21/7/21

EXP: 1 Study of various commands used for networking

Aim: Study of various networks used in linux and windows.

Basic networking commands:-

1, arp -a :- ARP is short form for address resolution protocal, it will show the IP address of your computer along with the IP address and mac address of your router.

$arp -a

- gateway (172.16.72.1) at 7C:5A:1C:CF:f
[ether] on wlp20 41

2. hostname :- simplest of all TCP/IP commands

$ hostname.

fedora.

3. ipconfig/all :- display detailed config inp about your TCP/IP connection inel router gateway, DNS, DHCP and type of ethernet adapter in your system.

$ ip a.

1. lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc

2. wps20: <BROADCAST, MULTICAST, UP, LOWER_UP>

4. nbstat -a :- command help solve problem with NETBIOS name resolution.

$ nmblookup fedora - Linux.

192.168.1.105 fedora - Linux. <00>

5. netstat - net stat display a variety of statistics about a computer active TCP / adp connections. It is a command line tool.

$ netstat

Active internet connections (w/o servers)

proto recv - q send - q local address

proto recv - q send q local address

tcp	0	0	fedora: 47148
tcp	0	0	fedora: 40456.

foreign address state.

191.144.160.34 : bc : https established.

servers - 108 - 159 - 10 : https time-wait

6. Lookup :- It is a tool used to perform DNS lookups in Linux

$ nslookup www.google.com

Server : 192.168.11

address : 192.168.1.1

non - authoritative answer:
name : www.google.com
address: 142.250.192.68

4. pathping :- pathping is unique to windows and is basically a combination of the ping and tracert commands.

$ nttr www.google.com
my traceroute [v0.94]
hostname (192.168.1.105) → www.google.com (142.250.192.68)

Keys : help display mode hostname statistics
order of fields quit

Host	loss%	snt	last	avg	best	wrst	stdev
1. 192.168.1.1	0.0%	10	0.2	0.7	0.6	0.9	0.1
2. 10.200.0.1	0.0%	10	5.2	4.9	4.6	5.3	0.2
3. 142-6-192-168	0.0%	10	2.5	19.9	19.5	20.5	0.3

5. ping - packet internet group command is the best way to test connectivity between two nodes. ping means to communication to other devices.

$ Ping 8.8.8.8
Ping 8.8.8.8 (8.8.8.8) 56 (84) bytes of data
64 bytes from 8.8.8.8 : icmp-seq=1 ttl=
115 time=12.3 ms

9. route print - route command is used to show or manipulate the IP routing table.

usage: route [-nrow] [-f-c] [<AFI>]
list kernel routing tables.

route {-V} --version} display version/ author and exit.

-v, --verbose be verbose.

-n, --numeric don't resolve names

-e, --extend display other / more info.

-c, --cache instead of FIB.

Linux networking commands:-

1. Show IP address:-
   $ ip address show
   wlp2s0...
   inet 172.16.75.17/21...
   inet6 2725:6845:abab:af65/64

2. Add an IP address
   $ sudo ip address add 192_168.1.254/24 dev wlp2s0
   RTNETLINK answer: File exists.

3. Relete an IP.
   $ sudo ip address add 192_168.1.254/24 dev wlp2s0

4. Bring interface IP:-
   $ sudo ip link set wlp2s0 ip

5. Bring interface down
   $ sudo iplink set wlp2s0 down

6. Enable promisous mode
   $ sudo iplink set wlp2s0 promisoas

7. Add default rate.
   $ sudo ipaddress add 192.168.1.254/dev wlp2s0
   $ sudo ip_route add default via 192.168.1.. dev wlp2s0.20

8, Add a route to 192.168.1.0/24 via gateway 192.168.1.254.

$ sudo ip route add 192.168.1.0/24 via 192.168.1.254

9. Add a route to 192.108.1.0/24 reachable device wlsp2s0.

$ sudo ip route add 192.168.1.0/24 dev wlp8s0.

10. Delete route for 19.2.168.1.0/24 via gateway 192.168.1.254.

$ sudo ip route delete 192.168.1.0/24 via 192.168.1.254.

11. Display route taken to IP 10.10.1.4.

$ ip route get 10.10.1.4.

10.10.1.4 via 172.16.72.1 dev wlp8s0 src 172.16.75:
uid 1000 cache.

12. ip config.

$ ip config

wlp2s0: flags: 163<up. BRODCAST, Running MULLTCAST> mto.0500

inet 172.16.76.17 network 255.255.248< broadcast 172.16.79.255

Cither 4c:82:a9:77:1f:19 t. yuhuon 1000 (ethernet)

RX packet 126870 bytes 70.4 min dropped 42

TX packet 245 36 bytes 11.3 m's

88

13. mtr google.com

packets.

Host Loss cnt Lost Avg Best wost

1. IN 115.245.95.4 0.0% 30 23.8 10.3 2.6 12.250.

2. VS 72.14.217.252 0.0% 3.1 6.5 15.5 3.9 36.588.3

14. mtr -b google.com

packets

172.16.12.122 (172.16.12.122) Loss%

172.16.12.122 (172.16.12.122) 0.0% cnt Lost Avg Best wost

8 3 6.2 14.8 8.2 24

0.0% 84 6.4 82.55 24.

15. mtr -c 10 google.com

115.245.95.249 Loss% cnt Lost Avg best wost stdev.

0.0% 8 23.1 57.6 2.3 30.0 11.3

0.0% 8 15.5 65.75 36 48.9.3

16. capture traffic on your wifi interface wlp2s0

$ sudo tcpdump -i wlp2s0

Listing on wlp2s0

01:47.0758 172.16.75.140 > 230.0.0.4

length 0

01:47.077 IP fedora-gateway PTR query

: A

34 packets captured.

732 packet received by filter

17. capture only 10 packets

sudo Tcpdump -i wlp2s0 -c 10

dropped print to tcpdump

Listening on wlp2s0, link type EN10MB

Snapshot length 262144 bytes

23:23:41 IP fedora 37160 > gateway domain PTR! ip6 arr

8 10 packet captured.
244 packet received by filter.
179 packet dropped by kernal.

18. To capture all port except port 80 and 25

$ sudo tcpdump -i wlp2s0 not port 53 and not port 25

23:36:487 fedora 44750 > 12.18100 net-http: udp length 2000

23.36: IP fedora 869776 > 10 conn.ell.mr.20p SYN, length...

⋮

144 packet captured.
2776 packet Received by filter.
2525 packet dropped by kernal.

19. Captured only DNS port 53 Traffic.

sudo tcpdump -i wlp2s0 port 53

23:38:32 fedora > gateway domain AAAA: ab.chatgpt.com

23:35:32 gateway domain > fedora. AAAA reply (2 records)

146 packet captured.
146 packet received by filter.
0 packet dropped by kernel.

20. For traffic comming from 8.8.8.8 me.

sudo tcpdump -i wlp2s0 -c host 8.8.8.8
dropped privon to tcpdump.
tcpdump: verbose output suppressed-
for full protocol decode
listening on wlp2s0, link type EN10MB
(Ethernet)
snapshot length 262144 bytes.
0 packets captured.
0 packets received by filter.
0 packets dropped by kernel.

21- To capture HTTPS Traffic.
sudo tcpdump -i wlp2s0 -c 1 host
www.google.com and port 443
0 packets captured.
4 packet received by filter.
0 packets dropped by kernel.

Students observation questions.

1, which command is used to find reachability of a host from your device?
Ping command is used to test the reachability of a host.
It sends Icmp echo request and await for replies from destination

2, which command will be give the details of hops taken by a packet to each its destination?

- The traceroute command is used to display route packet take to a destination it lists each I/P along the path and the response time from each router.

3. Which command display the I.P. config of your machine.

The ifconfig command is used to view I/P configuration. These commands sta I/P address interfaces another network details.

4. Which command display TCP port status in your machine?

The netstat -tulpn command is used to display TCP port status thus show active connection, listening ports and associate process.

5. Write modify I/P configuration in Linux machine.

The ip config on ip command is used to modify Ip settings in Linux

Example: sudo ip addr add 192.168.100/24 devethO.

assign on I/P to een Interface.

Result :-

Thus the study of various networks in Linux and windows is executed successfully.