Batch: D2	Roll No.: 16010123325
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 HostListThe 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.

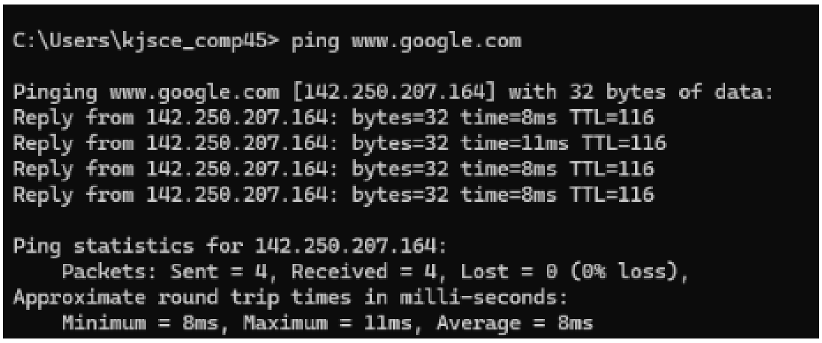
# hostname

12. SYSTEMINFO

Display information about a system.

IMPLEMENTATION:

1. Ping :- The ping command is a network administration utility used to test the reachability of a host

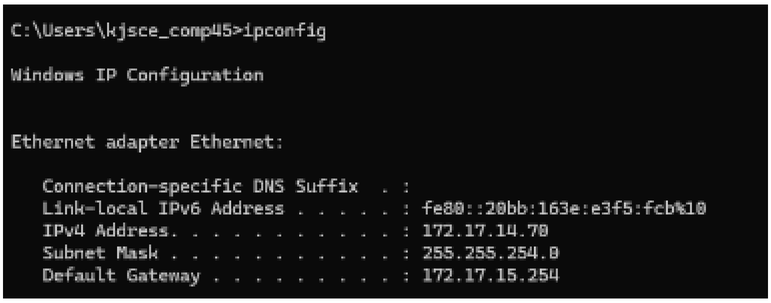


```
C:\Users\kjsce_comp45> ping www.google.com

Pinging www.google.com [142.250.207.164] with 32 bytes of data:
Reply from 142.250.207.164: bytes=32 time=8ms TTL=116
Reply from 142.250.207.164: bytes=32 time=11ms TTL=116
Reply from 142.250.207.164: bytes=32 time=8ms TTL=116
Reply from 142.250.207.164: bytes=32 time=8ms TTL=116

Ping statistics for 142.250.207.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 11ms, Average = 8ms
```

2. Ipconfig :- Displays all current TCP/IP network configuration values



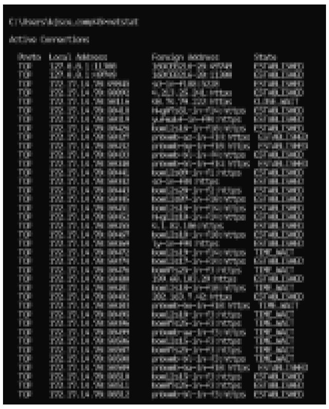
```
C:\Users\kjsce_comp45>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::20bb:163e:e3f5:fcb%10
   IPv4 Address. . . . . . . . . . . : 172.17.14.70
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.17.15.254
```

3. Netstat :- The netstat command, short for network statistics, is a command-line utility used to display various network-related information.

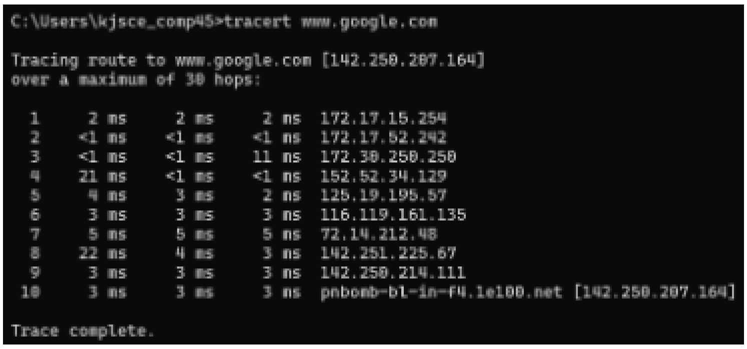


```
C:\Users\kjsce_comp45>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  [illegible]
```

4. Traceroute :- The traceroute command attempts to trace the route an IP packet follows to an Internet host



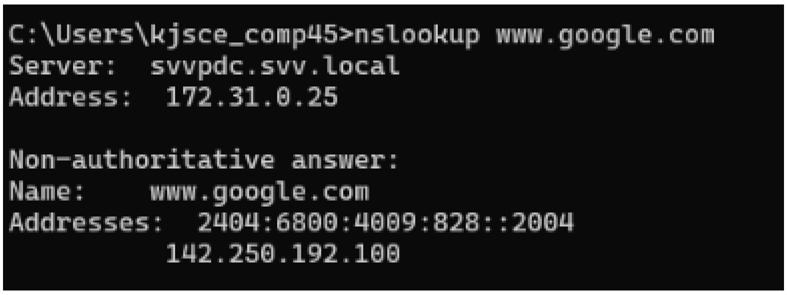
```
C:\Users\kjsce_comp45>tracert www.google.com

Tracing route to www.google.com [142.250.207.164]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  172.17.15.254
  2    <1 ms    <1 ms    <1 ms  172.17.52.242
  3    <1 ms    <1 ms    11 ms  172.30.250.250
  4    21 ms    <1 ms    <1 ms  152.52.34.129
  5     4 ms     3 ms     2 ms  125.19.195.57
  6     3 ms     3 ms     3 ms  116.119.161.135
  7     5 ms     5 ms     5 ms  72.14.212.48
  8    22 ms     4 ms     3 ms  142.251.225.67
  9     3 ms     3 ms     3 ms  142.250.214.111
 10     3 ms     3 ms     3 ms  pnbomb-bl-in-f4.1e100.net [142.250.207.164]

Trace complete.
```

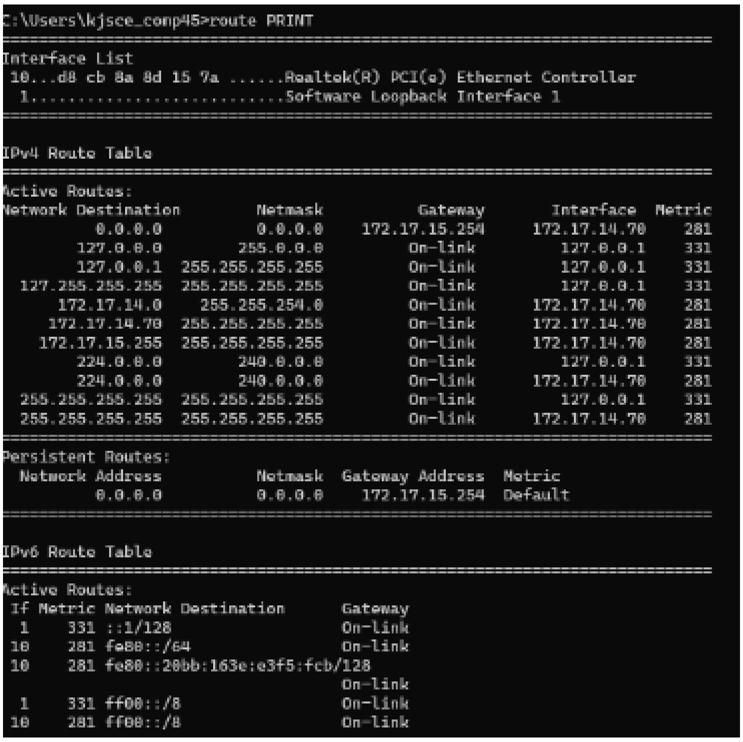
5. Nslookup :- The nslookup command is a command-line utility used for querying the Domain Name System (DNS) to obtain information about domain names, IP addresses, and other DNS records.



```
C:\Users\kjsce_comp45>nslookup www.google.com
Server:  svvpdc.svv.local
Address:  172.31.0.25

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:828::2004
          142.250.192.100
```

7. Route :- The route command is used to view and manipulate the IP routing table.

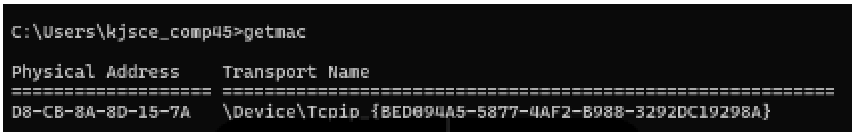


```
C:\Users\kjsce_comp45>route PRINT
===========================================================================
Interface List
 10...d8 cb 8a 8d 15 7a ......Realtek(R) PCI(e) Ethernet Controller
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.17.15.254    172.17.14.70    281
        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
      172.17.14.0    255.255.254.0         On-link     172.17.14.70    281
     172.17.14.70  255.255.255.255         On-link     172.17.14.70    281
    172.17.15.255  255.255.255.255         On-link     172.17.14.70    281
        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     172.17.14.70    281
  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     172.17.14.70    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0    172.17.15.254  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 10    281 fe80::/64                On-link
 10    281 fe80::20bb:163e:e3f5:fcb/128
                                    On-link
  1    331 ff00::/8                 On-link
 10    281 ff00::/8                 On-link
```

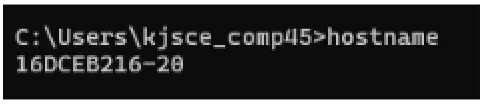
8. Getmac :- The getmac command is a built-in Windows command-line utility used to display the Media Access Control (MAC) address of a computer's network adapters.



```
C:\Users\kjsce_comp45>getmac

Physical Address    Transport Name
=================== ==========================================================
D8-CB-8A-8D-15-7A   \Device\Tcpip_{BED094A5-5877-4AF2-B988-3292DC19298A}
```

9. Hostname :- The hostname command is used to display or set the name of the current host system.



```
C:\Users\kjsce_comp45>hostname
16DCEB216-20
```

CONCLUSION:

Learned about network commands .

Post Lab Questions

1. What does the command ping -n 5 www.example.com do on a Windows system?

A. Sends 5 ICMP echo requests to www.example.com
B. Resolves the domain name 5 times
C. Pings 5 different IP addresses of www.example.com
D. Sends 5 TCP packets to www.example.com

2. Which command is used to display all active network connections and listening ports in Windows?

A. ipconfig /all
B. netstat -an
C. tracert
D. arp -a

3. On a Linux system, what does the ip a command display?

A. Active TCP connections
B. IP address configuration of all interfaces
C. Routing table
D. DNS server settings

4. Which command would you use to test DNS resolution for a domain in Linux?

A. ping
B. netstat
C. dig
D. traceroute

5. What does the traceroute command help you identify?

A. The MAC address of a remote host
B. The DNS server used by your system
C. The path packets take to reach a destination
D. The number of open ports on a host

6. Which command in Windows resets the TCP/IP stack to its default state?
A. ipconfig /renew
B. netsh int ip reset
C. ping localhost
D. netstat -r

7. What does the arp -a command display?
A. All active TCP connections
B. IP addresses and their MAC address mappings
C. DNS cache entries
D. Routing table entries

8. Which Linux command is used to monitor real-time network traffic on an interface?
A. netstat -i
B. tcpdump
C. ip monitor
D. iftop

9. What does ipconfig /flushdns do in Windows?
A. Clears the routing table
B. Resets the IP address
C. Clears the DNS resolver cache
D. Releases the DHCP lease

10. Which command would you use to test connectivity to a specific port on a remote server?
A. ping
B. netstat
C. telnet
D. ipconfig