NETWORK CASE

DOCUMENTATION FOR OLESH TELCO

OLesh TELECOM

Table of Contents

INTRODUCTION

PROJECT OVERVIEW

This project focuses on designing and implementing a telecommunications network that ensures reliable, scalable, and high-performance communication services, secure, scalable, and high-performance network to meet the company's growing demands including both data and voice transmission. The network will leverage modern communication technologies such as Fiber Optic, 5G, and Internet Protocol (IP) networks.

PROJECT OBJECTIVES

The primary objectives of the telecommunications networking system include:

- Ensuring high availability for business operations.
- Implement robust security measures to protect data and communication.
- Create a scalable design for future growth and expansion.
- Integrating voice, video, and data services into a unified system.
- Ensuring secure and efficient communication with minimal downtime.

PROJECT SCOPE

The scope of this project includes:

- Designing the network architecture for OLesh Telco, including both fixed and wireless connectivity.
- Configuring and deploying network devices (routers, switches, firewalls, etc.).
- Testing the network for performance, security, and reliability.
- Ensuring future scalability to accommodate growth in user traffic.

PROJECT TIME

Estimated at 12 months with phases:

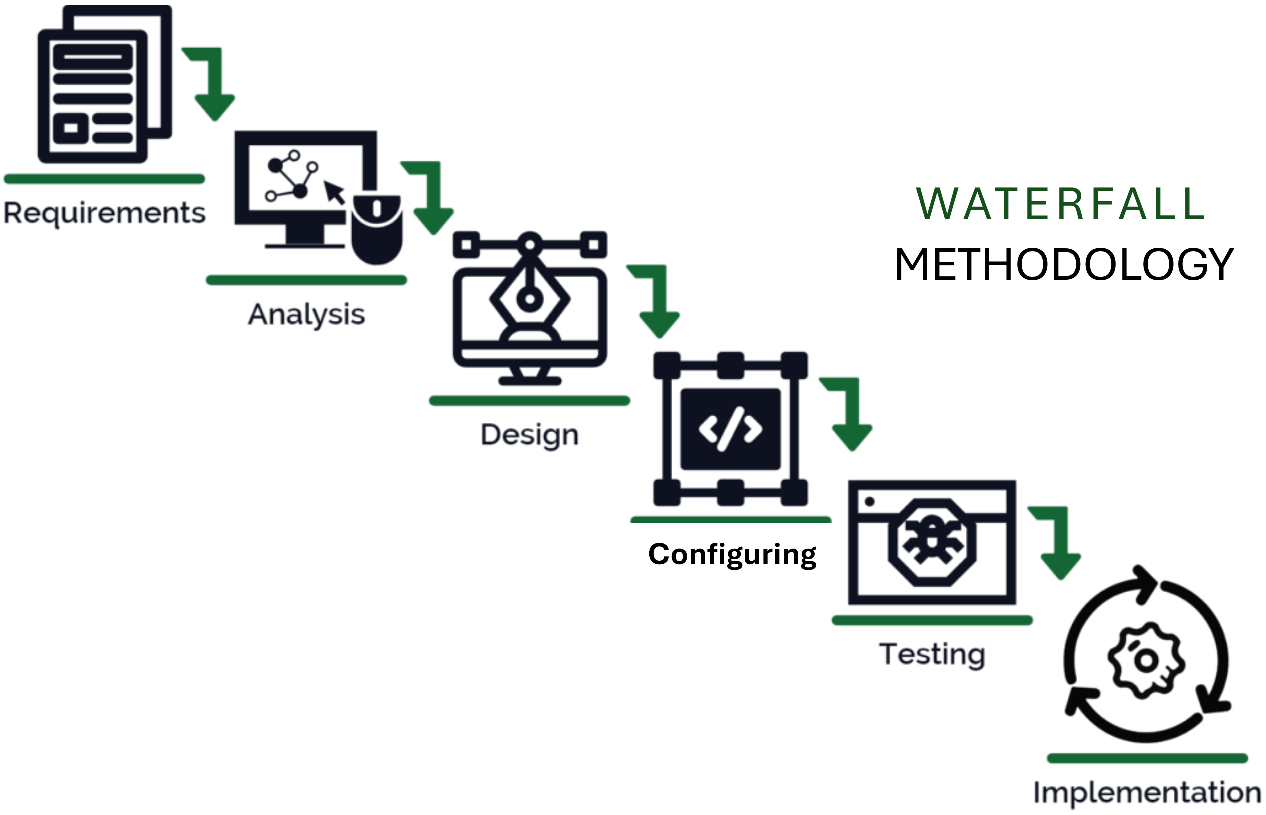
- **Phase 1 (Month 1-2)**: Infrastructure analysis and requirement gathering.
- **Phase 2 (Month 3-4)**: Network design and procurement.
- **Phase 3 (Month 5-8)**: Installation and configurations of Fiber Optic, 5G antennas, and Network devices.
- **Phase 4 (Month 9-10)**: Network integration and initial testing.
- **Phase 5 (Month 11)**: Security and performance optimization.
- **Phase 6 (Month 12)**: Final testing, training, and handover.

PROJECT COSTS

The estimated budget for this project is approximately R 47 million. This cost is broken down as follows:

- **Infrastructure Costs**: R 22.6 million for Fiber Optic cabling, 5G hardware, and network devices.
- **Labor Costs**: R 11.3 million for engineering, technical, and project management staff.
- **Software and Licenses**: R 5.7 million for required network management tools, security software, and IP licensing.
- **Training and Documentation**: R 1.9 million for staff training sessions and the development of comprehensive user guides.
- **Contingency Fund**: R 5.7 million reserved for unforeseen expenses and risk mitigation.

LIFE-CYCLE MODEL IMPLEMENTED



SYSTEM DESIGN

NETWORK ARCHITECTURE

The network is designed with a hierarchical model to ensure scalability, fault tolerance, and efficient data routing. It is divided into the following layers:

- **Core Layer:** High-capacity backbone interconnecting regional hubs.
- **Distribution Layer**: Intermediate layer connecting various sites within the network.
- **Access Layer:** The point where end-user devices connect, providing services to customers (e.g., DSL, fibre, Wi-Fi).

EQUIPMENT and TECHNOLOGIES USED OVERVIEW

The company has emphasized high performance, redundancy, scalability, and availability, and hence you are required to provide a complete OLesh Telco network infrastructure design and implementation. The company will be using the following IP address: 10.20.0.0/16 for WLAN, 192.168.10.0/24 for LAN, 172.16.10.0/24 for Voice, 10.10.10.0/28 for DMZ and 197.200.100.0 for public addresses.

Design Tool- Cisco Packet Tracer to design and implement the network solution.

Hierarchical Design- A hierarchical model providing redundancy at every layer.

ISPs- The network is connected to a Seacom ISP Router.

WLC- Each department has a WAP providing both employees and guest WIFI managed by WLC.

VoIP- Each department is equipped with IP phones.

VLAN- The LAN, WLAN, and VoIP VLANs remains at 50, 60 & 101 respectively for the entire network.

EtherChannel- Standard LACP as a method of link aggregation is implemented.

STP PortFast and BPDUguard- Configured the two protocols to enable faster port transition from blocking to forwarding.

Subnetting- Subnetting is carried out to allocate the correct number of IP addresses to each department

Inter-VLAN Routing- Devices in all the departments can communicate with each other with the Multilayer Switch configured with Inter-VLAN routing.

Core Switch- The Multilayer switches carry out both routing and switching functionalities and based on their IP addresses.

DHCP Server- All devices in the network (except IP phones) are assigned IP address dynamically from the AD servers located at the server farm site.

Cisco 2811 Router- The Cisco 2811 router can support telephony which is critical in this instance.

Static Addressing- Devices in the server room are allocated IP addresses statically.

Routing Protocol- OSPF has been implemented as the routing protocol to advertise routes both on the routers and multilayer switches.

Standard ACL for SSH- A simple standard ACL on the line VTY has been implemented to allow only the Senior Network Security Engineer to carry out all remote administrative tasks using SSH.

Cisco ASA Firewall- Security Levels, Zones, and Policies to define how resources are accessed in the network have been configured respectively.

TOPOLOGY

The network follows a star topology for the core network and a mesh topology for the regional interconnections. This design ensures optimal data flow and redundancy.

- **Star Topology**: All customer connections are routed through central hubs.
- **Mesh Topology:** Regional hubs are interconnected in a mesh to ensure there is no single point of failure.

BANDWIDTH and CAPACITY RUNNING

Core Network: 10Gbps links to handle high traffic volume.

Access Network: 1Gbps bandwidth per user for in each department in the company, with higher capacities available for enterprise customers.

IMPLEMENTATION

IMPLEMENTATION PHASES

- The project begins with the requirement analysis phase, where the primary focus was on understanding OLesh Telco’s needs for a secure and scalable network.
- After requirement analysis, we moved into the design phase. Here, we designed the network based on the infrastructure components and security needs, ensuring it would be secure, scalable, and efficient.
- The implementation phase involved configuring the physical network setup, VLANs, routing, and addressing. This stage followed the design phase and focused on translating the design into a functioning system.
- The testing phase confirmed that the design and implementation were functioning as expected. We carried out a series of validation checks to ensure all components were properly configured and secure.

CONFIGURATION DETAILS

- IP Addressing Scheme: The core network uses these private IP ranges and public IPs (10.20.0.0/16 for WLAN, 192.168.10.0/24 for LAN, 172.16.10.0/24 for Voice, 10.10.10.0/28 for DMZ and 197.200.100.0 for public addresses.)
- Routing Protocols: OSPF (Open Shortest Path First) is used for internal routing, while BGP (Border Gateway Protocol) is used for external connectivity to the internet.
- Security Configurations: Firewalls at the edge of the network, VPN tunnels for secure remote access, and intrusion detection systems (IDS) for traffic monitoring.

NETWORK SERVICES

- **Quality of Service (QoS)**: Configured to prioritize voice over data to ensure clear call quality.
- **Dynamic Host Configuration Protocol (DHCP**): For automatic IP address assignment in customer networks.
- **DNS and NTP Servers**: For name resolution and time synchronization across the network.

TESTING AND VALIDATION

NETWORKING PERFORMANCE TESTING

Bandwidth Test: Tools like iPerf were used to measure the throughput between different network segments.

Latency Test: Ping and traceroute commands were used to measure network latency.

Packet Loss Test: Simulated heavy traffic and tested for packet loss under high-load conditions.

FAULT TOLERANCE AND REDUNDANCY TESTS

- **Link Failover:** The redundancy built into the mesh topology was tested by shutting down primary links and ensuring traffic was rerouted through alternate paths.
- **Backup Power:** Uninterrupted power supply (UPS) systems and generators were tested for failover during power outages.

SECURITY TESTING

- **Penetration Testing**: Conducted to identify vulnerabilities within the network, such as open ports or misconfigured firewalls.
- **DDoS Attack Simulation**: A stress test was performed to simulate a Distributed Denial of Service (DDoS) attack to ensure the network could withstand such incidents

CHALLENGES AND SOLUTIONS

SECURITY VULNERABILITIES

Initial testing identified several security weaknesses, including open ports on some routers.

Solution: A comprehensive network audit was performed, firewalls were reconfigured, and additional layers of security (such as IDS) were implemented.

A firewall has been used to set security zones and filter traffic that moves in and out of the zones based on the configured inspection policies. We can now promise our customer that our infrastructure is secured, reliable, scalable, robust, and is paramount to safeguarding the Confidentiality, Integrity, and Availability of data and communication.

CONCLUSION

The telecommunications network was successfully designed, implemented, and tested. Key outcomes include:

- **Scalability:** The network is designed to handle increasing demand with minimal upgrades.
- **Reliability:** Redundancy and failover mechanisms ensure high availability.
- **Security:** Security measures such as firewalls, VPNs, and intrusion detection systems are in place to protect against external threats.

FUTURE EXPANSION

Planning for the future expansion of a telecommunications network requires a holistic approach, considering not only the growth in user demand but also the adoption of emerging technologies and the evolving regulatory landscape. Therefore, OLesh Telco plans on keeping up with the evolving technologies considering the safety of its customers information at the same time always ensuring maximum availability and reliability.

Technologies such as AI and Machine Learning for network optimization will be implemented in the near future to optimize network traffic and improve network security by detecting and responding to potential threats in real time.