**1**

**AIM : Use Wireshark for DHCP Packet capture and answer these Questions :**

1. Capture DHCP packets on Wireshark and open the DHCP request and reply packets.
2. What information is obtained from DHCP reply packet header fields ? Note down.
3. Find out the lease time , renewal time and rebinding time given to you by the DHCP server.
4. Which class is your IP address ? What is the DHCP server’s IP address.
5. Is the DHCP request unicast, multicast or broadcast ? And what can you comment on DHCP reply?

Sure, I can guide you through the process. First, you'll need to capture DHCP packets using Wireshark. Make sure your network interface is selected, and then start the capture. You can filter the packets by typing "dhcp" in the display filter bar. This will show you only DHCP packets. Look for DHCP request and reply packets in the captured data.

The DHCP reply packet header fields typically include:

Transaction ID

Flags

Client IP Address

Your (Client's) IP Address

Server IP Address

Gateway IP Address

Subnet Mask

Lease Time

Renewal Time

Rebinding Time

DHCP Message Type

DHCP Options (which can include additional information like DNS servers, domain name, etc.)

To find out the lease time, renewal time, and rebinding time, locate the DHCP reply packet and check the corresponding fields. These times are usually provided in seconds.

To determine the class of your IP address (e.g., Class A, B, C, etc.), you'll need to examine the IP address itself. The DHCP server's IP address will also be listed in the DHCP reply packet.

DHCP request packets are typically broadcast, meaning they are sent to all devices on the local network. DHCP reply packets are unicast, meaning they are sent directly from the DHCP server to the requesting client's MAC address. This ensures that only the intended client receives the configuration information. The DHCP reply contains the necessary network configuration information for the client, such as IP address, subnet mask, gateway, DNS servers, etc. It acknowledges the receipt of the DHCP request and provides the client with the lease information and network settings.

**2**

**AIM : Use Wireshark for DHCP Packet capture and answer these Questions :**

1. Capture DHCP packets on Wireshark and open the DHCP request and reply packets.
2. What information is obtained from DHCP reply packet header fields ? Note down.
3. Find out the lease time , renewal time and rebinding time given to you by the DHCP server.
4. Which version of IP address is allotted to you? What is the DHCP server’s IP address.
5. What is the subnet mask of your allotted IP address ? Is subnetting involved in this dynamic allocation?

To capture DHCP packets in Wireshark, you'll need to start a packet capture session on the network interface through which DHCP traffic flows. Once the capture is running, filter the packets to display only DHCP packets. Look for DHCP request and reply packets and inspect them.

The DHCP reply packet header fields typically include:

Transaction ID

Flags

Client IP Address

Your (Client's) IP Address

Server IP Address

Gateway IP Address

Subnet Mask

Lease Time

Renewal Time

Rebinding Time

DHCP Message Type

DHCP Options (which can include additional information like DNS servers, domain name, etc.)

To find out the lease time, renewal time, and rebinding time, locate the DHCP reply packet and check the corresponding fields. These times are usually provided in seconds.

The version of IP address allotted to you can be determined by examining the IP address itself. For example, if your IP address starts with 192.168.x.x, it's an IPv4 address. If it starts with something like 2001:0db8:x:x:x:x:x:x, it's an IPv6 address. The DHCP server's IP address will also be listed in the DHCP reply packet.

The subnet mask of your allotted IP address is typically provided in the DHCP reply packet. It specifies the network portion of your IP address. Subnetting can indeed be involved in dynamic IP address allocation, as it allows for more efficient use of IP address space by dividing a network into smaller subnetworks.

**3**

**AIM : To run the IP utility commands and answer these Questions :**

1. What is the physical address and hostname of your machine?
2. Find the IP address of your machine and the of the DNS server connected to you.
3. Is your IP address dynamic/static ? If dynamic, find out the IP address of DHCP server.
4. Find out how many hops required to get connected to [www.mu.ac.in](http://www.mu.ac.in) from your machine.
5. Find out the difference in the following IP utility commands : PING , PATHPING and TRACERT when executed to reach [**www.gmail.com**](http://www.gmail.com) server.

Certainly! Here are the IP utility commands you can use to answer each question:

1. To find the physical address (MAC address) and hostname of your machine:

- Command: `ipconfig /all` (Windows) or `ifconfig -a` (Linux/macOS)

2. To find the IP address of your machine and the DNS server connected to you:

- Command: `ipconfig` (Windows) or `ifconfig` (Linux/macOS)

3. To determine if your IP address is dynamic/static and find the IP address of the DHCP server (if dynamic):

- Command: `ipconfig /all` (Windows) or `ifconfig -a` (Linux/macOS)

4. To find out how many hops are required to get connected to a specific website (e.g., www.mu.ac.in):

- Command: `tracert www.mu.ac.in` (Windows) or `traceroute www.mu.ac.in` (Linux/macOS)

5. To understand the difference between PING, PATHPING, and TRACERT when executed to reach a specific server (e.g., www.gmail.com):

- PING: Measures the round-trip time for packets sent from your computer to the target server.

- PATHPING: Provides information about the path to a specified destination and measures packet loss at each hop along the way.

- TRACERT: Shows the route packets take to reach the destination server and measures round-trip times to each hop along the way.

**4**

**AIM : To run the IP utility commands and answer these Questions :**

1. What is the IP address of your machine? Is it IPv4 or IPv6 ? Which class does it belong to?
2. What is the IP address of the gateway , DNS and DHCP server you are connected to?
3. Do you own a private IP or a public/global IP? State the reason for your answer.
4. Find out how many hops it requires to get connected to [www.gmail.com](http://www.gmail.com) from your device.
5. Find out the difference in the following Utility commands : PING , PATHPING and TRACERT when executed to reach [www.mu.ac.in](http://www.mu.ac.in) server.

**Sure, let's go through each question step by step:**

1. To find the IP address of your machine and its type (IPv4 or IPv6) along with its class (if IPv4):

- Command: `ipconfig` (Windows) or `ifconfig` (Linux/macOS)

- Explanation: Look for the "IPv4 Address" or "IPv6 Address" field to find your machine's IP address. The address format will determine whether it's IPv4 or IPv6. For IPv4, you can determine the class based on the first octet of the IP address.

2. To find the IP address of the gateway, DNS server, and DHCP server you are connected to:

- Command: `ipconfig /all` (Windows) or `ifconfig -a` (Linux/macOS)

- Explanation: Look for the "Default Gateway," "DNS Servers," and "DHCP Server" fields to find the respective IP addresses.

3. To determine if you have a private or public/global IP address:

- If your IP address falls within one of the private IP address ranges (e.g., 192.168.x.x, 10.x.x.x, 172.16.x.x - 172.31.x.x), then it's a private IP address. Otherwise, it's likely a public/global IP address.

- Explanation: Private IP addresses are reserved for internal/private networks and are not routable over the internet. Public/global IP addresses are routable over the internet.

4. To find out how many hops it requires to get connected to www.gmail.com:

- Command: `tracert www.gmail.com` (Windows) or `traceroute www.gmail.com` (Linux/macOS)

- Explanation: This command will show you the route packets take to reach the www.gmail.com server and the number of hops (routers) along the way.

5. To understand the difference between PING, PATHPING, and TRACERT when executed to reach a specific server (e.g., www.mu.ac.in):

- PING: Measures the round-trip time for packets sent from your computer to the target server.

- PATHPING: Provides information about the path to a specified destination and measures packet loss at each hop along the way.

- TRACERT: Shows the route packets take to reach the destination server and measures round-trip times to each hop along the way.

You can execute these commands in your command prompt or terminal to obtain the respective information. Let me know if you need more assistance with any specific command or step!

**5**

**AIM : Use Wireshark for ARP Packet capture and answer these Questions :**

1. What do you mean by ARP ? How is it different than RARP?
2. Capture ARP request and reply packets on your host machine using Wireshark.
3. How many ARP requests has your device sent in first 20 seconds of connection and how many ARP requests were replied to ?
4. What mandatory information was obtained through ARP response for your PC? Note down.
5. What is your physical address ? Is it permanent or temporary?

Sure, let's address each question:

1. ARP stands for Address Resolution Protocol. It is used to map an IP address to a MAC address within a local network. When a device wants to communicate with another device on the same network, it needs to know the MAC address of the target device. ARP helps in this by broadcasting an ARP request containing the IP address of the target device, and the device with that IP address responds with its MAC address.

RARP, on the other hand, stands for Reverse Address Resolution Protocol. It performs the opposite function of ARP. RARP is used to find out the IP address of a device when its MAC address is known. However, RARP is less commonly used compared to ARP.

2. To capture ARP request and reply packets using Wireshark, you can start a packet capture session on your network interface and apply a display filter for ARP packets. The filter would be `arp`. This will show you all ARP request and reply packets on your host machine.

3. Within the first 20 seconds of connection, you can analyze the Wireshark capture to count the number of ARP requests sent by your device and the number of ARP replies received. This can be determined by examining the timestamp and type of each packet in the capture.

4. The mandatory information obtained through an ARP response for your PC typically includes:

- IP address of the device (sender)

- MAC address of the device (sender)

5. Your physical address, also known as MAC address or hardware address, uniquely identifies your network interface card (NIC). It is a 48-bit hexadecimal number typically represented as six pairs of digits separated by colons (e.g., XX:XX:XX:XX:XX:XX). The physical address is permanent and tied to the hardware of your NIC. You can find your physical address by checking the ARP packets captured in Wireshark or by using the `ipconfig /all` command on Windows or `ifconfig -a` command on Linux/macOS.

**6**

**AIM : Use Wireshark for ARP Packet capture and answer these Questions :**

1. What do you mean by ARP ? How is it different than RARP?
2. Capture ARP request and reply packets on your host machine using Wireshark.
3. How many ARP requests has your device sent in first 20 seconds of connection and how many ARP requests were replied to ?
4. What is your physical address ? How is it represented and is it fixed ?
5. What is your logical address ? Which version and class does it belong to ?

Sure, let's address each question:

1. \*\*ARP (Address Resolution Protocol)\*\*: ARP is a protocol used to map an IP address to a physical MAC address within a local network. It's essential for communication between devices on the same network segment. When a device wants to communicate with another device, it needs to know the MAC address of the target device. ARP helps in this by broadcasting an ARP request containing the IP address of the target device, and the device with that IP address responds with its MAC address.

\*\*RARP (Reverse Address Resolution Protocol)\*\*: RARP is essentially the reverse of ARP. It's used to determine the IP address associated with a known MAC address. This protocol was primarily used in older systems where diskless workstations needed to obtain their IP address from a server based on their MAC address. However, RARP is less commonly used nowadays compared to ARP.

2. To capture ARP request and reply packets using Wireshark, you can start a packet capture session on your network interface and apply a display filter for ARP packets. The filter would be `arp`. This will show you all ARP request and reply packets on your host machine.

3. Within the first 20 seconds of connection, you can analyze the Wireshark capture to count the number of ARP requests sent by your device and the number of ARP replies received. This can be determined by examining the timestamp and type of each packet in the capture.

4. Your physical address, also known as MAC address or hardware address, uniquely identifies your network interface card (NIC). It is a fixed 48-bit hexadecimal number typically represented as six pairs of digits separated by colons (e.g., XX:XX:XX:XX:XX:XX). You can find your physical address by checking the ARP packets captured in Wireshark or by using the `ipconfig /all` command on Windows or `ifconfig -a` command on Linux/macOS.

5. Your logical address is your IP address, which uniquely identifies your device on a network. It can be either IPv4 or IPv6. To determine the version and class of your IP address, you need to inspect its format. For IPv4 addresses, the class can be determined based on the range of the first octet. For IPv6 addresses, the version is explicitly specified in the address format. You can find your IP address by checking the ARP packets captured in Wireshark or by using the `ipconfig` command on Windows or `ifconfig` command on Linux/macOS.

**7**

**AIM : Use CISCO packet tracer to configure any network topology and answer these questions :**

1. Prepare a network with four hosts, two switches, two  routers and connect them to form a small network. Allot only Private IP addresses belonging to CLASS B to the hosts.
2. Simulate and Run to observe STP/ICMP protocol and display all results.
3. What are the different topologies observed in your network ?
4. What is the role of a switch and a router in the computer network ?
5. Name the routing protocols that can be implemented in your topology.

Sure, let's address each question:

1. \*\*Network Topology\*\*:

- Use Cisco Packet Tracer to create a network with four hosts, two switches, and two routers.

- Connect the hosts to the switches and the switches to the routers.

- Allot private IP addresses belonging to Class B (e.g., 172.16.x.x, 172.17.x.x, etc.) to the hosts.

2. \*\*Simulate and Run STP/ICMP\*\*:

- In Cisco Packet Tracer, you can simulate the Spanning Tree Protocol (STP) and Internet Control Message Protocol (ICMP) by configuring the switches and routers appropriately.

- Run the simulation and observe the behavior of STP and ICMP.

- You can view the results and any errors or warnings that occur during the simulation.

3. \*\*Different Topologies\*\*:

- In the network created, you may observe various topologies such as:

- Star Topology: Hosts connected to switches, switches connected to routers.

- Bus Topology: Devices connected linearly, though not directly applicable in this scenario.

- Partial Mesh Topology: Routers connected to each other forming a partial mesh network.

4. \*\*Role of Switch and Router\*\*:

- \*\*Switch\*\*: A switch operates at the data link layer (Layer 2) of the OSI model and is responsible for forwarding data packets between devices within the same network. It learns MAC addresses by examining incoming frames and uses this information to forward frames only to the appropriate port(s).

- \*\*Router\*\*: A router operates at the network layer (Layer 3) of the OSI model and is responsible for forwarding data packets between different networks. It uses IP addresses to determine the best path for packet forwarding and can connect multiple networks together.

5. \*\*Routing Protocols\*\*:

- In the topology created, you can implement various routing protocols such as:

- RIP (Routing Information Protocol)

- OSPF (Open Shortest Path First)

- EIGRP (Enhanced Interior Gateway Routing Protocol)

- Static Routing

These routing protocols can be configured on the routers to enable dynamic routing and efficient packet forwarding between networks.

**8**

**AIM : Use CISCO packet tracer to configure any network topology and answer these questions :**

1. Prepare a network with four hosts, two switches, two  routers and connect them to form a small network. Allot only Private IP addresses belonging to CLASS C to the hosts.
2. Simulate and Run to observe STP/ICMP protocol and display all results.
3. What are the different topologies observed in your network ?
4. What is the role of a switch and a router in the computer network ?
5. Name the routing protocols that can be implemented in your topology

Certainly! Here's how you can approach these questions in Cisco Packet Tracer:

1. \*\*Network Topology\*\*:

- Create a network with four hosts, two switches, and two routers in Cisco Packet Tracer.

- Connect the hosts to the switches, and the switches to the routers.

- Allot private IP addresses belonging to Class C (e.g., 192.168.x.x) to the hosts.

2. \*\*Simulate and Run STP/ICMP\*\*:

- Configure the switches in the network to enable Spanning Tree Protocol (STP) to prevent loops in the network.

- Configure the routers to allow ICMP (Internet Control Message Protocol) traffic.

- Run the simulation and observe the behavior of STP and ICMP.

- You can view the results and any events or messages related to STP and ICMP in the simulation panel.

3. \*\*Different Topologies\*\*:

- In the network created, you may observe various topologies such as:

- Star Topology: Hosts connected to switches, switches connected to routers.

- Partial Mesh Topology: Routers connected to each other forming a partial mesh network.

- Hierarchical Topology: Routers acting as core and distribution layers with switches and hosts connected to them.

4. \*\*Role of Switch and Router\*\*:

- \*\*Switch\*\*: A switch operates at the data link layer (Layer 2) of the OSI model. Its primary role is to forward frames within the same network based on MAC addresses. Switches create separate collision domains, increasing the efficiency of network communication.

- \*\*Router\*\*: A router operates at the network layer (Layer 3) of the OSI model. Its primary role is to forward packets between different networks based on IP addresses. Routers maintain routing tables to determine the best path for packet forwarding, allowing communication between devices on different networks.

5. \*\*Routing Protocols\*\*:

- In the topology created, you can implement various routing protocols such as:

- RIP (Routing Information Protocol)

- OSPF (Open Shortest Path First)

- EIGRP (Enhanced Interior Gateway Routing Protocol)

- BGP (Border Gateway Protocol)

These routing protocols can be configured on the routers to enable dynamic routing and efficient packet forwarding between networks. Each protocol has its own advantages and suitability depending on the network requirements.

**9**

**AIM : Use CISCO packet tracer to configure DNS client server model using Cisco packet tracer and answer :**

1. What is the DNS server IP address set to in your experiment and what is the client IP address used while sending a DNS query?
2. Take the print of the DNS client server model prepared and the settings being done for configuring DNS (step by step).
3. Attach the Simulation output screenshots
4. Give 3 to 4 examples of Country domain and generic domains.
5. What will the query name format for [www.fcrit.ac.in](http://www.fcrit.ac.in) ?

**Since I can't directly interact with external tools like Cisco Packet Tracer or access files or screenshots, I can guide you on how to set up the DNS client-server model in Cisco Packet Tracer and answer your questions based on that.**

1. \*\*DNS Server IP Address and Client IP Address\*\*:

- In your experiment, you can set the DNS server's IP address according to your network configuration. For example, it could be something like 192.168.1.100.

- The client's IP address used while sending a DNS query will depend on the network configuration in your setup. For example, it could be 192.168.1.10.

2. \*\*Settings for Configuring DNS\*\*:

- Open Cisco Packet Tracer and set up your network topology with DNS server and client devices.

- Configure the DNS server by assigning it an IP address and configuring DNS settings such as domain name, DNS records, etc.

- Configure the DNS client by specifying the DNS server's IP address in its network settings.

- Test the DNS configuration by sending DNS queries from the client device.

3. \*\*Simulation Output Screenshots\*\*:

- After configuring the DNS client-server model, you can run a simulation to test the DNS resolution process.

- Take screenshots of the simulation output showing the DNS queries and responses.

4. \*\*Examples of Country and Generic Domains\*\*:

- Country Domains: .us (United States), .uk (United Kingdom), .in (India), .de (Germany)

- Generic Domains: .com (commercial), .org (organization), .net (network), .edu (education)

5. \*\*Query Name Format for www.fcrit.ac.in\*\*:

- The query name format for www.fcrit.ac.in would be a fully qualified domain name (FQDN), which includes the hostname (www) and the domain name (fcrit.ac.in). So, the query name would be "www.fcrit.ac.in".

Ensure to follow the steps to configure the DNS client-server model accurately, and feel free to ask if you have any specific questions or need further clarification on any aspect of the setup!

**10**

**AIM : Perform Configuration of host machine from static to dynamic and vice versa and answer these Questions :**

1. What is the IP address of your machine ? Is it IPv4 or Ipv6 ? What is the CIDR value ?
2. Is your internet connection DHCP enabled currently ? If yes, find out the IP address of DHCP server. Find out the lease time allotted.
3. What is the MAC address of your machine ? Can it be changed ?
4. If you have dynamic configuration, change the settings to make your IP address static. Take the necessary screenshots.
5. Change the settings to make your IP address dynamic again. Take the necessary screenshots.

Sure, let's go through each question step by step:

1. \*\*IP Address and CIDR Value\*\*:

- Check the IP address of your machine by using the appropriate command based on your operating system (`ipconfig` for Windows, `ifconfig` for Linux/macOS).

- Determine whether it's IPv4 or IPv6 based on the address format.

- The CIDR value represents the subnet mask in CIDR notation. You can calculate it based on the subnet mask associated with your IP address.

2. \*\*DHCP Status and DHCP Server IP Address\*\*:

- Check if your internet connection is DHCP enabled by examining your network settings or using a command like `ipconfig /all` (Windows) or `ifconfig -a` (Linux/macOS).

- If DHCP is enabled, you can find the IP address of the DHCP server by examining your network settings or using a tool like `ipconfig /all` (Windows) or `ifconfig -a` (Linux/macOS). Additionally, the lease time allotted by the DHCP server can also be found in the same settings or command output.

3. \*\*MAC Address and its Changeability\*\*:

- Find the MAC address of your machine by using the appropriate command (`ipconfig /all` for Windows, `ifconfig -a` for Linux/macOS).

- Typically, a MAC address is hardcoded into the network interface's hardware and cannot be changed. However, some network interfaces may allow for MAC address spoofing, but this is not recommended and may violate network policies or regulations.

4. \*\*Changing from Dynamic to Static Configuration\*\*:

- To change your IP address from dynamic to static, you'll need to access your network settings and manually configure the IP address, subnet mask, default gateway, and DNS server addresses.

- Take screenshots of the relevant network settings before and after making the changes to demonstrate the transition from dynamic to static configuration.

5. \*\*Changing from Static to Dynamic Configuration\*\*:

- To change your IP address from static to dynamic, you'll need to access your network settings and configure them to obtain an IP address automatically (DHCP).

- Take screenshots of the relevant network settings before and after making the changes to demonstrate the transition from static to dynamic configuration.

Remember to carefully follow the steps to change your network configuration and take screenshots at each stage for documentation purposes. Let me know if you need further assistance with any specific step!

**11**

**AIM : Perform Configuration of host machine from static to dynamic and vice versa and answer these Questions**

1. What is the IP address of your machine ? What is the class and the subnet mask ?
2. Is your internet connection DHCP enabled currently ? If yes, find out the IP address of DHCP server.
3. Find out the lease time allotted, renewal time and rebinding time with current connection.
4. If you have dynamic configuration, change the settings to make your IP address static. Take the necessary screenshots.
5. Change the settings to make your IP address dynamic again. Take the necessary screenshots.

To perform the configuration changes from static to dynamic and vice versa, we'll need to use the network settings on your host machine. Here's how you can do it and answer your questions:

1. \*\*IP Address, Class, and Subnet Mask\*\*:

- Determine the current IP address of your machine by using the appropriate command (`ipconfig` for Windows, `ifconfig` for Linux/macOS).

- From the IP address, determine the class (A, B, or C) and the subnet mask.

2. \*\*DHCP Status and DHCP Server IP Address\*\*:

- Check if your internet connection is DHCP enabled by examining your network settings.

- If DHCP is enabled, you can find the IP address of the DHCP server by examining your network settings.

3. \*\*Lease Time, Renewal Time, and Rebinding Time\*\*:

- If your connection is DHCP enabled, you can find the lease time, renewal time, and rebinding time by examining your network settings. These values are typically provided in seconds.

4. \*\*Changing from Dynamic to Static Configuration\*\*:

- Access your network settings and configure a static IP address, subnet mask, default gateway, and DNS server addresses.

- Take screenshots of the network settings before and after making the changes.

5. \*\*Changing from Static to Dynamic Configuration\*\*:

- Access your network settings and configure them to obtain an IP address automatically (DHCP).

- Take screenshots of the network settings before and after making the changes.

For steps 4 and 5, the process may vary depending on your operating system. However, typically, you can find network settings in the Control Panel or Network Preferences on Windows and System Preferences on macOS.

After completing each step, ensure to take screenshots of the relevant network settings and any other relevant information requested in the questions. Let me know if you need further assistance with any specific step or have any questions!

**12**

**AIM : Use Wireshark to observe the TCP connection, termination and TCP segment format while uploading a file and answer these Questions**

1. The TCP segments are required to be captured and analyzed while UPLOADING the file :

Go the <http://gaia.cs.umass.edu/wiresharklabs/alice.txt> and now use this downloaded txt file to upload on <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3. How much time in seconds the TCP connection gives you the information about file being uploaded successfully?
4. Who has sent the finish segment to whom in order to terminate TCP connection and at what time after file had been uploaded?

To answer these questions, you would need to follow these steps:

1. \*\*Capture and Analyze TCP Segments\*\*:

- Use Wireshark to capture TCP segments while uploading the file `alice.txt` from http://gaia.cs.umass.edu/wiresharklabs/alice.txt to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.

- Ensure you capture the entire TCP connection process, including the connection establishment, data transfer, and connection termination.

2. \*\*IP Address and TCP Port Number of Client Computer\*\*:

- Analyze the captured TCP segments to find the IP address and TCP port number used by the client computer (source) transferring the file.

- The IP address and port number will be present in the source IP and port fields of the captured TCP segments.

3. \*\*IP Address of gaia.cs.umass.edu and Port Number\*\*:

- Analyze the captured TCP segments to find the IP address of gaia.cs.umass.edu and the port number it is using to send and receive TCP segments for this connection.

- The IP address of the server and the port numbers will be present in the destination IP and port fields of the captured TCP segments.

4. \*\*Time Taken for Successful File Upload\*\*:

- Analyze the captured TCP segments to find the time at which the TCP connection provides information about the file being uploaded successfully.

- This information may be inferred from ACK segments or other indicators in the captured packets.

5. \*\*TCP Connection Termination\*\*:

- Analyze the captured TCP segments to find the FIN (Finish) segment indicating the termination of the TCP connection.

- Identify which party sent the FIN segment (client or server) and to whom it was sent.

- Determine the time at which the FIN segment was sent after the file had been uploaded.

Once you have captured and analyzed the TCP segments using Wireshark, you can use the information obtained to answer each question accordingly. If you encounter any difficulties during the process, feel free to ask for clarification or assistance!

**13**

**AIM : Use Wireshark to observe the TCP connection, termination and TCP segment format while uploading a file and answer these Questions**

1. The TCP segments are required to be captured and analyzed while UPLOADING the file :

Go the <http://gaia.cs.umass.edu/wiresharklabs/alice.txt> and now use this downloaded txt file to upload on <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
2. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu?
3. How much time in seconds the TCP connection gives you the information about file being uploaded successfully? Which message gives us the indication?
4. Are there any number of retransmissions from source. Also find out of whether there were out of order segments.

To answer these questions, you would need to follow these steps using Wireshark:

1. \*\*Capture and Analyze TCP Segments\*\*:

- Use Wireshark to capture TCP segments while uploading the file `alice.txt` from http://gaia.cs.umass.edu/wiresharklabs/alice.txt to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.

- Start capturing packets before initiating the upload process and continue capturing until the file upload is completed.

2. \*\*IP Address and TCP Port Number of Client Computer\*\*:

- Analyze the captured TCP segments to find the IP address and TCP port number used by the client computer (source) transferring the file.

- Look for the source IP and port fields in the captured packets.

3. \*\*Sequence Number of TCP SYN Segment\*\*:

- Find the TCP SYN segment in the captured packets, which is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu.

- Identify the sequence number field in the TCP header of the SYN segment to determine its value.

4. \*\*Time Taken for Successful File Upload\*\*:

- Analyze the captured TCP segments to find the time it takes for the TCP connection to provide information about the file being uploaded successfully.

- Look for ACK segments or other indicators in the captured packets that confirm the successful upload of the file. Note the time difference between the start of the upload process and the indication of successful upload.

5. \*\*Retransmissions and Out-of-Order Segments\*\*:

- Check for any retransmissions from the source by looking for duplicate sequence numbers or retransmission flags in the captured packets.

- Look for any out-of-order segments by analyzing the sequence numbers of the packets to see if they arrive in a different order than expected.

Once you have analyzed the captured TCP segments using Wireshark, you can use the information obtained to answer each question accordingly. If you encounter any difficulties during the process, feel free to ask for clarification or assistance!

**14**

**AIM : Use Wireshark to observe the TCP connection, termination and TCP segment format while uploading a file and answer these Questions**

1. The TCP segments are required to be captured and analyzed while UPLOADING the file :

Go the <http://gaia.cs.umass.edu/wiresharklabs/alice.txt> and now use this downloaded txt file to upload on <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.

1. How much time in seconds the TCP connection gives you the information about file being uploaded successfully? Which message gives us the indication?
2. Are there any number of retransmissions from source. Also find out of whether there were out of order segments.
3. What are the TCP header fields obtained in the first SYN segment ? Note them down.
4. Who has sent the finish segment to whom in order to terminate TCP connection and at what time after file had been uploaded?

To answer these questions using Wireshark, follow these steps:

1. \*\*Capture and Analyze TCP Segments\*\*:

- Open Wireshark and start capturing packets.

- Go to http://gaia.cs.umass.edu/wiresharklabs/alice.txt and download the file.

- Upload the downloaded file to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.

- Continue capturing packets until the file upload is completed.

2. \*\*Time for Successful File Upload\*\*:

- Analyze the captured TCP segments to find the time it takes for the TCP connection to indicate that the file has been uploaded successfully.

- Look for ACK segments or other indicators in the captured packets that confirm the successful upload of the file. Note the time difference between the start of the upload process and the indication of successful upload.

3. \*\*Retransmissions and Out-of-Order Segments\*\*:

- Check for any retransmissions from the source by looking for duplicate sequence numbers or retransmission flags in the captured packets.

- Look for any out-of-order segments by analyzing the sequence numbers of the packets to see if they arrive in a different order than expected.

4. \*\*TCP Header Fields in the First SYN Segment\*\*:

- Find the first SYN segment in the captured packets, which is used to initiate the TCP connection.

- Note down the TCP header fields obtained in the SYN segment, such as source port, destination port, sequence number, acknowledgment number, window size, flags, etc.

5. \*\*Finish Segment for TCP Connection Termination\*\*:

- Identify the FIN segment in the captured packets, which is used to terminate the TCP connection.

- Determine which party sent the FIN segment (client or server) and to whom it was sent.

- Note the time at which the FIN segment was sent after the file had been uploaded.

After analyzing the captured TCP segments in Wireshark, you can answer each question based on the observations made during the file upload process. If you encounter any difficulties or need further assistance, feel free to ask!

**15**

**AIM : Use Wireshark to analyze the content IP packets and find the header field values and answer :**

1. Open any emailing platform website, try opening registration links simultaneously capturing these IP packets and find the version of IP being used.
2. Note down all the IP header fields in any one packet coming from the server to your device.
3. How many number of data bytes are contained in the packet sent by you to the server ?
4. How many number of hops are allowed for the packet being transmitted from you to the website server?
5. Which transport layer protocol is observed to be used ? Find out the source port and destination port numbers for the outgoing packet.

**16**

**AIM : Use Wireshark to analyze the content IP packets and find the header field values and answer Questions**

1. Open [www.youtube.com](http://www.youtube.com) and play a educational video for 5 seconds, simultaneously capturing these IP packets and find the type of packets being captured related to the video.
2. Note down all the IP header fields in any one packet coming from the youtube server to your device.
3. How many number of hops are allowed for the packet being transmitted from you to the website server?
4. Which transport layer protocol is observed to be used ? Find out the source port and destination port numbers for the outgoing packet.
5. Is there checksum calculated and validated in the IP packets coming from youtube server to you?

To analyze the content of IP packets using Wireshark and answer your questions, follow these steps:

1. \*\*Capture IP Packets from Emailing Platform Website\*\*:

- Open Wireshark and start capturing packets on the network interface through which your device is connected to the internet.

- Open any emailing platform website and try opening registration links or performing any activity that generates network traffic.

- While performing these actions, ensure Wireshark is capturing packets simultaneously.

2. \*\*Identify the Version of IP Being Used\*\*:

- After capturing packets, analyze the packet details to determine the version of IP being used.

- Look for IP packets in the packet list pane and check the IP version field in the packet details.

3. \*\*IP Header Fields in a Packet from Server to Your Device\*\*:

- Locate a packet from the server to your device in Wireshark's packet list pane.

- Note down all the IP header fields available in the packet details, such as source IP address, destination IP address, time to live (TTL), identification, protocol, header checksum, etc.

4. \*\*Number of Data Bytes in the Packet Sent by Your Device to the Server\*\*:

- Find a packet sent by your device to the server in Wireshark's packet list pane.

- Look for the length of the packet in the packet details, which includes both the IP header length and the payload (data) length. Subtract the IP header length to determine the number of data bytes.

5. \*\*Number of Hops Allowed for the Packet\*\*:

- Check the time to live (TTL) field in the IP header of a packet sent by your device to the website server.

- The TTL field represents the number of hops allowed for the packet before it is discarded. Note the TTL value to determine the number of hops allowed.

6. \*\*Transport Layer Protocol and Port Numbers\*\*:

- Identify the transport layer protocol used in the IP packets, which is typically TCP or UDP.

- For outgoing packets from your device, find the source port and destination port numbers in the packet details. These port numbers indicate the source and destination applications or services.

By following these steps and analyzing the captured IP packets in Wireshark, you can find the requested information and answer each question accordingly. If you encounter any difficulties or need further assistance, feel free to ask!

**17**

**AIM : Use CISCO packet tracer to configure RING/BUS/STAR topology and answer these questions :**

1. Prepare a network with four hosts, two switches, two  routers and connect them to form a small network as per the given topology. Allot only Private IP addresses belonging to CLASS A/B/C to the hosts.
2. Simulate and Run model with STP/ICMP protocol and display all results.
3. What is the role of a switch and a router in the computer network ?
4. Make a comparison table stating advantages and disadvantages of all network topologies.
5. Which are the intradomain and interdomain routing protocols ?

To configure the network in Cisco Packet Tracer and answer your questions, follow these steps:

1. \*\*Prepare Network Topology\*\*:

- Create a network with four hosts, two switches, and two routers in Cisco Packet Tracer.

- Connect the hosts to the switches, and the switches to the routers, forming the desired topology (ring, bus, or star).

- Allot private IP addresses belonging to Class A/B/C to the hosts according to the topology.

2. \*\*Simulate and Run with STP/ICMP Protocol\*\*:

- Configure the switches in the network to enable Spanning Tree Protocol (STP) to prevent loops in the network.

- Configure the routers to allow ICMP (Internet Control Message Protocol) traffic for network diagnostics.

- Run the simulation and observe the behavior of STP and ICMP.

- Analyze the simulation results to ensure proper functioning of the network.

3. \*\*Role of Switch and Router\*\*:

- \*\*Switch\*\*: A switch operates at the data link layer (Layer 2) of the OSI model. Its primary role is to forward frames within the same network based on MAC addresses. Switches create separate collision domains, increasing the efficiency of network communication.

- \*\*Router\*\*: A router operates at the network layer (Layer 3) of the OSI model. Its primary role is to forward packets between different networks based on IP addresses. Routers maintain routing tables to determine the best path for packet forwarding, allowing communication between devices on different networks.

4. \*\*Advantages and Disadvantages of Network Topologies\*\*:

| Topology | Advantages | Disadvantages |

|----------|-------------------------------------------|------------------------------------------|

| Ring | - Simple to implement | - Failure of one node can disrupt network |

| | - Equal access to resources for all nodes | - Adding or removing nodes can be complex |

| | - No collisions | |

| Bus | - Easy to add or remove nodes | - Single point of failure (the bus) |

| | - Cost-effective | - Limited scalability |

| | - Simple to understand and manage | - Performance can degrade with high traffic |

| Star | - Centralized management | - Dependency on central hub |

| | - Fault isolation | - Failure of hub affects entire network |

| | - Scalability | - Costlier due to additional equipment |

5. \*\*Intradomain and Interdomain Routing Protocols\*\*:

- \*\*Intradomain Routing Protocols\*\*: Also known as interior gateway protocols (IGPs), these protocols are used within a single autonomous system (AS). Examples include OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol).

- \*\*Interdomain Routing Protocols\*\*: Also known as exterior gateway protocols (EGPs), these protocols are used between different autonomous systems (ASes) to exchange routing information across the internet. The main protocol used is BGP (Border Gateway Protocol).

By following these steps, you can configure the network in Cisco Packet Tracer and answer the questions regarding network topologies and routing protocols. If you have any further questions or need clarification, feel free to ask!

**18**

**AIM : Use CISCO packet tracer to configure RING/BUS/STAR topology and answer these questions :**

1. Prepare a network with five hosts, four switches, two  routers and connect them to form a small network as per the given topology. Allot only Private IP addresses belonging to CLASS A/B/C to the hosts.
2. Simulate and Run model with STP/ICMP protocol and display all results.
3. What is the role of a switch and a router in the computer network ?
4. State advantages and disadvantages of the topology you prepared in this task.
5. Which all intradomain and interdomain routing protocols can be configured?

To configure the network in Cisco Packet Tracer and answer your questions, follow these steps:

1. \*\*Prepare Network Topology\*\*:

- Create a network with five hosts, four switches, and two routers in Cisco Packet Tracer.

- Connect the hosts to the switches, and the switches to the routers, forming the desired topology (ring, bus, or star).

- Allot private IP addresses belonging to Class A/B/C to the hosts according to the topology.

2. \*\*Simulate and Run with STP/ICMP Protocol\*\*:

- Configure the switches in the network to enable Spanning Tree Protocol (STP) to prevent loops in the network.

- Configure the routers to allow ICMP (Internet Control Message Protocol) traffic for network diagnostics.

- Run the simulation and observe the behavior of STP and ICMP.

- Analyze the simulation results to ensure proper functioning of the network.

3. \*\*Role of Switch and Router\*\*:

- \*\*Switch\*\*: A switch operates at the data link layer (Layer 2) of the OSI model. Its primary role is to forward frames within the same network based on MAC addresses. Switches create separate collision domains, increasing the efficiency of network communication.

- \*\*Router\*\*: A router operates at the network layer (Layer 3) of the OSI model. Its primary role is to forward packets between different networks based on IP addresses. Routers maintain routing tables to determine the best path for packet forwarding, allowing communication between devices on different networks.

4. \*\*Advantages and Disadvantages of the Topology\*\*:

- \*\*Ring Topology\*\*:

- Advantages: Simple to implement, equal access to resources, no collisions.

- Disadvantages: Failure of one node can disrupt network, adding or removing nodes can be complex.

- \*\*Bus Topology\*\*:

- Advantages: Easy to add or remove nodes, cost-effective, simple to understand and manage.

- Disadvantages: Single point of failure (the bus), limited scalability, performance can degrade with high traffic.

- \*\*Star Topology\*\*:

- Advantages: Centralized management, fault isolation, scalability.

- Disadvantages: Dependency on central hub, failure of hub affects entire network, costlier due to additional equipment.

5. \*\*Intradomain and Interdomain Routing Protocols\*\*:

- \*\*Intradomain Routing Protocols (IGPs)\*\*: Examples include OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol).

- \*\*Interdomain Routing Protocols (EGPs)\*\*: The main protocol used is BGP (Border Gateway Protocol).

By following these steps, you can configure the network in Cisco Packet Tracer and answer the questions regarding network topologies and routing protocols. If you have any further questions or need clarification, feel free to ask!