

M S Ramaiah Institute of Technology,

(Autonomous Institution Affiliated To)

Visvesvaraya Technological University, Belagavi)

M S Ramaiah Nagar, Mathikere, Bengaluru, Karnataka 560054

Nagar, Mathikere

BENGALURU - 560054

**Department
of
Master of Computer Applications**



**Lab Manual of
Computer Networks**

Course Code: MCA24

Faculty Incharge

Dr Manjunath M

Contents

1	IP addressing: Class Full Addressing	2
1.1	Hub	2
1.1.1	Characteristics	2
1.1.2	Example	3
1.1.3	Limitations	3
1.2	Switch	3
1.2.1	Characteristics	3
1.2.2	Example	3
1.2.3	Advantages	3
1.3	Steps to Create the LAN	4
1.4	Expected Outcome	6
2	Static Routing	7
2.1	Introduction to Router	7
2.2	Four Modes of Cisco Router Configuration	8
2.3	Basic Commands for Cisco Router Configuration with Examples	9
2.4	Static Routing Configuration	10
2.5	Expected Outcome	12
3	Installation and Configuration of FTP Server using ProFTPD	13
3.1	Steps to Install and Configure ProFTPD in Ubuntu	13
3.1.1	Expected Outcome	19
4	SSH Configuration and Remote Access Between Virtual Machines	20
4.1	Network Topology	20
4.2	Steps to Configure SSH Server on VM1	21
4.3	Configure SSH Client on VM2	23
4.4	Test SSH Access	23
4.5	Copy Files Using SCP	23
4.6	Expected Outcome	24

Lab Program - 1

1 IP addressing: Class Full Addressing

Using GNS3, create a Local Area Network (LAN) consisting of four VPCS nodes connected through a Hub as shown in figure 1. Assign appropriate IP addresses in the same subnet using the Class A private network 10.0.0.0/8. Configure each node to retain the settings across sessions, and verify end-to-end connectivity using the ping command.

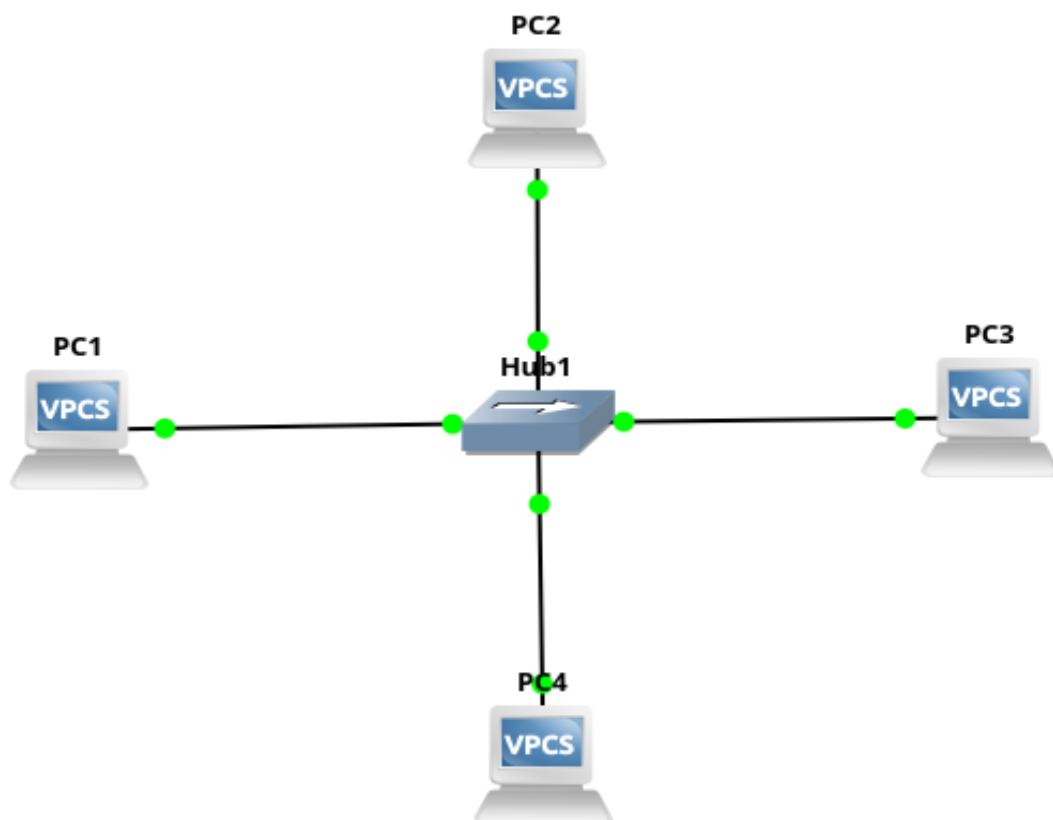


Figure 1: Local Are Network using Hub.

1.1 Hub

A **Hub** is a basic networking device that connects multiple devices in a Local Area Network (LAN). It operates at the **Physical Layer (Layer 1)** of the OSI model and forwards incoming data to **all connected devices**, regardless of the destination.

1.1.1 Characteristics

- Operates at OSI Layer 1 (Physical Layer)
- Broadcasts data to all connected ports

- Does not learn or store MAC addresses
- Cannot filter or direct traffic intelligently
- Creates one large collision domain

1.1.2 Example

If PC1 sends a message to PC2, the hub sends that message to PC2, PC3, and PC4, whether they need it or not.

1.1.3 Limitations

- Low efficiency and security
- High risk of collisions
- Not suitable for modern high-speed networks

1.2 Switch

A **Switch** is an intelligent networking device that connects devices in a LAN. It operates at the **Data Link Layer (Layer 2)** of the OSI model and forwards data only to the intended destination based on the **MAC address**.

1.2.1 Characteristics

- Operates at OSI Layer 2 (Data Link Layer)
- Learns and stores MAC addresses in a table
- Forwards data only to the correct device
- Supports full-duplex communication
- Each port has its own collision domain

1.2.2 Example

If PC1 sends data to PC2, the switch looks up the MAC address of PC2 and sends the data **only to PC2**, not to other devices.

1.2.3 Advantages

- Efficient use of bandwidth
- Reduced network traffic and collisions
- Improved security and performance

The table 1 highlights the key differences between a Hub and a Switch:

Feature	Hub	Switch
OSI Layer	Layer 1 (Physical)	Layer 2 (Data Link)
Data Forwarding	Broadcast to all devices	Forward to specific device
MAC Address Learning	No	Yes
Collision Domain	Single	One per port
Efficiency	Low	High
Security	Low	High
Usage Today	Rare	Common

Table 1: Comparison of Hub and Switch

1.3 Steps to Create the LAN

1. Create New Project:

- Open GNS3 and start a new project, e.g., LAN_Hub_Test.

2. Add a Hub:

- In the Devices panel, search for Hub.
- Drag and drop the Hub to the workspace.

3. Add 4 PCs (VPCS):

- Drag and drop VPCS nodes 4 times (VPCS1 to VPCS4).
- Place them around the Hub.

4. Connect PCs to the Hub:

- Use the Add Link tool (cable icon).
- Connect each VPCS's Ethernet0 to a unique port on the Hub.

5. Assign IP Addresses and Save:

- Open the console for each VPCS and Assign the IP Address as shown in figure 1
- VPCS1:
 - ip 10.0.0.1 255.0.0.0
 - save
- VPCS2:
 - ip 10.0.0.2 255.0.0.0
 - save

```

PC1> ip 10.0.0.1 255.0.0.0
Checking for duplicate address...
PC1 : 10.0.0.1 255.0.0.0

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show ip
NAME       : PC1[1]
IP/MASK    : 10.0.0.1/8
GATEWAY    : 255.0.0.0
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 10008
RHOST:PORT : 127.0.0.1:10009
MTU        : 1500
PC1>

```

(a) Assigning IP to PC1

```

PC2> ip 10.0.0.2 255.0.0.0
Checking for duplicate address...
PC2 : 10.0.0.2 255.0.0.0

PC2> save
Saving startup configuration to startup.vpc
. done

PC2> show ip
NAME       : PC2[1]
IP/MASK    : 10.0.0.2/8
GATEWAY    : 255.0.0.0
DNS        :
MAC        : 00:50:79:66:68:01
LPORT     : 10010
RHOST:PORT : 127.0.0.1:10011
MTU        : 1500
PC2>

```

(b) Assigning IP to PC2

```

PC3> ip 10.0.0.3 255.0.0.0
Checking for duplicate address...
PC3 : 10.0.0.3 255.0.0.0

PC3> save
Saving startup configuration to startup.vpc
. done

PC3> show ip
NAME       : PC3[1]
IP/MASK    : 10.0.0.3/8
GATEWAY    : 255.0.0.0
DNS        :
MAC        : 00:50:79:66:68:02
LPORT     : 10012
RHOST:PORT : 127.0.0.1:10013
MTU        : 1500
PC3>

```

(c) Assigning IP to PC3

```

PC4> ip 10.0.0.4 255.0.0.0
Checking for duplicate address...
PC4 : 10.0.0.4 255.0.0.0

PC4> save
Saving startup configuration to startup.vpc
. done

PC4> show ip
NAME       : PC4[1]
IP/MASK    : 10.0.0.4/8
GATEWAY    : 255.0.0.0
DNS        :
MAC        : 00:50:79:66:68:03
LPORT     : 10014
RHOST:PORT : 127.0.0.1:10015
MTU        : 1500
PC4>

```

(d) Assigning IP to PC4

Figure 2: IP assignment process for all four PCs in the LAN setup.

- VPCS3:
 - ip 10.0.0.3 255.0.0.0
 - save
- VPCS4:
 - ip 10.0.0.4 255.0.0.0
 - save

6. Test Connectivity:

- From VPCS1 console, use the following commands to test connectivity:
 - ping 10.0.0.2
 - ping 10.0.0.3
 - ping 10.0.0.4
- Ensure successful replies to confirm communication between all devices.
- **Note:** A successful reply from the destination indicates that the connection exists.
- **Time To Live (TTL):**

- TTL is a field in the IP header that indicates the number of routers (hops) a packet can cross.
- Default TTL values:
 - * Windows: 128
 - * Linux: 64
 - * Routers: 255
- If the TTL expires before reaching the destination, the packet is dropped.
- This prevents packets from endlessly looping in the network.
- **ARP Behavior During Ping:**
 - If the system does not know the destination MAC address (DMAC), it sends an ARP Request packet.
 - The destination system replies with an ARP Reply containing the MAC address.
 - The sender saves this mapping in the ARP table.

7. Optional Enhancements:

- Add Wireshark to monitor traffic (e.g., ARP, ICMP).
- Replace the Hub with a Switch and observe changes in traffic behavior.
- Simulate the same setup using:
 - Class B network: 172.16.0.0/16
 - Class C network: 192.168.1.0/24
- Compare address configuration differences between Class A, B, and C networks.

1.4 Expected Outcome

- All PCs (VPCS1 to VPCS4) should communicate via the hub or switch.
- Each PC should reply to ping from other PCs.
- ARP tables should show MAC mappings after pinging.
- Wireshark should capture ARP and ICMP packets.
- The setup shows basic LAN communication with manual IPs.

Lab Program - 2

2 Static Routing

- Static routing is a method of manually configuring routes in a router's routing table.
- In static routing, the network administrator defines the path for data packets manually.
- Unlike dynamic routing, routers do not automatically learn routes.
- Dynamic routing uses protocols like RIP and OSPF to discover routes automatically.

2.1 Introduction to Router

- A router is a networking device that connects multiple computer networks and directs data packets between them.
- It analyzes incoming data packets, determines their destination address, and chooses the best path to forward them.
- Routers operate at Layer 3 (Network Layer) of the OSI model.
- They are essential for establishing communication between different IP networks.
- Routers are widely used in homes, businesses, and data centers.
- They manage traffic between local networks (LANs) and the internet (WAN).

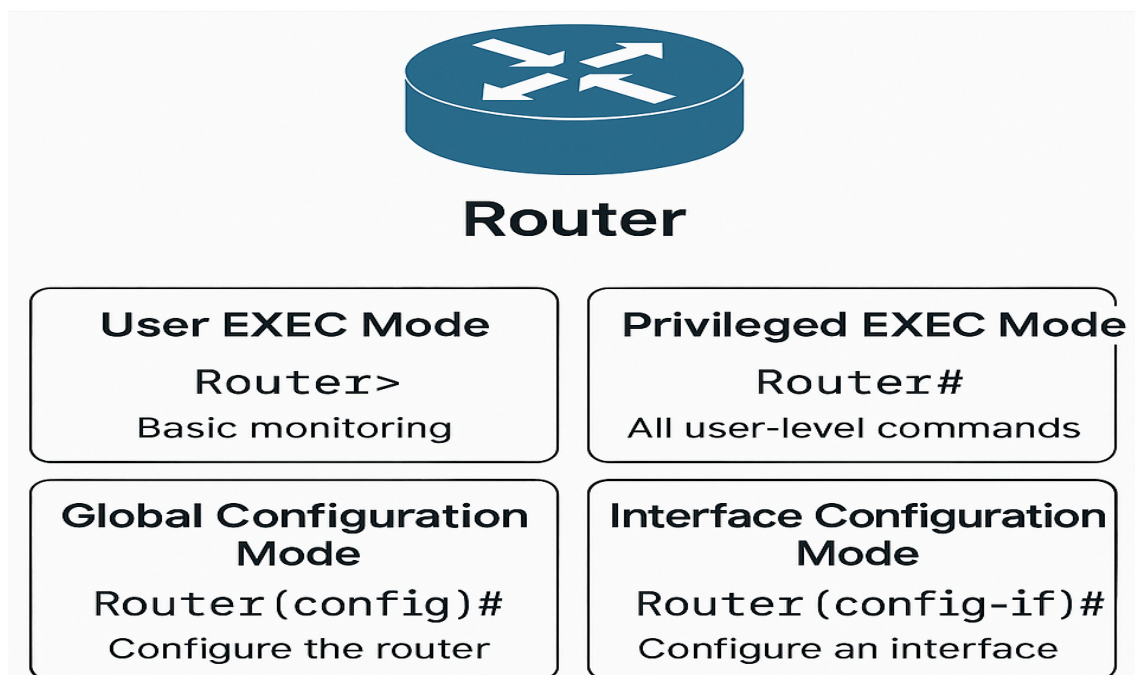


Figure 3: Operational Modes of a Cisco Router: User EXEC, Privileged EXEC, Global Configuration, and Interface Configuration

- Cisco routers offer various configuration modes for effective administration and troubleshooting.
- The four main modes of a Cisco router are listed below and shown in figure 3
 - User EXEC Mode
 - Privileged EXEC Mode
 - Global Configuration Mode
 - Interface Configuration Mode

2.2 Four Modes of Cisco Router Configuration

1. User EXEC Mode:

- Prompt: Router>
- This is the initial mode after accessing the router.
- Allows basic monitoring commands.
- Example: `show version`, `ping 8.8.8.8`

2. Privileged EXEC Mode:

- Prompt: Router#
- Entered by typing `enable` at the User EXEC prompt.
- Allows access to all configuration and management commands.
- Example: `show running-config`, `reload`

3. Global Configuration Mode:

- Prompt: Router(config)#
- Entered by typing `configure terminal` in Privileged EXEC Mode.
- Used to configure global router settings like hostname, routing, etc.
- Example: `hostname CoreRouter`

4. Interface Configuration Mode:

- Prompt: Router(config-if)#
- Entered by typing `interface FastEthernet0/0` in Global Config Mode.
- Used to configure individual interfaces (IP, speed, description).
- Example:
 - `ip address 192.168.1.1 255.255.255.0`
 - `no shutdown`

2.3 Basic Commands for Cisco Router Configuration with Examples

1. User EXEC Mode Commands:

- Prompt: Router>
- `ping 192.168.1.1` — Check if 192.168.1.1 is reachable.
- `traceroute 8.8.8.8` — Trace the route to Google DNS.
- `show version` — Displays OS version, memory, etc.
- `show ip interface brief` — Summarizes interface status and IPs.

2. Privileged EXEC Mode Commands:

- Prompt: Router#
- `enable` — Enter this to switch from user mode to privileged mode.
- `show running-config` — View current settings in RAM.
- `show startup-config` — View the saved config from NVRAM.
- `copy running-config startup-config` — Save config: Example: `copy running-config startup-config`
- `reload` — Restarts the router. Example: `reload`

3. Global Configuration Mode Commands:

- Prompt: Router(config)#
- `hostname CoreRouter` — Sets hostname to "CoreRouter".
- `interface FastEthernet0/0` — Enters config mode for FastEthernet0/0.
- `ip route 10.0.0.0 255.0.0.0 192.168.1.2` — Static route to network 10.0.0.0 via 192.168.1.2.

4. Interface Configuration Mode Commands:

- Prompt: Router(config-if)#
- `ip address 192.168.1.1 255.255.255.0` — Assigns IP to interface.
- `no shutdown` — Enables the interface.
- `description Link-to-Switch1` — Adds a label for the connection.
- `duplex full, speed 100` — Sets full duplex and 100 Mbps speed.

5. Other Useful Shortcuts:

- TAB — Typing `sh` + TAB autocompletes to `show`.
- Ctrl + Z — Exits to privileged EXEC mode from any config mode.
- Ctrl + C — Interrupts a ping or config command.
- ? — Typing `show ?` lists all "show" subcommands.

2.4 Static Routing Configuration

Consider the network as shown in figure 4 and configure static routing between two routers (R1 and R2) using FastEthernet interfaces. Assign IP addresses to each interface and verify connectivity using ping. Add static routes manually so that both routers can reach each other's LAN networks.

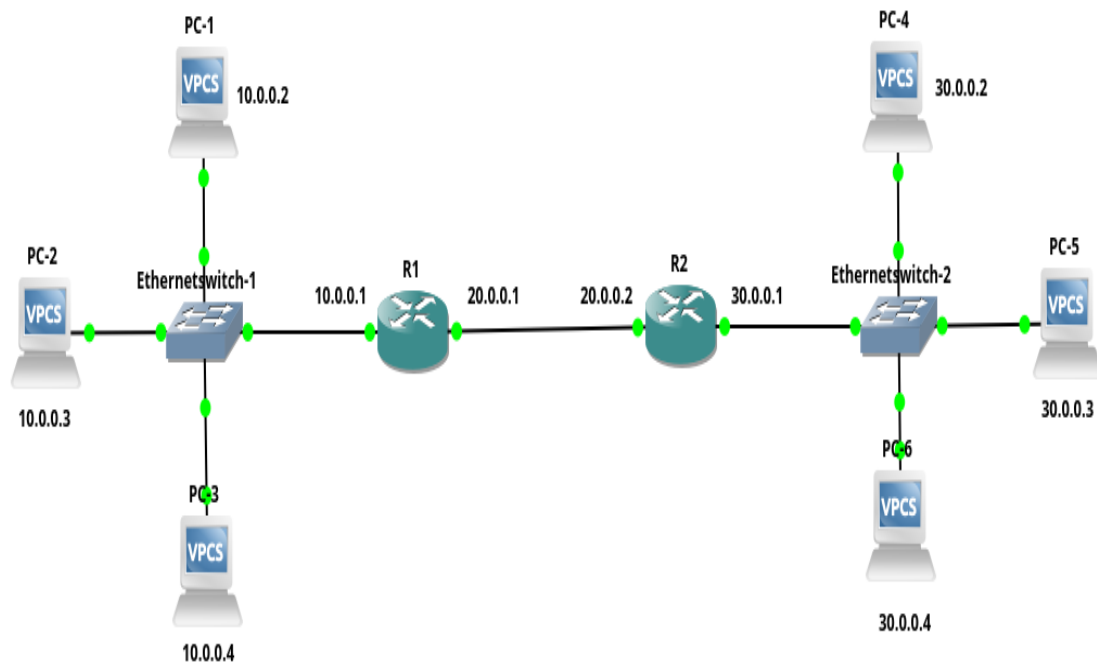


Figure 4: Operational Modes of a Cisco Router: User EXEC, Privileged EXEC, Global Configuration, and Interface Configuration

- **Network Details:**

- R1 FastEthernet0/0: 10.0.0.1 (10.0.0.0/8 network)
- R1 FastEthernet0/1: 20.0.0.1 (20.0.0.0/8 network)
- Interconnecting Network (between R1 and R2): 20.0.0.0/8
- R2 FastEthernet0/0: 20.0.0.2
- R2 FastEthernet0/1: 30.0.0.1

- **Router Configuration Commands:**

```
! R1 Configuration
```

```
R1(config)# interface fastethernet0/0
```

```
R1(config-if)# ip address 10.0.0.1 255.0.0.0
```

```
R1(config-if)# no shutdown
```

```
R1(config)# interface fastethernet0/1
```

```
R1(config-if)# ip address 20.0.0.1 255.0.0.0
```

```
R1(config-if)# no shutdown

! R2 Configuration
R2(config)# interface fastethernet0/0
R2(config-if)# ip address 20.0.0.2 255.0.0.0
R2(config-if)# no shutdown

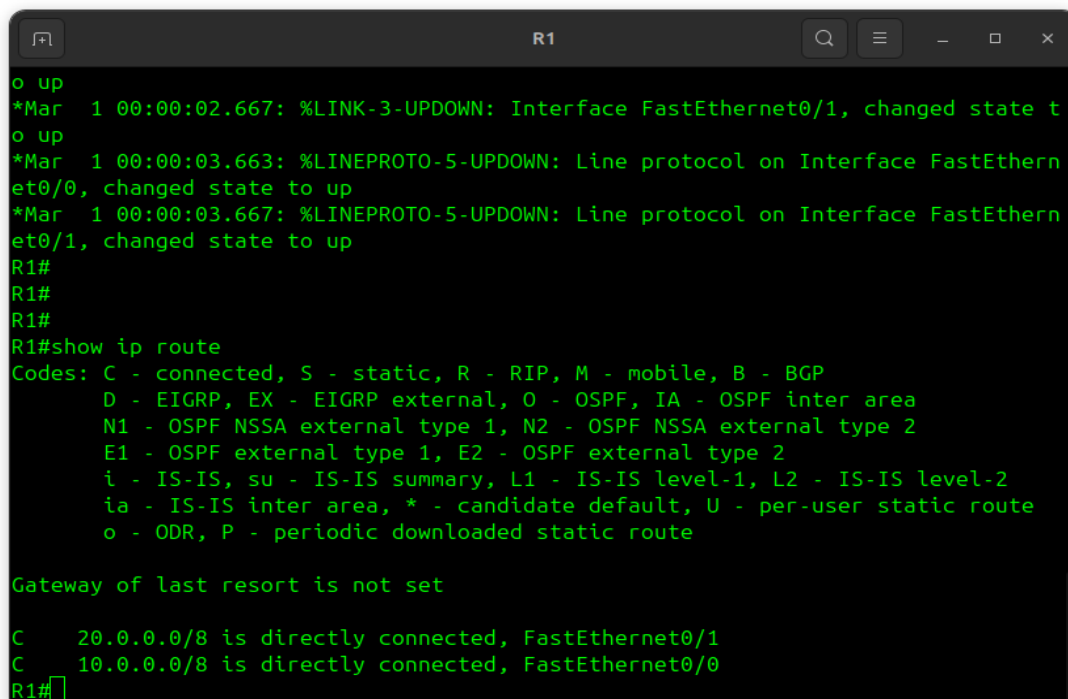
R2(config)# interface fastethernet0/1
R2(config-if)# ip address 30.0.0.1 255.0.0.0
R2(config-if)# no shutdown

! Static Route for R1
R1(config)# ip route 30.0.0.0 255.0.0.0 20.0.0.2

! Static Route for R2
R2(config)# ip route 10.0.0.0 255.0.0.0 20.0.0.1
```

Static Route Syntax

```
ip route <destination-network> <subnet-mask> <next-hop-IP>
```

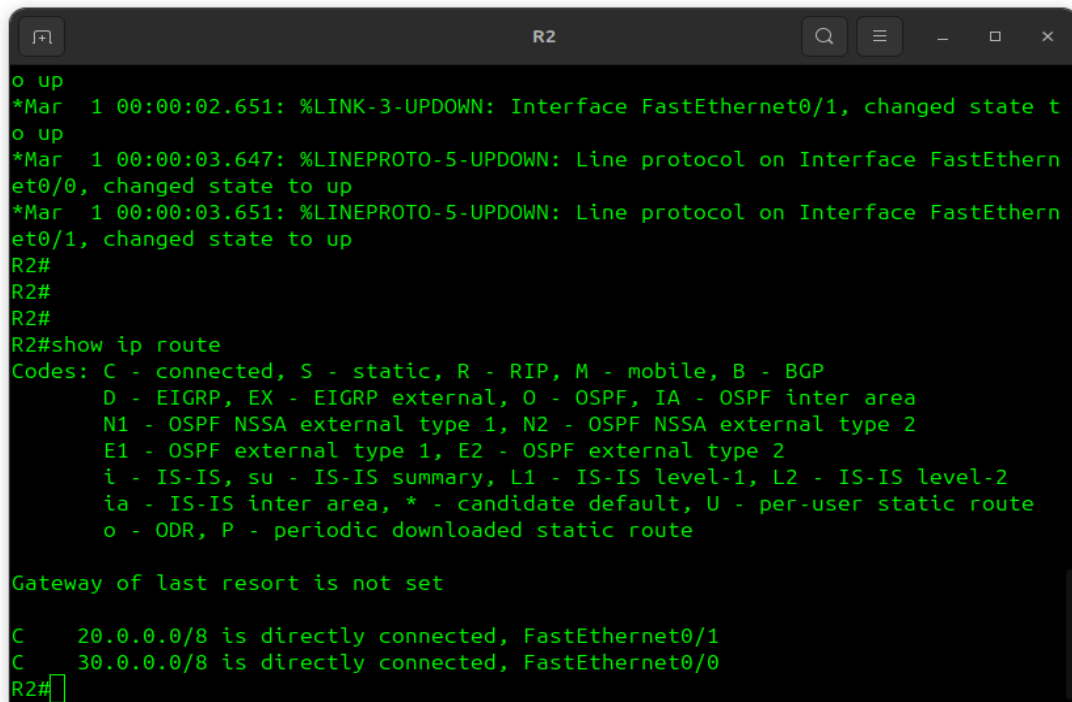


```
R1
o up
*Mar  1 00:00:02.667: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:00:03.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
*Mar  1 00:00:03.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R1#
R1#
R1#
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    20.0.0.0/8 is directly connected, FastEthernet0/1
C    10.0.0.0/8 is directly connected, FastEthernet0/0
R1#
```

Figure 5: Routing Table of R1 Router



```
R2
o up
*Mar  1 00:00:02.651: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
o up
*Mar  1 00:00:03.647: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:03.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2#
R2#
R2#
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    20.0.0.0/8 is directly connected, FastEthernet0/1
C    30.0.0.0/8 is directly connected, FastEthernet0/0
R2#
```

Figure 6: Routing Table of R2 Router

2.5 Expected Outcome

- All interfaces on both routers should transition to the up/up state after applying the no shutdown command.
- R1 and R2 should be able to successfully ping each other's LAN interfaces (10.0.0.1 and 30.0.0.1) through the 20.0.0.0/8 interconnecting network.
- The show ip route command should display the manually added static routes in the routing table as shown in figure 5 and 6 respectively.
- The show ip interface brief command should confirm correct IP addressing and interface status.
- This setup verifies the concept of static routing, where routes are manually configured to enable inter-network communication.

3 Installation and Configuration of FTP Server using ProFTPD

- To install and configure an FTP server on **PC1** using ProFTPD and allow FTP clients to upload and download files successfully.
- The setup should ensure secure user access with proper directory permissions and demonstrate file sharing from remote machines via FTP.

3.1 Steps to Install and Configure ProFTPD in Ubuntu

- **Update the system**
 - `sudo apt update`
- **Install ProFTPD as shown in figure 7**
 - `sudo apt install proftpd`
 - During installation, choose standalone mode and press Enter to finish.

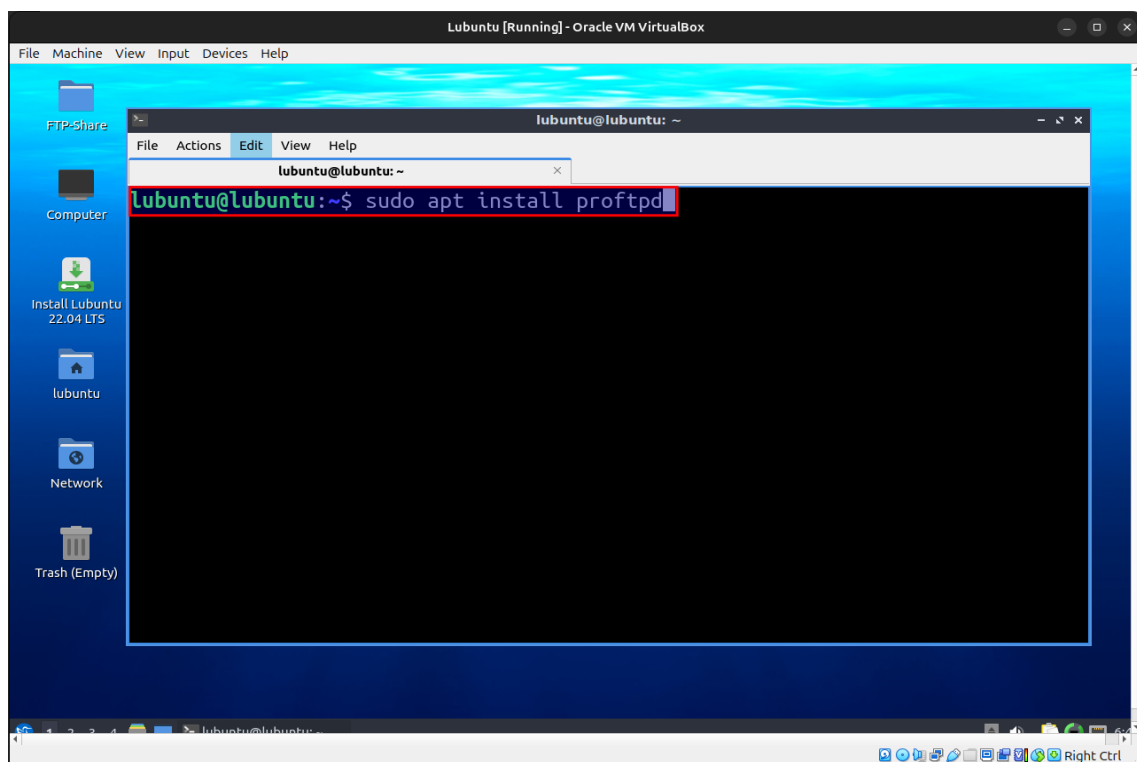
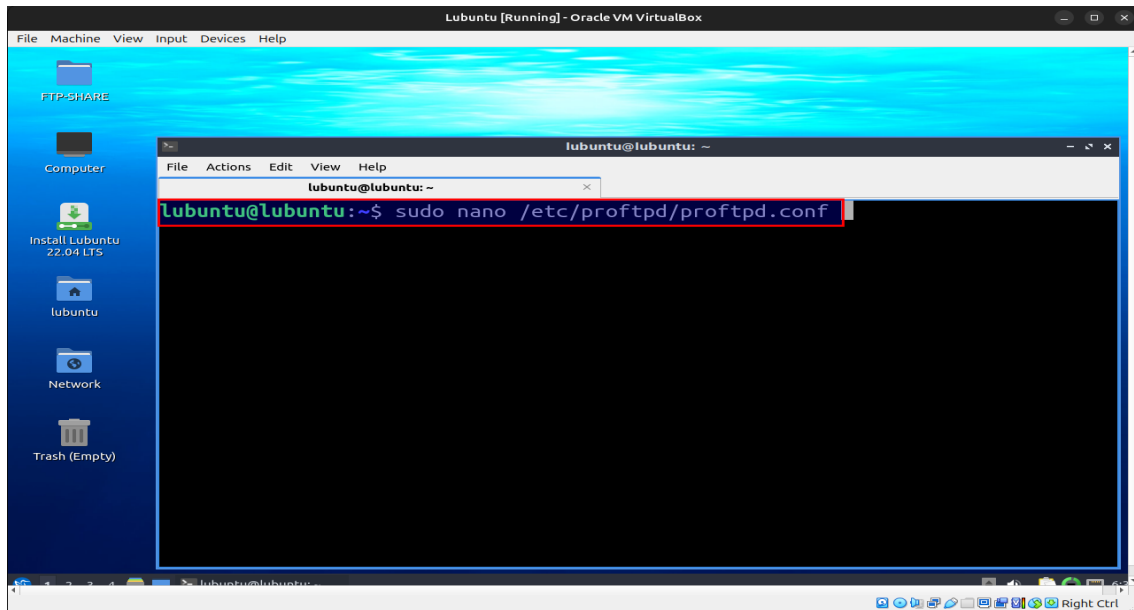
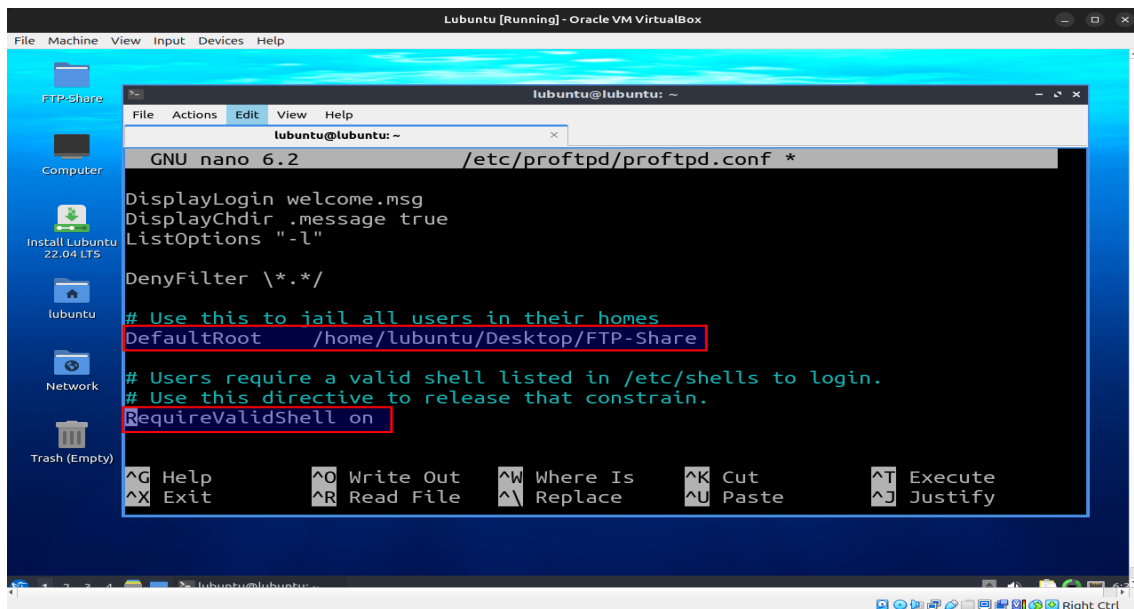


Figure 7: Proftpd Instalation

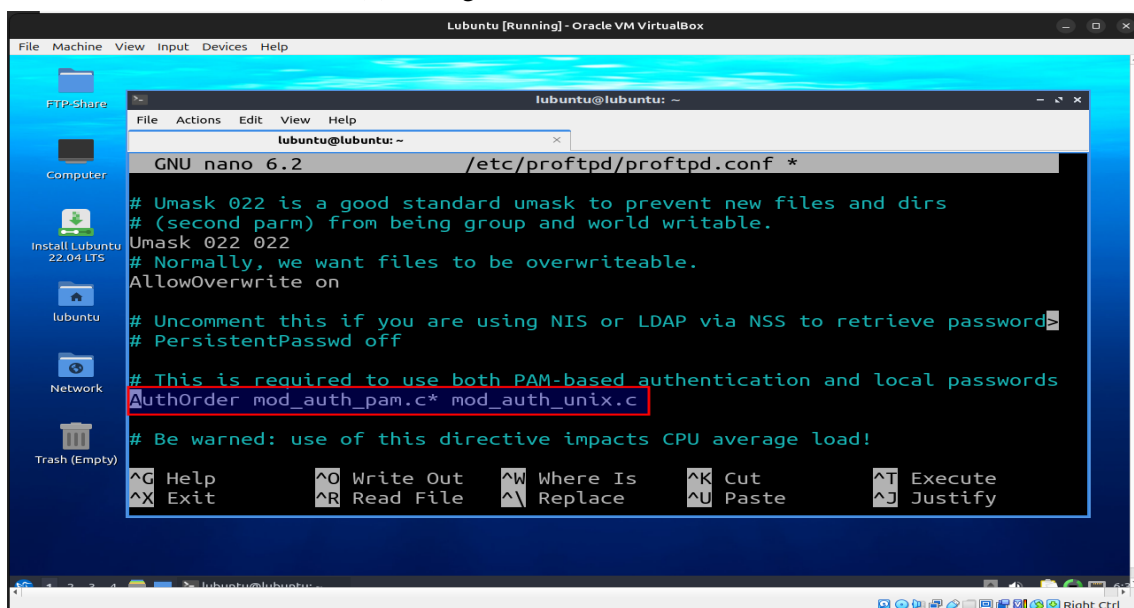
- **Configure ProFTPD as shown in figure 8a**
 - `sudo nano /etc/proftpd/proftpd.conf`
 - Make the following changes in the config file:



(a) Configuration file path of ProFTPD



(b) Configuration file of ProFTPD - 1



(c) Configuration file of ProFTPD - 2

- * Uncomment DefaultRoot /home/lubuntu/Desktop/FTP-Share as shown in figure 8b
 - * Set RequireValidShell on
 - * Uncomment AuthOrder mod_auth_unix.c as shown in figure 8c
 - Save and exit using Ctrl + O, Enter, and Ctrl + X.
- **Add /bin/false to valid shells**
 - sudo nano /etc/shells
 - Add the following line at the end: /bin/false as shown in figure 9

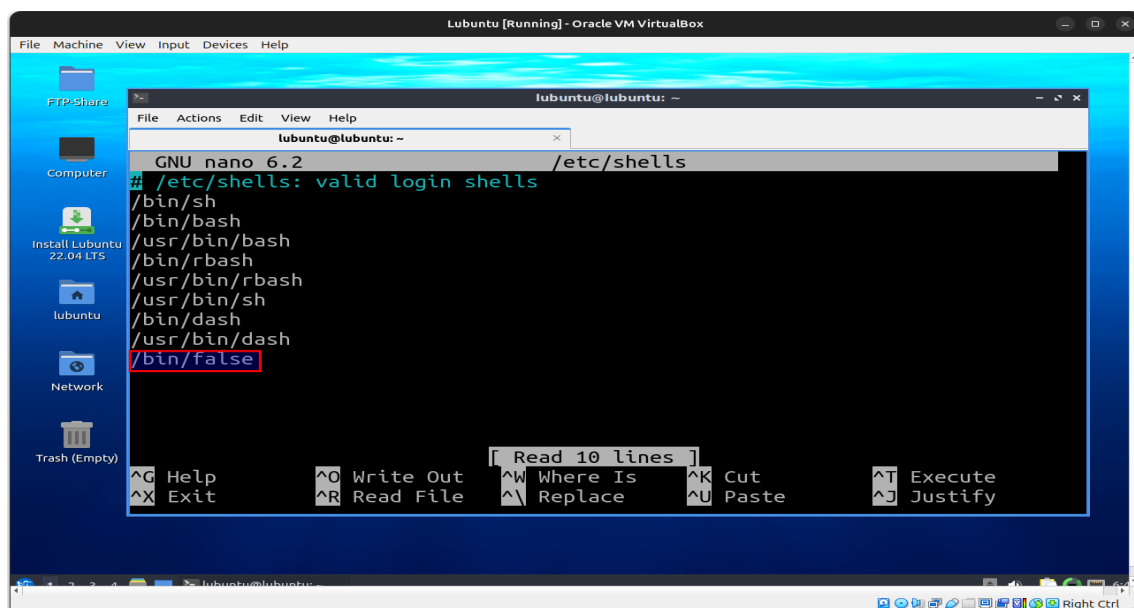


Figure 9: /etc/shells updated with /bin/false

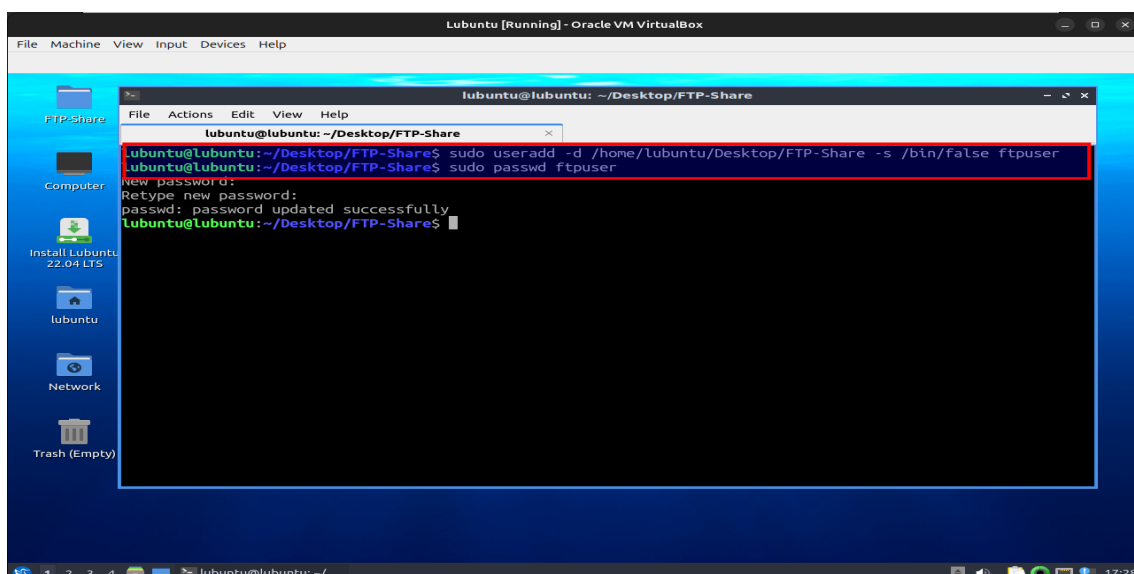


Figure 10: Creating FTP user ftpuser with /bin/false shell

- **Create FTP User**

- `sudo useradd -d /home/lubuntu/Desktop/FTP-Share -s /bin/false ftpuser`
as shown in figure 10
- `sudo passwd ftpuser`
- Set a password (e.g., 12345) when prompted.

- **Create FTP Directory and Set Permissions**

- `sudo chown ftpuser:ftpuser /home/lubuntu/Desktop/FTP-Share`

- **Restart ProFTPD Service**

- `sudo systemctl restart proftpd` as shown in figure 11

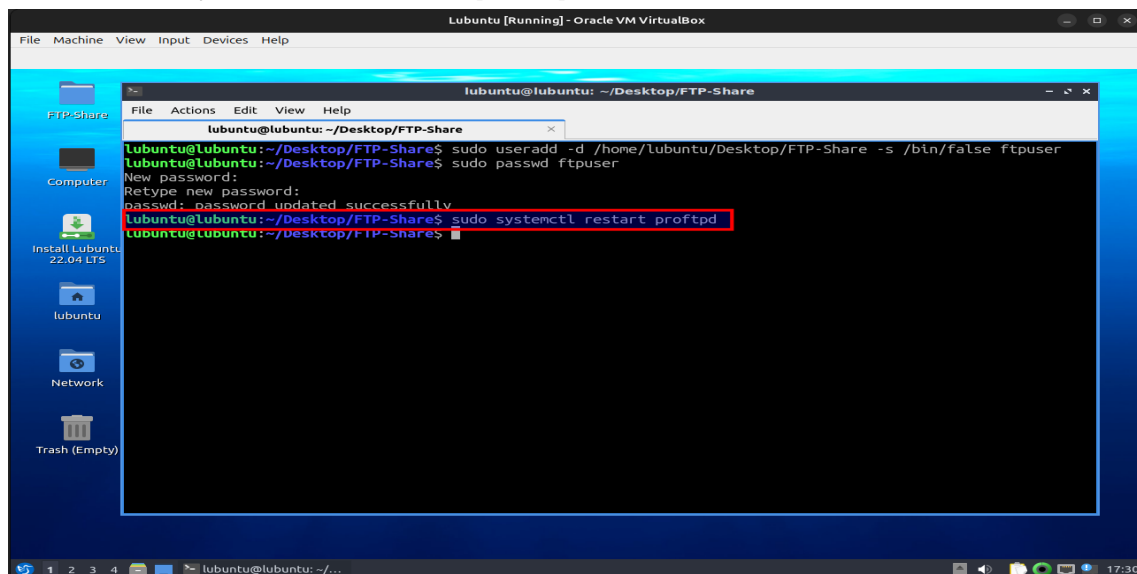


Figure 11: Restarting ProFTPD Service

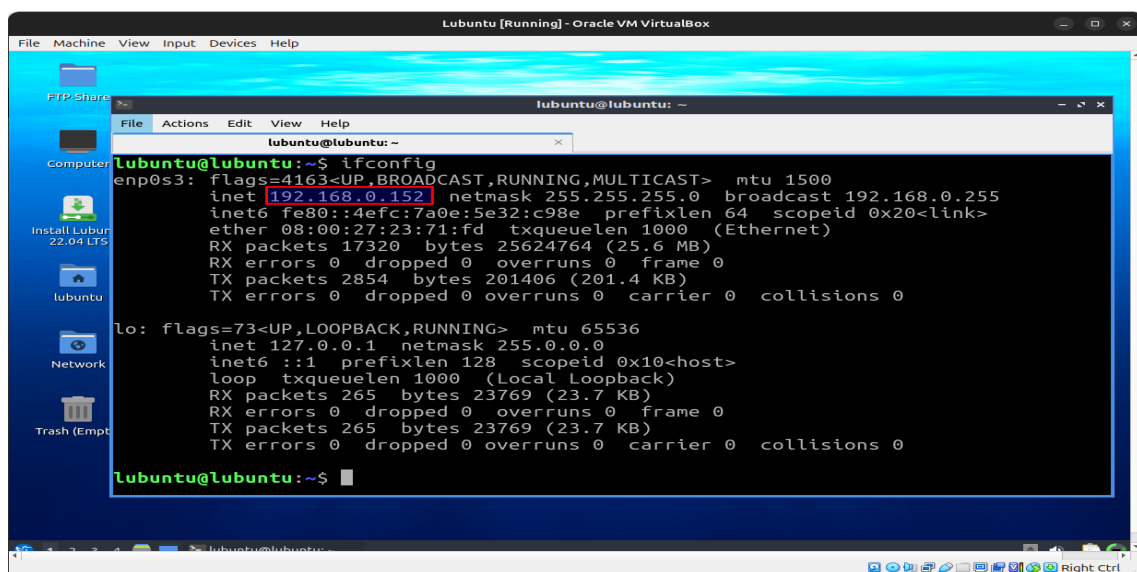


Figure 12: IP address of FTP Server

- **Verify and Access FTP Server**

- First, verify the IP address of the FTP server using the `ifconfig` or `ip a` command as shown in figure 12.

- **From a remote machine (e.g., PC2 or PC3), connect to the FTP server as shown in figure 13**

```
ftp 192.168.0.158
```

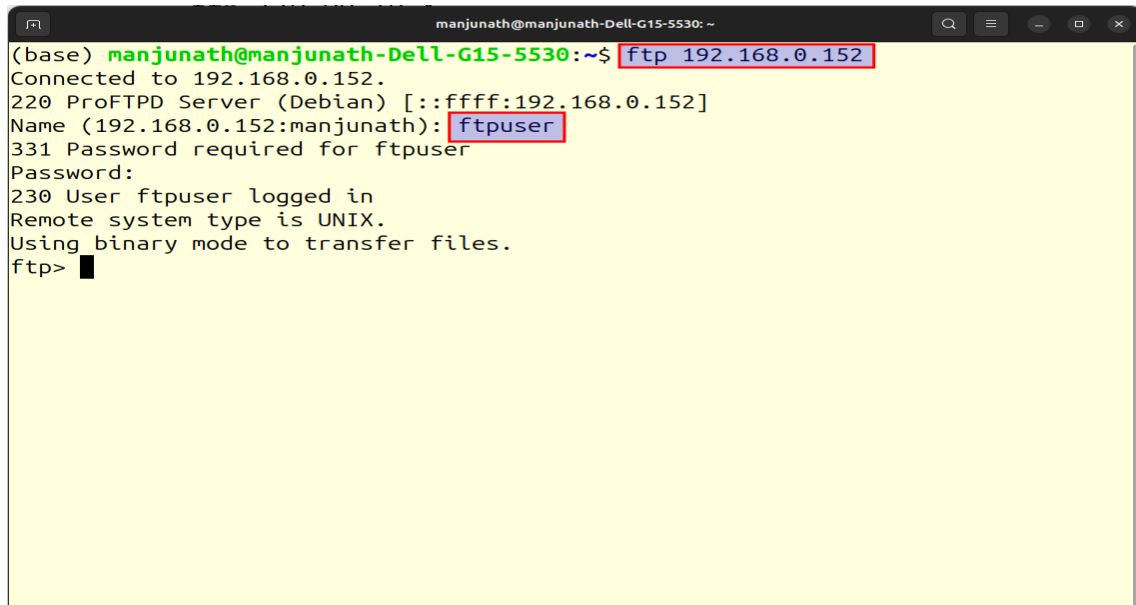


Figure 13: Connecting from Remote Machine

- **Test File Transfer Commands**

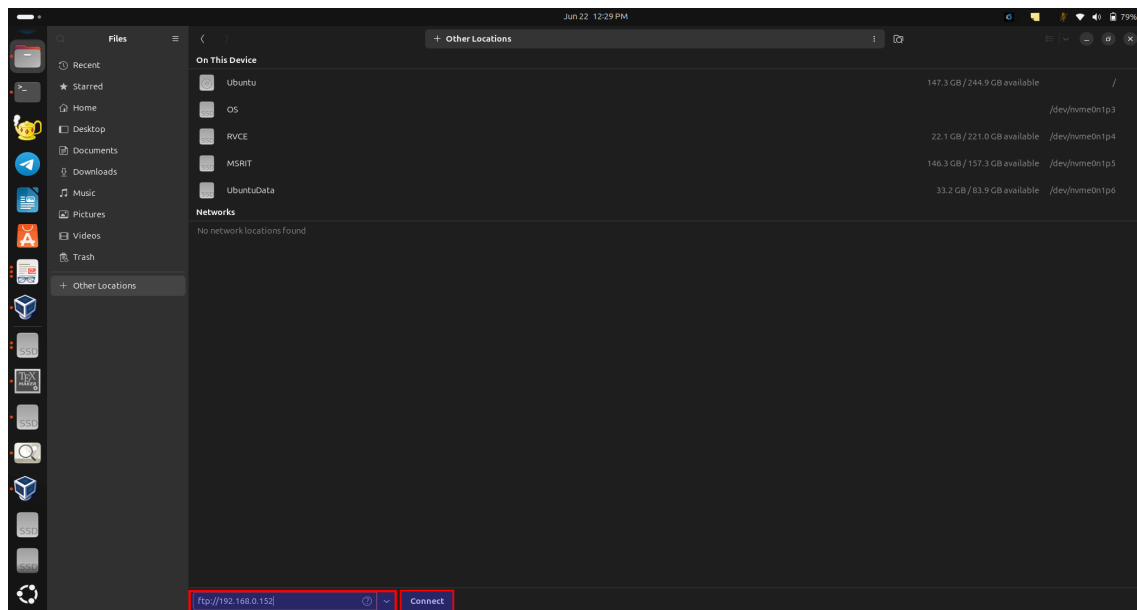
```
put Hello.txt      -- Upload a file to the server
get Hello.txt      -- Download a file from the server
ls                 -- List files on the server
quit               -- Exit the FTP session
```

- **Fix: 550 Permission Denied Error (if any)**

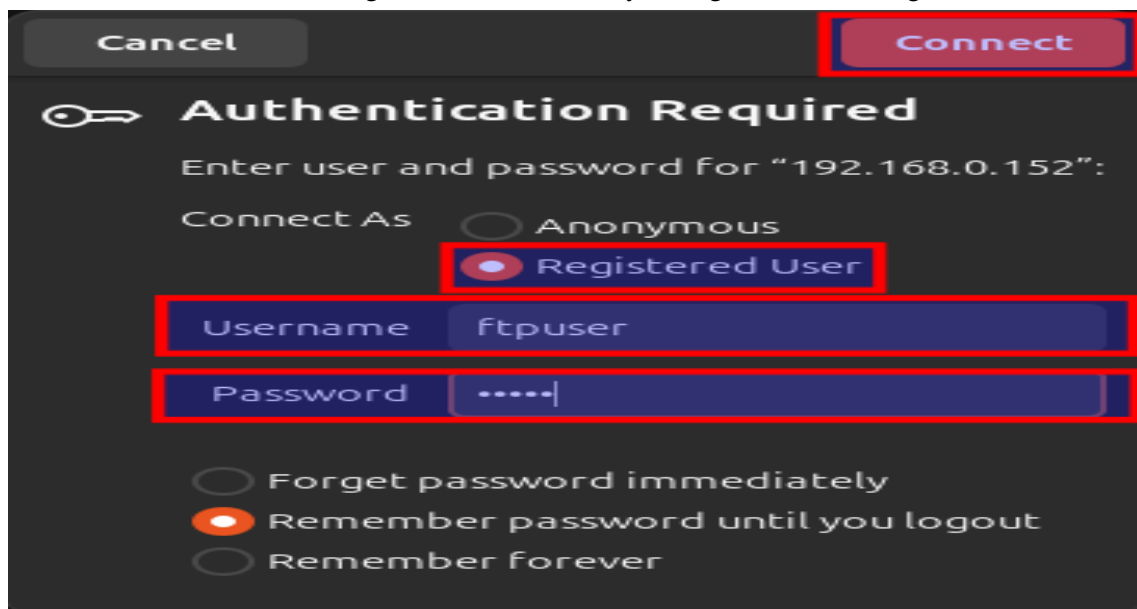
- This error usually indicates incorrect directory ownership or permissions.
- Run the following commands to resolve:

```
sudo chown ftpuser:ftpuser /home/lubuntu/Desktop/FTP-Share
sudo chmod 755 /home/lubuntu/Desktop/FTP-Share
sudo systemctl restart proftpd
```

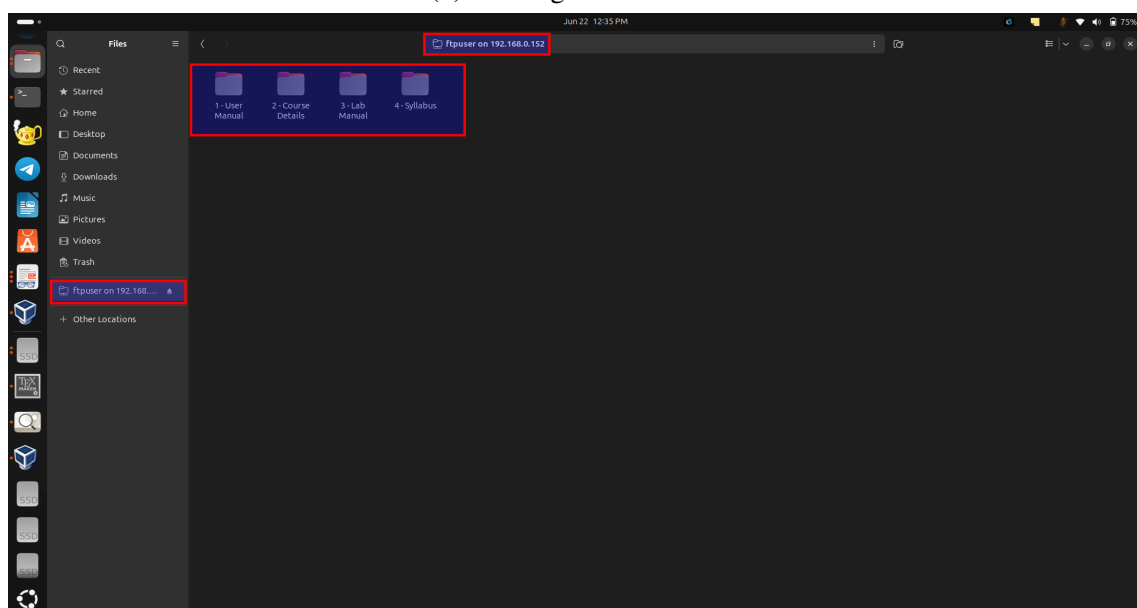
- Alternatively, on Ubuntu, go to Other Locations in the File Manager as shown in figure 14a and enter:



(a) Connecting FTP Server Remotely through the File Manager



(b) FTP login credentials



(c) Accessing File System for Downloading and Uploading files

`ftp://192.168.0.158`

- Provide the FTP login credentials as shown in figure 14b
 - Username: `ftpuser`
 - Password: (as set during user creation)
- Once connected, you can browse, upload, and download files as shown in figure 14c.

3.1.1 Expected Outcome

- The ProFTPD service should install successfully without errors.
- The configuration file should reflect the correct settings including the specified root directory and valid shell.
- The FTP user `ftpuser` should be created with restricted shell access using `/bin/false`.
- The directory `/home/lubuntu/Desktop/FTP-Share` should have correct ownership and permissions for file operations.
- The FTP server should be accessible from remote machines using both terminal-based FTP clients and GUI-based file browsers (via `ftp://`).
- File upload and download operations (`put`, `get`) should execute without errors such as permission denied or access issues.
- The login screen (via terminal or GUI) should successfully authenticate the `ftpuser` using the assigned password.
- Any file transferred from the client should be visible in the server's shared folder and accessible for further operations.
- The IP address of the FTP server should be correctly identified and reachable on the local network.
- In case of a permission error (e.g., `550 Permission denied`), applying the correct ownership and permission fix should resolve the issue.
- The ProFTPD service should remain active and restart successfully upon system reboot or manual restart.

4 SSH Configuration and Remote Access Between Virtual Machines

- To securely access a remote Linux-based virtual machine over a routed network, SSH (Secure Shell) is configured using the `openssh-server` package.
- This setup enables encrypted terminal access and secure file transfers using the `scp` command between VMs (e.g., VM2 to VM1).

4.1 Network Topology

- The network consists of six devices: four end systems (two VMs and four PCs) and two routers interconnected via switches as shown in figure 15.

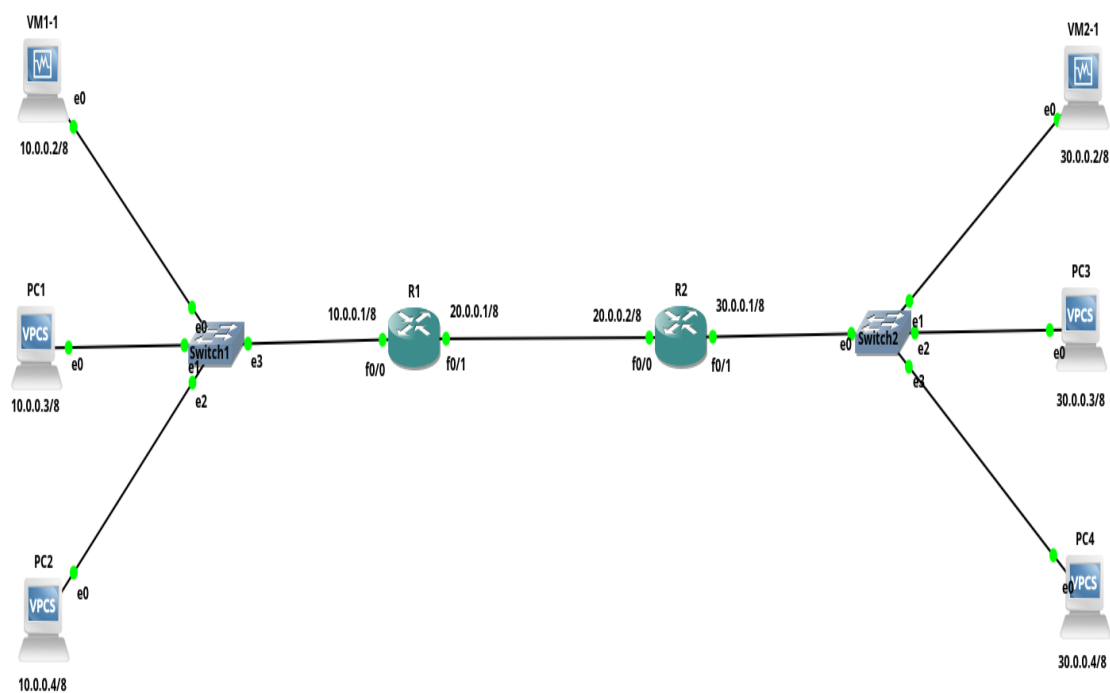


Figure 15: Network Topology

- The addressing and interface configuration is provided below:
 - VM1: 10.0.0.2/8
 - PC1: 10.0.0.3/8
 - PC2: 10.0.0.4/8
 - Router1:
 - * FastEthernet0/0: 10.0.0.1 255.0.0.0
 - * FastEthernet0/1: 20.0.0.1 255.0.0.0
 - Router2:

- * FastEthernet0/0: 20.0.0.2 255.0.0.0
 - * FastEthernet0/1: 30.0.0.1 255.0.0.0
 - VM2: 30.0.0.2/8
 - PC3: 30.0.0.3/8
 - PC4: 30.0.0.4/8
- Ensure static routing is configured between routers so that both subnets (10.0.0.0/8 and 30.0.0.0/8) are reachable end-to-end.

4.2 Steps to Configure SSH Server on VM1

- **Update Package Index as shown in figure 16**
 - `sudo apt update`

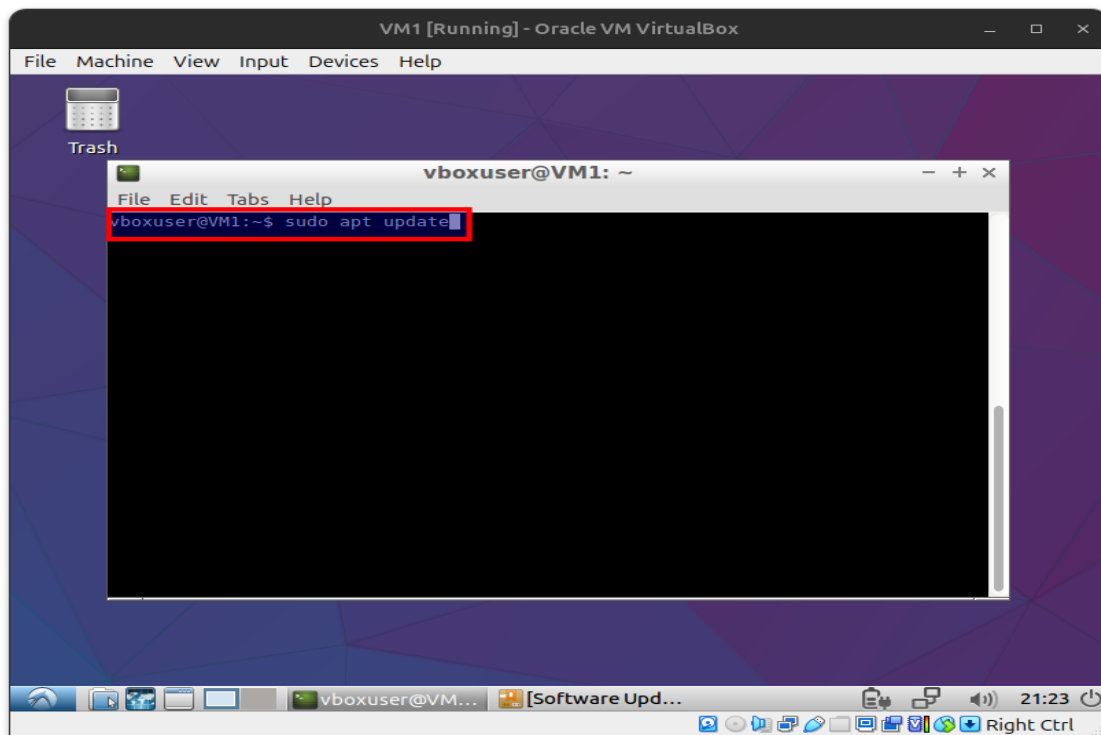
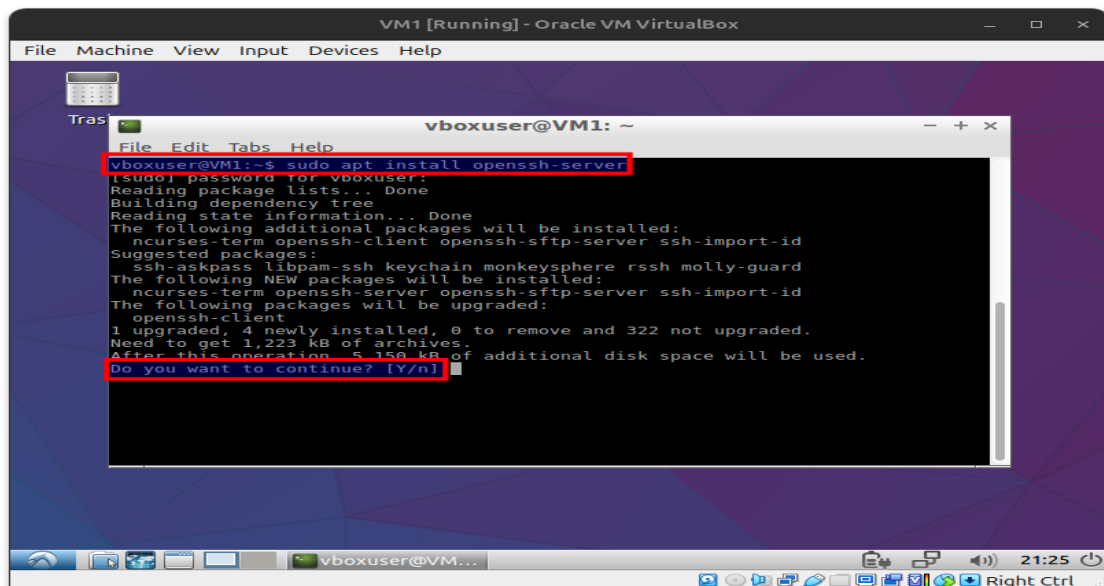


Figure 16: Updating Package Index

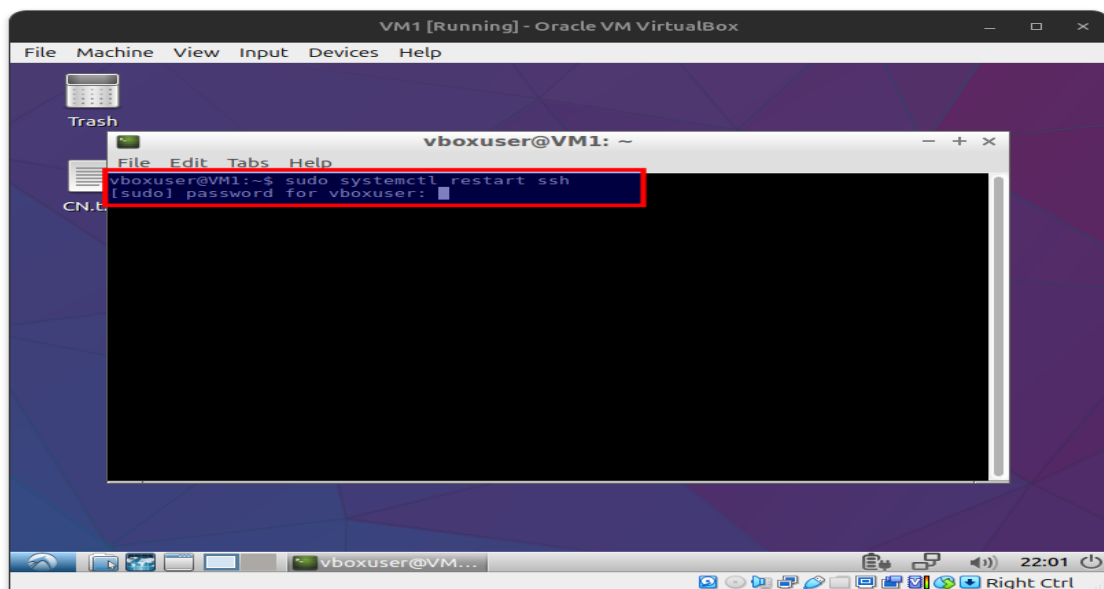
- **Install OpenSSH Server as shown in Figure 17a**
 - `sudo apt install openssh-server`
- **Restart SSH Service as shown in Figure**
 - `sudo systemctl restart ssh`



VM1 [Running] - Oracle VM VirtualBox

```
vboxuser@VM1: ~  
File Edit Tabs Help  
vboxuser@VM1:~$ sudo apt install openssh-server  
[sudo] password for vboxuser:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  ncurses-term openssh-client openssh-sftp-server ssh-import-id  
Suggested packages:  
  ssh-askpass libpam-ssh keychain monkeysphere rssh molly-guard  
The following NEW packages will be installed:  
  ncurses-term openssh-server openssh-sftp-server ssh-import-id  
The following packages will be upgraded:  
  openssh-client  
1 upgraded, 4 newly installed, 0 to remove and 322 not upgraded.  
Need to get 1,223 kB of archives.  
After this operation 5,150 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

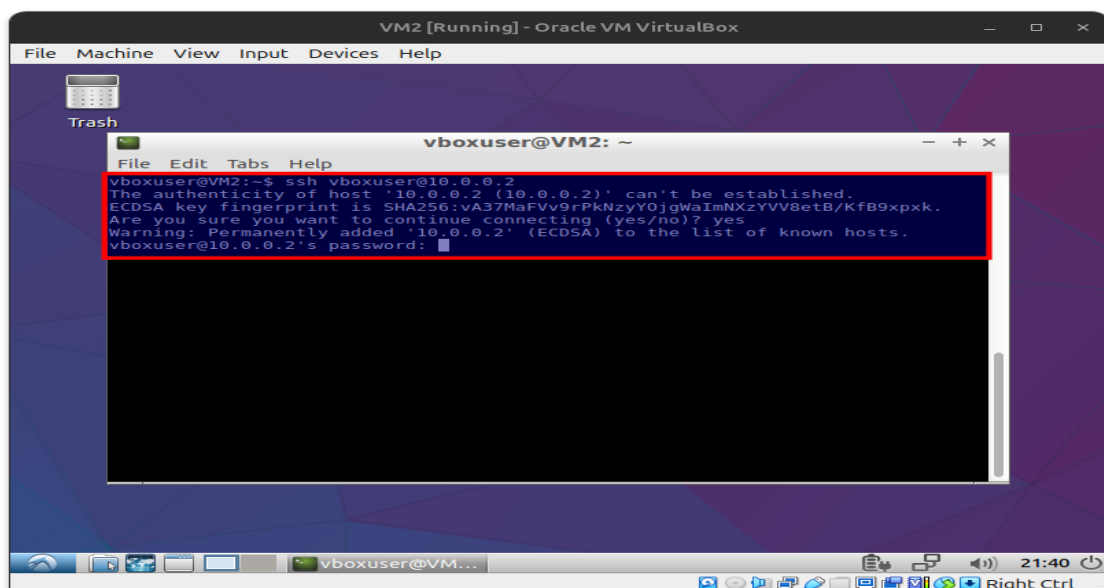
(a) Installing OpenSSH Server in VM1



VM1 [Running] - Oracle VM VirtualBox

```
vboxuser@VM1: ~  
File Edit Tabs Help  
vboxuser@VM1:~$ sudo systemctl restart ssh  
[sudo] password for vboxuser:
```

(b) Restarting the SSH Service



VM2 [Running] - Oracle VM VirtualBox

```
vboxuser@VM2: ~  
File Edit Tabs Help  
vboxuser@VM2:~$ ssh vboxuser@10.0.0.2  
The authenticity of host '10.0.0.2 (10.0.0.2)' can't be established.  
ECDSA key fingerprint is SHA256:vA37MaFVv9rPkNzyY0jgWaImNXzYVV8etB/KfB9xpxk.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.0.2' (ECDSA) to the list of known hosts.  
vboxuser@10.0.0.2's password:
```

(c) Establishing SSH Connection to Remote VM

4.3 Configure SSH Client on VM2

- Ensure network connectivity from VM2 to VM1 (test with `ping 10.0.0.2`).
- Repeat 4.2 on VM2 if SSH access to it is also required.

4.4 Test SSH Access

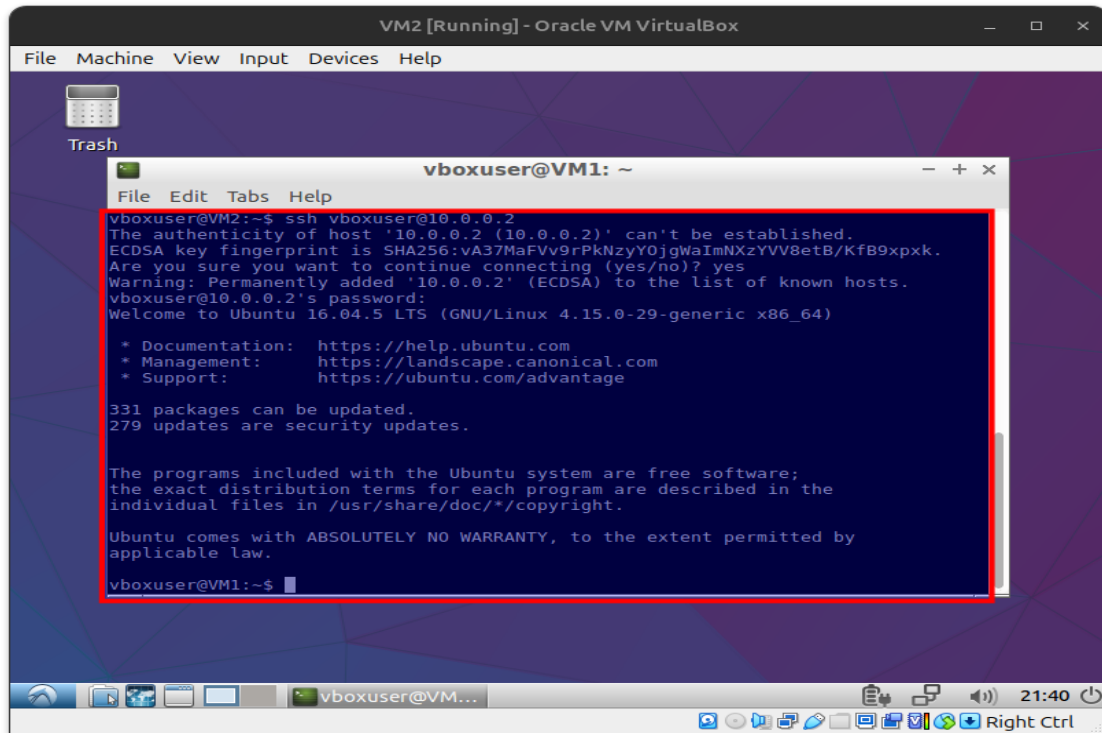


Figure 18: Successful SSH Login into VM1 from a Remote Machine

- **Access VM1 from VM2 via SSH as shown in figure 17c**
 - Execute the following command on VM2: `ssh vboxuser@10.0.0.2`
 - When prompted, enter the password: 12345
 - On successful authentication, a remote shell session to VM1 will be established

4.5 Copy Files Using SCP

- **Transfer a File from VM1 to VM2 Using scp**

- Use the following command on VM2:

```
scp file.txt vboxuser@30.0.0.2:/home/vboxuser/
```

- This copies `file.txt` from VM1 to the `/home/vboxuser/` directory on VM2 as shown in figure 19.
- Enter the password for user `vboxuser` when prompted.

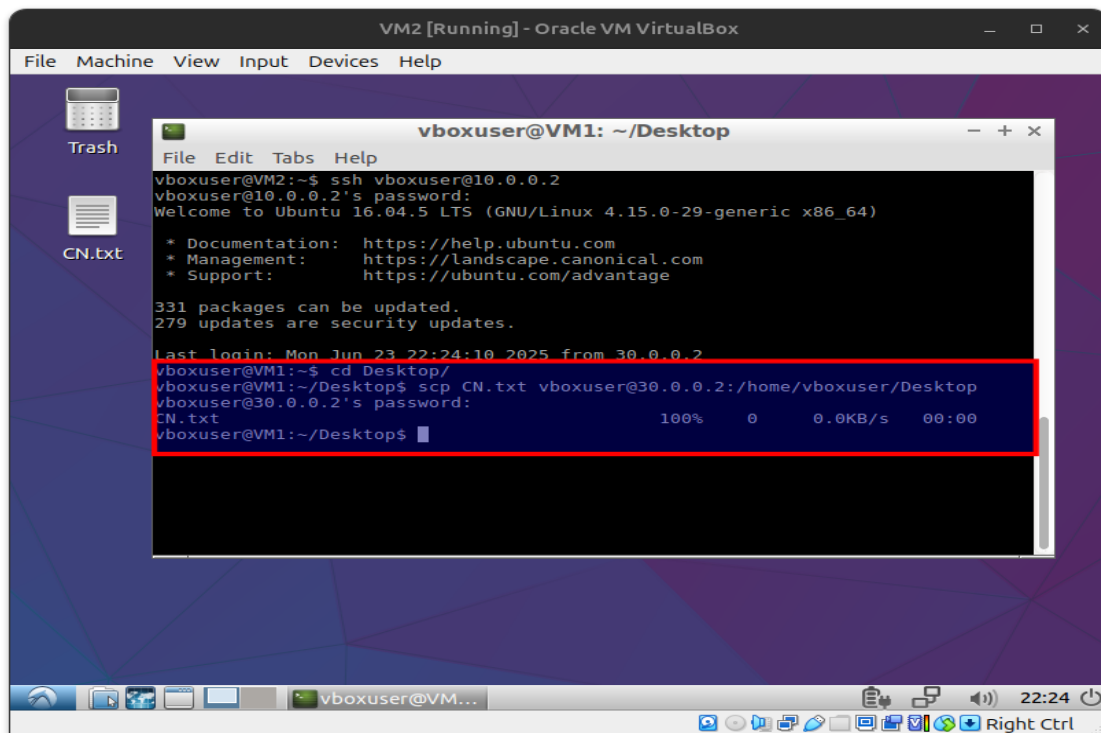


Figure 19: Transferring file from VM1 to VM3 using scp command

4.6 Expected Outcome

- SSH server starts successfully on VM1.
- Remote login from VM2 to VM1 using SSH works correctly.
- Files are successfully transferred using scp.
- `systemctl status ssh` shows the service is active (running).