen(buf) + 1) \* sizeof(char));

strcpy(ret\_buf, buf);

return ret\_buf;

}

void send\_ping(int ping\_sockfd,

struct sockaddr\_in\* ping\_addr,

char\* ping\_dom, char\* ping\_ip,

char\* rev\_host)

{

int ttl\_val = 64, msg\_count = 0, i, addr\_len, flag = 1,

msg\_received\_count = 0;

char rbuffer[128];

struct ping\_pkt\* r\_pckt;

struct ping\_pkt pckt;

struct sockaddr\_in r\_addr;

struct timespec time\_start, time\_end, tfs, tfe;

long double rtt\_msec = 0, total\_msec = 0;

struct timeval tv\_out;

tv\_out.tv\_sec = RECV\_TIMEOUT;

tv\_out.tv\_usec = 0;

clock\_gettime(CLOCK\_MONOTONIC, & tfs);

if (setsockopt(ping\_sockfd, SOL\_IP, IP\_TTL, &

ttl\_val, sizeof(ttl\_val))

!= 0) {

printf(

"\nSetting socket options to TTL failed !\n

& quot;);

return;

}

else {

printf("\nSocket set to TTL..\n & quot;);

}

setsockopt(ping\_sockfd, SOL\_SOCKET, SO\_RCVTIMEO,

(const char\*)&

tv\_out, sizeof tv\_out);

while (pingloop) {

flag = 1;

bzero(& pckt, sizeof(pckt));

pckt.hdr.type = ICMP\_ECHO;

pckt.hdr.un.echo.id = getpid();

for (i = 0; i & lt; sizeof(pckt.msg) - 1; i++)

pckt.msg[i] = i + '0';

pckt.msg[i] = 0;

pckt.hdr.un.echo.sequence = msg\_count++;

pckt.hdr.checksum

= checksum(& pckt, sizeof(pckt));

usleep(PING\_SLEEP\_RATE);

clock\_gettime(CLOCK\_MONOTONIC, & time\_start);

if (sendto(ping\_sockfd, &

pckt, sizeof(pckt), 0,

(struct sockaddr\*)ping\_addr,

sizeof(\*ping\_addr))& lt;

= 0) {

printf("\nPacket Sending Failed !\n

& quot;);

flag = 0;

}

addr\_len = sizeof(r\_addr);

if (recvfrom(ping\_sockfd,

rbuffer, sizeof(rbuffer), 0,

(struct sockaddr\*)&

r\_addr, & addr\_len)& lt;

= 0 & amp; & msg\_count & gt; 1) {

printf("\nPacket receive failed !\n

& quot;);

}

else {

clock\_gettime(CLOCK\_MONOTONIC, & time\_end);

double timeElapsed

= ((double)(time\_end.tv\_nsec

- time\_start.tv\_nsec))

/ 1000000.0 rtt\_msec

= (time\_end.tv\_sec - time\_start.tv\_sec)

\* 1000.0

+ timeElapsed;

if (flag) {

if (!(r\_pckt->hdr.type == 0 & amp; &

r\_pckt->hdr.code == 0)) {

printf(" Error..Packet received

with ICMP type

% d code % d\n

& quot;

, r\_pckt->hdr.type, r\_pckt->hdr.code);

}

else {

printf(" % d bytes from

% s(h

:

% s)(% s) msg\_seq

= % d ttl = % d rtt =

% Lf ms.\n & quot;

, PING\_PKT\_S, ping\_dom, rev\_host,

ping\_ip, msg\_count, ttl\_val,

rtt\_msec);

msg\_received\_count++;

}

}

}

}

clock\_gettime(CLOCK\_MONOTONIC, & tfe);

double timeElapsed

= ((double)(tfe.tv\_nsec - tfs.tv\_nsec)) / 1000000.0;

total\_msec = (tfe.tv\_sec - tfs.tv\_sec) \* 1000.0

+ timeElapsed

printf("\n == = % s ping statistics ==

=\n & quot;

, ping\_ip);

printf("\n % d packets sent, % d packets received,

% f percent packet loss.Total time

:

% Lf ms.\n\n & quot;

, msg\_count, msg\_received\_count,

((msg\_count - msg\_received\_count) / msg\_count)

\* 100.0,

total\_msec);

}

int main(int argc, char\* argv[])

{

int sockfd;

char \*ip\_addr, \*reverse\_hostname;

struct sockaddr\_in addr\_con;

int addrlen = sizeof(addr\_con);

char net\_buf[NI\_MAXHOST];

if (argc != 2) {

printf("\nFormat % s & lt;

address & gt;\n & quot;, argv[0]);

return 0;

}

ip\_addr = dns\_lookup(argv[1], & addr\_con);

if (ip\_addr == NULL) {

printf(

"\nDNS lookup

failed !Could not resolve hostname !\n

& quot;);

return 0;

}

reverse\_hostname = reverse\_dns\_lookup(ip\_addr);

printf("\nTrying to connect to '%s' IP

:

% s\n & quot;, argv[1], ip\_addr);

printf("\nReverse Lookup domain

:

% s & quot;, reverse\_hostname);

// socket()

sockfd = socket(AF\_INET, SOCK\_RAW, IPPROTO\_ICMP);

if (sockfd & lt; 0) {

printf(

"\nSocket file descriptor not received !!\n

& quot;);

return 0;

}

else

printf("\nSocket file descriptor % d received\n

& quot;

, sockfd);

signal(SIGINT, intHandler); // catching interrupt

// send pings continuously

send\_ping(sockfd, &

addr\_con, reverse\_hostname, ip\_addr, argv[1]);

return 0;

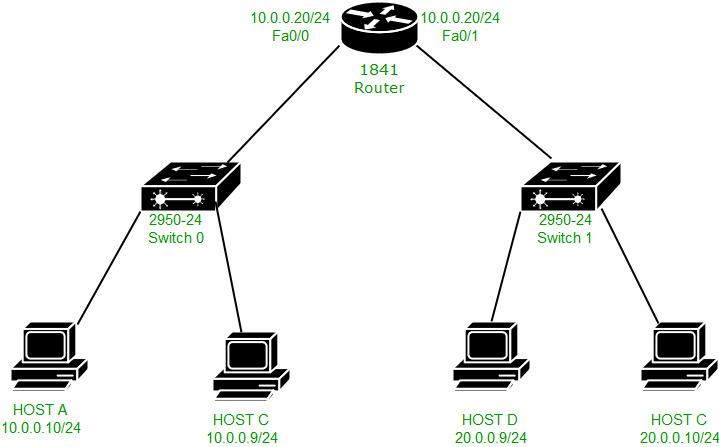
}

**10.Explain the basic flow of packet from PC to a web server located outside the campus.**

To deliver the packet to the destination host, the source IP, destination IP, source MAC address and destination MAC address should be known. Some basic rules for the packet flow:

1. If the destination host is present in the same network, then the packet is delivered directly to the destination host.
2. If the destination host is present in a different network then the packet is delivered to the default gateway first which in turn delivers the packet to the destination host.
3. If ARP is not resolved then ARP will be resolved first.
4. MAC address never crosses its broadcast domain.

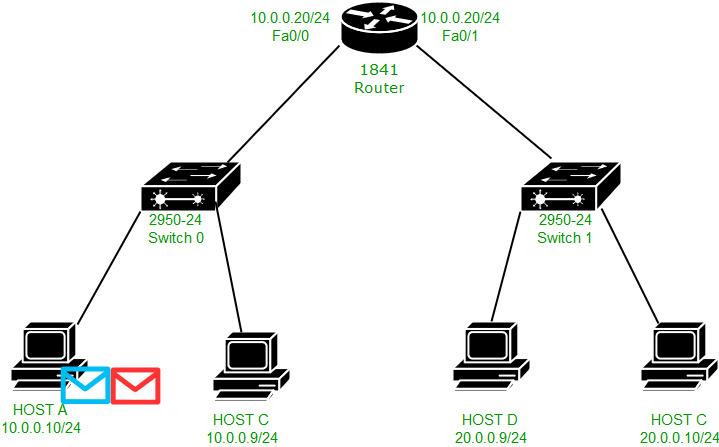
**Explanation –**



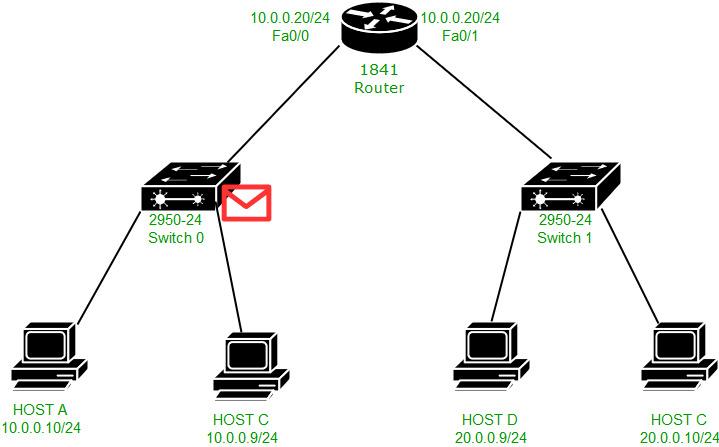
Here is a topology, in which there is host A (IP address – 10.0.0.10 and MAC address – 000D.BD22.7C22), host C (IP address – 10.0.0.9), host B (IP address – 20.0.0.10), host C (IP address-20.0.0.9 and MAC address – 00E0.A3E2.03DC) and the router (IP address – 10.0.0.20 and MAC address – 000B.BE8E.5201 on fa0/0,IP address – 20.0.0.20 and MAC address – 000B.BE8E.5202 on fa0/1 ).

Now we will try to ping from host A (IP address – 10.0.0.10) to host B (IP address – 20.0.0.10). First, **AND operation** is performed by source host between source IP address, source subnet mask, and destination IP address, source subnet mask to know if the destination is present in same or different network.

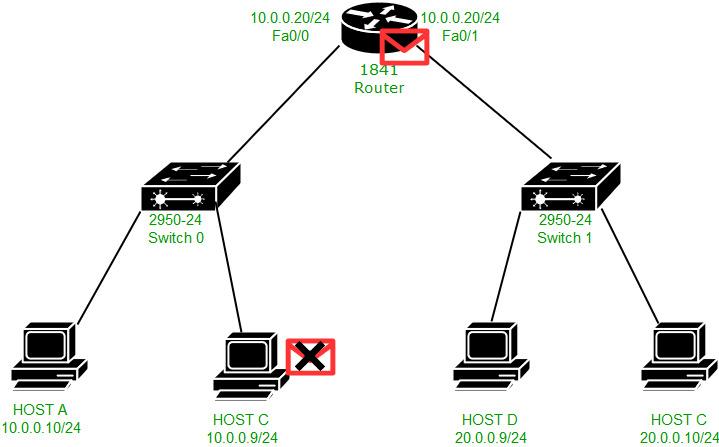
If the result is the same then the destination is in the same network otherwise in a different network. Here, the destination is present in different networks, therefore, the result will be different and the packet will be delivered to a default gateway.



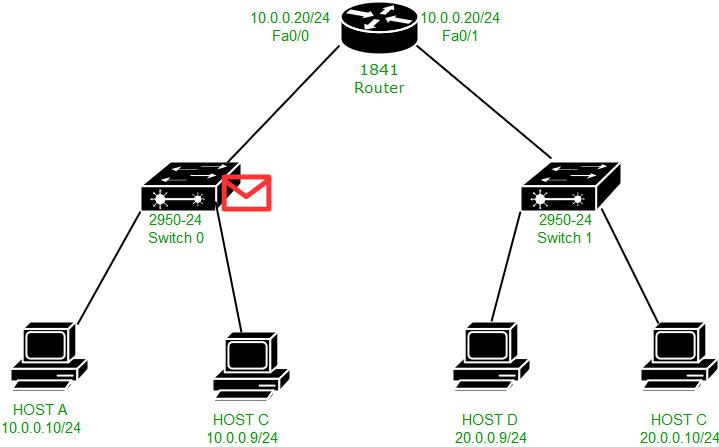
We see that 2 messages are generated ICMP(purple) and ARP(green). ARP has been generated because ARP has not been resolved.

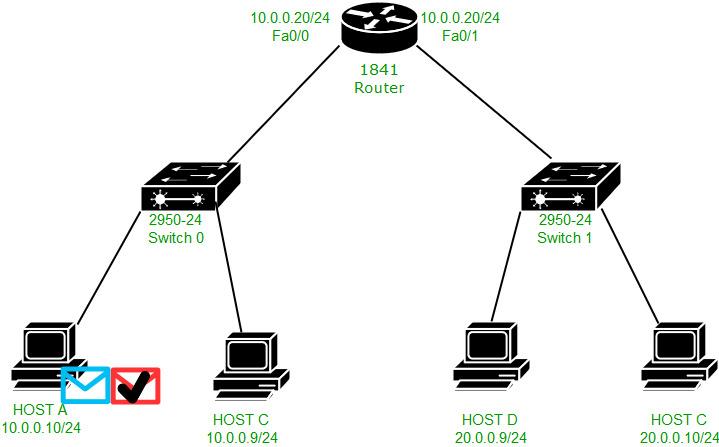


Now as the ARP should be resolved first, therefore the ARP request will be broadcast which is received by switch:

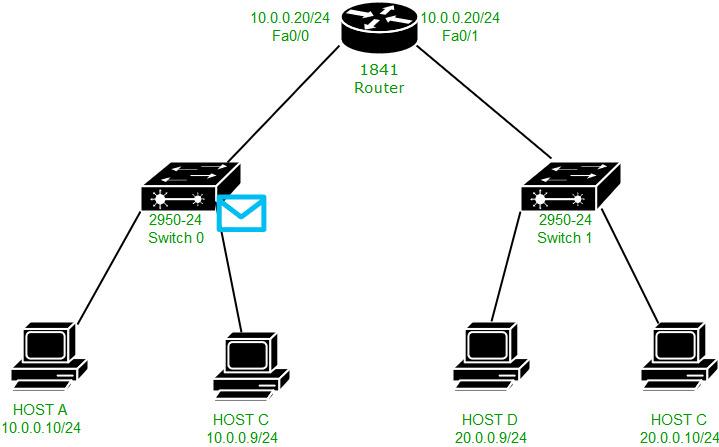


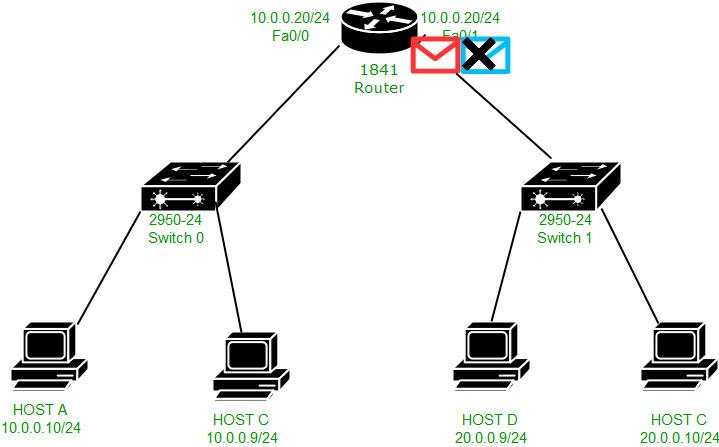
The switch in turn broadcast the ARP request to the host and the router. The PC discards the request and the router accepts it.





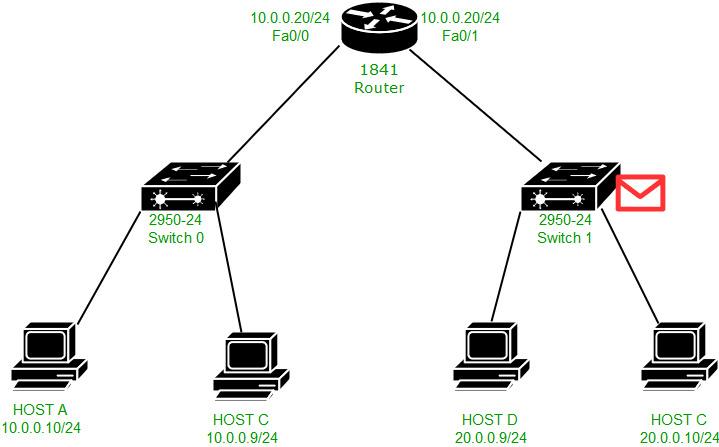
Now the ARP reply is unicast to host A by the router as shown in the above figure.

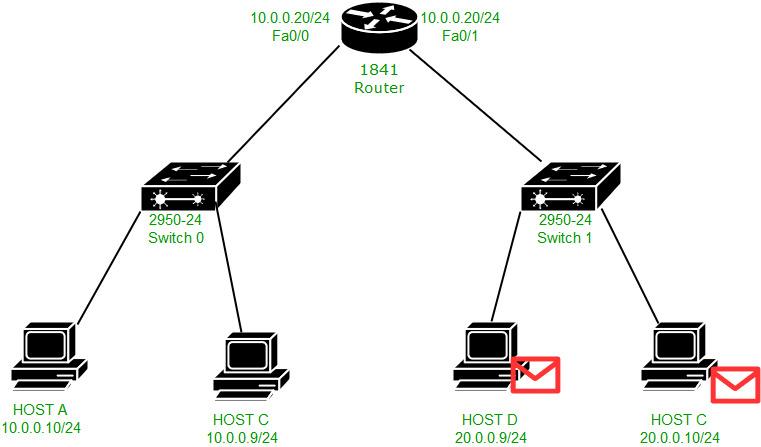




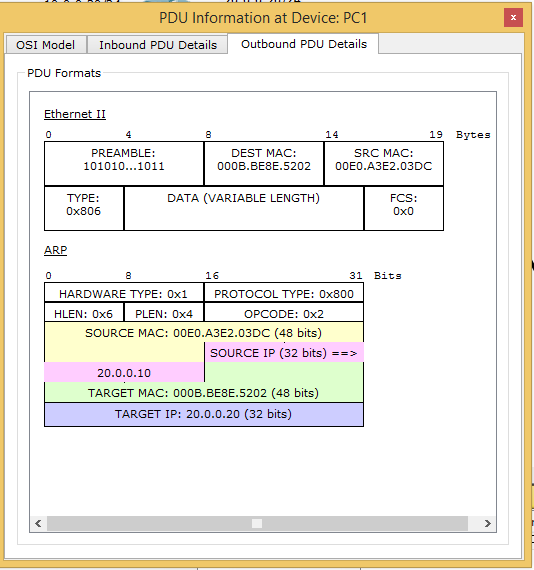
Now the ICMP packet will be unicast to the default gateway (IP address – 10.0.0.20 and MAC address – 000B.BE8E.5201) as shown in the above figures.

**Note –** The ICMP packet will be unicast to the default gateway as the ARP has been resolved now.



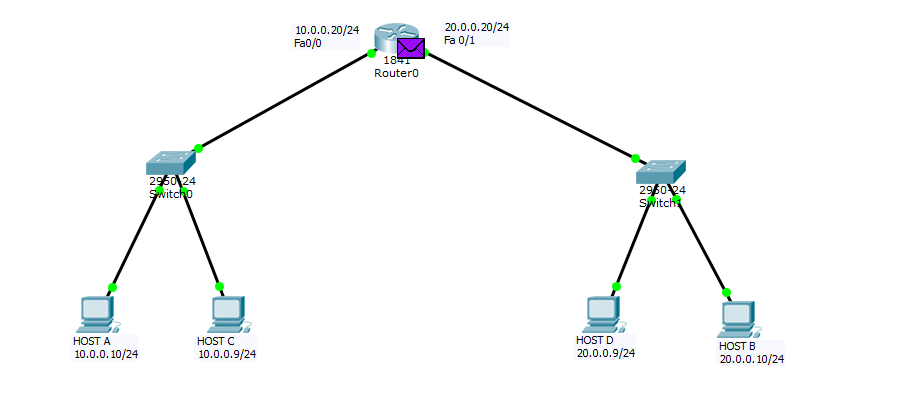


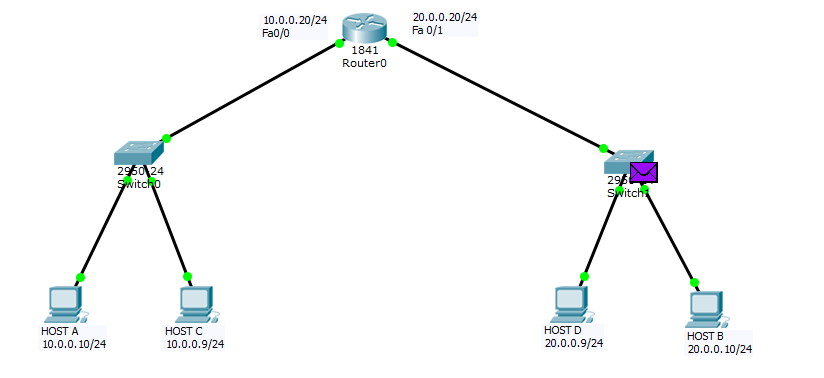
Now the ARP has to be resolved again because the router has to deliver the packet to host B and the ARP table has no entry for host B. Therefore, the ARP request is broadcast in the network 20.0.0.0/24. The packet is received by the Switch which in turn broadcast the request to host B and D. Host D will reject the request and host B will accept it and generate an ARP reply for the MAC address 000B.BE8E.5202 (router fa0/1 MAC address) because the ARP reply has to be given to that MAC address from which the ARP request has been received.

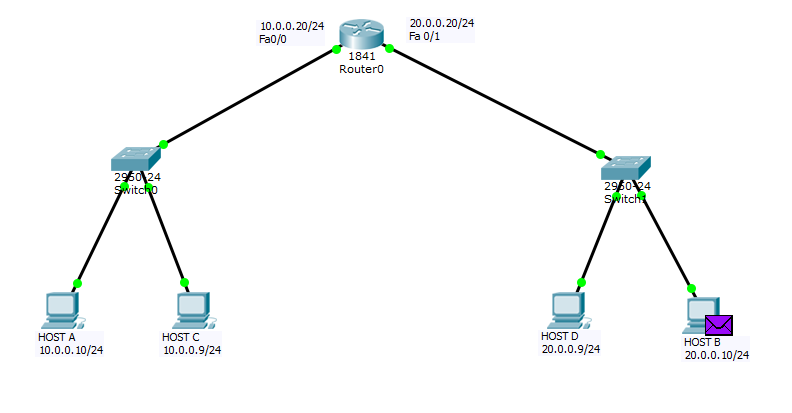


As you can see in the figure, the ARP reply packet is unicast to the router’s interface fa0/1 MAC address(000B.BE8E.5202) and the source MAC is 00E0.A3E2.03DC.

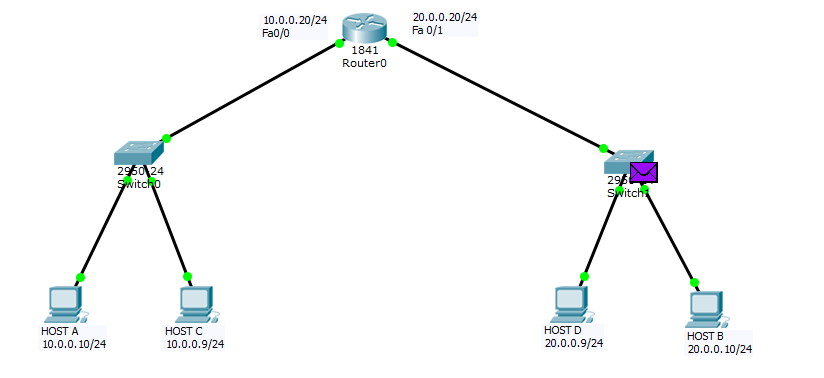
**Note –** Here, the target MAC address is the MAC address of host B (000B.BE8E.5202). Target MAC address is the MAC address of a device that the host wants to know through its ARP request to resolve ARP.

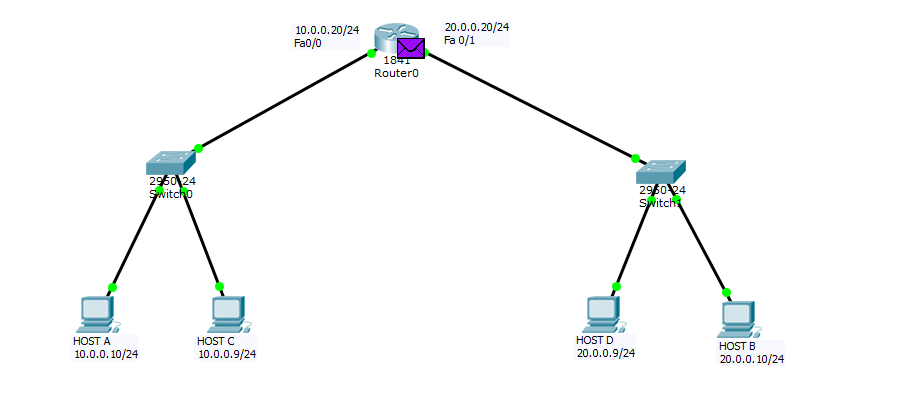


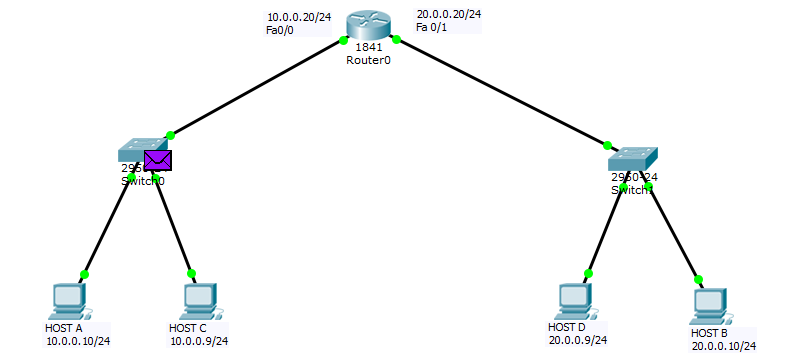


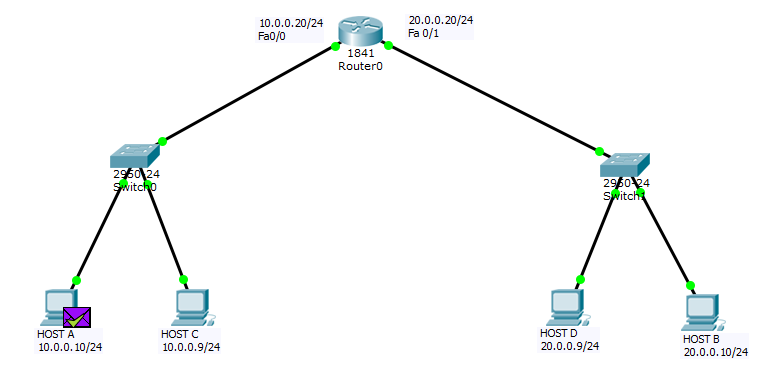


Now the ICMP echo-request packet will be unicast to the host B as shown in the above 3 figures.



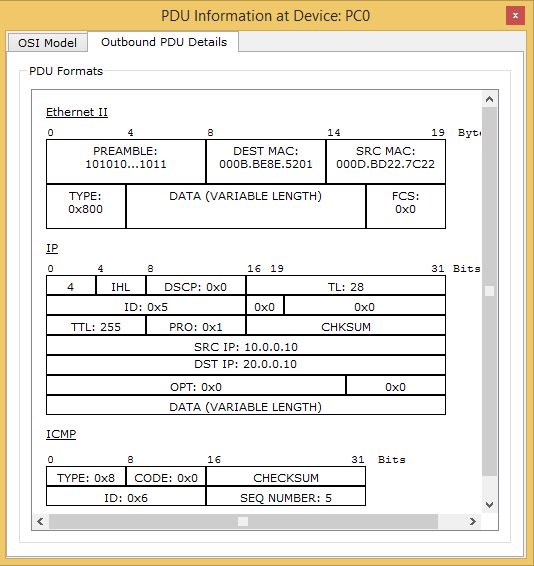




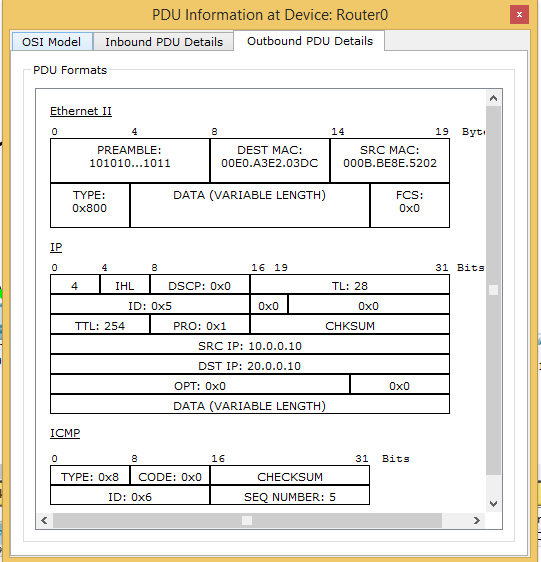


Host B will generate an ICMP echo reply in response to the ICMP echo request for host A which will be delivered to the 20.0.0.20 (router’s interface IP address) first and then unicast to host A.

**How does** **the MAC address never crosses its broadcast domain?**



This is the IP and Ethernet header when host A forwards the ICMP echo request to its default gateway. Therefore source IP is 10.0.0.10 and destination IP is 10.0.0.20, source MAC address is 000D.BD22.7C22 (host A MAC address) and destination MAC address is 000B.BE8E.5201 (router’s fa0/0 interface MAC address).



But now when the ICMP echo request message is forwarded from the router’s fa0/1 interface to host B then the source MAC address is changed to 000B.BE8E.5202 (router’s fa0/1 interface MAC address) and destination MAC address is 00E0.A3E2.03DC (host B MAC address).

Here router’s fa0/0 interface MAC address is not used as the source MAC address, instead the fa0/1 MAC address is used as a MAC address. Therefore, fa0/0 is not used in other broadcast domains (20.0.0.0/24 network) therefore MAC address never crosses its broadcast domain. IN this way, PING is performed in 2 different networks.