Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam - 603 110
(An Autonomous Institution, Affiliated to Anna University, Chennai)

UCS2511: NETWORKS LAB

Assignment 1: Network System Commands

Rohith M CSE-B

3122 21 5001 085 Date: 07-08-2023

Aim: To be proficient in executing various network system commands such as tcpdump, netstat, ifconfig, nslookup, traceroute, ping in the Linux environment.

1. ***tcpdump***

   This is a packet capture tool that can be used to view and analyze network traffic through a system. It can be used to troubleshoot network problems, analyze traffic and collect data for security analysis.

   Syntax: tcpdump [options][filter]

   Options: -a, -b, -c, -d, -e, -f, -h, -i, -l, -n, -p, -r, -s, -t, -D, -v, -w

   Examples:
   - ➔ tcpdump -D: lists all the network interfaces in the system.
   - ➔ tcpdump -i <interface>: captures the network traffic in the interface(port may be specified too).
   - ➔ tcpdump -w <filename>: Usually succeeded by another command like -i. The captured traffic is written in the given file.
   - ➔ tcpdump -a: captures all the packets in a network.
   - ➔ tcpdump -r <filename>: reads all the packets from the given file.

2. ***netstat***

   This is a command line tool that displays network connections, routing tables and interface statistics.

   Syntax: netstat [options]

   Options: -a, -b, -c, -d, -e, -f, -i, -l, -n, -o, -p, -q, -r, -s, -t, -u, -v

Examples:

- ➔ netstat -an: displays all the connections and listening ports in the system.
- ➔ netstat -bn: displays all active connections and listening ports, along with the executable that created the connection.
- ➔ netstat -e: displays all the ethernet statistics such as number of packets sent/received, number of bytes sent/received and number of errors.
- ➔ netstat -p tcp: displays all TCP connections, including the process ID (PID) of the process that owns the connection.
- ➔ netstat -q: displays a list of all TCP and UDP sockets that are currently listening for connections.

3. ifconfig

This is a system command that is used to configure network interfaces. It can be used to assign IP addresses, netmasks and broadcast addresses to network interfaces. It can also be used to disable network interfaces.

Syntax: ifconfig [options] [interface]

Options: -a, -b, -e, -f, -i, -l, -m, -n, -r, -s, -v

Examples:

- ➔ ifconfig -a: displays all active network interfaces in the system.
- ➔ ifconfig -m: displays the netmask for the network interface- a 32 bit number used to mask the IP address.
- ➔ ifconfig -s: displays the speed of the network interface, in bits/second.
- ➔ ifconfig -e <interface>: displays the Ethernet header for the specified network interface.
- ➔ ifconfig -f <interface>: displays the full configuration for the specified network interface. This includes the Ethernet header, the IP address, the netmask, the broadcast address, the MAC address, and other settings.

4. nslookup

This system command is used to query the Domain Name System(DNS). It can be used to find the IP address of the domain name, domain name of the IP address, and other DNS records.

Syntax: nslookup [options][host]

Options: -a, -c, -d, -h, -i, -l, -m, -n, -p, -r, -s, -t, -v, -w

Examples:

- ➔ nslookup -q <hostname>: queries the DNS for the IP address of the given hostname and lists the IP address and port of the DNS server and domain name.
- ➔ nslookup -d <IP_Address>: performs a reverse lookup to find the hostname for the IP address
- ➔ nslookup -m 4 <hostname>: performs a DNS query for the given hostname and specifies the maximum number of retries to 4.
- ➔ nslookup -r <hostname>: performs a recursive query to find the IP address for the given hostname.
- ➔ nslookup -v <hostname>: performs a DNS query for the given hostname and increases the verbosity of the output.

5. ***traceroute***

This is used to trace the path that a packet takes from the source to the destination. It does this by sending a series of ICMP Echo Request packets to the destination and then recording the IP addresses of the routes that the packets pass through.

Syntax: traceroute [options][host]

Options: -h, -i,-m, -n, -q, -r, -s, -t, -v, -w

Examples:

- ➔ traceroute -n <hostname>: traces the path of the hostname by displaying IP addresses of the routers in numeric form.
- ➔ traceroute -h: prints a help message that describes the syntax and options.
- ➔ traceroute -p N <hostname>: traces the path to the hostname and sends ICMP echo request packets to port N.
- ➔ traceroute <hostname> -q N: traces path to the hostname, but it will send only N packet(s) per hop. This is useful for troubleshooting.
- ➔ traceroute -t <IP_Address>: traces the path to the given IP address and sets the time to live, which is the number of hops a packet can travel before being dropped.

6. ***ping***

This is a command line tool that is used to test the reachability of a remote host. It does this by sending ICMP echo request packets to the remote host and then waiting for the ICMP echo reply packets to be returned.

Syntax: ping [options][host]

Options: -a, -b, -c, -d, -h, -i, -l, -n, -p, -r, -s, -t, -v, -w

Examples:

- ➔ ping -a <hostname>: pings the website and resolves the hostname to an IP address before sending ICMP echo request packets.
- ➔ ping -c N <hostname>: pings the given hostname N times and displays the IP address of the remote host, time taken for packets to travel, number of packets transmitted etc.
- ➔ ping -d <hostname>: pings the hostname and disables the ping's packet header, which has information about the ping like source and destination addresses. Raw data between the hosts can be viewed.
- ➔ ping -f <hostname>: pings the hostname and sets the Don't Fragment flag in the ICMP echo request packets. This flag tells routers to not fragment an incoming large packet.
- ➔ ping -l N <hostname>: pings the hostname and sets the size of the ICMP echo request packets to N bytes(default is 56 bytes).

Learning Outcomes:

- Learned the syntax and options for each command.
- Practiced using each command on a network environment.
- Understood how to troubleshoot network problems using the commands.