Batch:- D-2	**Roll No.:-** 16010122151
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. HOSTNAME

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

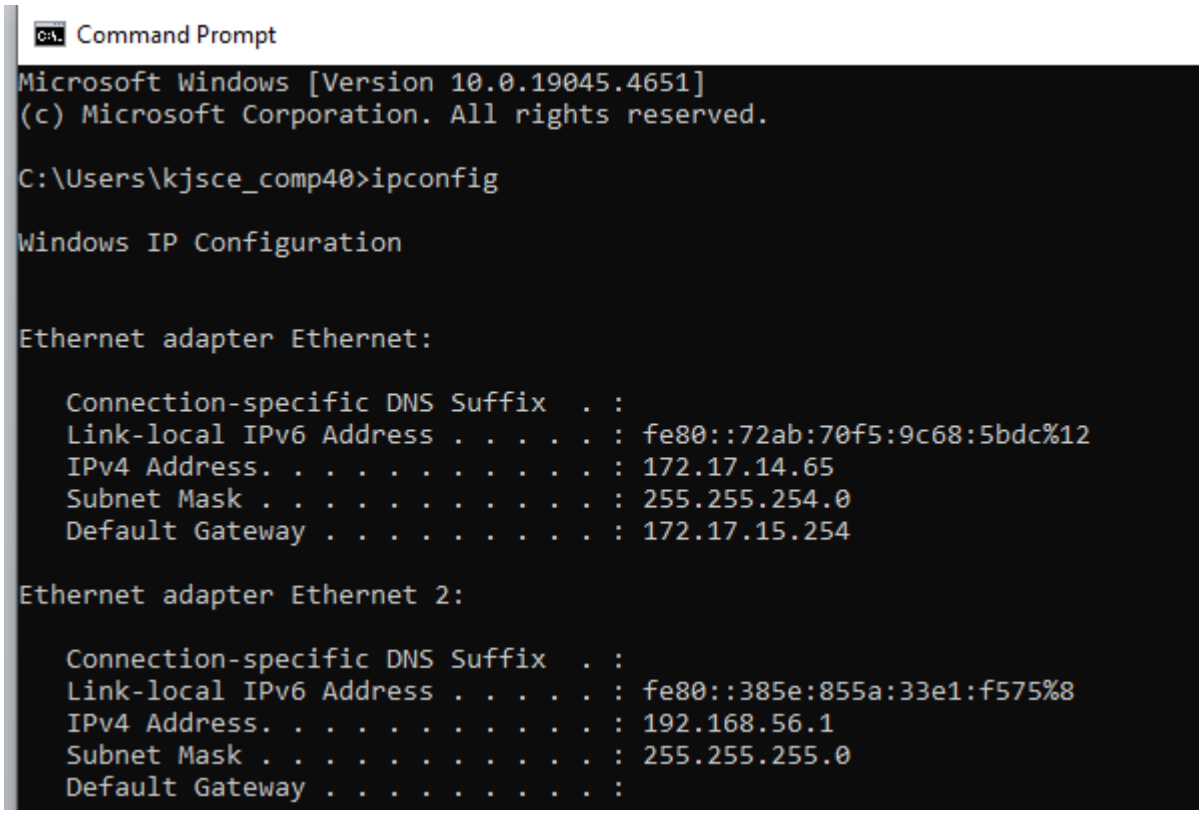
12. SYSTEMINFO

Display information about a system.

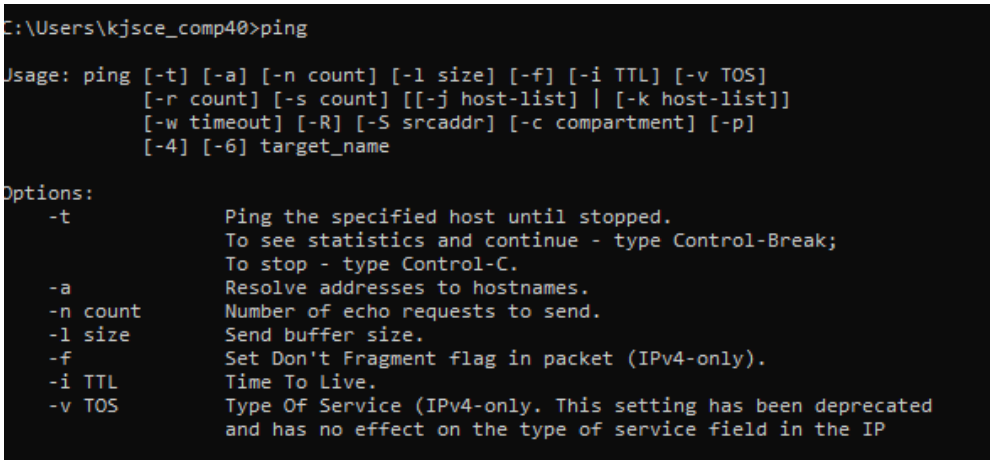
IMPLEMENTATION:

Show the use of different network commands:-

1) IPCONFIG



2) PING



3) TRACERT

```
C:\Users\kjsce_comp40>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

4) NETSTAT command

```
C:\Users\kjsce_comp40> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:11300        16DCEB216-15:49965     ESTABLISHED
  TCP    127.0.0.1:11300        16DCEB216-15:49993     ESTABLISHED
  TCP    127.0.0.1:49965        16DCEB216-15:11300     ESTABLISHED
  TCP    127.0.0.1:49993        16DCEB216-15:11300     ESTABLISHED
  TCP    172.17.14.65:7680      10.0.143.110:58019     TIME_WAIT
  TCP    172.17.14.65:7680      16DCEB210B-01:50233    TIME_WAIT
  TCP    172.17.14.65:49818     20.198.162.78:https    ESTABLISHED
  TCP    172.17.14.65:50066     sd-in-f188:5228        ESTABLISHED
  TCP    172.17.14.65:50175     bom07s31-in-f14:https  ESTABLISHED
  TCP    172.17.14.65:50176     bom12s12-in-f14:https  ESTABLISHED
  TCP    172.17.14.65:50177     bom07s36-in-f10:https  ESTABLISHED
  TCP    172.17.14.65:50178     bom07s36-in-f10:https  ESTABLISHED
  TCP    172.17.14.65:50187     bom07s16-in-f14:https  TIME_WAIT
  TCP    172.17.14.65:50188     bom07s29-in-f5:https   ESTABLISHED
  TCP    172.17.14.65:50218     bom07s29-in-f3:https   ESTABLISHED
  TCP    172.17.14.65:50229     bom07s29-in-f3:https   ESTABLISHED
  TCP    172.17.14.65:50332     ec2-3-111-151-190:https  ESTABLISHED
  TCP    172.17.14.65:50490     bom07s26-in-f10:https  TIME_WAIT
  TCP    172.17.14.65:50567     13.107.213.254:https   CLOSE_WAIT
  TCP    172.17.14.65:50575     13.107.253.254:https   CLOSE_WAIT
  TCP    172.17.14.65:50576     13.107.246.254:https   CLOSE_WAIT
  TCP    172.17.14.65:50611     bom05s12-in-f3:https   TIME_WAIT
  TCP    172.17.14.65:50635     151.101.193.91:https   ESTABLISHED
  TCP    172.17.14.65:50639     sd-in-f84:https        TIME_WAIT
  TCP    172.17.14.65:50663     bom05s11-in-f3:https   TIME_WAIT
  TCP    172.17.14.65:50672     sc-in-f84:https        ESTABLISHED
  TCP    172.17.14.65:50681     a23-58-93-162:https    CLOSE_WAIT
  TCP    172.17.14.65:50682     a23-58-93-130:https    CLOSE_WAIT
```

5) DIG:- Does not work on Windows Shell.

6) NSLOOKUP

```
C:\Users\kjsce_comp40>nslookup
Default Server:  svvpdc.svv.local
Address:  172.31.0.25
```

7) ROUTE

```
C:\Users\kjsce_comp40>nslookup
Default Server:  svvpdc.svv.local
Address:  172.31.0.25

> route
Server:  svvpdc.svv.local
Address:  172.31.0.25

*** svvpdc.svv.local can't find route: Non-existent domain
>
```

8) ARP

```
C:\Users\kjsce_comp40>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

9) ETHTOOL:- Does not work on Windows Shell.

10) TELNET :- Does not work on Windows Shell.

11) HOSTNAME

```
C:\Users\kjsce_comp40>hostname
16DCEB216-15
```

12) SYSTEMINFO

```
C:\Users\kjsce_comp40>systeminfo

Host Name:                 16DCEB216-15
OS Name:                   Microsoft Windows 10 Pro for Workstations
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Exam
Registered Organization:
Product ID:                00391-90090-00000-AA701
Original Install Date:     14-06-2024, 14:01:53
System Boot Time:          29-07-2024, 14:05:02
System Manufacturer:       LENOVO
System Model:              10HJA02AHF
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineIntel ~3500 Mhz
BIOS Version:              LENOVO FCKT99AUS, 18-11-2020
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     8,105 MB
Available Physical Memory: 4,209 MB
Virtual Memory: Max Size:  9,385 MB
Virtual Memory: Available: 5,559 MB
Virtual Memory: In Use:    3,826 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    SVV.local
```

CONCLUSION:- Network configuration commands are crucial for managing and troubleshooting network settings. On Windows, ipconfig provides interface details, netstat displays active connections, and tracert traces packet routes. For diagnostics, ping checks connectivity and nslookup queries DNS information. These tools help ensure proper network functionality and resolve issues.