19/07/2024 Practical - 1

BASIC NETWORKING COMMANDS USED IN WINDOWS

arp -a :-

ARP is shortform of address resolution protocol, it will show the IP address of your computer along with the IP address and MAC address of your router.

hostname :-

This is the simplest of all TCP/IP commands. It simply displays the name of your computer

ipconfig /all :-

This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP and type of Ethernet adapter in your system.

nbtstat -a :-

This command helps solve problems with NetBIOS name resolution.

netstat :-

Netstat displays a variety of statistics about a computers active TCP/IP connections.

It is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc..

nslookup :-

It is a tool used to perform DNS lookups in Linux. It is used to display DNS details such as IP address of a particular computer, the MX records for a domain or NS servers of a domain, nslookup can operate in two modes:

- Interactive
- Non-interactive

Pathping :-

Pathping is unique to Windows and is basically a combination of the Ping and Tracert commands.

It traces route to destination address, Launches 25 second test gathers statistics on rate of data loss at each hop.

Ping :-

(Packet Internet Groper)

It is used to test connectivity between two nodes. Ping use ICMP (Internet Control message Protocol) to communicate other devices.

ping hostname
ping ip address
ping fully qualified domain name

Route :-

It is a command used to show the routing table It is primarily used to setup static routes to specific host or networks via an interface

ip command:

ip address show:

It show the IP address assigned to an interface on your server.

Output:

1. lo <LOOPBACK, UP, LOWER_UP>
Inet 127.0.0.1/8 scope host lo.
2. enp2s0: <BROADCAST, MULTICAST, LOOPBACK>
Inet 172.16.8.118/22 brd 172.16.11.255
3. wlp3s0: <BROADCAST, MULTICAST, LOWER_UP>
Inet 172.16.11.83/22 brd 172.16.11.255 scope

ip address add 192.168.1.254/24 dev enp2s0:

To assign IP to an interface

ip address del 192.168.1.254/24 dev enp2s0:

To delete IP to an interface.

ip link set eth0 up

After the Interface status by bringing eth0 Online

ip link set eth0 down

After the Interface status by bringing eth0 down

ip route add 192.168.1.0/24 via 192.168.1.254

To add a route via the gateway at 192.168.1.254

ip route add 192.168.1.0/24 dev eth0

To add a route 192.168.1.0/24 that can be reached on device eth0.

ip route get 10.10.1.4

Outputs: 10.10.1.4 via 172.16.8.1 dev enp2s0
src 172.16.8.118 uid 0 cache

mtr command:

mtr google.com:

It shows the statistics, including each hop with time and loss %.

Output:

Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 172.16.8.1	0.0%	5	0.2	0.2	0.1	0.2	[illegible]
2. static 41.229.49	0.0%	5	3.4	[illegible]	0.1	0.4	[illegible]
3. 142.251.227.127							

mtr -n google.com:

It shows the numeric ip address instead of hostnames

Output:

ip localhost.localdomain (0.0.0.0)

Host ip address:

1. 172.16.8.1
2. 142.250.171.162
3. 142.251.227.217

mtr -c 10 google.com:

It sets the number of pings that you want to send.

tcpdump -D

Before starting any capture, you need to know which interfaces tcpdump can use. You will need "sudo" or have root access.

Output:

1. enp2s0 [Up, Running]
2. wlp3s0 [Up, Running]
3. any (Pseudo-device that captures on all interfaces)
4. lo [Up, Running]

nmcli connection show "New 802-3-ethernet connection" connection.autoconnect yes.

connection.id: New 802-3-ethernet connection
connection.autoconnect: yes
connection.slaves: --
connection.autoconnect-slaves: -1

nmcli connection show "New 802-3-ethernet connection" connection.interface-name: enp2s0.

Connection.id: New 802-3-ethernet connection
connection.uuid: 85ff109f-3f0e-42d5-904e.
connection.interface-name: enp1s0.
connection.readonly: no.

nmcli connection add con-name "New 802-3-ethernet connection" ifname enp2s0 type ethernet.
Connection 'New 802-3-Ethernet connection" successfully added.