Program 1: Familiarity with basics of network configuration files and networking commands in Linux - ifconfig, netstat, ping, arp, telnet, ftp, finger.

Program Objective:

Understanding and using of commands like ifconfig, netstat, ping, arp, telnet, ftp, finger, traceroute, whois

Program Description:

UNIX utilities are commands that, generally, perform a single task. It may be as simple as printing the date and time, or a complex as finding files that match many criteria throughout a directory hierarchy

IFCONFIG

The Unix command **ifconfig** (short for **i**nter**f**ace **config**urator) serves to configure and control TCP/IP network interfaces from a command line interface (CLI).

Common uses for ifconfig include setting an interface's IP address and netmask, and disabling or enabling a given interface. On some Unix-like operating systems, ifconfig is used to configure, or view the configuration of, a network interface.

Type ipconfig/all to see detailed configuration information for all network adapters configured on the computer.

The **ipconfig** (short for IP Configuration) is a basic, yet popular, Windows network command-line utility used to display the TCP/IP network configuration of a computer. If you are familiar with Linux, this tool is similiar to ifconfig. This tool is often used for troubleshooting network connectivity issues. With ipconfig, you can identify the types of network adapaters on your computer, the computer's IP address, the IP addresses of the DNS (Domain Name System) servers being used, and much more.

ifconfig -a

Displays the configuration of all interfaces, both active and inactive.

NETSTAT

netstat (**net**work **stat**istics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics.

It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

Parameters

Parameters used with this command must be prefixed with a hyphen (-) rather than a slash (/).

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

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

-f : Displays fully qualified domain names <FQDN> for foreign addresses.

-i : Displays network **i**nterfaces and their statistics (not available under Windows)

-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 Linux: **P**rocess : Show which processes are using which sockets

PING

Ping is a computer network tool used to test whether a particular host is reachable across an IP network; it is also used to self-test the network interface card of the computer, or as a speed test. It works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. Ping does not estimate the round-trip time, as it does not factor in the user's connection speed, but instead is used to record any packet loss, and print a statistical summary when finished.

The word *ping* is also frequently used as a verb or noun, where it is usually incorrectly used to refer to the round-trip time, or measuring the round-trip time. The ping command can be used to test end-to-end connectivity between two host devices. It measures the round-trip time for a message to get from source to destination. The ping command can be used to verify the connectivity between two network devices that are IP (Internet Protocol) based.

ARP

In computer networking, the **Address Resolution Protocol** (**ARP**) is the method for finding a host's link layer (hardware) address when only its Internet Layer (IP) or some other Network Layer address is known.

ARP has been implemented in many types of networks; it is not an IP-only or Ethernet-only protocol. It can be used to resolve many different network layer protocol addresses to interface hardware addresses, although, due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses.

How to Use ARP to Find a MAC Address

In Windows, Linux, and other operating systems, the command line utility ARP (Address Resolution Protocol) shows local MAC address information stored in the ARP cache. However, it only works within the small group of computers on a local area network (LAN), not across the internet.

ARP is intended to be used by system administrators, and it is not typically a useful way to track down computers and people on the internet.

TCP/IP computer networks use both the IP addresses and MAC addresses of connected client devices. While the IP address changes over time, the MAC address of a network adapter always stays the same.

Start by pinging the device you want the MAC to address for:

ping 192.168.86.45

The ping command establishes a connection with the other device on the network and should show a result like this:

Pinging 192.168.86.45 with 32 bytes of data:
Reply from 192.168.86.45: bytes=32 time=290ms TTL=128
Reply from 192.168.86.45: bytes=32 time=3ms TTL=128
Reply from 192.168.86.45: bytes=32 time=176ms TTL=128Reply from 192.168.86.45: bytes=32 time=3ms TTL=128

Use the following ARP command to get a list that shows the MAC address of the device you pinged:

arp -a

The results may look something like this but probably with many other entries:

Interface: 192.168.86.38 --- 0x3
Internet Address Physical Address Type
192.168.86.1 70-3a-cb-14-11-7a dynamic
192.168.86.45 98-90-96-B9-9D-61 dynamic
192.168.86.255 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
Find the device's IP address in the list. The MAC address is shown right next to it. In this example, the IP address is 192.168.86.45, and its MAC address is 98-90-96-B9-9D-61.

TELNET
Telnet (**Tel**ecommunication **net**work) is a network protocol used on the Internet or local area network (LAN) connections. In Linux, the telnet command is used to create a remote connection with a system over a TCP/IP network.
Typically, telnet provides access to a command-line interface on a remote machine.
The term *telnet* also refers to software which implements the client part of the protocol. Telnet clients are available for virtually all platforms.

Protocol details:
Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically this protocol is used to establish a connection to TCP port 23

FTP
File Transfer Protocol (**FTP**):
FTP is a network protocol used to transfer data from one computer to another through a network such as the Internet.FTP is a file transfer protocol for exchanging and manipulating files over a TCP computer network. An FTP client may connect to an FTP server to manipulate files on that server.FTP runs over TCP. It defaults to listen on port 21 for incoming connections from FTP clients. A connection to this port from the FTP Client forms the control stream on which commands are passed from the FTP client to the FTP server and on occasion from the FTP server to the FTP client. FTP uses out-of-band control, which means it uses a separate connection for control and data. Thus, for the actual file transfer to take place, a different connection is required which is called the data stream.
To establish an FTP connection to a remote system, use the ftp command with the remote system's IP address:

ftp [IP]

For instance, connecting to a remote server with the IP address 192.168.100.9:

ftp 192.168.100.9

FINGER:
In computer networking, the **Name/Finger protocol** and the **Finger user information protocol** are simple network protocols for the exchange of human-oriented status and user information.

Finger command is a user information lookup command which gives details of all the users logged in. This tool is generally used by system administrators. It provides details like login name, user name, idle time, login time, and in some cases their email address even.

finger -p ch
Display information about the user ch. Output appears similar to the following:

Login name: admin
In real life: Computer Hope
On since Feb 11 23:37:16 on pts/7 from domain.computerhope.com
28 seconds Idle Time
Unread mail since Mon Feb 12 00:22:52 2001

TRACEROUTE:
traceroute is a computer network tool used to determine the route taken by packets across an IP network . An IPv6 variant, **traceroute6**, is also widely available. Traceroute is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network. This can help identify routing problems or firewalls that may be blocking access to a site. Traceroute is also used by penetration testers to gather information about network infrastructure and IP ranges around a given host. It can also be used when downloading data, and if there are multiple mirrors available for the same piece of data, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

In other words, traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

The traceroute command in Windows is ***tracert***. On a Linux system, the command is *traceroute*.
A typical tracert on a Windows machine would look like the following.

tracert www.google.com
Tracing route to www.google.com [74.125.227.179]
over a maximum of 30 hops:
1 1 ms <1 ms 1 ms 192.168.1.1
2 7 ms 6 ms 6 ms 10.10.1.2
3 7 ms 8 ms 7 ms 10.10.1.45
4 9 ms 8 ms 8 ms 10.10.25.45
5 9 ms 10 ms 9 ms 10.10.85.99
6 11 ms 51 ms 10 ms 10.10.64.2
7 11 ms 10 ms 10 ms 10.10.5.88
8 11 ms 10 ms 11 ms 216.239.46.248
9 12 ms 12 ms 12 ms 72.14.236.98
10 18 ms 18 ms 18 ms 66.249.95.231
11 25 ms 24 ms 24 ms 216.239.48.4
12 48 ms 46 ms 46 ms 72.14.237.213

13 50 ms 50 ms 50 ms 72.14.237.214
14 48 ms 48 ms 48 ms 64.233.174.137
15 47 ms 47 ms 46 ms dfw06s32-in-f19.1e100.net [74.125.227.179]
Trace complete.

For all additional options of traceroute, check the manual page in the terminal with the man command:

man traceroute

WHO IS:
WHOIS (pronounced "**who is**"; not an acronym) is a query/response protocol which is widely used for querying an official database in order to determine the owner of a domain name, an IP address, or an autonomous system number on the Internet. WHOIS lookups were traditionally made using a command line interface, but a number of simplified web-based tools now exist for looking up domain ownership details from different databases. WHOIS normally runs on TCP port 43.
The WHOIS system originated as a method that system administrators could use to look up information to contact other IP address or domain name administrators (almost like "white pages").

whois 216.58.206.46

The following results may also be obtained via:

https://whois.arin.net/rest/nets;q=216.58.206.46?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2

NetRange: 216.58.192.0 - 216.58.223.255

CIDR: 216.58.192.0/19

NetName: GOOGLE

NetHandle: NET-216-58-192-0-1

Parent: NET216 (NET-216-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS15169

Organization: Google LLC (GOGL)

RegDate: 2012-01-27

Updated: 2012-01-27

Ref: https://whois.arin.net/rest/net/NET-216-58-192-0-1

OrgName: Google LLC

OrgId: GOGL

Address: 1600 Amphitheatre Parkway

City: Mountain View

StateProv: CA

PostalCode: 94043

Country: US

RegDate: 2000-03-30

Updated: 2017-12-21

Ref: https://whois.arin.net/rest/org/GOGL ...

whois google.com

Domain Name: GOOGLE.COM

Registry Domain ID: 2138514_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2011-07-20T16:55:31Z

Creation Date: 1997-09-15T04:00:00Z

Registry Expiry Date: 2020-09-14T04:00:00Z

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895740

Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited

Name Server: NS1.GOOGLE.COM

Name Server: NS2.GOOGLE.COM

Name Server: NS3.GOOGLE.COM

Name Server: NS4.GOOGLE.COM