Ex: 1

Date: 16/07/2024

Study of various Network commands used in Linux and windows:

Aim:

To Study of various Network commands used in Linux and Windows:

Basic Networking commands:

arp -a:

ARP is short form of address resolution Protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.

Output:

Interface: 172.16.11.159 --- 0X7

Internet Address	Physical Address	Type
172.16.8.1	7c-5a-1c-cf-be-45	dynamic
172.16.8.167	7c-57-58-38-db-20	dynamic
172.16.8.175	7c-57-58-35-10-dc	dynamic
172.16.10.107	d8-66-c1-c5-c6-8c	dynamic
172.16.11.210	88-ae-dd-15-ed-49	dynamic

Hostname:

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

Output:

M-A

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.

Output:

```
Windows IP Configuration
   Host Name . . . . . : M-A
   Primary Dns Suffix . . . :
Ethernet adapter Ethernet
   Connection-specific DNS Suffix . :
   Description . . . . . : Realtek PCIe GBE Family Controller
F-60
   DNS Servers . . . . . : 172.16.8.1
   NetBIOS over Tcpip . . . : Enabled
```

netstat:

(network statistics) netstat displays a variety of statistics about a computer's active TCP/IP connections.

Output:

```
Active connections
  Proto   Local Address          Foreign Address        State
  TCP     0.0.0.0:135            M-A:0                  LISTENING
  TCP     0.0.0.0:445            M-A:0                  LISTENING
  TCP     0.0.0.0:902            M-A:0                  LISTENING
```

UDP	0.0.0.0:53	*:*
UDP	0.0.0.0:500	*:*
UDP	0.0.0.0:3600	*:*

netstat -r:

(network statistics) netstat displays a variety of statistics about a computer's active TCP/IP connections.

output:

Interface List

7...08 bf 68 da 0f 60 ...Realtek PCIe GbE Family Controller
28...00 ff 68 e3 12 3a ...TAP-Windows Adapter V9
14...ce 47 40 eb 1a ab ...Microsoft Wi-Fi Direct Virtual Adapter

nbtstat -a:

This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP)

output:

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]]

nslookup:

(name server lookup) is a tool used to perform DNS lookups in Linux.

nslookup www.google.com

Output:

Server: Unknown
Address: 192.168.232.31
Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4007:82a::2004

Pathping:

Pathping is unique to window's, and is basically a combination of the Ping and Tracert commands.

output:

Usage: Pathping [-g host-list] [-h maximum-hops] [-i address]
[-P period] [-q num-queries] [-w timeout]
[-4] [-6] target_name

Options:

-g host-list : Loose Source route along host-list
-h maximum_hops Maximum number of hops to Sear
-i address Use the specified source address.

Ping:

(Packet INternet Groper) command is the best way to test connectivity between two nodes.

Ping localhost

output:

Pinging M-A [::1] with 32 bytes of data:

Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms.

Route:

Route command is used to show/manipulate the IP routing table.

output:

Manipulated network routing table.

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

-f clears the routing tables of all gateway entries.

-p when used with the ADD command, makes a route persistent across.

Some important Linux networking commands

1, ip

i, # ip address show

1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever

ii, # ip address add 192.168.1.254/24 dev enp2s0

iii, # ip route add default via 192.168.1.254 dev enp

2/ ifconfig

enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.8.93 netmask 255.255.252.0 broadcast 172.
inet6 fe80::e297:e98a:6769:7eda prefixlen 64 scopeid
ether 50:9a:4c:35:12:64 txqueuelen 1000 (Ethernet)

3/ mtr

i/ # mtr google.com

Localhost.Localdomain (0.0.0.0)
Keys: Help Display mode Restart statistics Order of fields quit

Host	Packets			Pings			
	Loss%	Snt	Last	Avg	Best	Wrst	
1/ 172.16.8.1	17.9%	140	0.2	3.2	0.1	48.	
2/ Static-41.229.49-tataidc.co.in	18.4%	140	2.7	5.1	2.6	313.	
3/ 142.250.171.162	17.9%	140	2.4	4.0	2.4	144.	

ii/ # mtr -6 google.com

Localhost.Localdomain (0.0.0.0)
Keys: Help Display mode Restart statistics Order of fields quit

Host	Packets			Pings			
	Loss%	Snt	Last	Avg	Best	Wrst	
1/ 172.16.8.1	0.0%	10	0.2	0.2	0.2	0.4	
2/ Static-41.229.249.49-tataidc.co.in (49.249.229.41)	0.0%	10	3.0	2.8	2.6	3.1	0.1
3/ 142.250.171.162	0.0%	10	3.3	3.0	2.4	3.7	0.8

4/ tcpdump

i/ # dnf install -y tcpdump

Last metadata expiration check: 2:35:59 ago on Tue 23 Jul 20
Package tcpdump-14:4.9.0-2.fc26.fc26.i686 is already installed.
Dependencies resolved.
Nothing to do.
Complete!

ii, # tcpdump -D

1, enp2s0 [up, Running]

2, any [up, Running]

3, Lo [up, Running, Loopback]

4, wlp3s0 [up]

5, bluetooth [Bluetooth adapter number 0]

iii, # tcpdump -i enp2s0

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
Listening on enp2s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:53:29.988324 ARP, Request who-has gateway tell 192.168.2.164,
10:53:29.988825 IP localhost.localdomain.43353 > gateway.domain:
10:53:29.989072 IP gateway > localdomain.saadomain: ICMP time

5, Ping

i, # Ping google.com

PING google.com (142.250.182.14) 56(84) bytes of data.
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=1
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=2
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=3
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=4

ii, # ping -c 10 google.com

PING google.com (142.250.182.14) 56(84) bytes of data.
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=1
64 bytes from maa05s18-in-f14.1e100.net (142.250.182.14): icmp_seq=2

Verification

1, Display the IP settings of the NIC:

ip address show enp2s0

enp2s0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500
Link/ether 50:9a:4c:35:12:64 brd ff:ff:ff:ff:ff:ff
inet 172.16.8.93/22 brd 172.16.11.255 scope global dynamic
Valid_lft forever Preferred_lft forever
inet6 fe80::e297:e98a:6769:7ed9/64 scope link
Valid_lft forever Preferred_lft forever

2, Display the IPv4 default gateway:

ip route show default

default via 172.16.8.1 dev enp2s0 proto static metric 100
172.16.8.0/22 dev enp2s0 proto kernel scope link src 172.16.8.93

3, Display the IPv6 default gateway:

ip-6 route show default

4, Display the DNS settings

cat/etc/resolv.conf

Generated by NetworkManager
nameserver 172.16.8.1

5, use the Ping utility to verify that this host can send packets to other hosts:

ping <localhost.localdomain>

bash: Syntax error near unexpected token 'newline'

Result: Thus the basic Linux & windows command have been studied & executed