LAB 2: Practice on Basic Networking Commands (ifconfig/ipconfig, tcpdump, netstat, ip, hostname, route, tracert/traceroute)

Objective(s): To understand basic command line operation with Linux operating system and network configuration, testing and verification.

Background

ifconfig

ifconfig is used to configure, or view the configuration of, a network interface. ifconfig stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system. ifconfig displays information about all network interfaces currently in operation.

- eth0 is the first Ethernet interface. (Additional Ethernet interfaces would be named eth1, eth2, etc.) This type of interface is usually a NIC connected to the network by a category 5 cable.
- lo is the loopback interface. This is a special network interface that the system uses to communicate with itself.
- wlan0 is the name of the first wireless network interface on the system. Additional wireless interfaces would be named wlan1, wlan2, etc.

Options:

ifconfig	: View All Network Setting
ifconfig -a	: Display Information of All Network Interfaces
ifconfig eth0	: View Network Settings of Specific Interface
sudo ifconfig eth1 up	: Enable an Network Interface
sudo ifconfig wlan0 down	:Disable an Network Interface
sudo ifconfig wlan0 69.72.169.1	:Assign a IP Address to Network Interface
sudo ifconfig eth1 netmask 255.255.255.0	:Assign a Netmask to Network Interface
sudo ifconfig wlan1 broadcast 172.16.25.98	:How to Assign a Broadcast to Network Interface

ipconfig

The default is to display only the IP address, subnet mask and default gateway for each adapter bound to TCP/IP.For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed.

Options:

ipconfig /all	:To display all of your current IP information for all adapters.
ipconfig /release	:Use IPCONFIG release to release your current IP information and obtain a new IP Address from the DHCP server.
ipconfig /renew	:Use to IPCONFIG renew to renew your IP Address if you have it set to obtain IP Address automatically.
ipconfig /displaydns	:This shows your current DNS resolver cache logs

tcpdump

tcpdump is a most powerful and widely used command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that received or transferred over a network on a specific interface.

Options:

tcpdump -i eth0	:Capture Packets from Specific Interface
tcpdump -c 5 -i eth0	:Capture Only N Number of Packets
tcpdump -A -i eth0	:Print Captured Packets in ASCII
tcpdump -D	:Display Available Interfaces
tcpdump -XX -i eth0	:Display Captured Packets in HEX and ASCII
tcpdump -w 0001.pcap -i eth0	:Capture and Save Packets in a File
tcpdump -r 0001.pcap	:Read Captured Packets File
tcpdump -n -i eth0	:Capture IP address Packets
tcpdump -i eth0 tcp	:Capture only TCP Packets
tcpdump -i eth0 port 22	:Capture Packet from Specific Port
tcpdump -i eth0 src 192.168.0.2	:Capture Packets from source IP
tcpdump -i eth0 dst 50.116.66.139	:Capture Packets from destination IP

netstat

netstat can be used to view your active network connections and TCP/IP connections.

Options:

netstat -a	:Displays all active TCP connections. And TCP / UDP ports.
netstat -e	:Displays ethernet statistics.
netstat -b	:Displays all active programs that are listening.
netstat -f	:Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
netstat -n	:Displays addresses and port numbers in numerical form.
netstat -o	:Displays the owning process ID associated with each connection.
netstat -s	:Showing Statistics by Protocol
netstat -r	:Displaying Kernel IP routing

ip

IFCONFIG command is deprecated and replaced by IP command in Linux. However, IFCONFIG command is still works and available for most of the Linux distributions.

Options:

ip addr show	:How to Check an IP Address
ip addr del 192.168.50.5/24 dev eth1	:Remove an IP Address
ip link set eth1 up	:Enable Network Interface
ip link set eth1 down	:Disable Network Interface
ip route show	:Check Route Table information of a system

hostname

hostname command in Linux is used to obtain the DNS(Domain Name System) name and set the system's hostname or NIS(Network Information System) domain name.

Options:

hostname -a	: This option is used to get alias name of the host system(if any).
hostname -b	: Used to always set a hostname. Default name is used if none specified.
hostname -d	: This option is used to get the Domain if local domains are set.
hostname -f	: This option is used to get the Fully Qualified Domain Name(FQDN).
hostname -i	:This option is used to get the IP(network) addresses.
hostname -I	: This option is used to get all IP(network) addresses.
hostname -s	: This option is used to get the hostname in short.
hostname -V	: Gives version number as output.

route

Route command is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface.

Options:

route	: Display Existing Routes with hosts
route -n	: Display Existing Routes with numerical value (IP)
route add default gw 192.168.1.10	: Adding a Default Gateway
route add -host 192.168.1.51 reject	: Reject Routing to a Particular Host or Network

Tracert/Traceroute

It a command-line utility that we can use to trace the path that an Internet Protocol (IP) packet takes to its destination. The TRACERT diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

- e.g.
  tracert google.com
  tracert 216.58.196.131