**Exp: no: 1**

**Aim:**

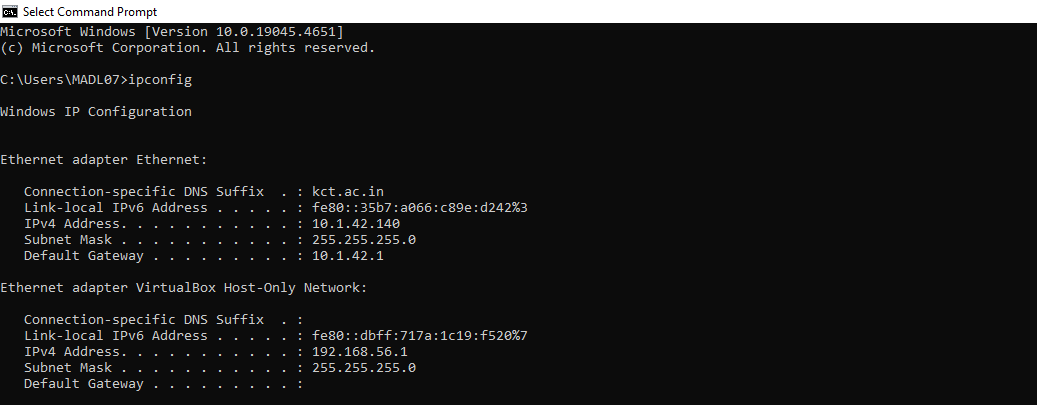
To demonstrate the working of network tools such as Ping, TCP Dump, Traceroute, Netstat and write the syntax, execute and place the screenshot for all the commands worked on.

1. Demonstrate the different *ipconfig* commands used to explore a system’s IP address.

*Sol:*

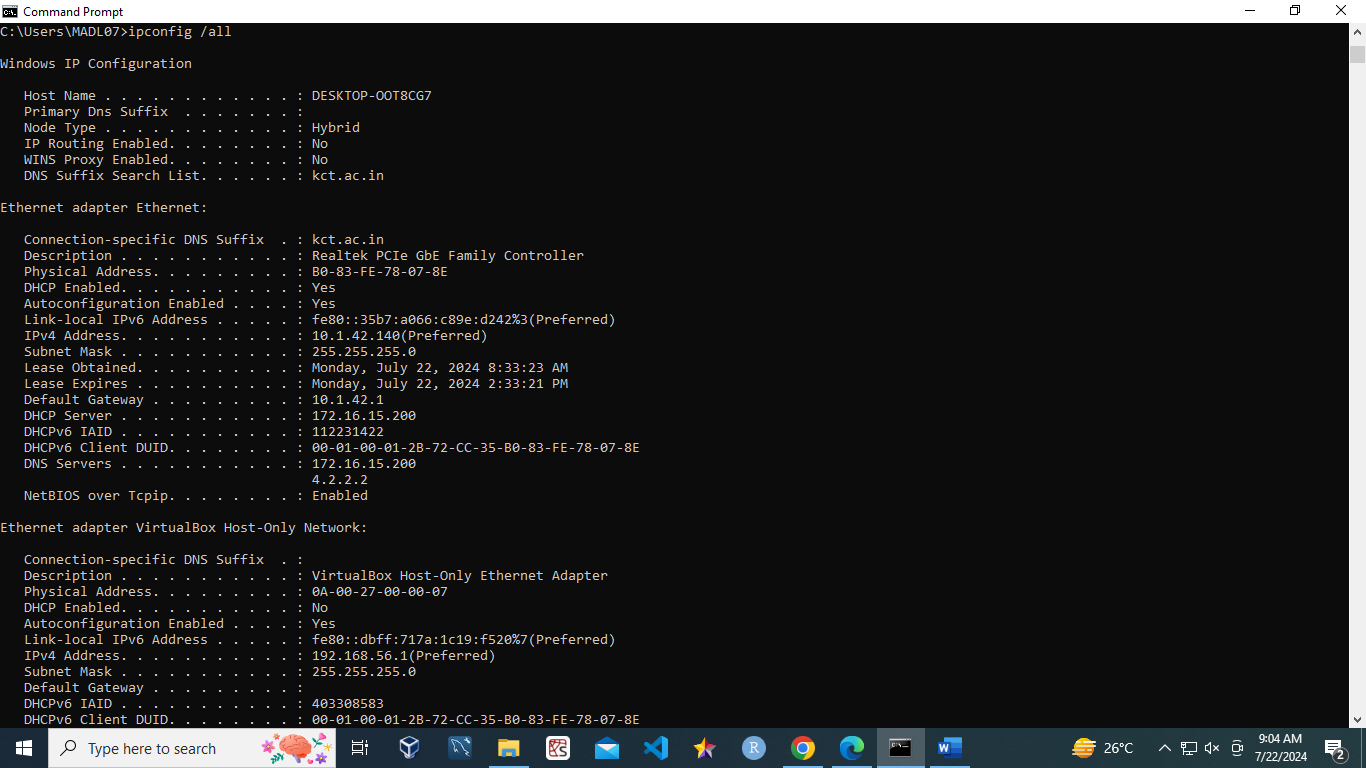
* **ipconfig**

ipconfig is a command-line utility in Windows that displays the current TCP/IP network configuration values for the computer. It is primarily used for troubleshooting network issues and managing network connections.



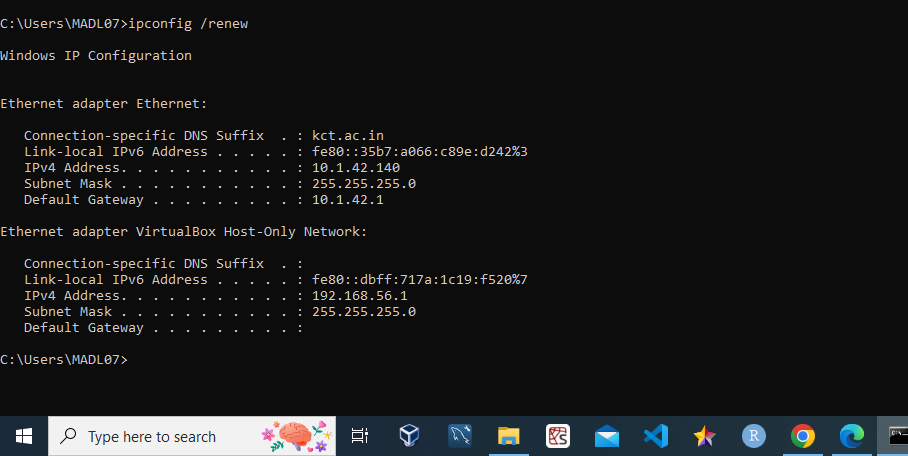
* **ipconfig /all**

**Description**: This command provides a detailed view of all network interfaces on the system, including physical (MAC) addresses, IP addresses, subnet masks, default gateways, DNS servers, and more.



* **ipconfig /renew**

The ipconfig /renew command requests a new IP address from a DHCP server for the specified network adapter in Windows.



1. To write the use of *ping* command and show the any 5 variants of the command.

**Ping Command**

The ping command is a fundamental network utility used to test connectivity between devices, measure round-trip time, diagnose network issues, perform name resolution testing, and monitor connection stability. The ping command is an essential tool for network diagnostics, providing valuable insights into the health and performance of network connections.

1. ping -t 10.1.42.140

* **Description**: Sends continuous ping requests to the specified host until interrupted (usually by pressing Ctrl + C).
* **Use Case**: Helpful for monitoring the stability of a connection over time or diagnosing intermittent connectivity issues.

A screenshot of a computer program

Description automatically generated

1. ping –a 10.1.42.140

* **Description**: Resolves the hostname of an IP address and displays it along with the ping results.
* **Use Case**: Useful for identifying the hostname of a given IP address, which can help in network diagnostics.

A computer screen with white text

Description automatically generated

1. ping -h

* **Description**: Displays help information for the ping command, including a list of available options and their descriptions.
* **Use Case**: Useful for quickly referencing the command syntax and available options.

A computer screen shot of a program

Description automatically generated

1. ping -l size 10.1.42.140

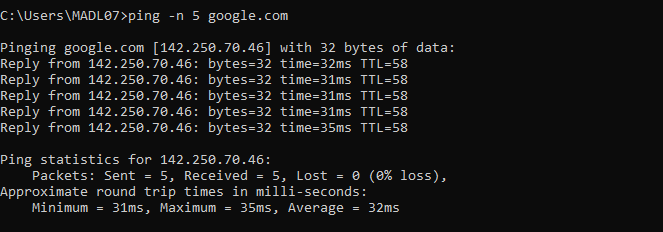
* **Description**: Specifies the size of the packet to be sent in bytes. The default size is typically 32 bytes.
* **Use Case**: Useful for testing how different packet sizes affect network performance and for diagnosing issues related to MTU (Maximum Transmission Unit) sizes.

A screen shot of a computer

Description automatically generated

1. ping -n 5 google.com

* **Description**: Sends a specified number of ping requests to the target host instead of the default continuous pings.
* **Use Case**: Useful for conducting a limited test to measure response times without overwhelming the network.



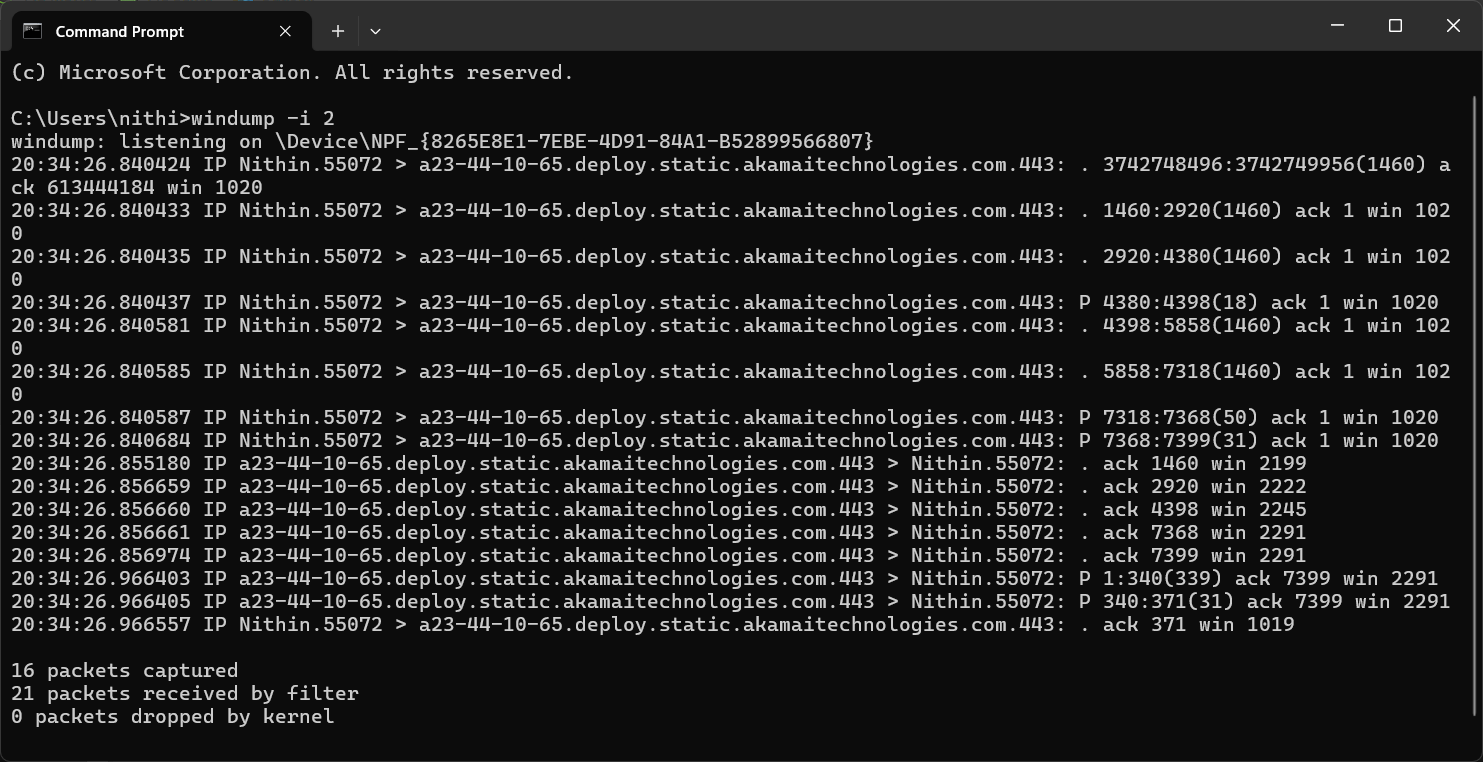
c. To write the use of *tcpdump(windump)* command execute the following commands.

**windump Command**

windump is the Windows port of the popular tcpdump tool used on Unix-like systems. It is a network packet analyzer that captures and displays the packet headers on a network interface. It can be used for network troubleshooting, monitoring, and analysis.

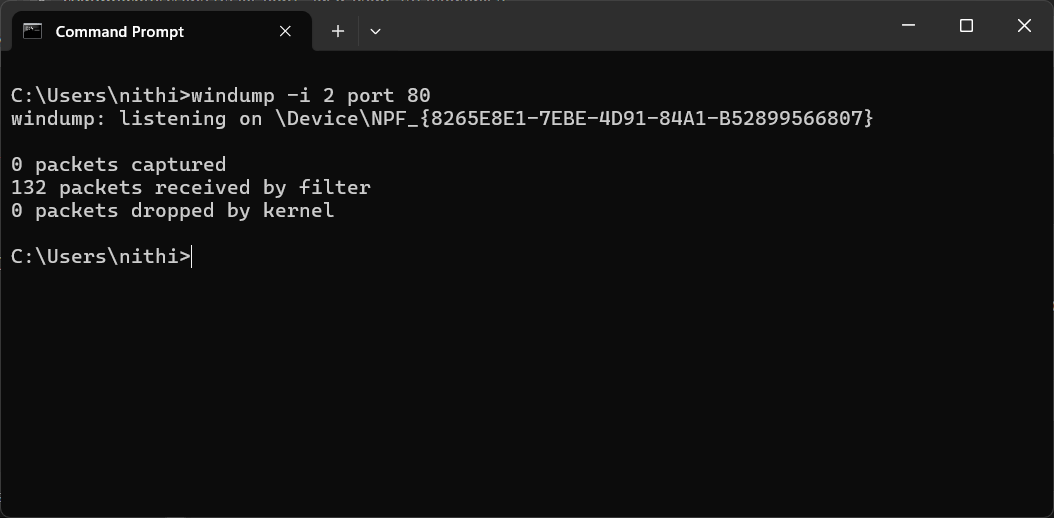
1. windump -i 1

* **Description:** Captures and displays all packets on the network interface with index 1 in real-time.
* **Use Case:** Useful for general network traffic monitoring and troubleshooting to understand the types and volume of traffic.



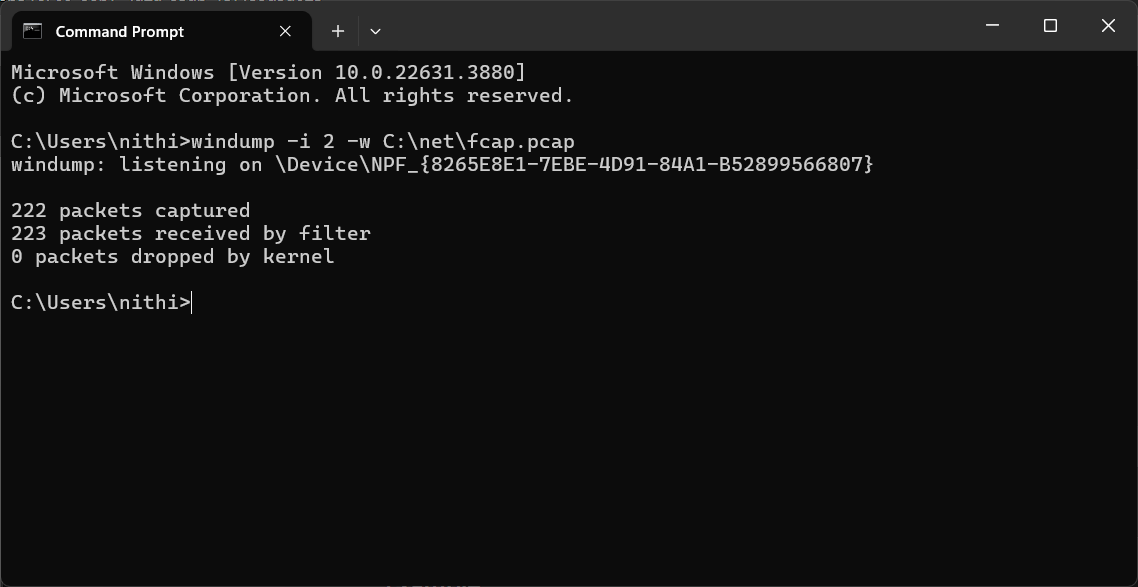
2. windump -i 1 port 80

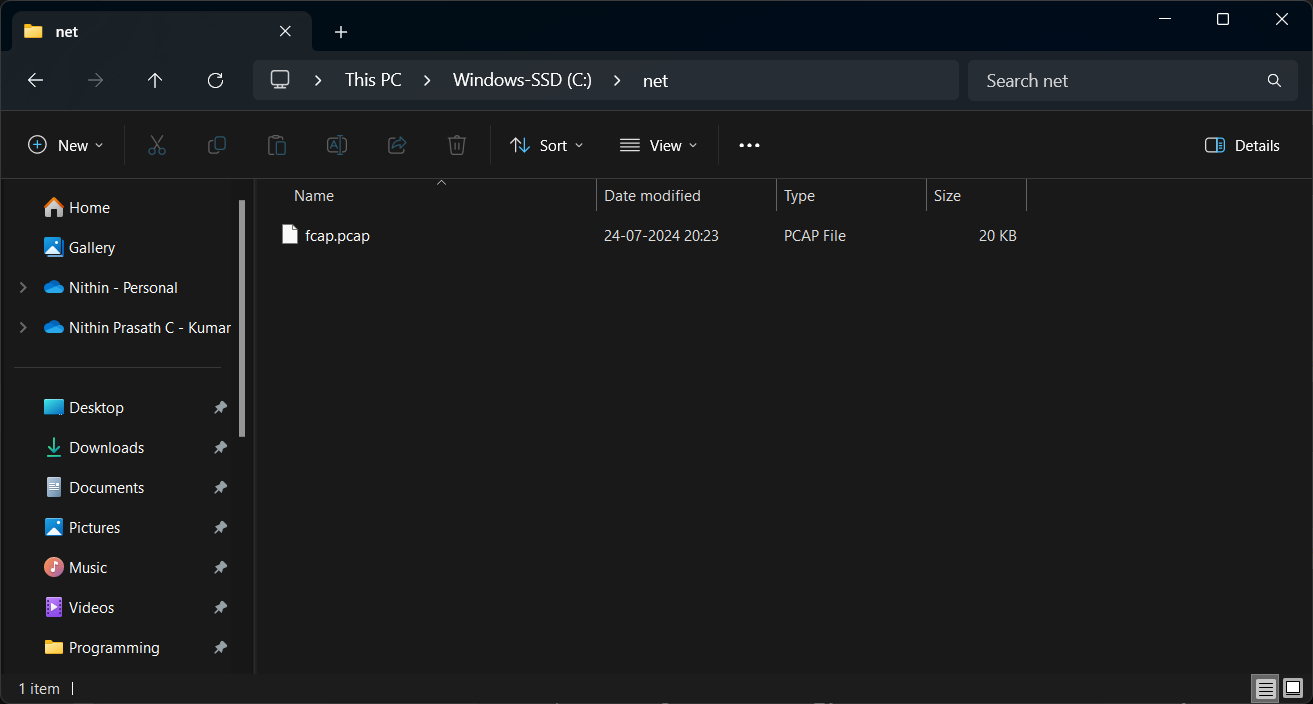
* **Description:** Captures packets on the network interface with index 1 that are destined for or originate from port 80 (HTTP traffic).
* **Use Case:** Ideal for monitoring and troubleshooting web traffic, allowing the analysis of HTTP communications between clients and servers.



3. windump -i 1 -w C:\net\fcap.pcap

* **Description:** Captures packets on the network interface with index 1 and writes them to a file named fcap.pcap in the C:\net directory.
* **Use Case:** Useful for saving network traffic data for later analysis with tools like Wireshark, aiding in detailed network forensic investigations.





d. To write the use of *traceroute* command and show the any 5 variants of the command.

Sol:

* 1. **Traceroute command**

The tracert command, known as traceroute in Unix-like systems, is a network diagnostic tool used to trace the path that packets take from a source to a destination over an IP network. It works by sending packets with incrementally increasing Time-To-Live (TTL) values, allowing it to identify each hop (router) along the route to the destination. This command helps network administrators troubleshoot connectivity issues by revealing where delays or packet losses occur, and it provides information about the round-trip time for each hop.

A screenshot of a computer program

Description automatically generated

* 1. tracert -j host-list 10.1.42.140
* **Description:** Specifies that the tracert command should use the "loose source routing" option to send packets to the destination. This allows you to specify a list of IP addresses that the packets should visit on the way to the destination.
* **Use Case:** Useful for testing connectivity through specific intermediate hosts or networks, or for bypassing certain network segments.

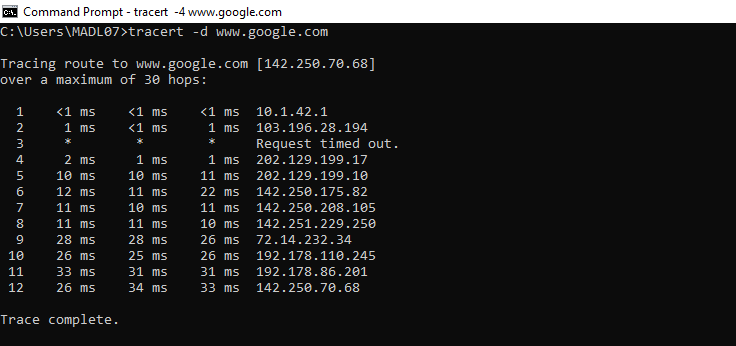
A screen shot of a computer

Description automatically generated

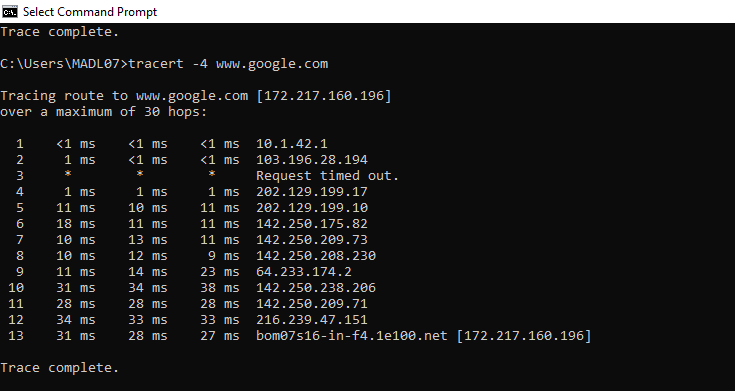
* 1. tracert -w 2000 www.google.com
* **Description**: Sets the maximum number of milliseconds to wait for a response to each probe. The default timeout is 4000 milliseconds (4 seconds).
* **Use Case**: Helpful for reducing the time spent waiting for unresponsive hops or for speeding up the overall traceroute process.



* 1. tracert -d www.google.com
* **Description**: Prevents tracert from attempting to resolve the IP addresses of intermediate hops to hostnames.
* **Use Case**: Speeds up the traceroute process by skipping the hostname resolution step, which can be slow or fail if DNS is not working properly.



* 1. tracert -4 www.google.com
* **Description**: Forces tracert to use IPv4 (-4) or IPv6 (-6) for the traceroute, even if the destination could be reached using the other protocol.
* **Use Case**: Useful for testing connectivity over a specific IP protocol version or for troubleshooting issues related to IPv4/IPv6 compatibility.



e. To write the use of *netstat* command and show the any 5 variants of the command.

*Sol:*

**netstat command**

The netstat command is a powerful networking tool used in Windows and other operating systems to display network connections, routing tables, interface statistics, and various network protocol statistics. It is essential for diagnosing network issues, monitoring network performance, and understanding the status of network connections.

1. netstat -a 10.1.42.140

* **Description**: Displays all active connections and listening ports, including both established connections and those that are waiting for incoming connections.
* **Use Case**: Useful for monitoring all network connections and identifying which ports are open and listening for connections.

A screen shot of a computer

Description automatically generated

1. netstat -h

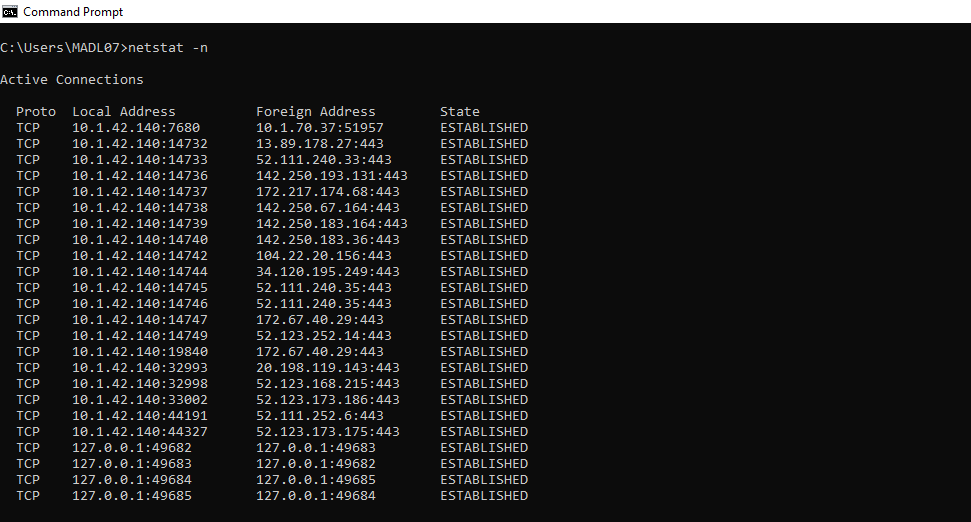
* **Description**: Displays help information about the netstat command, including available options and their descriptions.
* **Use Case**: Helpful for users who need guidance on how to use the command or want to explore its various options.

A screenshot of a computer screen

Description automatically generated

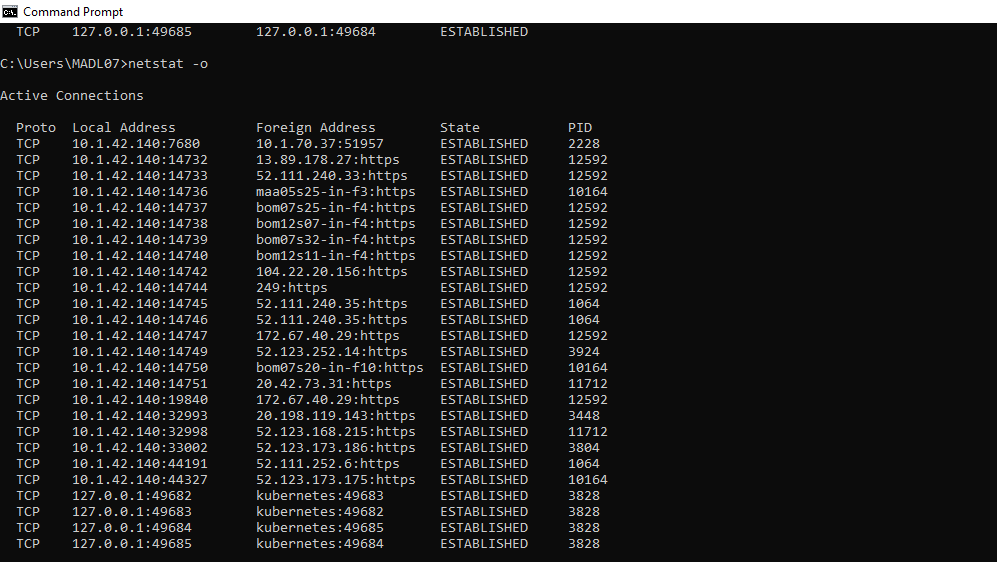
1. netstat -n

* **Description**: Displays addresses and port numbers in numerical format instead of resolving them to hostnames.
* **Use Case**: Useful for speeding up the output by avoiding DNS lookups, which can be slow or fail if there are DNS issues.



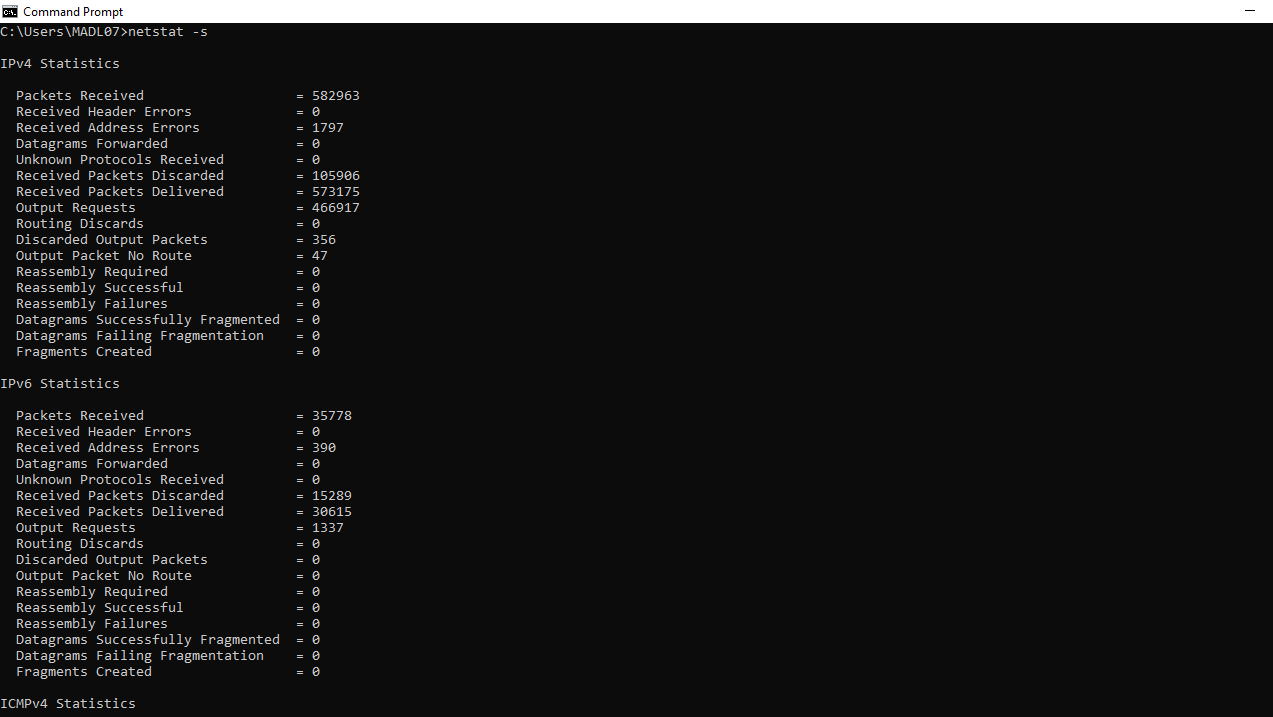
1. netstat -o

* **Description**: Displays active connections and includes the process ID (PID) associated with each connection.
* **Use Case**: Useful for identifying which applications are using specific network connections, aiding in troubleshooting and monitoring.



1. netstat -s

* **Description**: Displays statistics for each protocol (TCP, UDP, ICMP, etc.), providing detailed information about network activity and errors.
* **Use Case**: Helpful for diagnosing network issues by revealing statistics that indicate potential problems with specific protocols.



**Post Lab:**

**nslookup command:**

* **Description**: nslookup is a command-line tool used to query the Domain Name System (DNS) for information about domain names and IP addresses, enabling users to retrieve DNS records and perform reverse lookups.
* **Use Case:** It is commonly used for troubleshooting DNS issues by verifying domain name resolution, checking the IP address associated with a domain, and gathering DNS records to ensure proper configuration of web and email services.

A black screen with white text

Description automatically generated

**Result:**

All experiments have been successfully executed, with no errors or issues encountered. The expected results have been achieved, as demonstrated by the attached screenshots.

**Exp: no: 2**

Analyze the network traffic using Packet tracer tool .

**Aim:**

To analyse the network traffic using Cisco Packet tracer tool and write the syntax, execute and place the screenshot for all the commands worked on.

1. Configure a simple network connecting two LANs using Cisco Packet Tracer.

**Equipment:**

* 2 x 2960-24TT Switches
* 1 x ISR4331 Router
* 4 x PCs

**Syntax:**

**Step 1: Open Cisco Packet Tracer**

1. Open Cisco Packet Tracer on your computer.

**Step 2: Create the Network Topology**

1. **Drag and Drop Devices**: Drag two 2960-24TT Switches, one ISR4331 Router, and four PCs onto the workspace.
2. **Connect Devices**:
   * Use the Copper Straight-Through cable to connect:
     + PC0 to Switch0 (Port FastEthernet0/1)
     + PC1 to Switch0 (Port FastEthernet0/2)
     + PC2 to Switch1 (Port FastEthernet0/1)
     + PC3 to Switch1 (Port FastEthernet0/2)
     + Switch0 (Port GigabitEthernet0/1) to Router (Port GigabitEthernet0/0)
     + Switch1 (Port GigabitEthernet0/1) to Router (Port GigabitEthernet0/1)

**Step 3: Configure IP Addresses on PCs**

1. **PC0**:
   * IP Address: 192.168.1.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.1.1
2. **PC1**:
   * IP Address: 192.168.1.3
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.1.1
3. **PC2**:
   * IP Address: 192.168.2.2
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.2.1
4. **PC3**:
   * IP Address: 192.168.2.3
   * Subnet Mask: 255.255.255.0
   * Default Gateway: 192.168.2.1

**Step 4: Configure IP Addresses on Router**

1. **Router**:
   * Enter the CLI of the ISR4331 Router.
   * Execute the following commands:

Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1

Router(config-if)# ip address 192.168.2.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

A diagram of a computer network

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Configure a network using Ring/Bus/Tree Topology using Packet tracer tool.

**Equipment:**

* 2960-24TT Switches
* ISR4331 Router
* PCs
* Appropriate cables (Copper Straight-Through and Copper Cross-Over)

**Steps for Different Topologies:**

**1. Ring Topology:**

**Ring Topology** connects each device to exactly two other devices, forming a single continuous pathway for signals through each device.

**Step 1: Open Cisco Packet Tracer**

1. Open Cisco Packet Tracer on your computer.

**Step 2: Create the Network Topology**

1. **Drag and Drop Devices**: Drag three 2960-24TT Switches and four PCs onto the workspace.
2. **Connect Devices**:
   * Use the Copper Cross-Over cable to connect:
     + Switch0 (Port GigabitEthernet0/1) to Switch1 (Port GigabitEthernet0/1)
     + Switch1 (Port GigabitEthernet0/2) to Switch2 (Port GigabitEthernet0/1)
     + Switch2 (Port GigabitEthernet0/2) to Switch0 (Port GigabitEthernet0/2)
   * Use the Copper Straight-Through cable to connect:
     + PC0 to Switch0 (Port FastEthernet0/1)
     + PC1 to Switch1 (Port FastEthernet0/1)
     + PC2 to Switch2 (Port FastEthernet0/1)
     + PC3 to Switch0 (Port FastEthernet0/2)

**Step 3: Configure IP Addresses on PCs**

1. **PC0**:
   * IP Address: 192.168.1.2
   * Subnet Mask: 255.255.255.0
2. **PC1**:
   * IP Address: 192.168.1.3
   * Subnet Mask: 255.255.255.0
3. **PC2**:
   * IP Address: 192.168.1.4
   * Subnet Mask: 255.255.255.0
4. **PC3**:
   * IP Address: 192.168.1.5
   * Subnet Mask: 255.255.255.0

A diagram of a computer network

Description automatically generated

A screenshot of a computer

Description automatically generated

**2. Bus Topology:**

**Bus Topology** connects all devices to a single central cable, called the bus or backbone.

**Step 1: Open Cisco Packet Tracer**

1. Open Cisco Packet Tracer on your computer.

**Step 2: Create the Network Topology**

1. **Drag and Drop Devices**: Drag one 2960-24TT Switch and four PCs onto the workspace.
2. **Connect Devices**:
   * Use the Copper Straight-Through cable to connect:
     + PC0 to Switch0 (Port FastEthernet0/1)
     + PC1 to Switch0 (Port FastEthernet0/2)
     + PC2 to Switch0 (Port FastEthernet0/3)
     + PC3 to Switch0 (Port FastEthernet0/4)

**Step 3: Configure IP Addresses on PCs**

1. **PC0**:
   * IP Address: 192.168.1.2
   * Subnet Mask: 255.255.255.0
2. **PC1**:
   * IP Address: 192.168.1.3
   * Subnet Mask: 255.255.255.0
3. **PC2**:
   * IP Address: 192.168.1.4
   * Subnet Mask: 255.255.255.0
4. **PC3**:
   * IP Address: 192.168.1.5
   * Subnet Mask: 255.255.255.0

A screenshot of a computer

Description automatically generated

**3. Tree Topology:**

**Tree Topology** combines characteristics of Star and Bus topologies. It consists of groups of star-configured networks connected to a linear bus backbone.

**Step 1: Open Cisco Packet Tracer**

1. Open Cisco Packet Tracer on your computer.

**Step 2: Create the Network Topology**

1. **Drag and Drop Devices**: Drag three 2960-24TT Switches, one ISR4331 Router, and six PCs onto the workspace.
2. **Connect Devices**:
   * Use the Copper Straight-Through cable to connect:
     + Router (Port GigabitEthernet0/0) to Switch0 (Port GigabitEthernet0/1)
     + Switch0 (Port GigabitEthernet0/2) to Switch1 (Port GigabitEthernet0/1)
     + Switch0 (Port GigabitEthernet0/3) to Switch2 (Port GigabitEthernet0/1)
     + PC0 to Switch1 (Port FastEthernet0/1)
     + PC1 to Switch1 (Port FastEthernet0/2)
     + PC2 to Switch1 (Port FastEthernet0/3)
     + PC3 to Switch2 (Port FastEthernet0/1)
     + PC4 to Switch2 (Port FastEthernet0/2)
     + PC5 to Switch2 (Port FastEthernet0/3)

**Step 3: Configure IP Addresses on PCs**

1. **PC0**:
   * IP Address: 192.168.1.2
   * Subnet Mask: 255.255.255.0
2. **PC1**:
   * IP Address: 192.168.1.3
   * Subnet Mask: 255.255.255.0
3. **PC2**:
   * IP Address: 192.168.1.4
   * Subnet Mask: 255.255.255.0
4. **PC3**:
   * IP Address: 192.168.1.5
   * Subnet Mask: 255.255.255.0

A diagram of a computer network

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Configure a network for four departments in your college with a minimum of five PCs in a network.

**Equipment:**

* 2960-24TT Switches
* PCs
* Appropriate cables (Copper Straight-Through)

**Steps:**

**Step 1:** Open Cisco Packet Tracer

**Step 2:** Create the Network Topology

1. Drag and Drop Devices:
   * Drag four 2960-24TT Switches onto the workspace (one for each department).
   * Drag twenty PCs onto the workspace (five for each department).

**Step 3: Connect Devices**

1. **CSE Department:**
   * **Switch0 (CSE Department):**
     + **Use Copper Straight-Through cable to connect:**
       - PC0 to Switch0 (Port FastEthernet0/1)
       - PC1 to Switch0 (Port FastEthernet0/2)
       - PC2 to Switch0 (Port FastEthernet0/3)
       - PC3 to Switch0 (Port FastEthernet0/4)
       - PC4 to Switch0 (Port FastEthernet0/5)
2. **IT Department:**
   * **Switch1 (IT Department):**
     + **Use Copper Straight-Through cable to connect:**
       - PC5 to Switch1 (Port FastEthernet0/1)
       - PC6 to Switch1 (Port FastEthernet0/2)
       - PC7 to Switch1 (Port FastEthernet0/3)
       - PC8 to Switch1 (Port FastEthernet0/4)
       - PC9 to Switch1 (Port FastEthernet0/5)
3. **AIDS Department:**
   * **Switch2 (AIDS Department):**
     + **Use Copper Straight-Through cable to connect:**
       - PC10 to Switch2 (Port FastEthernet0/1)
       - PC11 to Switch2 (Port FastEthernet0/2)
       - PC12 to Switch2 (Port FastEthernet0/3)
       - PC13 to Switch2 (Port FastEthernet0/4)
       - PC14 to Switch2 (Port FastEthernet0/5)
4. **MECH Department:**
   * **Switch3 (MECH Department):**
     + **Use Copper Straight-Through cable to connect:**
       - PC15 to Switch3 (Port FastEthernet0/1)
       - PC16 to Switch3 (Port FastEthernet0/2)
       - PC17 to Switch3 (Port FastEthernet0/3)
       - PC18 to Switch3 (Port FastEthernet0/4)
       - PC19 to Switch3 (Port FastEthernet0/5)

**Step 4: Configure IP Addresses on PCs**

**CSE Department (Subnet: 192.168.1.1/24):**

1. PC0: IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0
2. PC1: IP Address: 192.168.1.3, Subnet Mask: 255.255.255.0
3. PC2: IP Address: 192.168.1.4, Subnet Mask: 255.255.255.0
4. PC3: IP Address: 192.168.1.5, Subnet Mask: 255.255.255.0
5. PC4: IP Address: 192.168.1.6, Subnet Mask: 255.255.255.0

**IT Department (Subnet: 192.168.2.1/24):**

1. PC5: IP Address: 192.168.1.7, Subnet Mask: 255.255.255.0
2. PC6: IP Address: 192.168.1.8, Subnet Mask: 255.255.255.0
3. PC7: IP Address: 192.168.1.9, Subnet Mask: 255.255.255.0
4. PC8: IP Address: 192.168.1.10, Subnet Mask: 255.255.255.0
5. PC9: IP Address: 192.168.1.11, Subnet Mask: 255.255.255.0

**AIDS Department (Subnet: 192.168.3.1/24):**

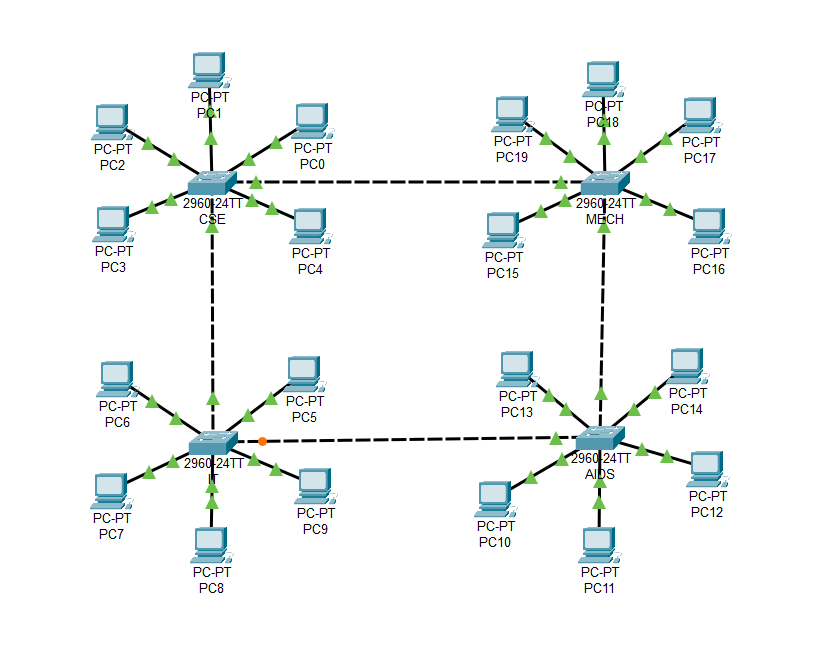
1. PC10: IP Address: 192.168.1.12, Subnet Mask: 255.255.255.0
2. PC11: IP Address: 192.168.1.13, Subnet Mask: 255.255.255.0
3. PC12: IP Address: 192.168.1.14, Subnet Mask: 255.255.255.0
4. PC13: IP Address: 192.168.1.15, Subnet Mask: 255.255.255.0
5. PC14: IP Address: 192.168.1.16, Subnet Mask: 255.255.255.0

**MECH Department (Subnet: 192.168.4.1/24):**

1. PC15: IP Address: 192.168.1.17, Subnet Mask: 255.255.255.0
2. PC16: IP Address: 192.168.1.18, Subnet Mask: 255.255.255.0
3. PC17: IP Address: 192.168.1.19, Subnet Mask: 255.255.255.0
4. PC18: IP Address: 192.168.1.20, Subnet Mask: 255.255.255.0
5. PC19: IP Address: 192.168.1.20, Subnet Mask: 255.255.255.0

**Step 5: Connect Switches**

1. **Use Copper Straight-Through cables to interconnect the switches:**
   * Switch0 (Port GigabitEthernet0/1) to Switch1 (Port GigabitEthernet0/1)
   * Switch0 (Port GigabitEthernet0/2) to Switch2 (Port GigabitEthernet0/1)
   * Switch3 (Port GigabitEthernet0/1) to Switch1 (Port GigabitEthernet0/2)
   * Switch3 (Port GigabitEthernet0/2) to Switch2 (Port GigabitEthernet0/2)



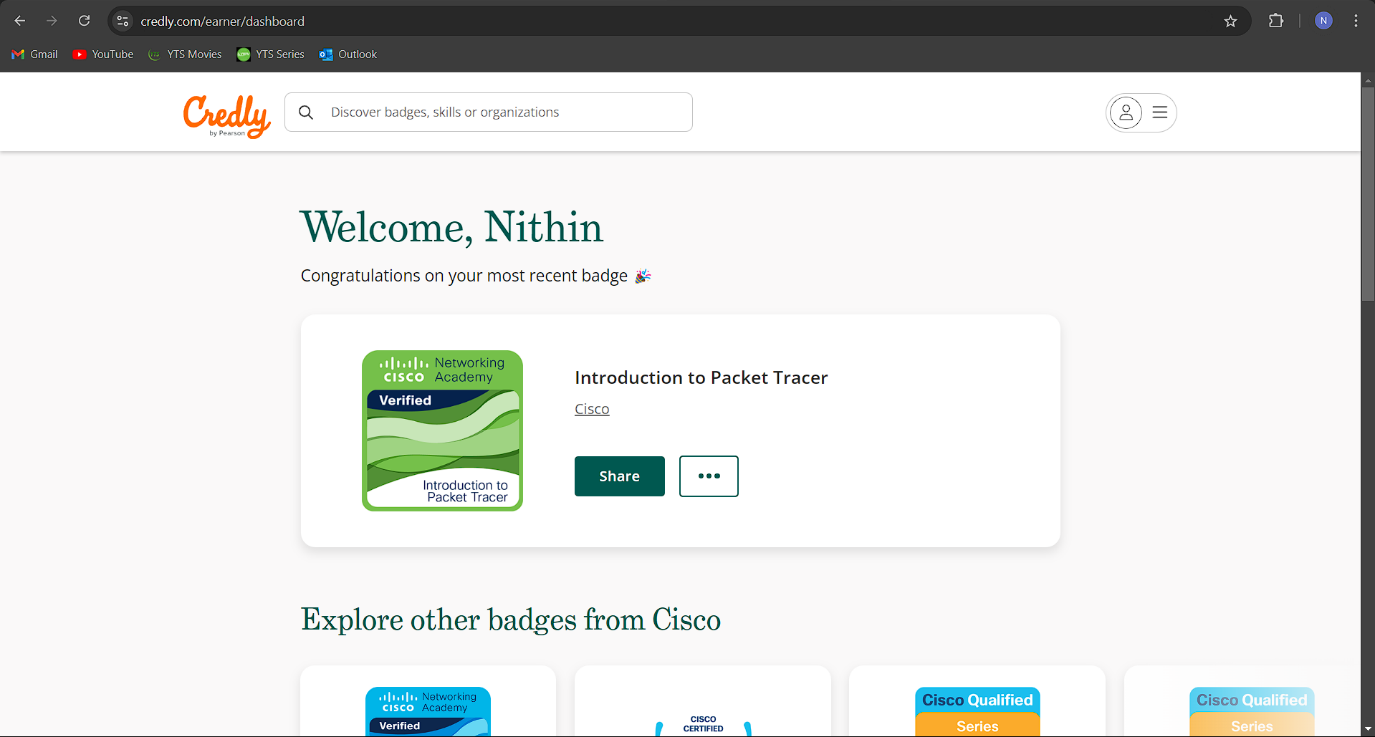
A screenshot of a computer

Description automatically generated

**PostLab:**

Completion of the Cisco Packet tracer fundamental course and attachment of the certificate.

[https://skillsforall.com/topics/cisco-packet-tracer?utm\_source=n...](https://skillsforall.com/topics/cisco-packet-tracer)



Certificate Verification Link:

<https://www.credly.com/badges/dc101725-a8e7-412d-85de-5a96cdb14653/public_url>

**Result:**

All experiments have been successfully executed, with no errors or issues encountered. The expected results have been achieved, as demonstrated by the attached screenshots.

**Exp: no: 3**

Analyse the network traffic using Wireshark tool.

**Aim:**

To analyse the network traffic using Wireshark tool and write the syntax, execute and place the screenshot of all the commands worked on.

a. Explain what is a packet analyzer ?

**Packet Analyzer**

A packet analyzer, also known as a network analyzer, protocol analyzer, or packet sniffer, is a tool used to capture, monitor, and analyze data packets traveling across a network. It allows network administrators, security professionals, and developers to examine the data being transmitted over a network in real-time or from saved packet capture files. By capturing all traffic on a network, a packet analyzer can provide detailed information about each packet, including its source and destination IP addresses, the protocols used, and the data payload. This capability makes packet analyzers indispensable for troubleshooting network issues, ensuring security, and optimizing network performance.

Beyond troubleshooting, packet analyzers are also crucial for security analysis. They can detect and help prevent unauthorized access, monitor for malicious activities, and identify vulnerabilities by examining the flow of data through a network. Additionally, developers use packet analyzers to test and debug network protocols, ensuring that applications interact with the network as intended. Popular tools like Wireshark, tcpdump, and SolarWinds offer varying degrees of functionality, from simple packet capture to advanced network traffic analysis, making packet analyzers versatile tools in both network management and cybersecurity.

**Applications of Packet Analyzers**

* **Network Monitoring and Troubleshooting:** Identifies network bottlenecks, misconfigurations, and connectivity issues.
* **Security Analysis:** Detects unauthorized access, malware, and suspicious activities.
* **Performance Optimization:** Analyzes traffic patterns to improve network performance.
* **Protocol Development and Debugging:** Assists developers in testing and debugging network protocols.

b. Explain the types of packet analyzers.

**Types of Packet Analyzers**

**1. Network Tap Analyzers:**

**Explanation:** Network Tap Analyzers rely on hardware devices called network taps to physically intercept network cables and capture all data passing through. They offer a passive monitoring approach, ensuring that the network's performance and integrity are unaffected during the analysis.

**Example:**

* Garland Technology Network Taps
* NetOptics Bypass Switch
* Datacom Systems TAPs

**2. Software-Based Packet Analyzers:**

**Explanation:** These packet analyzers are software applications installed on computers or servers to capture and examine network traffic on specific segments. They are versatile and widely used for various purposes, including troubleshooting and security monitoring.

**Example:**

* Wireshark
* tcpdump
* Microsoft Network Monitor

**3. Inline Packet Analyzers:**

**Explanation:** Inline packet analyzers are deployed directly within the network path, such as within firewalls or routers. They not only monitor network traffic but also have the capability to block or alter packets based on predefined rules, making them suitable for proactive security measures.

**Example:**

* Cisco Firepower
* Palo Alto Networks Next-Generation Firewall
* Juniper SRX Series Firewalls

**4. Remote Packet Analyzers:**

**Explanation:** Remote packet analyzers allow network administrators to capture and analyze traffic from distant locations without being physically present at the monitoring site. This capability is particularly useful for managing large-scale, distributed networks.

**Example:**

* SolarWinds Network Performance Monitor
* PRTG Network Monitor
* Nagios XI

**5. Protocol-Specific Packet Analyzers:**

**Explanation:** These analyzers focus on capturing and analyzing traffic for specific protocols like HTTP, FTP, or VoIP. They provide in-depth insights into the performance and behavior of specific applications or services on the network.

**Example:**

* SIPp (VoIP)
* Fiddler (HTTP)
* TShark (various protocols)

**6. Capture Appliances:**

**Explanation:** Capture appliances are dedicated hardware devices designed for long-term traffic capture and storage. These devices are optimized for high-speed data capture and are often used in environments where detailed and prolonged traffic analysis is required.

**Example:**

* EndaceProbe
* Riverbed SteelCentral
* VSS Monitoring Distributed Series

c. Dinesh a tech evangelist is interested to learn about packet analyzer tools and decided to use Wireshark. Dinesh trust in you, now your job is help Dinesh in learning Wireshark, now help Dinesh in installing Wireshark tool .

**Step 1:** Visit the official Wireshark website using any web browser. A page with different installers of Wireshark will be shown. Click on ‘Windows x64 Installer’.A screenshot of a computer

Description automatically generated

**Step 2:** Once the download is complete, open it. Setup screen will appear, click on Next.A screenshot of a computer

Description automatically generated

**Step 3:** The next screen will be of License Agreement, click on Noted.A screenshot of a computer

Description automatically generated

**Step 4:** This screen is for choosing components, all components are already marked so don’t change anything just click on the Next button.A screenshot of a computer

Description automatically generated

**Step 5:** This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.A screenshot of a computer program

Description automatically generated

**Step 6:** The next screen will be of installation location so choose the drive which will have sufficient memory space for installation. It needs only a memory space of 261.6 MB.A screenshot of a computer

Description automatically generated

**Step 7:** Next screen has an option to install Npcap which is used with Wireshark to capture packets. pcap means packet capture so the install option is already checked don’t change anything and click the next button.A screenshot of a computer

Description automatically generated

**Step 8:** Next screen is about USB network capturing so it is one’s choice to use it or not, click on Install.

A screenshot of a computer error

Description automatically generated

**Step 9:** After this installation process will start. This installation will prompt for Npcap and USBPcap installation. Agree to everything and click on next.A screenshot of a computer

Description automatically generated

**Step 10:** After the installation process of Wireshark is complete click on the Next button.

A screenshot of a computer

Description automatically generated

**Step 11:** Click on Finish after the installation process of Wireshark is complete. Wireshark is successfully installed on the system and an icon is created on the desktop.A screenshot of a computer

Description automatically generated

**Step 12:** Now run the software and see the interface. At this point, you have successfully installed Wireshark on your windows systemA screenshot of a computer

Description automatically generated

d. Now help Dinesh to understand the overview of Wireshark.

**Overview of Wireshark**

Wireshark is a powerful, widely used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network. It is an essential tool for network administrators, security professionals, and developers who need to diagnose network problems, troubleshoot issues, or analyze network traffic for security purposes.

**Key Features of Wireshark:**

* **Packet Capture:** Wireshark captures network packets in real-time, providing detailed information about each packet, including headers, payloads, and metadata. Users can capture traffic from live networks or read from previously saved capture files.
* **Detailed Protocol Analysis:** Wireshark supports a vast array of network protocols, offering detailed analysis and decoding for over a thousand protocols, including TCP/IP, HTTP, DNS, FTP, and many more. This makes it invaluable for understanding how different protocols operate and interact within a network.
* **User-Friendly Interface:** Wireshark's graphical user interface (GUI) is designed to be user-friendly, making it easier to navigate through captured data. The interface allows users to apply filters, search for specific data, and highlight important information.
* **Powerful Filtering Capabilities:** Wireshark provides robust filtering tools, allowing users to focus on specific types of traffic or packets of interest. Display filters, capture filters, and coloring rules can be applied to quickly isolate relevant data.
* **Cross-Platform Availability:** Wireshark is available on multiple platforms, including Windows, macOS, and Linux, making it accessible to a broad range of users.
* **Open-Source and Extensible:** Wireshark is an open-source tool, meaning it is freely available and supported by a large community. Users can extend its functionality by writing custom dissectors or plugins to analyze new or proprietary protocols.

**Common Use Cases:**

* **Network Troubleshooting:** Wireshark helps identify network bottlenecks, latency issues, and misconfigurations by analyzing packet flows and protocol behaviors.
* **Security Analysis:** Security professionals use Wireshark to detect malicious traffic, investigate security incidents, and analyze attacks such as packet sniffing, man-in-the-middle attacks, and more.
* **Protocol Development:** Developers use Wireshark to debug and test network protocols, ensuring they function correctly during communication between devices.
* **Educational Purposes:** Wireshark is a valuable educational tool, helping students and professionals learn about network protocols and their operations by providing a hands-on, interactive experience.

e. While you are explaining the overview of Wireshark Dinesh observed some IP address in the packet capturing window, Dinesh want to extract the information of particular IP address and see where it is going and from where it is receiving the information, help Dinesh to filter particular IP address and its source and destination.

**Step 1: Open Wireshark:** Launch Wireshark and start capturing packets on the desired network interface or open a saved capture file.

**Step 2: Start Packet Capture:** Begin capturing packets or load an existing capture to analyze.

**Step 3: Apply IP Address Filter:**

* Use ip.addr == 192.168.70.99 to filter traffic for a specific IP address.
* For filtering by source or destination, use ip.src == 192.168.70.99

**Step 4: Analyze Filtered Traffic:** Review the source and destination addresses to understand where the traffic is coming from and going to.

* **Time:** Timing of each packet captured during a network session.
* **Source:** The IP address that sent the packet.
* **Destination:** The IP address that received the packet.
* **Protocol:** The protocol used (e.g., TCP, UDP, HTTP).
* **Length:** Size of each packet captured during the network session.
* **Info:** Additional information about the packet, such as the ports used.

**Step 5:** **Examine Packet Details:** Click on any packet to view its detailed information in the packet details pane.

**Step 6: Export Filtered Data:** If needed, export the filtered packets for further analysis.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Result:**

Thus, the network traffic was analysed using Wireshark tool and the commands were executed and verified successfully.

**Exp: no: 4**

Simulation of Data Link layer and Network Layer Protocols.

**Aim:**

To simulate Data Link layer and Network Layer Protocols and write the syntax, execute and place the screenshot for all the commands worked on.

a. Demonstrate the frame transmission scenario using Sniffing tool.

**Syntax:**

1. Open Wireshark and start a new capture on the network interface you want to monitor (e.g., Ethernet, Wi-Fi).
2. Perform a network activity that involves communication between devices, like accessing a shared folder on a networked computer or pinging another computer on the same network.
3. Stop the capture in Wireshark after some packets have been captured.
4. Look for frames in the capture:
   * Filter for Data Link layer protocols like Ethernet by typing eth in the filter bar.
   * You should see frames with information like source and destination MAC addresses, Ether Type, etc.
5. Select a frame to view its details, including the frame header and payload.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

b. Demonstrate the packet transmission scenario using Sniffing tool.

**Syntax:**

1. In Wireshark, start a new capture again on the same network interface.
2. Perform a network activity that involves communication over IP, such as opening a website in a web browser or using ping to contact an external server (e.g., ping google.com).
3. Stop the capture after a few packets are captured.
4. Look for packets in the capture:
   * Filter for Network layer protocols like IP by typing ip in the filter bar.
   * You should see packets containing information like source and destination IP addresses, protocol types (e.g., TCP, UDP), etc.
5. Select a packet to view its details, including the IP header and encapsulated segment data.
6. To filter for specific protocols, use more detailed filters like:
   * tcp for TCP packets.
   * udp for UDP packets.
   * icmp for ICMP packets (used in ping).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Result:**

All experiments have been successfully executed, with no errors or issues encountered. The expected results have been achieved, as demonstrated by the attached screenshots.

**Exp: no: 5**

Performance analysis of routing protocols using simulation tool.

**Aim:**

To simulate routing protocols for Data Link layer and Network Layer, and to write the syntax, execute the commands, and capture the screenshots

a. Construct 3 to 4 networks each connected by a router and enable packet transmission between all the networks.

**Syntax:**

**Step 1: Setting up Devices**

**Components in the Topology:**

1. 3 Routers (1841) - Router 4, Router 5, Router 6
2. 3 Switches (2960) - Switch 0, Switch 1, Switch 2
3. 6 PCs - PC0, PC1 (Network A), PC2, PC3 (Network B), PC4, PC5 (Network C)

**Step 2: Device Connections**

**Connecting the Devices:**

* **PCs to Switches:**
  + Network A:
    - PC0 -> Switch0 (FastEthernet0/1)
    - PC1 -> Switch0 (FastEthernet0/2)
  + Network B:
    - PC2 -> Switch1 (FastEthernet0/1)
    - PC3 -> Switch1 (FastEthernet0/2)
  + Network C:
    - PC4 -> Switch2 (FastEthernet0/1)
    - PC5 -> Switch2 (FastEthernet0/2)
* **Switches to Routers:**
  + Switch0 -> Router 4 (FastEthernet0/0)
  + Switch1 -> Router 5 (FastEthernet0/0)
  + Switch2 -> Router 6 (FastEthernet0/0)
* **Router-to-Router Connections (using Serial Interfaces):**
  + Router 4 (Se0/0/0) -> Router 5 (Se0/0/0)
  + Router 5 (Se0/0/1) -> Router 6 (Se0/0/0)
  + Router 6 (Se0/0/1) -> Router 4 (Se0/0/1)

**Step 3: Configuring PCs**

For Each PC:

**Go to:** Desktop -> IP Configuration.

* **Network A (PC0, PC1):**
  + IP Addresses:
    - PC0: 192.168.1.2
    - PC1: 192.168.1.3
  + Subnet Mask: 255.255.255.0
  + Default Gateway: 192.168.1.1 (Router 4's IP)
* **Network B (PC2, PC3):**
  + IP Addresses:
    - PC2: 192.168.2.2
    - PC3: 192.168.2.3
  + Subnet Mask: 255.255.255.0
  + Default Gateway: 192.168.2.1 (Router 5's IP)
* **Network C (PC4, PC5):**
  + IP Addresses:
    - PC4: 192.168.3.2
    - PC5: 192.168.3.3
  + Subnet Mask: 255.255.255.0
  + Default Gateway: 192.168.3.1 (Router 6's IP)

**Step 4: Configuring the Routers**

Router Configuration Steps:

**Router 4 (Network A):**

1. Configure FastEthernet Interface (Fa0/0):
   * IP Address: 192.168.1.1
   * Subnet Mask: 255.255.255.0
   * Turn on the interface.
2. Configure Serial Interface (Se0/0/0) - Link to Router 5:
   * IP Address: 10.0.0.2
   * Subnet Mask: 255.0.0.0
   * Clock Rate: 148000
   * Turn on the interface.
3. Configure Serial Interface (Se0/0/1) - Link to Router 6:
   * IP Address: 11.0.0.1
   * Subnet Mask: 255.0.0.0
   * Clock Rate: 148000
   * Turn on the interface.

**Router 5 (Network B):**

1. Configure FastEthernet Interface (Fa0/0):
   * IP Address: 192.168.2.1
   * Subnet Mask: 255.255.255.0
   * Turn on the interface.
2. Configure Serial Interface (Se0/0/0) - Link to Router 4:
   * IP Address: 10.0.0.1
   * Subnet Mask: 255.0.0.0
   * Turn on the interface.
3. Configure Serial Interface (Se0/0/1) - Link to Router 6:
   * IP Address: 12.0.0.2
   * Subnet Mask: 255.0.0.0
   * Clock Rate: 148000
   * Turn on the interface.

**Router 6 (Network C):**

1. Configure FastEthernet Interface (Fa0/0):
   * IP Address: 192.168.3.1
   * Subnet Mask: 255.255.255.0
   * Turn on the interface.
2. Configure Serial Interface (Se0/0/0) - Link to Router 5:
   * IP Address: 12.0.0.1
   * Subnet Mask: 255.0.0.0
   * Turn on the interface.
3. Configure Serial Interface (Se0/0/1) - Link to Router 4:
   * IP Address: 11.0.0.2
   * Subnet Mask: 255.0.0.0
   * Turn on the interface.

**Step 5: Configuring Routing (RIP)**

Enabling RIP on Each Router:

1. Router 4 (Network A):
   * Network: 10.0.0.0 (Router 4 and Router 5 connection)
   * Network: 11.0.0.0 (Router 4 and Router 6 connection)
2. Router 5 (Network B):
   * Network: 10.0.0.0 (Router 4 and Router 5 connection)
   * Network: 12.0.0.0 (Router 5 and Router 6 connection)
3. Router 6 (Network C):
   * Network: 11.0.0.0 (Router 4 and Router 6 connection)
   * Network: 12.0.0.0 (Router 5 and Router 6 connection)

Save configurations after setting up RIP for all routers.

**Step 6: Testing the Network**

**To test the connectivity:**

1. Ping from a PC in one network to the router in the same network:
   * For example, from PC0 (192.168.1.2) to Router 4 (192.168.1.1).
2. Ping from a PC in one network to a router in a different network:
   * For example, from PC0 (192.168.1.2) to Router 6 (192.168.3.1).
3. Ping between PCs across networks:
   * Ping from PC0 (192.168.1.2) in Network A to PC4 (192.168.3.2) in Network C.
   * If the ping is successful, the routing between networks is configured properly.

**Output:**

**A diagram of a network

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Result:**

All experiments have been successfully executed, with no errors or issues encountered. The expected results have been achieved, as demonstrated by the attached screenshots.