SCHEME :K

Name :_____
Roll No.:_____ Year : 20 ___ 20 __
Exam Seat No. :_____

LABORATORY MANUAL FOR

ADVANCE COMPUTER NETWORK (315321)

COMPUTER ENGINEERING GROUP

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI
(Autonomous)(ISO21001:2018)(ISO/IEC27001:2013)

Vision

To ensure that the Diploma level Technical Education constantly matches the latest requirements of Technology and industry and includes the all-round personal development of students including social concerns and to become globally competitive, technology led organization.

Mission

To provide high quality technical and managerial manpower, information and consultancy services to the industry and community to enable the industry and community to face the challenging technological & environmental challenges.

Quality Policy

We, at MSBTE are committed to offer the best in class academic services to the students and institutes to enhance the delight of industry and society. This will be achieved through continual improvement in management practices adopted in the process of curriculum design, development, implementation, evaluation and monitoring system along with adequate faculty development programmes.

Core Values

MSBTE believes in the following:

- Skill development in line with industry requirements
- Industry readiness and improved employability of Diploma holders
- Synergistic relationship with industry
- Collective and Cooperative development of all stake holders
- Technological interventions in societal development
- Access to uniform quality technical education

A Practical Manual
for

Advance Computer Network

(315321)

Semester-V

BD/ CM/ CO/ CW/ HA/ IF/ SE

Maharashtra State Board of Technical Education, Mumbai
(Autonomous) (ISO 21001:2018) (ISO/IEC 27001:2013)

'K' Scheme Curriculum

Maharashtra State Board of Technical Education, Mumbai
(Autonomous) (ISO 21001:2018) (ISO/IEC 27001:2013)
4th Floor, Government Polytechnic Building
49, Kherwadi, Bandra (East), Mumbai – 400051

Maharashtra State Board of Technical Education
Certificate

This is to certify that Mr./Ms. ……Roll No……. of the Fifth Semester of Diploma in …… Engineering/Technology (Program Code - .....5K) of the Institute …… (Inst. Code……) has completed the practical work satisfactorily for the course Advance Computer Network (Course Code: 315321) for the academic year 20…– 20…..... as prescribed in the curriculum.

Place ……. Enrolment No……

Date: …..... Exam Seat No. …….....

Course Teacher **Head of the Department** **Principal**

Seal of the Institute

Preface

The primary focus of any engineering laboratory/field work in the technical education system is to develop the much-needed industry relevant competencies and skills. Therefore, for the successful implementation of this curriculum, every practical has been designed to serve as a 'vehicle' to develop this industry identified competency in every student. The practical skills are difficult to develop through 'chalk and duster' activity in the classroom situation. Accordingly, the 'K' scheme laboratory manual development team designed the practicals to focus on outcomes, rather than the traditional age-old practice of conducting practical's to 'verify the theory' (which may become a by product along the way).

This laboratory manual is designed to help all stakeholders, especially the students, teachers and instructors to develop in the student the pre-determined outcomes. It is expected from each student that at least a day in advance, they have to thoroughly read the concerned practical procedure that they will do the next day and understand minimum theoretical background associated with the practical. Every practical in this manual begins by identifying the competency, industry relevant skills, course outcomes and practical outcomes which serve as a key focal point for doing the practical. Students will then become aware about the skills they will achieve through procedure shown there and necessary precautions to be taken, which will help them to apply in solving real-world problems in their professional life.

This manual also provides guidelines to teachers and instructors to effectively facilitate student-centered lab activities through each practical exercise by arranging and managing necessary resources in order that the students follow the procedures and precautions systematically ensuring the achievement of outcomes in the students.

The Advance Computer Network course provides a comprehensive exploration of networking concepts and technologies. It covers Internet architecture, IP addressing, routing protocols (RIP, OSPF, BGP), TCP/UDP, DNS, and advanced technologies like SDN, 5G, 6G, and IP security. It equips students with hands-on skills for designing, managing, and troubleshooting modern computer networks.

Although all care has been taken to check for mistakes in this laboratory manual, yet it is impossible to claim perfection especially as this is the first edition. Any such errors and suggestions for improvement can be brought to our notice and are highly welcome.

Program Outcomes (POs) to be achieved through Course:

PO1	Basic and Discipline specific knowledge: Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the engineering problems.
PO2	Problem analysis: Identify and analyses well-defined engineering problems using codified standard methods.
PO3	Design/ development of solutions: Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs.
PO4	Engineering Tools, Experimentation and Testing: Apply modern engineering tools and appropriate technique to conduct standard tests and measurements.
PO5	Engineering practices for society, sustainability and environment: Apply appropriate technology in context of society, sustainability, environment and ethical practices.
PO6	Project Management: Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.
PO7	Life-long learning: Ability to analyses individual needs and engage in updating in the context of technological changes.

List of Relevant Skills

The following industry relevant skills of the competency "Apply Advanced Computer Networking Concepts" are expected to be developed in you by performing practical's of this laboratory manual.

1. IP Addressing & Subnetting – Understanding IPv4/IPv6 and subnet masks.
2. Routing & Switching – Configuring OSPF, BGP, RIP, VLANs for optimized traffic flow.
3. Network Security – Implementing firewalls, VPNs, intrusion detection (IDS/IPS), and encryption.
4. Troubleshooting – Managing troubleshooting in network.
5. Multimedia traffic analyser- Managing and analysis of traffic in network

Practical Course Outcome Matrix

Course Outcomes (COs)

CO1	Analyse the packet structure of IPv4 and IPv6.
CO2	Configure Static and Dynamic Routing Protocols Using Simulators.
CO3	Illustrate functions of Transport layer protocols.
CO4	Implement Application layer protocols on a network.
CO5	Work with various Wireless Networking Technologies.

Sr. No.	Title of the Experiment	CO1	CO2	CO3	CO4	CO5
1	*a)Identify IP allocations and Internet Service Providers for a student network Using WHOIS. b)Set up IP addresses and subnet masks on given network devices	✓				
2	Identify and resolve network issues using network diagnostic tools like ping, tracert, show,debug commands.	✓				
3	Run a Network Communication Script on "Kali Linux"	✓				
4	*Configure basic routing protocols using any relevant software/virtual lab.		✓			
5	Capture and Analyze ICMPv4 Packets using appropriate tool		✓			
6	*Configure, diagnose and troubleshoot TCP and UDP connection issues using diagnostic tools like netstat, wireshark, iperf			✓		
7	*Configure DNS using relevant software.				✓	
8	*Configure FTP using relevant software				✓	
9	Monitor network traffic using browser developer tools				✓	
10	*Design a simple network for SDN using Mininet					✓
11	Using Ping and Latency Tools i)Measure latency and packet loss over time using any suitable tool e.g. PingPlotter ii)Analyze network packets to detect performance bottlenecks using any suitable tool e.g.Wireshark					✓
12	Multimedia traffic analysis i)Capture and analyze HTTP video streaming traffic using any suitable tool e.g.Wireshark ii)Monitor RTP (Real-time Transport Protocol) packets from a multimedia stream using any suitable tool e.g.Wireshark					✓

Guidelines to Teachers

1. Teachers should align the explanation of the topic to teaching learning outcome (TLOs).
2. Refer to laboratory learning outcome (LLOs) for the execution of the practical to focus on the defined objectives.
3. Promote life-long learning by training the students to equip themselves with essential knowledge, skills and attitudes.
4. If required, provide demonstration for the practical emphasizing on the skills that the student should achieve.
5. Teachers should give opportunity to the students for exhibiting their skills after the demonstration.
6. Provide feedback and/or suggestions and share insights to improve effectiveness.
7. Assess students' skill achievement related to COs of each unit.

Instructions for Students

1. 100% attendance is compulsory for all practical sessions.
2. Students must adhere to ethical practices.
3. All the students must follow the schedule of practical sessions, complete the assigned work/activity and submit the assignment in stipulated time as instructed by the course teacher.
4. Students shall listen carefully the lecture given by teacher about importance of subject, learning structure, course outcomes.
5. Students shall understand the purpose of experiment and its practical implementation.
6. Students shall write the answers of the questions during practical.
7. Student should feel free to discuss any difficulty faced during the conduct of practical.
8. Students shall develop web based and window-based applications a expected by the industries.
9. Student shall attempt to develop related hands-on skills and gain confidence.
10. Students should develop habit to submit the write-ups on the scheduled dates and time.

Content Page

List of Practical and Formative Assessment Sheet

Sr. No	Practical Title	Date of Performance	Date of Submission	Assessment Marks (25)	Teacher's Sign	Remark
1	*a)Identify IP allocations and Internet Service Providers for a student network Using WHOIS. b)Set up IP addresses and subnet masks on given network devices					
2	Identify and resolve network issues using network diagnostic tools like ping, tracert, show,debug commands.					
3	Run a Network Communication Script on "Kali Linux"					
4	*Configure basic routing protocols using any relevant software/virtual lab.					
5	Capture and Analyze ICMPv4 Packets using appropriate tool					
6	*Configure, diagnose and troubleshoot TCP and UDP connection issues using diagnostic tools like netstat, wireshark, iperf					
7	*Configure DNS using relevant software.					
8	*Configure FTP using relevant software					
9	Monitor network traffic using browser developer tools					
10	*Design a simple network for SDN using Mininet					
11	Using Ping and Latency Tools i)Measure latency and packet loss over time using any suitable tool					

	e.g. PingPlotter ii)Analyze network packets to detect performance bottlenecks using any suitable tool e.g.Wireshark					
12	Multimedia traffic analysis i)Capture and analyze HTTP video streaming traffic using any suitable tool e.g.Wireshark ii)Monitor RTP (Real-time Transport Protocol) packets from a multimedia stream using any suitable tool e.g.Wireshark					
				Total		

***Total marks to be transferred to proforma published by MSBTE**

Note:

- '*' Marked Practical's (LLOs) Are mandatory.
- Minimum 80% of above list of lab experiment are to be performed.
- Judicial mix of LLOs are to be performed to achieve desired outcomes.

Practical No. 1: a) Identify IP allocations and Internet Service Providers for a student network Using WHOIS.

b) Set up IP addresses and subnet masks on given network devices

I Practical Significance

Understanding IP allocations and identifying Internet Service Providers (ISPs) using WHOIS has significant practical applications in network management and security, especially for student networks. By performing a WHOIS lookup, administrators can determine which organization owns a specific IP range, helping them track network activity and identify any unauthorized or suspicious traffic. This is particularly useful in cybersecurity, where detecting malicious IPs can prevent cyberattacks or data breaches.

II Industry / Employer Expected Outcome(s)

Develop standalone network.

III Course Level Learning Outcomes(s)

CO 1-Analyse the packet structure of IPv4 and IPv6.

IV Laboratory Learning Outcome(s)

LLO 1.1 Describe each component of output of WHOIS command

LLO 1.2 Configure a network by assigning IP addresses and subnet masks.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI Relevant Theoretical Background

WHOIS is a widely used query and response protocol that allows users to obtain detailed information about registered domain names and IP address allocations. It is especially useful for identifying IP allocations and associated Internet Service Providers (ISPs) within a network. By using WHOIS lookup tools, either online or via command-line utilities, users can access

ownership details, allocated IP ranges, Autonomous System Numbers (ASNs), and ISP information.

Stepwise Procedure

1.Using a Command-Line Tool: On most UNIX-based systems (or Windows with appropriate tools), you can open a terminal and type:

whois 192.0.2.0

replace 192.0.2.0 with the IP address or address block you want to check. The output will include details such as the netblock range (often seen under "inetnum" or "NetRange"), the organization ('OrgName'), and contact information.

Using Web-Based WHOIS Services: Websites like ARIN (American Registry for Internet Numbers), RIPE NCC, or APNIC allow you to perform WHOIS lookups through a web interface. For example, if your student network is located in India or uses an allocation from the Asia-Pacific registry (APNIC), the APNIC WHOIS search can provide relevant details.

2. Reading the Output: When you receive the WHOIS information:

IP Allocation: Look for fields like "inetnum" (or "NetRange") or "CIDR" which indicate the range of IP addresses. This tells you how the network block is assigned.

ISP/Organization Info: Check fields such as "OrgName," "netname," or "descr." This will show the organization managing the allocation, which is often the ISP or the institution managing the network.

3. Practical Considerations for a Student Network: Student networks may use IP blocks that are either part of a private range (like 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) or public ranges (if they're provided by an external ISP). For public addresses, WHOIS will usually show the ISP and possibly indicate if the range is dedicated to educational purposes. If the network uses private IP ranges, WHOIS information won't yield public details—instead, administrative and organizational records internal to the institution would be referenced.

Example: Suppose you run:

whois 203.0.113.15

You might see an output like:

NetRange: 203.0.113.0 - 203.0.113.255

CIDR: 203.0.113.0/24

NetName: STUDENT-NET

Organization: XYZ Educational Institute (XYZ-Edu)

This tells you that the address block from 203.0.113.0 to 203.0.113.255 is allocated to the student network, managed by XYZ Educational Institute which might be using services from a specified ISP or maintaining its own routing and connectivity.

B. Setting Up IP Addresses and Subnet Masks on Network Devices

1. Determining Your IP Scheme: Before configuration, ensure you have a clear IP address plan. For example, if your student network uses the 192.168.1.0/24 subnet, the standard subnet mask will be 255.255.255.0. Document which device (router, switch, or computer) is assigned which address. This plan helps avoid conflicts and ensures proper routing.

2. Configuring on Different Devices:

On a Cisco Router/Switch (CLI): Access the device via the console or remote terminal:

```
enable
configure terminal
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
Exit
```

 Replace GigabitEthernet0/0 with the appropriate interface, and the IP with the one you've planned for the device. Make sure you apply the configuration to every interface that requires connectivity within your network.

 On a Windows PC:

Open the Network Connections panel.

Right-click your active network adapter and select **Properties**.

Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Choose "Use the following IP address" and enter your IP address, subnet mask (e.g., 255.255.255.0), default gateway, and DNS servers as required.

 On a Linux Machine: You can use either the ifconfig command (older method) or the modern ip command:

sudo ip addr add 192.168.1.10/24 dev eth0

sudo ip link set eth0 up

3. Using a Subnetting Example: If your network requires segmentation into smaller subnets (say splitting a /24 into four /26 subnets), calculate the new subnet masks accordingly. The table below shows a simple breakdown:

Subnet	IP Range	Subnet Mask	Usable Host Range
1	192.168.1.0 - 192.168.1.63	255.255.255.192 (/26)	192.168.1.1 - 192.168.1.62
2	192.168.1.64 - 192.168.1.127	255.255.255.192 (/26)	192.168.1.65 - 192.168.1.126
3	192.168.1.128 - 192.168.1.191	255.255.255.192 (/26)	192.168.1.129 - 192.168.1.190
4	192.168.1.192 - 192.168.1.255	255.255.255.192 (/26)	192.168.1.193 - 192.168.1.254

Using the table above, you can assign each network interface within your devices an IP address that falls into the appropriate range. Remember to reserve the first IP (network address) and the last IP (broadcast address) in each subnet.

4. Verifying the Configuration: After setting the IP addresses and subnet masks:

Use the ping command to test connectivity between devices.

On Cisco devices, show ip interface brief will display your interface status and addresses.

On Windows, use ipconfig in the command prompt; on Linux, ifconfig or ip addr to check current IP settings.

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

IX Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Which command is commonly used to query WHOIS information for a domain or IP address?
2. What information can you typically obtain from a WHOIS query for an IP address?
3. Which subnet mask corresponds to a network with 256 possible IP addresses?
4. What is the purpose of assigning a subnet mask to a network device?
5. If a network device is assigned the IP address \192.168.1.10 \ with a subnet mask of \255.255.255.0 \, what is the network address?

……

……

……

……

……

……

……

……

……

……

X References:

1. https://www.whois.com/whois/
2. https://iplocation.io/ip-whois-lookup

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total(out of 25)	
	Dated Signature of Course Teacher	

Practical No. 2: Identify and resolve network issues using network diagnostic tools like ping, tracert, show,debug commands.

I Practical Significance

In practical applications, these tools are essential for ensuring optimal network performance, minimizing downtime, and enhancing security by detecting anomalies or misconfigurations. Whether it's troubleshooting slow connections, identifying failed links, or resolving routing errors, mastering these diagnostic commands empowers network professionals to maintain seamless and reliable communication across infrastructures.

II Industry / Employer Expected Outcome(s)

Optimized network performance: ISPs use these tools to diagnose packet loss, latency issues, and routing failures, improving service reliability.

Fault isolation: Traceroute helps ISPs identify bottlenecks in global network routes, ensuring efficient data transmission.

III Course Level Learning Outcomes(s)

Analyse the packet structure of IPv4 and IPv6.

IV Laboratory Learning Outcome(s)

LLO 2.1 Troubleshoot network problems.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI Relevant Theoretical Background

Effective troubleshooting relies on understanding the **OSI model**, **TCP/IP stack**, and **network protocols**. Identifying issues requires analyzing network traffic, connectivity, and performance.

Stepwise Procedure

1. Ping: Testing Basic Connectivity

What It Does:

Ping sends ICMP Echo Request packets to a target host and waits for an Echo Reply.

It's your first check to see if a device is reachable and to measure packet loss and latency.

How to Use It:

Command Example:

ping 8.8.8.8

Interpreting the Results:

Replies Received:

Indicates the target is reachable.

Check latency values for any significant delay.

Timeouts or Packet Loss:

May suggest connectivity issues, firewall blocking ICMP traffic, or network congestion.

Troubleshooting Steps:

Verify Local Configuration: Check IP settings and cabling.

Examine Firewalls: Make sure ICMP isn't being blocked by a firewall.

Rerun from Multiple Points: If possible, ping from different network segments to narrow down the issue.

2. Tracert/Traceroute: Mapping the Route

What It Does:

Tracert (on Windows) or **traceroute** (on Linux/Mac) displays the path packets take to reach a destination.

It highlights each "hop" (router or switch) along the way, which can reveal segments of the network where delays or blockages occur.

How to Use It:

Windows Command Example:

tracert google.com

Linux/Mac Command Example:

traceroute google.com

Interpreting the Results:

Hops with High Latency:

Identify a hop where the response time jumps significantly.

Missing or Asterisked Hops:

Indicates that replies aren't being returned (could be due to a firewall or an unreachable router).

Troubleshooting Steps:

Isolation: Pinpoint whether the issue is within your network or on an external segment.

Contact the ISP: If the issue is outside your control (beyond your router), you might need to reach out to your Internet Service Provider (ISP) for further diagnosis.

3. Show Commands: Inspecting the Device's Status

What It Does:

On network devices like Cisco routers or switches, **show commands** provide detailed, real-time information about their configuration and status.

Key Commands:

Interface Status:

```
show ip interface brief
```

Lists all interfaces along with their IP addresses, operational state, and status.

Current Configuration:

```
show running-config
```

Displays the active configuration which helps verify if settings have been applied as expected.

Troubleshooting Steps:

Identify Down Interfaces:

Use the output from show ip interface brief to discover if any interface is administratively down or in error.

Verify Configuration:

Compare show running-config with your network design documentation to ensure no misconfigurations.

Logs:

Use show log (or similar commands) to review system messages that may indicate hardware or software errors.

4. Debug Commands: Getting Live Traffic Data

What It Does:

Debug commands provide a real-time stream of what's happening on a device.
They can be incredibly powerful to see, for example, how packets are being processed or why certain routes are chosen.

How to Use It:

Example Command:

debug ip packet detail

This displays detailed information about IP packets as they move through the device.

Interpreting the Output:

Real-Time Data:

Watch for error messages, denied packets, or misrouted traffic.

Volume of Output: Debug commands can be very verbose; filter the debug output to reduce CPU usage and focus on your issue.

Important Considerations:

Performance Impact: Use debugging sparingly in a production environment because it can overload the device.

Always Disable After Use:

Stop debugging with:

```
undebug all
```

Troubleshooting Steps with Debug:

Enable and watch for anomalies when recreating the issue.

If the output indicates unexpected packet drops or routing errors, adjust configurations accordingly.

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

……..

……

……

IX

Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. What is the primary purpose of the 'ping' command?
2. Which protocol does the 'tracert' command primarily rely on?
3. What does the command 'show ip route' display?
4. Which command would you use to monitor real-time packet flow on a Cisco router?

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

X References:

1. https://www.geeksforgeeks.org/network-troubleshooting-techniques/
2. https://utilizewindows.com/network-troubleshooting-using-ping-tracert-ipconfig-nslookup-commands/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total(out of 25)	
	Dated Signature of Course Teacher	

Practical No. 3: Run a Network Communication Script on "Kali Linux"

I Practical Significance

Running a network communication script on Kali Linux has significant practical applications in cybersecurity, ethical hacking, and network administration. It enables professionals to scan networks, identify vulnerabilities, automate security testing, and monitor traffic efficiently. By leveraging tools like Nmap, Wireshark, and tcpdump, users can analyze packet data, detect anomalies, and simulate real-world cyber threats for penetration testing. Additionally, such scripts are crucial for incident response and forensic analysis, helping organizations strengthen their security posture and mitigate risks proactively.

II Industry / Employer Expected Outcome(s)

Organizations expect outcomes such as enhanced security through automated vulnerability detection and penetration testing, efficient network monitoring to identify threats in real time, and optimized incident response by analyzing packet data for forensic investigations.

III Course Level Learning Outcomes(s)

CO1 - Analyze the packet structure of IPv4 and IPv6.

IV Laboratory Learning Outcome(s)

LLO 3.1 Develop and run a network communication script to monitor network communication at IP layer.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI 1. Networking Concepts

- **OSI Model & TCP/IP Stack:** Understanding how network communication works across different layers.
- **Protocols:** TCP, UDP, ICMP, and HTTP are commonly used in network communication scripts.
- **Packet Analysis:** How data is transmitted, received, and interpreted in packet form.

2. Scripting for Network Communication

- **Python & Bash:** Popular scripting languages for automating network tasks.

- **Socket Programming:** Using Python's socket library to establish communication between devices.
- **Command-Line Tools:** ping, traceroute, netstat, and nc for network diagnostics.

Stepwise Procedure

1. Create a Python Script

Open a Terminal on Kali Linux.

Create a new file, for example named network_script.py, using a text editor like nano:

nano network_script.py

Paste the following sample code into the file:

python

#!/usr/bin/env python3import socketimport sys

```
def start_server():
    # The server will listen on all interfaces at port 5000.
    host = "  # " means all available interfaces.
    port = 5000
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        s.bind((host, port))
    except Exception as e:
        print(f"Error binding server: {e}")
        sys.exit(1)
        s.listen(1)
    print(f"Server listening on port {port}...")
    while True:
        conn, addr = s.accept()
        print(f"Connection established from {addr}")
        while True:
            data = conn.recv(1024)
            if not data:
break
```

```
            print("Received:", data.decode())
            # Sending a response back to the client.
            conn.sendall(f"ACK: {data.decode()}".encode())
        conn.close()
        print("Connection closed.")
def start_client():
    # The client connects to the server at the specified host and port.
    host = '127.0.0.1'  # Replace with server IP if running on different machines.
    port = 5000
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        s.connect((host, port))
    except Exception as e:
        print(f"Unable to connect to the server: {e}")
        sys.exit(1)
    message = "Hello from client!"
    print("Sending message:", message)
    s.sendall(message.encode())
    data = s.recv(1024)
    print("Received from server:", data.decode())
    s.close()
if __name__ == '__main__':
    if len(sys.argv) != 2:
        print("Usage: python3 network_script.py [server|client]")
        sys.exit(1)
        # Depending on the argument, run as server or client.
    if sys.argv[1].lower() == "server":
        start_server()
    elif sys.argv[1].lower() == "client":
        start_client()
    else:
        print("Invalid option. Use 'server' or 'client'.")
```

Save and exit the editor (in nano, press Ctrl + O, then Enter to save, and Ctrl + X to exit).

2. Prepare and Run the Script

Make the script executable (optional):

bash

chmod +x network_script.py

Open Two separate terminal windows (or use multiple tabs) because you'll run the server and client simultaneously.

Start the Server:

In the first terminal, run:

python3 network_script.py server

You should see output like:

Server listening on port 5000...

Run the Client:

In the second terminal, run:

python3 network_script.py client

The client will send the message, and you'll see output on both the client and server terminals that confirms the data was exchanged.

3. Troubleshooting & Considerations

Firewall or Network Restrictions: Ensure that Kali Linux's firewall or any network security rules are configured to allow connections on the port you choose (in this example, port 5000).

IP Address Adjustments: When running the server and client on separate machines, update the host variable in the client section with the server's IP address.

Error Handling: The script includes basic error handling. Watch for bind errors (if the port is already in use) or connection errors (if the server isn't running).

Use in Lab Environments: Kali Linux is designed for network testing and penetration labs—always ensure you have authorization when running these scripts outside your controlled lab environment.

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

IX Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Which Python library is commonly used for socket programming to establish network communication?
2. What command in Kali Linux is used to capture and analyze network packets in real-time?
3. Which tool in Kali Linux is primarily used for network scanning and discovering open ports?
4. What is the purpose of the '-sS' flag in the Nmap command?
5. Which command in Kali Linux can be used to test connectivity to a specific IP address or hostname?

……

……

……

……

……

……

……

……

X References:

1. https://www.geeksforgeeks.org/how-to-use-nmap-script-engine-nse-scripts-in-linux/
2. https://www.webasha.com/blog/how-to-use-shell-scripting-in-kali-linux-for-automation-the-complete-guide
3. https://www.cyberpratibha.com/blog/using-the-command-line-to-configure-network-interface-in-kali-linux/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total(out of 25)	
	Dated Signature of Course Teacher	

Practical No. 4: *Configure basic routing protocols using any relevant software/virtual lab.

I Practical Significance

Configuring basic routing protocols using relevant software or virtual labs has immense practical significance in networking and IT infrastructure management. It allows professionals to efficiently route data between networks, ensuring seamless communication and connectivity. Through hands-on configuration in virtual environments, users gain real-world experience with protocols like RIP, OSPF, and BGP, which are essential for optimizing network performance and scalability.

II Industry / Employer Expected Outcome(s)

Industries expect better security control over network traffic, faster troubleshooting, and adherence to standards set by certifications like CCNA or Network+.

III Course Level Learning Outcomes(s)

CO2 - Configure Static and Dynamic Routing Protocols Using Simulators.

IV Laboratory Learning Outcome(s)

LLO 4.1 Implement Routing Protocols.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI Relevant Theoretical Background

1. Understanding Routing Protocols

Routing protocols enable routers to communicate, exchange route information, and make decisions about forwarding packets. Basic routing protocols include:

RIP (Routing Information Protocol): Uses hop count as a metric to determine the best path.

OSPF (Open Shortest Path First): A link-state protocol that calculates the shortest path based on bandwidth and cost.

EIGRP (Enhanced Interior Gateway Routing Protocol): A hybrid protocol using both distance-vector and link-state concepts.

2. Types of Routing

Static Routing: Manually configured routes that do not change unless updated by an administrator.

Dynamic Routing: Routes are automatically updated based on network topology changes using protocols like RIP, OSPF, and EIGRP.

3. Virtual Lab Setup

For configuration practice, you can use Cisco Packet Tracer, GNS3, or EVE-NG:

Cisco Packet Tracer: A beginner-friendly simulator for configuring basic routing protocols.

GNS3: A more advanced emulator that supports real Cisco IOS images.

EVE-NG: A powerful networking lab environment used by professionals.

Stepwise Procedure

Step 1: Set Up the Virtual Environment

- Use **Cisco Packet Tracer** for a simple setup or **GNS3/EVE-NG** for a real-world experience.
- Add **routers** and **end devices** to your topology.
- Configure interface IP addresses using static addressing.

Step 2: Configure Basic Routing Protocols

1. RIP (Routing Information Protocol)

RIP is a simple distance-vector protocol used for smaller networks.

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# exit
Router(config)# write memory
```

- RIP uses hop count for path selection and broadcasts updates every 30 seconds.

2. OSPF (Open Shortest Path First)

OSPF is a link-state protocol suited for larger networks.

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Router(config-router)# network 10.0.0.0 0.0.0.255 area 0

Router(config-router)# exit

Router(config)# write memory

- OSPF organizes routers into areas to optimize routing.

3. Static Routing (Simple Manual Configuration)

Static routing can be set up when you want full control over the routes.

Router(config)# ip route 10.0.0.0 255.255.255.0 192.168.1.1

Router(config)# write memory

- This ensures traffic for **10.0.0.0/24** is sent via **192.168.1.1**.

Step 3: Test the Configuration

- Use ping to verify connectivity.
- Run show ip route to check routing table entries.
- Debug with debug ip routing (if needed).

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

……

……

……

IX Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. You set up a RIP routing configuration between two routers, but one router is not receiving routes. What are the first three troubleshooting steps you take?
2. In OSPF, what happens if two routers have different area IDs but belong to the same subnet? How would you resolve this issue?
3. After configuring EIGRP, you notice high latency in packet forwarding. What parameters would you check and modify to optimize performance?What is difference between = = ,equals() & compareTo()?

……

……

……

……

……

……

……

……

……

……

……

……

……

……

X References:

1. https://itexamanswers.net/lab-106-configuring-routing.html
2. https://www.geeksforgeeks.org/rip-routing-configuration-using-3-routers-in-cisco-packet-tracer/
3. https://jbcsec.com/networkplus-lab-understanding-routing/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
1.	Expected output:15%	
2.	Timely Submission:15%	
3.	Answer to sample questions:10%	
	Total (out of 25)	
	Dated Signature of Course Teacher	

Practical No. 5: Capture and Analyze ICMPv4 Packets using appropriate tool

I Practical Significance

Capturing and analyzing ICMPv4 packets using appropriate tools is essential for network diagnostics, security analysis, and troubleshooting connectivity issues. ICMPv4 (Internet Control Message Protocol version 4 helps identify network reachability, latency, and errors by exchanging control messages between devices.

II Industry / Employer Expected Outcome(s)

Capturing and analyzing ICMPv4 packets using appropriate tools leads to industry-expected outcomes such as improved network diagnostics, enhanced security monitoring, and efficient troubleshooting.

III Course Level Learning Outcomes(s)

CO2 - Configure Static and Dynamic Routing Protocols Using Simulators.

IV Laboratory Learning Outcome(s)

LLO 5.1 Tabulate and interpret the captured ICMPv4 packet parameters using relevant network analysis software.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI Introduction to ICMPv4

The **Internet Control Message Protocol version 4 (ICMPv4)** is a network layer protocol used for error reporting and diagnostics. It helps devices communicate network issues, such as unreachable destinations or excessive latency.

Packet Capture Tools

To analyze ICMPv4 packets, tools like **Wireshark** and **tcpdump** are commonly used. These tools allow network administrators to inspect packet headers, identify anomalies, and troubleshoot connectivity issues.

ICMPv4 Packet Structure

An ICMPv4 packet consists of:

- **Type**: Defines the message category (e.g., Echo Request, Destination Unreachable).
- **Code**: Provides additional context for the message type.
- **Checksum**: Ensures data integrity.
- **Identifier & Sequence Number**: Used for tracking requests and replies in Echo messages.

Capturing ICMPv4 Packets

Using **Wireshark**, you can filter ICMP packets by applying the filter icmp in the search bar. This allows you to view only ICMP traffic, making analysis more efficient.

Analyzing ICMPv4 Packets

Once captured, packets can be analyzed for:

- **Round-trip time (RTT)** in Echo Requests and Replies.
- **Error messages**, such as "Destination Unreachable" or "Time Exceeded."
- **Network congestion**

Stepwise Procedure

Step 1: Install a Packet Capture Tool

- **Wireshark** (GUI-based, user-friendly)
- **tcpdump** (CLI-based, used in Linux/macOS)
- **PingPlotter** (Windows, focuses on network latency)

Step 2: Start Capturing ICMP Packets

Using Wireshark

1. Open Wireshark and select your active network interface.
2. Start packet capture and apply a display filter for ICMP:
   Icmp
3. Run a ping command in the terminal to generate ICMP packets:
   ping 8.8.8.8

Observe ICMP **Echo Requests** and **Replies** in the capture window.

Using tcpdump (Linux/macOS)

1. Open a terminal and run:

sudo tcpdump -i eth0 icmp

Initiate a ping request:

ping 8.8.8.8

1. tcpdump will display the captured packets in real-time.

Step 3: Analyze the Packets

- Look for **Type and Code** values (e.g., Type 8 for Echo Request, Type 0 for Echo Reply).
- Check **TTL (Time-To-Live)** values to understand packet lifespan.
- Examine **checksums** to ensure integrity.
- Identify packet delays or dropped responses to diagnose network issues.

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

IX Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Which command in tcpdump captures only ICMPv4 packets?
2. What steps should you follow to filter ICMPv4 traffic in Wireshark?
3. How can you differentiate between an Echo Request and an Echo Reply in Wireshark?

4. What information does an ICMP Destination Unreachable packet provide?
5. Why is the Time Exceeded message useful in network troubleshooting?

X References:

1. https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/
2. https://library.mosse-institute.com/articles/2022/07/analyzing-icmp-traffic-with-wireshark/analyzing-icmp-traffic-with-wireshark.html
3. https://cammyd.com/wireshark-101-sending-and-analyzing-an-icmp-ping-part-1/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total out 25	
	Dated Signature of Course Teacher	

Practical No. 6: *Configure, diagnose and troubleshoot TCP and UDP connection issues using diagnostic tools like netstat, wireshark, iperf

I Practical Significance

Configuring, diagnosing, and troubleshooting TCP and UDP connection issues using diagnostic tools like netstat, Wireshark, and iperf is crucial for ensuring network reliability, performance, and security. These tools help professionals monitor data transmission, detect anomalies, and resolve connection bottlenecks efficiently.

II Industry / Employer Expected Outcome(s)

Configuring, diagnosing, and troubleshooting TCP and UDP connection issues using tools like netstat, Wireshark, and iperf leads to industry-expected outcomes such as enhanced network performance, improved security, and efficient troubleshooting.

III Course Level Learning Outcomes(s)

CO3 - Illustrate functions of Transport layer protocols.

IV Laboratory Learning Outcome(s)

LLO 6.1 Create and troubleshoot TCP and UDP connections.

V Relevant Affective Domain related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices

VI Relevant Theoretical Background

- **Integer class methods:**

TCP vs. UDP: Theoretical Background

- **TCP (Transmission Control Protocol)** ensures reliable, ordered, and error-checked delivery of data. It uses mechanisms like the **three-way handshake** (SYN, SYN-ACK, ACK) to establish connections and **ACK packets** for error recovery.**UDP (User Datagram Protocol)** is connectionless and does not guarantee delivery, making it faster but less reliable. It is commonly used for real-time applications like VoIP and gaming.

Diagnostic Tools for Troubleshooting

1. **Netstat**:
    - Displays active connections, listening ports, and routing tables.
    - Helps identify **TCP/UDP connection states** (e.g., ESTABLISHED, TIME_WAIT).
    - Useful for detecting **network congestion or dropped connections**.
2. **Wireshark**:
    - Captures and analyzes network packets.
    - Helps diagnose **TCP retransmissions, handshake failures, and UDP packet loss**.
    - Provides insights into **latency, jitter, and malformed packets**.
3. **Iperf**:
    - Measures network performance by generating TCP/UDP traffic.
    - Helps identify **bandwidth bottlenecks, jitter, and packet loss**.
    - Useful for **stress-testing network configurations**

Stepwise Procedure

Step 1: Identify Connection Issues

- TCP issues: May involve slow connections, dropped packets, or retransmissions.
- UDP issues: Often relate to lost packets, jitter, or inconsistent data delivery.

Step 2: Use Diagnostic Tools

1. Netstat (Checking Active Connections)

Netstat is a command-line tool used to inspect network connections.

- To list active TCP and UDP connections:

netstat –an

To check which application is using a specific port:

netstat -b (Windows)

netstat -tulpn (Linux)

To check which application is using a specific port:

netstat -an | findstr "LISTEN"

2. Wireshark (Packet Analysis)

Wireshark allows real-time inspection of TCP and UDP packets.

- Apply filters for TCP or UDP:

tcp || udp

- Check TCP retransmissions (tcp.analysis.retransmission) for packet loss issues.
- Look for UDP checksum errors or missing packets that indicate unreliable transmission.

3. Iperf (Network Performance Testing)

Iperf helps measure TCP and UDP bandwidth and latency.

- Run a TCP performance test between two systems:

iperf -s (Start server)

iperf -c <server_ip> (Run test from client)

Run a UDP test:

iperf -u -c <server_ip> -b 100M

- Check latency (-i 1 flag for interval monitoring) and jitter.

Step 3: Troubleshooting Common Issues

- High latency or packet loss? Adjust TCP window size and verify network congestion.
- UDP data loss? Ensure proper buffer size and use reliable transport alternatives.
- Application not responding? Verify firewall settings and listen states via netstat.

VII Resources required (Additional)

Sr. No.	Name of Resource	Broad Specification	Quantity	Remarks (If any)
1				

VIII Conclusion

……

……

……

……

……

IX Practical related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. How can you use netstat to identify active TCP connections on a server?
2. What does the TIME_WAIT state in netstat indicate about a TCP connection?
3. How would you use Wireshark to detect TCP retransmissions in a network capture?
4. What steps would you take in Wireshark to analyze a failed TCP three-way handshake?
5. Write a program to convert Integer object value into primitive datatype byte, short and double value

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

.....

.....

.....

.....

.....

.....

.....

X References:

1. https://www.cisconetsolutions.com/iperf-network-testing-and-troubleshooting-tool/
2. https://serverfault.com/questions/1117915/iperf3-test-bandwidth-tcp-much-slower-than-udp
3. https://e2e.ti.com/support/wireless-connectivity/wi-fi-group/wifi/f/wi-fi-forum/494755/udp---tcp-socket-examples-issues---iperf3

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total out of 25	
	Dated Signature of Course Teacher	

Practical No. 7: Configure DNS using relevant software.

I Practical Significance

Configure DNS involves setting up the Domain Name System (DNS), which is a fundamental part of the internet that translates human-readable domain names (like www.example.com) into IP addresses. DNS acts like a phonebook for the internet, enabling users to access websites and services easily. This practical helps understand how DNS works and its role in ensuring smooth and efficient network communication. Proper DNS configuration is crucial for reliable internet connectivity and system performance.

II Industry / Employer Expected Outcome(s)

Students to understand the role of DNS in network infrastructure and to demonstrate the ability of configuring and troubleshooting DNS settings effectively. This skill is essential for ensuring seamless network communication and system reliability in real-world IT environments.

III Course Level Learning Outcome(s)

CO4: Implement Application layer protocols on a network.

IV Laboratory Learning Outcome(s)

LLO7.1: Implement Application layer protocols on a network.

V Relevant Affective Domain Related Outcomes

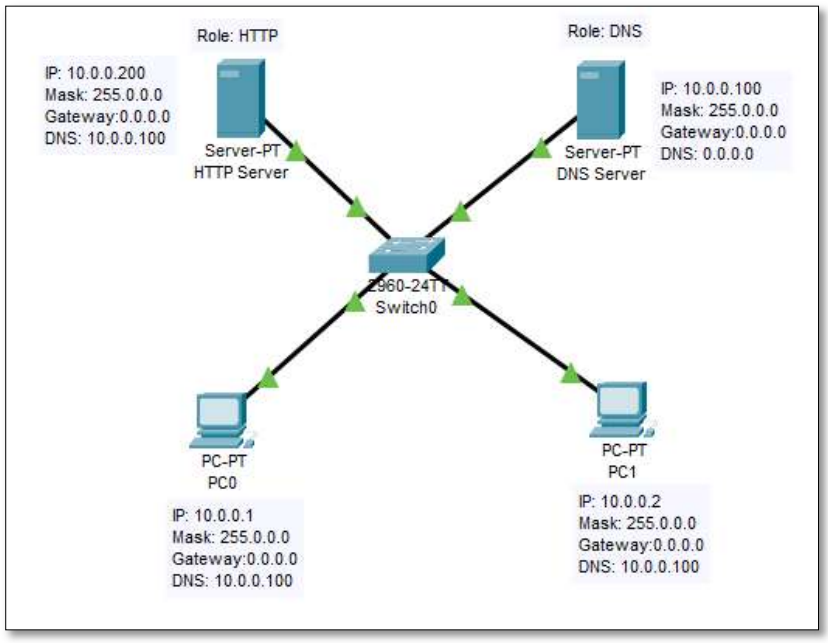
1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

The Domain Name System (DNS) is a hierarchical system that translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on a network. It acts like the internet's phonebook, allowing users to access websites and services using easy-to-remember names instead of numeric addresses. Name resolution is the process by which a DNS client (usually a computer or device) queries DNS servers to find the IP address corresponding to a domain name. When a user enters a domain name, the DNS resolver contacts DNS servers in a sequence to locate the correct IP address. Once found, this IP address is returned to the client, enabling it to connect to the desired website or service.

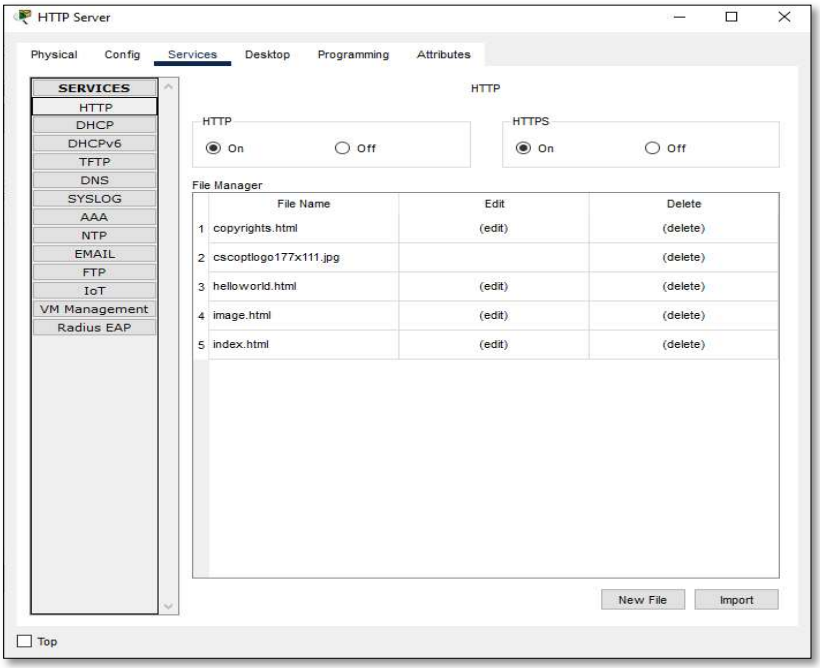
Stepwise Procedure

1. Topology

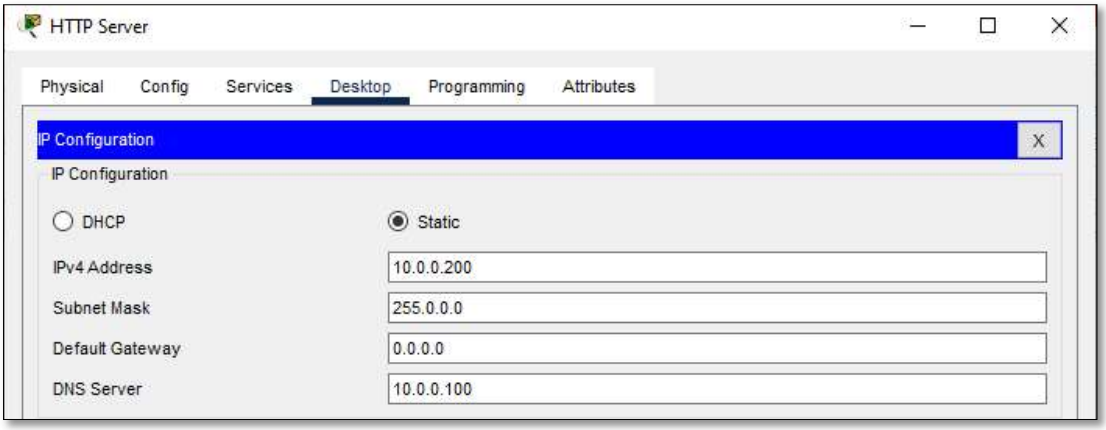


2. Configuring HTTP Server

Now, select HTTP Server, go to Services tab and start HTTP service. You will see already there are some webpages uploaded to webserver (HTTP). You can upload or create own page too.

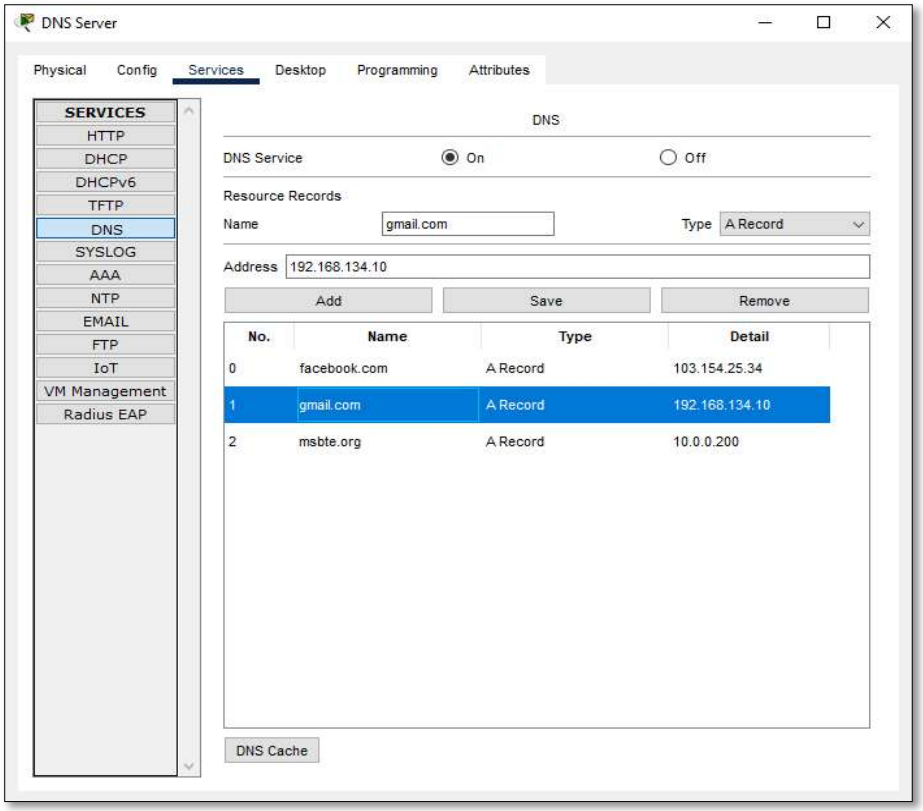


Now go to Desktop Tab and perform IP configuration for HTTP server as shown below and kept rest to defaults.

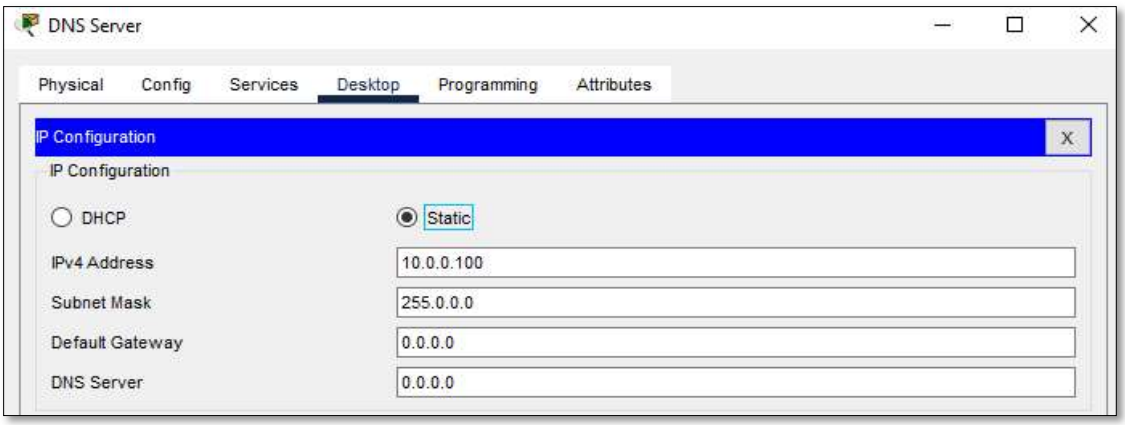


3. Configuring DNS Server

Now, select DNS Server, go to Services tab and start DNS service. You can also add new record to be resolved by using its domain name and corresponding IP address associated with it.

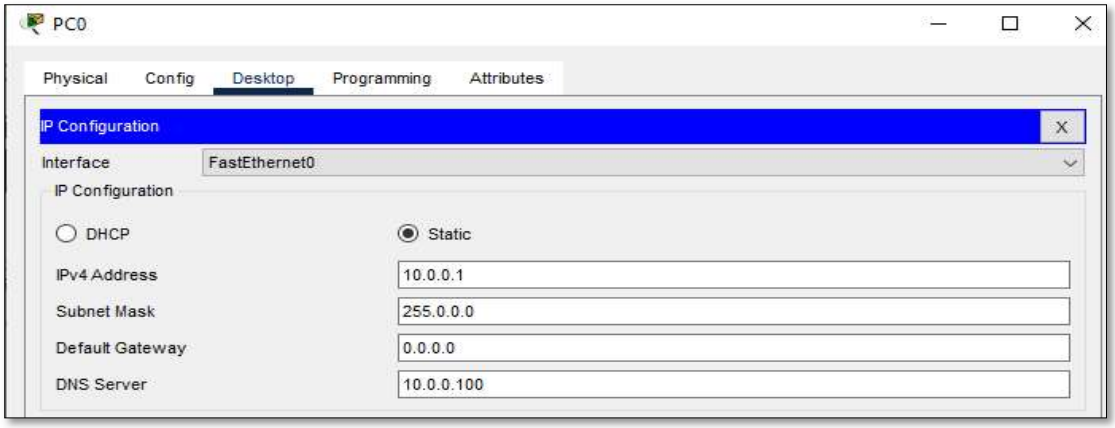


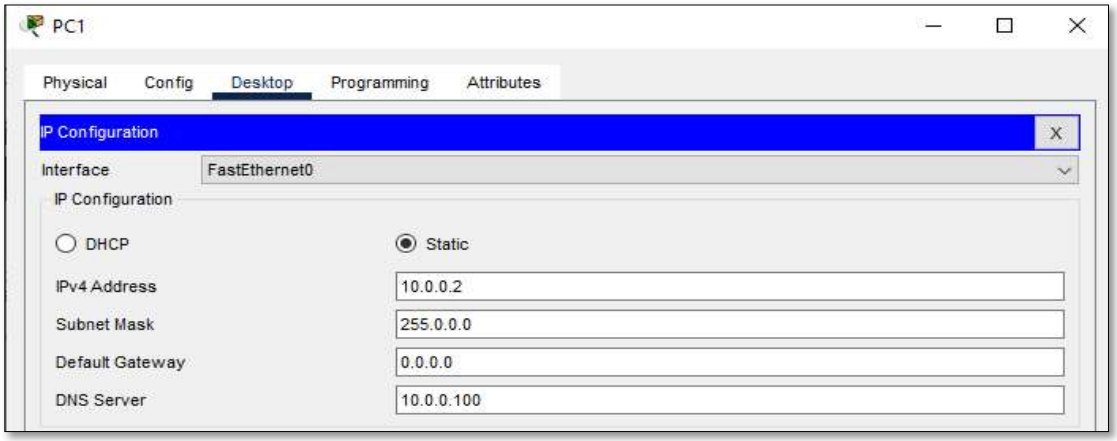
Now go to Desktop Tab and perform IP configuration for DNS server as shown below and kept rest to defaults.



4. Configuring PC

Perform IP Configuration for PCs, PC0 and PC1. Click on one the PC, go to Desktop Tab then select IP Configuration. Enter IP address details as shown in Topology.



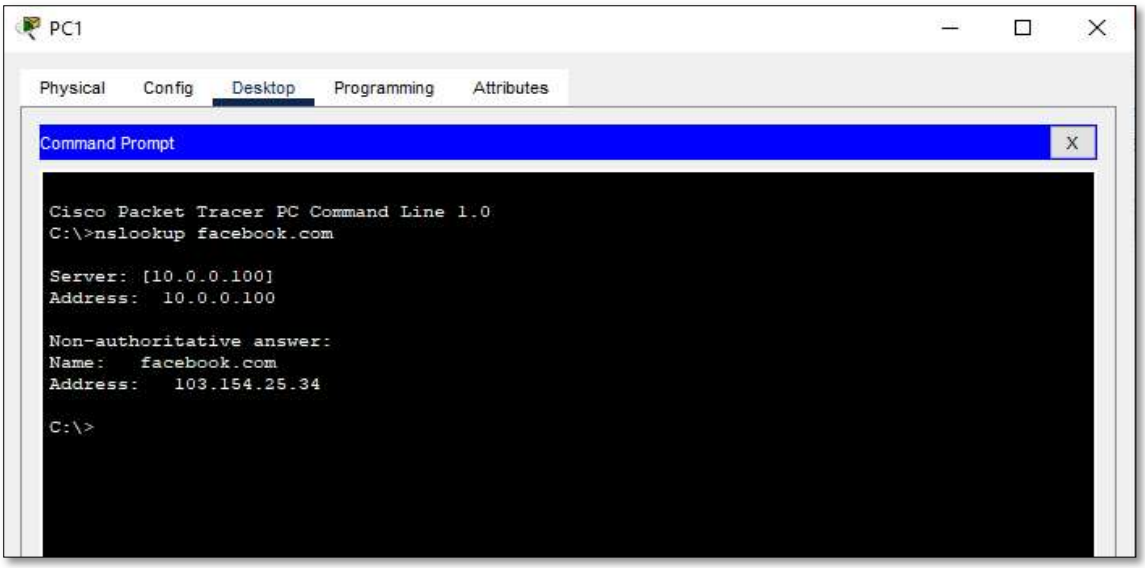


5. Observations to be done

In Cisco packet tracer there two modes one is Real time mode and second one is Simulation mode. We will first check how DNS help us to resolve the Domain name in real time mode and later we will use Simulation mode to check what is role of DNS in accessing a webpage using its name instead of IP Address.

Real Time Mode

1. Click on PC0 or PC1.
2. Go to Desktop tab and Open Command Prompt.
3. Enter command as: nslookup facebook.com, you will get answer as IP address associated with the domain name facebook.com
4. Similarly you can look for name resolution for other domain names too.



Simulation Mode

1. Choose mode as Simulation from lower left corner of Cisco Packet Tracer.
2. Click on PC0 or PC1.
3. Go to Desktop tab and open Web Browser.
4. Enter IP address of HTTP server to access web pages which are present at HTTP server. Observe the PDU transfer between HTTP server and PC you chose by clicking on fast forward button. You will observe in this communication there is no role of DNS server, as we are accessing website directly by using its IP address.

5. Now reset the communication and Open browser again and enter domain name associated with your web server. In this case if you look at DNS configuration we have domain name msbte.org which has same IP Address as that of HTTP server's IP Address. So msbte.org is domain associated with webpages present on the HTTP server. Let's see PDU transfer by clicking on fast forward button. Here you will observe DNS comes in role of name resolution.
6. So, observe both communication between HTTP server and PC using IP address and Domain associated with a particular website and how DNS has role in name resolution.

VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII Conclusion

……

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Explain the purpose of DNS in a computer network and how it helps users access websites.
2. Describe the basic steps involved in the DNS name resolution process.
3. How would you configure a DNS server to resolve a domain name to its corresponding IP address?
4. What troubleshooting steps would you take if a DNS server is not resolving domain names correctly?

……

……

……

……

……

X References:

1. https://www.geeksforgeeks.org/configuring-dhcp-and-web-server-in-cisco-packet-tracer/
2. https://www.cisco.com/c/en/us/support/docs/ip/domain-name-system-dns/24182-reversedns.html
3. https://drive.google.com/file/d/1dwkiRBQsmfQfnh0IVSndmR03LFFUhEBh/view?usp=drivesdk

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
7.	Logic formation:30%	
8.	Debugging ability:20%	
9.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
10.	Expected output:15%	
11.	Timely Submission:15%	
12.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 8: Configure FTP using relevant software.

I Practical Significance

Configuring FTP focuses on setting up and managing a File Transfer Protocol (FTP) service, which is used to transfer files between computers over a network. It is significant as FTP is widely used for website management, data backup, and file sharing in organizations. It helps us to understand client-server communication, user authentication, and access control in file transfers. Proper FTP configuration ensures secure and efficient data exchange in real-world IT environments.

II Industry / Employer Expected Outcome(s)

Demonstrate the ability to configure and manage FTP services for secure and efficient file transfer. They should understand FTP server-client communication, user access control, and basic troubleshooting. These skills are essential in roles involving website maintenance, network administration, and data management.

III Course Level Learning Outcome(s)

CO4: Implement Application layer protocols on a network.

IV Laboratory Learning Outcome(s)

LLO8.1: Configure and Test File Transfer Protocol (FTP).

V Relevant Affective Domain Related Outcomes

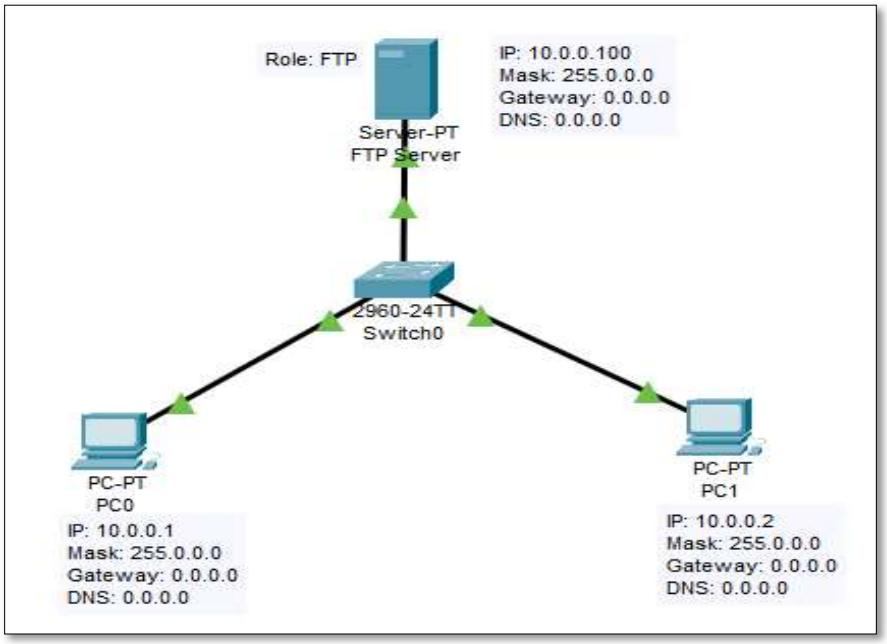
1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

FTP (File Transfer Protocol) is a standard network protocol used to transfer files between a client and a server over a TCP/IP network. It allows users to upload (put) files from the client to the server and download (get) files from the server to the client. FTP plays a key role in website management, data backup, and sharing large files within organizations. By supporting user authentication and file handling commands like put, dir, get, ls, and cd, FTP enables secure and organized remote file management.

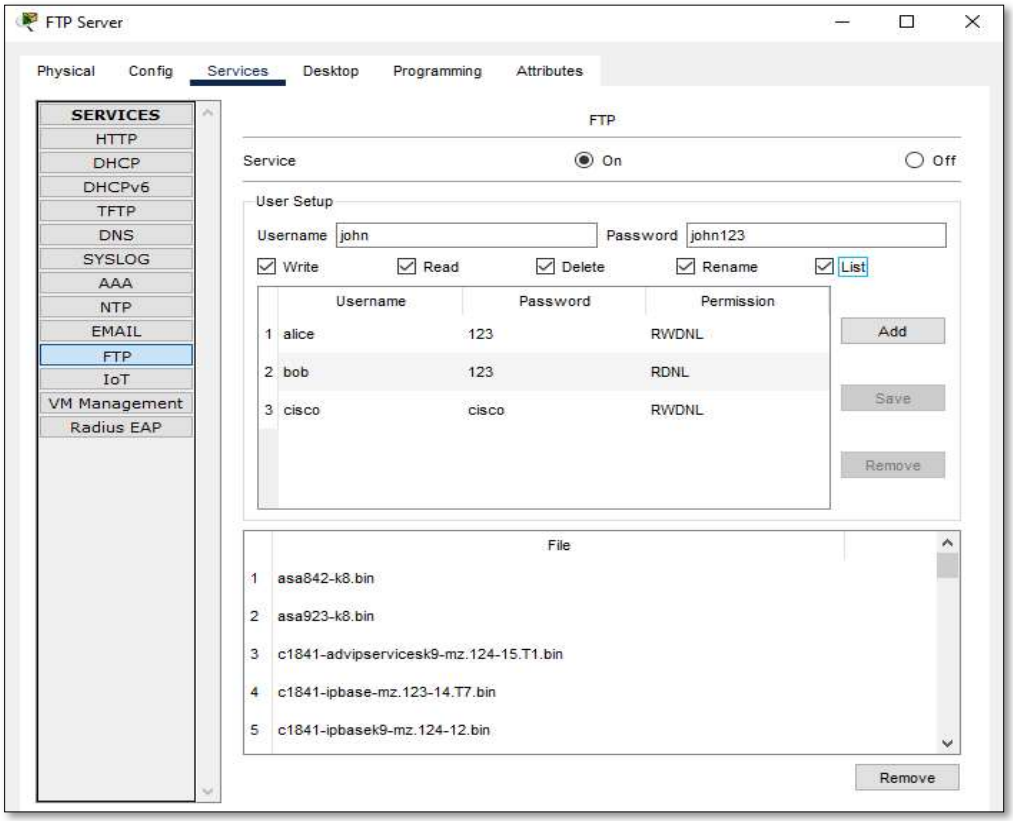
Stepwise Procedure

1. Topology



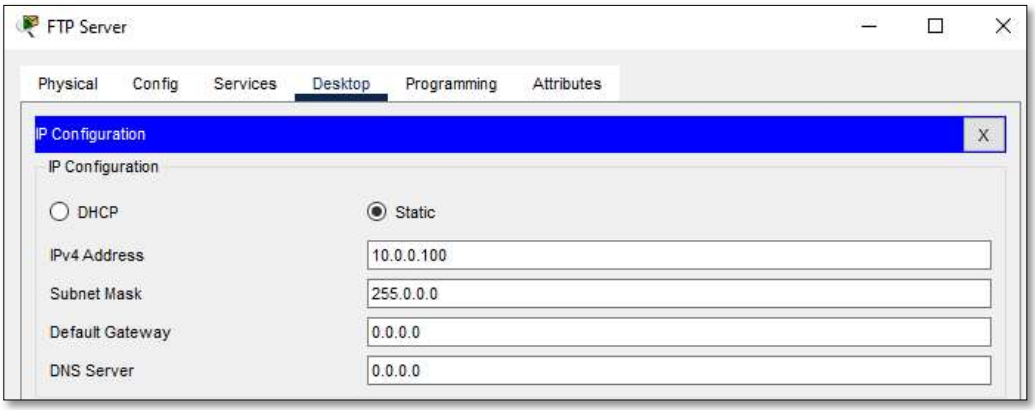
2. Configuring FTP Server

Now, select FTP Server, go to Services tab and start FTP service.



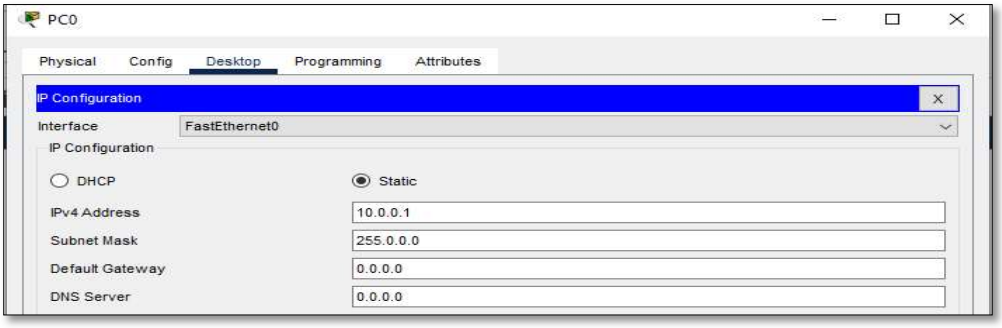
Make FTP service On. You can create and add new user who can avail services of FTP server by assigning credentials like username, password and various kinds of permission like write, read, rename, delete, list etc. can be allowed or denied based on type of user.

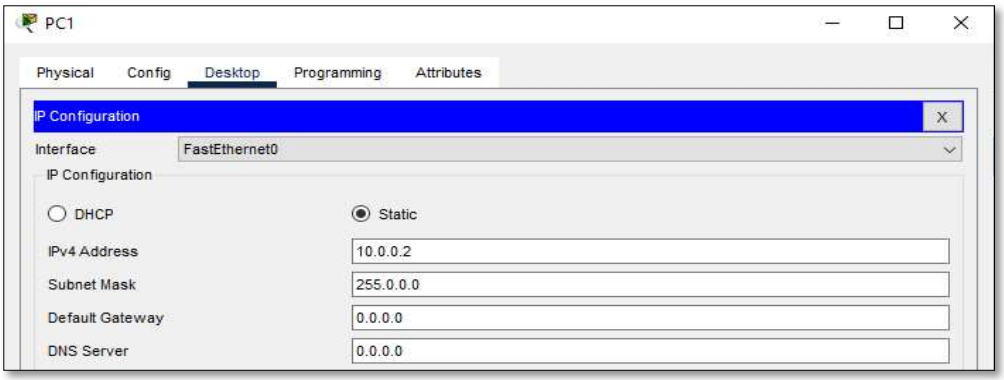
Similarly you can see some files which already uploaded or part of FTP server. Now go to Desktop tab and perform IP configuration for FTP Server as shown in topology.



2. Configuring PC

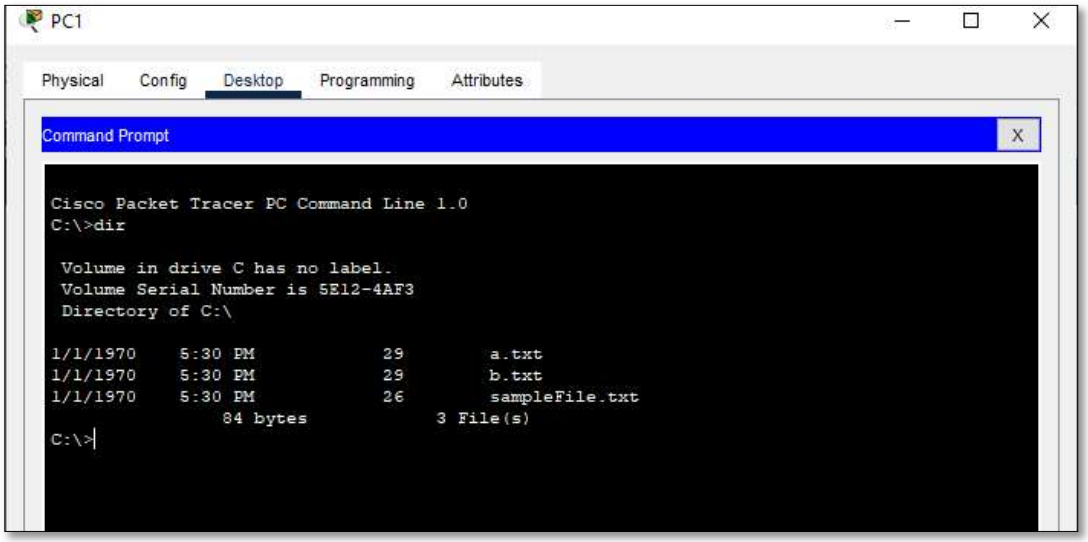
Perform IP Configuration for PCs, PC0 and PC1. Click on one the PC, go to Desktop Tab then select IP Configuration. Enter IP address details as shown in Topology.





3. Observation to be done

1. Open PC0 or PC1, Go to Desktop tab and open Text Editor and create a new text file and save it on your local drive.
2. From Desktop tab open command prompt and enter command as dir, you will all the directory and files which are part of your local drive.



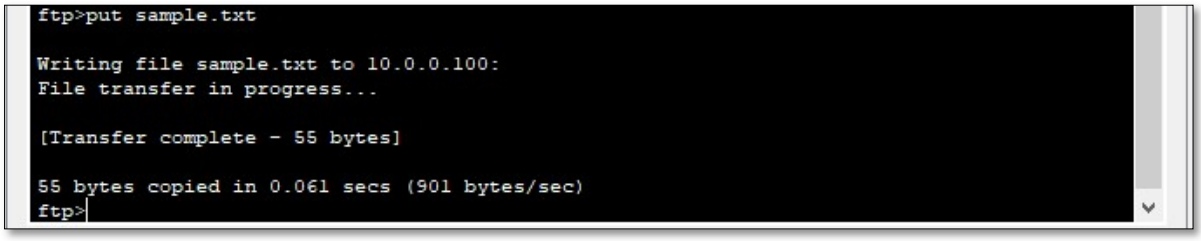
3. Connect with FTP server using its IP address on command prompt.

4. Once it connects it ask for username and password, we already created some users on FTP server with proper credentials and permissions.

5. Now we can use various FTP server commands to list content of directory, read, write, delete, and rename files on FTP.

6. Use dir command to list all directories and files present on FTP server.

7. Let's use put command to write data to FTP server from your local drive that we previously created using Text Editor. Once you finish you check whether it committed or not using dir command.



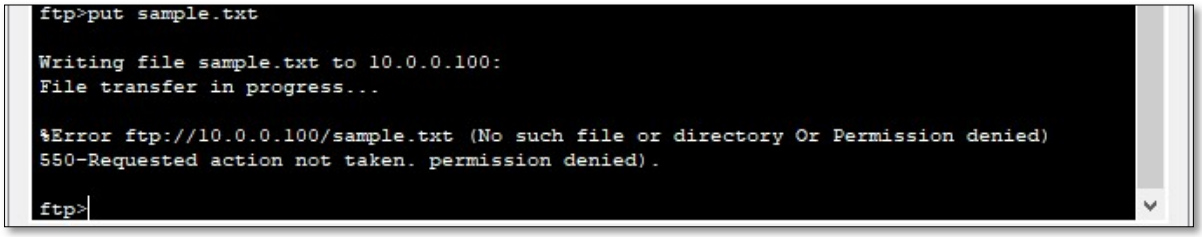
8. Similarly we can use get command to read/download data present on FTP server. It downloads data from FTP server to our local drive. Enter command as get filename. You can check whether file is downloaded or not by exiting from FTP server to local drive by using exit command and execute dir command.

9. We can rename a file present on FTP server using rename command. Enter command as rename oldfilename newfilename. You can check whether rename operation committed or not using dir command.

10. We can delete a file present on FTP server using delete command. Enter command as delete filename. You can check whether rename operation committed or not using dir command.

11. All these operation can be performed only if you have valid permissions do to so and assigned to you by your server administrator. You can remove one of the permission and check the result of that particular operation.

12. Let administrator revoked write permission from user “cisco”. Now I logged in as “cisco” and trying write on FTP server, so this operation will result in error as user “cisco” does not have permission to write.



VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII Conclusion

……

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. What steps are involved in setting up an FTP server on a computer?
2. How would you create and manage user accounts for secure access to an FTP server?
3. Which FTP command is used to upload a file to the server, and which is used to download a file? Explain with an example.
4. After connecting to an FTP server, how would you list the files in a directory and change to another directory?

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

X References:

1. https://www.geeksforgeeks.org/file-transfer-protocol-server-configuration-using-cisco-packet-tracer/
2. https://drive.google.com/file/d/1dxhpSN-14DmwTZ2mysNkm_MfynpojWad/view?usp=drivesdk

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 9: Monitor Network Traffic using Browser Developer tools.

I Practical Significance

Monitoring network traffic using browser developer tools is essential for analyzing how a website loads and communicates with servers. It helps identify slow-loading resources, failed requests, and inefficient API calls, allowing developers to improve performance and fix bugs quickly. Tis tools also aids in verifying data exchanges, testing backend connections, and ensuring secure transmission of information. Additionally, it supports optimization efforts by reveling caching behavior and bandwidth usage.

II Industry / Employer Expected Outcome(s)

To identify and resolve network related issues quickly using browser tools. This leads to faster, more secure, and high performing web applications.

III Course Level Learning Outcome(s)

CO4: Implement Application layer protocols on a network.

IV Laboratory Learning Outcome(s)

LLO9.1: Inspect and debug HTTP Traffic.

V Relevant Affective Domain Related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

HTTP (Hypertext Transfer Protocol) is the standard protocol that allows web browsers and servers to communicate. It uses methods like GET to retrieve data and POST to send data. Each HTTP request and response includes headers with vital details, such as the type of data being sent and its encoding. By monitoring these requests and responses using browser developer tools, you can identify issues like slow loading or missing files. This foundational understanding of HTTP is essential for effectively analyzing network traffic.

Stepwise Procedure

Step 1: Open Your Browser Developer Tools

1. Open browser available with you on your computer, most modern browsers like Google Chrome, Firefox, and Microsoft Edge have built-in developer tools.

2. To open browser's developer tools, In Chrome, Microsoft Edge: Press F12 or Ctrl + Shift + I (Windows/Linux) or Cmd + Option + I (macOS). You can also right-click anywhere on the webpage and select "Inspect".

Step 2: Navigate to the "Network" Tab

1. Finding the Tab: Once the developer tools open, you will see several tabs. Click on the "Network" tab.
2. What You'll See: This tab will display all HTTP requests the browser makes when loading a page. These include requests for HTML files, CSS, JavaScript, images, fonts, and any AJAX (XHR) requests.

Step 3: Capture the Network Traffic

1. Refresh to Capture: With the Network tab open, refresh the webpage by pressing F5 or clicking the refresh icon. Doing so allows the tool to capture all the HTTP requests that occur during the page load.
2. Clear Existing Data (Optional): Most developer tools provide a clear button (a circle with a line through it or a trash can icon). Use it to clear previous data if needed before refreshing.
3. Understanding Captured Data: Every resource loaded by the webpage is now recorded in a list that shows details like URL, request method (GET, POST, etc.), status code, file type, and load time.

Step 4: Explore the Requests List

Detail View: Click on any request in the list to open a detailed view. Here, you'll find several sub-tabs:

Headers:

- Request Headers: Include information such as browser details, content types accepted, cookies, etc.
- Response Headers: Provide details like response type, server information, caching policies, etc.

Preview: A user-friendly display of the response content (useful when it's JSON or HTML).

Response: The raw data returned from the server.

Timing: Breaks down the time taken at each step (DNS lookup, connection, waiting, etc.).

Cookies: Displays cookies related to the request, if any.

Step 5: Filter and Focus on Specific Traffic

Filtering Options:

Use the filter bar at the top of the Network panel to narrow the list of requests. For example, type "image" to see only image files.

Click the XHR (or Fetch) filter to view AJAX requests specifically. This is especially useful when working with dynamic content that loads after the page initially loads.

Custom Filters: If you're looking for a specific file or request URL pattern, type it directly into the filter box. Filtering helps you manage the potentially lengthy and complex list of network requests, allowing you to concentrate on the parts of the traffic that are most relevant to your current task.

Step 6: Analyze HTTP Methods and Status Codes

HTTP Methods:

GET: Used to request data from the server (most common for loading webpages).

POST: Used to submit data to the server (commonly seen in form submissions).

PUT, DELETE, etc.: Often used in API interactions for updating or deleting data.

Status Codes:

200: Request was successful.

404: The requested resource was not found.

500: Server encountered an error.

Step 7: Monitor Ongoing Traffic During Page Interaction

Real-Time Monitoring: Keep the Network tab open while you interact with the webpage. For example,

- Click on buttons or links.
- Submit forms.
- Trigger events that load new content (like scrolling or clicking a "Load More" button).

Observe Dynamic Requests: As you interact, watch for new requests appearing in the list. This is especially useful for modern web applications that use JavaScript frameworks to load data dynamically.

Step 8: Exporting and Saving Network Data

Saving Data for Analysis: Right-click anywhere within the Network tab and select "Save all as HAR"**.**

HAR File: A HAR (HTTP Archive) file contains all loader and request information that you can later review or share for debugging.

VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII.Conclusion

……

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. How do you open the network tab in a browser's developer tools?
2. How do you check if a website's image or file has loaded successfully using network tab?
3. How can you find out how much time a web page takes to load?
4. How can you tell if a file on a webpage failed to load?
5. How do you check the size of a file that loads on a website?

……

……

……

……

……

……

……

……

……

……

……

……

……

……

X References:

1. https://learn.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/
2. https://developer.chrome.com/docs/devtools/network

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 10: Design a simple network for SDN using Mininet.

I Practical Significance

Designing a simple SDN (Software-Defined Networking) network using Mininet is useful because it allows testing and understanding of modern network systems without using real hardware. Mininet is a free tool that runs on a computer and makes it easy to create and test virtual networks. It helps in learning how SDN controls and manages a network through software. This is a simple and low-cost way to practice and explore networking concepts.

II Industry / Employer Expected Outcome(s)

Ability to design, simulate, and troubleshoot SDN networks using tools like Mininet. Proficiency in software-based network control and understanding SDN architecture.

III Course Level Learning Outcome(s)

CO5: Work with various wireless networking technologies.

IV Laboratory Learning Outcome(s)

LLO10.1: Implement SDN using Mininet.

V Relevant Affective Domain Related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

Software-Defined Networking (SDN) is a modern approach to networking where the control of the network is handled by software instead of hardware devices like routers and switches. In SDN, the control plane (which makes decisions) is separated from the data plane (which forwards data), making the network easier to manage and more flexible. Mininet is a free network simulator that creates a virtual network on a single computer, allowing users to design, test, and understand SDN networks without using physical devices. This helps in learning how networks can be controlled and managed through software programs.

Stepwise Procedure

Below is a detailed, step-by-step guide to develop a simple SDN network using Mininet. This covers everything from installing Mininet to creating and testing a basic network topology.

1. Install Mininet

1. Set up your environment**:** It is recommended to use an Ubuntu-based system (or a virtual machine running Ubuntu). You can install Ubuntu via VirtualBox, VMware, or use a dedicated Ubuntu machine.
2. Open the Terminal: Press Ctrl+Alt+T or search for "Terminal" in your applications.
3. Update your system's package list using command: sudo apt-get update
4. Install Minine using command: sudo apt-get install mininet
5. Alternatively, for the latest version and additional features, clone the Mininet repository and run the installation script:

   git clone https://github.com/mininet/mininet.git
   cd mininet
   sudo util/install.sh –a
   The -a flag ensures that all additional packages (like Open vSwitch) are installed.
6. Verify the installation: Test the installation with a built-in test
   sudo mn --test pingall
   This command creates a small network, pings between the hosts, and shows the connectivity. If you see successful pings, the installation is complete.

2. Create a Simple SDN Network

1. Launch Mininet with a predefined topology: Use the following command to create a network with one switch and three hosts.
   sudo mn --topo single,3 --mac --switch ovsk --controller=default

   This command will does following tasks,
   - --topo single,3: Creates a topology with a single switch connected to 3 hosts.
   - --mac: Assigns unique MAC addresses to each host.
   - --switch ovsk: Uses Open vSwitch as the switching software.
   - --controller=default: Uses Mininet’s default controller; this controller is a simple inbuilt one for basic SDN operations.
2. Mininet will initialize and display a command prompt (mininet>), representing the network. Here, you can now interact with your virtual network.

3. Test and Interact with Your Network

1. Display network nodes: Type the command below to see all nodes (hosts and switches),

mininet> nodes

2. Test connectivity: Use the pingall command to test if every host can communicate with every other host.

mininet> pingall

You should see a table reporting the ping responses between the hosts. If every host pings successfully, your network is working correctly.

4. Interact with individual hosts: To open the command line for a specific host (e.g., host h1), type,

mininet> h1

5. Try pinging another host from h1:

h1> ping -c 4 h2

This command sends 4 ping requests from h1 to h2 to ensure network connectivity between those two hosts.

4. Exit and Clean Up

1. Leave the Mininet CLI:To exit Mininet and shut down the virtual network, simply type,

mininet> exit

This command terminates the Mininet session and cleans up the network configuration.

VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII Conclusion

……

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. What command will you use to verify that Mininet is correctly installed on your system, and what is the expected output indicating a successful installation?
2. Create a simple network topology with one switch and two hosts and run the pingall command within the Mininet CLI. What does the output tell you about the connectivity between the hosts?
3. What steps do you take to enter the host's CLI? Execute a ping command. Describe the expected results and what they indicate about the network connectivity?
4. sudo mn --topo tree,depth=2,fanout=2 --mac --controller=default, How many hosts and switches are created in this tree topology?

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

X References:

1. https://www.geeksforgeeks.org/mininet-emulator-in-software-defined-networks/
2. https://www.geeksforgeeks.org/software-defined-networking/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 11: Using Ping and Latency tools perform,

i) Measure latency and packet loss over time using any suitable tool e.g. PingPlotter.

ii) Analyze network packets to detect performance bottlenecks using any suitable tool e.g. Wireshark.

I Practical Significance

Tools like PingPlotter to measure latency and packet loss over time provides insights into the stability and reliability of a network connection, helping to identify intermittent connectivity issues or degraded performance. Continuous monitoring helps in detecting spikes in latency and patterns of packet loss that may not be obvious in short-term testing. Analyzing network packets using a tool like Wireshark enables detailed inspection of network traffic, revealing issues such as retransmissions, congestion, or protocol misconfigurations. This analysis is crucial for pinpointing performance bottlenecks and understanding the root causes of network slowdowns or failures. Together, these tools provide a comprehensive view of network health, supporting informed troubleshooting and optimization.

II Industry / Employer Expected Outcome(s)

To develop the ability to diagnose and resolve network performance issues efficiently using standard tools like PingPlotter and Wireshark. It includes gaining hands-on experience in monitoring latency, identifying packet loss, and analyzing traffic to ensure optimal network performance and minimal downtime.

III Course Level Learning Outcome(s)

CO5: Work with various wireless networking technologies.

IV Laboratory Learning Outcome(s)

LLO11.1: Measure latency and connectivity of wireless network.

V Relevant Affective Domain Related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

Latency is the time delay between sending and receiving data across a network, which directly impacts the speed and responsiveness of applications. Packet loss happens when data packets are lost in transmission,

leading to incomplete or disrupted communication. Understanding the OSI model, especially the network and transport layers, is important for analyzing data flow and identifying where issues occur. Tools like

Ping and PingPlotter use ICMP to measure latency and packet loss over time, while Wireshark captures and analyzes packets in real time to diagnose network performance and protocol-level problems. Familiarity with TCP/IP protocols, bandwidth, jitter, and common network topologies is essential for effective network troubleshooting.

Stepwise Procedure

i) Measure latency and packet loss over time using any suitable tool e.g. PingPlotter.

Step 1: Download and Install PingPlotter

1. Open your web browser and go to the official website: *www.pingplotter.com.*
2. Click on the "Download" button to download the free version of PingPlotter.
3. Once the download is complete, open the setup file and follow the on-screen instructions to install the software.
4. After installation, launch PingPlotter from the desktop or start menu.

Step 2: Understand the Interface

1. Target Bar**:** At the top, this is where you enter the website or IP address to test (e.g., google.com or 8.8.8.8).
2. Graph Section**:** Shows a real-time line graph of latency over time.
3. Trace Table**:** Displays hop-by-hop information (each step your packet travels).
4. Data Columns**:** Show values like average latency (Avg), maximum latency (Max), and packet loss percentage (PL%).

Step 3: Start a Test

1. In the Target Bar, type the IP address or domain name you want to test (e.g., 8.8.8.8).
2. Set the trace interval (the time between each ping). For example, use 2.5 seconds.
3. Click the "Start Tracing" button to begin the test.

Step 4: Monitor the Network

1. As the test runs, observe the line graph:
   - Smooth green lines = good connection.
   - Spikes or red lines = possible latency or packet loss.
2. The hop table will show where delays or losses are happening.

3. Let it run for a few minutes (5–10 minutes or longer) for better accuracy.

Step 5: Analyze the Results

1. Look at the Avg (average) and PL% (packet loss) columns:
   - Avg shows how much time the packet took (in ms).
   - PL% shows what percentage of packets were lost.
2. If packet loss or high latency appears early in the hops, the issue might be local (e.g., your router).
3. If it appears later, it could be a problem with your ISP or a remote server.

Step 6: Save or Export the Results

1. To save the graph or report:
   - Go to File > Save Image to save the graph.
   - Or use File > Export Sample Set for detailed data.

Step 7: Stop the Test

1. Once you have enough data, click the "Stop" button.
2. Close PingPlotter or begin testing another target if needed.

Try testing multiple destinations (e.g., local router IP, ISP server, and websites) to compare where the delay or loss starts. Green indicates good connectivity. Yellow/orange may suggest mild issues. Red shows serious network problems like packet loss or high latency.

ii) Analyze network packets to detect performance bottlenecks using any suitable tool e.g. Wireshark.

Step 1: Download and Install Wireshark

1. Open your web browser and go to the official website: *www.wireshark.org.*
2. Click on the “Download” button based on your operating system (e.g., Windows).
3. Run the downloaded setup file and follow the on-screen instructions.
4. During installation, allow installation of WinPcap/Npcap (required to capture live packets).
5. After installation, launch Wireshark from the desktop or start menu.

Step 2: Understand the Wireshark Interface

1. Capture Interface List**:** Shows all available network interfaces (Wi-Fi, Ethernet).
2. Packet List Pane**:** Displays captured packets in a list format.

3. Packet Details Pane**:** Shows detailed information of a selected packet.
4. Packet Bytes Pane**:** Displays raw data in hexadecimal and ASCII.
5. Filter Bar**:** Used to apply display filters to find specific traffic (e.g., tcp, http, icmp).

Step 3: Start Packet Capture

1. Select the correct network interface (e.g., your active Wi-Fi connection).
2. Click the **blue shark fin icon** or press **Ctrl + E** to start capturing packets.
3. Use your browser or another application to generate network traffic (e.g., open google.com).

Step 4: Apply Filters to Analyze Specific Traffic

1. In the filter bar, type common filters to isolate traffic:
   - icmp: shows ping-related traffic.
   - Tcp: filters TCP traffic.
   - ip.addr == 192.168.1.1: filters traffic to/from a specific IP.
2. Click Apply or press Enter to activate the filter.

Step 5: Analyze Packet Information

1. Click on any packet in the list to view its details below.
2. Expand sections like Ethernet**,** IP**,** TCP/UDP, and HTTP to see protocol-specific info.
3. Look for issues such as:
   - High TCP retransmissions (may indicate packet loss).
   - Duplicate ACKs (network congestion).
   - Long delays between packets (high latency).
   - ICMP errors (e.g., destination unreachable).

Step 6: Use Statistics for Deeper Analysis

1. Go to Statistics > Protocol Hierarchy to see traffic types and volume.
2. Use Statistics > Conversations to see data exchange between IP pairs.
3. Use Statistics > I/O Graphs to view packet trends and traffic over time.

Step 7: Save or Export the Capture (Optional)

1. To save the capture file, go to **File > Save As**, and choose a name and location.
2. You can open this file later to re-analyze without needing a live capture.

Step 8: Stop the Capture

1. Click the **red square icon** or press **Ctrl + E** to stop capturing packets.

VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII Conclusion

……

……

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Use PingPlotter to measure the latency to 8.8.8.8 for 5 minutes. What is the average latency and is there any packet loss? Explain what it indicates about the network connection.
2. Compare the latency and packet loss when testing two different websites (e.g., google.com and yahoo.com). Which one has better performance and why?
3. Identify and explain what you observe in the PingPlotter graph if there is a sudden spike in latency or appearance of red bars. What could be the possible reasons?

4. Capture live traffic using Wireshark and apply the filter icmp. Identify at least 3 ICMP packets and explain what type of message each one is?
5. Analyze a captured TCP session using Wireshark. Identify the three-way handshake (SYN, SYN-ACK, ACK) and explain its purpose.
6. Using the Wireshark statistics feature, find out which protocol (e.g., TCP, UDP, HTTP) is used most in your captured traffic. What does this tell you about the type of activity on the network?

……

……

……

X References:

1. https://www.pingplotter.com/manual/
2. https://www.wireshark.org/docs/wsug_html_chunked/

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	

Practical No. 12: Multimedia Traffic Analysis,

i) Capture analyze HTTP Video streaming traffic using any suitable tool e.g Wireshark.

ii) Monitor RTP (Real Time Transport Protocol) packets from a multimedia stream using any suitable tool e.g. Wireshark.

I Practical Significance

Analyzing multimedia traffic such as HTTP video streams and RTP packets is critical for understanding how multimedia content is delivered over networks. Tools Wireshark enable the identification of streaming protocols, buffering behavior, packet loss, and jitter all of which affect video/audio quality. This helps in troubleshooting quality issues and optimizing network performance for applications like YouTube, Zoom, or live broadcasting platforms. Through this practical, students gain insights into how streaming content is transmitted and how real-time protocols manage voice/video data.

II Industry / Employer Expected Outcome(s)

Able to capture and analyze multimedia traffic such as HTTP video streams and RTP packets using tools like Wireshark and will interpret network behavior, detect streaming issues, and troubleshoot real-time communication problems effectively.

III Course Level Learning Outcome(s)

CO5: Work with various wireless networking technologies.

IV Laboratory Learning Outcome(s)

LLO12.1: Capture and Analyze traffic for multimedia application over Internet.

V Relevant Affective Domain Related Outcomes

1. Follow precautionary measures.
2. Follow naming conventions.
3. Follow ethical practices.

VI Relevant Theoretical Background

HTTP streaming delivers video content in chunks over TCP, using protocols like HLS or MPEG-DASH, where latency and retransmissions can affect playback quality. RTP, used in real-time applications like VoIP and video conferencing, sends packets over UDP and includes timestamps and sequence numbers to

maintain timing. Analyzing such traffic helps detect jitter, packet loss, or out-of-order delivery, which directly impacts media quality. Wireshark helps visualize and diagnose these issues at protocol and packet levels.

Stepwise Procedure

Part I: Capture and Analyze HTTP Video Streaming Traffic using Wireshark

Step 1: Install Wireshark

1. Download Wireshark from *www.wireshark.org.*
2. Run the installer and allow Npcap installation (required for packet capture).
3. Launch Wireshark after installation.

Step 2: Prepare for the Capture

1. Close all unnecessary applications.
2. Connect to the internet and open a browser (e.g., Chrome).
3. Open a known streaming website (e.g., YouTube**,** Vimeo).

Step 3: Start the Capture

1. In Wireshark, select your active network interface (usually Wi-Fi or Ethernet**).**
2. Click the blue shark fin icon or press Ctrl + E to start capturing.
3. Begin playing a video in the browser.

Step 4: Apply Filters to View HTTP or Streaming Traffic

1. Use filters like:
   - `http`: shows HTTP traffic.
   - `tcp.port == 443`: if the video uses HTTPS.
   - `frame contains "mp4"`: to detect video files.
2. Observe requests for video segments (look for `.mp4`, `.ts`, `.m3u8`).

Step 5: Analyze Traffic Behavior

1. Identify:
   - Video segment downloads (in bursts).
   - Buffering patterns.
   - TCP retransmissions (which affect playback).
2. Expand packet layers (Ethernet > IP > TCP > HTTP) to view details.

Step 6: Use Statistics

1. Go to Statistics > HTTP to summarize HTTP requests.
2. Use I/O Graphs to visualize traffic volume during video playback.

Step 7: Stop and Save the Capture

1. Click the red square icon or press Ctrl + E to stop.
2. Save the capture via File > Save As for future analysis.

Part II: Monitor RTP Packets from a Multimedia Stream using Wireshark

Step 1: Set Up RTP-Generating Application

1. Use any app that uses RTP, such as:
   - Zoom, Google Meet, Skype, VLC (playing an RTP stream).
   - Alternatively, use two devices to conduct a call or media stream.

Note: Use a known port if possible, or determine it using initial signaling.

Step 2: Start Wireshark Capture

1. Open Wireshark and select the active interface.
2. Click the blue shark fin icon or press Ctrl + E to begin.
3. Start the RTP stream (begin a call or media play).

Step 3: Apply Filters to View RTP Traffic

1. Use filter:
   - rtp: if RTP is decoded.
   - udp: if RTP is encapsulated and not auto-decoded.
   - udp.port == xxxx: replace with actual port if known.

Step 4: Analyze RTP Packets

1. Observe **sequence numbers** and **timestamps**:
   - Out-of-order packets may indicate jitter.
   - Missing sequence numbers = packet loss.
2. Right-click on an RTP packet and choose:
   - Telephony > RTP > Stream Analysis.
3. Review:
   - Jitter, Packet Loss, Delta Time between packets.

Step 5: View RTP Statistics

1. Go to **Telephony > RTP > Streams**.

2. Select the stream and click **Analyze**.
3. Use **Graph** to visualize packet arrival behavior.

Step 6: Export Data (Optional)

1. Export stream data or statistics for reports.
2. File > Export Packet Dissections > as CSV or plain text.

Step 7: Stop and Save the Capture

1. Click the **red square** to stop.
2. Save the .pcapng file for future use.

VII Resource required (Additional)

Sr.No.	Name of Resource	Broad Specification	Quantity	Remarks

VIII Conclusion

……

……

IX Practical Related Questions

Note: Below given are few sample questions for reference. Teachers must design more such questions to ensure the achievement of identified CO.

1. Using Wireshark, how can you identify the video segments being downloaded during HTTP streaming?
2. What steps would you follow to capture and filter only the HTTP traffic related to a video being streamed on YouTube?
3. After capturing HTTP streaming traffic, how can you determine whether there were any TCP retransmissions affecting playback quality?
4. How can you apply a filter in Wireshark to view only RTP packets in a captured call or media stream?
5. What information in the RTP packet helps you detect packet loss or jitter?

.....

.....

.....

.....

.....

.....

X References:

1. https://developer.mozilla.org/en-US/docs/Web/Media/Streaming
2. https://wiki.wireshark.org/RTP

XI Assessment Scheme (25 Marks)

S. No.	Weightage- Process related: 60%	Marks-15
1.	Logic formation:30%	
2.	Debugging ability:20%	
3.	Follow ethical practices:10%	
	Weightage- Product related: 40%	**Marks-10**
4.	Expected output:15%	
5.	Timely Submission:15%	
6.	Answer to sample questions:10%	
	Total 25	
	Dated Signature of Course Teacher	