

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.

```
sysadmin@sysadmin:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 30:13:8b:f1:d0:93 txqueuelen 1000 (Ethernet)
    RX packets 360 bytes 96242 (96.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 125 bytes 19802 (19.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 memory 0x80a00000-80a20000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1251 bytes 150200 (150.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1251 bytes 150200 (150.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.18.38.229 netmask 255.255.254.0 broadcast 172.18.39.255
    inet6 fe80::950e:ab40:1164:6808 prefixlen 64 scopeid 0x20<link>
    ether 28:d0:43:1d:e8:9c txqueuelen 1000 (Ethernet)
    RX packets 25953 bytes 25459545 (25.4 MB)
    RX errors 0 dropped 175 overruns 0 frame 0
    TX packets 6769 bytes 2725471 (2.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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`

```
sysadmin@sysadmin:~$ traceroute www.google.com
traceroute to www.google.com (142.251.42.68), 30 hops max, 60 byte packets
 1  _gateway (172.18.38.1)  38.165 ms  38.345 ms  39.231 ms
 2  172.18.35.2 (172.18.35.2)  3.140 ms  3.326 ms  3.461 ms
 3  14.139.108.49 (14.139.108.49)  5.195 ms  5.179 ms  5.824 ms
 4  * * *
 5  10.152.7.38 (10.152.7.38)  5.749 ms  7.375 ms  9.490 ms
 6  10.152.7.234 (10.152.7.234)  5.696 ms  4.017 ms  4.499 ms
 7  142.250.172.80 (142.250.172.80)  333.911 ms  72.14.204.62 (72.14.204.62)  3.958 ms  142.250.172.80 (142.250.172.80)  331.989 ms
 8  * * *
 9  142.250.60.134 (142.250.60.134)  5.013 ms  142.250.239.170 (142.250.239.170)  5.216 ms  172.253.50.146 (172.253.50.146)  5.170 ms
10  142.251.69.105 (142.251.69.105)  4.278 ms  142.251.69.103 (142.251.69.103)  5.445 ms  142.251.69.105 (142.251.69.105)  4.376 ms
11  192.178.110.105 (192.178.110.105)  6.449 ms  bom12s21-in-f4.1e100.net (142.251.42.68)  4.113 ms  6.479 ms
sysadmin@sysadmin:~$
sysadmin@sysadmin:~$
```

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.

```
sysadmin@sysadmin:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 sysadmin:39802         bom07s35-in-f3.1e:https ESTABLISHED
tcp        0      0 sysadmin:50380         bom12s21-in-f10.1:https ESTABLISHED
tcp        0      0 sysadmin:50192         93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 sysadmin:60126         82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 sysadmin:47354         152.195.38.76:http      ESTABLISHED
tcp        0      0 sysadmin:52578         82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 sysadmin:48602         bom12s18-in-f3.1e1:http ESTABLISHED
tcp        0      0 sysadmin:48582         bom12s18-in-f3.1e1:http ESTABLISHED
tcp        0      0 sysadmin:50392         bom12s21-in-f10.1:https ESTABLISHED
tcp        0      0 sysadmin:37706         bom07s32-in-f10.1:https ESTABLISHED
tcp        0      0 sysadmin:39112         bom12s21-in-f1.1e:https ESTABLISHED
udp        0      0 sysadmin:bootpc        _gateway:bootps        ESTABLISHED
udp        0      0 sysadmin:55736         172.18.61.108:domain   ESTABLISHED
udp        0      0 sysadmin:55736         172.18.61.108:domain   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State       I-Node  Path
unix   3      [ ]     SEQPACKET  CONNECTED   27964    /run/dbus/system_bus_socket
unix   3      [ ]     STREAM     CONNECTED   32831    /run/dbus/system_bus_socket
unix   3      [ ]     STREAM     CONNECTED   30762    /run/dbus/system_bus_socket
unix   3      [ ]     STREAM     CONNECTED   7793     /run/dbus/system_bus_socket
unix   2      [ ]     DGRAM      CONNECTED   15981    /run/user/1000/bus
unix   3      [ ]     STREAM     CONNECTED   26968    /run/user/1000/bus
unix   3      [ ]     STREAM     CONNECTED   31801    /run/user/1000/bus
unix   3      [ ]     STREAM     CONNECTED   10762    /run/user/1000/bus
unix   3      [ ]     STREAM     CONNECTED   20408    /run/systemd/journal/stdout
unix   3      [ ]     STREAM     CONNECTED   29955    /run/systemd/journal/stdout
unix   3      [ ]     STREAM     CONNECTED   27965    /run/systemd/journal/stdout
unix   3      [ ]     SEQPACKET  CONNECTED   27965    /run/systemd/journal/stdout
```

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**

```
sysadmin@sysadmin:~$ arp
Address HWtype HWAddress      Flags Mask Iface
_gateway ether 68:2c:7b:59:31:e1 C wlp2s0
sysadmin@sysadmin:~$
```

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

```
sysadmin@sysadmin:~$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:          46 bits physical, 48 bits virtual
Byte Order:             Little Endian
CPU(s):                 20
On-line CPU(s) list:    0-19
Vendor ID:              GenuineIntel
Model name:             13th Gen Intel(R) Core(TM) i5-13500T
CPU family:             6
Model:                  191
Thread(s) per core:     2
Core(s) per socket:     14
Socket(s):              1
Stepping:               2
CPU(s) scaling MHz:     23%
CPU max MHz:            4600.0000
CPU min MHz:            800.0000
BogoMIPS:               3225.60
Flags:                  fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm constant_
tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc cpuid aperfperf tsc_known_freq pni pclmulqdq dtes64 monitor ds_cpl vnx smx est tm2 ssse3 sc
bg fma cx16 xtpr pcdm sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault epb ssbd ibrs lbrpb
stibp lbrs_enhanced tpr_shadow flexpriority ept vpid ept_ad fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid rdseed adx smap clflushopt clwb intel_pt sha
ni xsaveopt xsavec xgetbv1 xsaves split_lock_detect user_shstk avx_vnni dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_epp hwp_pkg_req hfi vnmi umi
p pku ospke waitpkg gfni vaes vpclmulqdq tme rdpid movdiri movdir64b fsrm md_clear serialize pconfig arch_lbr lbrt flush_l1d arch_capabilities

Virtualization features:
Virtualization:         VT-x
Caches (sum of all):
  L1d:                   544 KiB (14 instances)
  L1i:                   784 KiB (14 instances)
  L2:                    11.5 MiB (8 instances)
  L3:                    24 MiB (1 instance)
NUMA:
NUMA node(s):           1
NUMA node0 CPU(s):      0-19
Vulnerabilities:
Gather data sampling:    Not affected
Itlb multihit:          Not affected
L1tf:                   Not affected
Mds:                    Not affected
Meltdown:               Not affected
Mmio stale data:        Not affected
Reg File data sampling:  Mitigation; Clear Register File
Retbleed:               Not affected
Spec rstack overflow:    Not affected
Spec store bypass:      Mitigation; Speculative Store Bypass disabled via prctl
Spectre v1:             Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Spectre v2:             Mitigation; Enhanced / Automatic IBRS; IBPB conditional; RSB filling; PBSRB-eIBRS SW sequence; BHI BHI_DIS_S
Srbds:                  Not affected
Tsx async abort:        Not affected
sysadmin@sysadmin:~$
```

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.