

Department of Computer Engineering

Batch: A1 Roll No.: 16010123012

Experiment / assignment / tutorial No.: 02

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

Department of Computer Engineering

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

Department of Computer Engineering

Department of Computer Engineering

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

Department of Computer Engineering

Department of Computer Engineering

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.

Department of Computer Engineering

Department of Computer Engineering

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

Department of Computer Engineering

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:

1. IPCONFIG

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::34dd:6a48:4a88:4ba8%6
IPv4 Address . . . . . : 172.17.14.25
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 172.17.15.254
```

2. PING

```
C:\>ping 172.17.14.25

Pinging 172.17.14.25 with 32 bytes of data:
Reply from 172.17.14.25: bytes=32 time<1ms TTL=128

Ping statistics for 172.17.14.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Department of Computer Engineering

3. TRACEROUTE/ TRACERT

```
C:\>tracert -d
A target name or address must be specified.

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.
```

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

Tracing route to www.google.com [142.251.220.36]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms  172.17.15.254
  2      <1 ms     <1 ms     <1 ms  172.17.52.242
  3      <1 ms     <1 ms     <1 ms  172.30.250.250
  4      2 ms      1 ms      1 ms  14.142.143.97.static-mumbai.vsnl.net.in [14.142.143.97]
  5      2 ms      2 ms      2 ms  115.113.165.98.static-mumbai.vsnl.net.in [115.113.165.98]
  6      3 ms      2 ms      2 ms  142.251.225.9
  7      6 ms      3 ms      1 ms  142.251.70.57
  8     16 ms      6 ms      2 ms  pnbomb-ba-in-f4.1e100.net [142.251.220.36]

Trace complete.
```

4. DIG

```
C:\>dig
'dig' is not recognized as an internal or external command,
operable program or batch file.
```

Department of Computer Engineering

5. NETSTAT

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:11300        16DCEB217-15:49913    ESTABLISHED
  TCP    127.0.0.1:49913        16DCEB217-15:11300    ESTABLISHED
  TCP    172.17.14.25:49823    4.213.25.241:https   ESTABLISHED
  TCP    172.17.14.25:50101    se-in-f188:5228      ESTABLISHED
  TCP    172.17.14.25:50791    23.217.111.25:https  CLOSE_WAIT
  TCP    172.17.14.25:50792    104.208.16.92:https  CLOSE_WAIT
  TCP    172.17.14.25:50794    204.79.197.254:https CLOSE_WAIT
  TCP    172.17.14.25:50799    150.171.31.254:https CLOSE_WAIT
  TCP    172.17.14.25:50800    204.79.197.222:https CLOSE_WAIT
  TCP    172.17.14.25:50801    4.150.240.254:https CLOSE_WAIT
  TCP    172.17.14.25:50811    pnbomb-bk-in-f14:https ESTABLISHED
  TCP    172.17.14.25:50812    pnbomb-bb-in-f14:https ESTABLISHED
  TCP    172.17.14.25:50813    pnbomb-bp-in-f3:https ESTABLISHED
  TCP    172.17.14.25:50821    bom12s12-in-f10:https ESTABLISHED
  TCP    172.17.14.25:50824    bom12s20-in-f10:https ESTABLISHED
  TCP    172.17.14.25:50827    pnbomb-bp-in-f3:https ESTABLISHED
  TCP    172.17.14.25:50867    bom12s19-in-f5:https ESTABLISHED
  TCP    172.17.14.25:50900    pnbomb-bp-in-f10:https ESTABLISHED
  TCP    172.17.14.25:50920    bom12s19-in-f10:https ESTABLISHED
  TCP    172.17.14.25:50973    bom12s16-in-f10:https ESTABLISHED
  TCP    172.17.14.25:50975    pnbomb-bo-in-f10:https TIME_WAIT
  TCP    172.17.14.25:50976    sd-in-f84:https       TIME_WAIT
  TCP    172.17.14.25:50986    4.1.82.185:https     ESTABLISHED
```

6. NSLOOKUP

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

C:\>nslookup google.com
Server:  svvpdc.svv.local
Address:  172.31.0.25

Non-authoritative answer:
Name:      google.com
Addresses: 2404:6800:4009:830::200e
          142.251.42.46
```

Department of Computer Engineering

7. ROUTE

```
C:\>route PRINT
=====
Interface List
  6...44 8a 5b 57 26 7c .....Realtek PCIe GbE Family 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  172.17.14.25  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        172.17.14.25  281
          172.17.14.25     255.255.255.255  On-link        172.17.14.25  281
          172.17.15.255    255.255.255.255  On-link        172.17.14.25  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        172.17.14.25  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        172.17.14.25  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
  6    281 fe80:::/64         On-link
  6    281 fe80::34dd:6a48:4a88:4ba8/128
                           On-link
  1    331 ff00::/8          On-link
  6    281 ff00::/8          On-link
=====
Persistent Routes:
  None
```

Department of Computer Engineering

```
C:\>route PRINT -4
=====
Interface List
 6...44 8a 5b 57 26 7c ....Realtek PCIe GbE Family 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  172.17.14.25    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        172.17.14.25    281
         172.17.14.25  255.255.255.255  On-link        172.17.14.25    281
         172.17.15.255 255.255.255.255  On-link        172.17.14.25    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        172.17.14.25    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        172.17.14.25    281
=====
Persistent Routes:
Network Address      Netmask     Gateway Address Metric
          0.0.0.0        0.0.0.0   172.17.15.254 Default
=====
```

8. ARP

```
C:\>arp -a

Interface: 172.17.14.25 --- 0x6
  Internet Address        Physical Address      Type
  172.17.15.254           b0-aa-77-66-d1-41  dynamic
  172.17.15.255           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
  239.193.0.1              01-00-5e-41-00-01  static
  239.193.0.2              01-00-5e-41-00-02  static
  239.193.0.7              01-00-5e-41-00-07  static
  239.255.255.250          01-00-5e-7f-ff-fa  static
  255.255.255.255          ff-ff-ff-ff-ff-ff  static
```

Department of Computer Engineering

9. ETHTOOL

```
C:\>ethtool  
'ethtool' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\>ethtool eth0  
'ethtool' is not recognized as an internal or external command,  
operable program or batch file.
```

10. TELNET

```
C:\>telnet Aaryan  
'telnet' is not recognized as an internal or external command,  
operable program or batch file.
```

11. HOSTNAME

```
C:\>hostname  
16DCEB217-15
```

```
C:\>hostname  
Aaryan
```

12. GETMAC

```
C:\>getmac  
  
Physical Address      Transport Name  
=====  =====  
44-8A-5B-57-26-7C    \Device\Tcpip_{385D4BE6-7076-433C-AC9F-6D42681B3D4C}
```

Department of Computer Engineering

13. SYSTEMINFO

```
C:\>systeminfo

Host Name: 16DCEB217-15
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: ROB-03
Registered Organization:
Product ID: 00391-90090-00000-AA791
Original Install Date: 15-02-2024, 14:48:18
System Boot Time: 31-07-2025, 14:02:23
System Manufacturer: LENOVO
System Model: 10ASAB11IG
System Type: x64-based PC
Processor(s):
  1 Processor(s) Installed.
  [01]: Intel64 Family 6 Model 60 Stepping 3 GenuineIntel ~3700 Mhz
  LENOVO FCKT50AUS, 03-04-2014
BIOS Version:
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: 00000409
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 8,095 MB
Available Physical Memory: 3,684 MB
Virtual Memory: Max Size: 9,375 MB
Virtual Memory: Available: 4,673 MB
Virtual Memory: In Use: 4,702 MB
Page File Location(s): C:\pagefile.sys
Domain: SVV.local
Logon Server: \\SVVPDC
Hotfix(s):
  18 Hotfix(s) Installed.
  [01]: KB5056578
  [02]: KB5034468
  [03]: KB5011048
  [04]: KB5015684
  [05]: KB5062554
  [06]: KB5032907
  [07]: KB5034224
  [08]: KB5036447
  [09]: KB5037818
  [10]: KB5039336
  [11]: KB5041579
  [12]: KB5043935
  [13]: KB5043130
  [14]: KB5046823
  [15]: KB5050388
  [16]: KB5052916
  [17]: KB5054682
  [18]: KB5063706
Network Card(s):
  1 NIC(s) Installed.
  [01]: Realtek PCIe GbE Family Controller
    Connection Name: Ethernet
    DHCP Enabled: No
    IP address(es)
      [01]: 172.17.14.25
      [02]: fe80::34dd:6a48:4a88:4ba8
Hyper-V Requirements:
  VM Monitor Mode Extensions: Yes
  Virtualization Enabled In Firmware: No
  Second Level Address Translation: Yes
  Data Execution Prevention Available: Yes
```

CONCLUSION:

I have successfully completed the experiment on basic network administration commands and network configuration. Through this experiment, I learned to use essential networking commands such as ping, traceroute, nslookup, netstat, arp, route, telnet, and others to test connectivity, troubleshoot network issues, analyze routing tables, and obtain system and DNS information.

Post Lab Questions

- 1. Give details of minimum 5 commands which are not included in the write-up.**
 - a. curl - Used to fetch or test data from websites and servers
 - b. wget – Helps download files directly from the internet
 - c. ssh – Lets us securely log in and work on another computer over the network
 - d. ftp – Transfers files between local and remote systems
 - e. scp – Securely copies files from one computer to another
- 2. Give the reason why some commands are not working in the Lab.**
 - a. They require administrator/sudo rights to run.
 - b. The service isn't running on the target machine (for example, telnet)
 - c. Firewall or network restrictions may be blocking them.