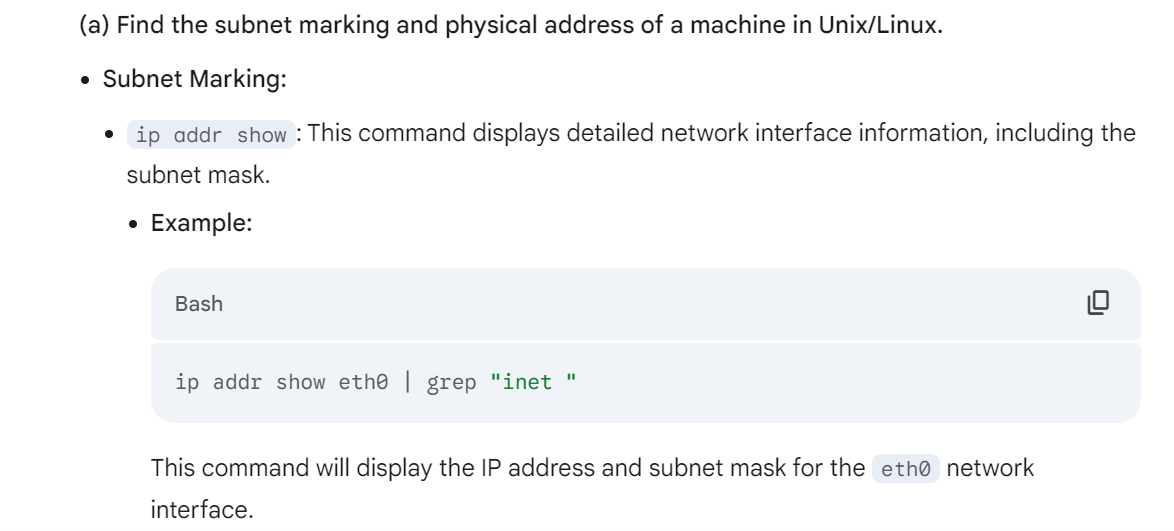
Q-Write down the UNIX/LINUX Command for the following operations : (verify the 20 results) (a) Find the subnet marking and physical address of a machine in Unix/Linux. (b) Enable authentication for single-user mode on Linux.





(b) Enable authentication for single-user mode on Linux.

Edit the /etc/security/authconfig file: This file controls authentication settings for various system services, including single-user mode.

Modify the relevant options:

Look for the section related to single-user mode.

Uncomment and set the desired authentication methods (e.g., USE\_PAM, USE\_PAM\_AUTH).

Save the changes to the file.

Run authconfig:

Execute the authconfig command to apply the changes.

Example (in /etc/security/authconfig):

# Single user mode authentication

USE\_PAM="yes"

USE\_PAM\_AUTH="yes"

Note:

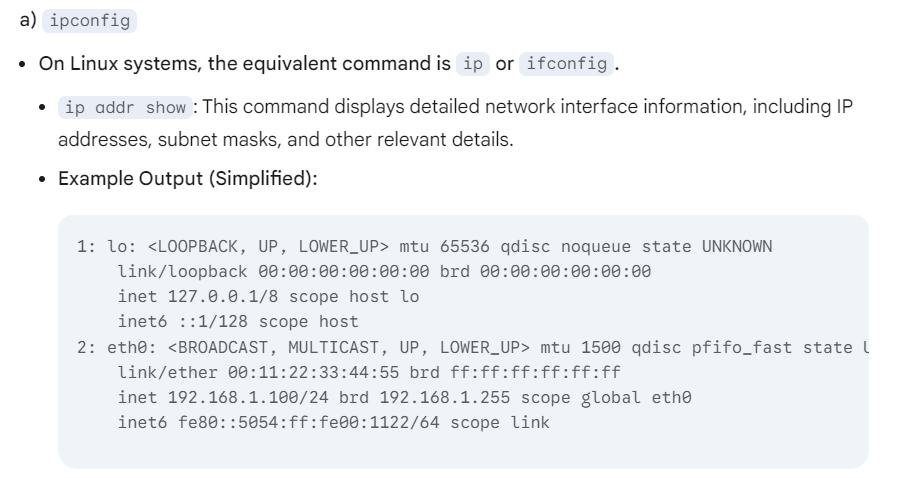
The specific options and their values may vary depending on your Linux distribution and security requirements.

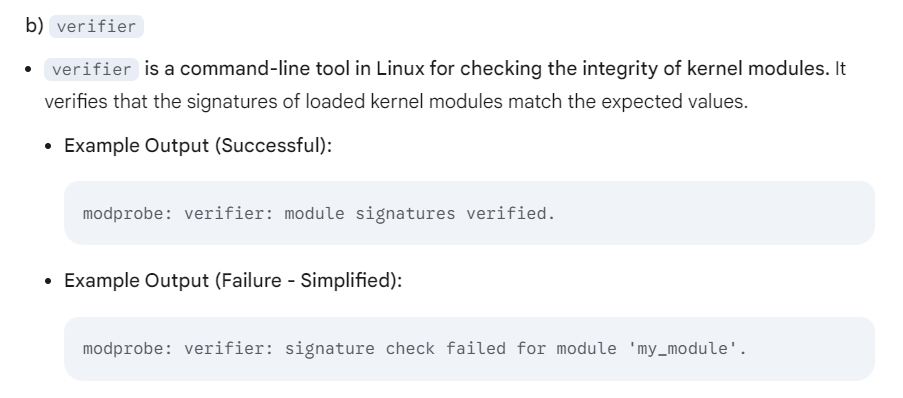
Refer to the authconfig man page (man authconfig) for detailed information and available options.

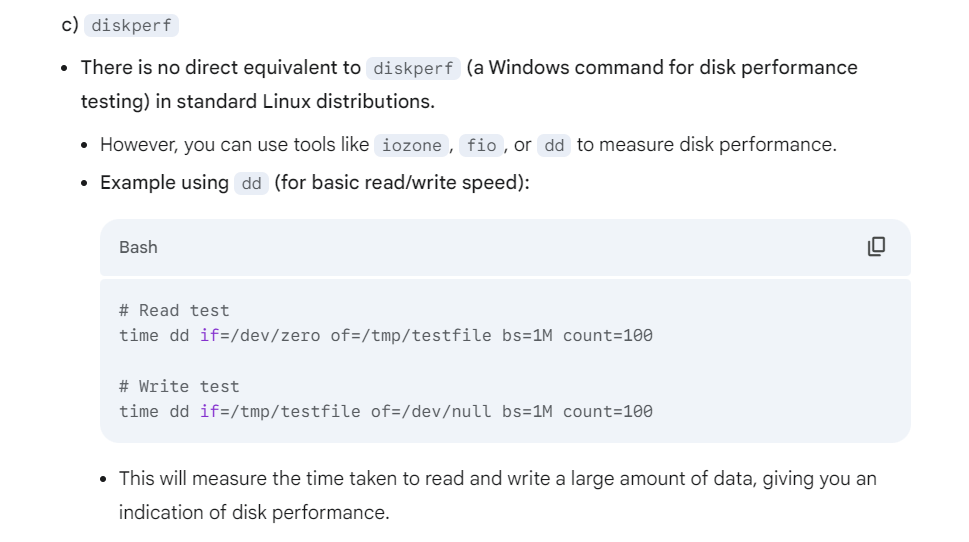
Q-2 Run the following commands on Linux and show/write their outputs. 20

(a) IP config (b) verifier

(c) diskperf (d) nslookup









\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-3 Create and Configure Samba Server in Linux. Demostrate step by step procedure. 20



**Refer PDF**

**1. Install Samba**

* **Update package lists:**

Bash

sudo apt update

* **Install Samba:**

Bash

sudo apt install samba samba-common-bin

**2. Configure Samba**

* **Edit the Samba configuration file:**

Bash

sudo nano /etc/samba/smb.conf

* **Make necessary changes:**
  + **[global]** section:
    - **workgroup = WORKGROUP** (Replace with your desired workgroup name)
    - **security = user**
    - **encrypt passwords = yes**
    - **passdb backend = tdbsam**
  + **Create a share (example: "my\_share"):**
  + [my\_share]
  + path = /path/to/your/share/directory
  + public = yes
  + writable = yes
  + guest ok = yes
  + read only = no
  + create mask = 0664
  + directory mask = 0775
    - Replace /path/to/your/share/directory with the actual path to the directory you want to share.
    - Adjust permissions (create mask, directory mask) according to your needs.
* **Save and close the smb.conf file.**

**3. Create Samba User Accounts**

* **Create a new user (optional):**

Bash

sudo adduser <username>

* **Set Samba password for the user:**

Bash

sudo smbpasswd -a <username>

**4. Restart Samba**

* **Restart the Samba service:**

Bash

sudo systemctl restart smbd

Bash

sudo systemctl restart nmbd

**5. Test the Samba Share**

* **On a Windows machine:**
  + Open **File Explorer**.
  + In the address bar, type \\<server\_name> (replace <server\_name> with the hostname or IP address of your Linux server).
  + You should see the shared folder ("my\_share" in this example).
  + Try to access and modify files within the shared folder.

**6. Troubleshooting**

* **Check Samba logs:**

Bash

sudo tail -f /var/log/samba/log.smbd

* **Use smbclient to test connectivity:**

Bash

smbclient //<server\_name>/my\_share -U <username>

Q-4 Configure a Remote Server and transfer a Directory to Remote Server in Linux.

**Refer PDF**

Q-5 Configure and test the inbuilt firewall in Linux.

**Refer PDF**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-6 Configure FTP server in Linux then install and test a FTP client.

**Refer PDF**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-7 Configure and test Telnet in Linux.

**Refer PDF**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-8 Create a group named "Student" using GUI tool in Linux. Write the rules and set permission for this new group.

**1. Accessing the Group Management Tool**

* **Graphical User Interface (GUI):**
  + **GNOME:**
    - Open "Users & Groups" application (usually found in the Activities overview).
  + **KDE:**
    - Open "System Settings" and navigate to "User Management".
  + **Other Desktop Environments:**
    - Look for a similar application related to user and group management (e.g., "User Manager").

**2. Creating the "Student" Group**

* **Locate Group Management:** Find the section within the GUI tool that deals with groups.
* **Create New Group:** Click on the button to create a new group (e.g., "Add" or "New Group").
* **Enter Group Name:** In the provided field, type "Student" as the group name.
* **Confirm and Create:** Click "Create" or "Add" to finalize the group creation.

**3. Managing Group Members (Optional)**

* **Add Users to the Group:**
  + Select the "Student" group in the group management tool.
  + Find the option to add users to the group (e.g., "Add User to Group").
  + Select the users you want to add to the "Student" group.
  + Click "Add" or "OK" to assign them to the group.

**4. Setting File/Directory Permissions (Example)**

* **Choose a File/Directory:** Select a specific file or directory you want to control access for.
* **Right-click:** Right-click on the selected file or directory.
* **Properties:** Select "Properties" from the context menu.
* **Permissions Tab:** Navigate to the "Permissions" tab.
* **Group Permissions:**
  + **Read:** Check the "Read" box to allow group members to read the file/directory.
  + **Write:** Check the "Write" box to allow group members to modify or create files within the directory.
  + **Execute:** Check the "Execute" box to allow group members to run executable files or enter the directory.

**5. Using chmod (Command-Line Alternative)**

* **Open Terminal:** Launch a terminal application.
* **Use chmod command:**
  + Example: chmod g+rw /path/to/file\_or\_directory
    - This command grants read and write permissions to the group for the specified file or directory.
  + For more complex permissions, refer to the chmod man page (man chmod) for detailed options.

**Important Notes:**

* **GUI tools may vary slightly** depending on the specific Linux distribution and desktop environment.
* **Permissions:** File and directory permissions are crucial for system security.
* **Best Practices:**
  + Use the principle of least privilege: Grant only the necessary permissions to users and groups.
  + Regularly review and adjust permissions as needed.

By following these steps, you can effectively create a group named "Student" and manage its permissions using GUI tools in your Linux environment. Remember to exercise caution when modifying permissions to maintain system security.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-9 Install and configure the POP and IMAP Server in Linux.

Refer PDF

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-10 Install and configure a proxy server on Linux.

Refer PDF

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-11 Write down the Unix/Linux commands for the following operations (verify the results) : 20

(a) Enable authentication for single-user mode on Linux operating system.

(b) Find the subnet mask and physical address of a machine in Unix/Linux.

Answer:

**a) Enable Authentication for Single-User Mode on Linux**

1. **Edit the /etc/security/authconfig file:** This file controls authentication settings for various system services, including single-user mode.

Bash

sudo nano /etc/security/authconfig

1. **Modify the relevant options:**
   * **Uncomment and set the desired authentication methods:**
   * USE\_PAM="yes"
   * USE\_PAM\_AUTH="yes"
2. **Run authconfig:**

Bash

sudo authconfig

1. **Reboot the system:** For the changes to take effect in single-user mode, a system reboot is usually required.

Bash

sudo reboot

**b) Find the Subnet Mask and Physical Address of a Machine in Unix/Linux**

* **Subnet Mask:**
  + **ip addr show:** This command displays detailed network interface information, including the subnet mask.

Bash

ip addr show eth0 | grep "inet "

* + - Replace eth0 with the actual interface name (e.g., enp0s3).
* **Physical Address (MAC Address):**
  + **ip link show:**

Bash

ip link show eth0 | grep "link/ether"

**Verifying Results:**

* **Subnet Mask:**
  + After running the ip addr show command, check the output for the line containing the IP address of the interface. The subnet mask will be displayed next to the IP address, typically in CIDR notation (e.g., 192.168.1.100/24).
* **Physical Address (MAC Address):**
  + The ip link show command will display the MAC address in the format "xx:xx:xx:xx:xx:xx".

**Note:**

* These commands provide the most common and reliable methods for obtaining subnet masks and MAC addresses in modern Linux systems.
* The specific interface names and output formats may vary slightly depending on the Linux distribution and system configuration.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-12 Create a group named "BCA" using GUI tool in Linux. Also, create a group administrator for this group "BCA". Write the rules and set the permissions for this group and group admin.

Answer

**1. Create the "BCA" Group**

* **Access Group Management Tool:**
  + **GNOME:** Open "Users & Groups" application.
  + **KDE:** Open "System Settings" and navigate to "User Management".
  + **Other DEs:** Look for a similar application (e.g., "User Manager").
* **Create New Group:**
  + Click on the button to create a new group (e.g., "Add" or "New Group").
  + Enter "BCA" as the group name.
  + Click "Create" or "Add".

**2. Create the "BCA" Group Administrator**

* **Create a New User:** Create a new user account specifically for the group administrator (e.g., "bca\_admin").
* **Add Administrator to "BCA" Group:**
  + Select the "BCA" group.
  + Add the "bca\_admin" user to the "BCA" group.

**3. Set Permissions for the "BCA" Group**

* **Choose a File/Directory:** Select a file or directory you want to control access for.
* **Right-click:** Right-click on the selected file or directory.
* **Properties:** Select "Properties" from the context menu.
* **Permissions Tab:** Navigate to the "Permissions" tab.
* **Group Permissions:**
  + **Read:** Check the "Read" box to allow group members to read the file/directory.
  + **Write:** Check the "Write" box to allow group members to modify or create files within the directory.
  + **Execute:** Check the "Execute" box to allow group members to run executable files or enter the directory.

**4. Set Permissions for the "BCA" Group Administrator**

* **Grant Administrator Privileges:**
  + The "bca\_admin" user should have higher privileges within the "BCA" group. This can be achieved by:
    - **Adding "bca\_admin" to the "sudo" group:** This grants them elevated privileges to execute commands with root permissions.
    - **Creating custom scripts or policies** that grant specific administrative powers to the "bca\_admin" user within the context of the "BCA" group.

**5. Example using chmod (Command-Line)**

* **Grant Read and Write to "BCA" Group:**

Bash

chmod g+rw /path/to/file\_or\_directory

**Important Considerations:**

* **Principle of Least Privilege:** Grant only the necessary permissions to the "BCA" group and its administrator.
* **Security:** Regularly review and adjust permissions as needed to maintain system security.
* **Group Administration:** Define clear responsibilities and procedures for the "bca\_admin" user to manage the "BCA" group effectively.

By following these steps, you can create a "BCA" group with a designated administrator and manage their permissions effectively within your Linux environment. Remember to adapt these instructions to your specific needs and security requirements.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-13 Write the command(s) to perform the following operations : 20

(a) To enable authentication for single user mode on Linux.

(b) Find the Round Trip Time (RTT) of a packet from the server.

Answer

Certainly, here are the commands for the specified operations:

**a) Enable Authentication for Single User Mode on Linux**

1. **Edit the /etc/security/authconfig file:** This file controls authentication settings for various system services, including single-user mode.

Bash

sudo nano /etc/security/authconfig

1. **Modify the relevant options:**
   * **Uncomment and set the desired authentication methods:**
   * USE\_PAM="yes"
   * USE\_PAM\_AUTH="yes"
2. **Run authconfig:**

Bash

sudo authconfig

1. **Reboot the system:** For the changes to take effect in single-user mode, a system reboot is usually required.

Bash

sudo reboot

**b) Find the Round Trip Time (RTT) of a packet from the server**

* **Use the ping command:**

Bash

ping -c 4 <hostname\_or\_ip\_address>

* + Replace <hostname\_or\_ip\_address> with the hostname or IP address of the server you want to ping.
  + -c 4 specifies that the ping command should send 4 packets.
* **Examine the output:** The ping command will display the RTT for each packet sent. Look for lines like:
* rtt min/avg/max/mdev = 0.123/0.142/0.158/0.011 ms
  + rtt: Round Trip Time
  + min: Minimum RTT
  + avg: Average RTT
  + max: Maximum RTT
  + mdev: Mean Deviation of RTT

This will give you an indication of the network latency between your machine and the server.

**Note:**

* For more detailed network diagnostics, you can use tools like traceroute or mtr to analyze the path taken by packets to the server and identify potential bottlenecks.

I hope this helps!

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-14 Write the command(s) to perform the following operations : 20

(a) Print out the header of network packets.

(b) List the routers your connection crosses when reaching out to a remote system.

Answer

**a) Print out the header of network packets**

* **Use tcpdump:**

Bash

sudo tcpdump -n -vv -s 0 -c 1 <interface>

* + Replace <interface> with the name of your network interface (e.g., eth0, enp0s3).
  + -n: Do not perform domain name resolution (faster).
  + -vv: Increase verbosity (more detailed output).
  + -s 0: Capture the entire packet.
  + -c 1: Capture only one packet.

This command will capture a single packet on the specified interface and display its header in detail.

**b) List the routers your connection crosses when reaching out to a remote system**

* **Use traceroute:**

Bash

traceroute <hostname\_or\_ip\_address>

* + Replace <hostname\_or\_ip\_address> with the hostname or IP address of the remote system.

traceroute sends packets with increasing Time-to-Live (TTL) values to the target system. As each router along the path receives a packet with an exceeded TTL, it sends an ICMP "Time Exceeded" message back to the source. traceroute uses these messages to identify the routers along the path

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-15 Configure the DHCP Server on the Linux operating system.

Refer PDF

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-------

Q-16 Install and configure the SMTP Server on Linux operating system.

Refer PDF

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-17 Write the commands to perform the following tasks : 20 (a) To provide information about network interfaces and all assigned IP addresses. (b) To provide a list of all routers your connection cross when reaching out to a remote system.

Answer:

**a) To provide information about network interfaces and all assigned IP addresses:**

Bash

ip addr show

This command will display a comprehensive list of all network interfaces on the system, along with their associated IP addresses, subnet masks, and other relevant information.

**b) To provide a list of all routers your connection crosses when reaching out to a remote system:**

Bash

traceroute <hostname\_or\_ip\_address>

* Replace <hostname\_or\_ip\_address> with the hostname or IP address of the remote system you want to trace.

traceroute sends packets with increasing Time-to-Live (TTL) values to the target system. As each router along the path receives a packet with an exceeded TTL, it sends an ICMP "Time Exceeded" message back to the source. traceroute uses these messages to identify the routers along the path.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

Q-18 Write the commands to perform the following tasks : 20 (a) Does a DNS query for the user (i. e. find out IP address for a particular system or system name). (b) To ensure that a network connection can be established with a remote system or test whether a network connection is good or not.

Answer:

**a) Perform a DNS Query**

* **Use nslookup:**

Bash

nslookup <hostname>

* + Replace <hostname> with the domain name or hostname you want to resolve (e.g., www.google.com, example.com).

nslookup will query the DNS server and display the IP address(es) associated with the given hostname.

* **Use dig:**

Bash

dig <hostname>

dig is a more powerful and flexible DNS query tool that provides more detailed information than nslookup.

**b) Test Network Connectivity**

* **Use ping:**

Bash

ping -c 4 <hostname\_or\_ip\_address>

* + Replace <hostname\_or\_ip\_address> with the hostname or IP address of the remote system.
  + -c 4 specifies that the ping command should send 4 packets.

If the ping command is successful, it indicates that a basic network connection can be established to the remote system. The output will display the Round Trip Time (RTT) for each packet, which can help assess the connection quality.

* **Use telnet (for testing port connectivity):**

Bash

telnet <hostname\_or\_ip\_address> <port\_number>

* + Replace <hostname\_or\_ip\_address> with the hostname or IP address of the remote system.
  + Replace <port\_number> with the port number you want to test (e.g., 22 for SSH, 80 for HTTP).

A successful telnet connection indicates that the port is open and accepting connections on the remote system.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_--

Q-19 Write the commands to perform the following tasks : 20 (a) Displays =a11 .connections including TCP and UDP as well as all multicast connections. (b) To enable authentication. for a single user mode on Linux.

Answer

**a) Display all connections (TCP, UDP, Multicast)**

* **Using ss (Socket Statistics):**

Bash

ss -tulp

* + -t: Show TCP connections.
  + -u: Show UDP connections.
  + -l: Show listening sockets.
  + -p: Show the process associated with each connection.
* **Using netstat:**

Bash

netstat -tulnp

* + -t: Show TCP connections.
  + -u: Show UDP connections.
  + -l: Show listening sockets.
  + -n: Display numerical addresses instead of resolving hostnames.
  + -p: Show the process associated with each connection.

To specifically list multicast connections, you can use:

Bash

netstat -g

**b) Enable Authentication for Single User Mode on Linux**

1. **Edit the /etc/security/authconfig file:**

Bash

sudo nano /etc/security/authconfig

1. **Modify the relevant options:**
   * **Uncomment and set the desired authentication methods:**
   * USE\_PAM="yes"
   * USE\_PAM\_AUTH="yes"
2. **Run authconfig:**

Bash

sudo authconfig

1. **Reboot the system:** For the changes to take effect in single-user mode, a system reboot is usually required.

Bash

sudo reboot

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_=

Q-20 Write the command(s) to perform the following tasks : 20

(a) Checking the status of destination host and communication with another host name.

(b) Finding host/domain name and IP address.

Answer

**a) Checking the status of destination host and communication**

* **ping:** This command is the most basic way to check if a host is reachable.

Bash

ping -c 4 <hostname\_or\_ip\_address>

* + Replace <hostname\_or\_ip\_address> with the hostname or IP address of the target host.
  + -c 4 specifies that the ping command should send 4 packets.

A successful ping indicates that the host is reachable and responding to ICMP echo requests.

**b) Finding host/domain name and IP address**

* **nslookup:** This command performs DNS lookups.
  + **Find IP address given hostname:**

Bash

nslookup www.example.com

* + **Find hostname given IP address:**

Bash

nslookup 8.8.8.8

* **dig:** A more advanced DNS lookup tool.

Bash

dig www.example.com

* **host:** Another command for DNS lookups.

Bash

host www.example.com

These commands will provide you with the IP address associated with a given hostname or the hostname associated with a given IP address.