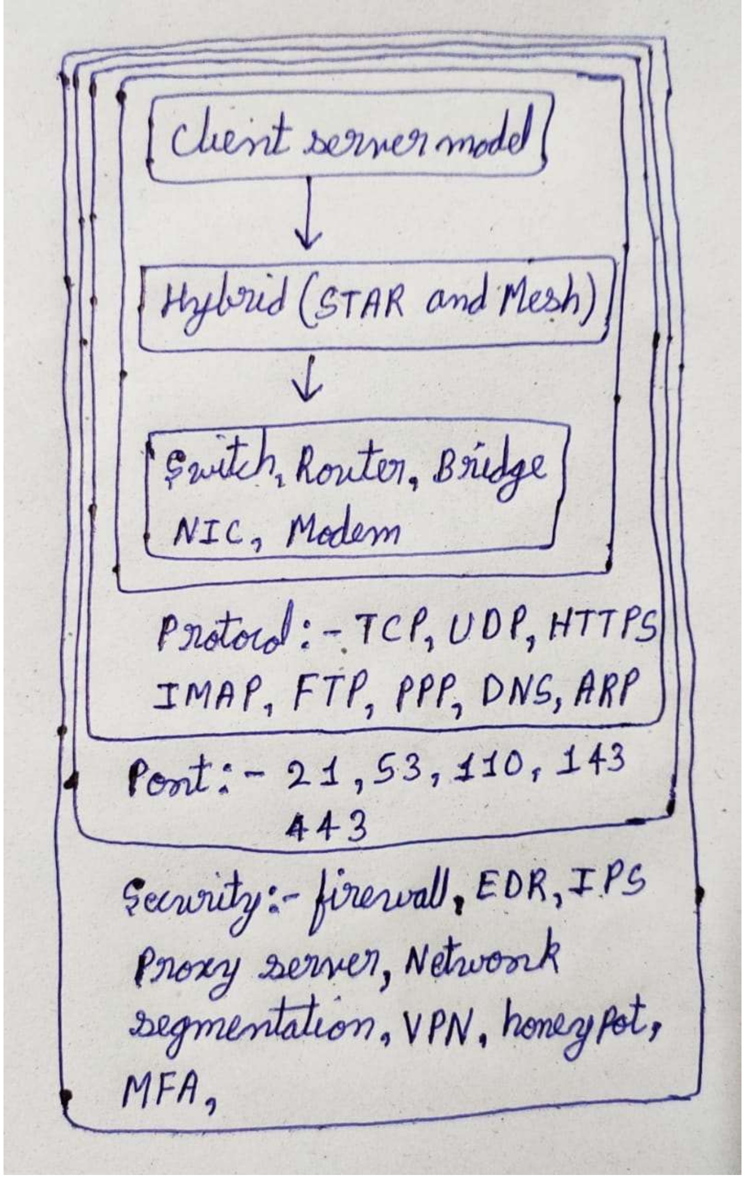
We are designing Network for a local bank



Client server model

↓

Hybrid (STAR and Mesh)

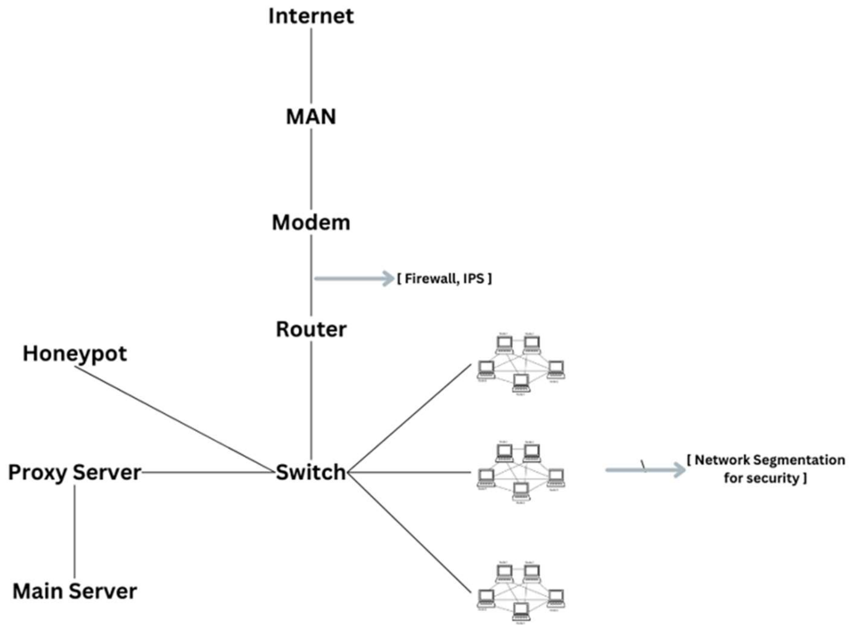
↓

Switch, Router, Bridge
NIC, Modem

Protocol:- TCP, UDP, HTTPS
IMAP, FTP, PPP, DNS, ARP

Port:- 21, 53, 110, 143
443

Security:- firewall, EDR, IPS
Proxy server, Network
segmentation, VPN, honeypot,
MFA,



Network Architecture

We are using client and server model instead of peer-to-peer network because in peer to peer all devices equal privileges and there is no server. The **client-server architecture** is a fundamental concept in system design. Here’s how it works:

- **Clients**: These are devices or programs that request services or resources. They interact with the server to access data or perform specific tasks.
- **Server**: The server is a powerful machine or software that provides these resources or services. It fulfils client requests by processing operations and managing data.

In this model, clients and servers communicate over a network, allowing multiple clients to connect to a centralized server. Examples of client-server applications include email, web browsing, online banking, and e-commerce.

Let’s explore the **advantages** and **disadvantages** of client-server architecture:

Advantages:

1. **Cost Efficiency**: Client-server architecture reduces maintenance costs. Servers can be powerful machines, while clients (end-user devices) can be simpler and less expensive.
2. **Centralized Data**: Data resides on the server, making backups and data recovery easier. Centralized management simplifies system administration.
3. **Scalability**: Servers can be upgraded independently, allowing for flexible capacity adjustments.
4. **Security**: Centralized control enhances security measures, such as access control and encryption.
5. **Resource Sharing**: Servers can provide shared resources (e.g., databases, files) to multiple clients efficiently.

Disadvantages:

1. **Complexity**: Setting up and maintaining servers can be complex, especially in large-scale systems.
2. **Single Point of Failure**: If the server fails, all connected clients are affected.
3. **Network Dependency**: Clients rely on network communication with the server. Network issues can impact performance.
4. **Cost Implications**: Servers require initial investment and ongoing maintenance.
5. **Scalability Challenges**: Scaling servers can be challenging, especially during sudden spikes in demand.

Topology

We have implemented a hybrid network topology that combines STAR and MESH topologies, allowing us to perform effective network segmentation. This approach offers the benefit of isolating infected network segments from the rest of the network in the event of an attack, thus preventing the spread of threats and bolstering our overall network security.

We have decided to use the Mesh topology instead of STAR. This is because if the main switch in the STAR topology within a sub-network encounters any issues, the entire department would be unable to communicate either internally or with other departments. With the MESH topology, all devices are interconnected. This means that even if one device encounters an issue, it won't affect the other devices.

The **star topology** is a network design where all nodes connect to a central hub or switch. Let’s explore its advantages and disadvantages:

Advantages:

1. **Reliability**: If one cable or device fails, other nodes continue to function.
2. **High Performance**: No data collisions occur since communication is direct.
3. **Ease of Installation**: Simple to set up and configure.
4. **Easy Troubleshooting**: Fault detection is straightforward due to identifiable links.
5. **Scalability**: Devices can be added or removed without disrupting the network.

Disadvantages:

1. **Cost**: Requires more cables than a linear bus topology.
2. **Single Point of Failure**: If the central hub fails, the entire network is affected.
3. **Resource Dependency**: Hub maintenance is essential.
4. **Extra Hardware**: Requires hubs or switches, adding to the cost.

In summary, star topology offers reliability and performance but can be costlier and has a single point of failure. It’s commonly used in Local Area Networks (LANs) with multiple connections.

Mesh topology is a network architecture where all devices connect directly to each other. Let's explore its advantages and disadvantages:

Advantages:

1. **Fault Tolerance**: Even if one device fails, the network remains functional because of multiple paths.
2. **Dedicated Links**: Each computer has a point-to-point link, ensuring efficient data transmission.
3. **Redundancy**: Mesh provides backup routes, enhancing reliability.
4. **Privacy and Security**: Direct connections limit unauthorized access.
5. **Consistent Data Transmission**: Failures don't disrupt ongoing processes.
6. **Scalability**: Adding devices doesn't affect existing data flow.

Disadvantages:

1. **Costly**: Implementing mesh is expensive compared to other topologies.
2. **Complex Installation**: Setting up mesh networks can be challenging.
3. **High Power Requirement**: All nodes must remain active, sharing the load.
4. **Redundant Connections**: Risk of unnecessary links.
5. **Maintenance Challenges**: Managing a mesh network is demanding.

Devices

We are using switch, router, bridge, NIC and modem.

Notes: we are using a bridge in case of expanding our network future.

Let's dive into the definitions of each device:

Switch:

- A **switch** is a device used in computer networks to connect multiple devices (such as computers, printers, or servers) within a local area network (LAN). It operates at the data link layer (Layer 2) of the OSI model.

- **Function**: A switch forwards data frames between devices based on their Media Access Control (MAC) addresses. It learns and maintains a MAC address table to efficiently direct traffic.
- **Example**: Ethernet switches are commonly used in offices and data centers to create efficient and secure LANs.

Router:

- A **router** is a networking device that connects different networks (such as LANs, WANs, or the Internet) and directs data packets between them. It operates at the network layer (Layer 3) of the OSI model.
- **Function**: Routers determine the best path for data packets to reach their destination using routing tables. They also perform network address translation (NAT) and provide security features.
- **Example**: Home routers connect local devices to the Internet and manage traffic between them.

Bridge:

- A **bridge** is a device that connects two separate network segments (usually LANs) and allows them to communicate as a single network. It operates at the data link layer (Layer 2).
- **Function**: Bridges filter and forward data frames based on MAC addresses. They reduce network collision domains and improve overall network performance.
- **Example**: Wireless access points (which bridge wired and wireless networks) are common examples.

Network Interface Controller (NIC):

- A **NIC**, also known as a network interface card or network adapter, is a hardware component that connects a computer to a network. It can be wired (Ethernet) or wireless (Wi-Fi).
- **Function**: NICs handle the physical connection to the network medium (such as cables or radio waves) and provide a unique MAC address for the device.

- **Example**: The Ethernet port on your computer or the Wi-Fi card in your laptop are both NICs.

Modem:

- A **modem** (short for modulator-demodulator) converts digital signals from a computer into analog signals suitable for transmission over telephone lines or other communication channels.
- **Function**: Modems allow computers to communicate over landlines (e.g., dial-up) or other media (e.g., cable or DSL). They modulate digital data for transmission and demodulate received analog signals back into digital data.
- **Example**: Dial-up modems were popular in the past, but broadband modems (such as cable modems) are more common today.

Protocol

We are using different protocols at different level in our network.

TCP (Transmission Control Protocol):

- TCP is a core protocol in the Internet suite.
- It ensures reliable, ordered, and error-checked delivery of data between applications over an IP network.
- Commonly used for web browsing, email, and file transfer.
- Operates at the transport layer (Layer 4) of the OSI model.

UDP (User Datagram Protocol):

- UDP is another Internet protocol for data transfer.
- Connectionless and prioritizes time over reliability.
- Used for time-sensitive applications like video streaming and DNS lookups.
- Operates at the transport layer (Layer 4) as well.

HTTPS (Hypertext Transfer Protocol Secure):

- Secure version of HTTP.
- Encrypts data between web servers and browsers.
- Protects sensitive information during transmission (e.g., login credentials).
- Often secured with SSL/TLS (FTPS) or replaced by SFTP.

IMAP (Internet Message Access Protocol):

- Allows email clients to retrieve messages from a mail server.
- Supports mailbox management across multiple clients.
- IMAP servers listen on port 143; IMAPS (over SSL/TLS) uses port 993.

FTP (File Transfer Protocol):

- Standard protocol for transferring files between a server and a client.
- Built on a client-server model with separate control and data connections.
- Often used for uploading/downloading files to/from servers.

PPP (Point-to-Point Protocol):

- Used to establish direct connections between two network nodes.
- Commonly used for dial-up connections and VPNs.

DNS (Domain Name System):

- Converts domain names (e.g., www.example.com) to IP addresses.
- Essential for web browsing and other network services.

ARP (Address Resolution Protocol):

- Maps IP addresses to MAC addresses in local networks.
- Helps devices find each other on the same subnet.

Port

We will be using the following port numbers 21, 53, 110, 143, 443. All other ports except these are closed.

Security

Following network security devices are used to improve security hardening.

Certainly! Let’s explore the definitions of these networking and security terms:

Firewall:

- A **firewall** is a network security device that monitors and controls incoming and outgoing traffic from a computer network.
- **Function**: It allows authorized traffic while blocking unwanted traffic, protecting against unauthorized access, malware, and security threats. Firewalls can also prevent sensitive data from leaving the network.

EDR (Endpoint Detection and Response):

- EDR continuously monitors end-user devices (endpoints) to detect and respond to cyber threats like ransomware and malware.
- **Function**: It records and analyzes endpoint behaviors, detects suspicious activity, and provides remediation suggestions to restore affected systems.

IPS (Intrusion Prevention System):

- An **IPS** is a network security system that identifies and prevents malicious activities within a network.
- **Function**: It logs information, blocks suspicious activity, and limits the spread of cyberattacks. IPS improves security by segmenting network traffic and enforcing policies.

Proxy Server:

- A **proxy server** acts as an intermediary between a client (requesting a resource) and the server providing that resource.
- **Function**: It improves privacy, security, and performance by controlling how traffic flows. Proxies can be forward (Internet-facing) or reverse (internal-facing).

Network Segmentation:

- **Network segmentation** divides a computer network into smaller parts to improve performance and security.
- **Function**: It limits congestion, reduces cyberattack damage, protects vulnerable devices, and simplifies compliance by compartmentalizing sub-networks.

VPN (Virtual Private Network):

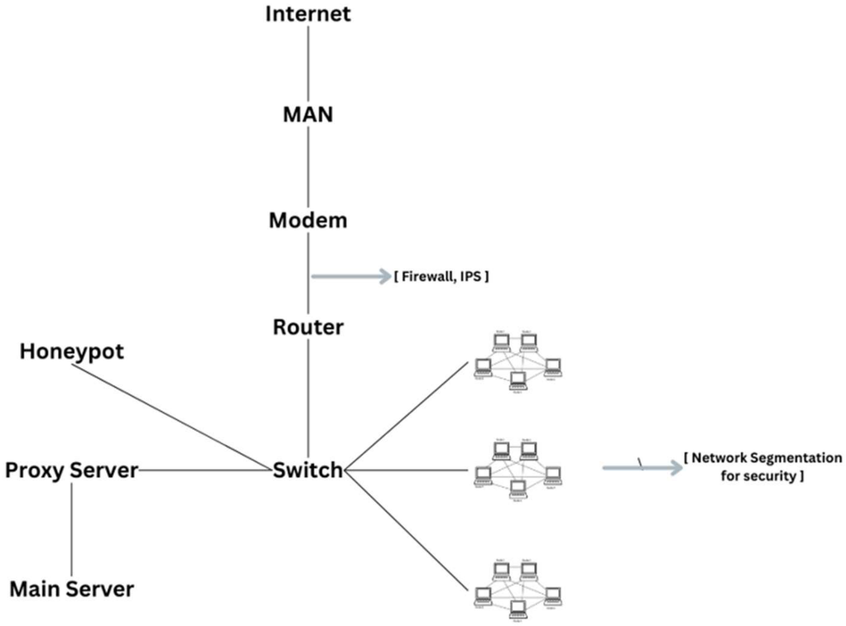
- A **VPN** creates a secure, encrypted connection between a user's device and a private network (e.g., corporate network or the Internet).
- **Function**: It ensures privacy, confidentiality, and data integrity by tunneling traffic through a secure channel.

Honeypot:

- A **honeypot** is a decoy system designed to attract and deceive attackers.
- **Function**: It lures attackers away from critical systems, allowing security teams to monitor and analyze their behavior without risking real assets.

MFA (Multi-Factor Authentication):

- **MFA** adds an extra layer of security by requiring users to provide multiple forms of identification (e.g., password, fingerprint, SMS code) to access a system.
- **Function**: It reduces the risk of unauthorized access even if one factor (e.g., password) is compromised.



Suggestion

1. Use SIEM tool for real time log analysis.
2. Install CCTV cameras at sensitive areas like server….
3. Give employees training and awareness related to different attacks and social engineering….