**A logo of a university

Description automatically generated**

**JOMO KENYATTA UNIVERSITY**

**OF**

**AGRICULTURE AND TECHNOLOGY**

**SCHOOL OF ELECTRICAL, ELECTRONIC AND INFORMATION**

**ENGINEERING**

**DEPARTMENT OF TELECOMMUNICATION AND INFORMATION ENGINEERING**

**5.2**

**ETI 2508**

**NETWORK DESIGN AND MANAGEMENT**

**GROUP MEMBERS**

|  |  |
| --- | --- |
| **MATIKO GEORGE MAROA** | **ENE221-0129/2020** |
| **GATONYE STEPHEN KURIA** | **ENE221-0107/2020** |
| **IFRAH FARAH** | **ENE221-0111/2020** |
| **NDONI WILLIAM OMONDI** | **ENE221-0125/2020** |
| **MAINA FAITH MURUGI** | **ENE221-0225/2020** |

**OBJECTIVES**

1. To design a scalable and efficient Campus Area Network (CAN) for a newly established university consisting of three academic blocks: the School of Engineering, the School of Computing, and the School of Business.
2. To propose a suitable network architecture that includes the selection of an appropriate topology and the identification of core, distribution, and access layer components.
3. To analyze and recommend appropriate communication protocols across different OSI layers, ensuring seamless connectivity, reliable data transmission, and effective routing within the campus network.
4. To evaluate the performance requirements of the CAN by assessing bandwidth needs, minimizing latency, and implementing Quality of Service (QoS) mechanisms to prioritize critical traffic.
5. To outline robust security measures including firewalls, access control, and encryption strategies to safeguard network infrastructure and user data.
6. To provide for future scalability and flexibility, ensuring the network can accommodate growth such as additional user devices or expansion to new campuses.
7. To develop an actionable implementation plan that includes deployment phases, cost estimates, and a Bill of Quantities (BoQ), guiding the successful rollout of the proposed CAN infrastructure.

**INTRODUCTION**

This report presents the design and proposed implementation strategy for a Campus Area Network (CAN) for a newly established university comprising three schools: the School of Engineering, the School of Computing, and the School of Business. Each school is housed in a separate physical block, necessitating a network design that ensures high availability, performance, and security across all locations.

The assignment is intended to help us, students, understand essential concepts in network design, including topology selection, hierarchical structuring, protocol application, bandwidth and latency considerations, and Quality of Service (QoS) implementation. Moreover, it emphasizes the importance of integrating robust security measures such as firewalls, access controls, and data encryption.

By engaging with this project, we will develop a practical understanding of network design principles, performance optimization strategies, and security requirements, all of which are fundamental to the deployment and management of modern campus networks.

**NETWORK DESIGN METHOGOLOGY**

1. **PLANNING**

The planning phase is the foundational step in the network design methodology. It involves a comprehensive assessment of both the business and technical requirements of the proposed Campus Area Network (CAN) for the university. The objective is to ensure that the network aligns with institutional goals while meeting performance, scalability, and security demands.

1. Requirements Analysis

We assumed a detailed requirement analysis was conducted to understand the user base, application needs, and data communication patterns within the university. Key considerations included:

* The presence of three academic schools: Engineering, Computing, and Business, each occupying a dedicated block.
* An estimated number of users per academic school: 5000 students and staff.
* Support for bandwidth-intensive applications such as video conferencing, online learning platforms, and cloud services.
* Expected simultaneous device connections per block: approximately 5000.

1. Site Survey and Feasibility Study

We assumed that a preliminary site survey was conducted which assessed the physical environment and infrastructure readiness and we made the following key findings:

* All three school blocks are interconnected suitable for fiber optic cables that are in the manholes..
* Availability of structured cabling ducts and power supply in each block.
* Wireless coverage planning considered potential interference sources such as walls, furniture, and electronic devices.
* Regulatory compliance with local building codes and IT safety standards was confirmed.

1. Capacity planning

We focused on estimating the network’s ability to handle current and future demands:

* We projected bandwidth requirement per block to be: 1–2 Gbps.
* We planned the future scalability for an additional 30–50% increase in users and devices.
* We prioritized the Quality of Service for time-sensitive traffic such as VoIP, Learning Management System(LMS) usage, and administrative operations.
* We developed the baseline traffic models based on anticipated academic activities and institutional schedules.

1. Business and technical goals

We assumed we made an engagements with academic and administrative stakeholders which provided insights into the university’s strategic goals which included:

* Enhancing academic delivery through uninterrupted access to digital resources.
* Reducing operational costs via centralized services.
* Enabling future expansion (e.g., new schools or buildings).

Our network design intends to support the above university’s goals.

**Some of the technical goals** that we highlighted included:

* High network availability (>99.98%)
* Low latency (<5 ms within campus)
* Strong security posture through access control and encryption
* Efficient management and ease of maintenance

#### ****Design Phase****

The design phase transforms the planning requirements into a structured and scalable network blueprint. This includes the development of both the logical and physical designs, selection of communication protocols, and the definition of network security strategies.

Our proposed network for the university follows a three-tier hierarchical model comprising the **Access Layer**, **Distribution Layer**, and **Core Layer**.

1. Logical Network Design

Our proposed Campus Area Network (CAN) adopts a **hierarchical star topology**, which offers improved scalability, ease of management, and fault isolation.

1. Access Layer

* Comprises **Layer 2 switches** that provide end-user connectivity within the School of Engineering, School of Computing, and School of Business.
* Devices such as student computers, staff PCs, IP phones, and wireless access points are connected at this layer.
* Each department is segmented using **Virtual LANs (VLANs)** to ensure logical separation of traffic and enhanced security.

1. Distribution Layer

* Two centralized Layer 3 switches are deployed in the main network facility to aggregate traffic from all access layer switches across the campus.
* These switches are responsible for inter-VLAN routing, traffic aggregation, and implementing QoS policies.
* To ensure gateway redundancy and high availability, Hot Standby Router Protocol (HSRP) is configured between the two distribution switches.HSRP provides a virtual IP address per VLAN, ensuring continuous gateway availability in the event of a switch failure.
* An EtherChannel link is configured between the two Layer 3 switches to increase bandwidth and allow for stateful failover of HSRP sessions.
* The distribution switches connect to the **firewall** via high-speed links, ensuring secure traffic inspection and filtering before passing data to the core router. The firewall acts as the perimeter security device, managing access control and threat prevention.
* The **firewall** is then connected to the **core router** via a high-speed 2 Gbps fiber optic link, ensuring fast and secure routing between the network's internal and external segments.
* OSPF is used as the routing protocol for dynamic route management and scalability, with the firewall allowing or blocking traffic based on security policies.

1. Core Layer

* The **core network consists of a high-performance router and a dedicated enterprise firewall** deployed at the central data center.
  + The **router** serves as the **gateway to external networks**, such as the internet and any future remote campus sites. It does **not perform internal routing**, as all inter-building and inter-VLAN routing is managed at the distribution layer.
  + The **firewall** provides **perimeter protection**, including intrusion detection/prevention, Virtual Private Network (VPN) access, Network Address Translation (NAT), and centralized access control policies.
* All distribution switches are connected to the core router via a firewall using **2 Gbps fiber optic links** to ensure low-latency and high-throughput data transfer.

##### **Physical Network Design**

The physical network layout implements the logical design using structured cabling and network devices:

* **Core Infrastructure**: Router and firewall located in a secure central data center.
* **Fiber Backbone**: All school blocks are interconnected using **underground multi mode fiber optic cables routed through manholes**, allowing for efficient maintenance and scalability.
* **Access Switches**: Housed in network closets on each building, connected via CAT6 cables to endpoint devices.
* **Wireless Infrastructure**: Ethernet 802.11ac/ax dual-band access points are deployed to provide reliable campus-wide Wi-Fi coverage.

1. Protocol selection

We selected appropriate communication protocols based on reliability, scalability, and compatibility:

* ****Data Link Layer****: IEEE 802.3 (Ethernet) and IEEE 802.11ac/ax (Wi-Fi) for wired and wireless connections.
* **Network Layer**: IPv4 addressing with **OSPF(Open Shortest Path First)** for internal dynamic routing between VLANs.
* **Transport Layer**: TCP for reliable applications (e.g., LMS, portals), and UDP for real-time applications (e.g., video conferencing).
* **Application Layer**: DNS, HTTP/HTTPS, SMTP, SNMP for core services and management.

1. Security design

Security will be integrated into every layer of the network:

* **Firewall** at the core enforces external access control, threat prevention, and VPN policies.
* **VLAN segmentation** isolates user groups to limit broadcast domains and enhance internal security.
* **Access controls** such as MAC filtering, WPA3 encryption on wireless APs, and user-based policies are enforced.
* **Network monitoring** with SNMP and Syslog ensures visibility and alerting for network events.

1. **Implementation**

This phase involves the practical deployment of our designed Campus Area Network (CAN). This includes the procurement of hardware and software, physical installation, configuration of network devices, and comprehensive testing to ensure the network operates according to specifications. Our implementation strategy is phased to minimize disruptions and ensure smooth integration.

1. **Phase 1: Pre-deployment**

* Finalize procurement of all network components.
* Prepare documentation including network design blueprints, IP plans, and device configurations.
* Establish a rollback plan in case of deployment issues.

1. **Phase 2: Physical Installation**

* Install core and distribution switches in the central server room and each school block.
* Lay fiber optic backbone between the buildings.
* Deploy access switches and wireless access points in classrooms, offices, and labs.
* Install UPS and power management systems for critical infrastructure.

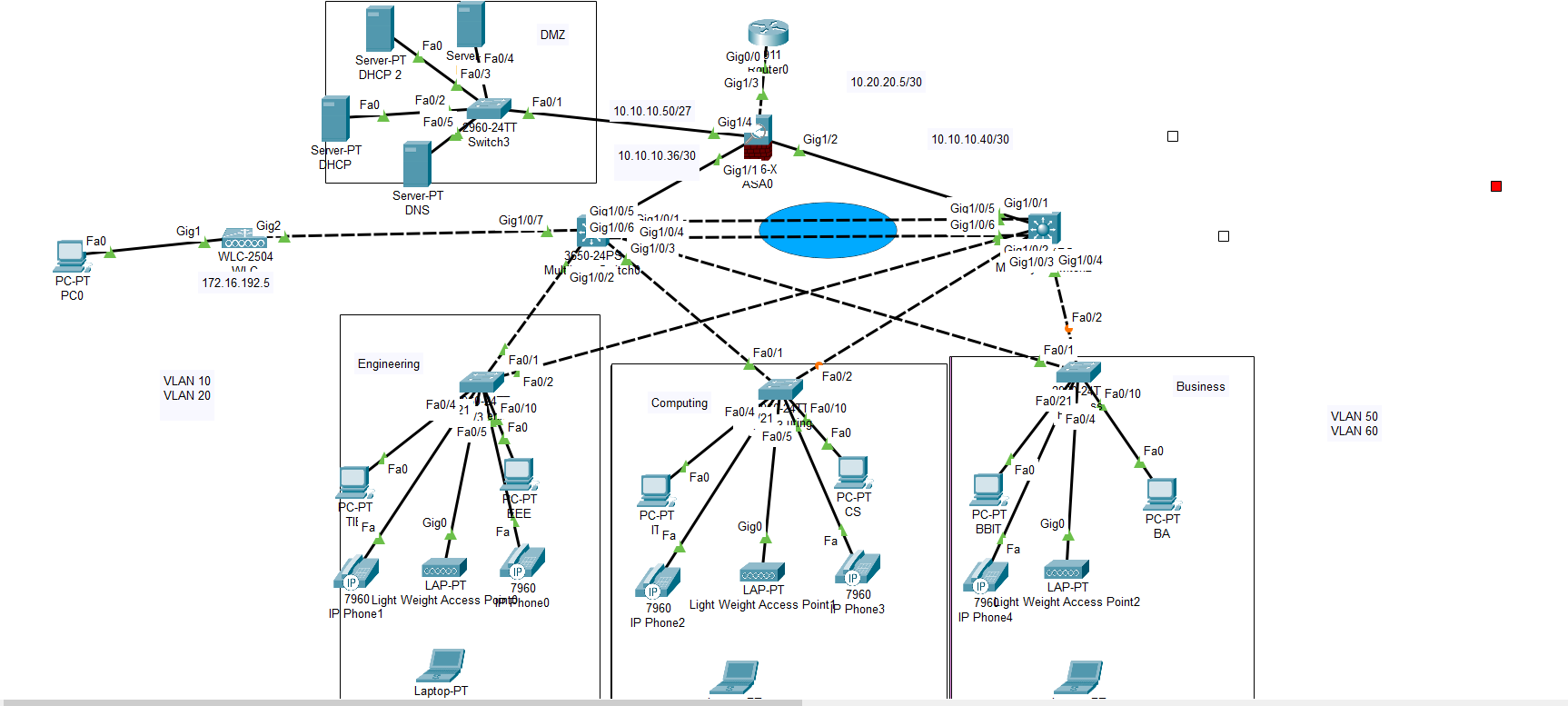
1. **Phase 3: Configuration**

* Configure VLANs, IP addressing, and routing protocols (OSPF).
* Set up DHCP, DNS, and firewall policies.
* Configure access points with SSIDs, security protocols (WPA3), and bandwidth controls.
* Apply QoS settings for real-time applications.s

1. **Phase 4: Testing and Validation**

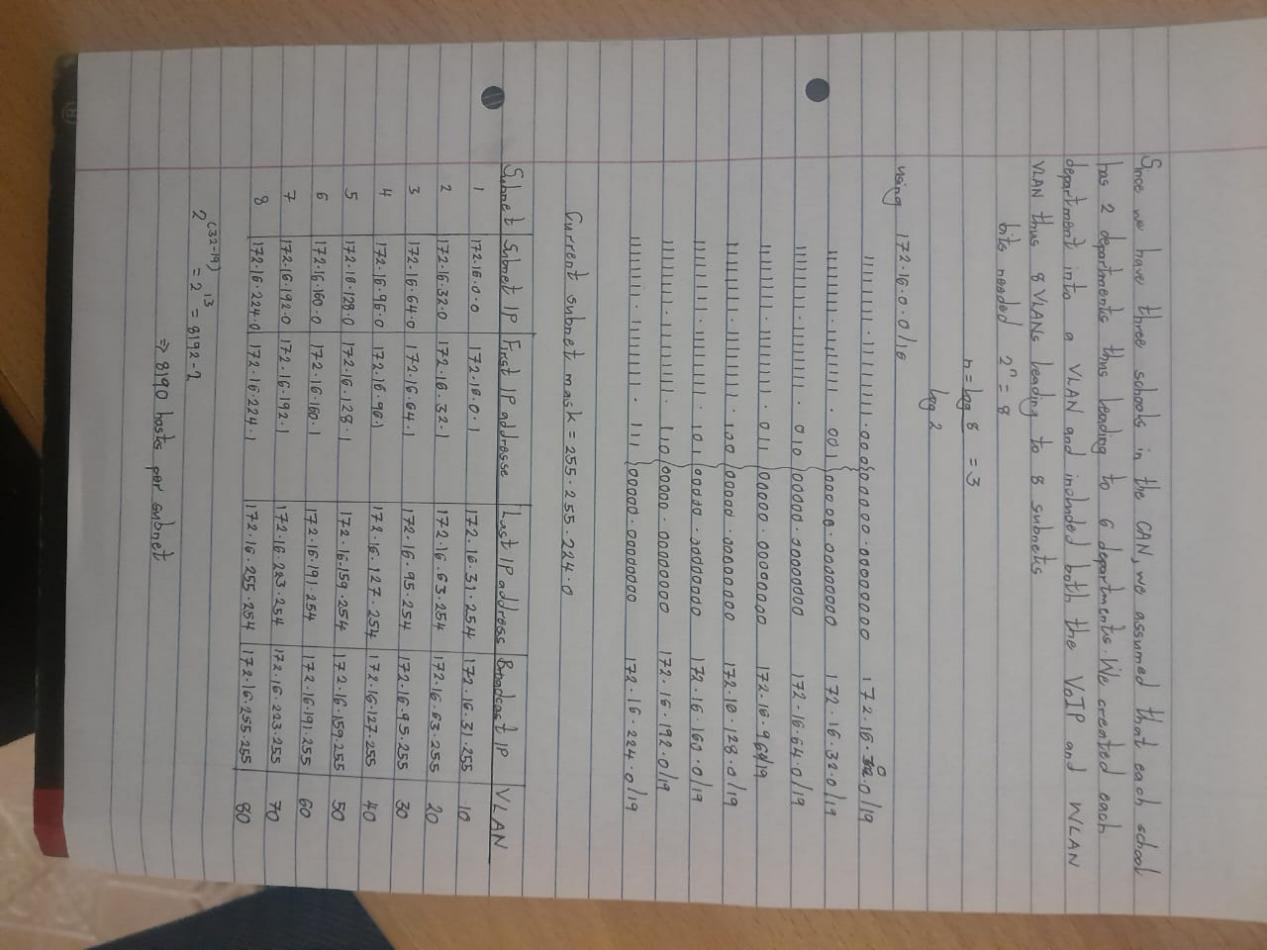
* Conduct connectivity, throughput, and latency testing.
* Perform penetration tests and vulnerability scans.
* Validate failover and redundancy mechanisms.
* Simulate user access scenarios and peak traffic conditions.

1. **Phase 5: Simuluation**



Since we have been told to design a campus area network with three schools namely School of Engineering, School of Computing and School of Business, we decided to use three-layer hierechical model that divides the network into the access, distribution and core layers. The access layers include the layer 2 access switches and the end devices. The distribution layer includes the layer 3 switches which are used for the inter-vlan routing and its routing capabilities while the core layer encomposes the router which connects us to the larger outside network.

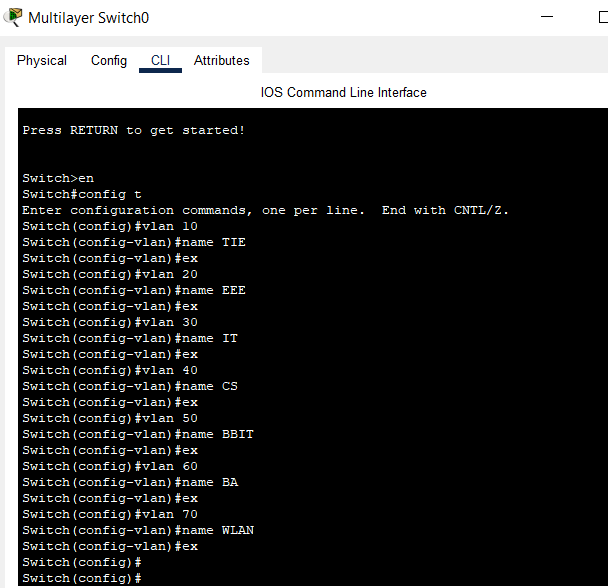
We decided to demonstate using 7 data VLANs assuming that each school has two departments and we have a vlan Wireless Access Points and 1 Voice Vlan for VoIP.This 8VLANs lead to the formation of 8 subnets as shown below;



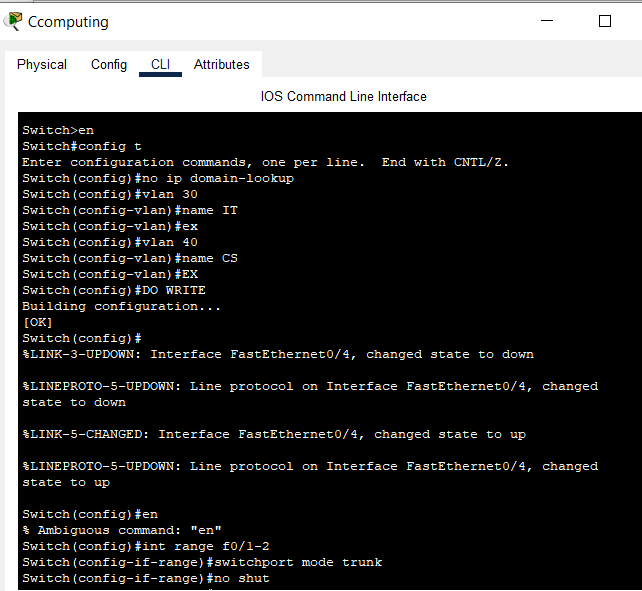
|  |  |
| --- | --- |
| VLAN | Department |
| 10 | TIE |
| 20 | EEE |
| 30 | IT |
| 40 | CS |
| 50 | BBIT |
| 60 | BA |
| 70 | WLAN |
| 80 | VoIP |

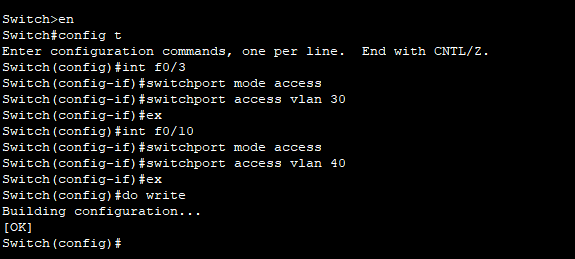
Access Layer

We created the above VLANs on the three access switches and the two multilayer switches using the commands shown below:



On the access layer 2 switches we assigned the various ports as access ports and assigned them their various intended VLANs since we decided to use port based VLANs. We also assigned trunk ports to the ports that connect the layer 2 switches to the layer threee switches as shown below;

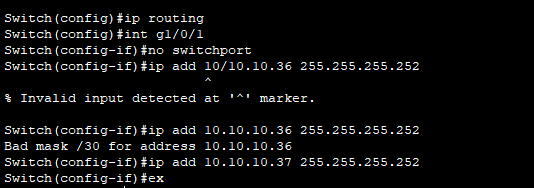




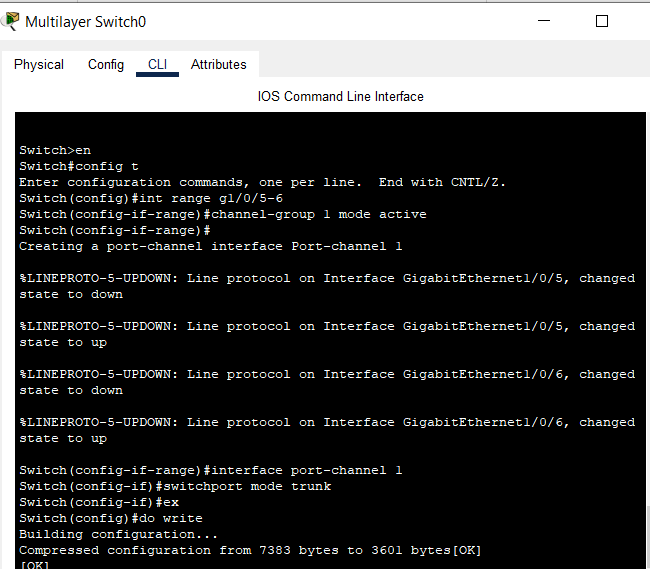
**Distribution Layer**

On the **Distribution Layer,**we used the Layer the 3 switches that enables the inter-vlan routing allowing communication between different VLANs by routing the packets between the different subnets. We also

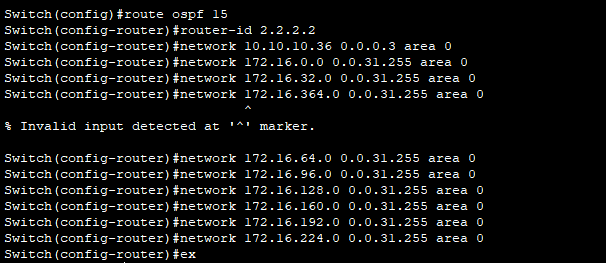
the link connecting the layer 3 switch to the core layer through a firewall into a routed port from a switchport using the **no switchport** command and assigned the interface an ip address as shown below;



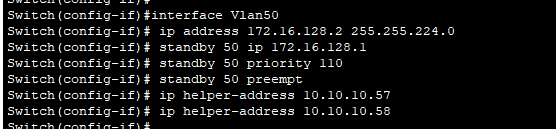
We also created Etherchannels (bundling multiple physical links into 1 logical link) between the 2 layer three swiches as shown below.Etherchannels are important since they provide redundancy and fault tolerance because if one link fails ,traffic continues in the remaining likns. Etherchannel also helps in load balancing since traffic can be distributed across the logical links.

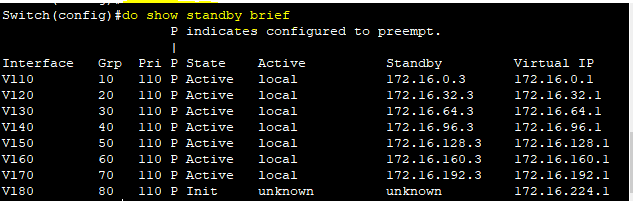


We also used the OSPF routing protocol between our firewall and the two layer 3 switches which automatically eliminates the need to manually configure static routes between VLANs by automatically learning routes to the other networks eg. DMZ,firewall, internet.We created a single area design of the ospf (area 0) as shown below;



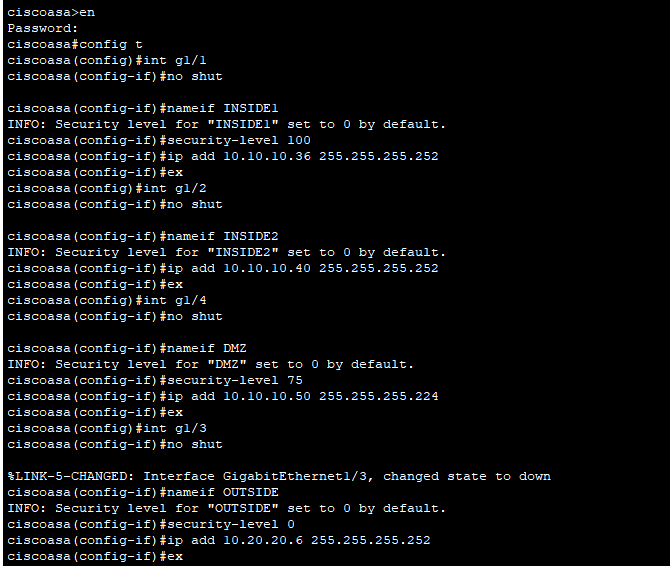
Since one of the layer 3 switches is a standby switch for the active one,we used the HSRP(hot standby routing protocol) as shown below whereby we assigned virtual ip as our default gateways .The active switch handles our traffic while the standby swich is ready to take over in case of failure thus ensuring continuous connectivity.



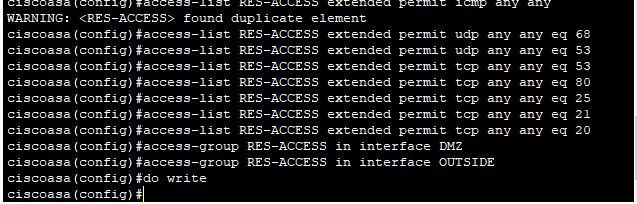


**Core Layer**

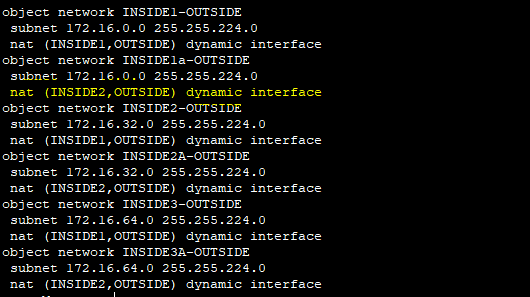
On our core layer we have a firewall and a core router.In the firewall we configured security levels and zones depending on its interfaces.This interface configuration ensures that the firewall acts as a **trusted gateway** for the internal network ( **INSIDE** security zone) while controlling traffic between different network zones such as the DMZ, or OUTSIDE as shown below;



We also implemented the **Access Control List (ACL)** to control traffic flowing between the **DMZ** (Demilitarized Zone) and other network zones. The ACLs provide specific rules that govern which traffic is allowed to enter or leave the DMZ, helping to secure the network while enabling necessary services and bound them to their necessary interfaces as shown below;



We also implemented the **Network Address Translation (NAT)** rules to enable devices from different internal subnets to access external OUTSIDE networks e.g. the internet while preserving the security of the internal network as shown below;



Our router serves as the gateway to external networks such as the internet and any future remote campus sites thus allowing for scalability.

**Quality of Service Implementation**

Quality of Service is a set of techniques used in networking to manage and prioritize traffic to ensure that critical and time-sensitive data is delivered reliably,efficiently and with minimal delay, jitter or packet loss.

We intend to use the following QoS implementation techniques;

1. **Classification and Marking.**Classificationinvolves identifying and grouping traffic either by application,port number,source and destination IP while marking involves tagging of packets with priority levels using Differentiated Services Code Points(DSCP) and Class of Service(CoS) whereby you can map VoIP packets with higher DSCP value.
2. **Queueing** whereby we organize packets into queues based on priority and higher priority queues are served before lower priority ones.
3. **Traffic Policing and Shaping.**Policing is mainly used on ingress(incoming) traffic whereby packets that exceed a defined rate are dropped or remarked.Shaping is mainly used in egress/outgoing traffic involves smoothing traffic bursts to fit within the allowed bandwidth eg. you can allow only 2Mbps of video traffic while dropping the excess traffic.

**BILL OF QUANTITIES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Quantity** | **Unit Price** | **Total Price** |
| 2911 Cisco router | 1 | 200,000 | 200,000 |
| Cisco ASA 5506 K9 Firewall | 1 | 75,000 | 75,000 |
| HPE DL380 Servers | 1 | 390,000 | 390,000 |
| CISCO Catalyst 3650 Layer 3 switch | 2 | 140,000 | 280,000 |
| CISCO Catalyst 2960 Layer 2 switch | 3 | 80,000 | 240,000 |
| CP-7942G IP phones | 15 | 16,500 | 247,500 |
| Light Weight Access Point | 8 | 40,000 | 320,000 |
| Multi Mode Fibre cable | - | - | 14,000 |
| CAT 6 Twisted Pair Cables | - | - | 6,000 |
| RJ45 Connectors | 400 | 5 | 4,000 |
| Miscellaneous | - | - | 20,000 |
| **Total Budget** |  |  | **1,796,500** |