

**INDIRA GANDHI NATIONAL OPEN UNIVERSITY****Assignment Submission****Regional Centre Delhi-1****For Term End Exam (DEC/ 2024)**

1. Name of the Student :- NITIN KUMAR AGNIHOTRI
  2. Enrollment Number :- 2200421211
  3. Programme Code :- BCAOL
  4. Course Code :- BCSL-058
  5. Course Title :- Computer oriented Numerical techniques Lab
  6. Assignment Number :- BCA(V)/L-058/Assignment/2024-25
  7. Regional Centre Code :- COE:CENTRE FOR ONLINE EDUCATION IGNOU
  8. Mobile Number :- +91 9891367726
  9. E-mail ID :- NITINAGNIHOTRI10@GMAIL.COM
- 10. Above information is cross checked and it is correct:- Yes**

**Q1. (a) Write a shell script which will accept the PID of a process and display the details of that process.**

## Answer:

# ← Shell Script →

## ← Display the Details of Process →

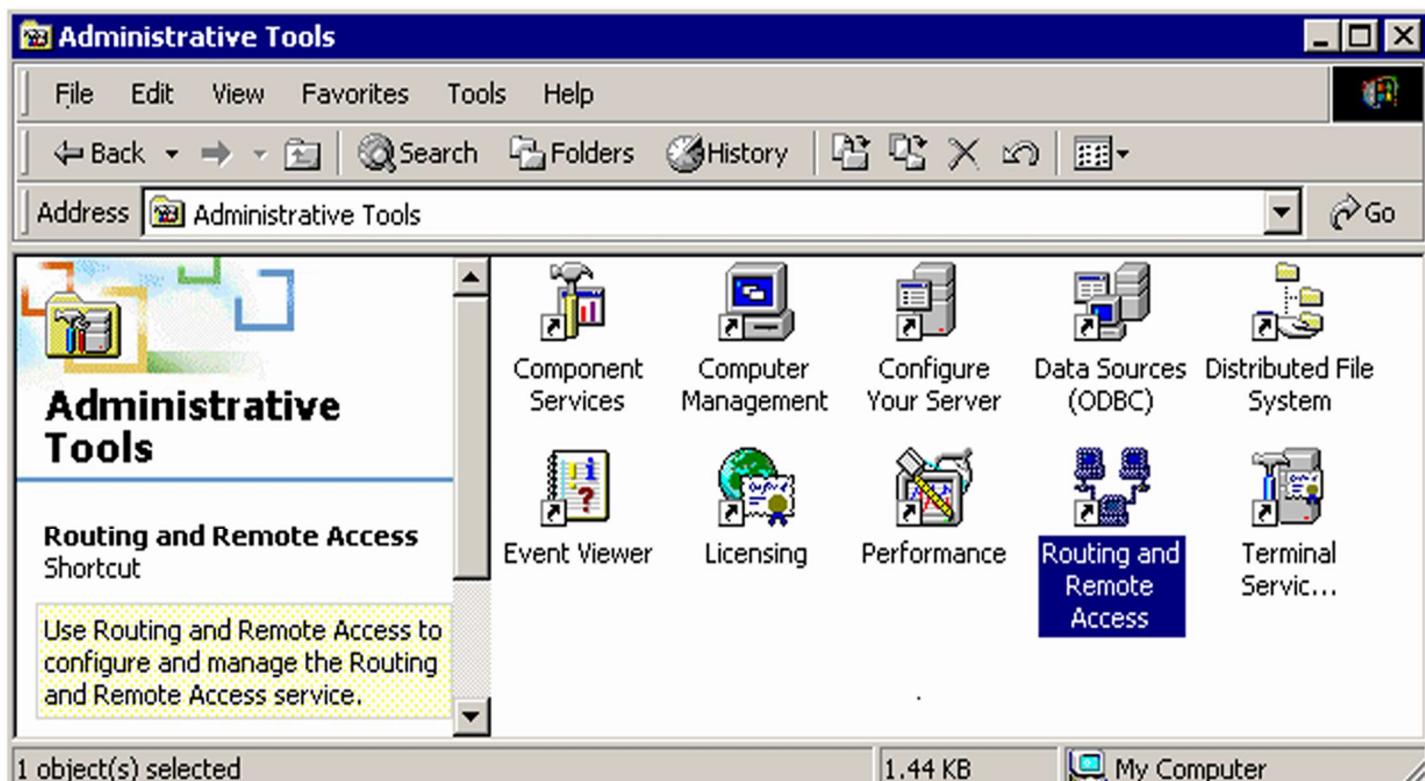
```
root@Nitin-Agnihotri:~# vi process_info.sh
root@Nitin-Agnihotri:~# chmod +x process_info.sh
root@Nitin-Agnihotri:~# ./process_info.sh 1
Details of process with PID 1:
 PID  PPID USER      STAT  CMD          STARTED      TIME
   1     0 root      Sl  /init          12:50:30  00:00:00
root@Nitin-Agnihotri:~# ./process_info.sh 10
Process with PID 10 does not exist.
root@Nitin-Agnihotri:~# |
```

**Q:1(b) Create Remote Access Policy. Show how you can change to Remote Access Logging setting in Windows 2000.**

---

**Answer :**

**← Remote Access Policy →**





## Routing and Remote Access Configuration Wizard



### Dial-in or demand dial interfaces

Your server has a number of external interfaces (such as modems or ISDN adapters) which you can selectively enable for dial-in access and/or demand-dial router ports.

Note: Devices which support a number of logical ports (such as a T1 card) must be enabled as a whole.

- Enable all devices for routing
- Enable all devices for remote access
- Enable all devices for both routing and remote access
- Configure each device individually

< Back

Next >

Cancel

## Routing and Remote Access Configuration Wizard



### Authentication and encryption



Specify the authentication methods supported by this server.

- All methods, including clear text passwords
- Only methods which secure the user's password

Encryption for dial-up and PPTP connections will be determined by the policy and profile in force for each connection.

If this server will support L2TP VPN connections, you can require these connections to use IPSEC encryption.

- Encrypt all L2TP connections

< Back

Next >

Cancel

## Routing and Remote Access Configuration Wizard



### Routing and Remote Access

Define the access rights for remote systems.



Note the protocols that have been loaded on your server and specify whether dial-up or VPN connections have access to this server, or to the entire network.

Protocols:

TCP/IP

- Access this server only  
 Access entire network

< Back

Next >

Cancel

## Routing and Remote Access Configuration Wizard



Completing the Routing and Remote Access Configuration Wizard

The basic configuration for routing and remote access is now complete.

If you enabled routing, you must use the Routing and Remote Access Administration snap-in in the Microsoft Management Console to set interface addresses or other router configuration details.

If you enabled dial-in access, that service is now ready for use. You can adjust server settings from the Routing and Remote Access Administration snap-in.

Per user settings are managed in the Directory Services snap-in. Rule based settings (based on user group and other parameters) can be defined in the Remote Access Policy snap-in.

To close the wizard, click Finish.

< Back

Finish

Cancel

## Routing and Remote Access Administration



The Routing and Remote Access service has now been installed. Would you like to start the service?

Yes

No

## Service Control



Attempting to start Routing and Remote Access service  
on SRVRC500.

### Routing and Remote Access

Action View | Back Forward | File | Tools | Help |

Routing and Remote Access

- Server Status
- s1

Name

- Dial-In Clients (0)
- Ports
- IP Routing
- Remote Access Policies
- Logging

**Routing and Remote Access**

Action View | Back Forward | Refresh | New | Open | Save | Delete | Help

Name	Device	Comment	Status
WAN Miniport (PPTP) (VPN3-4)	VPN		Inactive
WAN Miniport (PPTP) (VPN3-3)	VPN		Inactive
WAN Miniport (PPTP) (VPN3-2)	VPN		Inactive
WAN Miniport (PPTP) (VPN3-1)	VPN		Inactive
WAN Miniport (PPTP) (VPN3-0)	VPN		Inactive
WAN Miniport (L2TP) (VPN2-4)	VPN		Inactive
WAN Miniport (L2TP) (VPN2-3)	VPN		Inactive
WAN Miniport (L2TP) (VPN2-2)	VPN		Inactive
WAN Miniport (L2TP) (VPN2-1)	VPN		Inactive
WAN Miniport (L2TP) (VPN2-0)	VPN		Inactive
Sportster Flash V.90 Voice Pn...	MODEM		Inactive

**Q2:(a) Write a shell program to scan all the files in a particular directory and list only those files which start (file\_name) with "a" or "A".**

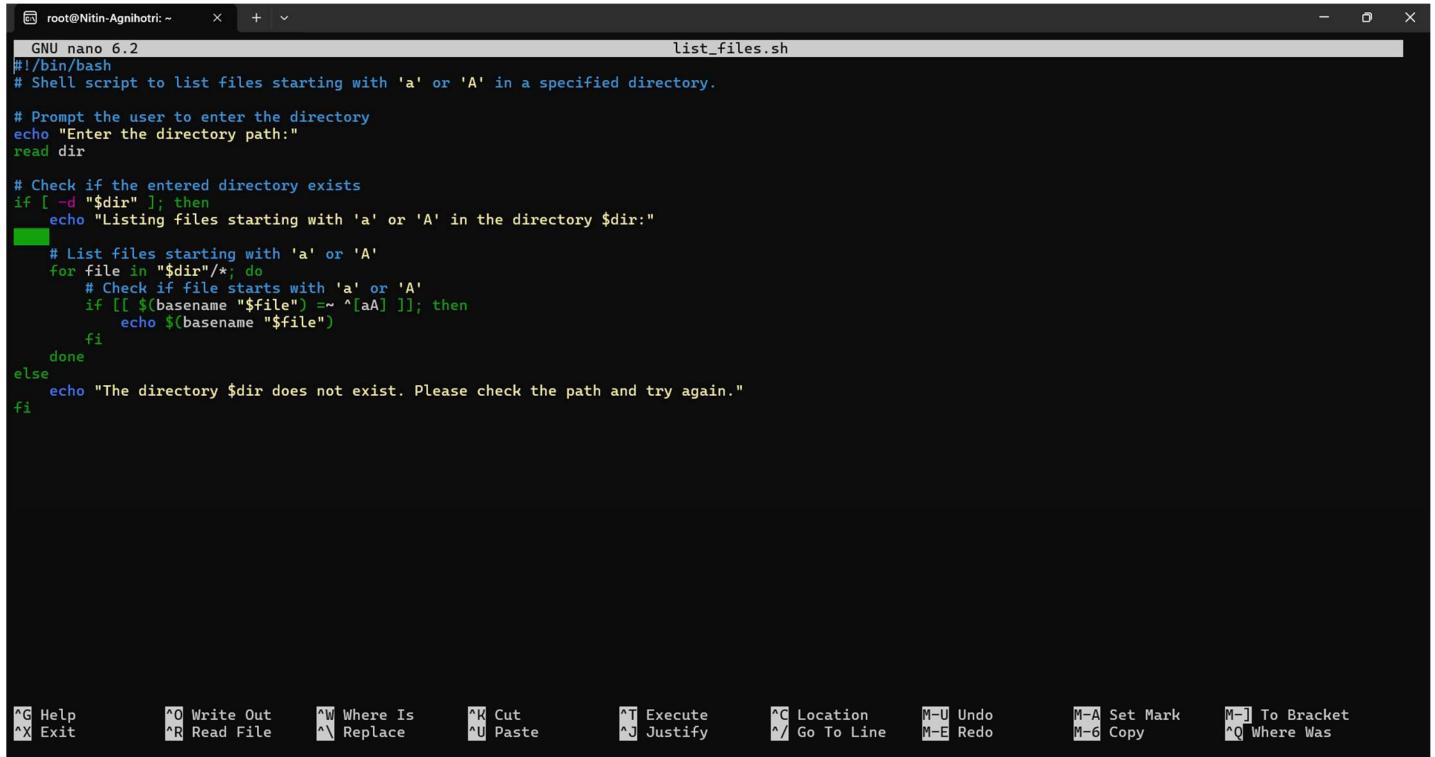
---

**Answer:**

←Shell Program→



A terminal window titled 'root@Nitin-Agnihotri: ~'. The command 'nano list\_files.sh' is entered at the prompt.



```
root@Nitin-Agnihotri: ~      + | v
GNU nano 6.2                      list_files.sh
#!/bin/bash
# Shell script to list files starting with 'a' or 'A' in a specified directory.

# Prompt the user to enter the directory
echo "Enter the directory path:"
read dir

# Check if the entered directory exists
if [ -d "$dir" ]; then
    echo "Listing files starting with 'a' or 'A' in the directory $dir:"
```

The screenshot shows the 'list\_files.sh' script in the nano text editor. The script uses a for loop to iterate through files in the specified directory and checks if the basename of each file starts with 'a' or 'A' using the =~ operator with the pattern '[aA]'.

```
    # List files starting with 'a' or 'A'
    for file in "$dir"/*; do
        # Check if file starts with 'a' or 'A'
        if [[ ${basename "$file"} =~ ^[aA] ]]; then
            echo ${basename "$file"}
        fi
    done
else
    echo "The directory $dir does not exist. Please check the path and try again."
fi
```

At the bottom of the screen, there is a menu bar with various keyboard shortcuts for file operations like Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, Copy, To Bracket, and Where Was.

```
root@Nitin-Agnihotri:~ x + v
root@Nitin-Agnihotri:~# nano list_files.sh
root@Nitin-Agnihotri:~# ./List_files.sh
Enter the directory path:
/mnt/c/Users/Nitin/Documents/NetBeansProjects
Listing files starting with 'a' or 'A' in the directory /mnt/c/Users/Nitin/Documents/NetBeansProjects:
AppletIgnou
AppletProject
root@Nitin-Agnihotri:~# |
```

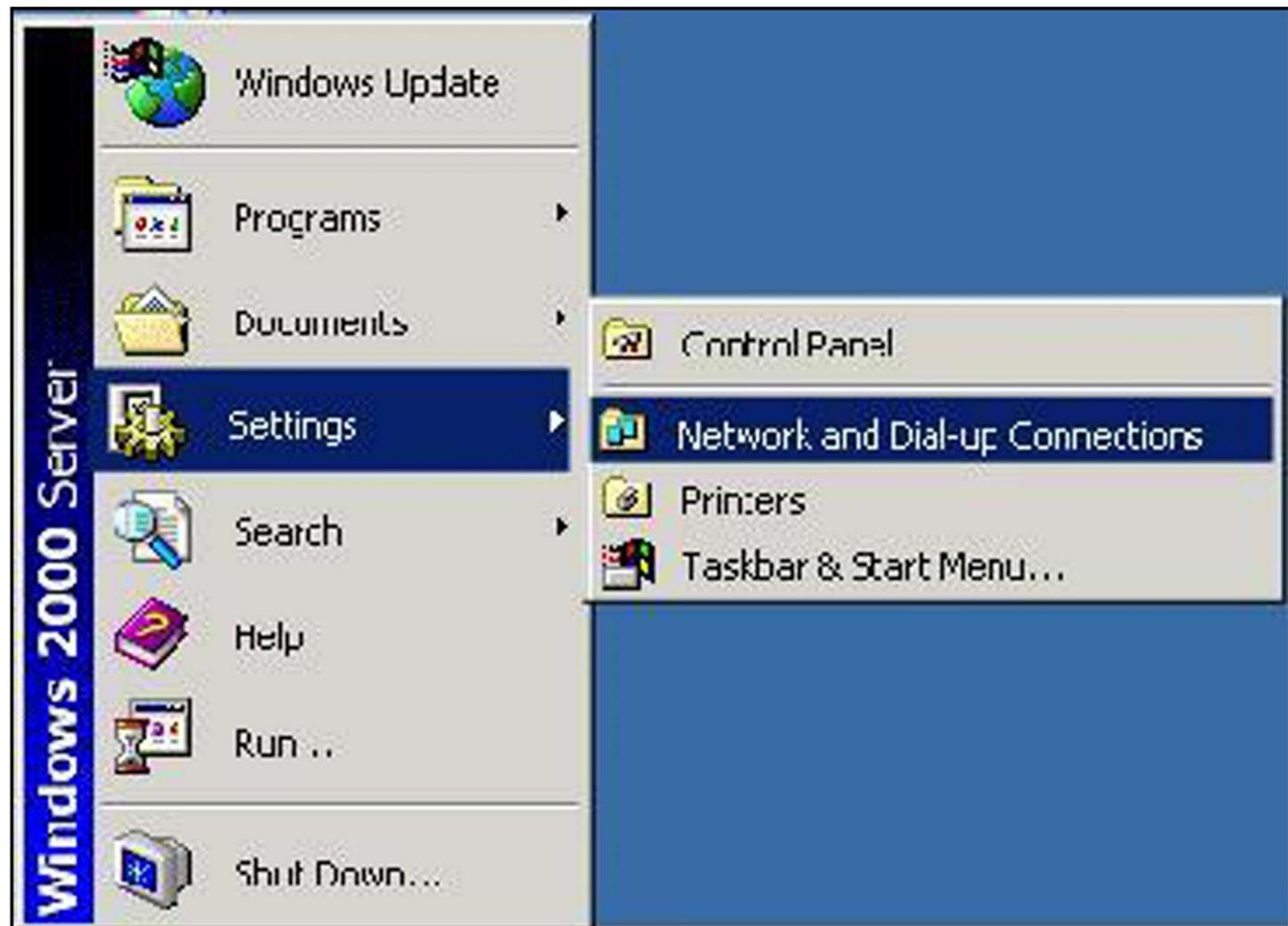
**Q2:(b) Install and configure TCP/IP settings in LINUX/UNIX operating system.Explain with step by step procedure.**

---

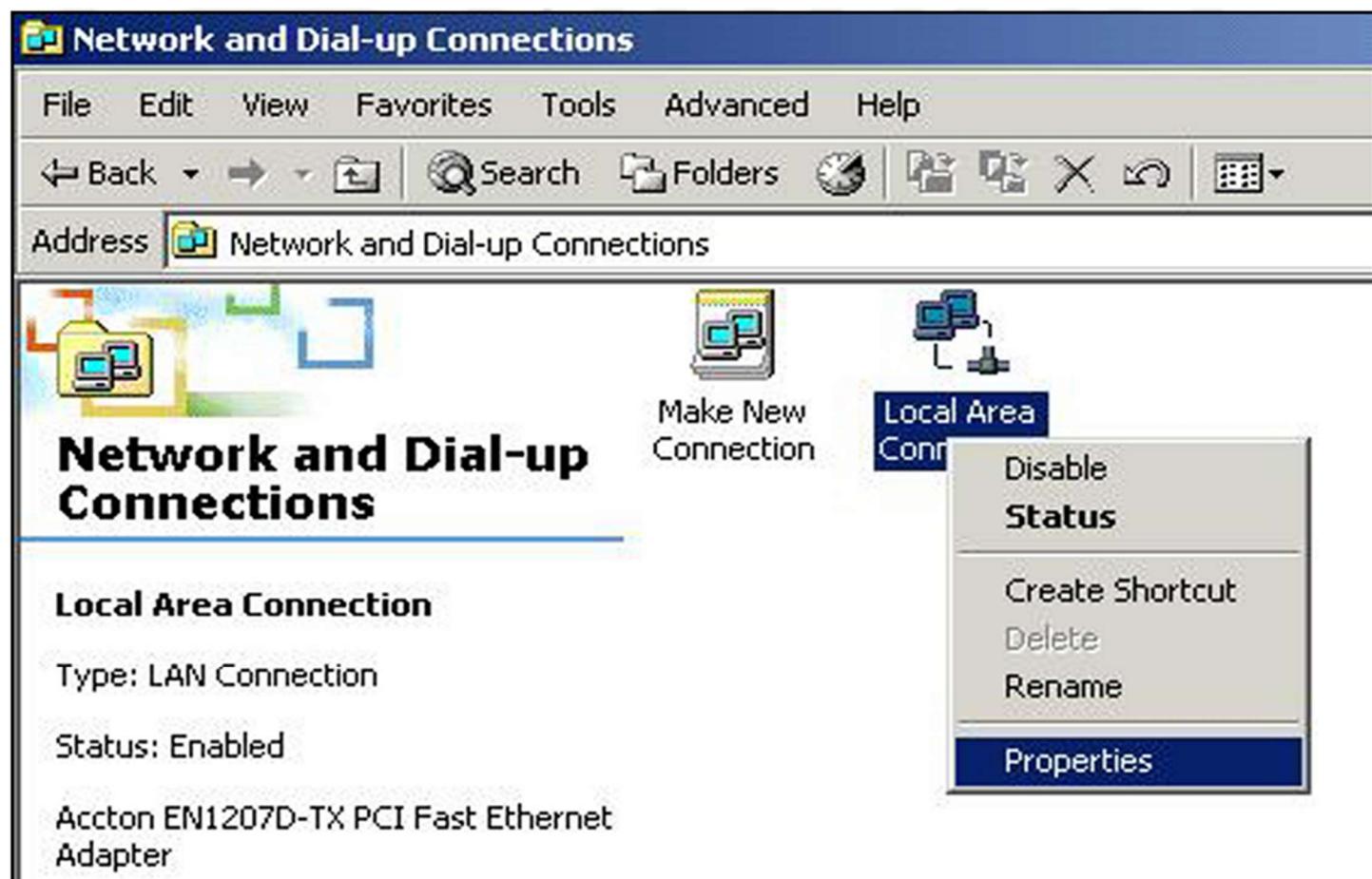
**Answer :-**

**← Installing TCP/IP →**

**STEP 1 : Open the Network and Dial-Up Connections folder**

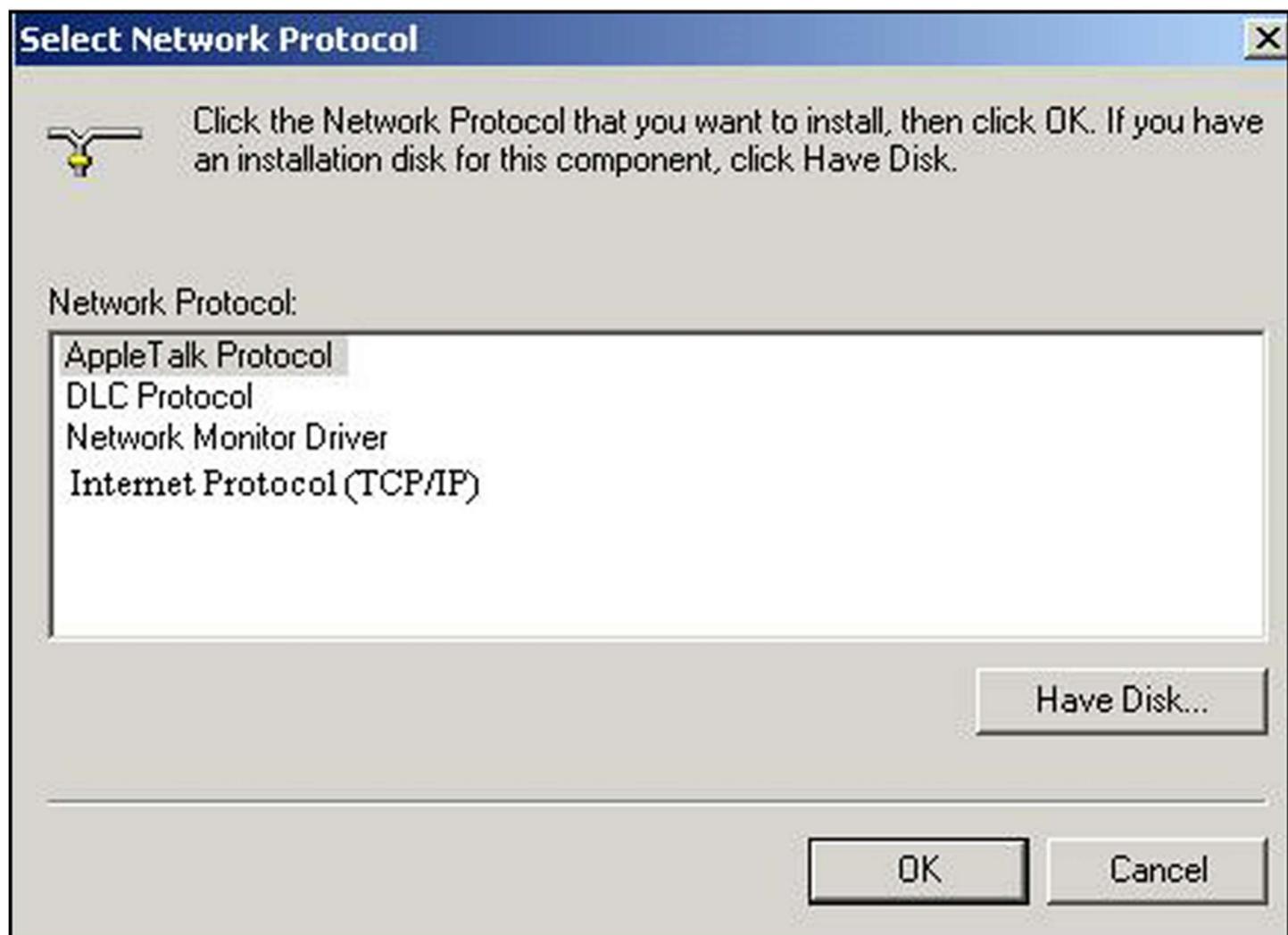


**STEP 2 : Right click the Local Area Connection icon and choose the properties.**



**STEP 3:- Now Click the Install... button, you will see the Select Network Component Type dialog box. Select protocol and click the Add... button**

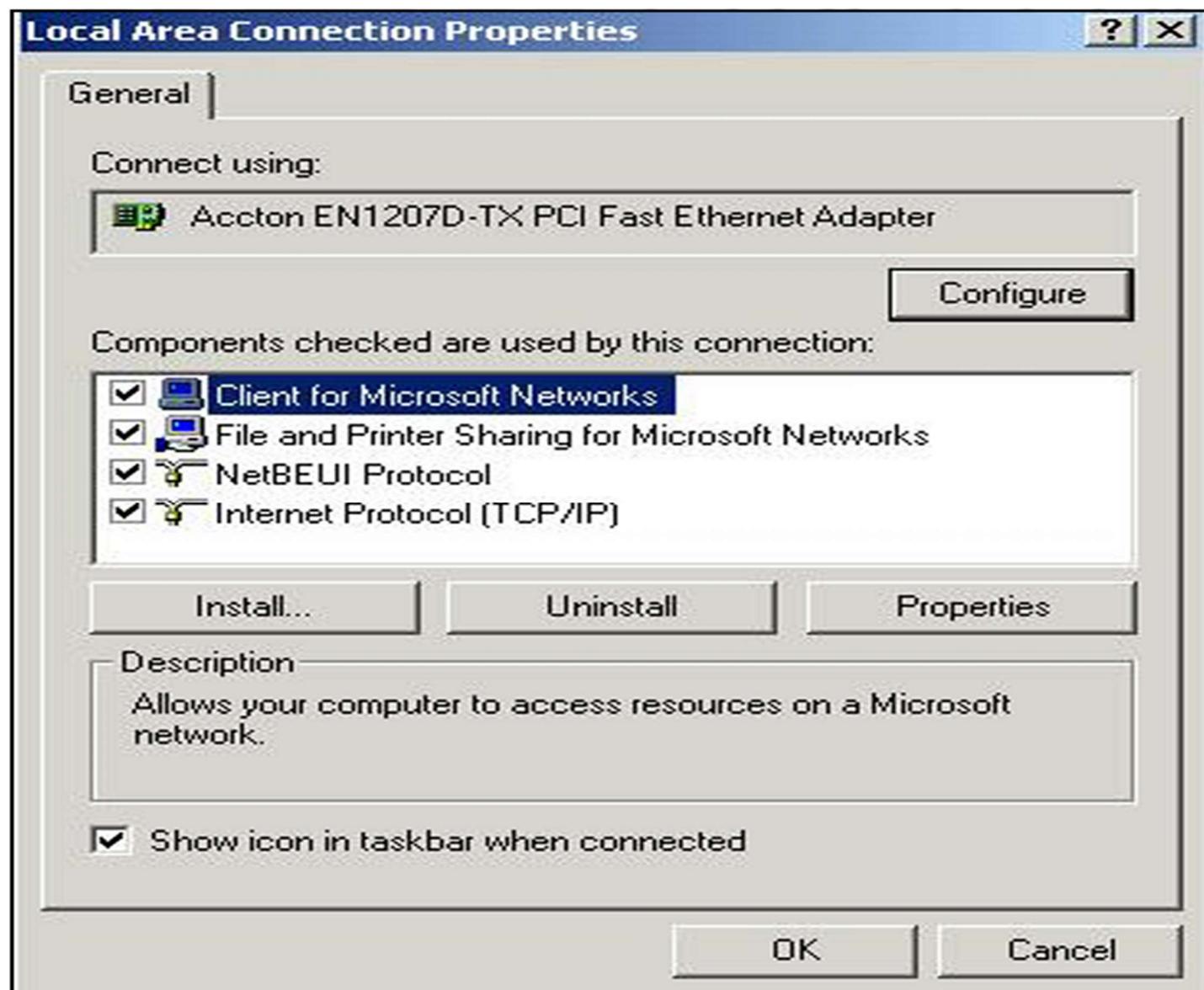
**STEP 4 : Choose Internet Protocol (TCP/IP), and then click the OK button.**



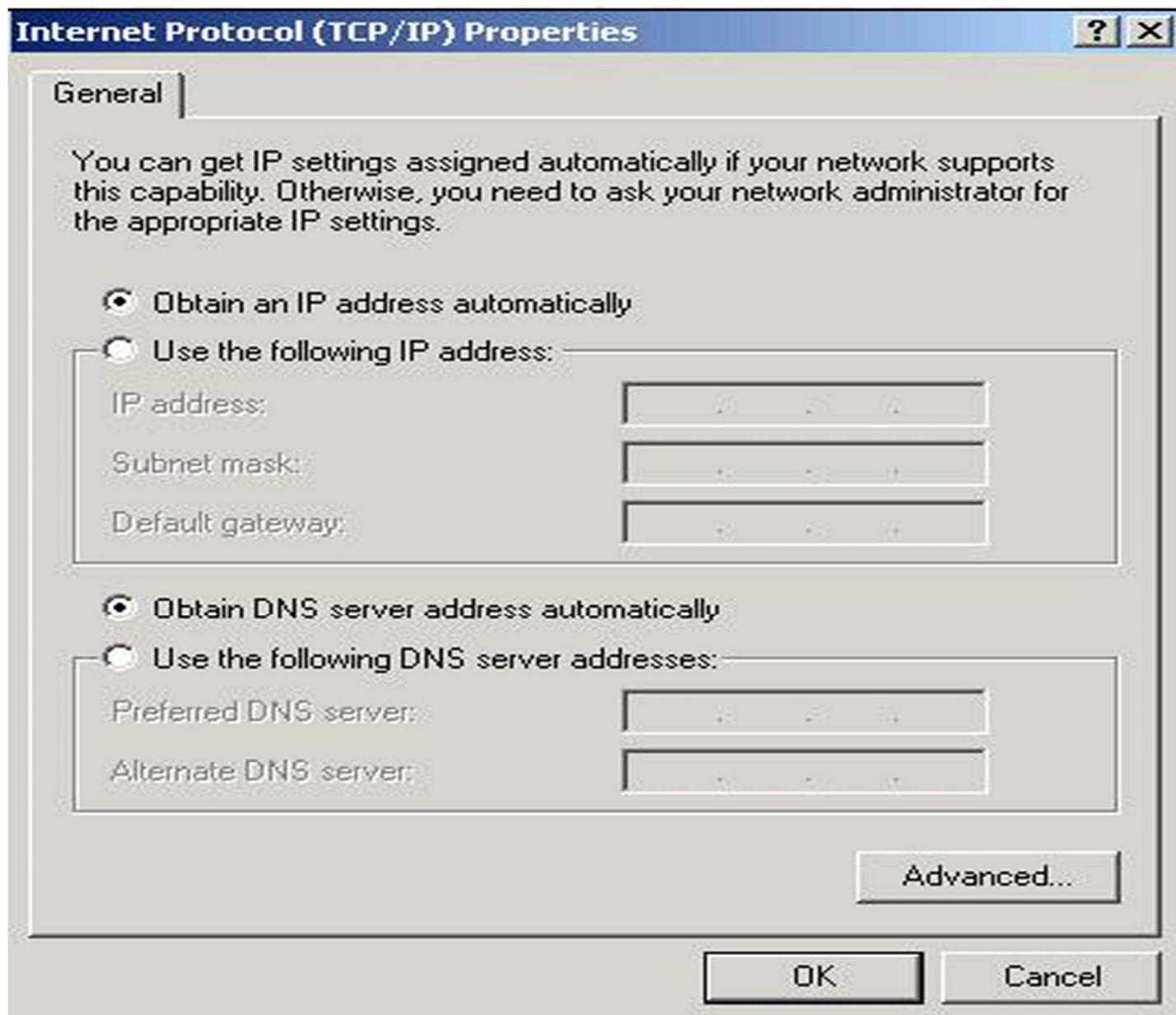
**←Configuring TCP/IP Settings→**

**STEP 1:** First you select an IP Address, which is not currently in use by another device (e.g., I am selecting “192.162.6.142” in this example). Also ensure that you know the correct subnet mask to use with that IP address (e.g., 255.255.255.0 in this example).

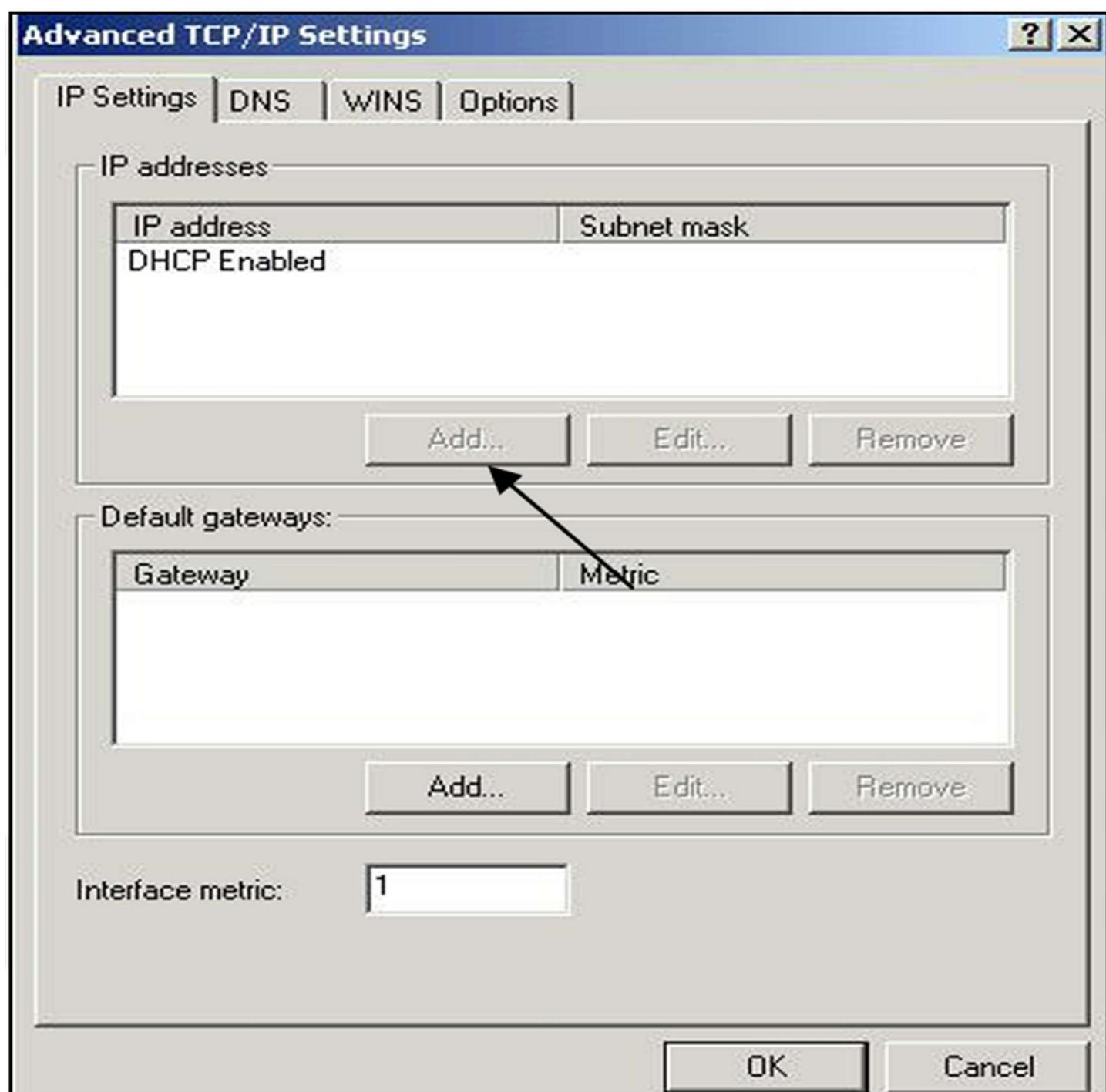
**STEP 2 :** Open the Network and Dial-Up Connections folder (Start>Settings>Network and Dial-UP Connections) similar to the previous example right click the Local Area Connection icon and choose the properties command and Local Area Connect Properties dialog box appears.



**STEP 3: Select Internet Protocol (TCP/IP) in the Components list, and then click the Properties button. The Internet Protocol (TCP/IP) Properties dialog box will appear. We want to manually configure it so we will move to Advanced setting.**



**STEP 4: The Advanced TCP/IP properties dialog box will appear when you click the Advanced ... button.**



**STEP 5: Click the Add... button in the IP Addresses control group. The TCP/IP Address dialog box will appear. In that you type the IP address and subnet mask we selected in Step 1.**

**STEP 6 : Click the OK button in the Advanced TCP/IP Settings dialog box. Then similarly click the OK in the Internet Protocol (TCP/IP) Properties dialog box and in the Local Area Connection properties dialog box**

**Q3: (a) Create a user account in the LINUX/UNIX Server. Set its password and define its permission like'an administrator.**

---

**Answer:**

**Step 1: Create a New User :-**

- Open a terminal.
- Use the useradd command to create a new user account.

```
root@Nitin-Agnihotri:~# sudo useradd -m 'Nitin'
```

A screenshot of a terminal window with three tabs. The active tab shows the command 'sudo useradd -m 'Nitin''. The window has standard Linux-style window controls at the top right.

**Step 2: Set a Password for the New User :-**

```
root@Nitin-Agnihotri:~# sudo useradd -m 'Nitin'  
root@Nitin-Agnihotri:~# sudo passwd "Nitin"  
> 2200421211
```

A screenshot of a terminal window with three tabs. The active tab shows the command 'sudo passwd "Nitin"' followed by a password entry prompt (> 2200421211). The window has standard Linux-style window controls at the top right.

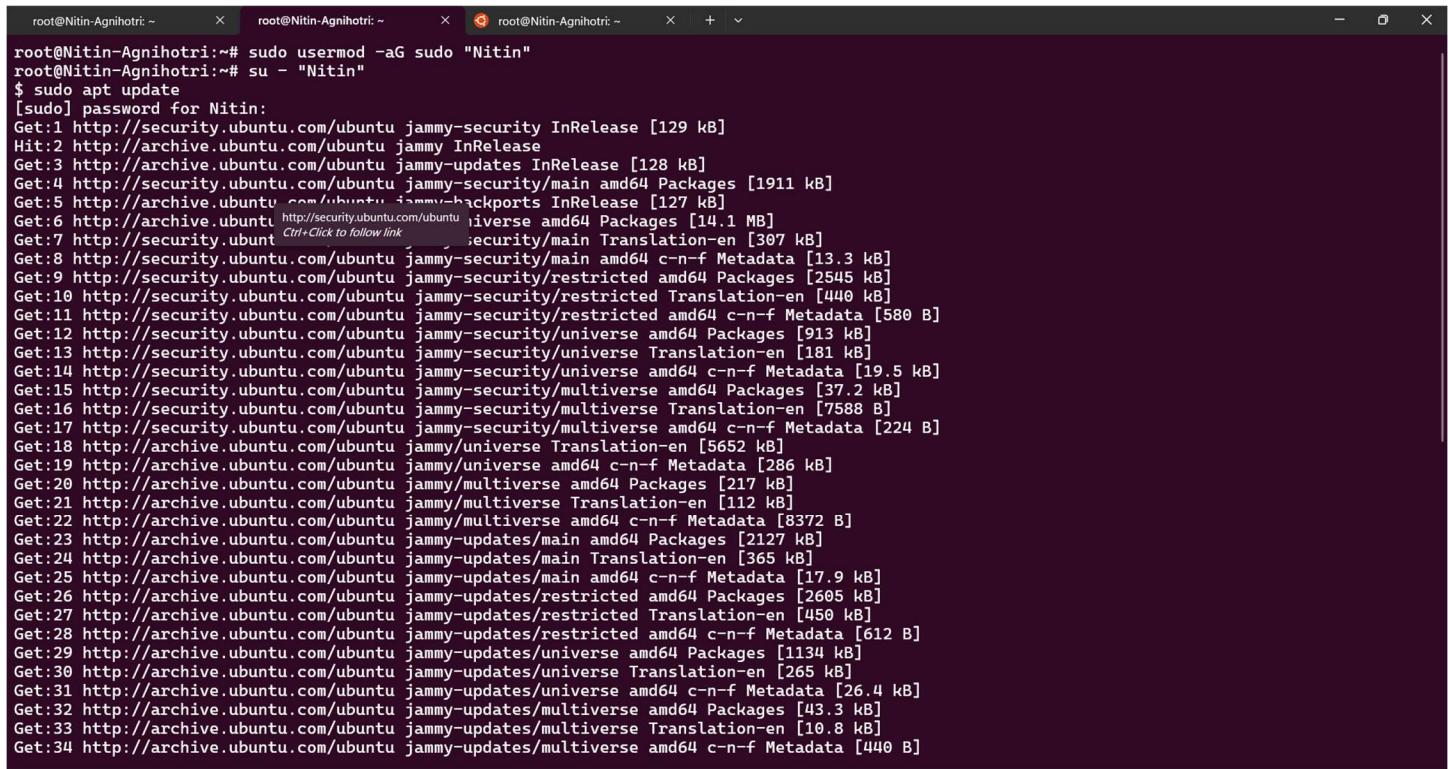
**Step 3: Grant Administrator Privileges:-**

```
root@Nitin-Agnihotri:~# sudo usermod -aG sudo "Nitin"
```

A screenshot of a terminal window with three tabs. The active tab shows the command 'sudo usermod -aG sudo "Nitin"'. The window has standard Linux-style window controls at the top right.

## Step 4: Verify the User's Permissions:

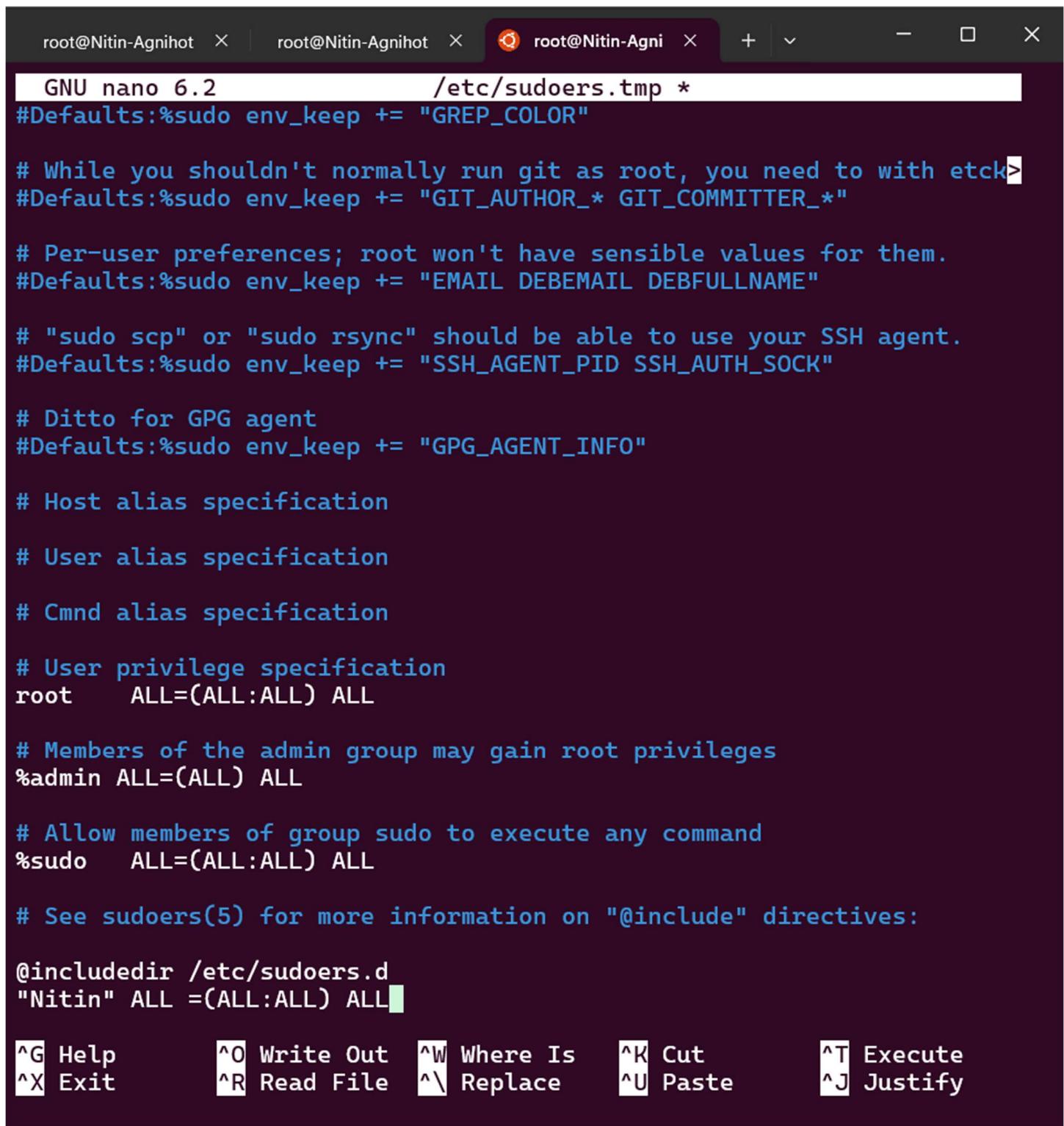
- Switch to the new user account to check if they have sudo privileges:
- Test the sudo privileges by running a command that requires administrative access, like:



```
root@Nitin-Agnihotri:~# sudo usermod -aG sudo "Nitin"
root@Nitin-Agnihotri:~# su - "Nitin"
$ sudo apt update
[sudo] password for Nitin:
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1911 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [127 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [14.1 MB]
Ctrl+Click to follow link
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [307 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.3 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2545 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [440 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [580 B]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [913 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [181 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [19.5 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [37.2 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [7588 B]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [224 B]
Get:18 http://archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:19 http://archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:20 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:21 http://archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:22 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:23 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2127 kB]
Get:24 http://archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [365 kB]
Get:25 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [17.9 kB]
Get:26 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [2605 kB]
Get:27 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [450 kB]
Get:28 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [612 B]
Get:29 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1134 kB]
Get:30 http://archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [265 kB]
Get:31 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [26.4 kB]
Get:32 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [43.3 kB]
Get:33 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [10.8 kB]
Get:34 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [440 B]
```

## STEP 5 : Modify Permissions in the sudoers File (for Fine-Tuning):

- Open the sudoers file using visudo, a command that safely edits the file:
- Add a line for the new user, if needed, to define specific administrative permissions.



```
root@Nitin-Agnihot ~ | root@Nitin-Agnihot ~ | root@Nitin-Agni ~ + - □ ×

GNU nano 6.2          /etc/sudoers.tmp *
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etck>
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d
"Nitin" ALL =(ALL:ALL) ALL

^G Help      ^O Write Out  ^W Where Is  ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify
```

Save and close the file to apply changes.

**Q3.(b) Configure a DNS Server as a Root Name Server in Windows 2000 Server.**  
**Explain with step by step procedure.**

---

## **ANSWER :**

**To configure a DNS Server as a Root Name Server in Windows 2000 Server, I would follow these steps:**

### **1. Open DNS Management Console:**

I would open the DNS management console by navigating to Start -> Programs -> Administrative Tools -> DNS.

### **2. Create Forward Lookup Zones:**

In the DNS console, I would right-click on the server name and select "New Zone..." Then, I would select "Primary Zone" and click Next.

I would then enter the name of the zone, for example, ". (Root)" and choose "Allow dynamic updates" (if needed).

### **3. Create Reverse Lookup Zones:**

Similar to forward lookup zones, I would create a reverse lookup zone for the root domain. This is also a primary zone and in the name field, we would use "0.0.127.inaddr.arpa" or "0.in-addr.arpa". I would select "Allow dynamic updates" (if needed).

### **4. Add Root Hints:**

I need to add a few root servers as hints to the DNS server so it can access the root zone.

- Open the DNS Manager console.
- Select the Forward Lookup Zone of the root server.
- Right-click and choose "New..." then select "Host (A or AAAA)".
- Set the values according to root server details. For example:
  - Name : a.root-servers.net
  - IP: 198.41.0.4
  - Name : b.root-servers.net

- IP: 192.228.79.201
- Name : c.root-servers.net
- IP: 192.33.4.12
- etc.

## 5. Configure Zone Transfers (Optional):

If it is desired for other DNS servers to receive updates on the root zone, I would configure zone transfers.

## 6. Restart the DNS Server :

I would restart the DNS server to apply the changes.

**Q4(a): In LINUX/UNIX system, access your account available at a remote machine. Download a file from the remote location, modify that file and upload back to the remote machine.**

---

### **Answer :-**

To access a remote machine, download a file, modify it, and then upload it back in Linux/UNIX, you can use tools like SSH, SCP, and nano/vim for editing. Here's a step-by-step guide to accomplish this:

**Assume:**

- Username is `nitin`.
- Remote IP is `192.168.1.10`.
- The file you need to edit is located at `/home/nitin/example.txt`.

### **Step 1: Connect to the Remote Machine**

Use SSH to access our account on the remote machine.

```
ssh nitin@192.168.1.10
```

## **Step 2: Download a File from the Remote Machine:**

**Use `scp` (Secure Copy Protocol) to download the file from the remote location to our local machine.**

```
scp nitin@192.168.1.10:/home/nitin/example.txt /home/nitin/local_copy
```

## **Step 3: Modify the File Locally:**

**Open the file in a text editor like `nano` or `vim` to make the required modifications.**

```
nano /home/nitin/local_copy/example.txt
```

**Make your changes and save the file.**

## **Step 4: Upload the Modified File Back to the Remote Machine:**

**Once you've made the necessary changes, upload the modified file back to the remote machine using “scp”.**

```
scp /home/nitin/local_copy/example.txt nitin@192.168.1.10:/home/nitin/
```

**Q4(b):Configure TCP/IP setting in LINUX/UNIX. Assume IP address is 192.168.1.2 and Port is 446. Explain with step by step procedure.**

---

## **ANSWER:**

**To configure TCP/IP settings in Linux/Unix with an IP address of “192.168.1.2” and set up a service to listen on port “446”, We have to follow these steps:**

### **Step 1: Access Network Configuration File**

**On Linux/Unix systems, network configurations are typically stored in “/etc/network/interfaces”(Debian-based systems) or “/etc/sysconfig/network-scripts/ifcfg-<interface>” (Red Hat-based systems). Here, we’ll focus on the Debian-based approach.**

#### **1. Open the configuration file:**

```
sudo nano /etc/network/interfaces
```

## Step 2: Configure the Static IP Address

**2. In the configuration file, identify the network interface (often “eth0” for wired connections or “wlan0” for wireless). For example, if the interface is “eth0”, configure it as follows:**

```
auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.1
```

- **address:** Set to the IP address you want, “192.168.1.2”.
- **netmask:** Typically “255.255.255.0” for a Class C network.
- **gateway:** The router’s IP address, commonly “192.168.1.1”.

**3. Save and exit the file (Ctrl + X , then Y, and Enter in nano editor).**

## **Step 3: Restart the Network Service:**

**4. Restart the network service to apply the changes:**

```
sudo systemctl restart networking
```

## **Step 4: Verify IP Configuration:**

**5. Use the `ip addr` or `ifconfig` command to verify the IP address is set correctly:**

```
ip addr show eth0
```

**Look for “192.168.1.2” in the output.**

## Step 5: Set Up a Service to Listen on Port 446

6. Create a simple listener on port `446`. You can use `netcat` (if installed) to listen on this port as a test:

```
sudo nc -lvp 446
```

- **-l: Listen mode.**
- **-v: Verbose mode to display additional information.**
- **-p: Specifies the port number.**

You can replace `netcat` with any service or script you want to run on this port.

## **Step 6: Verify the Port is Open :**

**7. Use netstat or ss to check that the port is open and listening:**

```
sudo ss -tuln | grep 446
```

**You should see LISTEN status for port 446.**

**You've now configured a static IP address on your Linux system and set up a service to listen on port `446`. This setup is ideal for local network communication and can be adapted further based on network requirements.**

## **Q5. List and execute the following LINUX/UNIX commands:**

- a) To list all the current users logged in the system.**
- b) To print and set the date.**
- c) To show the reference and name of the terminal.**
- d) To create a new file with name "abc" in the current directory.**
- e) To kill a process with its PID.**

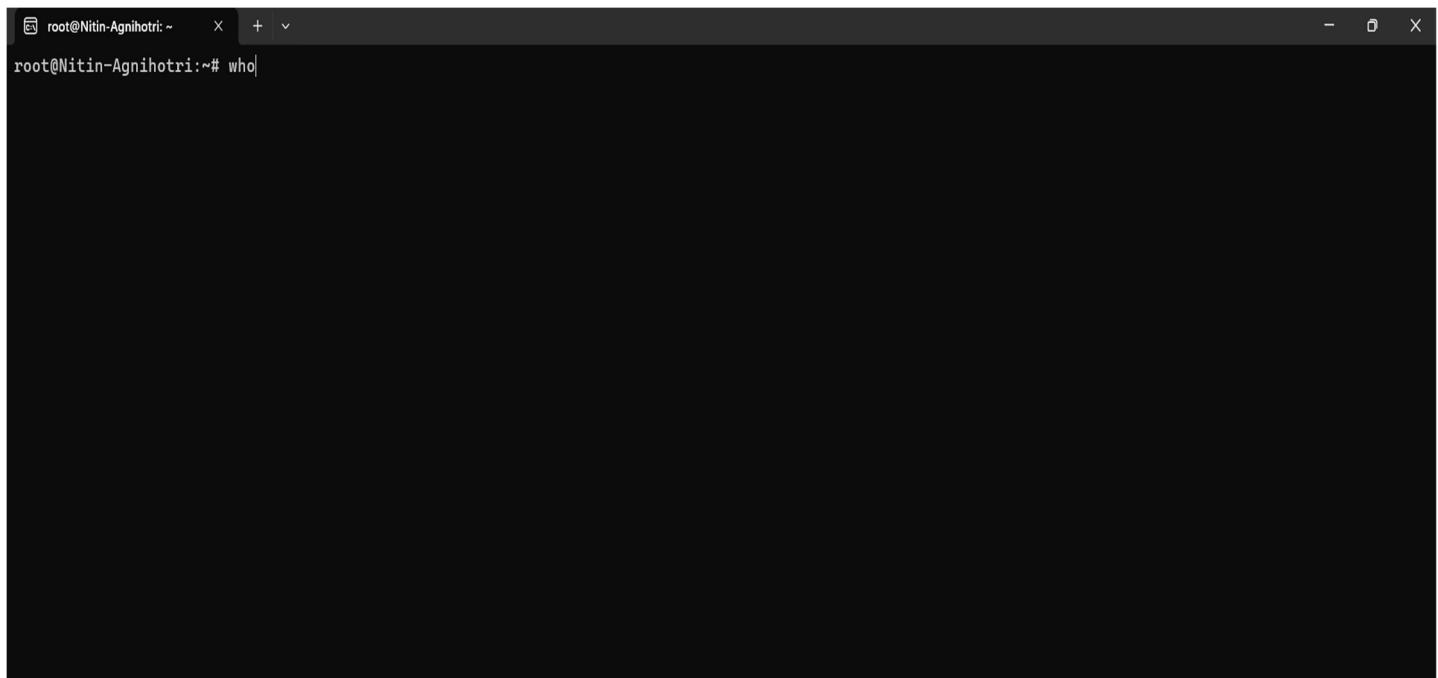
---

### **ANSWER :**

#### **(a) To List All the Current Users Logged in the System:**

**Command: ( “who” )→**

**← Use the who command to list all users currently logged in. →**



A screenshot of a terminal window titled 'root@Nitin-Agnihotri: ~'. The window shows a single line of text: 'root@Nitin-Agnihotri:~# who|'. The background of the terminal is black, and the text is white.

**Explanation:** This command displays the usernames, terminals, and login times for all active sessions.

## **(b) To Print and Set the Date:**

Use the date command to display and modify the system date.

- **To print the current date:**

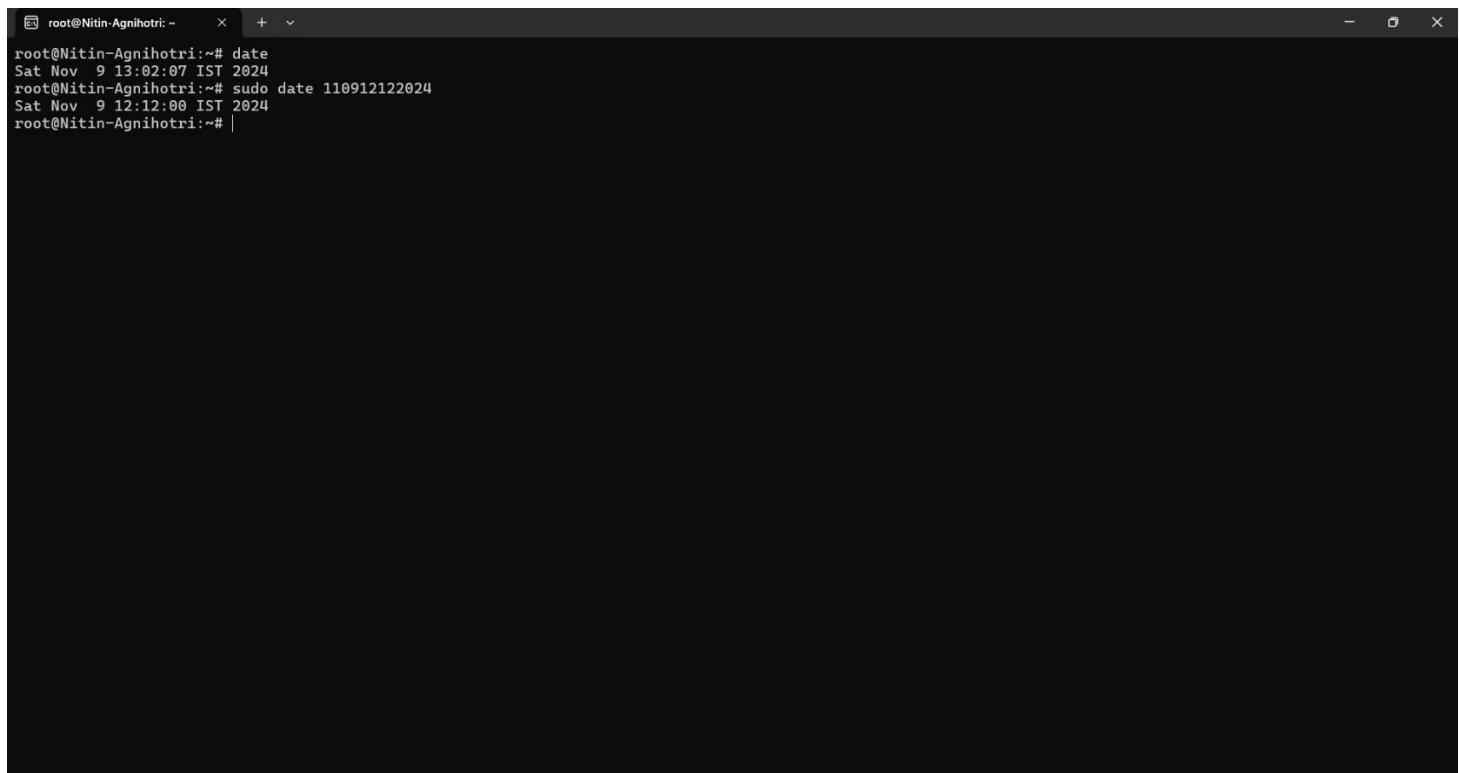
**Command: (“date”):**

- **To set a new date :**

**Command: “sudo date MMDDhhmmYYYY”:**

→ Replace **MM** with the month, **DD** with the day, **hh** with the hour, **mm** with the minutes, and **YYYY** with the year.

→ Example: To set the date to November 9, 2024, 12:12, use:

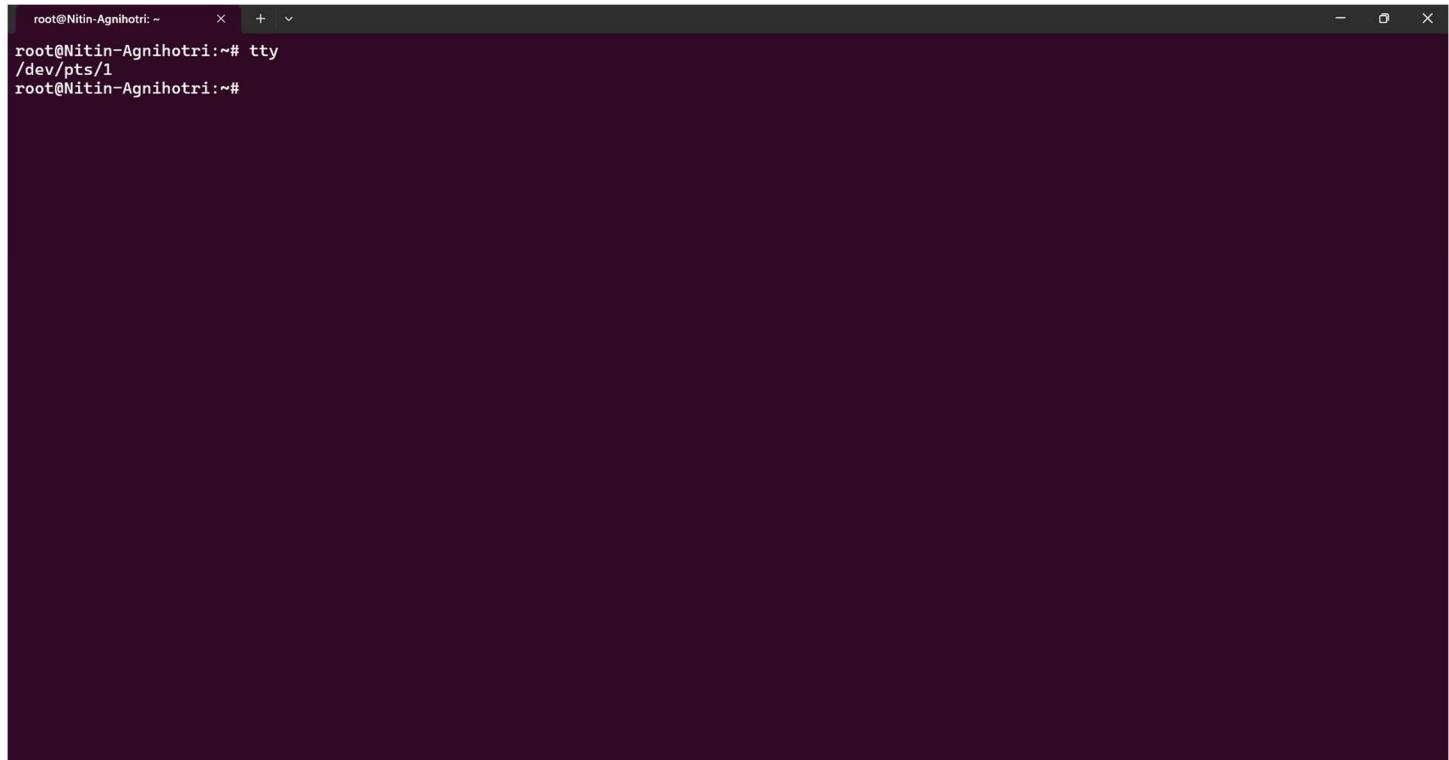


The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "root@Nitin-Agnihotri:~". Below that, the user runs the "date" command, which outputs the current date and time: "Sat Nov 9 13:02:07 IST 2024". Then, the user runs the "sudo date 110912122024" command, which changes the date and time to "Sat Nov 9 12:12:00 IST 2024". Finally, the user presses the enter key again at the prompt.

```
root@Nitin-Agnihotri:~# date
Sat Nov 9 13:02:07 IST 2024
root@Nitin-Agnihotri:~# sudo date 110912122024
Sat Nov 9 12:12:00 IST 2024
root@Nitin-Agnihotri:~# |
```

**(c) To Show the Reference and Name of the Terminal:**

→ Command: (“tty”):



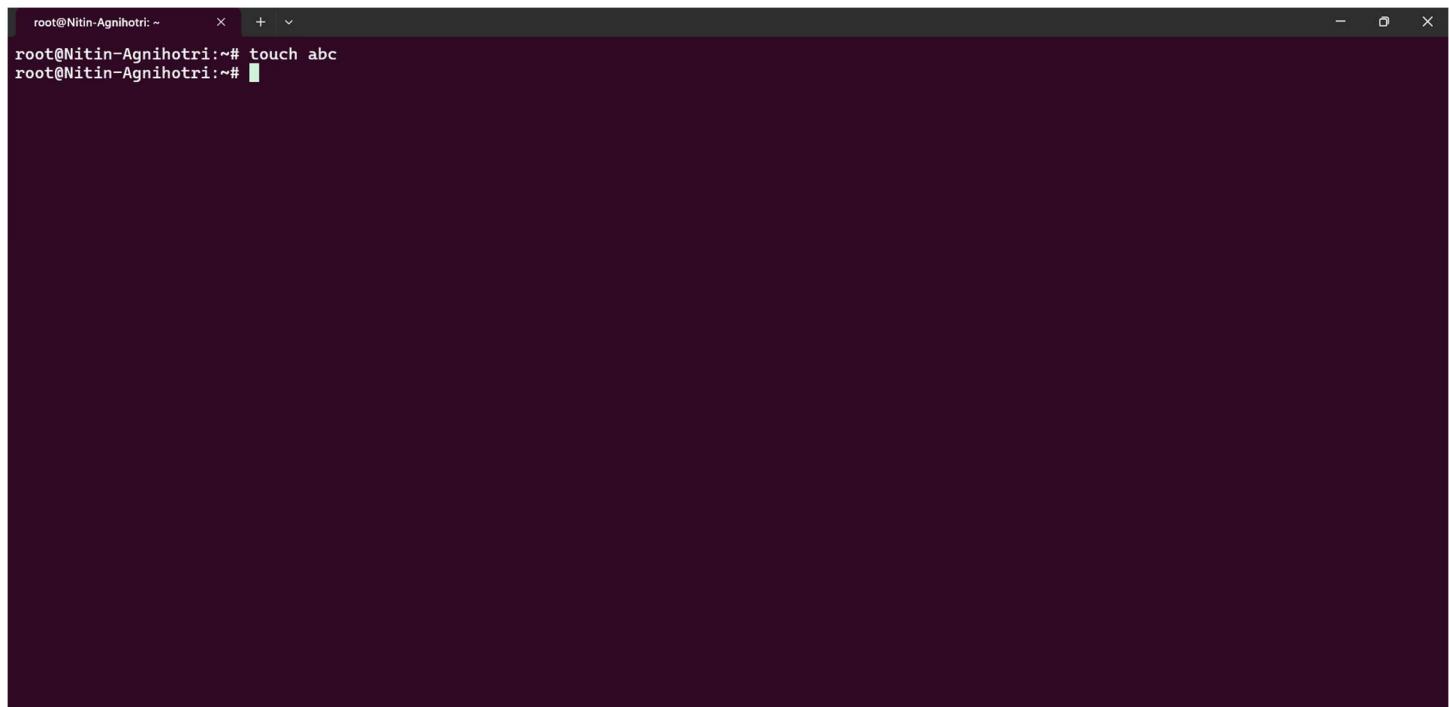
A screenshot of a terminal window titled "root@Nitin-Agnihotri:~". The window contains the following text:  
root@Nitin-Agnihotri:~# tty  
/dev/pts/1  
root@Nitin-Agnihotri:~#

**Explanation:** This command returns the file name of the terminal connected to standard input, showing the active terminal name.

**(d) To Create a New File with Name "abc" in the Current Directory:**

**Command: ( "abc" )**

**← Use the “touch” command to create an empty file named "abc". →**



A screenshot of a terminal window titled 'root@Nitin-Agnihotri: ~'. The window shows the command 'touch abc' being typed at the root prompt. The terminal has a dark background and light-colored text.

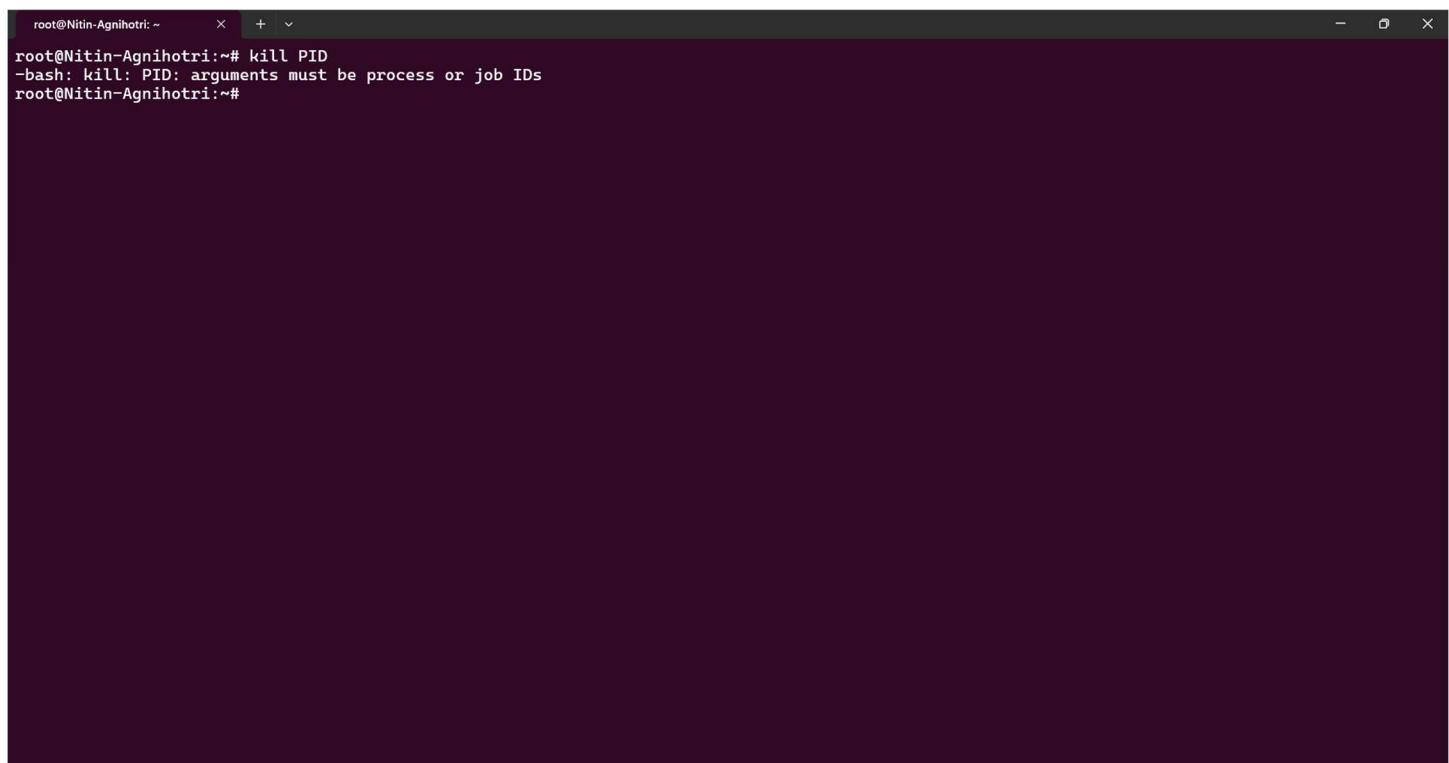
```
root@Nitin-Agnihotri:~# touch abc
```

**Explanation:** “touch” creates a new, empty file named "abc" in the current directory if it doesn't already exist.

## (e) To Kill a Process with Its PID:

**Command : “kill” :**

→ Use the “kill” command followed by the Process ID (PID) to terminate a process.

A screenshot of a terminal window titled "root@Nitin-Agnihotri: ~". The window has standard Linux-style window controls at the top. Inside the terminal, the user has entered the command "kill PID". The system has responded with an error message: "-bash: kill: PID: arguments must be process or job IDs". The prompt "root@Nitin-Agnihotri:~#" is visible at the bottom, indicating the user is root.

**Explanation:** Replace PID with the actual process ID of the process you want to terminate.