Experiment No: 14	
Name	Vaibhav Sharma
PRN	22070126125
Date of Performance	16th October 2024
Title	To implement Network Troubleshooting using command line tools
Theory (short)	Networking commands are essential tools that allow users to interact with and diagnose network connections, resolve DNS issues, inspect routing tables, and capture data packets. These commands are universal in the sense that they can be used across different operating systems (Windows, macOS, Linux), though some minor variations in syntax may exist. Each of these commands serves a different function, but they all contribute to understanding the flow of data within a networked environment.
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

```
PS C:\Users\Sudhanshu> ping medium.com

Pinging medium.com [162.159.153.4] with 32 bytes of data:
Reply from 162.159.153.4: bytes=32 time=9ms TTL=58
Reply from 162.159.153.4: bytes=32 time=7ms TTL=59
Reply from 162.159.153.4: bytes=32 time=14ms TTL=57
Reply from 162.159.153.4: bytes=32 time=7ms TTL=59

Ping statistics for 162.159.153.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 14ms, Average = 9ms
```

Vaibhav Sharma

Fig 1- Pinging a website

```
PS C:\Users\Sudhanshu> tracert medium.com

Tracing route to medium.com [162.159.153.4]
over a maximum of 30 hops:

  1    22 ms     4 ms     2 ms  10.11.16.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    11 ms     9 ms    16 ms  162.159.153.4

Trace complete.
```

Vaibhav Sharma

Fig 2- Tracing a route to a website

```
PS C:\Users\Sudhanshu> ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : sitin.sitpune.edu.in
   Link-local IPv6 Address . . . . . : fe80::84e2:de03:9700:79ba%13
   IPv4 Address. . . . . . . . . . . : 10.11.18.206
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 10.11.16.1

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Vaibhav Sharma

Fig 3- ipconfig of my Wi-Fi

```
PS C:\Users\Sudhanshu> nslookup medium.com
Server:  SITDC.sitin.sitpune.edu.in
Address:  10.24.1.7

Non-authoritative answer:
Name:    medium.com
Addresses:  2606:4700:7::a29f:9804
          2606:4700:7::a29f:9904
          162.159.152.4
          162.159.153.4
```

Fig 4- Finding DNS using nslookup

```
PS C:\Users\Sudhanshu> netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Rhino:0                LISTENING
  TCP    0.0.0.0:445            Rhino:0                LISTENING
  TCP    0.0.0.0:5040           Rhino:0                LISTENING
  TCP    0.0.0.0:5357           Rhino:0                LISTENING
  TCP    0.0.0.0:6850           Rhino:0                LISTENING
  TCP    0.0.0.0:7680           Rhino:0                LISTENING
  TCP    0.0.0.0:9012           Rhino:0                LISTENING
  TCP    0.0.0.0:9013           Rhino:0                LISTENING
  TCP    0.0.0.0:9014           Rhino:0                LISTENING
  TCP    0.0.0.0:12177          Rhino:0                LISTENING
  TCP    0.0.0.0:27036          Rhino:0                LISTENING
  TCP    0.0.0.0:49664          Rhino:0                LISTENING
  TCP    0.0.0.0:49665          Rhino:0                LISTENING
  TCP    0.0.0.0:49668          Rhino:0                LISTENING
  TCP    0.0.0.0:49669          Rhino:0                LISTENING
  TCP    0.0.0.0:49676          Rhino:0                LISTENING
  TCP    0.0.0.0:49693          Rhino:0                LISTENING
  TCP    10.11.18.206:139       Rhino:0                LISTENING
  TCP    10.11.18.206:49424     20.198.119.143:https   ESTABLISHED
  TCP    10.11.18.206:57433     hkg12s09-in-f10:https  ESTABLISHED
  TCP    10.11.18.206:57446     155.133.225.20:https   ESTABLISHED
  TCP    10.11.18.206:58595     sm-in-f188:5228        ESTABLISHED
  TCP    10.11.18.206:58679     ec2-13-126-70-76:https  ESTABLISHED
  TCP    10.11.18.206:58716     bom07s32-in-f10:https  ESTABLISHED
  TCP    10.11.18.206:58718     bom07s32-in-f10:https  ESTABLISHED
  TCP    10.11.18.206:58726     ec2-13-126-70-76:https  ESTABLISHED
  TCP    10.11.18.206:58913     bom12s12-in-f14:https  TIME_WAIT
```

Vaibhav Sharma

Fig 5- Finding active network connections using netstat

```
PS C:\Users\Sudhanshu> arp -a

Interface: 10.11.18.206 --- 0xd
  Internet Address      Physical Address      Type
  10.11.16.1            c0-c5-20-83-b1-f2     dynamic
  10.11.16.199          94-08-53-3a-3a-71     dynamic
  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
  224.77.77.77          01-00-5e-4d-4d-4d     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Vaibhav Sharma

Fig 6- Mapping IP's using arp command

```
PS C:\Users\Sudhanshu> route print
===========================================================================
Interface List
  3...c8 5e a9 22 8c 9d ......Microsoft Wi-Fi Direct Virtual Adapter
 11...ca 5e a9 22 8c 9c ......Microsoft Wi-Fi Direct Virtual Adapter #2
 13...c8 5e a9 22 8c 9c ......Intel(R) Wi-Fi 6 AX201 160MHz
  6...08 bf b8 c5 8e 9b ......Realtek PCIe GbE Family Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.11.16.1     10.11.18.206     45
       10.11.16.0    255.255.248.0         On-link      10.11.18.206    301
     10.11.18.206  255.255.255.255         On-link      10.11.18.206    301
     10.11.23.255  255.255.255.255         On-link      10.11.18.206    301
        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
        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      10.11.18.206    301
  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      10.11.18.206    301
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 13    301 fe80::/64                On-link
 13    301 fe80::84e2:de03:9700:79ba/128
                                    On-link
  1    331 ff00::/8                 On-link
 13    301 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Fig 7- Routing table in Windows

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 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. ○ **Dropped packets**: Observing dropped packets or retransmissions can highlight network instability, congestion, or hardware failures.
Self-assessment Q&A	Q: What is the purpose of the ping command in network troubleshooting? Ans: ping checks the connectivity between your system and a remote host by sending ICMP Echo Requests and receiving Echo Replies. Q: How does the traceroute command help in identifying network issues? Ans: traceroute shows the path packets take to reach a destination, helping to identify where delays or failures occur in the network. Q: What does the ipconfig command display? Ans: ipconfig displays the IP configuration of a system, including IP addresses, subnet masks, and default gateways.
Conclusion	Networking commands like ping, traceroute, ipconfig/ifconfig, nslookup, netstat, arp, route, and tcpdump provide invaluable insights into the structure, health, and performance of a network. These tools enable users to test connectivity, resolve DNS issues, inspect routing tables, analyze network traffic, and detect security vulnerabilities. Regularly utilizing these commands allows network administrators and users alike to maintain optimal network performance, quickly identify and resolve problems, and ensure network security. Mastery of these tools is essential for anyone involved in managing or troubleshooting networks, forming the foundation for effective network diagnostics and analysis.