

**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**

**R**oute 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:**

**Show the use of different network commands:**

Microsoft Windows [Version 10.0.18363.418]

(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\kjsce\_comp10>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::80a:19b6:68b7:c111%6

IPv4 Address. . . . . . . . . . . : 172.17.14.20

Subnet Mask . . . . . . . . . . . : 255.255.254.0

Default Gateway . . . . . . . . . : 172.17.15.254

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::490f:5:dfde:4b4e%15

IPv4 Address. . . . . . . . . . . : 192.168.56.1

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . :

C:\Users\kjsce\_comp10>ping 127.17.14.23

Pinging 127.17.14.23 with 32 bytes of data:

Reply from 127.17.14.23: bytes=32 time<1ms TTL=128

Reply from 127.17.14.23: bytes=32 time<1ms TTL=128

Reply from 127.17.14.23: bytes=32 time<1ms TTL=128

Reply from 127.17.14.23: bytes=32 time<1ms TTL=128

Ping statistics for 127.17.14.23:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kjsce\_comp10>traceroute 127.17.14.23

'traceroute' is not recognized as an internal or external command,

operable program or batch file.

C:\Users\kjsce\_comp10>tracert 127.17.12.23

Tracing route to 127.17.12.23 over a maximum of 30 hops

1 <1 ms <1 ms <1 ms 127.17.12.23

Trace complete.

C:\Users\kjsce\_comp10>netstat

Active Connections

Proto Local Address Foreign Address State

TCP 172.17.14.20:49998 sc-in-f188:5228 ESTABLISHED

TCP 172.17.14.20:50072 bom12s18-in-f14:https ESTABLISHED

TCP 172.17.14.20:50083 bom12s17-in-f14:https ESTABLISHED

TCP 172.17.14.20:50102 maa03s45-in-f10:https ESTABLISHED

TCP 172.17.14.20:50116 20.198.118.190:https ESTABLISHED

TCP 172.17.14.20:50148 a23-207-180-137:https TIME\_WAIT

TCP 172.17.14.20:50204 sg-in-f113:https ESTABLISHED

TCP 172.17.14.20:50215 bom07s33-in-f14:https ESTABLISHED

TCP 172.17.14.20:50216 bom07s30-in-f3:https ESTABLISHED

TCP 172.17.14.20:50219 hkg12s10-in-f3:https ESTABLISHED

TCP 172.17.14.20:50220 hkg12s10-in-f3:https ESTABLISHED

TCP 172.17.14.20:50221 bom07s37-in-f14:https ESTABLISHED

TCP 172.17.14.20:50222 bom07s36-in-f3:https ESTABLISHED

TCP 172.17.14.20:50224 bom07s36-in-f1:https ESTABLISHED

TCP 172.17.14.20:50225 bom07s37-in-f14:https ESTABLISHED

TCP 172.17.14.20:50226 maa03s46-in-f14:https ESTABLISHED

TCP 172.17.14.20:50227 bom07s25-in-f13:https ESTABLISHED

TCP 172.17.14.20:50228 maa05s24-in-f10:https ESTABLISHED

TCP 172.17.14.20:50229 maa03s40-in-f4:https ESTABLISHED

TCP 172.17.14.20:50230 maa03s40-in-f4:https ESTABLISHED

TCP 172.17.14.20:50231 maa05s24-in-f10:https ESTABLISHED

TCP 172.17.14.20:50244 a-0001:https ESTABLISHED

TCP 172.17.14.20:50245 a-0001:https ESTABLISHED

TCP 172.17.14.20:50247 a122-252-138-234:https ESTABLISHED

TCP 172.17.14.20:50248 13.107.6.254:https ESTABLISHED

TCP 172.17.14.20:50249 13.107.253.48:https ESTABLISHED

TCP 172.17.14.20:50250 204.79.197.254:https ESTABLISHED

TCP 172.17.14.20:50251 204.79.197.222:https ESTABLISHED

TCP 172.17.14.20:50252 20.219.9.219:https TIME\_WAIT

C:\Users\kjsce\_comp10>nslookup www.google.com

Server: svvpdc.svv.local

Address: 172.31.0.25

Non-authoritative answer:

Name: www.google.com

Addresses: 2404:6800:4009:827::2004

142.250.195.132

C:\Users\kjsce\_comp10>arp -a

Interface: 172.17.14.20 --- 0x6

Internet Address Physical Address Type

172.17.14.52 d8-cb-8a-8d-20-aa dynamic

172.17.14.60 d8-cb-8a-8d-15-0f dynamic

172.17.14.66 d8-cb-8a-8d-10-b6 dynamic

172.17.15.254 b0-aa-77-66-d1-41 dynamic

172.17.15.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 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

Interface: 192.168.56.1 --- 0xf

Internet Address Physical Address Type

192.168.56.255 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

C:\Users\kjsce\_comp10>telnet 172.17.14.19

'telnet' is not recognized as an internal or external command,

operable program or batch file.

C:\Users\kjsce\_comp10>Enable-WindowsOptionalFeature -Online -FeatureName TelnetClient

'Enable-WindowsOptionalFeature' is not recognized as an internal or external command,

operable program or batch file.

C:\Users\kjsce\_comp10>hostname

16DCEB217-10

C:\Users\kjsce\_comp10>hostname 172.17.14.19

sethostname: Use the Network Control Panel Applet to set hostname.

hostname -s is not supported.

C:\Users\kjsce\_comp10>systeminfo

Host Name: 16DCEB217-10

OS Name: Microsoft Windows 10 Pro for Workstations

OS Version: 10.0.18363 N/A Build 18363

OS Manufacturer: Microsoft Corporation

OS Configuration: Member Workstation

OS Build Type: Multiprocessor Free

Registered Owner: ROB-03

Registered Organization:

Product ID: 00391-90090-60463-AA574

Original Install Date: 08-09-2022, 11:23:37

System Boot Time: 01-08-2023, 05:30:52

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 FCKT69AUS, 10-04-2015

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: 3,403 MB

Virtual Memory: Max Size: 9,385 MB

Virtual Memory: Available: 4,011 MB

Virtual Memory: In Use: 5,374 MB

Page File Location(s): C:\pagefile.sys

Domain: SVV.local

Logon Server: \\SVVPDC

Hotfix(s): 7 Hotfix(s) Installed.

[01]: KB4601556

[02]: KB4513661

[03]: KB4516115

[04]: KB4517245

[05]: KB4521863

[06]: KB4577586

[07]: KB4517389

Network Card(s): 2 NIC(s) Installed.

[01]: Realtek PCIe GbE Family Controller

Connection Name: Ethernet

DHCP Enabled: No

IP address(es)

[01]: 172.17.14.20

[02]: fe80::80a:19b6:68b7:c111

[02]: VirtualBox Host-Only Ethernet Adapter

Connection Name: VirtualBox Host-Only Network

DHCP Enabled: No

IP address(es)

[01]: 192.168.56.1

[02]: fe80::490f:5:dfde:4b4e

Hyper-V Requirements: VM Monitor Mode Extensions: Yes

Virtualization Enabled In Firmware: No

Second Level Address Translation: Yes

Data Execution Prevention Available: Yes

C:\Users\kjsce\_comp10>nslookup

Default Server: svvpdc.svv.local

Address: 172.31.0.25

> ww.google.com

Server: svvpdc.svv.local

Address: 172.31.0.25

Non-authoritative answer:

Name: www3.l.google.com

Addresses: 2404:6800:4009:80a::200e

172.217.160.174

Aliases: ww.google.com

**CONCLUSION:** Thus we have understood the working of various networking commands. We used windows platform to execute various commands that give information about the network. We found out the IP address, mac address of devices. From these commands we can get information about various aspects of the network like number of jumps and route to another device.