COLLEGE REPORT

Topic: IP Command Documentation

Submitted By: Aarit Haldar
USN: ENG24CY0073
Department of CYBER SECURITY

1. Introduction to the IP Command

The 'ip' command is a powerful network configuration tool included in the iproute2 package. It was developed as a modern replacement for older utilities such as ifconfig, route, arp, and netstat. The command allows administrators to configure IP addresses, manage network interfaces, control routing, and monitor network activity.

History and Authors

The iproute2 suite, which includes the 'ip' command, was primarily developed by Alexey Kuznetsov and other Linux kernel networking developers. It was introduced in the early 2000s to support advanced networking features like IPv6, traffic shaping, and policy-based routing.

2. Importance of the IP Command for System Administrators

System administrators depend on the 'ip' command because it provides extensive and detailed control over the system's networking components. It supports modern networking protocols and provides real-time configuration and monitoring capabilities. Compared to legacy tools, it is more accurate, flexible, and feature-rich.

3. How the IP Command Works (with Examples)

Show all network interfaces:

Command:
ip a

Bring interface up:

Command:
sudo ip link set eth0 up

Add IP address:

Command:
sudo ip addr add 192.168.1.10/24 dev eth0

Delete IP address:

Command:
sudo ip addr del 192.168.1.10/24 dev eth0

Show routing table:

Command:
ip route show

Show ARP/Neighbor table:

Command:

ip neigh show

4. SNAPSHOTS

•

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP
    inet 192.168.1.5/24 brd 192.168.1.255 scope global eth0
```

•

```
sudo ip link set eth0 down
```

•

```
sudo ip addr add 192.168.1.20/24 dev eth0
```

•

```
$ ip route
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.5
```

•

```
$ ip neigh
192.168.1.1 dev eth0 lladdr a4:5e:60:3a:b2:1c REACHABLE
```

5. Options and Flags of the IP Command

ip addr: Displays or manages IP addresses.

ip link: Manages network interfaces.

ip route: Shows or configures routing tables.

ip neigh: Manages ARP/NDP entries.

ip -s: Displays statistics (packet count, errors).

ip monitor: Monitors changes in interfaces, addresses, or routes.

ip -br: Provides brief, clean interface output.

2nd question

tshark – CLI version of Wireshark

tshark – Command Line Version of Wireshark

1. Introduction to tshark (History, Invention and Authors)

tshark is the command-line version of Wireshark, a network protocol analyzer. It was originally released as Ethereal in 1998 by Gerald Combs. Due to trademark issues, it was renamed Wireshark in 2006 and tshark was introduced as its CLI variant. It is maintained by the Wireshark Development Community.

2. Importance of tshark for System Administrators

- Lightweight and fast.
- Works without GUI, suitable for remote SSH servers.
- Can be automated using scripts.
- Useful for real-time traffic monitoring.
- Essential in cybersecurity investigations and network forensics.

3. Working of tshark (with Examples)

Example Commands:

tshark -i eth0

tshark -i eth0 -c 20

tshark -i eth0 -w output.pcap

tshark -r output.pcap

tshark -i eth0 -f "tcp port 80"

tshark -T fields -e ip.src -e ip.dst

4. Snapshots of tshark Execution

```
$ tshark -D
1. eth0
2. wlan0
3. any
```

```
$ tshark -i eth0
Capturing on 'eth0'
1   0.001231   192.168.1.10 → 192.168.1.1   DNS   Standard query A google.com
2   0.020459   192.168.1.1  → 192.168.1.10  DNS   Standard query response A 142.250.182.110
```

```
$ tshark -i eth0 -w capture.pcap
Capturing... Press Ctrl+C to stop
```

```
$ tshark -r capture.pcap
```

5. Important Options and Flags

- -i <interface> : selects interface

- -c <count> : capture packet count

- -f <filter> : add capture filter

- -w <file> : write to pcap file

- -r <file> : read pcap file

- -T fields : extract specific fields

- -Y <filter> : apply display filter

- -V : detailed verbose output