Assignment 3

1. Client-Server, Peer-to-Peer, and Hybrid Architectures: Scalability & Security

Client-Server:
This is the most common type of architecture where clients (like your laptop or phone) make requests and servers respond. It's great for scaling because you can keep adding more servers or beef up the existing ones. Security is also easier to manage since everything is centralized. But the downside? If the server goes down, everyone's stuck. A good example would be a banking app—everything is controlled, monitored, and secure from a central server.

Peer-to-Peer (P2P):
Here, every device is both a client and a server. There's no central control, so it scales nicely when more peers join. But it's way harder to secure since everyone has some level of access. Think of file sharing apps like BitTorrent—super scalable but risky if someone shares a malicious file.

Hybrid:
This combines both approaches. You get the control of client-server and the flexibility of P2P. Video games are a good example—matchmaking might be server-based, but gameplay can be P2P to reduce lag.

2. VLANs, Segregation, Segmentation, and Isolation in a Multi-Tier App Architecture

- Web layer (handles user input)
- Application layer (does the processing)
- Database layer (stores the actual data)

To keep things safe and organized, we use three network concepts:

- Segregation is like putting things into different rooms. Each layer (web, app, DB) is in its own VLAN so they don't share broadcast traffic.
- Segmentation adds rules about *who* can talk to *whom*. This is where firewalls or ACLs come in—like saying the web layer can talk to the app layer, but not directly to the database.

- Isolation takes it a step further. Think of it as locking the door. You might isolate your database VLAN so only certain services or IPs (like the app server) can reach it, and absolutely no one else.

Real Example:

Let's say you have:

- VLAN 10 → Web Layer
- VLAN 20 → App Layer

You can set firewall rules like:

- Allow VLAN 10 to access VLAN 20 on port 443 (HTTPS)
- Allow VLAN 20 to access VLAN 30 on port 3306 (MySQL)

3. OSI Model's Role in Modern Internet Comms (Layer 3 & 4 focus)

The OSI model is basically a guidebook that explains how data moves from one device to another over a network. It has 7 layers, but the key ones here are:

- Layer 3 – Network Layer
  This is where IP (Internet Protocol) lives. It handles routing—so it's in charge of figuring out how to get your data from your computer in San Jose to a server in New York. Think of it like GPS for your data packets.

- Layer 4 – Transport Layer
  This one deals with end-to-end connections. TCP (Transmission Control Protocol) is reliable—it checks if everything got delivered. UDP (User Datagram Protocol) is faster but doesn't care about lost packets. You'll see TCP with stuff like file downloads, and UDP with video calls or games where speed matters more than perfection.

How this maps to real-world tech:

- DNS (Domain Name System) helps resolve a domain name like `openai.com` to an IP address. It works mostly over UDP (Layer 4) using Layer 3's IP to send and receive messages.
- HTTP/HTTPS sits on Layer 7 (Application Layer) but relies on TCP underneath it (Layer 4), which in turn uses IP (Layer 3) to travel across the internet.

- SSL/TLS (used in HTTPS) works between Layer 5 and Layer 7, but again, it builds on TCP to ensure the secure connection is reliable.

4. Zero-Trust Architecture: Security Zones & Access Control in Multi-Cloud

In a zero-trust network, nothing is trusted by default—not even inside the network. Everything needs to be verified before getting access.

Security zones help separate parts of the network:

- Public Zone – Open to everyone (like websites)
- Internal Zone – For company employees
- Restricted Zone – Very sensitive info (like finance data)
- Management Zone – For admins and IT tools

In a multi-cloud setup (like using AWS, Azure, GCP), you create zones in each cloud and only allow necessary communication between them.

To stop hackers from moving around (lateral movement), you can use:

- IAM roles to limit what users can do
- MFA to verify identity
- Micro-segmentation and firewall rules to block unnecessary connections

5. BGP, Dynamic Routing & NAT in Large Networks

Dynamic routing lets routers automatically find the best path for data. BGP is used in large networks to connect different ISPs or company branches. It helps route data across multiple internet paths.

NAT (Network Address Translation) comes in when two networks use the same private IP range. BGP and NAT work together to avoid confusion. For example, if two offices use 192.168.1.0/24, NAT changes one set of IPs before advertising it through BGP.

NAT444 adds an extra translation layer:

- Your device → home router (1st NAT)
- Home router → ISP router (2nd NAT)

- ISP router → internet (3rd NAT)

This helps deal with **IPv4 exhaustion** by letting many users share the same public IP, even with overlapping private addresses.

6. IPv6 Addressing, Header, and Transition Challenges

IPv6 uses 128-bit addresses, giving way more IPs than IPv4. There are different types:

- Global Unicast – Used on the internet
- Link-Local – Used for local communication between devices
- Multicast – Sends data to multiple devices at once

The IPv6 header is simpler and fixed at 40 bytes, making it more efficient.

Challenges in switching to IPv6:

- Address planning becomes more complex
- Some tools and devices might still only support IPv4
- Companies need to upgrade firewalls, routers, and security tools

7. ICMP, ARP, NDP, and Their Roles in Address Resolution

ICMP helps test and troubleshoot networks (e.g., with `ping`). In **IPv4**, **ARP** is used to find MAC addresses for IP addresses.

In **IPv6**, ARP is replaced by **NDP**, which works through **ICMPv6**. NDP helps with:

- Finding routers
- Resolving MAC addresses
- Making sure an IP isn't already used

If ICMP or NDP is blocked by mistake, devices won't know how to find each other or route traffic—this can cause full network failures, especially in IPv6 networks.

8. MPLS, LSP, and Traffic Engineering in a Multi-Branch Network

MPLS uses labels instead of IP lookups to move data faster through a network. It's like a shortcut that routers follow.

In a big company with many offices, MPLS helps set up Label Switched Paths (LSPs) which are fixed paths for important data, like video calls or financial transactions.

Traffic Engineering (TE) lets you control which path traffic takes and balance loads across multiple links.
To design this:

- Use multiple LSPs for redundancy (high availability)
- Apply **QoS rules** to give priority to critical traffic
- Monitor usage to avoid congestion and reroute if needed

9. Subnetting 172.16.0.0/16 into 64 Subnets

To make 64 subnets from 172.16.0.0/16, we need 6 more bits (because $2^6 = 64$). So the new subnet mask becomes **/22** or **255.255.252.0**.

Each /22 subnet gives us **1024 IPs**, but only **1022 are usable** (excluding network and broadcast addresses).

First four subnets:

1. 172.16.0.0 – 172.16.3.255
2. 172.16.4.0 – 172.16.7.255
3. 172.16.8.0 – 172.16.11.255
4. 172.16.12.0 – 172.16.15.255

Why it matters:
Subnetting helps break a large network into smaller ones, which improves performance, limits broadcast traffic, and helps in managing IPs better across different departments.

10. Subnetting & Routing Efficiency in a Corporate Network

Subnetting is basically dividing one big network into smaller chunks. This makes things more organized and helps reduce congestion. Instead of sending traffic across the whole network, it stays within a subnet—so it's faster and more efficient.

It also helps with **IP address allocation**. You can assign specific subnets to different teams, floors, or offices, and avoid wasting IPs. For example, giving the IT team a /24 subnet with 254 usable IPs means they have enough room, without using up the whole /16 range.

In routing, smaller subnets make routing tables easier to manage and improve speed, especially in a big company with many branches.