

TRAINING DAY 14 REPORT

Understand Computer Networking

Today, I learn some important concept

Port addressing

Port addressing refers to the method of identifying specific processes or services on a device (typically a computer or server) within a network using **port numbers**. It plays a crucial role in networking, especially in TCP/IP-based networks like the internet.

Process-to-Process Communication

Process-to-process communication is the method by which **two applications (processes)** running on different (or the same) devices exchange data over a network. It's a fundamental concept in computer networks, especially in the **transport layer** of the **OSI model** and the **TCP/IP model**.

Proxies and Proxy Servers

A **proxy** or **proxy server** acts as an **intermediary** between a client (like your browser) and a destination server (like a website). Instead of connecting directly to the target server, your request first goes through the proxy.

A **proxy server** is a computer or software system that sits between your device and the internet. It receives your network requests, forwards them to the intended destination, then sends the response back to you.

How Does a Proxy Server Work?

A **proxy server** works by acting as an **intermediary** between your device (client) and the internet (server). When you send a request to access a website or service, the proxy **receives the request, forwards it** to the destination server, **retrieves the response**, and **sends it back** to you.

Uses of a Proxy Server

A **proxy server** serves multiple purposes in networking, security, performance, and access control.

- Boost your internet speed
- Hide your IP address
- Access Blocked websites
- Security

Types of Proxy Servers

Forward Proxy – A proxy that routes client requests to external servers, often used for filtering or anonymity.

Reverse Proxy – A proxy that routes incoming traffic to internal servers, commonly used for load balancing and security.

Transparent Proxy – A proxy that intercepts traffic without modifying it and without user awareness.

Anonymous Proxy – A proxy that hides the client's IP address but reveals it's a proxy.

Elite Proxy (High Anonymity Proxy) – A proxy that hides both the user's IP and the fact that it's a proxy.

Distorting Proxy – A proxy that hides the real IP and provides a fake one to the destination server.

VPN (Virtual Private Network)

A **VPN (Virtual Private Network)** is a secure tunnel that encrypts your internet traffic and routes it through a remote server, hiding your IP address and protecting your privacy online.

How a VPN Works

1. You connect to a **VPN server** (e.g., in the US).
2. Your internet traffic is **encrypted** and routed through the VPN server.
3. Websites and services see the **VPN server's IP**, not yours.

4. Your connection appears to come from the VPN location, not your actual location.

Advantages of a VPN

- Hides your IP address
- Encrypts internet traffic
- Bypasses geo-restrictions
- Bypasses censorship and firewalls
- Secures public Wi-Fi usage
- Enables secure remote access
- Prevents ISP throttling

Disadvantages of VPN

- May slow down internet speed
- Good VPNs often cost money
- Can be complex to set up
- Not fully anonymous (logs may exist)
- Some websites block VPN traffic
- Limited features on free plans

TOR (The Onion Router)

TOR is a free, decentralized network that enables anonymous internet browsing by routing your traffic through multiple volunteer-run servers (nodes) to hide your identity and location.

How TOR Works

- Your data is encrypted multiple times (like layers of an onion).
- It passes through **3+ random nodes** (relays) in the TOR network.
- Each relay decrypts a layer, knowing only the previous and next relay.
- The final relay sends the data to the destination, hiding your IP from the target site.

Advantages of TOR

- Provides strong anonymity by hiding your IP address
- Helps bypass censorship and access blocked websites
- Decentralized and free to use
- Protects against traffic analysis and surveillance
- Allows access to .onion (hidden) services
- Used by journalists, activists, and whistleblowers for privacy

Disadvantages of TOR

- Slower internet speeds due to multiple relays
- Some websites block or restrict TOR traffic
- Exit nodes can potentially see unencrypted traffic
- Not suitable for all activities (e.g., streaming or gaming)
- Can be targeted or flagged by some network administrators
- Potential misuse by malicious actors on the network

Port Forwarding

Port forwarding is a network technique that directs incoming internet traffic on a specific port to a designated device or service within a private local network.

Types of Port Forwarding

- 1. Local Port Forwarding**
 - Forwards traffic from a local machine's port to a remote server's port.
 - Used to securely access remote services through an SSH tunnel.
- 2. Remote Port Forwarding**
 - Forwards traffic from a remote server's port to a local machine's port.
 - Allows external users to access a service running on your local machine.
- 3. Dynamic Port Forwarding**
 - Creates a SOCKS proxy that dynamically forwards traffic to any destination.
 - Useful for routing traffic through an SSH server to multiple hosts.
- 4. Static Port Forwarding**
 - Fixed mapping of a specific external port to an internal IP and port.
 - Most common type used in home routers to expose local servers.

How Port Forwarding Works

- Your router receives incoming traffic on a particular port (e.g., port 80).
- It forwards that traffic to a specific device's local IP and port inside your network.
- Enables external devices to access services (like a web server or game server) hosted on your private network.