

16/7/24

PRACTICAL - I

AIM

Study of various Network commands used in Linux and Windows

BASIC NETWORKING COMMANDS:

Windows Commands:

- 1) arp -a - windows

Output:

Interface : 192.168.134.107 --- 0xb

Internet Address	Physical address	Type
192.168.134.205	1b-17-10-e6-16-bf	dynamic
192.168.134.255	ff-ff-ff-ff-ff-ff	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-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

- 2) hostname - windows

Output : LAPTOP-PN19Q8AT

- 3) ipconfig /all

Output :

Windows IP configuration

Hostname : LAPTOP-PN19Q8AT

Primary Dns Suffix :

Node Type : Hybrid

IP Routing Enabled : No

WINS Proxy Enabled : No

Ethernet adapter Ethernet 2 :

Media State	: Media disconnected
Connection-specific DNS Suffix	: .local
Description	: ExpressVPN TAP Adapter
Physical Address	: 00-FF-5F-7C-80-77
DHCP Enabled	: Yes
Autoconfiguration Enabled	: Yes

Unknown adapter Local Area Connection :

Media State	: Media disconnected
Connection-specific DNS Suffix	: .local
Description	: Microsoft WiFi Direct Virtual Adapter #2
Physical address	: A2-2B-20-A2-BF-9F
DHCP Enabled	: Yes
Autoconfiguration Enabled	: Yes

Wireless LAN Adapter WiFi 1 :

Connection-specific DNS suffix : .local

Description	: Realtek RTL8852AE
-------------	---------------------

WiFi 6 802.11ax PCIe Adapter

Physical address	: 20-2B-20-A2-BF-9F
DHCP Enabled	: Yes
Autoconfiguration Enabled	: Yes
IPv6 Address	: 2401:4900:7b81:35e6:

Temporary IPv6 address : 2401:4900:7b81:35e6:

b512:42a3:15bb:2a2d (Preferred)

Link-local IPv6 Address : fe80::14b2:3799:

7cfc:ed93-11 (Preferred)

: 192.168.184.107 (Preferred)

: 255.255.255.0

IPv4 Address

Subnet Mask

Lease Obtained : 15 July 2024 09:28:07 PM
Lease Expires : 15 July 2024 10:28:07 PM
Default Gateway : fe80::1427:10ff:fe61:6bf7/11
 : 192.168.134.205
DHCP Server : 192.168.134.205
DHCPv6 IAID : 136325920
DHCPv6 Client DUID : 00-01-00-01-2B-59-27-AE-7C-4D-
 : 8F-10-82-0F
DNS Servers : 192.168.134.205
NetBIOS over Tcpip : Enabled

Ethernet adapter Ethernet:

Media Status : Media disconnected
Connection-specific DNS suffix :
Description : Realtek Gaming GbE Family
Physical address : 7C-9D-8F-10-82-0F
DHCP Enabled : Yes
Autoconfiguration Enabled : Yes

4) nbtstat -a :

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]]

-a (Adapter status) Lists the remote machine's
name table given its name

-A (Adapter status) Lists the remote machine's
name table given its IP Address.

- c (cache) Lists NBT's cache of remote machine names and their IP addresses.
- n (names) Lists local NetBIOS names.
- r (resolved) Lists names resolved by broadcast and via WINS
- R (Reload) Purges and reloads the remote cache name table
- S (sessions) Lists sessions table with the description IP addresses
- s (sessions) Lists sessions table converting destination IP addresses to computer NetBIOS names.
- RR (Release Refresh) Sends name Release packets to WINS and then, starts Refresh.

RemoteName Remote host machine name.

IP Address Dotted decimal representation of the IP address.

interval Redisplays selected statistics, pausing interval seconds between each display.

Press Ctrl+C to stop redisplaying

statistics.

5) netstat - windows

Output:

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49670	LAPTOP-PN19Q8AT:49671	Established
TCP	127.0.0.1:49671	LAPTOP-PN19Q8AT:49670	Established
TCP	127.0.0.1:49672	LAPTOP-PN19Q8AT:49673	Established
TCP	127.0.0.1:49673	LAPTOP-PN19Q8AT:49672	Established
TCP	127.0.0.1:62681	LAPTOP-PN19Q8AT:62683	Established

TCP [27.0.0.1:62683] [APTOP-PN19Q8FT:62681] Established
TCP [192.168.134.107: 20.198.118.190: https] Established
62702
TCP [192.168.134.107: 20.198.118.190: https] Established
62742
TCP [192.168.134.107: 23-59-175-67: https] Close-wait
63031
TCP [192.168.134.107: 20.187.186.89: https] Established
63168
TCP [192.168.134.107: 20.44.10.122: https] Established
63199
TCP [192.168.134.107: 20.44.10.122: https] Established
63206
TCP [2401:4900:7b81: [2620:1ec:bdf::254]] Close-wait.
35e6:b512:42a3: https
15bb:2a2dJ:62811
TCP [2401:4900:7b81: whatsapp-chatd-edge-1] Established.
35e6:b512:42a3: shr-02-6ir3:https
15bb:2a2dJ:62999
TCP [2401:4900:7b81: [2620:1ec:bdf:254]] Close-wait
35e6:b512:42a3: https
15bb:2a2dJ:63000
TCP [2401:4900:7b81: 81-in-f188:5228] Established
35e6:b512:42a3:
15bb:2a2dJ:63167
TCP [2401:4900:7b81: [2620:1ec:bdf::58]] Established
35e6:b512:42a3: https
15bb:2a2dJ:63196
TCP [2401:4900:7b81: maa05816-in-205:] time-wait
35e6:b512:42a3: https.
15bb:2a2dJ:63197

b) nslookup www.google.com -> windows
output:
Server: www.google.com
Addresses: 210.1.68.0:4007:82a::2001
192.250.196.36
DNS request timed out
timeout was 2 seconds.
DNS request timed out
timeout was 2 seconds.
*** Request to www.google.com timed out

7) Pathping

Output:

Usage: pathping [-g host-list] [-h maximum-hops]
[-I address] [-n] [-p period] [-q num-queries]
[-w timeout] [-A] [-B] target-name.

Options:

- g host-list Loose source route along host-list
- h maximum-hops Maximum number of hops to search for target
- I address Use the specified source address.
- n Do not resolve addresses to hostnames
- p period Wait period milliseconds btw pings.
- q num-queries Number of queries per hop
- w timeout Wait timeout milliseconds for each reply
- A Force using IPv4
- B Force using IPv6.

Pa

Ou

Tc

Ov

e

C

I

8)

ah

ah

ah

ah

ah

ah

Pathping -4 172.16.8.92
Output:

Tracing route to DESKTOP-FL3B4QV [172.16.8.92]
over a maximum of 30 hops:
6 DESKTOP-FL3B4QV [172.16.8.92]
1 DESKTOP-FL3B4QV [172.16.8.92]

Computing statistics for 25 seconds...

Source to Here This Node/Hop

HOP	RTT	Lost/Sent = Pct	Lost/Sent = PCT	Address
6	0ms	0/100=0%	0/100=0%	DESKTOP-FL3B4QV [172.16.8.92]
1	0ms	0/100=0%	0/100=0%	DESKTOP-FL3B4QV [172.16.8.92]

Trace complete.

8) Ping localhost - windows

Output:

Pinging LAPTOP-PN19Q8A [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
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

ping 1.2.2.2 - windows
output:

Pinging 1.2.2.2 with 32 bytes of data:
Reply from 1.2.2.2: bytes=32 time=67ms TTL=54
Reply from 1.2.2.2: bytes=32 time=69ms TTL=54
Reply from 1.2.2.2: bytes=32 time=71ms TTL=54
Reply from 1.2.2.2: bytes=32 time=58ms TTL=54

Ping statistics for 1.2.2.2:

Packets: Sent=4, Received=4, Lost=0 (0% loss),

Approximate round trip times in milliseconds:

Minimum=58ms, Maximum=71ms, Average=66ms

ping www.facebook.com - windows

Output:

Pinging star-mini.107.facebook.com [2a03:2880]:

-f184:81:face:b00c:0:25de] with 32 bytes of data.

Reply from 2a03:2880: f184:81:face:b00c:0:25de:

time=26ms

Reply from 2a03:2880: f184:81:face:b00c:0:25de:

time=32ms

Reply from 2a03:2880: f184:81:face:b00c:0:25de:

time=25ms

Reply from 2a03:2880: f184:81:face:b00c:0:25de:

time=34ms

Ping statistics for 2a03:2880:f184:81:face:

b00c:0:25de:

Approx Packets: Sent=4, Received=4, Lost=0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum=25ms, Maximum=34ms, Average=29ms

9) Route - windows
Output:
Manipulates network routing tables.

ROUTE [-f] [-P] [-A|-B] [destination]
[mask netmask] [gateway] [METRIC metric]
[IF interface]

-f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.

-P When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.

-A Force using IPv4

-B Force using IPv6

Command One of these:

PRINT Prints a route

ADD Adds a route

DELETE Deletes a route

CHANGE Modifies an existing route

destination	specifies the host.
MASK	Specifies that the next parameter is the 'netmask' value.
netmask	Specifies a subnet mask value for this route entry. If not specified, it defaults to 255.255.255.255.
gateway	Specifies gateway.
interface	the interface number for the specified route.
METRIC	Specifies the metric, i.e. cost for the destination.

~~Symbolic names~~ Linux commands:

1) Route - Linux command to view routes

Output:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	gateway	0.0.0.0	UG	100	0	0	enp2s0
172.16.8.0	0.0.0.6	255.255.252.0	U	100	0	0	enp2s0

2) ping hostname - Linux command

Output:

PING localhost (localhost (::1)) 56 data bytes

64 bytes from localhost (::1): icmp_seq=1

ttl=64 time=0.074ms

64 bytes from localhost (::1): icmp_seq=2

ttl=64 time=0.083ms

ping 4.2.2.2 : Linux
Output:

PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=53 time=36.1ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=53 time=35.5ms

Ping www.facebook.com
Output:

PING star-mini.c10r.facebook.com (157.240.192.35)

56(84) bytes of data.
64 bytes from edge-star-mini-shv-02-mad2.facebook.
com (157.240.192.35): icmp_seq=1 ttl=59 time=2.76 ms

3) arp -a

Output:

gateway (172.16.8.1) at 7c:5a:1c:cfa:bca:45
[ether] on enp2s0.

4) hostname

Output:

localhost, localdomain

5) ifconfig

Output:

enp2s0: flags=4163<UP,BROADCAST,running,
multicast > mtu 1500

10: flags=73<UP,LOOPBACK,running> mtu 65536

wlp3s0: flags=4099<UP,broadcast,multicast>
mtu 1500

~~nmblookup -A <ip address>~~

6) nmblookup -A 14.99.10.232

Output:

Looking up status of 14.99.10.232

workgroup : <00> -> <Group> B <Actives>

DESKTOP-BQ498VC <00> -> B <Actives>

MAC Address = 50-9A-9C-34-D3-C3

7) nslookup www.google.com

Output:

Server: 172.16.8.1

Address: 172.16.8.1#53

Non-authoritative answer:

Name: www.google.com

Address: 142.250.183.228

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 { commands }.

Example: ip address show.

1:10: <loopback, up, lower-up> mtu 6553
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.

2) ip /ifconfig :

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

Output :

enp2so : flags=4163<UP,BROADCAST,RUNNING
MULTICAST > mtu 15000
inet 172.16.11.207
netmask 255.255.252.0
broadcast 172.16.11.255

3) mtr :

serves as a network diagnostic tool

Output : my trace route (v0.87)

local host : localdomain (8!)

Keys : Help display mode Restart Standby
order of fields : quit

Host

l :: l

Packets:

Pings

loss%	snt	last	avg	Boot	wts	stddev
0.0%	17.8	6.1	0.1	0.0	0.1	0.0

4) tcpdump: designed for capturing and displaying packets.

O/P:

tcpdump -D

1. enp260 [up, running]
2. any (pseudo; device that capture on all interfaces) [up, running]
3. lo [up, running, loopback].
4. wlp380.
5. Bluetooth 0 (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 localhost

ping localhost (localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp-seq=1
ttl=64 time=0.053 ms.

Ping -c 2 www.google.com

PING google.com (216.58.206.174) 56/84)
bytes of data 64 bytes from sof62527-in-
f14.1@100.net (216.58.206.174): Pcmpe-seq=1:
56 time=10.7ms 64 bytes from sof0827-
in-f14.1@100.net (216.58.206.174):
icmp-seq=2 ttl=56 time=10.2ms

Observation

- 1) Which command is used to find the reachability of a host machine from your device?

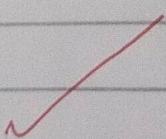
Ans: Ping - command <hostname or IP>
ping is the primary TCP/IP command used to troubleshoot connectivity, reachability and name resolution.

- 2) Which command will be given the details of hops taken by a packet to reach its destination?

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

- 3) Which commands display the IP configuration of your machine?

Ans: ip <options> <object> <command>
IP command can show address information, manipulate routing, plus display network various devices network various devices interfaces & net funnels.



4) Which command display the TCP port status in your machine?
 Ans : netstat

netstat displays variety of statistics about a computer active TCP / IP connections.

5) Write the modify ip configuration in a linux machine?

Ans :

1) assigning IP address to Interface

ip address add 192.168.1.254/24
 dev enp50.3.

2) detecting IP address:

ip address del 192.168.1.254/24
 dev enp50.3.

Q. No
Tb/T24

RESULT

The experiment on various network and linux commands are observed & studied.