Name: Sushant Bagul

Roll No : 221070011

Batch-A

Experiment No. 3

Aim : Execution of basic networking commands in terminal.

Theory :

What Are Networking Commands?

Every system is connected to various networks and systems through internal or external network channels. These network configurations can sometimes encounter issues, impacting the system's performance. To resolve such network problems, 'networking commands' are used. These commands are designed to troubleshoot network issues with minimal complexity using the Windows Command Prompt tool.

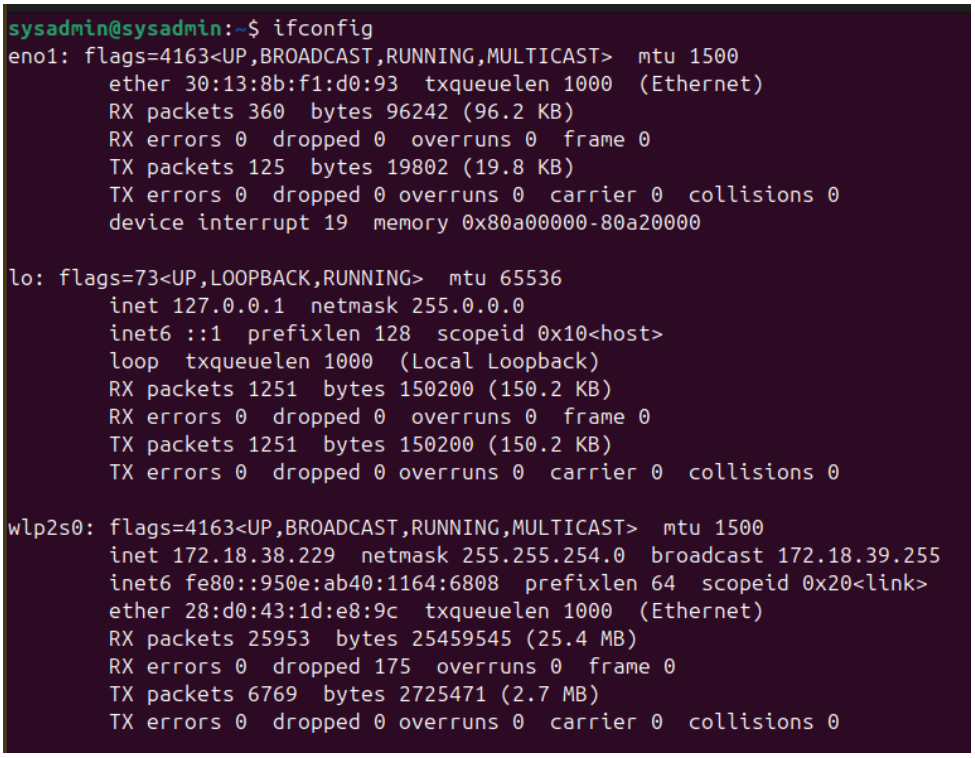
1. IPCONFIG

- When you enter ipconfig in the Command Prompt, it displays the current IP address, subnet mask, and default gateway for each network adapter on your system. This basic information is often enough to identify network configuration problems, such as incorrect IP addresses or subnet masks.
- The IPCONFIG network command offers a detailed overview of the IP address configuration for the device in use. It also provides variations of the primary command to target specific system settings or data, including:

ipconfig /all - Displays the primary output along with additional information about network adapters.

ipconfig /renew - Renews the system's IP address.

ipconfig /release - Releases the system's current IP address.



2. NSLOOKUP

- The NSLOOKUP command is a valuable tool for troubleshooting network connectivity issues, particularly those related to DNS (Domain Name System) resolution.
- By using the nslookup command, you can obtain detailed information about your system's DNS server, including the domain name and its corresponding IP address. This command is especially useful for diagnosing issues where a domain name fails to resolve to an IP address or when verifying the current DNS settings.
- Check for issues in DNS propagation, ensuring that changes to DNS records have been properly updated and disseminated across the network.
- Verify which DNS server your system is currently using, aiding in diagnosing network configuration issues.

```
sysadmin@sysadmin:~$ nslookup
> www.amazon.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.amazon.com  canonical name = tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com        canonical name = d3ag4hukkh62yn.cloudfront.net.
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 18.172.80.86
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:6600:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:e400:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:9e00:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:7a00:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:e800:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:1600:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:c600:7:49a5:5fd3:b641
Name:   d3ag4hukkh62yn.cloudfront.net
Address: 2600:9000:264c:600:7:49a5:5fd3:b641
>
```

3.HOSTNAME

The HOSTNAME command displays the hostname of the system. The hostname command is much easier to use than going into the system settings to search for it.

Command to enter in Prompt – hostname

```
sysadmin@sysadmin:~$ hostname
sysadmin
sysadmin@sysadmin:~$
```

4.PING

The Ping command is one of the most widely used commands in the prompt tool, as it allows the user to check the connectivity of our system to another host.

This command sends four experimental packets to the destination host to check whether it receives them successfully, if so, then, we can communicate with the destination host. But in case the packets have not been received, that means, no communication can be established with the destination host.
Command to enter in Prompt - ping www.destination_host_name.com

```
sysadmin@sysadmin:~$ ping www.youtube.com
PING youtube-ui.l.google.com (142.250.77.78) 56(84) bytes of data.
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=1 ttl=117 time=35.7 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=2 ttl=117 time=98.4 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=3 ttl=117 time=257 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=4 ttl=117 time=68.8 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=5 ttl=117 time=605 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=6 ttl=117 time=321 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=7 ttl=117 time=241 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=8 ttl=117 time=29.6 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=9 ttl=117 time=34.7 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=10 ttl=117 time=103 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=11 ttl=117 time=41.4 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=12 ttl=117 time=15.0 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=13 ttl=117 time=31.1 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=14 ttl=117 time=9.60 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=15 ttl=117 time=31.5 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=16 ttl=117 time=30.6 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=17 ttl=117 time=24.2 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=18 ttl=117 time=80.4 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=19 ttl=117 time=104 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=20 ttl=117 time=241 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=21 ttl=117 time=121 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=22 ttl=117 time=169 ms
64 bytes from bom07s27-in-f14.1e100.net (142.250.77.78): icmp_seq=23 ttl=117 time=38.7 ms
^C
--- youtube-ui.l.google.com ping statistics ---
23 packets transmitted, 23 received, 0% packet loss, time 22031ms
rtt min/avg/max/mdev = 9.596/118.709/605.478/135.577 ms
sysadmin@sysadmin:~$
```

```
sysadmin@sysadmin:~$ ping -c 5 www.vjti.ac.in
PING www.vjti.ac.in.cdn.hstgr.net (154.41.235.186) 56(84) bytes of data.
64 bytes from 154.41.235.186: icmp_seq=1 ttl=53 time=173 ms
64 bytes from 154.41.235.186: icmp_seq=2 ttl=53 time=42.5 ms
64 bytes from 154.41.235.186: icmp_seq=3 ttl=53 time=14.3 ms
64 bytes from 154.41.235.186: icmp_seq=4 ttl=53 time=37.8 ms
64 bytes from 154.41.235.186: icmp_seq=5 ttl=53 time=34.0 ms

--- www.vjti.ac.in.cdn.hstgr.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 14.260/60.350/173.179/57.227 ms
sysadmin@sysadmin:~$
```

5. TRACERT

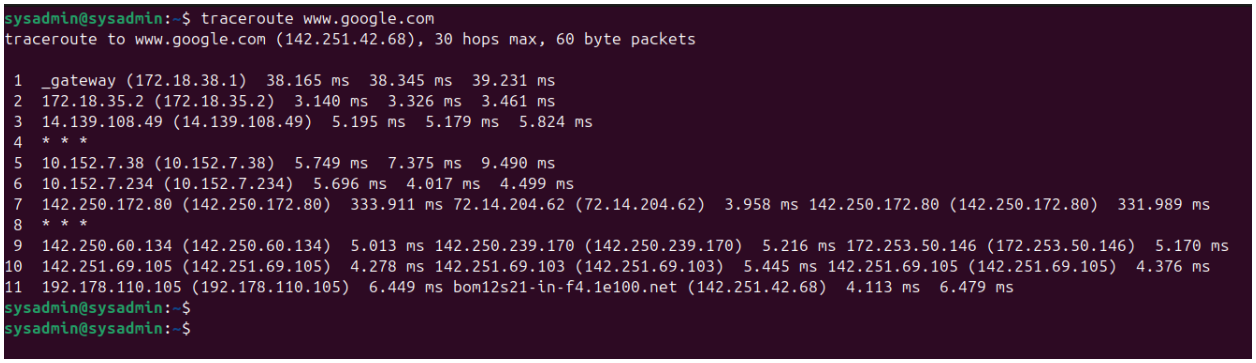
The TRACERT command is used to trace the route during the transmission of the data packet over to the destination host and also provides us with the “hop” count during transmission.

Using the number of hops and the hop IP address, we can troubleshoot network issues and identify the point of the problem during the transmission of the data packet.

Command to enter in Prompt- tracert IP-address

OR

tracert www.destination_host_name.com

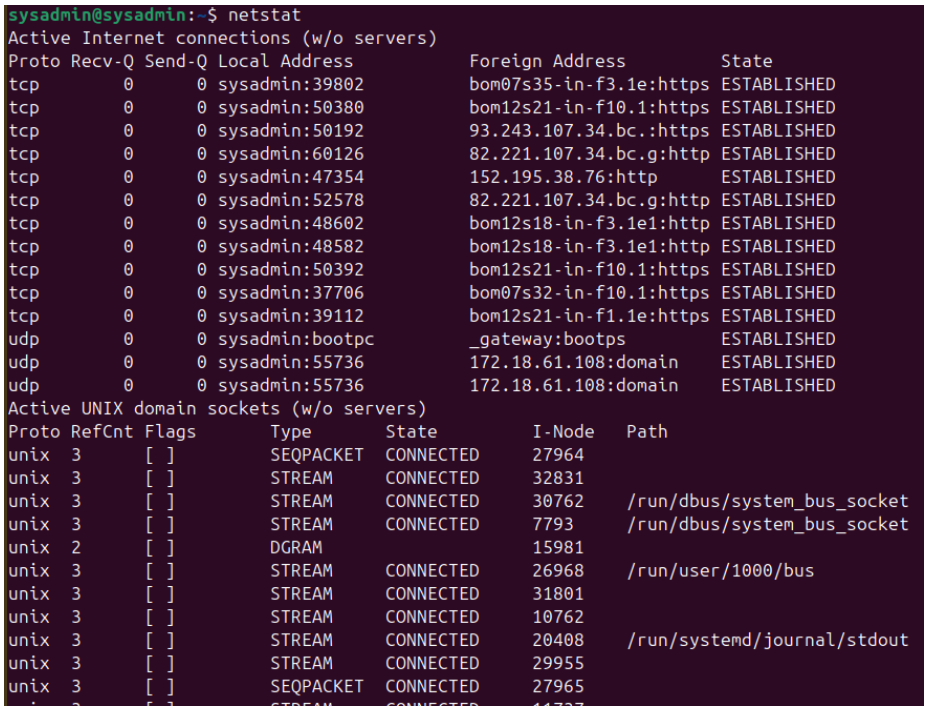


6. NETSTAT

The netstat command provides a comprehensive overview of all network connections on a device. It displays a detailed table that includes information about the connection protocol (such as TCP or UDP), local and foreign addresses, and the current state of each network connection (like ESTABLISHED, LISTENING, or TIME_WAIT). This information is crucial for monitoring network activity, diagnosing connectivity issues, and identifying potential security threats such as unauthorized connections or unusual traffic patterns.

Beyond basic connection information, netstat offers various options to display more specific data. For example, netstat -a lists all active connections and listening ports, netstat -n shows addresses and port numbers in numerical form, and netstat -o includes the Process ID (PID) of each connection, allowing users to trace connections back to specific applications. Using these

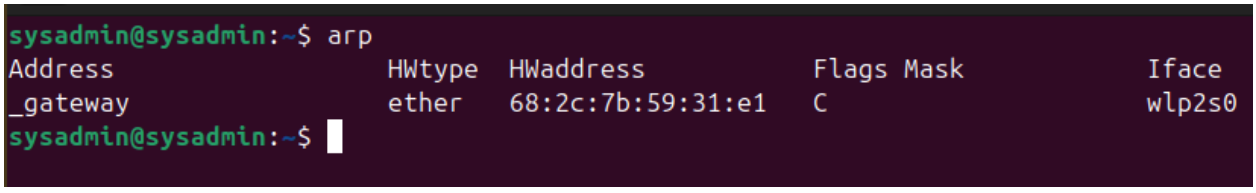
options, administrators and users can gain insight into the system's network behavior, troubleshoot network-related problems, and ensure that no unauthorized services are running.



7. ARP(Address Resolution Protocol)

The ARP command is used to access the mapping structure of IP addresses to the MAC address. This provides us with a better understanding of the transmission of packets in the network channel.

Command to enter in Prompt - **arp**



8. SYSTEMINFO

Using the SYSTEMINFO command, we can access the system's hardware and software details, such as processor data, booting data, Windows version, etc. Command to enter in Prompt - systeminfo

Conclusion

In this article on 'Networking Commands', we understood the need of using network commands and the way to implement them in the Windows command prompt. We also learned about the different network commands to troubleshoot and configure.