Experiment No: 14	
Name	Suyash Tambe
PRN	22070126117
Date of Performance	
Title	To implement Network Troubleshooting using command line tools
Theory (short)	Networking commands are crucial tools for interacting with and diagnosing network connections, resolving DNS problems, inspecting routing tables, and collecting data packets. These commands are universal in the sense that they may be used on a variety of operating systems (Windows, macOS, and Linux), however slight syntax changes may occur. Each of these commands has a distinct purpose, but they all help to comprehend the flow of data in a networked system.

Procedure	**1. Ping - Test Connectivity** • **Objective**: Verify if a device can reach another device over the network. • **Steps**: 1. Open a terminal/command prompt. 2. Type the following: **Windows/Linux/macOS**: ping <hostname or IP address> **2. Traceroute - Trace Path of Data** • **Objective**: Determine the route data packets take from your device to the destination. • **Steps**: 1. Open a terminal/command prompt. 2. Type the following: **Linux/macOS:** traceroute <hostname or IP address> **Windows:** tracert <hostname or IP address> **3. IPConfig/Ifconfig - Display Network Configuration** • **Objective**: Display the current network settings of your system. • **Steps**: 1. Open a terminal/command prompt. 2. Type the following:

- **Linux**:
  ifconfig
- **Mac:**
  ifconfig
- **Windows:**
  ipconfig

4. Nslookup – Query DNS Information

- **Objective**: Resolve domain names to IP addresses and vice versa.
- **Steps**:
  1. Open a terminal/command prompt.
  2. Type the following:
     - **Linux/macOS/Windows:**
       nslookup <hostname or domain>

5. Netstat – View Network Connections

- **Objective**: Display network connections and ports in use.
- **Steps**:
  1. Open a terminal/command prompt.
  2. Type the following:
     - **Linux/macOS/Windows**:
       netstat -a

6. ARP – View/Manage Address Resolution Protocol Table • **Objective**: View IP-to-MAC address mappings.

- **Steps**:
  1. Open a terminal/command prompt.

2. Type the following:
   - **Linux/macOS/Windows**:

     arp -a

7. Route - Display/Modify Routing Table

- **Objective: View or modify the IP routing table that governs data flow.**
- **Steps:**
  1. **Open a terminal/command prompt.**
  2. **To view the routing table, type the following:**
     - **Linux:** route -n
     - **MacOS:**

       netstat -rn
     - **Windows:**

       route print

	8. Tcpdump - Capture Network Traffic (Linux/macOS) • **Objective**: Capture and analyze network packets. • **Steps**: 1. Open a terminal. 2. Run the following command to start capturing network packets: **Linux/macOS:** sudo tcpdump **Windows** Use Wireshark or WinDump
Output Screenshots	

```
Pinging store.steampowered.com [96.6.33.28] with 32 bytes of data:
Reply from 96.6.33.28: bytes=32 time=6ms TTL=59
Reply from 96.6.33.28: bytes=32 time=6ms TTL=59
Reply from 96.6.33.28: bytes=32 time=6ms TTL=59
Reply from 96.6.33.28: bytes=32 time=6ms TTL=59

Ping statistics for 96.6.33.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

Fig 1- Pinging a website

```
Tracing route to store.steampowered.com [104.114.89.231]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1 [192.168.1.1]
  2    15 ms     2 ms     2 ms  110.226.15.255
  3     3 ms     3 ms     5 ms  125.20.27.9
  4    22 ms    23 ms    22 ms  182.79.141.70
  5    22 ms    22 ms    22 ms  a104-114-89-231.deploy.static.akamaitechnologies.com [104.114.89.231]

Trace complete.
```

Fig 2- Tracing a route to a website

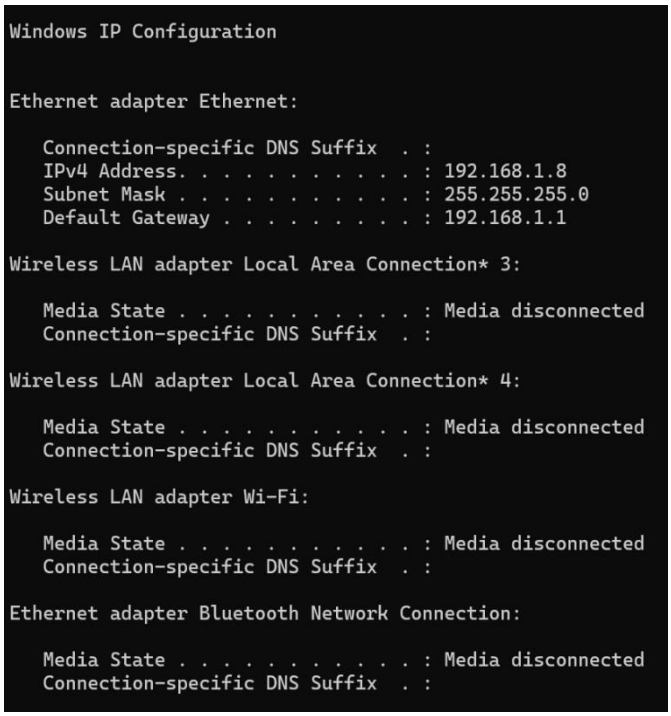

Fig 3- ipconfig of my Wi-Fi

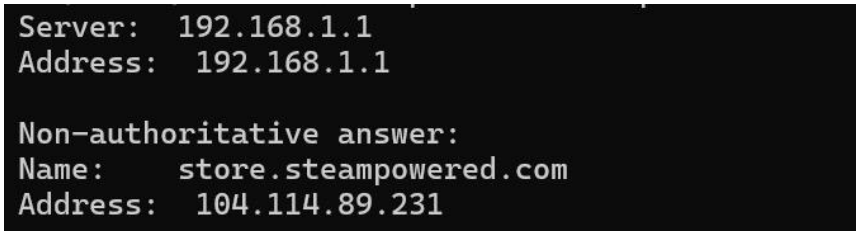

Fig 4- Finding DNS using nslookup

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            SAM:0                  LISTENING
  TCP    0.0.0.0:445            SAM:0                  LISTENING
  TCP    0.0.0.0:902            SAM:0                  LISTENING
  TCP    0.0.0.0:912            SAM:0                  LISTENING
  TCP    0.0.0.0:2869           SAM:0                  LISTENING
  TCP    0.0.0.0:4343           SAM:0                  LISTENING
  TCP    0.0.0.0:4449           SAM:0                  LISTENING
  TCP    0.0.0.0:5040           SAM:0                  LISTENING
  TCP    0.0.0.0:5141           SAM:0                  LISTENING
  TCP    0.0.0.0:6742           SAM:0                  LISTENING
  TCP    0.0.0.0:27036          SAM:0                  LISTENING
  TCP    0.0.0.0:49664          SAM:0                  LISTENING
  TCP    0.0.0.0:49665          SAM:0                  LISTENING
  TCP    0.0.0.0:49668          SAM:0                  LISTENING
  TCP    0.0.0.0:49669          SAM:0                  LISTENING
  TCP    0.0.0.0:49670          SAM:0                  LISTENING
  TCP    0.0.0.0:49759          SAM:0                  LISTENING
  TCP    0.0.0.0:54235          SAM:0                  LISTENING
  TCP    0.0.0.0:58995          SAM:0                  LISTENING
  TCP    127.0.0.1:1337         SAM:0                  LISTENING
  TCP    127.0.0.1:5141         checkhost:64988        ESTABLISHED
  TCP    127.0.0.1:5354         SAM:0                  LISTENING
  TCP    127.0.0.1:6742         checkhost:65014        ESTABLISHED
  TCP    127.0.0.1:9000         SAM:0                  LISTENING
  TCP    127.0.0.1:9001         SAM:0                  LISTENING
  TCP    127.0.0.1:9001         checkhost:62533        ESTABLISHED
  TCP    127.0.0.1:9002         SAM:0                  LISTENING
  TCP    127.0.0.1:9002         checkhost:62518        ESTABLISHED
  TCP    127.0.0.1:9002         checkhost:62532        ESTABLISHED
```

Fig 5- Finding active network connections using netstat

```
Interface: 192.168.1.8 --- 0x13
  Internet Address      Physical Address      Type
  192.168.1.1           e4-66-ab-2d-2e-6c     dynamic
  192.168.1.9           6c-f6-da-80-aa-f2     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Fig 6- Mapping IP's using arp command

```
Interface List
 19...40 c2 ba f9 48 d1 ......Killer E3100G 2.5 Gigabit Ethernet Controller
  5...6c f6 da 80 aa f3 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 11...6e f6 da 80 aa f2 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 17...6c f6 da 80 aa f2 ......Killer(R) Wi-Fi 6E AX1675i 160MHz Wireless Network Adapter (211NGW)
  6...6c f6 da 80 aa f6 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.8     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link       192.168.1.8    281
      192.168.1.8  255.255.255.255         On-link       192.168.1.8    281
    192.168.1.255  255.255.255.255         On-link       192.168.1.8    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       192.168.1.8    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       192.168.1.8    281
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  1    331 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

3384	87.282189	10.11.18.206	104.18.32.47	TCP	54 59123 → 443 [ACK] Seq=30643 Ack=688551 Win=514 Len=0
3385	87.303958	104.18.32.47	10.11.18.206	TCP	1514 443 → 59123 [ACK] Seq=688551 Ack=30643 Win=18 Len=1460 [TCP PDU reassembled in 3386]
3386	87.303958	104.18.32.47	10.11.18.206	TLSv1.2	1257 Application Data
3387	87.303986	10.11.18.206	104.18.32.47	TCP	54 59123 → 443 [ACK] Seq=30643 Ack=691214 Win=514 Len=0
3388	87.315163	fe80::14c8:9fd2:dbe…	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
3389	87.315765	10.11.18.161	224.0.0.251	MDNS	87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
3390	87.327423	104.18.32.47	10.11.18.206	TCP	1257 [TCP Spurious Retransmission] 443 → 59123 [PSH, ACK] Seq=690011 Ack=30643 Win=18 Len=
3391	87.327423	104.18.32.47	10.11.18.206	TCP	1514 443 → 59123 [ACK] Seq=691214 Ack=30643 Win=18 Len=1460 [TCP PDU reassembled in 3392]
3392	87.327423	104.18.32.47	10.11.18.206	TLSv1.2	1289 Application Data
3393	87.327446	10.11.18.206	104.18.32.47	TCP	66 [TCP Dup ACK 3387#1] 59123 → 443 [ACK] Seq=30643 Ack=691214 Win=514 Len=0 SLE=690011
3394	87.327480	10.11.18.206	104.18.32.47	TCP	54 59123 → 443 [ACK] Seq=30643 Ack=693909 Win=514 Len=0
3395	87.338396	10.11.16.52	224.0.0.251	MDNS	208 Standard query response 0x0000 PTR 20d6b6a83ff4dad7._spotify-connect._tcp.local SRV 0
3396	87.350101	fe80::e453:83ff:fe0…	ff02::fb	MDNS	107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
3397	87.352851	104.18.32.47	10.11.18.206	TCP	1514 443 → 59123 [ACK] Seq=693909 Ack=30643 Win=18 Len=1460 [TCP PDU reassembled in 3398]
3398	87.352851	104.18.32.47	10.11.18.206	TLSv1.2	1289 Application Data
3399	87.352870	10.11.18.206	104.18.32.47	TCP	54 59123 → 443 [ACK] Seq=30643 Ack=696604 Win=514 Len=0
3400	87.370056	104.18.32.47	10.11.18.206	TCP	1514 443 → 59123 [ACK] Seq=696604 Ack=30643 Win=18 Len=1460 [TCP PDU reassembled in 3401]
3401	87.370056	104.18.32.47	10.11.18.206	TLSv1.2	1289 Application Data
3402	87.370090	10.11.18.206	104.18.32.47	TCP	54 59123 → 443 [ACK] Seq=30643 Ack=699299 Win=514 Len=0
3403	87.392593	104.18.32.47	10.11.18.206	TCP	1514 443 → 59123 [ACK] Seq=699299 Ack=30643 Win=18 Len=1460

Fig 7- Routing table in Windows

Fig 8- tcpdump for Windows(Taken from Wireshark since there is no command for native windows)

Observation	**1. Ping – Testing Connectivity** • **Observations**: ○ **Response time**: Measures how long it takes for packets to travel to the destination and back. High response times indicate network latency. ○ **Packet loss**: Shows whether packets are being dropped along the path. Any packet loss suggests a problem with the network connection (e.g., poor link quality, misconfiguration, or congestion). ○ **Unreachable Host**: If the ping fails, it indicates that the target is either down or unreachable due to routing issues, firewall settings, or host unavailability. **2. Traceroute – Path Analysis** • **Observations**: ○ **Number of hops**: Displays the number of routers (hops) a packet passes through. A higher-than-expected number of hops can indicate suboptimal routing. ○ **Response times at each hop**: Helps identify where delays are occurring in the network. If a particular hop shows a high delay or failure to respond, it might indicate congestion, a network bottleneck, or an outage at that point. ○ **Path deviation**: The route should generally follow a known or expected path. If packets take unexpected

routes, it could indicate a routing issue or misconfiguration.

3. IPConfig/Ifconfig – Network Configuration

- **Observations**:
  - **IP Address**: Ensure that the device has the correct IP address assigned, either static or dynamically assigned by DHCP. An invalid or missing IP address could cause connectivity issues.
  - **Subnet mask and gateway**: Check if the subnet mask and default gateway are correct. A wrong subnet or

gateway can prevent the device from communicating outside its local network.

- **MAC address**: Displays the hardware address of the network interfaces, useful for identifying devices on the network.

4. Nslookup – DNS Resolution

- **Observations**:
  - **IP address resolution**: Nslookup should resolve the hostname into the correct IP address. If the resolution fails or returns the wrong IP, it indicates a DNS misconfiguration.
  - **DNS server response**: If the DNS server is unreachable or returns an error, it suggests an issue with the DNS server configuration, or the server may be down.
  - **Reverse lookup**: Using nslookup with an IP address should return the correct domain name if reverse DNS is configured correctly. If not, it could indicate a lack of reverse DNS records.

5. Netstat – Network Connection Status

- **Observations**:
  - **Active connections**: Lists all active network connections. This is useful for identifying which services or applications are using the network and their associated IP addresses and ports.

- **Listening ports**: Observing open or listening ports helps to ensure that necessary services are running. Unexpected open ports could indicate a security risk (e.g., an open port vulnerable to attack).
- **Foreign addresses**: Displays the IP addresses and ports of remote systems connected to your device. Unrecognized connections may indicate malicious activity or unauthorized access.

6. ARP – Address Mapping

- **Observations**:

- **IP-to-MAC mapping**: The ARP table shows how IP addresses are mapped to MAC addresses within the local network. A missing or incorrect ARP entry could explain communication failures between devices.
- **Suspicious entries**: Unexpected ARP entries (i.e., IP addresses or MAC addresses that don't belong to known devices) may indicate an ARP spoofing attack, where a malicious actor is impersonating another device on the network.

7. Route - Routing Table Inspection

- **Observations**:
  - **Default gateway**: Ensure that the default gateway is correctly configured. An incorrect or missing gateway could prevent access to other networks, including the internet.
  - **Routing paths**: Verify that routes to other networks (such as internal subnets) are present and accurate. Missing or wrong routes may cause traffic to be misrouted, resulting in unreachable networks.
  - **Metric**: The routing metric helps to determine the priority of a route. Lower metrics take precedence. Multiple routes to the same destination with different metrics could indicate load balancing or redundancy.

8. Tcpdump - Packet Capture and Analysis

- **Observations**:
    - **Packet details**: View the data flowing through the network in real time. Analyzing the source and destination of packets helps in diagnosing issues like communication errors, protocol misconfigurations, or unauthorized traffic.
    - **Traffic anomalies**: Unusual or excessive traffic from specific sources may indicate network misuse, a DDoS attack, or malware infection.
    - **Protocol analysis**: By examining specific protocol traffic

    (e.g., HTTP, DNS, TCP), you can pinpoint issues with

	specific services, such as web servers, DNS servers, or database applications. o **Dropped packets**: Observing dropped packets or retransmissions can highlight network instability, congestion, or hardware failures.
Self-assessment Q&A	NA
Conclusion	Networking programs like as ping, traceroute, ipconfig/ifconfig, nslookup, netstat, arp, route, and tcpdump can offer vital information on a network's structure, health, and performance. Users may use these tools to test connection, troubleshoot DNS problems, review routing tables, analyze network traffic, and identify security flaws. Regular use of these commands enables network managers and users to maintain peak network performance, swiftly discover and address problems, and assure network security. Anyone involved in network management or troubleshooting must have a solid understanding of these tools, which serve as the foundation for efficient network diagnostics and analysis.