Q1. Copying a folder with multiple files to destination machine folder using SCP command.

Enabling SSH on the Destination Machine

sudo apt install openssh-server openssh-client

sudo systemctl enable --now ssh

Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.e

Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.

admin@Ubuntu:~/Downloads$ sudo systemctl status ssh

● ssh.service - OpenBSD Secure Shell server

Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>

Active: active (running) since Tue 2025-03-04 16:06:44 IST; 8s ago

TriggeredBy: ● ssh.socket

Docs: man:sshd(8)

man:sshd\_config(5)

Process: 4669 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)

Main PID: 4672 (sshd)

Tasks: 1 (limit: 4614)

Memory: 1.2M (peak: 1.7M)

CPU: 37ms

CGroup: /system.slice/ssh.service

└─4672 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 04 16:06:44 Ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell >

Mar 04 16:06:44 Ubuntu sshd[4672]: Server listening on :: port 22.

Mar 04 16:06:44 Ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell s>

lines 1-17/17 (END)

admin@Ubuntu:~/EmbedURTrainin$ scp -r ~/EmbedURTrainin/mod5/\* admin@10.0.2.15:/home/admin/Downloads/DestFold

admin@10.0.2.15's password:

file2.txt 100% 19 9.3KB/s 00:00

file1.txt 100% 1 0.4KB/s 00:00

file.txt 100% 34 23.8KB/s 00:00

file4.txt 100% 27 7.4KB/s 00:00

file3.txt 100% 34 19.9KB/s 00:00

error.log 100% 672 1.5MB/s 00:00

file\_analyzer.sh 100% 1568 986.6KB/s 00:00

output.txt 100% 1587 698.2KB/s 00:00

test.txt 100% 16 8.6KB/s 00:00

admin@Ubuntu:~/Downloads/DestFold$ ls

dir1 error.log file\_analyzer.sh output.txt test.txt

Q2) 2. Host a FTP and SFTP server and try PUT and GET Operations

FTP:

Start FTP server using

admin@Ubuntu:~/EmbedURTrainin$ sudo systemctl enable --now vsftpd

Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd

Check the status using

admin@Ubuntu:~/EmbedURTrainin$ sudo systemctl status vsftpd

● vsftpd.service - vsftpd FTP server

Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: e>

Active: active (running) since Tue 2025-03-04 16:16:30 IST; 46s ago

Main PID: 10731 (vsftpd)

Tasks: 1 (limit: 4614)

Memory: 708.0K (peak: 1.5M)

CPU: 18ms

CGroup: /system.slice/vsftpd.service

└─10731 /usr/sbin/vsftpd /etc/vsftpd.conf

Mar 04 16:16:30 Ubuntu systemd[1]: Starting vsftpd.service - vsftpd FTP server.>

Mar 04 16:16:30 Ubuntu systemd[1]: Started vsftpd.service - vsftpd FTP server.

admin@Ubuntu:~/EmbedURTrainin$ sudo ufw allow 21/tcp

admin@Ubuntu:~/EmbedURTrainin$ sudo adduser usershar

info: Adding user `usershar' ...

info: Selecting UID/GID from range 1000 to 59999 ...

info: Adding new group `usershar' (1002) ...

info: Adding new user `usershar' (1002) with group `usershar (1002)' ...

info: Creating home directory `/home/usershar' ...

info: Copying files from `/etc/skel' ...

New password:

BAD PASSWORD: The password contains the user name in some form

Retype new password:

passwd: password updated successfully

Changing the user information for usershar

Enter the new value, or press ENTER for the default

Full Name []: Sharan

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] y

info: Adding new user `usershar' to supplemental / extra groups `users' ...

info: Adding user `usershar' to group `users' ...

admin@Ubuntu::~$ ftp 10.0.2.15

Connected to 10.0.2.15.

220 (vsFTPd 3.0.5)

Name (10.0.2.15:admin): usershar

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> put mod1/Output.txt

local: file\_analyzer.sh remote:file\_analyzer.sh

200 PORT command successful. Consider using PASV.

550 Permission denied.

ftp> get ~/EmbedURTrainin/mod5/file\_analyzer.sh

local: /home/admin/EmbedURTrainin/mod5/file\_analyzer.sh remote: ~/EmbedURTrainin/mod5/file\_analyzer.sh

229 Entering Extended Passive Mode (|||63885|)

550 Failed to open file

**SFTP:**

admin@Ubuntu:~/EmbedURTrainin$ sftp admin@10.0.2.15

admin@10.0.2.15's password:

Connected to 10.0.2.15.

sftp> get file\_analyzer.sh

File "/home/admin/file\_analyzer.sh" not found.

sftp> get EmbedURTrainin/mod5/file\_analyzer.sh

Fetching /home/admin/EmbedURTrainin/mod5/file\_analyzer.sh to file\_analyzer.sh

file\_analyzer.sh 100% 1568 4.6MB/s 00:00

sftp> put test.txt

stat test.txt: No such file or directory

sftp> put mod1/Output.txt

Uploading mod1/Output.txt to /home/admin/Output.txt

Output.txt 100% 1601 836.5KB/s 00:00

sftp> exit

Q3) Explore with Wireshark/TCP-dump/cisco packet tracer tools and learn about packets filters

TCP Dump:

It’s a common command line network packet analyser which is used to capture and inspect the network traffic in real time. It is widely used for like network trouble shooting, to do security analysis and some protocol debugging.

The common flags are:

-i: Captures packets on a specific interface

-w: Writes captured packets to a file

-r: Reads packets from a saved .pcap file

-c: Captures only a specific no of packets.

-n: Disables hostname resolution

-nn: disables both hostname and port name resolution

-D: Checks which interfaces are available

-dst: Filter packets based on the destination ip\_address

-src: Filter packets based on the source ip\_address

Some Examples for the tcpdump:

1.Capture all packets on a interface say eth0: tcpdump –I eth0

2.Capture packets from a specific IP: tcpdump –I eth0 host 192.168.1.100

3.Capture only from port 80: tcpdump –I eth0 tcp port 80

4. Capture and save to a file: tcpdump –I eth0 –w traffic.pcap

5. Read from a saved file: tcpdump –r traffic.pcap

WireShark:

Wireshark is a GUI-based network packet analyser which has similar functionalities to tcpdump. It is also used to capture and inspect network traffic in realtime.

The common ways to do filtering in wireshark is:

1.To isolate traffic based on a specific IP:

Ip Based Filtering: ip.addr == 192.168.1.100

2.To focus on traffic types:

http,tcp,udp,dns etc.

3.To based on ports:

Tcp.port==80

4.based on the length of packets:

Frame.len>500

5.based on packet content

Frame contains “test”

Q4) Understand linux utility commands like - ping, arp (Understand each params from ifconfig output)

PING: ping command is a network connectivity utility tool used to test the reachability of a host on the network. IT can be used to determine the network latency using thr RTT (round trip time) taken for each icmp echo it pings to the host.

The common flags are:

-c: Specfies the number of packets to send ping –c 5 google.com

-i: Sets the interval between pings ping –I 2 8.8.8.8

-w: specifies a timeout for the ping test ping –w 10 google.com

-s: sets the packet size ping –s 128 8.8.8.8

-f: enables flood ping ping –f 192.168.1.1

ARP:

Arp or address resolution protocol command is used to view and manipulate the ARP table which maps the IP address to MAC Address.

The common flags are:

-a: Displays the current ARP table arp -a

-n: Shows IP Address in numeric form arp -n

-d: Deletes an ARP entry arp –n 192.168.1.1

-s: Manually adds a static ARP Entry arp –s 192.168.1.1 00:1A:2B:3C:4D:5E

IFCONFIG: it is used to configure network interfaces and has several parameters to set IP Addesses, enable/disable interfaces and such.

The common viewing parameters are:

<interface>: display the info for a specific network interface ifcongid eth0

-a : shows all interfaces ifconfig –a

-s : displays a short summary ifconfig –s

Some common configuring parameters are:

<interface> up : enables the interface ifconfig eth0 up

<interface> down : disables an interface ifconfig eth0 down

<interface> <IP> assigns IP address to an interface ifconfig eth0 192.168.1.1

The output of the ifconfig usually has :

Flags: shows whetehr the interface is active

Inet: signifies the IPv4 address

Inet6: signifies the ipv6 address.

Ether- shows the MAC address

RX TX: shows the total packets received and transmitted in bytes.

MTU: maximum transmission unit (the max packet size that can be transfered).

**Q5) Understand what happens if a duplicate IPs configured in a network.**

When two devices on the same network are assigned the same IP Address, it creates an IP conflict, leading to connectivity issues and network instability. This usually occurs due to manual configuration of the IP Addresses. Since every device is supposed to have unique IP Address to communicate properly, this duplication can cause issues in Data routing.

Usually in Os like Windows,Linux or MacOS, there are duplicate IP detections and they pop an error stating “has detected an IP address conflict”. But when this happens continuously , it can cause disruptions to the network traffic.It also causes a ARP table instability. Since ARP maps IP Addresses to MAC address, conflicting devices keep updating their MAC in the ARP table causing incorrect data routing. And thus this can lead to sending packets to a wrong device or dropped packets and can even complicate things while troubleshooting.

Some ways to detect and prevent duplicate IP addresses are:

Admins can check ARP tables to identify duplicate entries.

DHCP server logs can also detect conflicts.

Re-assigning a unique IP to static IP devices is also one solution.

In larger networks, Dynamic ARP Inspection (DAI) can be enabled to prevent unauthorized ARP modifications, reducing the risk of conflicts and spoofing attacks.

**Q6) Understand how to access remote system using (VNC viewer, Anydesk,Teamviewer)**

VNC Viewer:

On the remote computer, install the VNC server and on the local device install the VNC Viewer.

Setup the VNC server on the remote computer by providing password for access.

Connect using your RealVNC account and select the remote computer to connect. Use the password to authenticate.

This can also be done in linux using tigervnc.

Anydesk:

Download and install Anydesk on both the computers.

Share the access code shown on the remote computer to the local computer user.

Enter the access code on the local machine and accept the connection request on the remote computer to establish control of the remote computer.

Teamviewer:

Install Teamviewer on both the remote and local devices.

Share the iD and the password of the remote device to the local machine user.

Enter the ID and authenticate using the password to establish control and start the session.

Remote Desktop Connection:

Some windows edition have the tool for remote desktop .

We can connect to the pc using the RDP clients and by entering the PC name.

Q7) Check if default gateway is reachable or not and understand about default gateways

To get the default gateway use and see if its reachable or not,

admin@Ubuntu:~/EmbedURTrainin$ netstat -rn

Kernel IP routing table

Destination Gateway Genmask Flags MSS Window irtt Iface

0.0.0.0 10.0.2.2 0.0.0.0 UG 0 0 0 enp0s3

10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3

admin@Ubuntu:~/EmbedURTrainin$ ip route | grep default

default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100

admin@Ubuntu:~/EmbedURTrainin$ ping 10.0.2.2

PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.

64 bytes from 10.0.2.2: icmp\_seq=1 ttl=255 time=0.941 ms

64 bytes from 10.0.2.2: icmp\_seq=2 ttl=255 time=0.837 ms

64 bytes from 10.0.2.2: icmp\_seq=3 ttl=255 time=0.515 ms

64 bytes from 10.0.2.2: icmp\_seq=4 ttl=255 time=0.330 ms

64 bytes from 10.0.2.2: icmp\_seq=5 ttl=255 time=0.422 ms

64 bytes from 10.0.2.2: icmp\_seq=6 ttl=255 time=0.901 ms

64 bytes from 10.0.2.2: icmp\_seq=7 ttl=255 time=0.532 ms

64 bytes from 10.0.2.2: icmp\_seq=8 ttl=255 time=0.936 ms

64 bytes from 10.0.2.2: icmp\_seq=9 ttl=255 time=0.844 ms

64 bytes from 10.0.2.2: icmp\_seq=10 ttl=255 time=0.327 ms

^C

--- 10.0.2.2 ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9122ms

rtt min/avg/max/mdev = 0.327/0.658/0.941/0.243 ms

Understanding Default Gateways:

It’s a device that serves as an access point for a network to communicate with other networks, including the internet. It acts as an intermediary , and helps forwarding the packets from a local network to external destinations. If the destination IP address does not belong to a local network, the data is sent to the default gateway after checking the routing table and forwards it to the final destination.

**Q8) Check iwconfig/ifconfig to understand in detail about network interfaces (check about interface speed, MTU and other parameters)**

IFCONFIG:

It is used to display and configure the network interfaces, such as assigning IP address , enabling interfaces and setting parameters like MTU.

Some key parameters are:

Interface Name: eth0, lo (loopback) ,wlan0 (Wifi)

Flags: UP , BROADCAST,RUNNING,MULTICAST

Inet: IPv4 address assigned to the interface

Inet6: IPv6 address if available

Netmask: Subnet mask

Broadcast: broadcast IP address.

Ether: MAC address of the interface

MTu: Maximum transmission unit (default is 1500 bytes)

RxTx: received and transmitted packet counts.

Bytes: data received and sent.

IWCONFIG:

It Is used to display and configure wireless interfaces like Wi-fi. It provides wifi-signal strength , mode, frequency, bitrate, and power management.

The key parameters in the iwconfig Output is:

Interface name : wlan0

IEEE Standard: IEEE 802.11

Mode: Managed,Master,Monitor

Frequency: Operating frequency in Ghz

Accesspoint: MAC Address of the wifi router

Bit Rate: Current speed in Mbps

Tx-power Tranmission power in dBm

Link Quality: Signal Quality

Signal Level: Signal Strength in dBm

Q9) Log in to your home router's web interface (usually at 192.168.1.1 or 192.168.0.1) and check the connected devices list.

Type in 192.169.1.1 in any browser.

A user interface of the wifi network wil be shown and enter the admin username and password.

Once logged in, Go to the user info.

There you can see the parameters of the connected devices and its list.

Another way to check in linux is using the command arp-scan

admin@Ubuntu:~$ sudo arp-scan --localnet

Interface: enp0s3, type: EN10MB, MAC: 08:00:27:b4:64:ad, IPv4: 10.0.2.15

WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied

WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied

Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)

10.0.2.2 52:55:0a:00:02:02 (Unknown: locally administered)

10.0.2.3 52:55:0a:00:02:03 (Unknown: locally administered)

2 packets received by filter, 0 packets dropped by kernel

Ending arp-scan 1.10.0: 256 hosts scanned in 2.118 seconds (120.87 hosts/sec). 2 responded

Q10) Explain how DHCP server assigns IP addresses to devices in your network

A DHCP server automatically assigns IP addresses and other network configurations to devices over a network. This eliminates the need for a manual IP assignment and ensure there is no conflicts regarding the same.

The process involved is:

1. DHCP Discover (Broadcast): if a client device has no IP address yet , it sends a DHCP discover message as a broadcast to find a DHCP server.
2. DHCP Offer: This is the server receiving the request and responding with a DHCP offer message. It wil include an available IP address, subnet mask, default gateway router, DNS servers and lease time.
3. DHCP Request: The client chooses the offered IP and sends a DHCP request to the server.
4. DHCP acknowledge: The DHCP confirms the assignment by sending a DHCP acknowledgement message.

The assigned IP is temporary and has a lease time. Befire it expires the client sends a DHCP request again to renew the lease.If the lease expires without renewal, the IP is returned to the pool for other devices.

Q11) Using a terminal, connect to a remote machine via SSH and telnet.

SSH:

Install ssh using

sudo apt install openssh-server openssh-client

Create a session using

admin@Ubuntu:~$ sudo systemctl enable --now ssh

[sudo] password for admin:

Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.

Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh.service.

admin@Ubuntu:~$ sudo systemctl status ssh

● ssh.service - OpenBSD Secure Shell server

Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>

Active: active (running) since Tue 2025-03-04 18:19:49 IST; 15s ago

TriggeredBy: ● ssh.socket

Docs: man:sshd(8)

man:sshd\_config(5)

Process: 14626 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCES>

Main PID: 14627 (sshd)

Tasks: 2 (limit: 4614)

Memory: 3.1M (peak: 3.7M)

CPU: 57ms

CGroup: /system.slice/ssh.service

├─11379 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

└─14627 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 04 18:19:49 Ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell >

Mar 04 18:19:49 Ubuntu systemd[1]: ssh.service: Found left-over process 11379 (>

Mar 04 18:19:49 Ubuntu systemd[1]: ssh.service: This usually indicates unclean >

Mar 04 18:19:49 Ubuntu sshd[14627]: Server listening on :: port 22.

Mar 04 18:19:49 Ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell s>

ESCOC

sharubuntu@Ubuntu:~$ ssh admin@10.0.2.15

admin@10.0.2.15's password:

Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-52-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

40 updates can be applied immediately.

To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.

See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue Mar 4 18:22:49 2025 from 10.0.2.15

TELNET:

Install telnet using

Sudo apt install telnetd –y on the server

Sudo apt install telnet on the client

admin@Ubuntu:~$ sudo systemctl enable xinetd

[sudo] password for admin:

Synchronizing state of xinetd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.

Executing: /usr/lib/systemd/systemd-sysv-install enable xinetd

admin@Ubuntu:~$ sudo systemctl status xinetd

● xinetd.service - Xinetd A Powerful Replacement For Inetd

Loaded: loaded (/usr/lib/systemd/system/xinetd.service; enabled; preset: e>

Active: active (running) since Tue 2025-03-04 18:56:42 IST; 1min 17s ago

Docs: man:xinetd

man:xinetd.conf

man:xinetd.log

Main PID: 1125 (xinetd)

Tasks: 1 (limit: 4608)

Memory: 916.0K (peak: 1.1M)

CPU: 151ms

CGroup: /system.slice/xinetd.service

└─1125 /usr/sbin/xinetd -stayalive -dontfork

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Reading included configuration file: /etc/>

Mar 04 18:56:43 Ubuntu xinetd[1125]: 2.3.15.4 started with libwrap loadavg labe>

Mar 04 18:56:43 Ubuntu xinetd[1125]: Started working: 0 available services

lines 1-23

Client Side:

telnet -l telnet 172.31.244.70