|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Pratik Pujari** | | |
| **UID no.** | **2020300054** | **Class:** | **Comps C Batch** |
| **Experiment No.** | 2 | | |

|  |  |
| --- | --- |
| **AIM:** | To find the network utilities and its commands |
| **EXPERIMENT 1** | |
| **COMMANDS:** | **PING Command**  Most Linux users are familiar with the ping command and know how to use it in its basic form. However, there are many additional ping options and variations. In this guide, we will walk you through some of the most usefulLinux ping commands with examples.  The commands in this article work with any UNIX or Linux distribution.  The ping command allows you to:   * Test your internet connection. * Check if a remote machine is online. * Analyze if there are network issues, such as dropped packages or high latency.   When you try to “ping” a remote host, your machine starts sending ICMP echo requests and waits for a response. If the connection is established, you receive an echo reply for every request.  **How to Use the ping Command**  The basic ping syntax includes ping followed by a hostname, a name of a website, or the exact IP address.  ping [option] [hostname] or [IP address]  Hence, to check whether a remote host is up, in this case, *google.com*, type in your terminal:  ping google.com |
| **EXAMPLES:** | Example Pinging Google.com    Example Bing com |
| **COMMANDS:** | **ARP Command** On Linux operating systems, the arp command manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one, or display the current content.  ARP stands for Address Resolution Protocol, which is used to find the address of a network neighbor for a given IPv4 address.  Installing arp  Arp is part of the net-tools package. For example, on systems that use APT for package management, it can be installed with apt-get:  sudo apt-get update && sudo apt-get install net-tools |
| **EXAMPLES:** |  |
| **COMMANDS:** | **IFCONFIG** **Command**  ifconfig (interface configuration) is a network management tool. It is used to configure and view the status of the network interfaces in Linux operating systems. With ifconfig, you can assign IP addresses, enable or disable interfaces, manage ARP cache, routes, and more.  In this article, we’ll explore how to use the ifconfig command  **How to Use the ifconfig Command**  The basic syntax of the ifconfig command is shown below:  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]  Copy  Where:   * interface - is the name of the network interface. * address - is the IP address that you want to assign.   The configurations set with the ifconfig command are not persistent. After a system restart, all changes are lost. To make the changes permanent, you need to edit the distro-specific configuration files or add the commands to a startup script.  Only root or users with sudo privileges can configure network interfaces  **Assign an IP address and Netmask to a Network Interface**  With the ifconfig command, you can assign an IP address and netmask to a network interface.  Use the following syntax to assign the IP address and netmask:  ifconfig [interface-name] [ip-address] netmask [subnet-mask]  Copy  For example, to assign the IP address 192.168.0.101 and netmask 255.255.0.0 to the interface eth0, you would run:  ifconfig eth0 192.168.0.101 netmask 255.255.0.0Copy  You can also assign a secondary IP address to a network interface using the interface aliasing:  ifconfig eth0:0 192.168.0.102 netmask 255.255.0.0  **Enable and Disable a Network Interface**  Sometimes, you may need to reset the network interface. In this case, the ifconfig command can be used to enable or disable a network interface.  To disable an active network interface , enter the device name followed by the down flag:  ifconfig eth0 downCopy  To enable an inactive network interface, use the up flag:  ifconfig eth0 up |
| **EXAMPLES:** |  |
| **COMMANDS:** | **NSLOOKUP Command**  **nslookup**, which stands for "name server lookup", finds information about a named domain.  By default, **nslookup** translates a domain name to an IP address (or vice versa). For instance, to find the IP address of **microsoft.com**, you could run the command:  nslookup microsoft.com  Server: 8.8.8.8  Address: 8.8.8.8#53  Non-authoritative answer:  Name: microsoft.com  Address: 134.170.185.46  Name: microsoft.com  Address: 134.170.188.221  **Technical description**  **nslookup** is a program used to query Internet domain name servers for information.  **nslookup** has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts |
| **EXAMPLES:** |  |
| **COMMANDS:** | **Installing Net-tools on Linux:**  Netstat is part of a package named net-tools. You can get the net-tools package on Ubuntu with the command:  *$*sudo apt install net-tools    **Check Version of Netstat:**  Upon installation, check the installed version of Netstat:  *$*netstat –v    How to Use netstat on Linux |
| **EXAMPLES:** | **Netstat command in Linux:**  **Display Routing table:**  Netstat command shows the routing table detail on the terminal. If you wish to see the routing table, use the –nr flag with Netstat; it shows the kernel routing table in the same way that route does. Use the below command:  *$*netstat -nr    Instead of using symbolic address names, the -nr option allows Netstat to print addresses divided by dots |
| **COMMANDS:** | **TRACEROUTE Command**  Traceroute is a command used in network troubleshooting for mapping the path packets travel through the network. The tool aids in the discovery of possible routes of information from source to destination. Additionally, the command also helps calculate the transfer times between points    **How Does Traceroute Work?**  The protocol sends ICMP (Internet Control Message Protocol) packets to every router transferring between the source and destination. When you run a traceroute, the output displays:   * The IP address of the router that successfully received the packet. * The travel latency, or the amount of time it took to get a response for each of the three probes.   Traceroute acts as a series of ping commands. While ping requests a response from the destination, traceroute gathers the intermediate information as well.  Diagram of the traceroute iterations path  **Run a Traceroute on Linux**  On Ubuntu, the **traceroute** command is not available by default. Install the tool using the apt package manager.  1. Open the terminal (**CTLR**+**ALT**+**T**) and install traceroute with:  sudo apt install traceroute  2. In the terminal, run a traceroute with:  traceroute [options] <hostname or IP> [packet length]  For example, traceroute one of phoenixNAP's speed test IP locations:  traceroute 131.153.40.84 |
| **EXAMPLES:** |  |
| **RESULT:** I Learnt about the different network utilities and how to install it. We can type sudo app-get install to install different utilities easily  I learnt about the different pinging commands to trace a website | |