HARI KISHOR SINGH GOVERNMENT POLYTECHNIC SHEOHAR

LABORATORY MANUAL

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

V SEMESTER

DATA COMMUNICATION AND COMPUTER NETWORK

SUBJECT CODE: P2418501

LIST OF EXPERIMENTS

S. No.	Laboratory Practical Title	Relevant CO
1	Identify Different Networking Devices	CO-1
2	Prepare Different Types of UTP Cable	CO-1
3	Connect Computers in Star Topology	CO-2
4	Configure Wireless NIC and Transfer Files Between Systems in Wireless Network	CO-2
5	Configure Network and Internet Setting	CO-2
6	Establish Peer-to-Peer Network Connection Using Cross Cable	CO-2
7	Capture Packet and Analyse Header Using Network Simulator	CO-3
8	Perform Remote Login Using Telnet	CO-5
9	Create HTTP Server	CO-5
10	Create FTP Server	CO-5

Course Outcomes (COs):-

CO-1 Choose the appropriate transmission media type based on the needs.

CO-2 Explain the function of Data link layer protocols.

CO-3 Create subnet for given IP.

CO-4 Explain the function of Transport layer protocols.

CO-5 Create FTP and HTTP server.

Programme Outcomes (POs):-

- 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 analyse 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 system components or processes to meet specified needs.
- PO4: Engineering Tools, Experimentation and Testing - Apply modern engineering tools and appropriate techniques to conduct standard tests and measurements.
- PO5: Engineering Practices for Society, Sustainability and Environment - Apply appropriate technology in the 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 analyse individual needs and engage in updating in the context of technological changes.

Programme Specific Outcomes (PSOs):-

- PSO1: Apply the fundamentals of computer science, including algorithms and programming, to analyse complex problems and develop robust solutions.

- PSO2: Design and implement computer science solutions with emphasis on energy efficiency, sustainability, and eco-friendly technologies.

COURSE ARTICULATION MATRIX (CAM)

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO-1	1	-	-	-	-	-	1	-	-
CO-2	2	2	1	1	-	-	1	-	-
CO-3	2	2	1	1	-	-	-	-	-
CO-4	2	3	1	1	-	-	-	-	-
CO-5	2	3	1	1	-	-	-	-	-

Legend: High (3), Medium (2), Low (1), No mapping (-)

Suggested Specification Table for Laboratory (Practical):-

S. No.	Laboratory Practical Titles	Relevant COs	PRA* (%)	PDA** (%)	Viva-Voce (%)
1	Identify different Networking devices.	CO-1	40	50	10
2	Prepare different types of UTP cable.	CO-1	40	50	10
3	Connect computers in Star topologies.	CO-1	40	50	10
4	Configure wireless NIC and transfer files between systems in Wireless.	CO-2	30	60	10
5	Configure Network and Internet Setting.	CO-2	40	50	10
6	Establish Peer to Peer network connection using cross cable.	CO-2	50	40	10
7	Capture packet and analysis header using network simulator.	CO-3	50	40	10
8	Perform remote login using Telnet.	CO-5	50	40	10
9	Create HTTP sever	CO-5	70	20	10
10	Create FTP server	CO-5	50	40	10

EXPERIMENT NO: 1

1.1 Identify Different Networking Devices

AIM: To identify different networking devices used in a computer network and understand the function and OSI layer of operation of each device.

RELEVANT CO: CO-1 (Choose the appropriate transmission media type based on the needs.)

SOFTWARE / HARDWARE REQUIRED:-

- Windows / Linux based computer
- Web browser (Chrome / Firefox / Edge)
- Cisco Packet Tracer (optional, for simulation)
- Physical networking devices available in the lab: Hub, Switch, Router, Modem, Repeater, Bridge, Gateway, Access Point, NIC
- Internet connection

THEORY:-

A computer network is formed by interconnecting devices so that they can exchange data and share resources such as files, printers, and internet access. Networking devices are the hardware components that make this interconnection possible, and each device operates at a specific layer of the OSI reference model.

1. Hub

- A basic, low-intelligence device that connects multiple computers in a network.
- Broadcasts incoming data to all connected ports irrespective of the destination.
- Works at the Physical Layer (Layer 1) of the OSI model.

2. Switch

- An intelligent device that forwards data only to the intended destination port using the MAC address.
- Reduces network collisions compared to a hub and improves bandwidth utilisation.
- Works at the Data Link Layer (Layer 2) of the OSI model.

3. Router

- Connects two or more different networks and forwards data packets between them.
- Uses IP addresses and routing tables to determine the best path for data.
- Works at the Network Layer (Layer 3) of the OSI model.

4. Modem (Modulator-Demodulator)

- Converts digital signals from a computer into analog signals for transmission and vice versa.
- Commonly used to provide Internet access through telephone or cable lines.

5. Repeater

- Regenerates and amplifies a weak or degraded signal.
- Used to extend the maximum distance a signal can travel on a network.

6. Bridge

- Connects and filters traffic between two LAN segments using MAC addresses.
- Reduces overall network traffic by segmenting collision domains.

7. Gateway

- Connects two dissimilar networks that use different protocols.

- Acts as a protocol converter between the two networks.

8. Network Interface Card (NIC)

- Allows a computer to physically connect to a network (wired or wireless).
- Every NIC has a unique 48-bit MAC address burned into it by the manufacturer.

Device	OSI Layer	Primary Function
Hub	Physical (L1)	Broadcasts data to all connected ports
Repeater	Physical (L1)	Regenerates/amplifies signals
Switch	Data Link (L2)	Forwards frames using MAC address
Bridge	Data Link (L2)	Segments and filters LAN traffic
Router	Network (L3)	Routes packets between networks using IP
Gateway	All / Application	Converts between different protocols

PROCEDURE:-

1. Power ON the computer systems available in the networking laboratory.
2. Physically inspect the Hub, Switch, Router, Modem, and other devices available in the lab; note down the make, model, and number of ports on each.
3. Observe the LED/link indicators on each device and note their significance (link, activity, collision, speed).
4. Open a web browser and study the working of each networking device using the manufacturer's documentation.
5. Open Device Manager on a Windows PC (Right-click This PC → Manage → Device Manager → Network adapters) and note the installed NIC.
6. Optionally, open Cisco Packet Tracer, drag each device (Hub, Switch, Router) from the device panel into the workspace, and observe its icon and default port configuration.
7. Tabulate the observations for each device: name, OSI layer, and function, as shown in the theory table.

PROGRAM / COMMAND(S):-

```
> ipconfig /all          (Windows - view NIC details)
$ ifconfig -a            (Linux - view NIC details)
$ lspci | grep -i network (Linux - list network hardware)
```

SAMPLE OUTPUT:-

```
Ethernet adapter Ethernet:
   Description . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . : 00-1A-2B-3C-4D-5E
   DHCP Enabled. . . . . . . . . . : Yes
   IPv4 Address. . . . . . . . . . : 192.168.1.10
```

PRECAUTIONS:-

- Handle networking devices carefully; avoid static discharge on exposed circuitry.
- Do not force connectors into ports; align them correctly before insertion.
- Switch off power before physically inspecting the internal parts of any device.

RESULT:-

Thus, different networking devices such as Hub, Switch, Router, Modem, Repeater, Bridge, Gateway, and NIC were successfully identified, and their functions and OSI layers of operation were studied.

VIVA-VOCE QUESTIONS:-

8. What is the difference between a Hub and a Switch?
9. At which OSI layer does a Router operate?
10. What is the purpose of a Network Interface Card?
11. Differentiate between a Bridge and a Gateway.
12. Why is a Switch preferred over a Hub in modern LANs?

EXPERIMENT NO: 2

1.2 Prepare Different Types of UTP Cable

AIM: To practically prepare and test a Straight-Through UTP cable and a Cross-Over UTP cable using a crimping tool, following the T568A and T568B wiring standards.

RELEVANT CO: CO-1 (Choose the appropriate transmission media type based on the needs.)

SOFTWARE / HARDWARE REQUIRED:-

- UTP (Unshielded Twisted Pair) Cable - Cat5e / Cat6
- RJ-45 Connectors (2 per cable)
- Crimping (Clamping) Tool
- Cable Stripper / Cutter
- LAN Cable Tester
- Two computers or networking devices for testing

THEORY:-

Unshielded Twisted Pair (UTP) cable is the most common guided transmission medium used to connect networking devices in a LAN. It contains four pairs of twisted copper wires, colour-coded, which are terminated with RJ-45 connectors.

Types of UTP (Ethernet) Cables

- Straight-Through Cable: Both ends follow the same wiring standard (T568A-T568A or T568B-T568B). Used to connect dissimilar devices, e.g., Computer to Switch, Computer to Router.
- Cross-Over Cable: One end follows T568A and the other follows T568B. Used to connect similar devices directly, e.g., Computer to Computer, Switch to Switch (most modern NICs auto-detect and no longer strictly require this, but it remains an important concept).

Pin	T568A Standard	T568B Standard
1	White-Green	White-Orange
2	Green	Orange
3	White-Orange	White-Green
4	Blue	Blue
5	White-Blue	White-Blue
6	Orange	Green
7	White-Brown	White-Brown
8	Brown	Brown

PROCEDURE:-

Part A: Making a Straight-Through Cable

13. Cut the required length of UTP cable using the cutter.
14. Strip about 2 cm of the outer insulation from both ends using the cable stripper.
15. Untwist the four pairs and arrange the eight wires in T568B order on BOTH ends: White-Orange, Orange, White-Green, Blue, White-Blue, Green, White-Brown, Brown.

16. Trim the wires evenly and insert them fully into an RJ-45 connector, ensuring each wire reaches the front of the connector.
17. Place the connector in the crimping tool and press firmly to seat the pins into the wires.
18. Repeat the same T568B order on the other end of the cable.

Part B: Making a Cross-Over Cable

19. Arrange the wires at one end in T568A order.
20. Arrange the wires at the other end in T568B order.
21. Insert into RJ-45 connectors and crimp both ends firmly.

Part C: Testing the Cable

22. Connect both ends of the cable into a LAN cable tester.
23. Switch ON the tester and observe the sequence of LEDs on the transmitter and receiver units.
24. For a correctly made straight-through cable, LEDs 1 to 8 should blink in the same sequence on both units.
25. For a cross-over cable, pins 1-2 and 3-6 should be swapped between the two ends.
26. Alternatively, connect the cable between two computers/devices, assign IP addresses, and verify with the ping command.

PROGRAM / COMMAND(S):-

```
> ping 192.168.1.2
```

SAMPLE OUTPUT:-

```
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

PRECAUTIONS:-

- Do not over-strip the outer insulation; exposed twisted pairs should be as short as possible to reduce crosstalk.
- Ensure all eight wires touch the front end of the RJ-45 connector before crimping.
- Do not crimp a connector twice; a mis-crimped connector should be cut off and replaced.

RESULT:-

Thus, the Straight-Through UTP cable and the Cross-Over UTP cable were successfully prepared using the crimping tool as per the T568A/T568B standards and verified using a cable tester.

VIVA-VOCE QUESTIONS:-

27. What is the difference between T568A and T568B standards?
28. When is a straight-through cable used and when is a cross-over cable used?
29. What is the maximum recommended length for a UTP cable segment?
30. Why are the wires in a UTP cable twisted in pairs?
31. Name the categories of UTP cable and their approximate bandwidth.

EXPERIMENT NO: 3

2.1 Connect Computers in Star Topology

AIM: To design and implement a Local Area Network using Star topology with a network switch and multiple computers, and to verify connectivity between all the connected systems.

RELEVANT CO: CO-2 (Explain the function of Data Link Layer protocols.)

SOFTWARE / HARDWARE REQUIRED:-

- Desktop / Laptop computers (3 or more)
- Network Switch
- Straight-through UTP (Ethernet) cables
- Network Interface Card (NIC) in each computer
- Command Prompt (Windows) / Terminal (Linux)

THEORY:-

Star topology is a network arrangement in which every computer (node) is connected individually to a central device, usually a switch or a hub, using a separate cable. All communication between two nodes passes through the central device.

Advantages

- Easy to install, manage, and troubleshoot; a single cable fault affects only one node.
- Adding or removing a node does not disturb the rest of the network.
- Centralised monitoring and control is possible from the switch.

Disadvantages

- The entire network depends on the central switch; if it fails, the whole network goes down.
- Requires more cable compared to bus topology.

PROCEDURE:-

32. Place the network switch at a central location and the computers around it.
33. Connect each computer to a port on the switch using a straight-through UTP cable.
34. Power ON the switch and all the computers; observe the link LEDs to confirm physical connectivity.
35. On each computer, open Network and Sharing Centre → Change adapter settings → Ethernet → Properties → Internet Protocol Version 4 (TCP/IPv4) and assign a unique static IP address on the same subnet, as given below.

Computer	IP Address	Subnet Mask
PC-1	192.168.1.1	255.255.255.0
PC-2	192.168.1.2	255.255.255.0
PC-3	192.168.1.3	255.255.255.0

36. Open Command Prompt on PC-1 and test connectivity to the other systems using the ping command.
37. Repeat the ping test from every computer to every other computer to confirm that the star network is fully functional.

PROGRAM / COMMAND(S):-

```
> ping 192.168.1.2
> ping 192.168.1.3
```

SAMPLE OUTPUT:-

```
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

PRECAUTIONS:-

- Ensure all computers are assigned unique IP addresses on the same subnet.
- Check that link LEDs on the switch are glowing before testing connectivity.
- Disable any active firewall temporarily if ping requests are being blocked, for testing purposes only.

RESULT:-

Thus, a Local Area Network was successfully implemented using Star topology, and connectivity between all the connected computers was verified using the ping command.

VIVA-VOCE QUESTIONS:-

38. What is a Star topology and how does it differ from Bus topology?
39. What happens to the network if the central switch fails in a Star topology?
40. Why is Star topology the most commonly used LAN topology today?
41. What is the role of a switch in a Star topology network?

EXPERIMENT NO: 4

2.2 Configure Wireless NIC and Transfer Files Between Systems in Wireless Network

AIM: To configure a wireless Network Interface Card (NIC), connect two systems over a wireless network, and transfer files between them.

RELEVANT CO: CO-2 (Explain the function of Data Link Layer protocols.)

SOFTWARE / HARDWARE REQUIRED:-

- Two computers/laptops with built-in or USB Wireless NIC
- Wireless Router / Access Point (or mobile hotspot)
- Windows Operating System
- File sharing feature enabled

THEORY:-

A wireless network allows devices to communicate without physical cables, using radio frequency (RF) signals as per the IEEE 802.11 (Wi-Fi) family of standards.

Wireless NIC

A wireless NIC is a hardware adapter that enables a computer to connect to a Wi-Fi network. It converts data into radio signals for transmission and reconverts received radio signals back into data.

Modes of Wireless Operation

- Infrastructure Mode: All wireless devices connect to a central Access Point/Router, which also connects to the wired network.
- Ad-hoc Mode: Wireless devices connect directly to each other without a central access point.

IEEE 802.11 Standards

Standard	Frequency Band	Approx. Max Speed
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5 GHz	600 Mbps
802.11ac	5 GHz	1300+ Mbps
802.11ax (Wi-Fi 6)	2.4/5/6 GHz	9.6 Gbps

PROCEDURE:-

42. Ensure the Wireless NIC is enabled: Settings → Network & Internet → Wi-Fi → Turn ON, or enable via Device Manager if disabled.
43. Click the Wi-Fi icon in the taskbar and select the SSID of the wireless router/hotspot to be used.
44. Enter the wireless network security key (WPA2/WPA3 passphrase) and connect.
45. Repeat the above steps on the second computer so that both systems join the same wireless network.
46. Open Command Prompt and run ipconfig on both systems to note their assigned IPv4 addresses.
47. Verify wireless connectivity between the two systems using the ping command.
48. On the sender system, right-click the file/folder to be shared → Properties → Sharing tab → Share, and grant Read/Write permission to Everyone or a specific user.
49. On the receiver system, open File Explorer and type \\<sender-IP-address> in the address bar to access the shared folder.

50. Copy the required file from the shared folder to complete the file transfer, and confirm the file has been received correctly.

PROGRAM / COMMAND(S):-

```
> netsh wlan show interfaces
> ipconfig
> ping 192.168.0.15
```

SAMPLE OUTPUT:-

```
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

PRECAUTIONS:-

- Ensure both systems are connected to the SAME wireless network/SSID before testing.
- Keep the wireless security key confidential; use WPA2/WPA3 encryption, never an open network, for sharing sensitive files.
- Turn off metered connection settings that may restrict background file sharing.

RESULT:-

Thus, the Wireless NIC was successfully configured, connectivity between two systems was established over a wireless network, and a file was successfully transferred between them.

VIVA-VOCE QUESTIONS:-

51. What is the difference between Infrastructure mode and Ad-hoc mode?
52. What is an SSID?
53. Name a few IEEE 802.11 wireless standards.
54. What security protocols are used to protect a Wi-Fi network?
55. How is a wireless NIC different from a wired NIC?

EXPERIMENT NO: 5

2.3 Configure Network and Internet Setting

AIM: To configure IPv4 network settings (IP address, subnet mask, default gateway, DNS) and Internet settings on a Windows computer, and verify the configuration.

RELEVANT CO: CO-2 (Explain the function of Data Link Layer protocols.)

SOFTWARE / HARDWARE REQUIRED:-

- Windows 10 / Windows 11 computer
- Command Prompt
- Internet connection

THEORY:-

Every computer participating in a TCP/IP network must be configured with a valid IPv4 address, subnet mask, default gateway, and DNS server address, either manually (static) or automatically (via DHCP).

Key Parameters

- IP Address: Uniquely identifies the device on the network (e.g., 192.168.1.10).
- Subnet Mask: Separates the network portion and host portion of the IP address (e.g., 255.255.255.0).
- Default Gateway: The router's IP address through which traffic destined for another network is forwarded.
- DNS Server: Resolves human-readable domain names (e.g., www.google.com) into IP addresses.
- DHCP (Dynamic Host Configuration Protocol): Automatically assigns IP configuration to devices on the network.

PROCEDURE:-

Part A: Configure Static IPv4 Address

56. Go to Control Panel → Network and Internet → Network and Sharing Centre → Change adapter settings.
57. Right-click on the active adapter (Ethernet/Wi-Fi) and select Properties.
58. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
59. Select 'Use the following IP address' and enter the IP Address, Subnet Mask, and Default Gateway.
60. Select 'Use the following DNS server addresses' and enter the Preferred and Alternate DNS server addresses.
61. Click OK and Close to apply the settings.

Part B: Configure Automatic (DHCP) Settings

62. In the same TCP/IPv4 Properties window, select 'Obtain an IP address automatically' and 'Obtain DNS server address automatically'.
63. Click OK; the system will now receive its IP configuration from the DHCP server automatically.

Part C: Verify Configuration

64. Open Command Prompt and run ipconfig /all to view the complete network configuration.
65. Run ping 8.8.8.8 to check Internet connectivity.
66. Run nslookup www.google.com to verify DNS name resolution.

PROGRAM / COMMAND(S):-

```
> ipconfig /all
```

```
> ping 8.8.8.8
> nslookup www.google.com
```

SAMPLE OUTPUT:-

```
IPv4 Address. . . . . . . . . . . : 192.168.1.10
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=21ms TTL=115
```

PRECAUTIONS:-

- Do not assign an IP address that is already in use by another device on the network (IP conflict).
- Ensure the subnet mask and default gateway are consistent with the rest of the network.
- Note down the original network settings before changing them, so they can be restored later if required.

RESULT:-

Thus, the IPv4 network settings and Internet settings were successfully configured on the computer, and connectivity was verified using ipconfig, ping, and nslookup commands.

VIVA-VOCE QUESTIONS:-

67. What is the difference between a static IP and a dynamic IP address?
68. What is the role of the default gateway?
69. What does the subnet mask determine?
70. What is DHCP and why is it useful?
71. What is the purpose of a DNS server?

EXPERIMENT NO: 6

2.4 Establish Peer-to-Peer Network Connection Using Cross Cable

AIM: To establish a direct Peer-to-Peer network connection between two computers using a cross-over UTP cable, without using a switch, and to verify communication and file sharing between them.

RELEVANT CO: CO-2 (Explain the function of Data Link Layer protocols.)

SOFTWARE / HARDWARE REQUIRED:-

- Two computers, each with a Network Interface Card
- Cross-over UTP cable
- Command Prompt / Terminal

THEORY:-

A Peer-to-Peer (P2P) network is the simplest form of network in which two computers are connected directly to each other, without any central device such as a switch, and communicate as equals — each computer can act as both a client and a server.

To connect two computers directly, a cross-over cable is traditionally required because the transmit pins of one NIC must be wired to the receive pins of the other. Most modern NICs support Auto-MDI-X, which automatically detects and adjusts for this, allowing even a straight-through cable to work; however, the cross-over cable remains the standard method taught for direct connections.

PROCEDURE:-

72. Connect the two computers directly using a cross-over UTP cable (one end wired to T568A and the other to T568B).
73. On PC-1, open Network Adapter Properties → TCP/IPv4 and assign IP Address 192.168.2.1, Subnet Mask 255.255.255.0.
74. On PC-2, assign IP Address 192.168.2.2, Subnet Mask 255.255.255.0.
75. Ensure both computers belong to the same Workgroup name under System Properties → Computer Name.
76. Open Command Prompt on PC-1 and test connectivity using ping 192.168.2.2.
77. Enable file sharing: right-click a folder on PC-1 → Properties → Sharing → Share → add 'Everyone' with Read/Write permission.
78. On PC-2, open File Explorer and enter \\192.168.2.1 in the address bar to access the shared folder on PC-1.
79. Copy a test file between the two systems to confirm that the Peer-to-Peer connection is fully functional.

PROGRAM / COMMAND(S):-

```
> ping 192.168.2.2
```

SAMPLE OUTPUT:-

```
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

PRECAUTIONS:-

- Confirm the cable is wired as a proper cross-over cable (T568A on one end, T568B on the other).
- Both computers must be on the same subnet and, ideally, the same workgroup for easy file sharing.
- Disable the firewall temporarily only for testing purposes, and re-enable it afterwards.

RESULT:-

Thus, a Peer-to-Peer network connection was successfully established between two computers using a cross-over cable, and connectivity along with file sharing was verified.

VIVA-VOCE QUESTIONS:-

80. What is a Peer-to-Peer network? How is it different from Client-Server network?
81. Why is a cross-over cable required for direct PC-to-PC connection?
82. What is Auto-MDI-X?
83. What is a Workgroup in Windows networking?

EXPERIMENT NO: 7

3.1 Capture Packet and Analyse Header Using Network Simulator

AIM: To capture live network packets using a network protocol analyser (Wireshark) and analyse the Ethernet, IP, and TCP/UDP header fields contained in the captured packets.

RELEVANT CO: CO-3 (Create subnet for given IP.)

SOFTWARE / HARDWARE REQUIRED:-

- Wireshark (Network Protocol Analyser)
- Windows / Linux computer with an active network connection
- Web browser (to generate sample traffic)

THEORY:-

Wireshark is a widely used, open-source network protocol analyser (packet sniffer) that captures data travelling over a network interface in real time and displays it in a human-readable form, layer by layer, allowing a detailed study of protocol headers.

Encapsulated Header Structure of a Captured Packet

- Frame: Wireshark's own capture metadata (timestamp, frame length, interface).
- Ethernet II Header: Contains source MAC address, destination MAC address, and EtherType.
- Internet Protocol (IP) Header: Contains source IP, destination IP, TTL, protocol number, header checksum.
- Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Header: Contains source port, destination port, sequence/acknowledgement numbers (TCP), flags (SYN, ACK, FIN), checksum.
- Application Layer Data: The actual payload, e.g., HTTP request/response, DNS query.

Common Capture Filters

Filter	Purpose
ip.addr == 192.168.1.1	Show packets to/from a specific IP address
tcp.port == 80	Show packets on TCP port 80 (HTTP)
icmp	Show only ICMP (ping) packets
http	Show only HTTP protocol packets
dns	Show only DNS query/response packets

PROCEDURE:-

84. Download and install Wireshark from the official website (wireshark.org).
85. Launch Wireshark and select the active network interface (Ethernet/Wi-Fi) from the start screen.
86. Click the blue shark-fin icon to start capturing packets.
87. Generate some network traffic — open a browser and visit a website, or run a ping command from another terminal.
88. Click the red square icon to stop the capture after a few seconds.
89. Apply a display filter, e.g., http or icmp, in the filter bar and press Enter to narrow down the results.
90. Click on an individual packet in the packet list pane; examine the packet details pane below to expand the Frame, Ethernet, IP, and TCP/UDP headers.

91. Note down the Source IP, Destination IP, Source Port, Destination Port, TTL value, and TCP flags for the selected packet.
92. Use Statistics → Protocol Hierarchy to view a summary of all protocols captured during the session.

PROGRAM / COMMAND(S):-

```
Filter used: http
Filter used: ip.addr == 142.250.190.14
```

SAMPLE OUTPUT:-

```
Frame 25: 543 bytes on wire, 543 bytes captured
Ethernet II, Src: 00:1a:2b:3c:4d:5e, Dst: 00:11:22:33:44:55
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 142.250.190.14
Transmission Control Protocol, Src Port: 52344, Dst Port: 80, Seq: 1, Ack: 1
   Flags: 0x018 (PSH, ACK)
Hypertext Transfer Protocol: GET / HTTP/1.1
```

PRECAUTIONS:-

- Capture traffic only on networks you are authorised to monitor.
- Stop the capture promptly to avoid generating excessively large capture files.
- Apply filters before analysis to avoid being overwhelmed by irrelevant packets.

RESULT:-

Thus, network packets were successfully captured using Wireshark, and the Ethernet, IP, and TCP/UDP header fields were analysed for the captured traffic.

VIVA-VOCE QUESTIONS:-

93. What is the difference between a capture filter and a display filter in Wireshark?
94. What information does the TCP header contain?
95. What is the significance of the TTL field in the IP header?
96. What are the TCP flags SYN, ACK, and FIN used for?
97. How does Wireshark differ from a firewall?

EXPERIMENT NO: 8

5.1 Perform Remote Login Using Telnet

AIM: To enable the Telnet client and Telnet server, and perform a remote login from one computer to another over the network using the Telnet protocol.

RELEVANT CO: CO-5 (Create FTP and HTTP server.)

SOFTWARE / HARDWARE REQUIRED:-

- Two Windows computers on the same network (Client and Server)
- Telnet Client and Telnet Server Windows features
- Command Prompt

THEORY:-

Telnet (Telecommunication Network) is an application layer protocol that allows a user to log in to a remote computer and execute commands on it as if working directly at that machine's console. Telnet uses TCP port 23 for communication.

Telnet transmits data, including usernames and passwords, in plain text (unencrypted), which makes it insecure for use over untrusted networks. It has largely been replaced by SSH (Secure Shell) for secure remote administration but remains important to study the fundamentals of remote login.

PROCEDURE:-

Part A: Enable Telnet Client (on both systems)

98. Open Control Panel → Programs → Turn Windows features on or off.
99. Check the box for 'Telnet Client' and click OK to install it.

Part B: Enable Telnet Server (on the server system)

100. Check the box for 'Telnet Server' in the same Windows Features dialog (available on Windows Server editions; on client Windows editions a third-party Telnet server such as SolarWinds or Xming may be used).
101. Open Services (services.msc), locate the Telnet service, set its Startup type to Automatic, and Start the service.
102. Note down the IP address of the server using ipconfig.

Part C: Perform Remote Login from the Client

103. On the client system, open Command Prompt.
104. Type telnet <server-IP-address> and press Enter.
105. Enter the valid username and password of the server system when prompted.
106. On successful login, execute a few basic commands (e.g., dir, ipconfig) remotely on the server.
107. Type exit to close the Telnet session.

PROGRAM / COMMAND(S):-

```
> telnet 192.168.1.20
```

SAMPLE OUTPUT:-

```
Connecting to 192.168.1.20...
```

```
Welcome to Microsoft Telnet Server.
login: admin
password: ********
*===============================================================
C:\Users\admin> dir
 Volume in drive C has no label.
 Directory of C:\Users\admin
```

PRECAUTIONS:-

- Use Telnet only within a trusted, isolated lab network, never over the open Internet.
- Ensure the Telnet service is stopped after the practical to avoid leaving an insecure port open.
- Use strong credentials, since Telnet does not encrypt login information.

RESULT:-

Thus, the Telnet client and server were successfully configured, and a remote login was performed from the client system to the server system over the network.

VIVA-VOCE QUESTIONS:-

108. Which port number does Telnet use?
109. Why is Telnet considered insecure?
110. What protocol is generally recommended as a secure alternative to Telnet?
111. What is the purpose of remote login?

EXPERIMENT NO: 9

5.2 Create HTTP Server

AIM: To create and configure a simple HTTP (Hyper Text Transfer Protocol) server and access the hosted web page from a client system's browser over the network.

RELEVANT CO: CO-5 (Create FTP and HTTP server.)

SOFTWARE / HARDWARE REQUIRED:-

- Python 3 (built-in http.server module) or XAMPP/Apache Web Server
- Two computers on the same network (Server and Client)
- Web browser
- Command Prompt / Terminal

THEORY:-

HTTP (Hyper Text Transfer Protocol) is an application layer protocol that governs communication between web clients (browsers) and web servers. HTTP normally operates on TCP port 80 (and HTTPS on port 443).

A web server is software that listens for incoming HTTP requests from clients, retrieves the requested resource (an HTML page, image, or file), and sends it back to the client as an HTTP response. Python's built-in http.server module provides a very simple, ready-to-use HTTP server for learning and testing purposes.

PROCEDURE:-

112. On the server computer, create a new folder, e.g., C:\webroot, and inside it create a simple index.html file with some sample content.
113. Verify that Python 3 is installed by running python --version in Command Prompt.
114. Open Command Prompt, navigate into the webroot folder using the cd command.
115. Start the HTTP server by running: python -m http.server 8080
116. Note the IP address of the server computer using ipconfig.
117. On the client computer (connected to the same network), open a web browser and navigate to http://<server-IP-address>:8080/
118. Verify that the index.html page hosted on the server is displayed correctly in the client's browser.
119. Observe the request log printed in the server's Command Prompt window for every request received.
120. Press Ctrl + C in the server's Command Prompt to stop the HTTP server when done.

PROGRAM / COMMAND(S):-

```
C:\webroot> python -m http.server 8080
```

SAMPLE OUTPUT:-

```
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.1.15 - - [20/Jul/2026 10:15:02] "GET / HTTP/1.1" 200 -
192.168.1.15 - - [20/Jul/2026 10:15:02] "GET /style.css HTTP/1.1" 200 -
```

PRECAUTIONS:-

- Ensure the chosen port (e.g., 8080) is not already in use by another application.

- Allow the port through the Windows Firewall if the client is unable to connect.
- Do not host sensitive files in the webroot folder, since http.server has no authentication by default.

RESULT:-

Thus, an HTTP server was successfully created and configured, and the hosted web page was accessed from a client system's browser over the network.

VIVA-VOCE QUESTIONS:-

121. Which port number does HTTP use by default?
122. What is the difference between HTTP and HTTPS?
123. What is the role of a web server?
124. Name a few common HTTP status codes and their meaning (200, 404, 500).
125. What is the difference between a GET and a POST request?

EXPERIMENT NO: 10

5.3 Create FTP Server

AIM: To create and configure an FTP (File Transfer Protocol) server and perform file upload/download operations from a client system.

RELEVANT CO: CO-5 (Create FTP and HTTP server.)

SOFTWARE / HARDWARE REQUIRED:-

- FTP Server software (e.g., FileZilla Server, or IIS FTP feature on Windows Server)
- FTP Client (Windows built-in ftp command, or FileZilla Client)
- Two computers on the same network (Server and Client)

THEORY:-

FTP (File Transfer Protocol) is an application layer protocol used to transfer files between a client and a server over a TCP/IP network. FTP uses two separate TCP connections: Port 21 for control (commands, login) and Port 20 for actual data transfer in active mode.

FTP Modes

- Active Mode: The server initiates the data connection back to the client.
- Passive Mode: The client initiates both the control and the data connections, which works better through firewalls/NAT.

Common FTP Client Commands

Command	Purpose
open <ip>	Connect to the FTP server
user	Login with username and password
dir / ls	List files in the current remote directory
get <file>	Download a file from the server
put <file>	Upload a file to the server
bye / quit	Close the FTP session

PROCEDURE:-

126. Download and install FileZilla Server on the server computer.
127. Launch the FileZilla Server interface and create a new user account with a username and password.
128. Set the Shared Folder / Home Directory for that user and grant Read, Write, and Delete permissions as required.
129. Start the FTP server service; by default it listens on TCP port 21.
130. Note the IP address of the server computer using ipconfig.
131. On the client computer, open Command Prompt and connect to the server using: ftp <server-IP-address>
132. Enter the username and password created earlier to log in to the FTP server.
133. Use the dir command to list the files present on the server.
134. Use the get <filename> command to download a file from the server to the client.
135. Use the put <filename> command to upload a file from the client to the server.

136. Type bye to close the FTP session, and verify the transferred files at both ends.

PROGRAM / COMMAND(S):-

```
> ftp 192.168.1.20
ftp> get report.pdf
ftp> put assignment.docx
ftp> bye
```

SAMPLE OUTPUT:-

```
Connected to 192.168.1.20.
220 FileZilla Server ready
User (192.168.1.20:(none)): student
331 Password required
Password: ********
230 Logged on
ftp> get report.pdf
226 Transfer OK
ftp: 245760 bytes received in 0.20Seconds 1228.80Kbytes/sec.
```

PRECAUTIONS:-

- Use strong FTP account credentials since standard FTP transmits data in plain text.
- Restrict each FTP user's permissions to only the required shared folder.
- Allow the required FTP ports through the firewall on both server and client.

RESULT:-

Thus, an FTP server was successfully created and configured, and file upload/download operations were successfully performed between the client and the server.

VIVA-VOCE QUESTIONS:-

137. Which TCP ports are used by FTP for control and data connections?
138. What is the difference between Active and Passive FTP modes?
139. Differentiate between FTP and HTTP.
140. What is the purpose of the 'get' and 'put' commands in FTP?
141. Is FTP a secure protocol? What is a secure alternative to FTP?