Bahrain Polytechnic

Kalam Telecom Internet Service Provider Network Design Document

Version <1.0>
2026-02-14

Document Details

Approvals

The Supervisor and the Client shall approve this document.

Document Change Control

Initial Release:	
Current Release:	
Date of Last Review:	
Date of Next Review:	
Target Date for Next Update:	

Distribution List

This following list of people shall receive a copy of this document every time a new version of this document becomes available:

Customer :<Wakil Sarfaraz>

Team Members:

<Hasan Bahzad>

<Wakil Sarfaraz>

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description

TABLE OF CONTENTS

Introduction

This document outlines the detailed network design document for the proposed Kalam Telecom ISP MPLS backbone infrastructure. This project was developed to support the company’s expansion across Bahrain with the adoption of MPLS layer 3 VPN technology. The project focuses on building a scalable, reliable and redundant ISP backbone capable of providing high performance connectivity to more than one enterprise customers, as well as enabling seamless interconnectivity between Kalam Telecom MPLS network with other regional ISPs such as Batelco.

The main purpose of this document is to describe and discuss the design; architecture and the technical elements required to implement and deploy the upgraded backbone infrastructure. The document provides detailed explanations of the MPLS configuration, routing protocols, security practices and redundancy mechanisms that will become the foundation of Kalam Telecom enhanced network.

This design document is mainly intended to other network engineers, project managers, academic assessors and technical people which require a clear understanding of design decisions, methodologies and technologies used throughout the project development it also may assist any future engineers who need a reference on how to expand, maintain and integrate with the proposed backbone infrastructure project.

The main points in this document are organized into multiple sections to facilitate easy navigation:

- Introduction
- Context
- Location Floor Plan
- IP addressing schema
- Logical design
- Physical design
- Layer 2 features
- Layer 3 features
- Internet layer decision
- Presentation layer decision
- Security Services Layer Decisions
- Deployment diagram

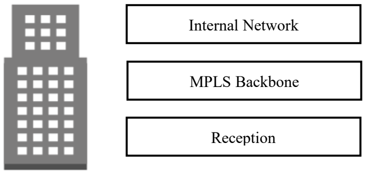
Network Design

This section focuses on the network infrastructure design and provides guidance on topologies as well as configurations; it is intended for the network architect who is designing the logical and physical network topology.

Context

The proposed solution will be deployed with Kalam Telecom existing network infrastructure. Kalam Telecom current network infrastructure consists of basic networking devices that provide ISP garde connectivity but lack the capacity of running and supporting VPN services across Bahrain. These limitations restrict Kalam Telecom ability to compete with other national ISP where enterprise customers increasingly demand high performance, secure and distributed network services. Kalam Telecom is focusing on modernizing its current backbone infrastructure by developing an MPLS enabled infrastructure capable of serving and supporting complex MPLS layer 3 VPN service. In addition, the up upgraded infrastructure aims to facilitate seamless interconnection with other regional ISPs MPLS network enabling Kalam Telecom to provide broader reachability for their services.

Location Floor Plans



Kalam Telecom network involves three primary site categories:

1. **ISP MPLS Backbone on the second floor**:
   The data center includes dedicated racks for all the MPLS backbone routers such as Provider Edge routers and Provider routers in addition, to redundant backup power feed up such as the Uninterrupted Power Supplies units and generators alongside with the main power source. This decision has been taken so in any natural causes such as water flooding the MPLS core network will still be functional and working flawlessly

2. **Internal ISP network and data center on the third floor**:
   The internal network of the ISP includes racks for Layer 3 switches, normal switches and enterprise grade router acting as the gateway for the internal users of the ISP network in addition to the multiple racks that are designed for the data center that are hosting the essential network services such as AAA, Syslog and NTP server.

Addressing Scheme

The IP addressing scheme of Kalam Telcom is carefully designed and divided into segments to support the ISP sections such as the MPLS backbone and the internal network, each department in Kalam Telecom internal network is assigned a specific range to ensure pure isolation and traffic control between the departments. The bellow table shows a summary of each section of the ISP with its IP address range:

Kalam Telecom IP Addresses Summary	
Internal Network	172.17.0.0/16
MPLS backbone	192.168.1.0/24
Public IP	74.211.4.0/27

The internal IP addressing of the internal network is carefully structured to make sure that each department has enough useable IP addresses to be assigned to end user's devices for any future expansion. The next tables outline each department IP ranges for the internal network of Kalam Telecom:

Kalam Telecom VLANs	
IT Department	172.17.10.0/24
Finance Department	172.17.20.0/24
HR Department	172.17.30.0/24
SWManagement VLAN	172.17.99.0/24
Infrastructure Devices	172.17.100.0/24

Kalam Telecom IP Address Shema				
Device	Interface	IP Address	Subnet Mask	Default Gateway
Kalam-PE1	E0/0 (Kalam-PE2)	192.168.1.1	255.255.255.252	N/A
	E0/1 (Kalam-PE3)	192.168.1.5	255.255.255.252	N/A
	S1/0 **(XYZ-1-CE)**	74.211.4.5	255.255.255.252	N/A
	S1/1 **(ABC-1-CE)**	74.211.4.1	255.255.255.252	N/A
	Lo0	1.1.1.1	255.255.255.255	N/A
	Lo1	11.11.11.1	255.255.255.255	N/A
Kalam-PE2	E0/0 (Kalam-PE1)	192.168.1.2	255.255.255.252	N/A
	E0/1 (Kalam-P2)	192.168.1.9	255.255.255.252	N/A
	E0/2 (Kalam-R1)	172.17.255.2	255.255.255.252	N/A
	S1/0 **(Batelco-PE1)**	74.211.4.9	255.255.255.252	N/A
	S1/1 (XYZ-1-CE)	74.211.4.13	255.255.255.252	N/A
	Lo0	1.1.1.2	255.255.255.255	N/A
	Lo1	11.11.11.2	255.255.255.255	N/A
Kalam-PE3	E0/0 (Kalam-P1)	192.168.1.13	255.255.255.252	N/A
	E0/1 (Kalam-PE1)	192.168.1.6	255.255.255.252	N/A
	E0/2 (Kalam-R1)	172.17.255.6	255.255.255.252	N/A
	S1/0 **(ABC-1-CE)**	74.211.4.17	255.255.255.252	N/A
	Lo0	1.1.1.3	255.255.255.255	N/A
	Lo1	11.11.11.3	255.255.255.255	N/A
Kalam-PE4	E0/0 (Kalam-PE6)	192.168.1.38	255.255.255.252	N/A
	E0/1 (Kalam-PE5)	192.168.1.33	255.255.255.252	N/A
	S1/0 (XYZ-2-CE)	74.211.4.21	255.255.255.252	N/A
	S1/1 **(ABC-2-CE)**	74.211.4.25	255.255.255.252	N/A
	Lo0	1.1.1.4	255.255.255.255	N/A

	Lo1	11.11.11.4	255.255.255.255	N/A
Kalam-PE5	E0/0 (Kalam-P3)	192.168.1.30	255.255.255.252	N/A
	E0/1 (Kalam-PE4)	192.168.1.34	255.255.255.252	N/A
	E0/2 (Kalam-R2)	172.17.255.14	255.255.255.252	N/A
	S1/0 **(ABC-2-CE)**	74.211.4.29	255.255.255.252	N/A
	Lo0	1.1.1.5	255.255.255.255	N/A
	Lo1	11.11.11.5	255.255.255.255	N/A
Kalam-PE6	E0/0 (Kalam-PE4)	192.168.1.37	255.255.255.252	N/A
	E0/1 (Kalam-P4)	192.168.1.26	255.255.255.252	N/A
	E0/2 (Kalam-R2)	172.17.255.10	255.255.255.252	N/A
	S1/1 (XYZ-2-CE)	74.211.4.33	255.255.255.252	N/A
	Lo0	1.1.1.6	255.255.255.255	N/A
	Lo1	11.11.11.6	255.255.255.255	N/A
Kalam-P1	E0/0 (Kalam-PE3)	192.168.1.14	255.255.255.252	N/A
	E0/1 (Kalam-P3)	192.168.1.21	255.255.255.252	N/A
	Lo0	1.1.2.1	255.255.255.255	N/A
Kalam-P2	E0/0 (Kalam-P4)	192.168.1.17	255.255.255.252	N/A
	E0/1 (Kalam-PE2)	192.168.1.10	255.255.255.252	N/A
	Lo0	1.1.2.2	255.255.255.255	N/A
Kalam-P3	E0/0 (Kalam-PE5)	192.168.1.29	255.255.255.252	N/A
	E0/1 (Kalam-P1)	192.168.1.22	255.255.255.252	N/A
	Lo0	1.1.2.3	255.255.255.255	N/A
Kalam-P4	E0/0 (Kalam-P2)	192.168.1.18	255.255.255.252	N/A
	E0/1 (Kalam-PE6)	192.168.1.25	255.255.255.252	N/A
	Lo0	1.1.2.4	255.255.255.255	N/A
Kalam-R1	E0/0 (Kalam-PE2)	172.17.255.1	255.255.255.252	N/A
	E0/1 (KKalam-PE3)	172.17.255.5	255.255.255.252	N/A
	E0/2.10	172.17.10.1	255.255.255.0	N/A
	E0/2.20	172.17.20.1	255.255.255.0	N/A
	E0/2.99	172.17.99.1	255.255.255.0	N/A
	E0/2.100	172.17.100.1	255.255.255.0	N/A
	E0/3 (Kalam-R2)	172.17.255.18	255.255.255.252	N/A
	Lo0	1.1.3.1	255.255.255.255	N/A
Kalam-R2	E0/0 (Kalam-PE6)	172.17.255.9	255.255.255.252	N/A
	E0/1 (Kalam-PE5)	172.17.255.13	255.255.255.252	N/A
	E0/2.10	172.17.10.2	255.255.255.0	N/A
	E0/2.20	172.17.20.2	255.255.255.0	N/A
	E0/2.99	172.17.99.2	255.255.255.0	N/A
	E0/2.100	172.17.100.2	255.255.255.0	N/A
	E0/3 (Kalam-R1)	172.17.255.17	255.255.255.252	N/A
	Lo0	1.1.3.2	255.255.255.255	N/A
Kalam-SW1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.100
Kalam-SW2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.100
Kalam-SW3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.100
IT-Desktop	E0	172.17.10.10	255.255.255.0	172.17.10.100
Finance-	E0	172.17.20.10	255.255.255.0	172.17.20.100

Desktop				
AAA-Syslog Server	E0	172.17.100.10	255.255.255.0	172.17.100.100

Batelco IP Address Schema				
Device	Interface	IP Address	Subnet Mask	Default Gateway
Batelco-PE1	E0/0 (Batelco-PE2)	54.40.61.1	255.255.255.252	N/A
	E0/1 (Batelco-PE3)	54.40.61.5	255.255.255.252	N/A
	S1/0 **(Kalam-PE1)**	74.211.4.10	255.255.255.252	N/A
	Lo0	2.2.2.1	255.255.255.255	N/A
Batelco-PE2	E0/0 (Batelco-PE1)	54.40.61.2	255.255.255.252	N/A
	E0/1 (Batelco-PE4)	54.40.61.9	255.255.255.252	N/A
	Lo0	2.2.2.2	255.255.255.255	N/A
Batelco-PE3	E0/0 (Batelco-PE4)	54.40.61.13	255.255.255.252	N/A
	E0/1 (Batelco-PE1)	54.40.61.6	255.255.255.252	N/A
	Lo0	2.2.2.3	255.255.255.255	N/A
Batelco-PE4	E0/0 (Batelco-PE3)	54.40.61.14	255.255.255.252	N/A
	E0/1 (Batelco-PE2)	54.40.61.10	255.255.255.252	N/A
	S1/0 **(XYZ-3-CE)**	54.40.61.17	255.255.255.252	N/A
	Lo0	2.2.2.4	255.255.255.255	N/A

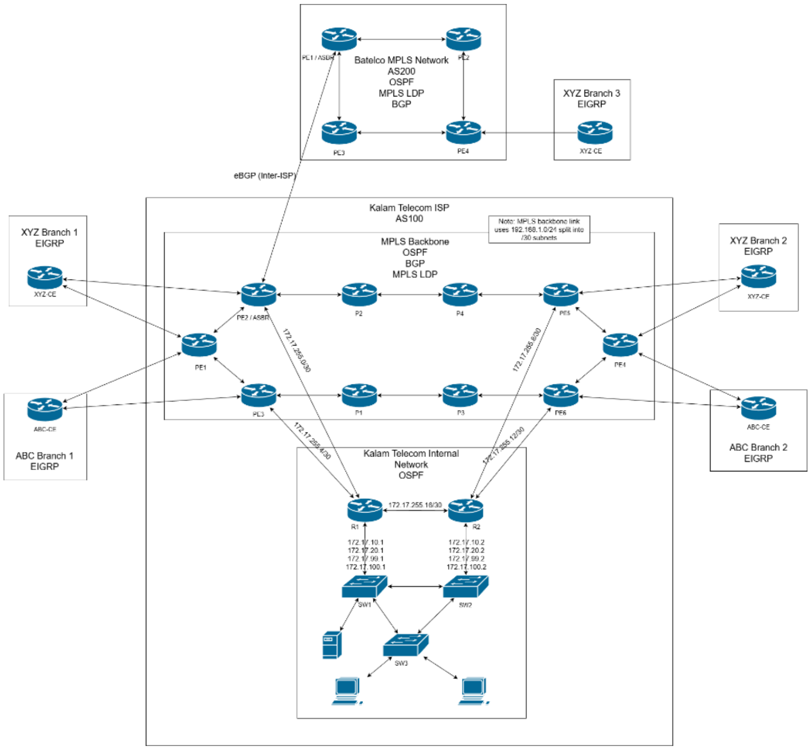
ABC Company Branch 1 (172.20.0.0/16)				
Device	Interface	IP Address	Subnet Mask	Default Gateway
ABC-1-CE	S1/0 **(Kalam-PE3)**	74.211.4.18	255.255.255.252	N/A
	S1/1 **(Kalam-PE1)**	74.211.4.2	255.255.255.252	N/A
	E0/0.10	172.20.10.1	255.255.255.0	N/A
	E0/0.20	172.20.20.1	255.255.255.0	N/A
	E0/0.99	172.20.99.1	255.255.255.0	N/A
	Lo0	10.10.10.10	255.255.255.255	N/A
ABC Company Branch 2 (172.21.0.0/16)				
Device	Interface	IP Address	Subnet Mask	Default Gateway
ABC-2-CE	S1/0 **(Kalam -PE5)**	74.211.4.30	255.255.255.252	N/A
	S1/1 **(Kalam -PE4)**	74.211.4.26	255.255.255.252	N/A
	E0/0.10	172.21.10.1	255.255.255.0	N/A
	E0/0.20	172.21.20.1	255.255.255.0	N/A
	E0/0.99	172.21.99.1	255.255.255.0	N/A
	Lo0	20.20.20.20	255.255.255.255	N/A

XYZ Company Branch 1 (172.23.0.0/16)				
Device	Interface	IP Address	Subnet Mask	Default Gateway
XYZ-1-CE	S1/0 **(Kalam-PE1)**	74.211.4.6	255.255.255.252	N/A
	S1/1 **(Kalam-PE2)**	74.211.4.14	255.255.255.252	N/A
	E0/0.10	172.23.10.1	255.255.255.0	N/A

	E0/0.20	172.23.20.1	255.255.255.0	N/A
	E0/0.99	172.23.99.1	255.255.255.0	N/A
	Lo0	110.110.110	255.255.255.255	N/A
XYZ Company Branch 2 (172.24.0.0/16)				
Device	Interface	IP Address	Subnet Mask	Default Gateway
XYZ-2-CE	S1/0 **(Kalam-PE4)**	74.211.4.22	255.255.255.252	N/A
	S1/1 **(Kalam-PE6)**	74.211.4.34	255.255.255.252	N/A
	E0/0.10	172.24.10.1	255.255.255.0	N/A
	E0/0.20	172.24.20.1	255.255.255.0	N/A
	E0/0.99	172.24.99.1	255.255.255.0	N/A
	Lo0	120.120.120.120	255.255.255.255	N/A
XYZ Company Branch 3				
Device	Interface	IP Address	Subnet Mask	Default Gateway
XYZ-3-CE	S1/0 (Batelco-PE4)	54.40.61.18	255.255.255.252	N/A
	E0/0.10	172.25.10.1	255.255.255.0	N/A
	E0/0.20	172.25.20.1	255.255.255.0	N/A
	E0/0.99	172.25.30.1	255.255.255.0	N/A
	Lo0	130.130.130.130	255.255.255.255	N/A

Network Topologies (Logical Design)

The logical design of the proposed MPLS backbone infrastructure for Kalam Telecom network adopts a very strict and hierarchical architecture design that aims to integrate the MPLS network with the already existing internal network of the ISP. This merged approach ensures that the VPN service is delivered to the customer, structured routing behaviour between the section of the infrastructure and reliable communication between the three-layer core, distribution and access layers.



The network uses a hierarchical design, and it is divided into two logical domains:

1- ***MPLS Backbone**: serving external enterprises customers and inter-AS connectivity between national ISPs*
2- ***The internal network of Kalam Telecom**: supporting Kalam Telecom internal operational users and systems*

MPLS Backbone logical design:
Backbone forms the provider network that is responsible for forwarding label traffic between the PE routers, enabling VPN separation for customers. The MPLS backbone consists of 3 main routers:

- Provider (P) Router
- Provider Edge (PE) Router
- Autonomous System Border Router (ASBR)

Provider Router:
This router is the core of the MPLS VPN network since it is responsible for providing a high speed transmit links between the PE routers. Below are the roles and features of the P router:

- Maintain Internal gateway protocol mainly OSPF for core connectivity
- Does not hold VRF or customer prefixes.
- Forward labels between the PE routers
- Provide fast backbone switching capabilities for customer traffic

Provider Edge Router:

PE router interacts directly with the CE routers and handles the logic behind the VPN service. The below text outlines the features and responsibilities of the PE router:

- Connects to the Customer Edge Routers
- Participate in MP-BGP between PE routers to exchange VPNv4 routes
- Holds the customer VRFs

Autonomous System Border Router:
The ASBR routers marks the boundary between Kalam Telecom infrastructure and the external ISPs. The roles and responsibilities of the ASBR are as follows:

- Establish eBGP peering sessions with other for inter-AS routing
- Exchange labelled VPNv4 routes using the MPLS VPN inter-AS Option B
- Extend the customer reachability across other regional MPLS networks

Internal network logical design:
The internal network supports Kalam Telcom corporate operation, network engineers and the management system. The internal network follows a client-server model with a segmentation that considered to be logical. The main components of the internal network are:

- Enterprise routers
- Layer 2 switches
- Departments PCs
- Servers

Enterprise routers:
These routers act at the distribution layer at the Kalam Telecom whole infrastructure, and they connect the internal networks with the infrastructure core. The following points are the enterprised routers roles and functionality:

- Provide connectivity between the internal departments and the infrastructure core
- Provide inter-VLAN routing for the internal departments
- Acts as the default gateway for the internal departments
- Use redundancy protocol such as HSRP for high availability
- Applying routing policies and Access control list

Layer 2 switches:
Layer 2 switches on the Kalam Telecom infrastructure act as the access layer for the PCs and server. Roles and responsibilities of these switches are:

- Provides logical and physical access to the PCs and servers
- Support VLAN segmentation for departments
- Extend the connectivity to wired users and local services devices

Server:
The internal servers host critical services that are essential for the Kalam Telecom daily operations. The point below outlines which services are hosted on the internal server:

- AAA provides centralized authentication, access and accounting control
- Syslog provides a central place to log all changes in the infrastructure devices

Reference Model:
The logical design maps closely to the OSI layer model:

Physical and media structure – layer 1:

- Fiber optic cables are used for the MPLS core and inter-AS ISP links
- Copper ethernet cabling for the internal segment of the infrastructure

Segmentation and switching – layer 2:

- VLAN based segmentation of internal departments and services
- Redundant path for the layer 2 to the gateway
- CE and PE handoff for customer segmentation

Routing protocols and MPLS services – layer 3:

- OSPF and EIGRP is used for internal and customer CE-PE routing
- MP-BGP for VPNv4 label distribution within the backbone
- LDP for label distribution and forwarding in MPLS
- VRF for isolate the customer traffic

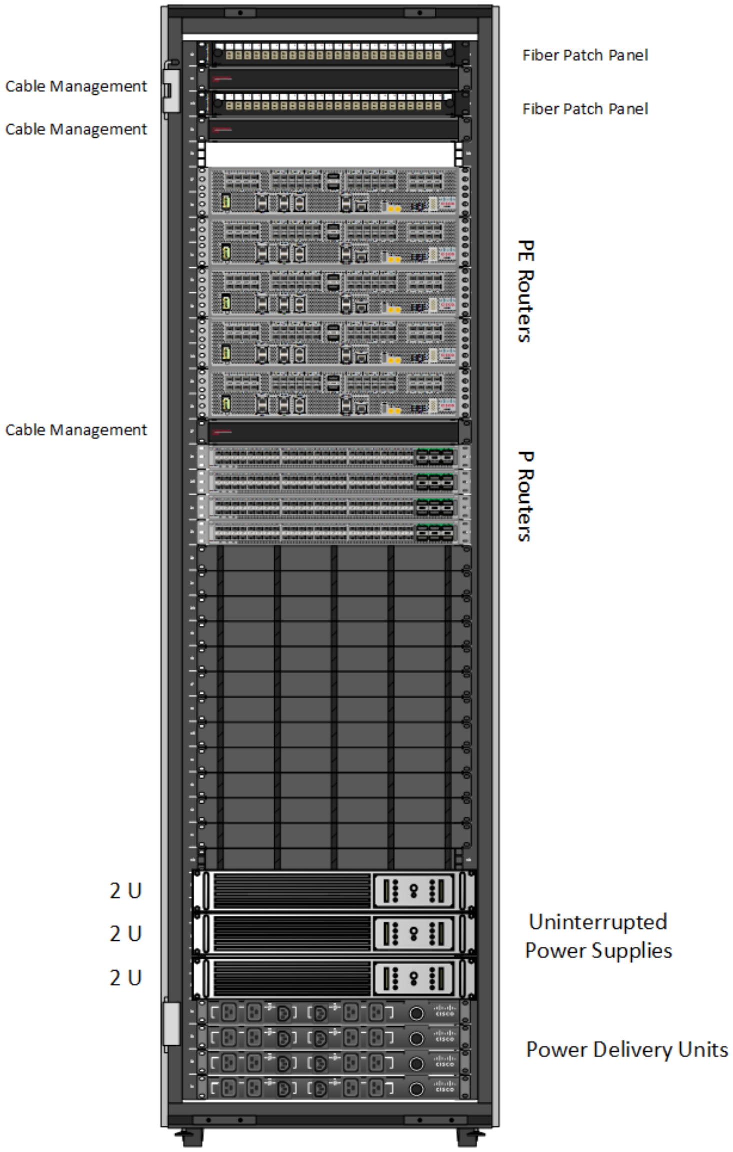
Physical Design

This section will outline the rack design of both MPLS backbone and internal network for Kalam Telecom and how the devices are organized for each network rack

***MPLS Backbone**:*

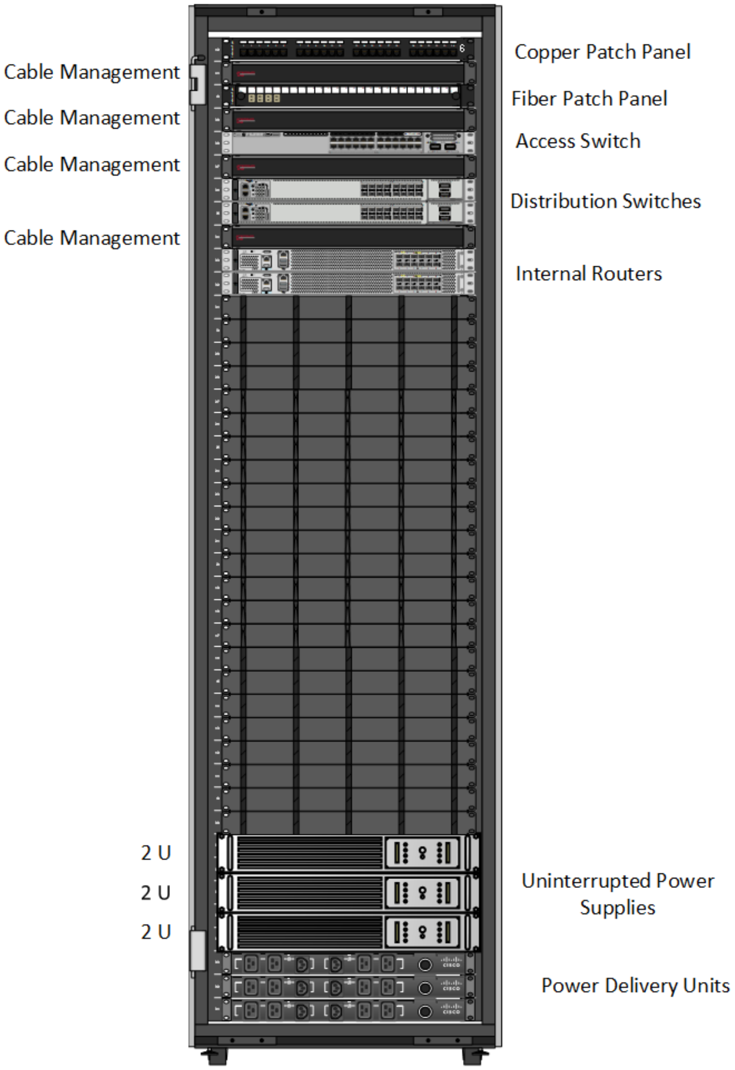
As we can see the MPLS backbone uses a single 42U rack to houses the required equipment to make the MPLS backbone up and running. Starting from the top we have the first Fiber patch panel to connects this rack with the other network devices of the ISP followed up a cable management unit. A second Fiber optic patch panel is placed directly below to act as a redundant link to the other network devices of the ISP. Under the second Fiber patch panel is a small spacer to improve the airflow and cooling.

Next at the middle section, the 6 PE routers mounted on top of each other with an additional cable management panel placed under them followed up by the 4 P routers to complete the functionality of the MPLS backbone. Finally, at the bottom of the rack the uninterrupted power supplies alongside the power delivery units are mounted.



***Internal network**:*
The internal network used a single 42U that have all the required and necessary networking equipment to make the internal network running 24/7 without any problems. Starting from the very top of the rack we have a cat6 patch panel that connects directly to each department switch followed up by a cable management unit to organize the cables. A Fiber optic patch panel is placed directly below to connects the internal router to the main ISP routers under the Fiber optic patch panel these is a second cable management unit.

Next at middle part of the rack we have the Access switch with a cable management unit directly below it then followed by the two distribution switches and internal router with a cable management unit between them. Finally, the bottom of the rack we have a 3 uninterrupted power supplies with 3 power delivery units.



Layer 2 Design and Features

The following section defines how the access layers of Kalam Telecom internal network interact ensuring to provides reliable, stable and strong connectivity, efficient switching operations and logical segmentation of the internal network. The design includes separation using VLAN, trunk interfaces standards, link redundancy, loop prevention and essential layer 2 security features and mechanisms to ensure predictable and safe traffic flow across the whole enterprise environments.

Department and VLAN assignment*:*
Each department will have a dedicated VLAN to separate and isolate the broadcast domains and to enhance the security of the infrastructure. Below is the department allocation:

- *IT Department → VLAN 10*
- *Finance Department → VLAN 20*
- *HR Department → VLAN 30*
- *SWManagement → VLAN 99*
- *Infrastructure Devices → VLAN 100*

Port Type*:*

To support and enhanced VLAN distribution across all the switches within the internal network, the design utilizes a mixture of trunk and access ports:

802.1Q trunk port
This port mode is used for inter-switch and router-to-switch links to carry multiple VLANs tags across the link. Trunk ensures that all relevant VLANs are pushed across the entire switch network inside the infrastructure.

Access port
This port mode is configured on specific interfaces, interfaces that are connected to any end-user device, local equipment or servers. Each port is configured to be assigned to a single VLAN which are corresponding to the department the device belongs to.

***Loop prevention using Spanning Tree Protocol**:*
To prevent layer 2 loops and ensure that the layer 2 devices provide excellent convergence, the spanning tree protocol is used on all switches in the internal network.

- *Core switches are configured with lower priority to ensure it is elected as the root bridge*
- *VLANs will be distributed on both core switches so it can STP load balancing*
- *Access layer switches configured with high priority to make sure they are not elected as the root bridge*

***Layer 2 redundant features**:*
To maintain an uninterrupted connection:

- *Redundant links from the access switch to both the distribution switches and core switches which are already implemented*
- *Portfast is enabled on the edge facing interfaces to ensure that these ports are always ready to provide access to the intendent host device*

***Virtual Trunking Protocol**:*
VTP is used to manage and simplifies the VLAN distribution from a central location to reduce administrative overhead:

- *A designated switch which will operates as a VTP server, maintaining the VLAN database*
- *All other switches will operate as a VTP client to automatically learning VLANs and their changes*
- *VTP ensures consistent VLAN configuration across the entire Layer 2 domain*

Layer 3 Design and Features

This section describes the routing structure, IP topology and service interaction across both part of Kalam Telecom network the MPLS backbone and Kalam Telecom internal network. This layer ensures VPN separation, end-to-end reachability and controlled service insertion between the MPLS core and internal network devices. This design combines a mix of interior gateway protocols, MPLS routing, NAT, VRF and inter-AS mechanisms to support both internal ISP operations and customer connectivity.

***MPLS backbone routing design**:*
The MPLS backbone considered to be the service provider core routing domain, and it is the responsible for forwarding all customer traffic, maintaining customer VPN separation and distributing labels. Routing protocols are designed with clear distinction between the internal gateway protocol functions, MPLS functions and BGP distribution. Below is each routing protocol used in the MPLS backbone:

- *OSPF (Process 1) is deployed specifically on the provider MPLS core to ensure reachability between the PE and P routers*
- *The primary reason for deploying the OSPF (Process 1) is to advertise routers loopbacks for the MP-BGP sessions and maintain stable internal convergence*
- *MP-BGP VPNv4 is used only on the PE routers to exchange customer VPN prefixes across the entire MPLS network of Kalam Telecom*

- *Label distribution protocol provides label bindings between the PE and P routers which leads to a enabling end-to-end label switched forwarding*

***VRF definition and route targets**:*
VRF ensures complete customer network isolation within the MPLS network, VRF instances are defined and deployed for each customer on the PE routers. VRF components are as follows:

- *A Route-Distinguisher to keep the customer route unique across all the MPLS backbone*
- *A Route-Target controls the importing and exporting routing policies within PE routers which can enable site-to-site communication, multiple sites VPN relationship or traffic isolation between customers*

***CE-PE routing**:*
The relationship between both the CE-PE routers defines how the customer routes enter Kalam Telecom MPLS cloud. CE-PE routing methods are below:

- *EIGRP is selected in the CE-PE routing protocol.*
- *The CE routers advertise the branches prefixes to the PE routers so the PE can inject the customer routes into the VRF*
- *The return routes from the other side are transmitted via MP-BGP over the MPLS network, allowing inter branch communication.*

***Internal Network**:*
The internal enterprised network of Kalm Telecom uses a different layer 3 design (OSPF Process 2) from the MPLS backbone. The internal network supports the corporate services, operational devices and management systems.
Internal network IGP (OSPF process 2) functions:

- *Runs between the internal network and the ISP PE router*
- *This design keeps the internal routing domain isolated from the Core network of the ISP*
- *Internal users reach the public internet through the NAT implemented ad the PE router, to ensure that the private IP addresses are hidden from the global routing tables*

***ASBR and Inter-AS MPLS**:*
ASBR routers allows Kalam Telecom to extend their services broader outside the boundaries of Kalam Telecom, ASBR handles the interconnection with other regional ISP. Inter-AS MPLS operation explained below:

- *MPLS VPNv4 routes are exchanged between ASes using inter-AS Option B, enable VPN label route transfer via MP-BGP*
- *The standard global IPv4 routes are exchanged via eBGP sessions*
- *This model maintains VPN separation while expanding the customer reachability across multiple service providers*

Internet/Virtual Layer Decisions

This section defines how both normal internet connectivity and MPLS-delivered internet access are provided within the ISP environment. This layer address two distinct but related aspects on how the ISP itself obtaining and managing its internet connectivity and how customer receives the internet through the ISP MPLS VPN service. These two processes operate in parallel and its needs the ISP needs to manage its own presence on the global internet while also acting as an internet provider for its own MPLS VPN customers.

***ISP internet design**:*
ISP maintains its own dedicated connection with the global internet independently from the MPLS core. For the ISP to achieve this, the ISP connects to more than one upstream internet providers through dedicated internet edge router placed in the main data center. There internet edge router serves a specific purpose which is acting as the ISP official presence on the global worldwide internet in addition to handling all the external routing and

communication with the broader internet. The connection between Kalam Telecom and the upstream ISP uses a high-capacity Fiber to ensure suitable bandwidth and resiliency.

This internet connection does not used only to provides internet service to customers but its also for the ISPs internal departments and systems. Public facing servers such as public DNS servers rely on this upstream internet connectivity also the ISP maintains a private DNS services for the infrastructure management systems such as AAA and Syslog servers. Thus, the ISP's Internet design ensures reliable global connectivity, supports public services, and integrates with the internal management systems that maintain and monitor both the MPLS and customer networks.

***Customer internet design**:*
Customers are connected through the ISP MPLS VPN network do not receive an internet directly from the global internet instead they are relying on the ISP centralized network. Each customer sites connect to the ISP through the Customer Edge Router (CE), which is forwarding the customer traffic into the MPLS cloud through the Provider Edge Router (PE) after that the traffic travels across the MPLS backbone inside the dedicated VRF ensuring separation of the packets from other customers network and maintaining secure and private transportation. When the customer devices send a packet destined for the public network this packet will travel from the CE router to the PE router and then across the MPLS cire until it's reached the ISP edge router at this point the MPLS encapsulation is removed, and the traffic is routed through the global internet via the ISP upstream providers either by the ISP assigning a dedicated public IP to its customer or performs Network Address Translation on behalf of the customer who uses private IP addressing.

Presentation Layer

This project does not focus on the presentation layer, as the main core of this project is to design and deployment of Kalm Telecom MPLS VPN services and integrate its MPLS network with other ISPs networks. While end-user application, interfaces and associated protocols typically fail under this layer, they are outside the scope of the project. The focus of this project remains on establishing a robust MPLS VPN, integrating MPLS networks, deploying AAA and Syslog systems and ensuring secure and reliable connectivity across the service provider and customer environments.

Security Services Layer Decisions

This section outlines the security mechanisms and protocols used across the ISP network infrastructure. The security layer main objective is to restrict unauthorized traffic from accessing the network, controlling the administrative access and protect the MPLS backbone devices alongside the internal department from any misuse or malicious activity. The following measures has been applied on all the ISP networking devices:

- *AAA Server*
- *Access Control List*
- *Port Security*

***AAA Server**:*
AAA Server stands for Authentication, Authorization and Accounting Server is implemented to filter and secure administrative access to the critical networking devices in the infrastructure including the P router, PE router, ASBRs and even the internal routers of the departments. Objectives of the AAA Server:

- *Only authorized personnel can log into the network equipment command line interface*
- *Create different privileges levels for the administrators and IT staff*
- *Provides a centralized authentication using radius alongside with a local AAA as backup*
- *Providing accountability by logging any administrative actions*

***Access Control List**:*

ACL is applied throughout all the network to control the traffic in multiple points and layers. These ACLs are designed to protect the internal network and MPLS backbone and internal communication within each department.

***Infrastructure ACLs**:*
These ACLs are designed to protect the control plane of the MPLS backbone routers by blocking any traffic destined to

- *MPLS backbone router loopback interfaces*
- *Management interfaces such as SSH*

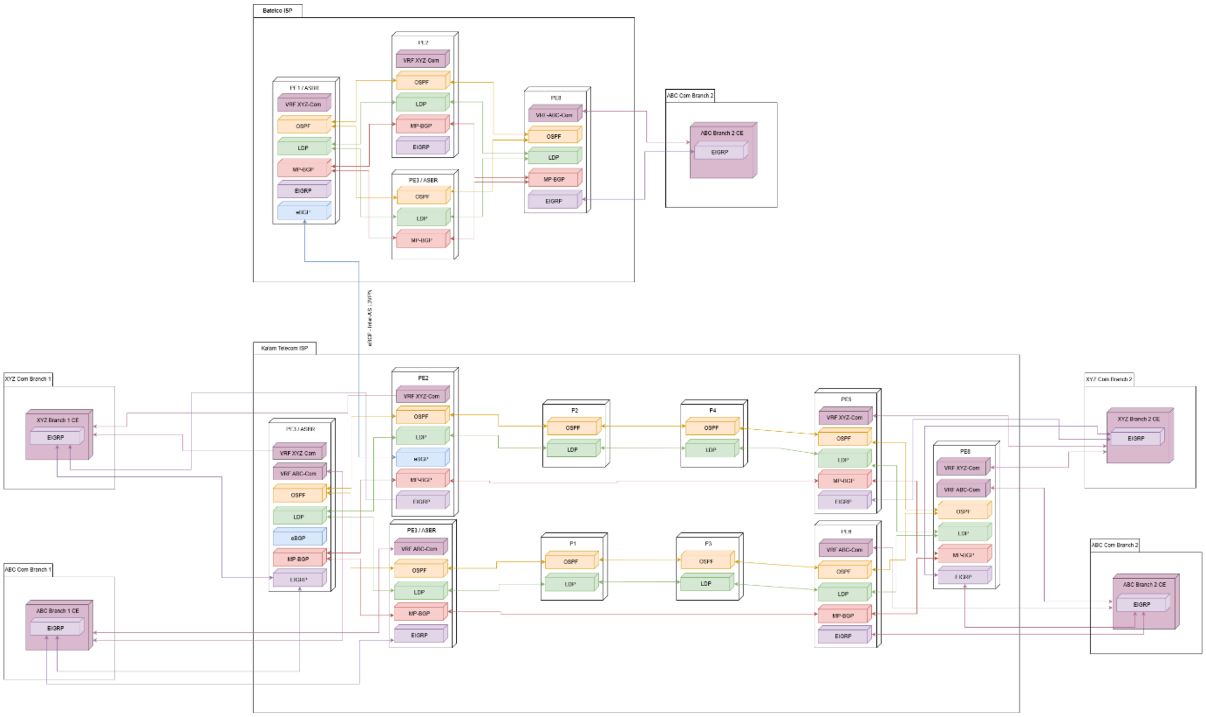
***Inter-VLANs ACLs**:*
These ACLs provide security between the internal departments and between the internal network and the edge routers:

- *Limit the communication between the departments*
- *Control which service is allowed to be reachable by the end user*
- *Restricted any unnecessary inbound or outbound traffic*

***Port Security**:*
Port security is implemented specifically on access switches to block unauthorized end-devices from access or joining the network. The port security mainly is applied on the ports that are connected to PCs, printers and other end user equipment.

- *Limiting the MAC addresses on each port that connects to any department PC to a maximum of one MAC address*
- *Prevent any rouge/unauthorized switches from connecting*
- *If any security measures have been violated the switch will trigger the security action with either restrict or shutdown*

Deployment Diagram


Batelco ISP
PE1 / ASBR
VRF XYZ-Com
OSPF
LDP
MP-BGP
EIGRP
eBGP
PE2
VRF XYZ-Com
OSPF
LDP
MP-BGP
EIGRP
PE3 / ASBR
OSPF
LDP
MP-BGP
PE8
VRF-ABC-Com
OSPF
LDP
MP-BGP
EIGRP
ABC Com Branch 2
ABC Branch 2 CE
EIGRP
eBGP - Inter-AS L3VPN
Kalam Telecom ISP
XYZ Com Branch 1
XYZ Branch 1 CE
EIGRP
ABC Com Branch 1
ABC Branch 1 CE
EIGRP
PE3 / ASBR
VRF XYZ-Com
VRF ABC-Com
OSPF
LDP
eBGP
MP-BGP
EIGRP
PE2
VRF XYZ-Com
OSPF
LDP
eBGP
MP-BGP
EIGRP
PE3 / ASBR
VRF ABC-Com
OSPF
LDP
MP-BGP
EIGRP
P2
OSPF
LDP
P4
OSPF
LDP
P1
OSPF
LDP
P3
OSPF
LDP
PE5
VRF XYZ-Com
OSPF
LDP
MP-BGP
EIGRP
PE6
VRF ABC-Com
OSPF
LDP
MP-BGP
EIGRP
PE8
VRF XYZ-Com
VRF ABC-Com
OSPF
LDP
MP-BGP
EIGRP
XYZ Com Branch 2
XYZ Branch 2 CE
EIGRP
ABC Com Branch 2
ABC Branch 2 CE
EIGRP