

Exercise: 1

Date: 16.07.24

STUDY OF VARIOUS NETWORK

COMMANDS

USED IN LINUX AND WINDOWS

Aim:

To study the various network commands used in Linux and windows.

Networking commands used in windows:

i) 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 : 192.168.32.1 --- 0x7

Internet Address	physical Address	Type
192.168.32.255	ff-ff-ff-ff-ff-ff	Static
224.0.0.2	01-00-5e-00-00-02	Static
224.0.0.22	01-00-5e-00-00-16	Static
224.0.0.251	01-00-5e-00-00-fb	Static
224.0.0.252	01-00-5e-00-00-fc	Static
239.255.255.250	01-00-5e-00-ff-fa	Static

Interface : 192.168.80.1 --- 0x13

Internet Address	physical Address	Type
192.168.80.255	ff-ff-ff-ff-ff-ff	Static
224.0.0.2	01-00-5e-00-00-02	Static
224.0.0.22	01-00-5e-00-00-16	Static

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

Output: DESKTOP-FL3B4QN

iii) ipconfig/all : This command displays detailed configuration information about your TCP/IP connection including, router, gateway, DNS, DHCP, and type of Ethernet adapt in your system.

Output:

Windows IP Configuration

HOST Name : LAPTOP-SGIMBD7IGI

Primary DNS Suffix :

Node Type : Mixed

IP Routing Enabled : No

WINS Proxy Enabled : No

wireless LAN adapter Local Area Connection 1

Media State : Media disconnected

Connection-specific DNS Suffix :

Description : Microsoft WiFi Direct

Physical Address : 1E-CE-51-62-87-8F

DHCP Enabled : Yes

Autoconfiguration : Yes

Enabled

est of all
displays

isplays
oo about
ng, ready,
6 Ethernet

SGIMBD71G7

connection 1:

disconnected

direct

apter

2-87-8F

OPT

ON

Wireless LAN adapter Local Area connection #2:

Media State : Media disconnected

Connection-specific DNS suffix :

Description : Microsoft WiFi Direct virtual
Adapter #2

Physical Address: 9C-CE-51-62-87-8F

DHCP Enabled : Yes

Auto-configuration Enabled : Yes

Wireless LAN adapter WIFI:

Connection-specific DNS suffix :

Description : Realtek RTL8822CE 802.11ac

Physical address: 1C-CE-51-62-87-8F

DHCP Enabled : Yes

Auto-configuration Enabled : Yes

IPv6 Address : 2401:4900:1C99:1999:8106

DHCP Server : 192.168.1.1

DNS Server : 2401:4900:50:9::280

2401:4900:50:9:9

Primary 192.168.1.1

Primary WINS Server : 192.168.1.1

NetBIOS over TCP/IP : Enabled.

TCP/IP

IV) nbtstat -a :

This command helps solve
problem with NetBIOS name resolution.

(Nbt stands for NetBIOS over TCP/IP)

-a / Lists the remote machines

(adapter status) name table given its name

-A 0.0.0.0 / Lists the remote machines

(adapter status) name table given its IP address

-c
(cache) List NBT's cache of remote machine names and their IP addresses

-n
(names) List local NetBIOS names

-r
(resolved) List names resolved by broadcast and via WINS

-R
(reload) Purges and reloads the remote cache name table

-S
(sessions) List session tables with the destination IP addresses

-RR
(Release Refresh) Sends Name Release packets to WINS and then, Refresh.

Command: nbtstat -a 127.0.0.1:49677

Output:

WIFI:

Node IP Address: [192.168.1.5]

Scope Id: []

~~Host not found~~

~~local connection * 1:~~

Node IP Address: [0.0.0.0]

Scope Id: []

~~Host not found.~~

at remote
and their
names

ed by
ia WINS

adds the
ame table

es circu
IP

x packe
men,

0.0.1:49677

1.5]

d: []

[]

[]

Local Area connection * 2:

Node IP Address: [0.0.0.0]

ScopeId: []

Host not found.

v) netstat:

(network statistics) netstat
displays a variety of statistics about
a computer's active TCP/IP connections.
It is a command line tool to monitoring
network connection both incoming and
outgoing as well as viewing routing
tables, interface statistics etc.

- a displays all connection and listening ports
- b displays all executable involved in creating each connection or listening port.
- e displays ethernet statistics.
- f displays Fully qualified domain Name (FQDN) for foreign addresses.
- i displays time spent by a TCP connections in its current state.
- n displays addresses and port number in numerical form.
- o displays the owning process ID associated with connection.
- r displays the routing table.

command-1: netstat -e 127.0.0.1:4967

output:

Interface statistics

	Received	Sent
Bytes	2953017390	615787514
unicast packets	3286062	2165094
discards	0	0
Errors	0	0
unknown protocols	0	0
Non unicast packets	84490	16068

command-2: netstat -8 127.0.0.1:4967

output:

Interface list

17...1e ce 5f 62 87 8f	Microsoft WiFi port virtual adapter
15...1c ce 5f 62 87 8f	Realtek RTL8820 802.11ac PCIe
<u>1...software loopback interface</u>	

IPV4 Route table.

Active routes:

IF Network destination

IS 306 ::/0

1 331 ::/128

IS 3062401:4900:1cc9:1a99::/64

Gateway

fe80::1

on-link

on-link

27.0.0.1:4967

15 306 2401:4900:1cc9:1a99:1/28 on-link.
15 306 fe80::1/64 on-link
1 331 ff00 ::1/8 on-link
15 306 ff00 ::1/8 on-link

sent

persistent Routes : None.

5737514
2165094
0
0
16068
0.0.1:4967

vi) nslookup : (name server lookup)
It is a tool used to perform DNS lookup in Linux. It is used to display DNS details, such as the IP address of a particular computer, the MX records for a domain or the NS servers of a domain. nslookup can operate in two modes: interactive and non-interactive.

command : nslookup
olp : Default Server : unknown
Address : 172.16.8.1
> www.google.com
Server : unknown
Address : 172.16.8.1

Non authoritative answer:
Name : www.google.com
Address : 2401:6800:4007:81e::200,
142.250.183.228.

vii) pathping :

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

Pathping traces the route to the destination address then launches a 2s round trip of each traceroute along the way, gathering statistics on the rate of data loss along each hop.

options:

- g host-list Loose source route
- n maximum Maximum number of hops to March to target.
- i address use the specified source address.
- n nohostname do not resolve address to hostname.
- P period wait period milliseconds between pings.
- q numqueries A number of queries per hop.
- w timeout wait timeout milliseconds for each reply.

-4 Force using IPv4

-6 Force using IPv6.

command - i: pathping -4 172.16.8.92

O/P: Tracing route to DESKTOP-FL38U
[172.16.8.92] over a maximum of
30 hops.

Page _____
Date _____

Page _____
Date _____

traces a 25
bytes along
on the
each hop.

0 DESKTOP - FL3B4QV [172.16.8.92]
1 DESKTOP - FL3B4QV [172.16.8.92]

computing statistics for 25 seconds ...

source to Here This node/Link
Hop RTT Lost/Sent = Pct Lost/Ext = Pct
0 0ms 0/100 = 0% 0/100 = 0% Desktop
1 0ms 0/100 = 0% 0/100 = 0% FL3B4QV [172.16.8.92]

trace complete.

command-2: pathping -n 127.0.0.1

tracing route to 127.0.0.1 over a maximum
of 30 hops

0 127.0.0.1

1 127.0.0.1

computing statistics for 25 seconds ...

Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 0ms 0/100 = 0% 0/100 = 0% 127.0.0.1
1 0ms 0/100 = 0% 0/100 = 0% 127.0.0.1

Trace complete.

viii) ping: (packet internet protocol)

Command is the best way to test connectivity
between two nodes. Ping uses ICMP (internet
control message protocol) to communicate
to other devices.

command - 1: ping localhost

O/P:

Pinging DESKTOP-FL3BLQV [::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

command - 2: ping -l 172.16.8.92

Pinging 172.16.8.92 with 32 bytes of data

Reply from 172.16.8.92: bytes=32 time < 1ms

Reply from 172.16.8.92: bytes=32 time < 1ms TTL=

ping statistics for 172.16.8.92:

packets: sent = 4, received = 4, lost = 0

approximate round trip times in
milliseconds.

minimum = 0ms, maximum = 0ms, Avg = 0ms

command - 3: ping www.rec.com.

Pinging www.rec.com [23.227.38.65]
with 32 bytes of data.

lost

1 with

Reply from 23.227.38.65 byte=3 time=7ms TTL=59
 Reply from 23.227.38.65 byte=3 time=7ms TTL=59
 Reply from 23.227.38.65 byte=3 time=7ms TTL=59
 Reply from 23.227.38.65 byte=3 time=7ms TTL=59

ping statistics for 23.227.38.65:

packets: sent=4 received=4, lost=0

Approximate round trip times in ms:

minimum=6ms, maximum=7ms, Avg=6ms.

ix) Route: Route command is used to show / manipulate IP routing table. It is primarily used for setup static routes to specific host or networks via an interface.

Output: Kernel IP Routing table

destination	gateway	genmask	flags	metric	ref	use	interface
default	gateway	0.0.0.0	UG	100	0	0	enps
0							
172.16.8.0	0.0.0.0	255.255.252.0	U	100	0	0	enps
0							

= 0

= 0ms

[65]

Linux console outputs:

1. arp -a : a: unknown host
2. hostname : localhost.localdomain
3. ifconfig :


```
enp2s0: flags=4163<UP,BROADCAST,RUNNING,
          MULTICAST mtu 1500
          inet 172.16.11.207
              netmask 255.255.252.0
              broadcast 172.16.11.255.
```
4. nslookup www.google.com:


```
server: 172.16.8.1
Address: 172.16.8.1#53
```

Non-authoritative answers:

- Name: www.google.com
 Address: 142.250.183.228
 Name: www.google.com
 Address: 2404:6800:4007:8fe::2004.

5. netstat:

It gives proto, Recv-Q, send-Q,
 local address, foreign address, state of
 active internet connections (w/o servers).

also gives Proto, Recv-Q, flags,
 type, state, I-node, path of active unix
 domain sockets. (w/o servers)

Important Linux Networking commands:

1. ip:

ip command is one of the basic commands every administrator will need in daily work, from setting up new system and assigning IP's to troubleshooting existing systems.

usage: ip [options] object [command]

Example: ip address show

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65535 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 brd 0.0.0.0 scope host lo
       inet6 ::1/128 brd :: scope host lo
            valid_lft forever preferred_lft forever
```

2. ifconfig:

To assign an address to a network interface and to configure or display the current network interface configuration information.

output:

```
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 172.16.11.207 brd 172.16.11.255 netmask 255.255.252.0
          broadcast 172.16.11.255
```

3. **traceroute**: serves as a network diagnostic tool
output: my trace route (v6-87)
local host: localdomain (e.g.)
keys: Help Display mode Restart start
order of fields: quit

Host
l.: localhost or host principle name
packets:

	Pings	packets
loss %	Snt	Last
0.0%	178	0.1
		0.1
		0.0
		0.0

4. **tcpdump**: designed for capturing and displaying packets.

o/p: `tcpdump -c 10 -w expso.pcap`

`tcpdump -D`

1. `enp260` [up, running]

2. `any` (pseudo-device that captures on all interfaces) [up, running]

3. `lo` [up, running, loopback]

4. `wlp3s0`

5. `bluetooth` (Bluetooth adapter number 0).

5. **ping**:

tool to verify IP-level connectivity to another TCP/IP computer by sending Internet control message protocol (ICMP) echo request messages.

output:
ping to
64 bytes

PING 64 bytes

64 bytes

(216.58.61.6)

time=1

ms

observes

1. which reaches device?

ping used

and s

2. which of destination

from provider much

NEW MAHADEV GOLD
Page _____ Date _____

the diagnostic tool
route (v0-87)
(e:
restart eternally
maximum
maximum bytes
at wts stdver
0 0% 0.0
capturing and
an eth0
throughput
captures
back] 1
connection
uplink
uplink
uplink
connectivity
sending
(C:\temp)

NEW MAHADEV GOLD
Page _____ Date _____

Output : ping localhost
ping localhost (localhost (:) 56 data bytes
64 bytes from localhost (:) : ICMP-Seq=1
ttl = 64 time = 0.053 ms

www.
ping -c 2 google.com
PING google.com (216.58.206.174) 56(84) bytes of data
64 bytes from sof02S2T-in-f14-1e100.net
(216.58.206.174) : ICMP-Seq=1 ttl = 56 time = 10.7ms
64 bytes from sof02S2T-in-f14-1e100.net
(216.58.206.174) : ICMP-Seq=2 ttl = 56
time = 10.2 ms

Observation

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

Ans: Ping - command < hostname or IP >
ping is the primary TCP/IP command used to troubleshoot connectivity, reachability and name resolution.

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

Ans: tracert (mat's trace route)
~~tracert command will show the route from a computer to a specified host. tracert provides a lot of statistics about each hop, such as response time and percentage.~~

3. which commands displays the IP configuration of your machine?

Ans: ip <options> <objects> <commands>
IP command can show address information, manipulate routing, plus display network various devices network various devices, interfaces & tunnels.

4. which command displays the TCP port status in your machine?

Ans: netstat
netstat displays variety of statistics about a computer active TCP/UDP connections.

5. write the modify the IP configuration in a Linux machine?

i) assigning IP Address to interface

ip address add 192.168.1.254/24
dev enps03

ii) deleting IP Address:

~~ip address del 192.168.1.254/24
dev enps03.~~

Result:

The various Linux & Windows commands is successfully studied.