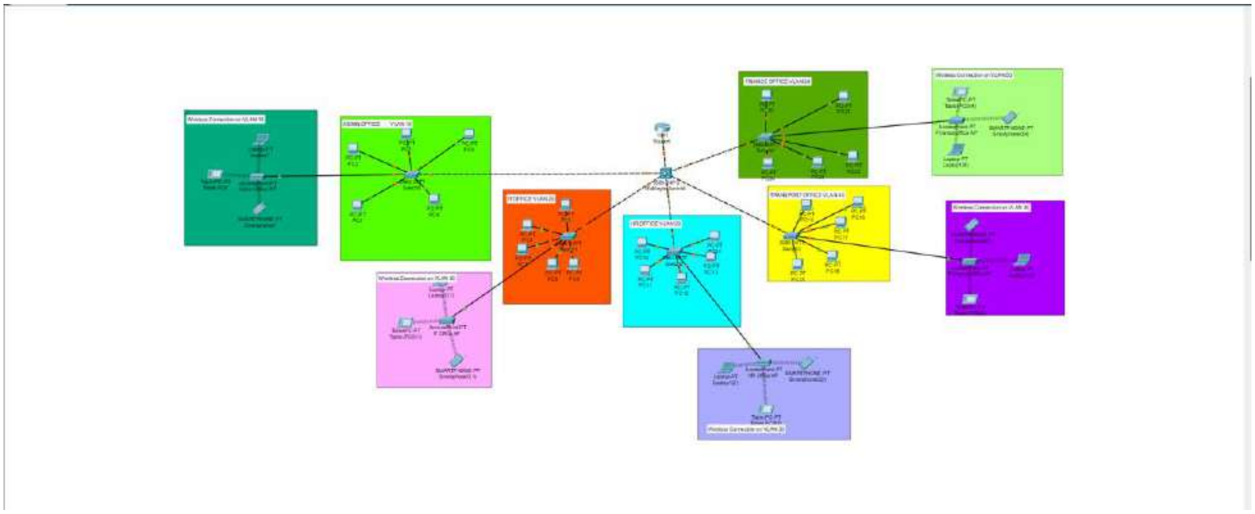
Network Design Report for Company with 500 Machines

1. Network Design and Decision Rationale

Large organization needs a flexible, secure and robust network that will server 500 user accross five different department in the company. For these purposes, the VLANs and optimal IP sub-netting plan are proposed to design the network.



1. VLAN Implementation
VLANs are beneficial when the network is divided into different subgroups by departments. This has the effect of reducing broadcast domains and further segregating all network traffic pertaining to each department on the organization. The following VLANs are defined:

- **VLAN 10**: Admin Office
- **VLAN 20**: IT Office
- **VLAN 30**: HR Department
- **VLAN 40**: Transport Department
- **VLAN 50**: Finance Department

Every VLAN is made to function as a separate virtual network so that there is improved ability to monitor and manage traffic and resources. For instance, traffic originating from the Admin Office is no longer mixed with that of the Finance Department. Also, with VLANs it becomes easier to diagnose the problems because a guaranteed fault is isolated in segments of the network.

Benefits of VLANs and Inter-VLAN Routing

Thus the incorporation of VLAN in the conceptual design of the network yields a considerable advantage in segmenting, enhancing performance and opening up of security features on the network. VLANs isolate actual physical network into different categories to minimize the broadcast domain and hence improve network traffic. Admin, IT, HR, Transport and Finance each gets own VLAN because all the dept traffic stays in dept VLAN helping to reduce traffic and increase efficiency.

With the use of Layer 3 switch, Inter- VLAN routing is enabled hence enabling communication between VLANs but still being distinguishable. This helps to reduce congestion in traffic traffic across departments and at the same time protects the data that is most sensitive in respect to access by unauthorized personnel.

Finally, VLANs make a system more secure as people within the same department are allowed to use the resources as per the set policy. For VLAN communication, the network administrators can employ a method known as the Access Control Lists ACL which enhances security to the data.

---

2. Sub-netting

Each VLAN needs 120 IPs (all devices with 100 IPs, leaving 20 IPs to expand in the future). In order to satisfy this condition a /25 is selected as the subnet mask, which allows 128 IPs per subnet.

- **Why /25?**
  Subnets in binary are created in powers of 2. The closest available subnet sizes are 64 addresses (/26) and 128 addresses (/25). Since 64 addresses are insufficient for the required 120 IPs, the /25 subnet was chosen to provide ample IP space and room for growth.

VLAN	Gateway IP	IP Range	Subnet Mask
VLAN 10 (Admin)	172.16.0.1	172.16.0.1 - 172.16.0.126	255.255.255.128 (/25)

VLAN 20 (IT)	172.16.0.129	172.16.0.129 - 172.16.0.254	255.255.255.128 (/25)
VLAN 30 (HR)	172.16.1.1	172.16.1.1 - 172.16.1.126	255.255.255.128 (/25)
VLAN 40 (Transport)	172.16.1.129	172.16.1.129 - 172.16.1.254	255.255.255.128 (/25)
VLAN 50 (Finance)	172.16.2.1	172.16.2.1 - 172.16.2.126	255.255.255.128 (/25)

The IP address allocation is as follows:

Benefits of this Subnetting Plan:

- **Optimal Address Utilization**: Ensures no IP addresses are wasted, while still leaving room for growth.
- **Improved Network Management**: Each VLAN operates as a distinct subnet, simplifying IP address management.
- **Simplified Troubleshooting**: Issues can be localized to specific VLANs/subnets.
- **Enhanced Security**: By isolating IP address spaces, internal traffic remains protected and segmented.

---

3. Network Components

The hardware chosen ensures seamless connectivity, inter-VLAN routing, and support for wired and wireless devices.

- **Layer 3 Switch**:
  - Used for **inter-VLAN routing**, allowing communication between VLANs.
  - Virtual interfaces (SVIs) are configured on the Layer 3 switch for each VLAN.
  - Advantage: Eliminates the need for multiple physical router interfaces.
- **5 Layer 2 Switches**:
  - Each Layer 2 switch connects devices (PCs, Access Points) within a single VLAN.
  - VLAN segmentation ensures traffic remains isolated within the department.
- **Router-on-a-Stick**:

  - The router is connected to the Layer 3 switch using a **trunk link**.
  - Sub-interfaces are configured on the router, one for each VLAN, enabling routing between VLANs.
  - **Benefit**: This approach uses a single physical router interface to handle inter-VLAN traffic, reducing hardware costs.
- **Access Points**:
  - Each VLAN has one Access Point to provide **wireless connectivity** for devices like laptops, smartphones, and tablets.
  - Devices are assigned IP addresses within their respective VLAN subnets.

Example Workflow:

1. A PC in VLAN 10 (Admin) sends a packet to a PC in VLAN 20 (IT).
2. The packet is forwarded to the Layer 3 switch, which routes the traffic to the appropriate VLAN via its virtual interfaces.
3. If the traffic needs to leave the network, it is routed to the external router.

Rationale for the Design

1. **Efficient IP Address Management**:
   The /25 subnet mask ensures sufficient IP addresses per department while avoiding waste. Each VLAN has room to accommodate additional devices in the future.
2. **Logical Segmentation**:
   VLANs divide the network into smaller, manageable segments, reducing broadcast domains and improving performance. For instance:
   - Admin VLAN traffic does not mix with IT VLAN traffic.
   - HR devices cannot directly access Transport VLAN resources without proper routing and permissions.
3. **Improved Security**:
   VLANs enhance security by isolating traffic between departments. Unauthorized users cannot access resources from other VLANs unless explicitly permitted through **Access Control Lists (ACLs)**.
4. **Scalability**:
   The design allows for future expansion:

   - New VLANs can be added without major reconfiguration.
   - Additional switches and access points can be integrated seamlessly.
5. **Centralized Management**:
   Using a Layer 3 switch with router-on-a-stick configuration centralizes routing and VLAN management, reducing complexity and hardware costs.
6. **Support for Wired and Wireless Devices**:
   Access Points provide flexibility by enabling wireless connectivity, ensuring all user devices (PCs, laptops, tablets, and smartphones) can connect seamlessly within their VLAN.

---

2. Design Model and WAN Protocol

Design Model

The network design adheres to the **hierarchical model**, which is a proven architecture that divides the network into three distinct layers. This approach improves performance, scalability, and ease of management.

1. **Access Layer**
   - The Access Layer consists of **Layer 2 switches**.
   - These switches connect **end devices** such as PCs, laptops, smartphones, tablets, and Access Points.
   - **Function**:
     - Provides port connectivity for devices.
     - Handles VLAN assignments and forwards traffic within the VLAN.
     - Controls access through technologies like port security, enabling MAC filtering to prevent unauthorized devices.
2. **Distribution Layer**
   - The **Layer 3 switch** operates at this layer.
   - **Primary Functions**:

        - Performs **inter-VLAN routing** by managing traffic between VLANs through **SVIs (Switched Virtual Interfaces)**.
        - Provides policy enforcement using **Access Control Lists (ACLs)** to control traffic between VLANs.
        - Aggregates traffic from Access Layer switches and forwards it to the Core Layer.
    - The Layer 3 switch is connected to the router using a **trunk link** to carry traffic from multiple VLANs.
3. **Core Layer**
    - The **router** handles the network's external connectivity (WAN).
    - **Function**:
        - Routes traffic to external networks using a **Router-on-a-Stick** configuration, which allows the router to manage VLAN traffic over a single physical interface using sub-interfaces.
        - Provides WAN connectivity to remote sites or the internet.

Advantages of the Hierarchical Model:

- **Simplified Management**: Each layer has a defined function, making troubleshooting and administration more manageable.
- **Scalability**: New switches, VLANs, or devices can be easily added without disrupting the existing network.
- **Improved Performance**: Traffic is organized into VLANs, reducing broadcast traffic and enhancing overall network performance.
- **Redundancy**: By design, hierarchical models allow for redundant links and failover capabilities, ensuring reliability.

WAN Protocol

To connect the organization's internal network to remote locations or external networks, **WAN protocols** are required. The network uses **Frame Relay** or **PPP (Point-to-Point Protocol)** for WAN connectivity.

1. **Frame Relay**
    - Frame Relay is a packet-switched WAN protocol that provides **cost-effective connectivity** for multiple remote locations over a shared network infrastructure.
    - **Benefits**:
        - **Cost-Effective: Relies on a shared network, therefore costs of operation are cheaper than the cost of leased lines.**
        - Efficient: It is good for bursty traffic since it puts into practice bandwidth on demand.

- Scalability: Allows connectivity to several Virtual Circuits which connect to different branch offices or remote sites.

2. **PPP (Point-to-Point Protocol)**

PPP is another such protocol used in WANs for establishing point to point link to serial connection. It offers reliability, security features and backup for authentication.

Benefits:

- Secure: The target systems can authenticate remote connections, using suitable protocols, such as CHAP (Challenge-Handshake Authentication Protocol).
- Reliable: Increases error detection and allows for correction of the errors making it suitable for mission critical traffic.
- Flexible: Works well with most of the networking technologies and equipments.

WAN Protocol	**Advantages**	**Use Case**
Frame Relay	Cost-effective, scalable	Connecting multiple branch offices remotely
PPP	Secure, reliable, flexible	Reliable point-to-point WAN connectivity

Justification

The chosen hierarchical model and WAN protocols provide the following benefits:

1. **Simplified Network Management**:
   The hierarchical model clearly separates network functionality across three layers, making it easier to manage, troubleshoot, and scale the network.
2. **Scalability**:
   - VLANs and Layer 3 routing allow for the easy addition of new departments, VLANs, and devices without disrupting the overall network.
   - WAN protocols like Frame Relay support expansion to additional remote locations.
3. **Performance**:
   VLAN segmentation at the Access Layer reduces congestion and broadcast traffic. Layer 3 routing at the Distribution Layer ensures efficient traffic flow between departments.
4. **Cost-Effectiveness**:
   - Frame Relay reduces operational costs for organizations with multiple branch connections.
   - PPP offers secure and reliable point-to-point connections without requiring expensive leased lines.
5. **Security**:

- **Internal Security**: VLANs isolate departmental traffic, and ACLs on the Layer 3 switch control inter-department communication.
- **WAN Security**: PPP provides robust authentication through CHAP, preventing unauthorized access.

---

3. Security Risks and Mitigations

Security is a critical component of any network design, and risks must be addressed at multiple layers of the TCP/IP stack. Below are the identified security risks and their corresponding mitigations at **Layer 1 (Physical Layer)**, **Layer 2 (Data Link Layer)**, and **Layer 3 (Network Layer)**.

Layer 1: Physical Layer

The **Physical Layer** involves hardware components, cabling, and the physical infrastructure of the network. Security risks at this layer primarily stem from unauthorized physical access and equipment damage.

Risks:

1. **Physical Tampering: Malcontents integrating switch, routers, and/or servers they have no right opening in the first place.**
2. Unauthorized Cable Connections: To join unauthorised devices to the network.

3. Hardware Damage: Fluorescent lamps may fail due to power failures, overheating or because they have been intentionally switched off.

Mitigations:

1. **Controlled Physical Access**:
    - Limit accessibility of Server room, Data center and Network equipment room only to some selected personnel.
    - Install keycard doors, biometric doorlocks and use the register of the visitors.
2. **Physical Security Measures**:
    - Do not leave networking devices around the store where anyone can access them which can be on open shelves or racks.
    - Authorized install surveillance systems(Security cameras) for monitoring strategic regions.
3. **Hardware Protection**:
    - Invest in UPS's to guard against fluctuations and complete power outages.
    - Establish right measures to cool the body to avoid heat stroke.
    - Physical care involves taking regular care to check on some of the basic setup to check their readiness to provide support.

Layer 2: Data Link Layer

A part of the Data Link Layer focuses on device oriented communication and switching. Threats at this layer are spoofing attacks, VLAN attacks, and ARP poisoning attacks.

Risks:

1. MAC Address Spoofing: An attacker enters into an unauthorized position by pretending to be a genuine device through MAC address emulation.
2. VLAN Hopping: An attacker uses VLAN misconfigurations to forward traffic between VLANs so that they cross necessary security barriers.
3. ARP Poisoning: Intercepting or redirecting traffic in between connected devices by altering contents of ARP table.

Mitigations:

1. **Port Security**:
    - The next option allows the setting up of the Layer 2 switch for port security with an aim of limiting MAC address per port.
    - Ports that have noted unauthorized MAC address should be closed.
2. **VLAN Security**:

  - Use VACLs which can be configured to determine what traffic is allowed or denied on VLANs to avoid traffic from unauthorized areas.
  - Switch off unused ports and place them into a vacuous VLAN.
3. **ARP Spoofing Prevention**:
  - Turn on DAI on switches to prevent ARP fakes and allow only valid ones on a network.
  - Where ever possible, prefer to use static ARP mappings for essential network resources.

Layer 3: Network Layer

The Network Layer has the functions of routing packets between two or more networks. Challenges in this layer include the ability to spoof IP address, change routing tables and break into a network.

Risks:

1. IP Spoofing: The attacker has to forge the IP addresses to mimic an identity that is welcome in order to gain entry.
2. Routing Attacks: Changing routing protocols or tables specially to reroute traffic in an improper and malicious way.
3. Unauthorized Access: Initial attackers trying to gain unauthorized access into the network.

Mitigations:

1. **Access Control Lists (ACLs)**:
  - Filter traffic on all access-exiting Layer 3 devices such as routers and Layer 3 switches to admit only accepted traffic.
  - Block traffic from some suspicious and unknown IP addresses.
2. **Firewall Policies**:
  - Setup filters on routers to properly handle any malicious activity, attempts of unauthorized access and port probing.
  - Stateful firewall is used to filter traffic according to the session states which are continually changing.

3. **Network Address Translation (NAT)**:
    - NAT should be used in order to conceal internal private IP addresses when communicating with outsiders, thus the attackers are least likely to have direct access to the networks.
    - Use **PAT (Port Address Translation)** to further enhance security by mapping multiple internal addresses to a single public IP.
4. **Routing Security**:
    - Use secure routing protocols like **OSPF with authentication** to prevent routing table tampering.
    - Regularly monitor routing configurations for anomalies.

Summary

Addressing security risks at Layers 1, 2, and 3 ensures a comprehensive defense strategy:

- **Layer 1** focuses on physical protections such as controlled access and equipment safeguards.
- **Layer 2** implements measures to secure MAC addresses, VLANs, and ARP processes to protect switching operations.
- **Layer 3** leverages ACLs, firewalls, and NAT to safeguard routing and network-layer traffic.

By implementing these mitigations, the network is fortified against common threats, ensuring reliability, confidentiality, and integrity.

---

4. Protocols at Layers 1, 2, and 3

Layer	Protocol	Description
Layer 1 (Physical)	Ethernet (IEEE 802.3), IEEE 802.11	Physical transmission of data (cables, Wi-Fi).

Layer	Protocol	Description
Layer 2 (Data Link)	VLANs, STP, MAC	Data frame delivery and switch-based separation.
Layer 3 (Network)	IPv4, ICMP, OSPF, PPP	Logical addressing, routing, and communication.

5. Detailed Cost Table

Option 1: High-Performance Setup

Item	Quantity	Unit Price (GBP)	Total Cost (GBP)
Layer 3 Switch	1	£2,500	£2,500
Layer 2 Switches (L2)	5	£800	£4,000
Router	1	£1,200	£1,200

Item	**Quantity**	**Unit Price (GBP)**	**Total Cost (GBP)**
Access Points	5	£300	£1,500
Workstations (PCs)	25	£600	£15,000
Laptops	5	£800	£4,000
Smartphones	5	£500	£2,500
Tablets	5	£400	£2,000
Cabling and Installation	1	£1,500	£1,500
Total Cost			£**34,200**

Option 2: Cost-Effective Setup

Item	**Quantity**	**Unit Price (GBP)**	**Total Cost (GBP)**
Layer 3 Switch	1	£1,500	£1,500
Layer 2 Switches (L2)	5	£500	£2,500
Router	1	£800	£800

Item	**Quantity**	**Unit Price (GBP)**	**Total Cost (GBP)**
Access Points	5	£200	£1,000
Workstations (PCs)	25	£400	£10,000
Laptops	5	£600	£3,000
Smartphones	5	£300	£1,500
Tablets	5	£250	£1,250
Cabling and Installation	1	£1,000	£1,000
Total Cost			**£22,550**

6. Cost Comparison

Criteria	**Option 1: High-Performance**	**Option 2: CostEffective**
Total Cost	£34,200	£22,550
Hardware Performance	High	Moderate
Scalability	Excellent	Good
Future Proofing	Strong	Moderate
Budget Consideration	High Investment	Cost-Friendly

7. Conclusion

The proposed network design comprehensively addresses the organization's requirement to support **500 devices**, ensuring a robust, scalable, and secure infrastructure that meets both current operational demands and potential future growth. By integrating VLANs for logical segmentation, effective IP subnetting, and a hierarchical network model, the design optimizes resource allocation, minimizes broadcast domains, and enhances overall manageability.

1. **Scalability**:
    - The design allows seamless integration of additional devices or departments in the future by allocating extra IP addresses within the subnetting scheme.
    - VLAN-based segmentation ensures new departments or users can be added without disrupting existing configurations.
2. **High Performance**:
    - The Access, Distribution, and Core layers form the hierarchical model; this keeps traffic stress at a check while at the same time improving data throughput that experiences minimal delay.
    - Inter VLAN routing is well done by layer 3 switches and router onion skin to ensure that both wired and wireless users will feel the optimum in accessing the network.
3. **Security**:
    - As a result, Layer 1 (Physical), Layer 2 (Data Link) and Layer 3 (Network) meet good security standards of port security, ARP inspection, firewall, and access control list (ACL).
    - The inbound security is complemented by Network Address Translation (NAT) and secure WAN protocols.

Cost Options

To cater to the organization's diverse financial capabilities and strategic priorities, two cost options have been provided:

High-Performance Setup:

- This option targets organizations that are willing to invest in the long term in reliability, scalability, and features giving steep performance.
- Here are the high-quality products that adept for enterprise uses they are switches, routers, and large capacity APs to sustain network usage.
- Most advantageous in organizations expected to grow greatly or those with essential functions because system unavailability is inconceivable.

2. **Cost-Effective Setup**:

- This features is aimed at organizations with limited budgets to help them achieve the best balance between functionality and price.

- Employs mid-range equipment sufficient to meet present requirements but could need replacement when the organization grows.

- Ideal for firms that do not necessary have the resources to spend much money but still need some form of a system to work with.

The design of a /25 subnet mask and VLAN business segmentation also allows for future accommodation. The address space for each VLAN is enough to support users and the bandwidths can always be increased if the number of users goes beyond 500. This hierarchical structure also makes it easier to incorporate even new network elements, be it added switches or the wireless access points with relative small impact on the whole hierarchy.

The choice between the two cost options will depend on the organization's budgetary priorities and long-term strategic goals:

- If the company foresees rapid growth or operates in a high-demand environment, the **High-Performance Setup** is recommended for its scalability and reliability.
- For organizations aiming to meet immediate needs within a limited budget, the **Cost-Effective Setup** is a practical and sustainable choice.

Regardless of the selected option, this network design delivers a secure, scalable, and high-performing solution that aligns with the organization's operational goals and supports its success in the digital era.

8.References

1. Cisco Systems, Inc. (2021). VLAN Configuration Guide. Available at: https://www.cisco.com.
2. Tanenbaum, A. S. and Wetherall, D. J. (2011). Computer Networks. 5th edn. Boston: Pearson.
3. Stallings, W. (2020). Data and Computer Communications. 11th edn. Upper Saddle River, NJ: Pearson.
4. Kurose, J. F. and Ross, K. W. (2021). Computer Networking*:* A Top-Down Approach. 8th edn. Boston: Pearson.
5. IEEE (2020). 802.1Q: Standards for VLAN Tagging. Available at: https://ieeexplore.ieee.org.
6. Doyle, J. (2020). Routing TCP/IP. 2nd edn. Indianapolis: Cisco Press.
7. Oppenheimer, P. (2010). Top-Down Network Design. 3rd edn. Indianapolis: Cisco Press.
8. Cisco Systems, Inc. (2022). Port Security Configuration. Available at: https://www.cisco.com.

9. Ramaswamy, S. (2021). Dynamic ARP Inspection and Security Mechanisms. Journal of Networking Technology, 14(3), pp. 45-50.
10. Chappell, L. (2017). Wireshark Network Analysis. 3rd edn. Lawrence: Protocol Analysis Institute.
11. Garg, S. (2018). Networking Protocols and Performance Analysis. IEEE Communications Surveys and Tutorials, 20(2), pp. 85-102.
12. Microsoft (2023). Best Practices for NAT Implementation. Available at: https://docs.microsoft.com (Accessed: 17 December 2024).
13. Gallo, M. A. and Hancock, W. M. (2001). Networking Explained. 3rd edn. Burlington, MA: Elsevier.
14. Gartner, Inc. (2023). Cost Analysis of Networking Equipment. Available at: https://www.gartner.com.
15. He, J., Luo, X. and Chan, H. C. (2019). Securing Layer 2 and 3 of TCP/IP Stack. International Journal of Computer and Network Security, 11(2), pp. 89-98.