Batch: A2	**Roll No.: 16010121045**
Experiment / assignment / tutorial No 2	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

Experiment No. 2

Title: Study of basic network administration commands and network configuration.

AIM: Study networking commands –ping, traceroute, nslookup, arp, rarp, netstat, telnet.

Expected Outcome of Experiment:

1. Understand the fundamentals of network administration.

Books/ Journals/ Websites referred:

1. *Linux Lab - Open source Technology : Ambavade –Dreamtech*
2. http://manpages.ubuntu.com/manpages/trusty/man8/rarp.8.html
3. http://computernetworkingnotes.com/comptia-n-plus-study-guide/network-tool-command.html

Pre Lab/ Prior Concepts: Computer Network

New Concepts to be learned: Command line operation to handle networks.

Computers are connected in a network to exchange information or resources each other. Two or more computer connected through network media called computer network. There are number of network devices or media are involved to form computer network. Computer loaded with Windows and Linux Operating System can also be a part of network whether it is small or large network by its multitasking and multiuser natures. Maintaining of system and network up and running is a task of System / Network Administrator's job.

Frequently used network configuration and troubleshoot commands in Linux/Windows are as follows:

1. IFCONFIG/ IPCONFIG

ifconfig (interface configurator) command is use to initialize an interface, assign IP Address to interface and enable or disable interface on demand. With this command you can view IP Address and Hardware / MAC address assign to interface and also MTU (Maximum transmission unit) size.

ifconfig with interface (eth0) command only shows specific interface details like IP Address, MAC Address etc. with -a options will display all available interface details if it is disable also.

Syntax: # ifconfig eth0

To enable or **disable** specific Interface, we use example command as follows.

Enable eth0: # ifup eth0

Disable eth0: # ifdown eth0

To Setting MTU Size:

By default, MTU size is 1500. We can set required MTU size with below command.

Replace XXXX with size.

Syntax: # ifconfig eth0 mtu XXXX

Set Interface in Promiscuous mode.

Network interface only received packets belongs to that particular NIC. If you put interface in promiscuous mode, it will receive all the packets. This is very useful to capture packets and analyse later. For this you may require superuser access.

Syntax: # ifconfig eth0 - promisc

2. PING

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices.

It verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

ping [-c count] [-i wait] [-l preload][-s packetsize] host

-c count
Stop after sending (and receiving) count ECHO_RESPONSE packets.

-i wait
Wait wait seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.

-l preload
If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior.

-s packetsize
Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

PING Command Example:

ping 4.2.2.2

ping -c 5 www.tecmint.com

3. TRACEROUTE/ TRACERT

traceroute is a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path. Below we are tracing route to global DNS server IP Address and able to reach destination also shows path of that packet is traveling.

Syntax:

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

Parameters

-d : Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.

-h: MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

-j: HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostList.The HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.

-w : Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be

received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

4. **NETSTAT command**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Netstat provides statistics for the following:

Proto - The name of the protocol (TCP or UDP).

Local Address - The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

Foreign Address - The IP address and port number of the remote computer to which the socket is connected. The names that correspond to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

(state) Indicates the state of a TCP connection. The possible states are as follows:
CLOSE_WAIT
CLOSED
ESTABLISHED
FIN_WAIT_1
FIN_WAIT_2
LAST_ACK
LISTEN
SYN_RECEIVED
SYN_SEND
TIMED_WAIT

Syntax
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters

Used without parameters, netstat displays active TCP connections.

-a Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

-e Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.

-n Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.

-o Displays active TCP connections and includes the process ID (PID) for each connection.

-p Shows connections for the protocol specified by Protocol.

-s Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.

-r Displays the contents of the IP routing table.

Netstat (Network Statistic) command display connection info, routing table information etc. To displays routing table information use option as -r.

netstat –r

5. DIG

Dig (domain information groper) query DNS related information like A Record, CNAME, MX Record etc. This command mainly uses to troubleshoot DNS related query.

dig www. Ipadress.com

6. NSLOOKUP

The name "nslookup" means "name server lookup". nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It displays information from Domain Name System (DNS) name servers.

nslookup command also use to find out DNS related query.

Example:

C:\Documents and Settings\sysadm>nslookup itu.dk
Server: ns3.inet.tele.dk
Address: 193.162.153.164

Non-authoritative answer:
Name: itu.dk
Address: 130.226.133.2
nslookup www. Googel.com

7. ROUTE

Route command also shows and manipulate ip routing table. To see default routing table in Linux, type the following command.

route

8. ARP

When we need an Ethernet (MAC) address we can use arp(address resolution protocol). In other words it shows the physical address of an host.

Syntax
arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]

Parameters

Used without parameters, ping displays help
-a [InetAddr] [-N IfaceAddr] Displays current ARP cache tables for all interfaces.

-g [InetAddr] [-N IfaceAddr] Identical to -a.

-d InetAddr [IfaceAddr] Deletes an entry with a specific IP address, where InetAddr is the IP address.

-s InetAddr EtherAddr [IfaceAddr] Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr.

To add a static ARP cache entry to the table for a specific interface, use the IfaceAddr parameter where IfaceAddr is an IP address assigned to the interface

ARP (Address Resolution Protocol) is useful to view / add the contents of the kernel's ARP tables. To see default table use the command as.

arp -e

Address	HWtype	HWaddress	Flags Mask	Iface
192.168.50.1	ether	00:50:56:c0:00:08	C	eth0

9 . ETHTOOL

ethtool is a replacement of mii-tool. It is to view, setting speed and duplex of your Network Interface Card (NIC). You can set duplex permanently in /etc/sysconfig/network-scripts/ifcfg-eth0 with ETHTOOL_OPTS variable.

Syntax: # ethtool eth0

10. **TELNET**

The telnet command is used to communicate with another host using the TELNET protocol. If telnet is invoked without the host argument, it enters command mode, indicated by its prompt (telnet>) In this mode, it accepts and executes the commands listed below. If it is invoked with arguments, it performs an open command with those arguments.

To login to a remote machine, use this syntax:

% **telnet <*hostname*>**

The options are as follows:

-8 Specifies an 8-bit data path. This causes an attempt to negotiate the TELNET BINARY option on both input and output.

-E Stops any character from being recognized as an escape character.

-K Specifies no automatic login to the remote system.

11. HOTENAME

hostname is to identify in a network. Execute hostname command to see the hostname of your box. You can set hostname permanently in /etc/sysconfig/network. Need to reboot box once set a proper hostname.

hostname

12. SYSTEMINFO

Display information about a system.

IMPLEMENTATION:

Ipconfig: The ipconfig command displays the basic IP addressing information for each network interface on the Windows system. This information includes both the IP address and subnet mask.

```
C:\Users\jain4>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c0:104d:e4ea:1383:766:e103:e0fc
   Temporary IPv6 Address. . . . . . : 2409:40c0:104d:e4ea:c4f1:50f1:95de:8671
   Link-local IPv6 Address . . . . . : fe80::226d:1259:3dfb:8117%13
   IPv4 Address. . . . . . . . . . . : 192.168.202.202
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c43:62ff:fec8:3d8%13
                                       192.168.202.161
```

Ifconfig: The command ifconfig stands for interface configurator. This command enables us to initialize an interface, assign IP address, enable or disable an interface. It display route and network interface. You can view IP address, MAC address and MTU (Maximum Transmission Unit) with ifconfig command.

```
~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1440
        inet 192.168.39.28  netmask 255.255.255.255  broadcast 192.168.39.28
        ether ba:75:fb:ad:92:b9  txqueuelen 0  (Ethernet)
        RX packets 536  bytes 141845 (141.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 485  bytes 764218 (764.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ping: ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

```
PS C:\Users\jain4> ping 4.2.2.2

Pinging 4.2.2.2 with 32 bytes of data:
Request timed out.
Reply from 4.2.2.2: bytes=32 time=306ms TTL=58
Reply from 4.2.2.2: bytes=32 time=215ms TTL=58
Reply from 4.2.2.2: bytes=32 time=334ms TTL=58

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 215ms, Maximum = 334ms, Average = 285ms
PS C:\Users\jain4>
```

Tracert: Traceroute is a simple yet clever command-line tool for tracing the path an IP packet takes across one or many networks.

```
C:\Users\jain4>tracert www.google.com

Tracing route to www.google.com [172.217.166.36]
over a maximum of 30 hops:

  1     2 ms     3 ms     3 ms  10.0.0.1
  2     4 ms     4 ms     2 ms  172.30.250.250
  3    18 ms    15 ms    15 ms  182.73.90.241
  4    20 ms    19 ms    17 ms  182.79.146.170
  5     8 ms    10 ms     7 ms  72.14.213.254
  6    11 ms     6 ms    11 ms  142.251.225.9
  7     7 ms     5 ms     5 ms  108.170.235.51
  8    10 ms     5 ms     6 ms  bom07s18-in-f4.1e100.net [172.217.166.36]

Trace complete.
```

Netstat: The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

```
C:\Users\jain4>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.89.114:49418      20.198.119.143:https   ESTABLISHED
  TCP    10.0.89.114:51274      104.26.7.215:https     ESTABLISHED
  TCP    10.0.89.114:51276      104.26.7.215:https     ESTABLISHED
  TCP    10.0.89.114:51278      sf-in-f188:5228        ESTABLISHED
  TCP    10.0.89.114:51291      104.26.7.215:https     ESTABLISHED
  TCP    10.0.89.114:51349      bom12s15-in-f10:https  TIME_WAIT
  TCP    10.0.89.114:51353      bom12s01-in-f3:https   ESTABLISHED
  TCP    10.0.89.114:51372      bom12s06-in-f3:https   ESTABLISHED
  TCP    10.0.89.114:51375      ec2-3-110-247-150:https  TIME_WAIT
  TCP    10.0.89.114:51378      ec2-3-110-247-150:https  TIME_WAIT
  TCP    10.0.89.114:51379      40.74.98.193:https     TIME_WAIT
  TCP    10.0.89.114:51390      ec2-3-110-247-150:https  TIME_WAIT
```

Dig: The dig command in Linux is used to gather DNS information. It stands for Domain Information Groper, and it collects data about Domain Name Servers. The dig command is helpful for troubleshooting DNS problems, but is also used to display DNS information.

```
~$ dig google.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30447
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             30      IN      A       142.250.97.101
google.com.             30      IN      A       142.250.97.100
google.com.             30      IN      A       142.250.97.113
google.com.             30      IN      A       142.250.97.139
google.com.             30      IN      A       142.250.97.102
google.com.             30      IN      A       142.250.97.138

;; Query time: 4 msec
;; SERVER: 10.96.0.10#53(10.96.0.10) (UDP)
;; WHEN: Tue Aug 08 09:55:06 UTC 2023
;; MSG SIZE  rcvd: 195
```

Nslookup: Nslookup is the name of a program that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

```
C:\Users\jain4>nslookup google.com
Server:  svvdc02.svv.local
Address:  172.31.0.26

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    google.com
Address:  142.250.183.110
```

Route: In computing, route is a command used to view and manipulate the IP routing table in Unix-like and Microsoft Windows operating systems and also in IBM OS/2 and ReactOS. Manual manipulation of the routing table is characteristic of static routing.

```
C:\Users\jain4>route PRINT
===========================================================================
Interface List
  4...1c 99 57 1e 4a 57 ......Microsoft Wi-Fi Direct Virtual Adapter
 10...1e 99 57 1e 4a 56 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 13...1c 99 57 1e 4a 56 ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1      10.0.89.114     45
         10.0.0.0    255.255.128.0         On-link       10.0.89.114    301
     10.0.89.114  255.255.255.255         On-link       10.0.89.114    301
    10.0.127.255  255.255.255.255         On-link       10.0.89.114    301
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link       10.0.89.114    301
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link       10.0.89.114    301
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 13    301 fe80::/64                On-link
 13    301 fe80::226d:1259:3dfb:8117/128
                                    On-link
  1    331 ff00::/8                 On-link
 13    301 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

Arp: The arp command displays and modifies the Internet-to-adapter address translation tables used by the Address in Networks and communication management. The arp command displays the current ARP entry for the host specified by the HostName variable.

```
~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
169.254.1.1              ether   ee:ee:ee:ee:ee:ee   C                     eth0
```

Ethtool: Ethtool is a Network Interface Card configuration command that allows you to retrieve information and change your NIC settings. These settings include Speed, Duplex, Auto-Negotiation, and many other parameters.

```
┌──(mrhacker㉿kali)-[~]
└─$ ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised pause frame use: No
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Auto-negotiation: on
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        MDI-X: off (auto)
netlink error: Operation not permitted
        Current message level: 0x00000007 (7)
                               drv probe link
        Link detected: yes
```

Hostname: The /usr/bin/hostname command displays the name of the current host system.

```
C:\Users\jain4>hostname
LAPTOP-H55K2586
```

```
~$ hostname
project-37c6b235-c3dc-4563-9a6a-d4faacc59311
~$
```

Systeminfo: List system configuration. The output includes OS configuration, security info, product ID, RAM, disk space, and network cards.

```
C:\Users\jain4>systeminfo

Host Name:                 LAPTOP-H55K2586
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          jain47031@outlook.com
Registered Organization:   N/A
Product ID:                00327-36264-96710-AAOEM
Original Install Date:     01-11-2022, 14:36:32
System Boot Time:          08-08-2023, 14:37:47
System Manufacturer:       LENOVO
System Model:              82FE
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~1007 Mhz
BIOS Version:              LENOVO FKCN46WW(V3.09), 31-01-2023
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,975 MB
Available Physical Memory: 2,372 MB
Virtual Memory: Max Size:  12,839 MB
Virtual Memory: Available: 6,984 MB
Virtual Memory: In Use:    5,855 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-H55K2586
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5028851
                           [02]: KB5012170
                           [03]: KB5028185
                           [04]: KB5028320
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) Wi-Fi 6 AX201 160MHz
                                 Connection Name: Wi-Fi
                                 DHCP Enabled:    Yes
                                 DHCP Server:     172.31.0.25
                                 IP address(es)
                                 [01]: 10.0.89.114
                                 [02]: fe80::226d:1259:3dfb:8117
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes

C:\Users\jain4>
```

CONCLUSION: Learned and applied the various network administrations and configurations commands in Linux and windows.