TRAINING DAY 14 REPORT:

- ## What is Port Addressing?

Port addressing is a method used in computer networks **to identify specific processes or services** running on a device (host).

IP address → identifies **host (device)**

Port number → identifies **specific application/service** on that host

Just like an apartment address:

Building (IP) tells *which house*

Flat number (Port) tells *which room in that house*

Why Port Addressing?

Because a single computer can run **multiple apps** (browser, email, file transfer) at the same time. Each needs a unique **port number** to receive/send data.

Process-to-Process Communication

The **Transport Layer** (like TCP/UDP) uses **port numbers** to:

- **Send data** from a process on one computer
- **Deliver it** to the right process on another computer

Port Number Ranges

Range	Use
0 – 1023	**Well-known ports** (e.g., HTTP: 80, FTP: 21)
1024 – 49151	**Registered ports** (used by user apps)
49152 – 65535	**Dynamic/Private ports** (used temporarily)

Examples

Service	Protocol	Port
HTTP	TCP	80
HTTPS	TCP	443
FTP	TCP	21
SSH	TCP	22
DNS	UDP/TCP	53

- ## What is a Proxy?

  A proxy is an **intermediate system** that **acts as a bridge between a user and the internet.**
  It sends/receives requests on behalf of the user.

  Think of it like a middleman who talks to websites for you.

What is a Proxy Server?

A proxy server is the actual system/software that:

1. Accepts your request (like opening a website)
2. Forwards it to the **destination server**
3. Receives the response (like a webpage)
4. Sends it back to **you**

Uses of Proxy Servers:

Use	Description
Anonymity	Hides your IP address from the destination

Use	Description
Security	Filters and blocks malicious sites or content
Content Control	Used in schools/offices to block social media, etc.
Caching	Saves copies of frequently visited pages to load faster
Bypass Restrictions	Access geo-restricted or blocked websites

Types of Proxies:

Type	Description
Forward Proxy	Sits between client and internet (most common)
Reverse Proxy	Sits in front of web servers to manage incoming requests
Transparent Proxy	Doesn't modify requests/responses; user may not know it's used
Anonymous Proxy	Hides your IP; provides anonymity
High Anonymity Proxy	Changes your IP and doesn't reveal itself as a proxy

In Summary:

- Proxy = **middleman** between you and the internet

- Helps with **anonymity, security, content control, caching**, and **access**

- Widely used in **corporate networks, cybersecurity, and privacy tools**

- ## What is a VPN (Virtual Private Network)?

A VPN is a secure, encrypted connection between your device and the internet, which passes through a **remote server** run by the VPN provider.

Think of it like a **private tunnel** through a public network (the internet).

- **Your real IP address is hidden.**
- Your **internet data is encrypted**.

Main Features & Benefits:

Benefit	**Explanation**
Privacy	Hides your IP and browsing activity
Security	Encrypts data, even on public Wi-Fi
Access Blocked Sites	Bypasses geo-blocks or censorship
Anonymity	Prevents tracking by websites/ISPs
Remote Access	Allows secure access to company networks from anywhere

Common Uses of VPN:

1. Accessing **Netflix, YouTube, etc.** in other countries

2. Secure browsing on public Wi-Fi (cafes, airports)

3. Bypassing censorship in restricted countries

Limitations of VPN:

1. May **slow down** internet speed (due to encryption)

2. Free VPNs can be **unreliable or risky**

- ## What is Tor (The Onion Router)?

Tor is a free, open-source network that helps you stay anonymous online by routing your internet traffic through multiple volunteer-operated servers (nodes) worldwide.

Just like layers of an onion, it **encrypts your data in layers** and sends it through **3 different nodes** to hide your identity and location.

- Your **data is encrypted** in layers.

- Each node only knows **its next hop**, not the full path.

- The final website **can’t trace your real IP**.

Key Features:

Feature	**Description**
Anonymity	Hides your IP and browsing behavior
Decentralized	Uses volunteer-operated relays worldwide
Free to Use	Open-source, accessible to all
Blocks tracking	Prevents surveillance and fingerprinting

- ## Tor Browser:

  - A special web browser (built on Firefox)

  - Accesses websites using the **.onion** domain

  - Helps bypass **censorship** and **firewalls**

Limitations of Tor:

Limitation	**Explanation**
Slow speed	Due to multiple relays
Not fully secure	If exit node is malicious
Blocked content	Some sites block Tor traffic
Illegal activity risk	Some misuse Tor for dark web activities

- ## Use Cases:

  1. Journalists & activists in **restricted regions**

2. Users in countries with **internet censorship**

3. People who want **privacy and anonymity**

- ## Remote Login: SSH & Telnet

Remote login allows a user to access and control another computer over a network as if they were sitting in front of it.

Two common protocols used:

- **Telnet**
- **SSH (Secure Shell)**

1. Telnet (TELecommunication NETwork)

- Old protocol used for remote login

- Sends data **in plain text** (NOT secure)

- You can control a remote system via **command line**

- Not used today due to **security risks**

Example command:

```
telnet 192.168.1.1
```

2. SSH (Secure Shell)

- Secure alternative to Telnet

- All data is **encrypted**, including username and password

- Commonly used to manage **Linux servers remotely**

- Works over **port 22**

Example command:

```
ssh user@192.168.1.1
```

Telnet vs SSH:

Feature	Telnet	SSH
Security	Not secure (no encryption)	Encrypted and secure
Port used	23	22
Data type	Plain text	Encrypted
Usage now	Rarely used (not recommended)	Widely used for secure access

Use Case of SSH:

1. System admins use it to manage **Linux/Unix servers**
2. Developers use it for **code deployment**
3. Used in **remote troubleshooting**

Warning:

1. Telnet is not safe on public or sensitive networks.

2. SSH should always be preferred for secure communication.