17/7/2025

Practical-I

Windows Commands

arp -a

Interface: 192.168.1.126 --- 0xf

Internet Address	Physical Address	Type
192.168.1.1	c0-eb-d8-cb-9a-5d	dynamic
192.168.1.66	c0-35-32-24-f5-a7	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static

hostname

LAPTOP-MMLRRFI8

nbtstat -a

Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP)

NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n]
[-r] [-R] [-RR] [-s] [-S] [interval]]

ipconfig/all

Windows IP Configuration
- Host Name
- Primary DNS Suffix
- Node Type
- ⋮

Wireless LAN adapter Wi-Fi 2:
- Media State
- Description
- Physical Address
- ⋮

Wireless LAN adapter Wi-Fi 4:

Media State
Description
Physical address
!

Wireless LAN adapter Wi-Fi:

Description
Physical Address
DHCP Enabled
!

Ethernet adapter Bluetooth Network Connection:

Media State
Description
Physical Address
!

netstat

Active Connections

Proto	Local Address	Foreign Address	State
Tcp	127.0.0.1:49679	LAPTOP-MMLRRFI8:49680	ESTABLISHED
Tcp	127.0.0.1:49680	LAPTOP-MMLRRFI8:49679	ESTABLISHED
Tcp	192.168.1.126:53492	a104-86-188-120:https	CLOSE_WAIT

!

nslookup

Default Server: Unknown

Address: 192.168.1.1

pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
[-p period] [-q num_queries] [-w timeout]
[-4] [-6] target_name

pathping google.com

Tracing route to google.com [142.251.222.206]
over a maximum of 30 hops:
0 LAPTOP-MMLRRFI8 [192.168.1.126]
1 192.168.1.1
2 * 10.209.0.1
3 * * *

ping

ping twitter.com

Pinging twitter.com [162.159.140.229] with 32 bytes of data:
Reply from 162.159.140.229: bytes=32 time=4ms TTL=58
!
Ping statistics for 162.159.140.229:
Packets: Sent=4, Received=4, Lost=0 (0% loss)

route

Manipulates network routing tables

ROUTE [-f] [-p] [-4|-6] command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

Linux commands

ip

ip address show

1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

2: enp0s31f6: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000

3: wlp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000

Sudo ip address add 192.168.1.254/24 dev wlp2s0
ip addr show dev wlp2s0

3: wlp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc no queue state UP group default qlen 1000

inet 192.168.1.254/24 scope global wlp2s0
valid_lft forever preferred_lft forever

Sudo ip address del 192.168.1.254/24 dev wlp2s0
ip addr show dev wlp2s0

3: wlp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc no queue state UP group default qlen 1000

Sudo ip link set wlp2s0 up
ip addr show dev wlp2s0

3: wlp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc noqueue state UP group default

Sudo ip link set wlp2s0 down

3: wlp2s0: <BROADCAST, MULTICAST> mtu 1500 qdisc noqueue state DOWN group default qlen 1000

Sudo ip link set wlp2s0 promisc on

3: wlp2s0: <BROADCAST, MULTICAST, PROMISC, UP, LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000

Sudo ip route add default via 192.168.1.254 dev wlp2s0

ip route show

default via 172.16.75.130 dev wlp2s0

default via 172.16.72.1 dev wlp2s0 proto static metric 600

192.168.1.0/24 dev wlp2s0 proto kernel scope link src 192.168.1.254

Sudo ip route add 192.168.1.0/24 via 192.168.1.254

RTNETLINK answers: File exists

Sudo ip route add 192.168.1.0/24 dev wlp2s0

ip route show

default via 172.16.72.1 dev wlp2s0 proto static metric 600

192.168.1.0/24 dev wlp2s0 scope link

ip route get 10.10.1.4

10.10.1.4 via 172.16.72.1 dev wlp2s0 src 172.16.75.130 uid 1000 cache

ifconfig: Command used to view or configure network interfaces. Shows details like IP address, MAC address and interface status.

enp0s31f6: flags=4099<UP, BROADCAST, MULTICAST> mtu 1500

lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536

wlp2s0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500

mtr : A network diagnostic tool that combines the functions of ping and traceroute, showing the path and performance of packets.

mtr google.com

My traceroute [v0.95]

Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. _gateway	0.0%	4	6.1	9.2	2.5	16.1	6.1
2. 142.250.171.162	0.0%	4	11.5	103.3	4.8	391.5	192.2

tcpdump : Packet analyzer used to capture and display network traffic going through the system's interfaces.

tcpdump -D: Lists all available network interfaces on the system

1. wlp2s0 [Up, Running, Wireless, Associated]

2. any

⋮

11. nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]

tcpdump -i wlp2s0 : Starts capturing packets from mentioned interface.

tcpdump -i wlp2s0 -c2 : Captures 2 packets from given interface.

dropped privs to tcpdump

tcpdump: verbose output suppressed

Listening on wlp2s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

01:46:09.840280 IP ntp6.nuum-in.hosts.301-moved.de.ntp

01:46:09.915248 IP fedora.32956 > gateway.domain: 21489+ PTR?

2 packets captured

Capture traffic to and from one host

```
sudo tcpdump -i wlp2s0 -c 2 host 8.8.8.8
dropped privs to tcpdump
tcpdump: verbose output suppressed
listening on wlp2s0,
23:13:40.803057 IP fedora > dns.google: ICMP echo request
23:13:41.046899 IP dns.google > fedora: ICMP echo reply
```

Traffic coming from 8.8.8.8

```
sudo tcpdump -i wlp2s0 src host 8.8.8.8
dropped privs to tcpdump
tcpdump: verbose output suppressed
listening on wlp2s0
23:21:22.453708 IP dns.google > fedora: ICMP echo reply
```

Traffic going to 8.8.8.8

```
sudo tcpdump -i wlp2s0 dst host 8.8.8.8
23.22.26.409233 IP fedora > dns.google: ICMP echo request
```

Capture traffic to and from a network

```
sudo tcpdump -i wlp2s0 net 10.1.0.0 mask 255.255.255.0
tcpdump: verbose output suppressed
listening on wlp2s0,
11:21:23.696721 IP 172.25.141.91 > 10.1.0.0: ICMP echo request
```

```
tcpdump -i eth0 port 53
```

ping : A tool that sends ICMP echo requests to a host to check if its reachable and measure response time.

```
ping google.com
PING google.com (142.251.222.206) 56(84) bytes of data.
64 bytes from hkg07s55-in-f14.1e100.net (142.251.222.206): icmp-seq=1
```

1. Which command is used find the reachability of a host machine from your device?
   ping

2. Which command will give the details of hops taken by a packet to reach its destination.
   traceroute

3. Which command displays the TCP port status in your machine?
   netstat

4. Which command displays the ip config of machine?
   ipconfig

5. Write the modify ip configuration in a linux machine?
   Use ip address add or ip route add

Result:

The windows and linux commands were executed successfully.

31/8/23