BAHRAIN POLYTECHNIC بوليتكنك البحرين

Assessment Cover Sheet

Assessment Title	Thesis Document		
Assessment Type	Uncontrolled	Individual	Not must-pass
Due Date	28th December 2025	**Course Code**	IT7099
Course Title	IT Project		
Internal Moderator's			
External Examiner's			

Instructions:

1. This cover sheet must be completed (section in red below) and attached to your assessment before submission in hard copy/soft copy.
2. The time allowed for this assessment is 8 weeks
3. This assessment carries 30 marks assessing CILO 1, CILO 2 and CILO 4.
4. The materials allowed for use in this assessment are Thesis (Design + Technical) document.
5. The use of generative AI tools is strictly prohibited.
6. References consulted (if any) must be properly acknowledged and cited.
7. The assessment has a total of XXX pages.

Learner ID	202001980	**Date Submitted**	28/12/2025
Learner Name	Hasan Bahzad		
Programme Code	IT8030		
Programme Title	Networking		
Lecturer's Name	Hussain ALZain – PM, Wakil Sarfaraz – Supervisor		

By submitting this assessment for marking, I affirm that this assessment is my own work.

Learner Signature	Hasan Bahzad

Do not write beyond this line. For assessor use

Assessor's Name			
Marking Date		**Maks**	

Comments:

Kalam Telecom Internet Service Provider – MPLS Networking Topology

By

202001980 Hasan Bahzad

A Thesis Submitted in

(Partial) fulfillment of the

Requirements of the Degree of

Bachelor of information and communication

Technology Networking

At

Bahrain Polytechnic

December 2025

Title

Using MPLS to Develop a Network Infrastructure for Kalam Telecom Internet Service Provider

Copyright

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature: Hasan Bahzad **Name: Hasan Bahzad** **Date: 28th December 2025**

Approval Signatures

APPROVED FOR THE ICT PROGRAMME

_____

(thesis supervisor), Thesis Supervisor Date

_____

(writing tutor), Technical Writing Tutor Date

Abstract

As the enterprise companies aiming towards expanding their presence in Bahrain by opening multiple branches, the needs of inter communication between these branches is a must for ease of and secure communication. Kalam Telecom is a major Internet service provider which is facing a lot of challenges when it comes to their network reliability, performance, redundant and scalable network. These issues make the internet service provider fall behind other ISP competitors in Bahrain. The purpose of this project is to design a network infrastructure for Kalam Telecom that will be capable of providing network reliability, high performance and redundant connections to their enterprise customers in addition to providing some additional service that allows multiple branches to inter communicate securely using private dedicated links.

The methodology starts with identifying the current issues and challenges of the existing network infrastructure of Kalam Telecom and defining the specific needs of the current state of the market to improve the infrastructure and customer expectations. Based on these output, the new infrastructure design will be built to provide the customers and Kalam Telecom with an organized, redundant, secure, reliable and excellent performance network.

Acknowledgements

I would first like to express my sincere gratitude to my supervisor, Mr. Wakil Sarfaraz, whose expert guidance, detailed feedback, and continuous support were invaluable throughout every major phase of this project. His dedication and availability played a crucial role in ensuring the successful completion of this work.

Second, I extend my appreciation to my Project Management tutor, Dr. Hussain ALZain for his promise to deliver the course material and for providing mentorship. His regular follow-ups, useful advice helped keep this project aligned with academic expectations and enabled me to plan and execute each task effectively.

Third, I would like to express my gratitude to Dr. Mohammed Elkenzi for his significant support and insightful feedback. His contributions greatly improved the quality and clarity of this project.

Finally, it needs to be acknowledged that I am grateful to my parents and family for their continuous support during the most challenging time. The continuous motivational boosts alongside the support during this moment was very beneficial during the course journey.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviations	Definition
CE Router	Customer Edge Router
PE Router	Provider Edge Router
P Router	Provider Router
AAA	Authentication, Authorization and Accounting
Syslog	System Logging Protocol
HSRP	Host Standby Router Protocol
VTP	VLAN Trunking Protocol
VLAN	Virtual Local Area Network
STP	Spanning Tree Protocol
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
LDP	Label Distribution Protocol
IGP	Internal Gateway Protocol
OSPF	Open Shortest Path First
EIGRP	Enhanced Interior Gateway Routing Protocol
BGP	Border Gateway Protocol
MP-BGP	Multi Protocol Border Gateway Protocol
ACL	Access Control List
AS	Autonomous System
NAT	Network Address Translation
VRF	Virtual Routing and Forwarding
QoS	Quality of Service
ISP	Internet Service Provider
LSP	Label Switched Path
TE	Traffic Engineering
VoIP	Voice Over Internet Protocol
RFC	Request For Comments
AD	Administrative Distance
LSA	Link State Advertisement
LSR	Link State Request
LSU	Link State Update
LSAck	Link State Acknowledgement
LSDB	Link State Database
AF	Address Family
ASA	Adaptive Security Appliance

Table 1 - Abbreviation Table

Introduction

Project Rationale

The rapid transformation for digital networks in Bahrain increased the demand of a reliable, secure, resilient and high-performance internet services and internet connectivity. As the number of the enterprise companies grows alongside with the expansions of their sites the Internet Service Providers are required to maintains and provides a reliable, scalable and efficient traffic routing network across all Bahrain. For ISPs such as Kalam Telecom, the absence and the lack of a MPLS backbone network and redundant design will restrict the ISP ability to provide carrier-grade services to the normal customers and the enterprise customers.

Kalam Telecom current network relays on traditional IP routing which will continuously face traffic congestion and limitation on redundancy, all these issues leads to internet service interruptions and inconsistent experience for the users. Furthermore, the absence of the Multiprotocol Label Switching (MPLS) protocol, Quality of Services (QoS) and Traffic Engineering (TE) will lead the network to failure when it comes to prioritize the mission critical application. As a result, the Services will be unstable for enterprise customers. If these issues are not addressed Kalam Telecom will face frequent outages, route instability, degraded performance and weaker competitive position in Bahrain.

The motivation behind this project is to develop a scalable, high performance MPLS backbone that are capable of providing high availability and efficient network across Bahrain.

Purpose and Objectives

The purpose of this project is to design and develop a complete MPLS based network backbone for Kalam Telecom that uses and integrate advanced routing protocol, customer VPN services and redundant connectivity. The main aim is to replace the current legacy network of Kalam Telecom with a carrier-grade network model that are capable of providing hundreds of

thousands of customers and enterprise companies distributed across Bahrain geographical area. The following points will specify the objectives of the new backbone infrastructure:

Technical Objectives:

- Design a hierarchical ISP backbone infrastructure with a clear segmentation between its layers
- Implement MPLS Label Distribution, MPLS layer 3 VPN and traffic engineer mechanisms to enable route optimization and guaranteed service performance
- Configure internal routing protocol and external routing protocol for effective inter-AS connectivity
- Apply redundant techniques such as VRF and redundant physical links
- Implement QoS policies to prioritize essential traffic
- Integrate ISP services including PPP, Static NAT and secure management access
- Strength the security by using AAA and route maps and role-based access control

Business Objectives:

- Improve network reliability
- Reduce service interruption
- Provide scalable infrastructure that support easy future expansions.
- Improving customer satisfaction by providing stable connectivity and high-performance connectivity.

Prior Work

This section will review two project that are related to the design and deployment of MPLS based network, the first one is on the implementation of MPLS technologies and the second one focuses on conceptual technologies and designs of MPLS VPN. These project guided my project design decisions while also highlighting the gap between my project and their project clearly.

1- *Implementation of MPLS VPN* (Gurung, 2015):

Gurung work focuses on using the MPLS Layer 3 VPN service within a simulated service provider scenario. The project provides a clear explanation of the concept of the label switching such as MPLS, route distinguishers, virtual routing and forwarding (VRF) also the formation of the label-switched path in addition to how MPLS can be flexible and scalable for the infrastructure. Gurung work also include a practical explanation using GNS3 and Wireshark to demonstrate how the Provider Edge (PE) routers, Provider (P) router and Customer Edge (CE) router works in an MPLS network, also validating how the label distribution and VPN routing using mechanisms like label distribution protocol (LDP) and Border Gateway Protocol (BGP) routes exchange. This work is valuable for understanding basic MPLS VPN behavior and packet flow within a network.

2- *Multiprotocol Label Switching Virtual Private Network* (Al-Selwi, 2013):

Al-Selwi examines MPLS VPN architecture in a service provider environment. His work covers core MPLS concepts such as label switching, label distribution, VRF designs, route distinguishers, route target and Multiprotocol-Border Gateway Protocol (MP-BGP) route propagation, alongside the demonstration on a cisco router using detailed configuration examples and step by step explanation. A key contribution of Al-Selwi work is to explains different types of advanced MPLS VPN topologies such as intra-net, extra-net, central service and inter-Autonomous system VPN designs. This project provides a strong theoretical and configuration-focused view of MPLS VPN technology.

Although both Gurung (2015) and Al-Selwi (2013) provides valuable studies on MPLS VPN technology, both work presents a limitation when viewed against the objective of this proposed project for Kalam Telecom.

- Gurung work on *Implementation of MPLS VPN* focuses primarily on demonstrating basic MPLS VPN functionality in a small simulated environment. Gurung works offers a clear and well written explanation of label switching and VRF. However, it does not explore

large scale ISP requirements such as Traffic Engineering (TE), Quality of Services (QoS), hybrid routing or backbone redundancy.

- Al-Selwi work on *Multiprotocol Label Switching Virtual Private Network* provides a very detailed conceptual and configuration-based discussion of MPLS VPN as well as multiple VPN topologies, but it remains limited and does not address ISP-grade scalability, inter-provider routing or performance optimization features required by the ISP.

In the other hand, this project for Kalam Telecom aims to design a comprehensive, carrier-grade MPLS backbone that incorporates TE, QoS, Multi-protocol routing and redundancy mechanisms suitable for a medium-sized ISP.

Hypothesis

This thesis hypothesizes that implementing an MPLS based backbone network with traffic engineers, quality of services and structured routing protocol will improve and enhance Kalam Telecom network significantly in these area's scalability, reliability and performance compared to the traditional based IP routing infrastructure. Prior research shows that applying MPLS will significantly enhance the routing predictability and congestion control in service provider (Rosen 2001; Awduche 1999). Therefore, the proposed solution is expected to enhanced the scalability, performance and achieving failover and efficient routing which is capable of supporting ISP level operations. in addition to interconnectivity for customers sites.

Proposed Solution

The current System of Kalam Telecom lacks the segmentation, scalability and resilience that is required to operate as a national ISP in Bahrain. To address Kalam Telecom issues, this thesis

proposed an upgraded backbone that uses and relays on MPLS. This new solution introduces Traffic engineering and structured routing protocols to improve path selection, enhanced overall network stability and congestion reduction. Through MPLS L3 VPNs and VRF the entire backbone can securely support multiple enterprise customer across entire Bahrain. The new system will also integrate redundant core and edge links to ensure availability and service continuity during failures. QoS policies will prioritize important traffic while the IGP will optimize internal routing and BGP will handle the inter-AS MPLS label exchange.

Description of the Report

The next sections in this thesis will explain the proposed solution. Each section will represent a specific topic alongside highlighting the approaches that were used throughout the project. Firstly, the background section that will highlight the necessary background information on technical terms alongside the technologies used in the project. Secondly, there is the design and requirements section which will highlight the designing approaches and decisions that the proposed solution will follow in addition to the methodologies that the project followed. Thirdly is the implementation section which will show step by step how this project is built. Fourthly is the testing section which will include the testing plan that the project is following, and any other things related to testing furthermore, this section is considered the most critical section of all sections since it will outline if the product is effective and achieve the main goals or not. Finally, the last section will focus on the Discussion and Conclusion which will cover all the obstacles and the objectives achieved alongside whether there is any suggestions for future upgrades to the product in addition to the LESPI and a reflection.

Background

This section of the document explains the background required to understand the design and implementation of an internet service provider network infrastructure. It explains the fundamental networking concepts that's runs the internet service provider networks. Kalam Telecom ISP environment needs a highly efficient MPLS based network, Quality of services classification and traffic engineering tunnel to optimize the flow within the MPLS network.

Related Theory

ISP Backbone Architecture

An ISP operates on a large network that are called a backbone network which is the main transit layer that carries the internet traffic across cities and customer in Bahrain. A backbone network is typically built and divided into layers, core layer which is mainly handling highspeed traffic and an edge layer which is mainly used to connect the customer to the ISP network. **According to Popa (2024)** hierarchical design is so important since it will enhance performance and improve reliability, performance, security and management.

Multiprotocol Label Switching

MPLS is a technique used by so many ISPs to move packets more efficiently. Instead of using the traditional methods of IP lookups, MPLS attached a label on the packet that tells the router where the packet must go. **According to GeeksforGeeks (2025)** that MPLS establish pre-determined label-switched path that allows the network to optimize the packet flow and ensure consistent performance throughout the network.

MPLS Traffic Engineering

Traffic engineering is an MPLS exclusive feature that helps the ISP to decide how the traffic flows across the backbone network**. Ergun (2023)** explains that TE allows the network engineers to optimize the network by allowing them to choose an explicit path to route traffic within it to avoid congestion. TE is similar to how a navigation app selects the least crowded road.

Routing Protocols

Routing protocols are considered the set of rules that the router follows to exchange information about the network. Routing protocols are divided into two types the IGP which is used internally within a single ISP domain and the EGP which is used externally between two different ISPs domain. Furthermore, the IGP help the router to update and share their information between the router and EGP manages and establish communication between multiple different networks.

Quality of Services

QoS is a method used to prioritize specific type of network packets so that the important application receives better performance**. Fortinet (2016)** explains that the QoS classifies and manages network packets in a different way based on the priority that they have been given such as video and voice calls. QoS helps to maintain high performance and speed even when the network is under heavy load.

Project Technologies

The following section is focused on discussing the technologies used when developing the proposed MPLS-based backbone ISP for Kalam Telecom and also outlines the alternative solutions that were considered but not been used in this project. This section is considered the

most crucial part. The goal of this section is to describe and justify why this technologies is chosen while explaining why other solutions were unsuitable for the project.

Technology	The purpose of the technology
EVE-NG	During this project implementation phase eve-ng was used since it is considered to be one of the most widely used network virtualization platforms out there for the networking field since it provides the network engineers with a safe environment to build and configure network topologies. It has multi-vendor image support, and it is commonly used for configuring BGP, MPLS and ISP grade simulations. The EVE-NG official documentation website highlights the ability of the EVE-NG to emulate large-scale network without any specialized hardware (EVE-NG, 2023). Alternatives solutions: GNS3 is the second most widely network virtualization network platform however GNS3 needs more manual configurations also it relies heavily on dynamips images which is not stable as much as the IOL images when running large scale MPLS networks.
 Cisco L2 & L3 image	Cisco L3 image provide the routing feature that is needed to the ISP backbone simulated network to function including MPLS, LDP, MPLS VPN, EIGRP, OSPF, QoS, TE and BGP. According to Cisco IOS documentation all IOS based routers are widely used in the enterprise and ISP network due to their

	stability and its ability to support rich features protocols (Cisco, 2023). Cisco L2 image simulates the core switching function such as VLAN, STP, VTP, VLAN Trunking. These features are needed to replicate the core, distribution and access switches with provides additional realistic to the emulated testing environment. Cisco website describes L2 as the foundation of the ISP internal network. (Cisco, 2030). Alternatives solutions: CSR1000v and ASR1000v offers advanced features when configuring the MPLS and MPLS VPN but these type of images required licensing fees in addition to the fees these routers are resource hungry which will not be a suitable solution to run it on consumer grade devices.
 Windows Server 2012 R2	Windows Server 2012 R2 was used to simulate and manages the essential services that are being used in any enterprise network in this project, the server hosts service such as the AAA and Syslog services. Alternative Solutions: Linux based-servers can provides the same functionality of windows server but Linux server does not have a GUI interface

	which will make it easier for demonstrations, testing and visualization.
 Windows 7	The Windows 7 client machine was included to simulate and represent the end-user device. These end-devices allows for testing and assessing the functionality of connectivity, service reliability and routing protocols from the perspective of the user. Alternative Solutions: any Linux distribution will also perform similar to the functionality of windows clients but on the other hand Linux distributions require additional configuration and also it differs from the common enterprise desktop environments. Moreover, MacOS is less accessible on a virtual machine since the MacOS are designed and optimized to run on arms chips, specially the M series chips.
 Vovsift Syslog Server	Vovsoft Syslog Server is considered as a lightweight syslog tool for collecting system logs form other devices such as routers and switches and stores them in a centralized server. According to SolarWinds (2019) centralized logging is essential for any network since it will monitor any changes, events and network failures and will send an alert to the relevant team. Alternative Solutions: WinSyslog server from Adiscon offers more advanced features than the

	Vovsoft syslog server but WinSyslog required a extensive configuration to be able to use the syslog.
 WinRadius	WinRadius is an open-source AAA application that provides the AAA service for other network devices. AAA services is a common requirement for ISP network since it ensure that only the authorized personnel can modify the configuration of the devices also, it provide accountabilities for all of the authorized personnel (Fortinet, 2020). Alternative Solutions: FreeRADIUS is a more powerful AAA service, but it is much harder and more complex when it comes to configuring it and it is available only on Linux based server distributions.
 Putty	Putty is a terminal emulator which is mainly used to access the network devices using either SSH or telnet. It allow us to configure the routers and switches by using a secure command line interface. According to putty documentation, putty is widely used for remote network administrative tasks due to its simple GUI and its reliability (Putty, 2022). Alternative Solutions: SecureCRT is one of the best SSH/Telnet clients out there, but the SecureCRT is a

	commercial software with a hefty license fees that need to be renewed yearly.
 VMWare	VMware is a virtualization software that is used to run virtual machines such as windows operating systems. In this project the VMware was used to simulate the ENE-NG virtual machine enabling the entire project to run smoothly. According to OVHcloud VMware explains that virtualization helps to simulate multi-device without the need for multiple physical hardware. Alternative Solutions: VirtualBox is a free virtualization software, and it mostly know for small labs or testing scenarios since it less stable that VMWare in addition to that VMWare is more compatible with EVE-NG.
 Wireshark	Wireshark is an open-source application that was included in this project to capture and analyze the incoming and outgoing packets inside the simulation environment. Wireshark allow for monitoring packets in real time within the simulation. Alternative solutions: Capsa Network Manager is a great network capturing and analyzing software but it is much harder to setup since the full application features is not in the trial version which is not very useful for this project.

Table 2 - Technologies Used

Related work and Literature Review

The following section examine and explore the current existing research of the related technologies and designs for ISP such as ISP network architecture, MPLS technology, Internal routing protocols, external routing protocols, QoS, TE and MPLS VPN. The primary goal of this thesis document is to develop an ISP infrastructure using MPLS, routing protocol, QoS, TE, MPLS VPN and redundancy mechanisms, since there is no related work published on the internet since the MPLS based network designs are considered as intellectual properties. This section will focus only on the literature review, and it will be divided into 7 divided sections:

- ISP network architecture:

  Most ISPs network are structured into several layers this approach is taken to ensures scalability and efficient routing. **Allen (2023)** describes the hierarchical model which consists of core, distribution and access layer are one of the most widely opted network architecture designs due to it improving the stability and efficiency of the network in addition to simplifying network operations. The 3-layer architecture are designed to reduce congestion and improving the predictability of routing by dividing and separating network function across multiple tiers and layers. However, most of the available documentation focuses on the large-scale ISP which offers a limited amount of design guidance for medium ISPs operating with fewer resources than the global ISPs. This reveals a gap for designing solutions focused to ISPs operating within a national scale.

- MPLS technology:

  Multiprotocol Label Switching improves the forwarding flow of the packets by using a short label instead of the traditional IP lookups. **Rosen, Viswanathan, and Callon's MPLS architecture (2001)** introduced the label switched path to the world as a unidirectional tunnel to forward data which provides the ability to predict the routing path and reduced forwarding delays which is necessary and critical for ISP networks, while MPLS is widely documented and explained, most of the published literature focuses on implementing the MPLS technology on a tier-1 ISP networks making little documents and references to the deployment challenges that may face any smaller ISP when implementing MPLS on their networks. However, the publicly accessed MPLS guides and instruction rarely discusses the design strategies for MPLS networks for medium sized ISP. These limitations justify the need for this thesis to discuss the designing strategies and demonstrating a practical MPLS backbone solution specifically adapted by a ISP such as Kalam Telecom.

- Internal Routing Protocols:

  Internal gateway protocol such as OSPF and EIGRP determines how routers within the same autonomous system share information about the network**. According to the specification of OSPF**, link state routing allows the routers to adapt to any routing information changes within the network quickly, which is essential for the operation of the backbone of any ISP. **Cisco's documentation for EIGRP (2019)** highlight the protocol efficiency and speed in calculating the optimal paths. However, the majority of vendors and ISPs consider and treat these protocol independently and all the published resources provides limited examples of the hybrid usage of both of them in the same autonomous system. Since Kalam Telecom's design uses both OSPF and EIGRP, this thesis helps fill the gap by showing how multiple internal routing protocols can coexist in an ISP backbone.

- External routing:

  Border Gateway Protocol (BGP) is considered to be the dominant protocol when its comes to communicating and exchanging routing information between autonomous systems around the world. **Honig, Katz, Mathis, Rekhter and Yu (2023)** explains that BGP relays on policy-based routing since it allows the ISP to control the inbound and outbound traffic flow. All the published literature about BGP explains how important it is for global internet connectivity in addition, to the importance of BGP to global internet connectivity the literature also explains that the BGP can be beneficial to the smaller or even medium sized organizations. However, most of the documentation that discuss the BGP on the internet focus on a large-scale organization or a global carrier service provider and does not address any of the operational and designing challenges encountered by the medium-sized ISP or smaller organization implementing the BGP protocol for the first time. This project contributes by demonstrating how BGP can be configured and applied efficiently with any network.

- Quality of Service:

  Quality of Service is mainly used to prioritize traffic during the congestion periods. **Fortinet's QoS overview (2020) and GeeksforGeeks' QoS definition (2025)** explains how such techniques like classification and scheduling ensures that real-time applications such as Voice Over Internet Protocol (VoIP) and video calls receives much higher bandwidth and priority than regular data. While these techniques are well explained on the internet, most QoS research and literature that are publicly accessible often focuses on the enterprises network rather than ISP infrastructure or a global carrier provider. Furthermore, the published documentation on QoS explains how to implement the QoS on a Non-MPLS network. This thesis addresses that gap by providing a practical explanation on how QoS interact with MPLS-based network.

- Traffic Engineering:

  MPLS Traffic Engineering (TE) is used on top of MPLS to help direct traffic through a certain path instead of relaying on the shortest path routing algorithm. **According to Request For Comments No. 2702 by Awduche (1999)** that TE enables the network to manage bandwidth more effectively by choosing a path based on the network tunnels configuration. Despite TE benefits, most of the published resources on the internet do not show how to configure the MPLS TE in a medium/balanced congested networks instead they focused on implementing the TE on a large carrier provider network. This limitation made the TE one of the highest relevant topic in this project as the thesis demonstrates how a regional ISP such as Kalam Telecom can implement TE within its network.

- MPLS VPN:

  MPLS layer 3 VPNs will give the ISP the ability to separate customers traffic using a specific technology called virtual routing and forwarding (VRF). **According to RFC No. 4364 by Rosen & Rekhter (2006)** it explains how MPLS VPNs support multi-site enterprises by isolating the routing tables into multiple virtual routing tables for each customer while still having one backbone infrastructure. This technology is ideal for ISPs when serving multiple corporate customers. However, most of the available resources on public internet are focusing on large scale service providers offering commercial MPLS VPN services and does not provide any information or practical example for medium regional ISP building their first MPLS VPN infrastructure. That is why this thesis paper exists by showing how MPLS VPNs can be designed for smaller or even medium sized organizational or ISPs.

Design and Requirements

The design section will explain how the proposed system was planned and designed to address the problem that was identified earlier in this thesis. Describing the overall approach which has been taking during the design process and how each part of the system participate to help finding a final solution. This section present the structure of the proposed network which outlines the methodologies followed during the design phase and additionally explain the reasons behind the chosen architecture decisions. For more additional details about the design and IP address schema refer to the appendix 2 – Design Specification.

Full system use case diagram

The below figures outline the complete system use-case diagram for the proposed system for Kalam Telecom. A full system use-case diagram provides visual insights about the summary of how users interact differently with the system by using the functional requirements as a representation through a structured diagram. **According to Lucidchart (2023)** a use-case diagram helps define the system behavior by identifying the actors of the system, the tasks they are performing, and the actor-component relationship. **Additionally, GeeksforGeeks (2025)** states that the full system use-case diagrams are essential items when gathering requirements, as they reveal clear boundaries of responsibility between the actors and the other components.

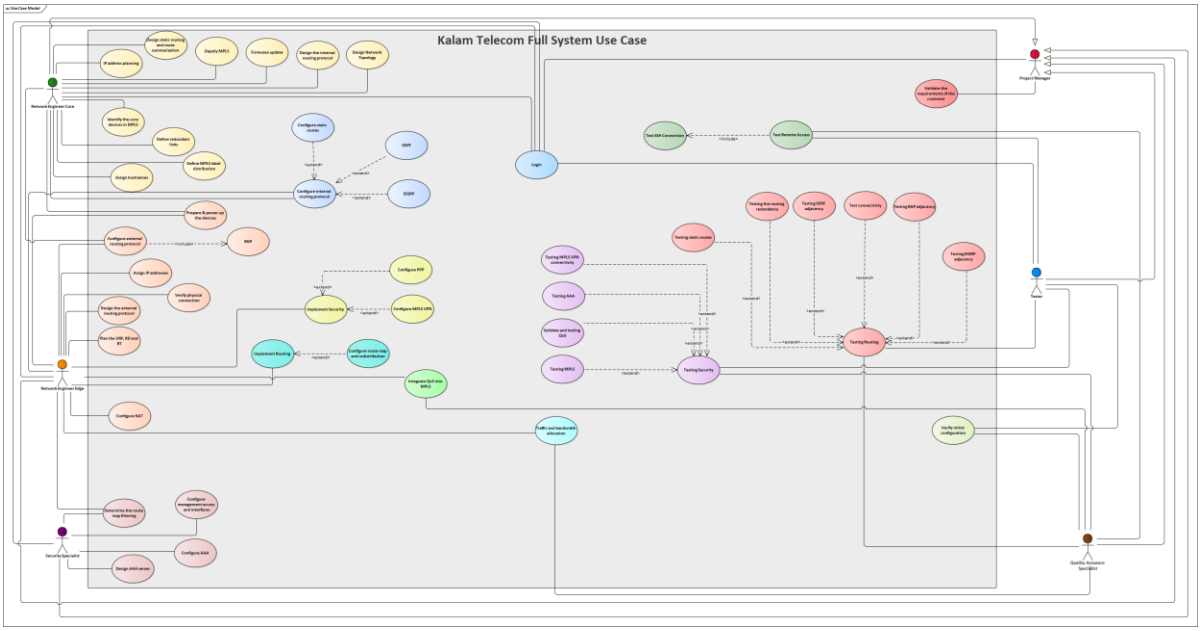

Figure 1 - Full System Use-case Diagram describing the system behavior

Activity Diagram

The following Activity diagram represents the operational flow of the QoS processing for the proposed system of Kalam Telecom. The diagram illustrate how the packet travels from the customer router side until it reaches the ISP border router and how the DSCP values are checked and handled. The activity diagrams is very effective for modeling the behavior of dynamic network and describing the action in a sequence order on data packets within Kalam Telecom network devices. **According to GeeksforGeeks (2025)** Activity diagrams, it is very helpful when you need to represent a technical process flow of certain elements to a non-technical person such as management. Furthermore, **Visual Paradigm (2023)** states that the activity diagrams help in identifying the parallel activity, decision activity and overall workflow structure, which making this diagram particularly useful for explaining how different components interact during the execution of the system.

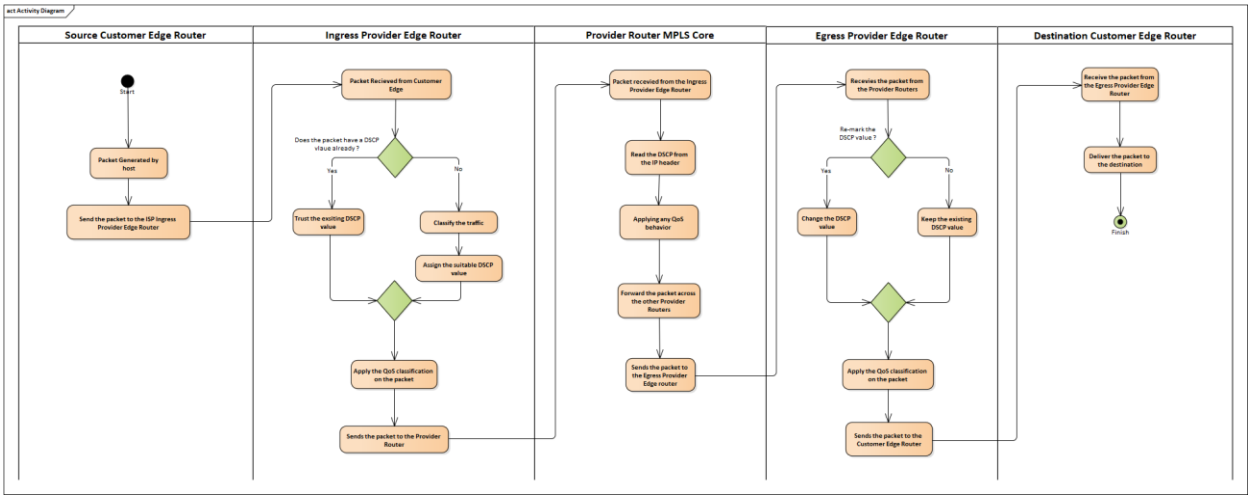

Figure 2 - Packet Flow Diagram for QoS describing the flow of the operation of QoS

Network Topology

The figure below shows the network topology diagram that illustrate the structured layout of the proposed network for Kalam Telecom, which is shows how routers, switches, servers and end-devices are connected to the ISP backbone to support its operations. Network topology diagrams help visualize the positions of the network components and their communication paths in a logical way. **According to Editorial Team (2022)** a network topology gives the technical and non-technical people a clear representation of how the data flows through the network infrastructure which allows the network designer and other networking staff to evaluate the network performance and scalability. Additionally, **Jackson and Goodwin (2025)** explains that the network topology can show the bigger picture of the infrastructure since the network topology can help the engineers to identify where modifications can be made or expanded when any issue appears.

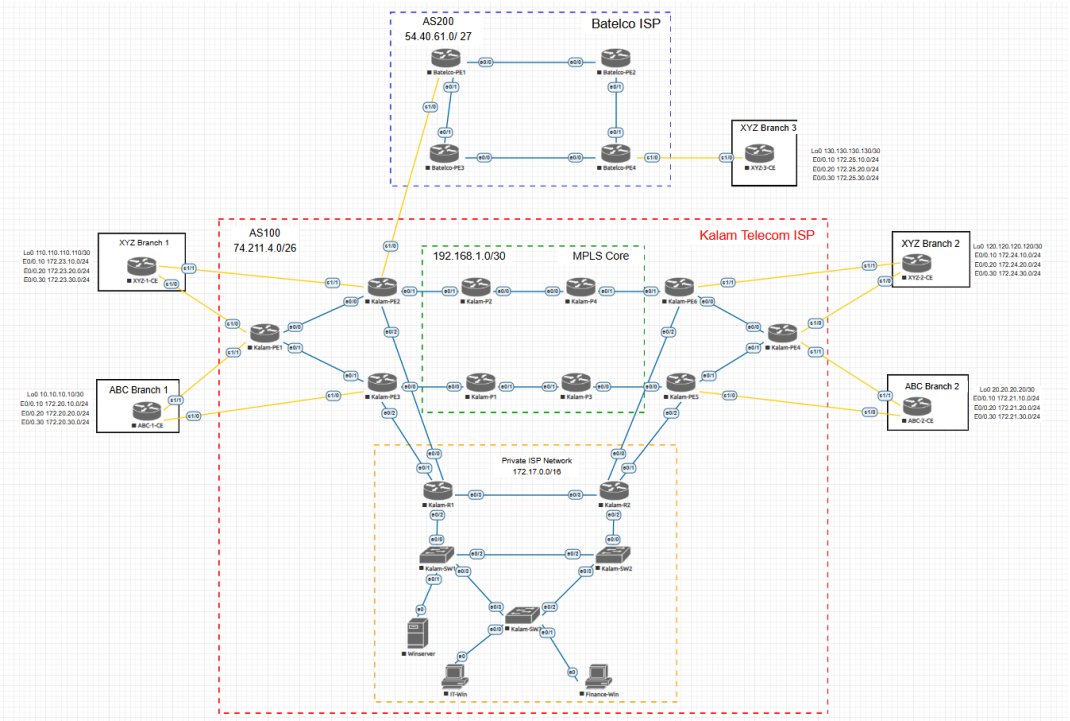

Figure 3 - Network Topology Logical View

Architecture Diagram

The architecture diagram outlines a clear structured view of how the main components of the proposed system of Kalam Telecom work to achieve the intendent functions. This diagram help to understand the logical arrangement of service layers and flow of communication within the project. **According to Guthrie (2021)** the architecture diagrams outlines and shapes a high-level blueprint that explains how the different components on the system are collaborating with each other in addition to highlighting the responsibilities and how data is moving inside the system. This makes the architecture diagram very important and essential when validating the system requirements achievement. **AWS (2023) states** that the architecture diagram also helps to identify the most effective and efficient ways when it comes to scalability. Furthermore, architecture diagrams can help in reducing the development risk since it can identify if there is any faulty logic design or incorrect assumptions.

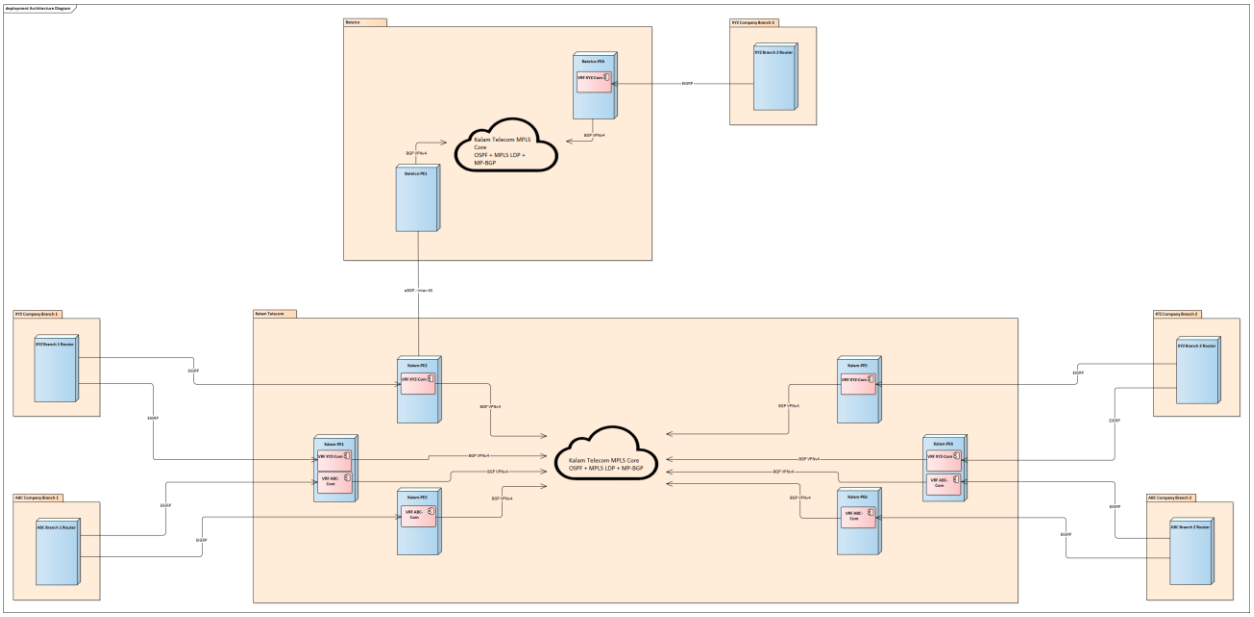

Figure 4 - Architecture Diagram

Deployment Diagram

Deployment diagrams illustrate how the components of the system, either physically or virtually distributed across the entire network. Deployment diagrams are mainly used to show where does the service and network elements exist in, additionally, how they all communicate across the different nodes in the topology. **According to Miro (2025)** the deployment diagram improves the process of clarification when its comes to the hardware configuration by representing the devices, services that running inside the device and the connection between the devices. **GeeksforGeeks (2024) explains** that deployment diagrams can be more challenging and more complicated in big systems with lots of nodes. However, this diagram can be beneficial since it provides an excellent amount of details during the system operation.

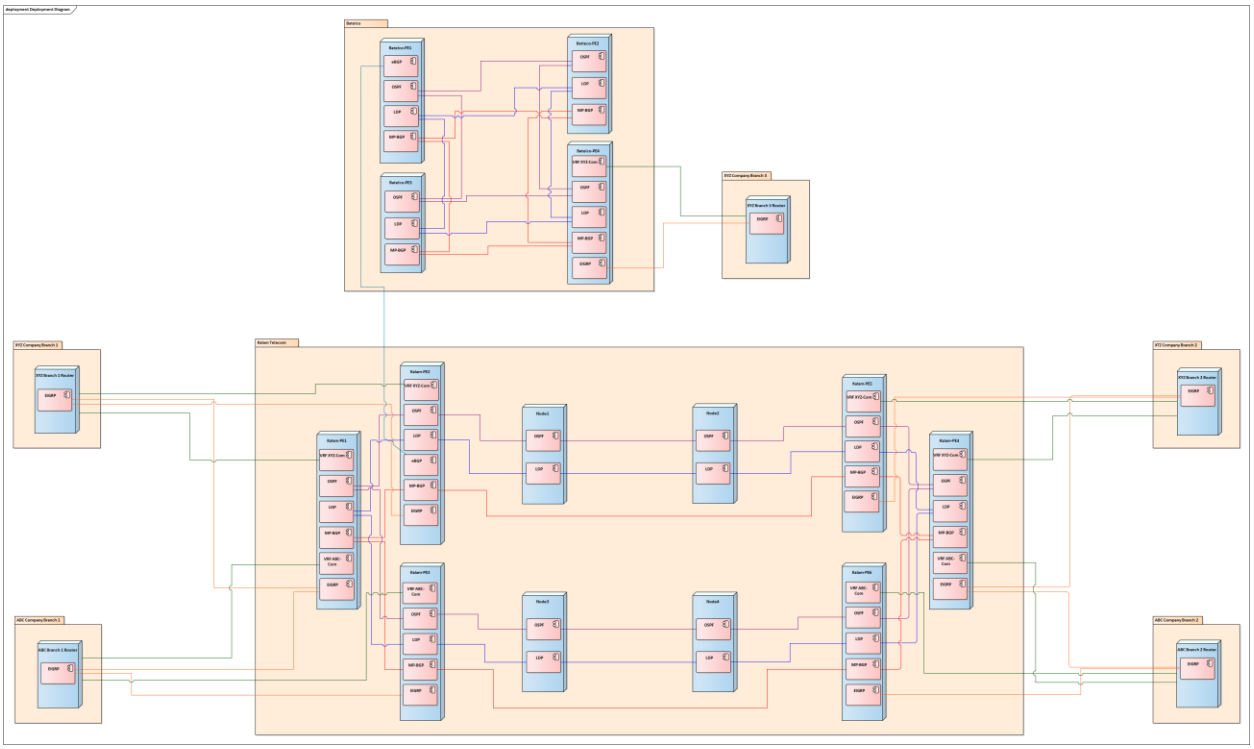

Figure 5 - Deployment Diagram

Implementation

The following section outlines the main steps followed to implement the proposed design of Kalam Telecom MPLS-based network. The detailed configuration steps are documented and are available in the Appendix 3 – System implementation and not covered in this section. This implementation focuses on preparing the virtual lab environment to implement the system, configuring the core and edge routers with the necessary routing protocols in addition to enable the MPLS and VPN services and setting up supportive services such as AAA and Syslog

Virtual Environment Setup

The full topology of Kalam Telecom was implemented inside EVE-NG virtual networking platform, community edition. Virtual environment resources allocated:

- CPU: 4 virtual CPUs
- RAM: 16 GB
- Storage: 450 GB

Basic Device Configuration for Kalam Telecom Router

All the network devices in the topology were configured with:

- Hostname
- IP addresses
- Domain Name
- Banner
- SSH
- Password encryption
- Internal routing protocols
- External routing protocols

The following figure shows the basic configuration when using the show run command.

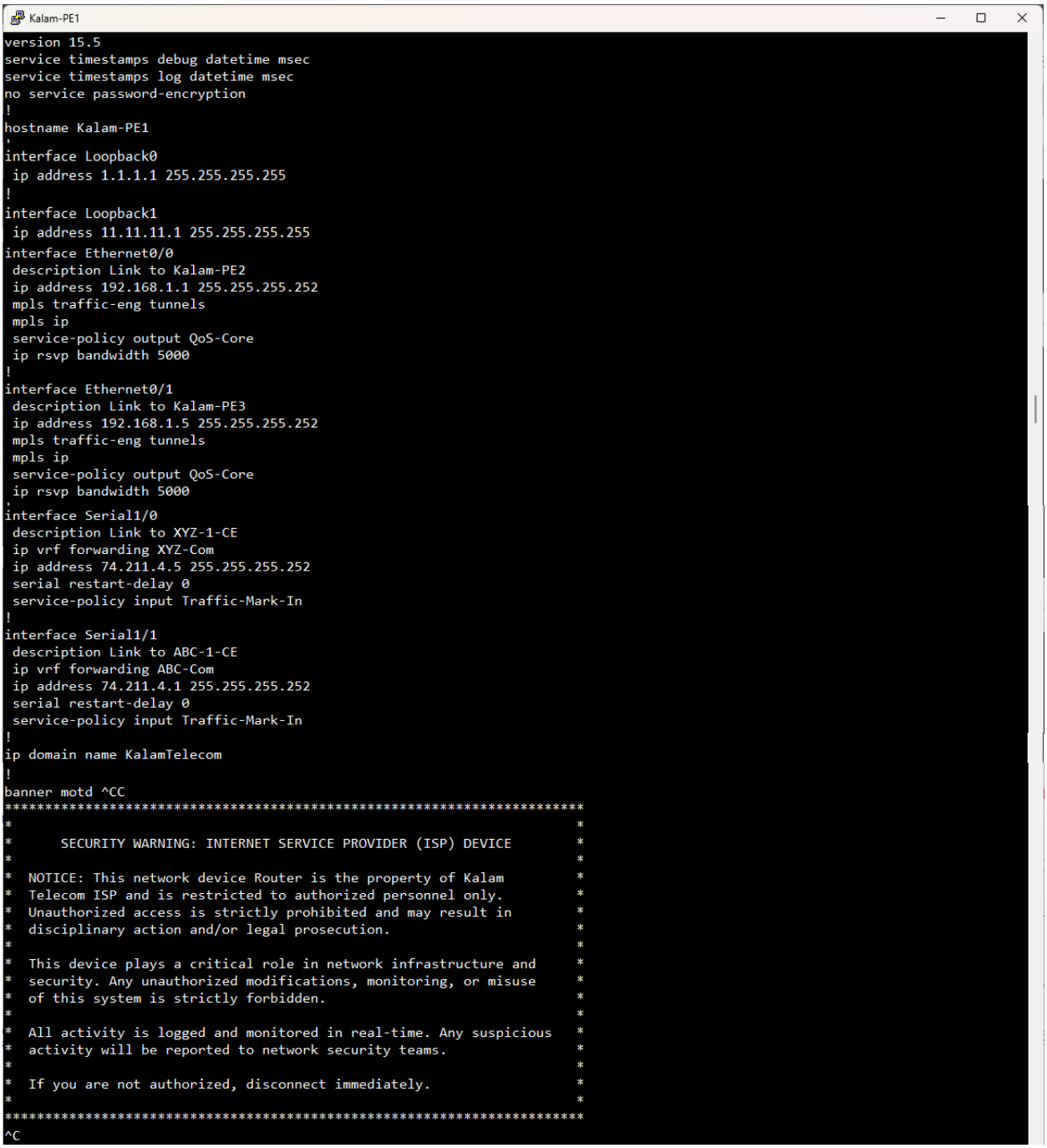

Figure 6 Basic Device Configuration Example

Note: all the Kalam Telecom devices has similar configurations put with different IP addresses.

Routing configuration for Kalam Telecom routers

Each layer of Kalam Telecom network uses a different Internal Gateway Protocol (IGP). The MPLS layer uses OSPFv2, EIGRP and BGP and the internal network uses OSPFv2.

OSPF

The MPLS backbone layer uses OSPF process ID of 1 and Area ID of 0. The internal network layer uses OSPF process ID of 5 and Area ID of 0.

OSPF 1 Routing implementation details:

- Initiate the routing process
- Assigning router ID
- Advertise the network
- Verify neighbor relationship

The below figure shows all the devices that participate in OSPF 1:

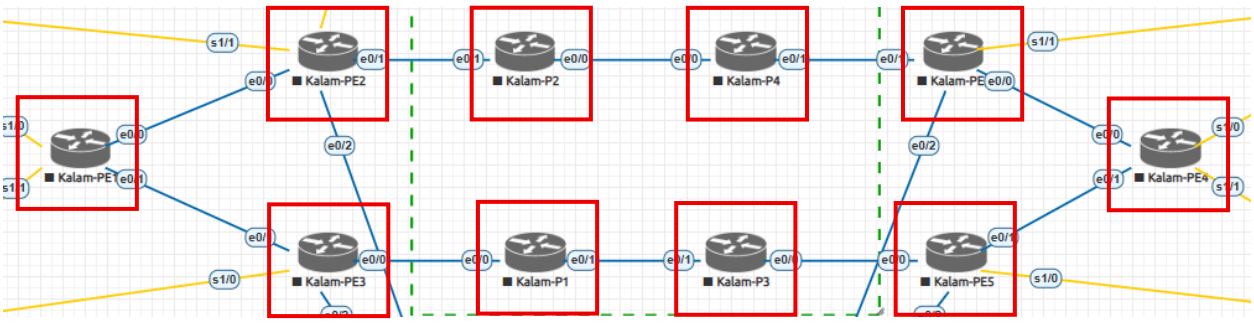

Figure 7 OSPF 1 Devices

OSPF 1 process configuration:

The figures below shows the OSPF process 1 configuration on Kalam-P1, Kalam-P2, Kalam-P3, Kalam-P4, Kalam-PE1, Kalam-PE2, Kalam-PE3, Kalam-PE4, Kalam-PE5 and Kalam-PE6. All these devices are considered to be from MPLS backbone layer which uses process ID 1 to manage all the routing information inside Kalam Telecom. OSPF in generally very suitable for this position since it is considered as link state advertised protocol.

The router-ID are manually configured to 1.1.2.1 for Kalam-P1, 1.1.2.2 for Kalam-P2, 1.1.2.3 for Kalam-P3, 1.1.2.4 for Kalam-P4, 1.1.1.1 for Kalam-PE1, 1.1.1.2 for Kalam-PE2, 1.1.1.3 for Kalam-PE3, 1.1.1.4 for Kalam-PE4, 1.1.1.5 for Kalam-PE5 and 1.1.1.6 for Kalam-PE6. additionally, the OSPF process 1 have a keychain named OSPF_AuthenKey to authenticate the communication between the devices that runs process 1 of OSPF alongside a key value of 1 to differentiate multiple key values if there is any. The key string word of the key value 1 is KalamOSPF1. Furthermore, the network statement is manually added to the OSPF 1 to advertise the IP prefix to the neighbors.

This configuration show a clean methods to identifies the neighbor when it comes to the MPLS Backbone layer and advertise the needed and necessary interfaces into the network along with an authenticated line for communication.

Explaining the commands:

- “router-id <ID>” ⇨ assign a manual router ID.
- “network <IP address> <Mask> <area ID>” ⇨ advertise a specific network.
- “key chain <chain name>” ⇨ Create a key chain.
- “key <value>” ⇨ assign key value for the key chain.
- “key-string <string>” ⇨ assign the string to be applied on the key chain.
- “cryptographic algorithm <algorithm name>” ⇨ specify the algorithm that will be used for the authentication.

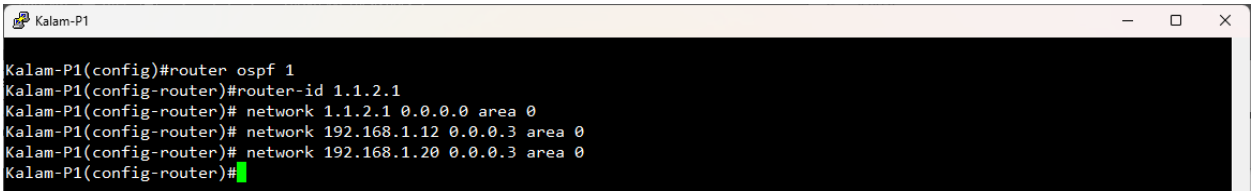

Figure 8 Kalam-P1 OSPF 1 Configuration Commands

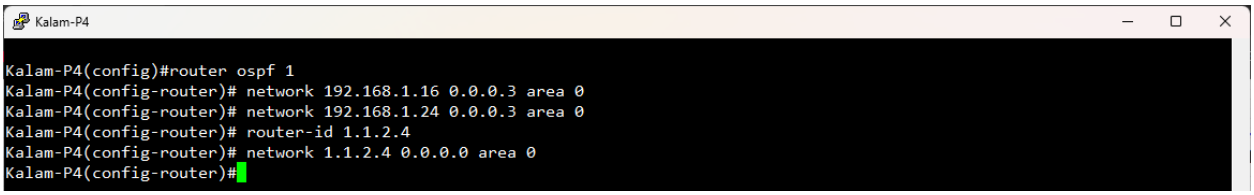

Figure 9 Kalam-P4 OSPF 1 Configuration Commands

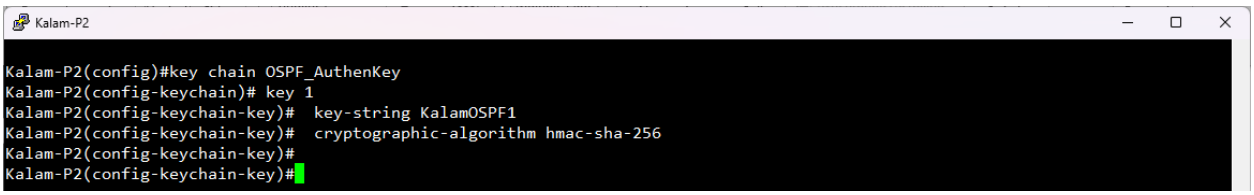

Figure 10 Kalam-P2 OSPF 1 authentication Configuration Commands

Adjacency verification for OSPF 1

The upcoming figures shows and outline that the OSPF routing tables and the adjacency across all the MPLS Backbone layer.

Note: This verification section contains different set of routers than those used in the configuration section. This approach is used to show that all routers are successfully forming an OSPF adjacencies for OSPF process 1. this verification section, the selected routers for are Kalam-P2 and Kalam-P3.

Across Kalam-P2 and Kalam-P3, each of them form an OSPF adjacency via their Ethernet interface demonstrate a correct configuration for the OSPF. Matching the process ID and the area ID.

In the routing table each “O” (OSPF) proves that there is a successful OSPF adjacency, the “O” confirming it is an internal OSPF adjacency within the same OSPF process. Additionally, the IP prefixes of 1.1.2.1/30 and 1.1.2.4/30, which were configured under OSPF 1 on Kalam-P1 and

Kalam-P4, visually appear on Kalam-P2 and Kalam-P3 router routing table, this proves that all routers in OSPF 1 are configured correctly. Furthermore, the numbers between the square brackets contains the administrative distance which is be default 100 for OSPF and the OSPF cost which is calculated by dividing the reference bandwidth/interface bandwidth.

Kalam-P3 router commands ”sh ip ospf neighbor” output is little bit different due to the fact that the P3 router is connected to PE5.

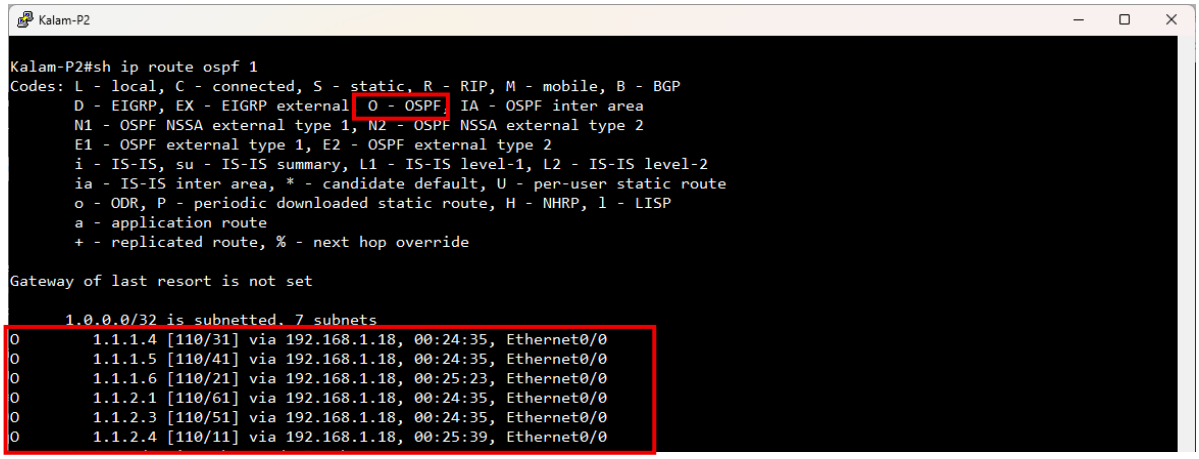

Figure 11 Kalam-P2 OSPF 1 Routing table

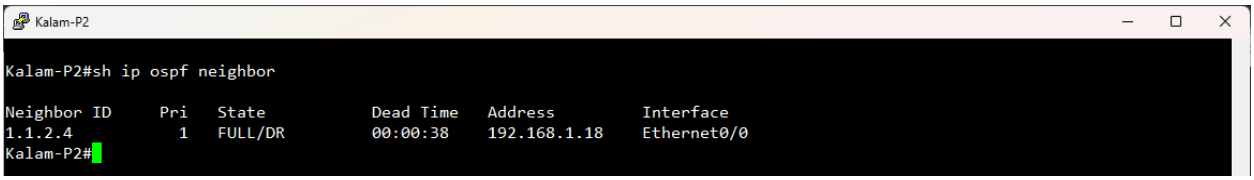

Figure 12 Kalam-P2 OSPF 1 Neighbors

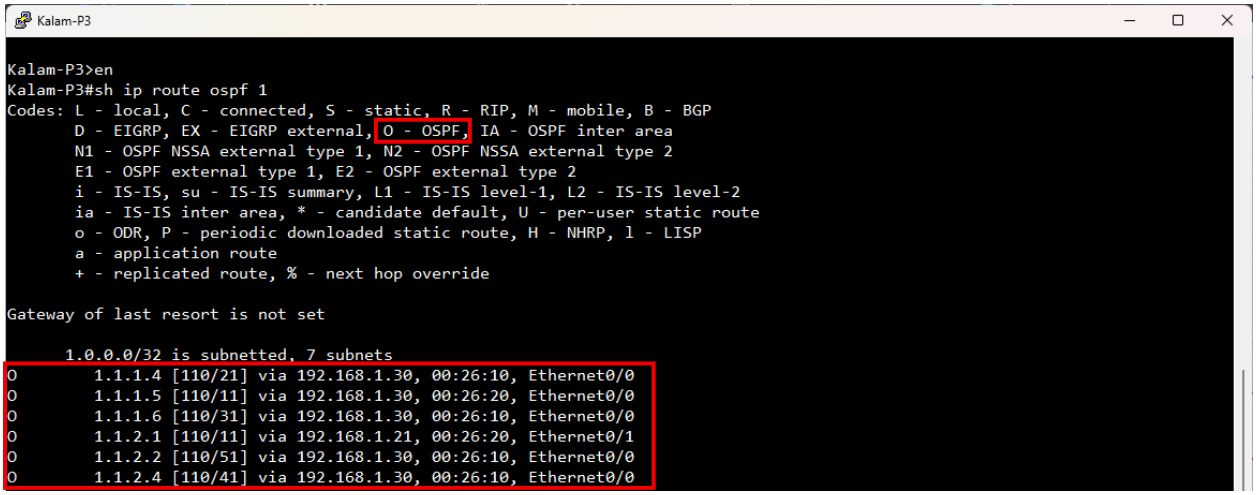

Figure 13 Kalam-P3 OSPF 1 Routing table

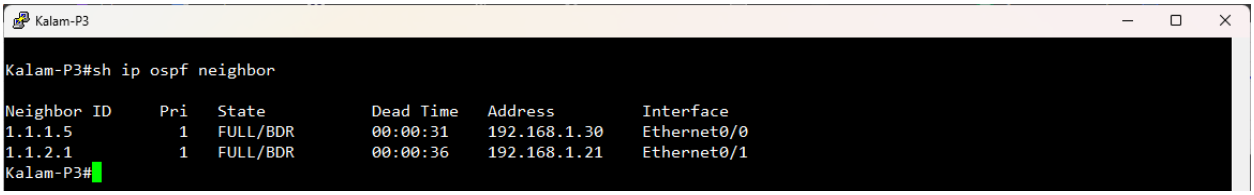

Figure 14 Kalam-P3 OSPF 1 Neighbors

OSPF process 1 Wireshark packet capture

The next figures will demonstrate a Wireshark packet capturing for two router Kalam-P2 and Kalam-P4 which are involved in OSPF process 1 routing.

upcoming figure explains the packets sent by the P2 and P4 which includes a hello packet, Database description, Link state request, Link state update and Link state Acknowledgement. All of these packet take part when forming an OSPF adjacency.

Hello packets are mainly used to discover if there is any other OSPF neighbors and verify that the requirement parameters match before forming an adjacency. These parameters are the Area ID, hello and dead intervals timers and authentication settings if configured. After the neighbors are discovered, Database Description (DBD) packets are exchanged between the neighbors to compare the content of the Link State Databases (LSDB) between them. Based on this comparison, the router will send a Link State Request (LSR) packet to request any missing or outdated Link State Advertisement (LSA). The Link State Update (LSU) packet are then used to send the requested LSA to the neighbor, allowing both of them to have identical LSDBs. Finally Link State Acknowledgement packets are exchanged to confirm reliable receipts of the LSAs and finalizing the adjacency formation process.

OSPF Hello Packets

This figures shows that Kalam-P2 sends a Hello Packet with a source address of 192.168.1.17 to the 224.0.0.5 destination IP which represent the multicast address for all routers that are running OSPF. Also, we can see the protocol name and number of this packet under layer 3

header which is OSPF IGP with a number of 89. Furthermore, the OSPF header show the router ID of Kalam-P2 which is 1.1.2.2 and the area ID of 0.0.0.0 plus the message type and the authentication parameters.

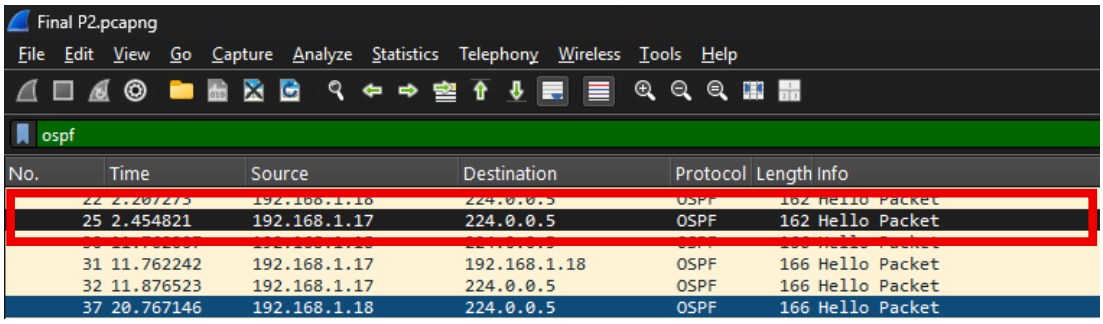

Figure 15 Kalam-P2 OSPF Hello Packet

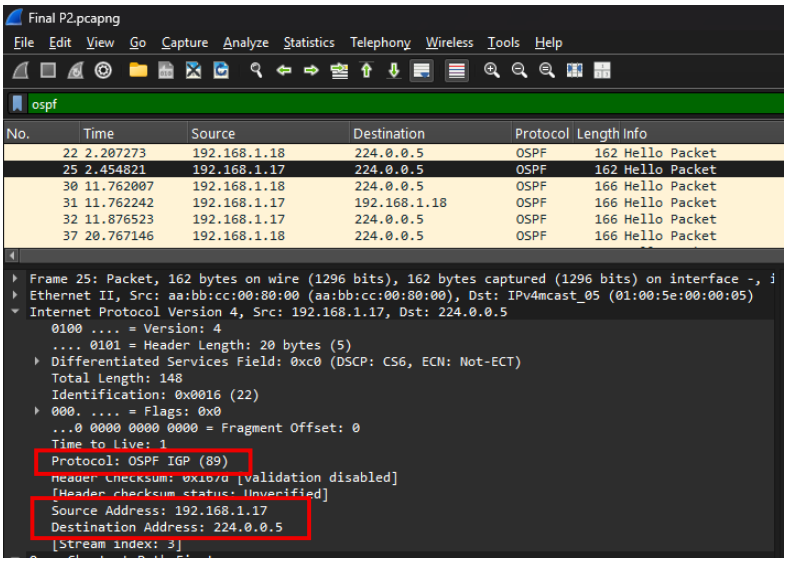

Figure 16 Kalam-P2 OSPF Hello Packet Layer 3 Header Inspection

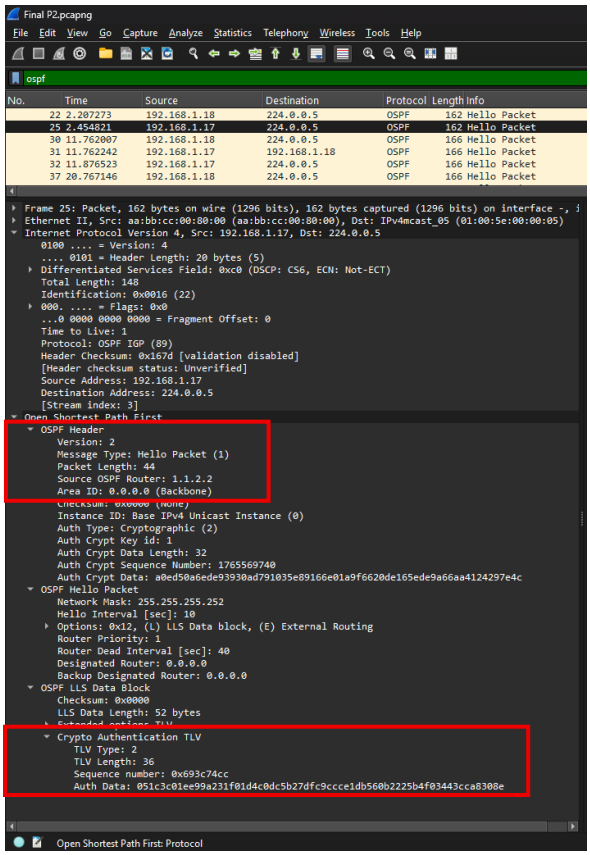

Figure 17 Kalam-P2 OSPF Hello Packet OSPF Header Inspection

In the other hand, Kalam-P4 also sends a hello packet with a source address of 192.168.1.18 and a destination address of 224.0.0.5. The layer 2 header also show the source address and destination address of Kalam-P2 in addition to the protocol name. In the OSPF header we can see the parameters of OSPF such as the router ID of Kalam-P4 1.1.2.4, area ID 0.0.0.0, authentication parameters and packet type which is Hello packet.

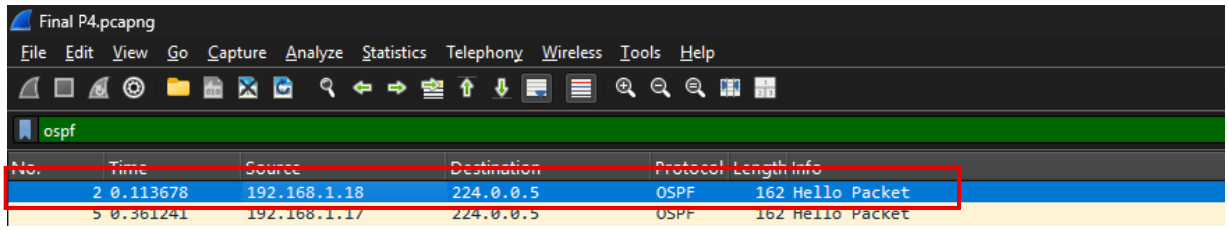

Figure 18 Kalam-P4 OSPF Hello Packet

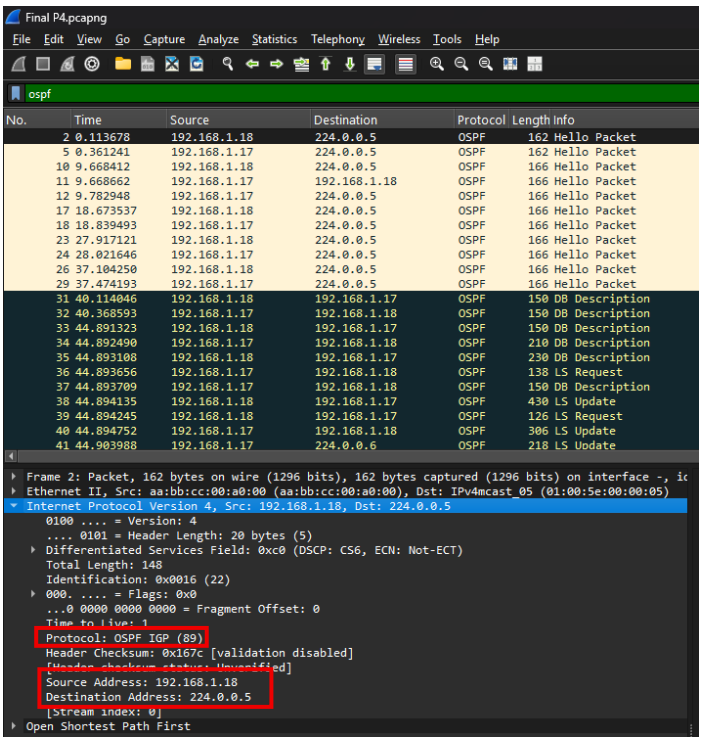

Figure 19 Kalam-P4 OSPF Hello Packet Layer 3 Header Inspection

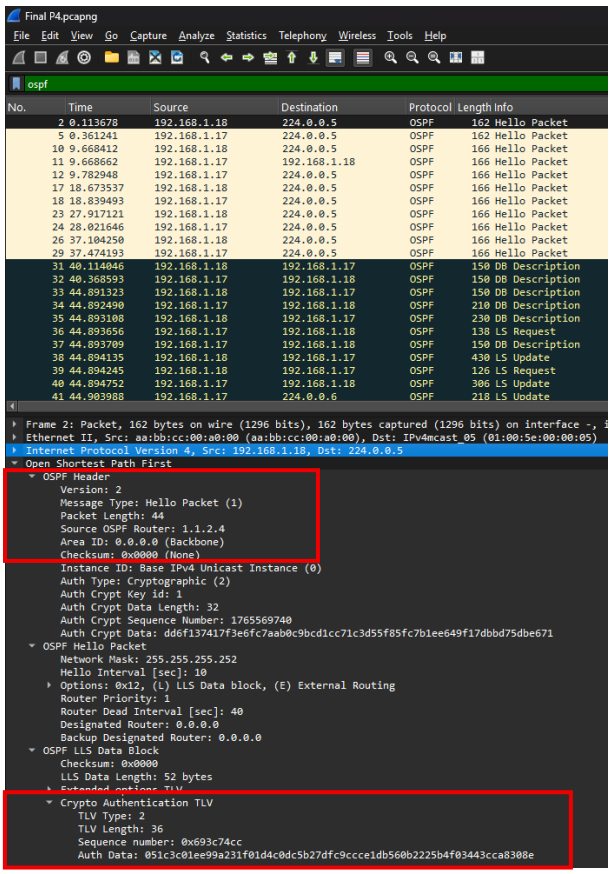

Figure 20 Kalam-P4 OSPF Hello Packet OSPF Header Inspection

OSPF Database Description (DBD) Packets

After the Hello Packets are exchanged and the necessary parameters has been checked and validated the DBD packets are used to exchange the LSDB of each router within OSPF process 1.

The DBD packets are sent in two phases, the first phase used to negotiate which will have the role of the master and which one will have the role of slave, agreeing on the sequence number for the packets. Then the second phase used to compare the actual database header entries between routers after the DBD phase 1 parameter has been obtained.

The following figures shows the DBD phase 1 packet exchange and inspection of Kalam-P2. With the source address of 192.168.1.17 and a destination address of 192.168.1.18. in addition, it also show the DBD of the packet which identifies which state the DBD packet is, this can be

identified from the line (I) Init: Set which means this is the initiate DBD packet. Furthermore, the packet also shows the status of the router, whether it is a matter or slave from this line (MS) Master: Set.

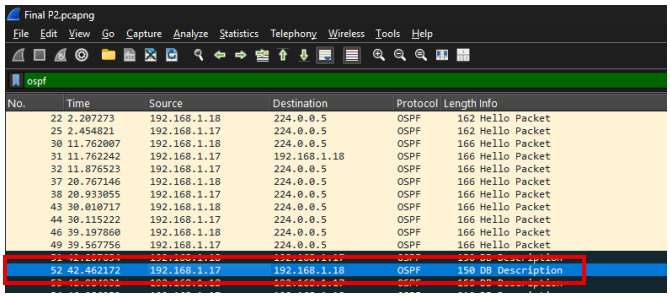

Figure 21 OSPF DBD Phase 1 Packet from Kalam-P2

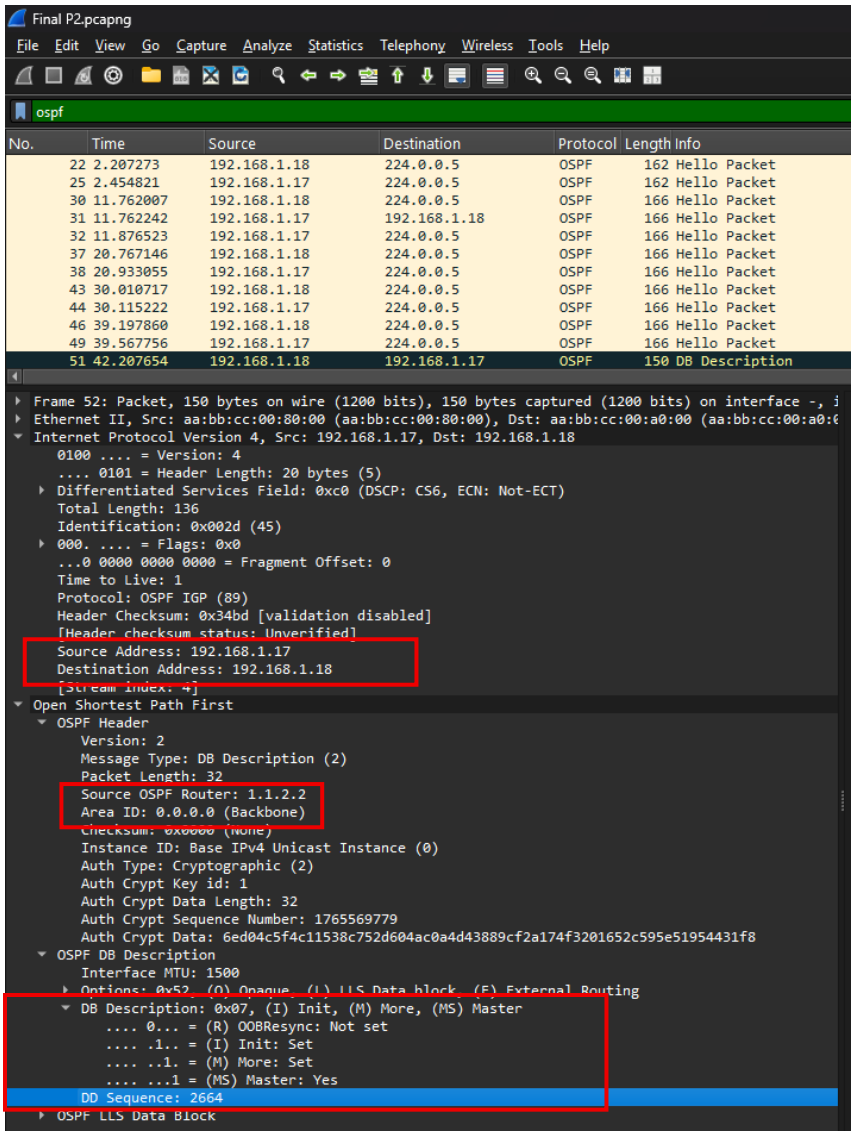

Figure 22 OSPF DBD Phase 1 Packet Inspection from Kalam-P2

In the other side Kalam-P4 will have similar output but with different sets of IPs, a source address of 192.168.1.18, a destination address of 192.168.1.17 alongside with the other DBD packet parameter which been explained in Kalam-P2 figures above.

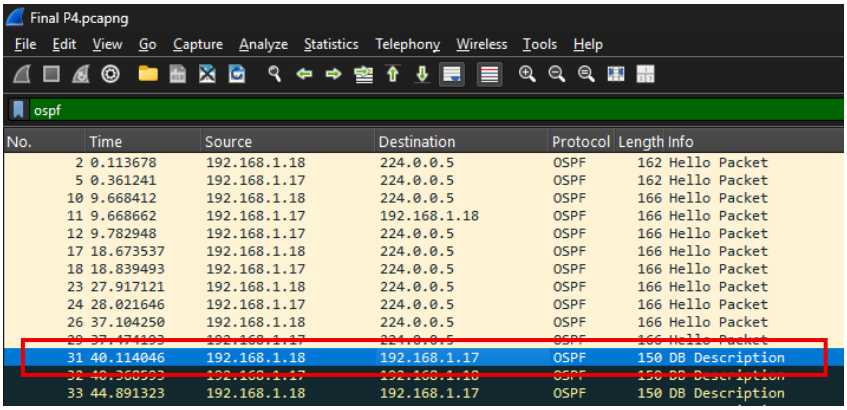

Figure 23 OSPF DBD Phase 1 Packet from Kalam-P4

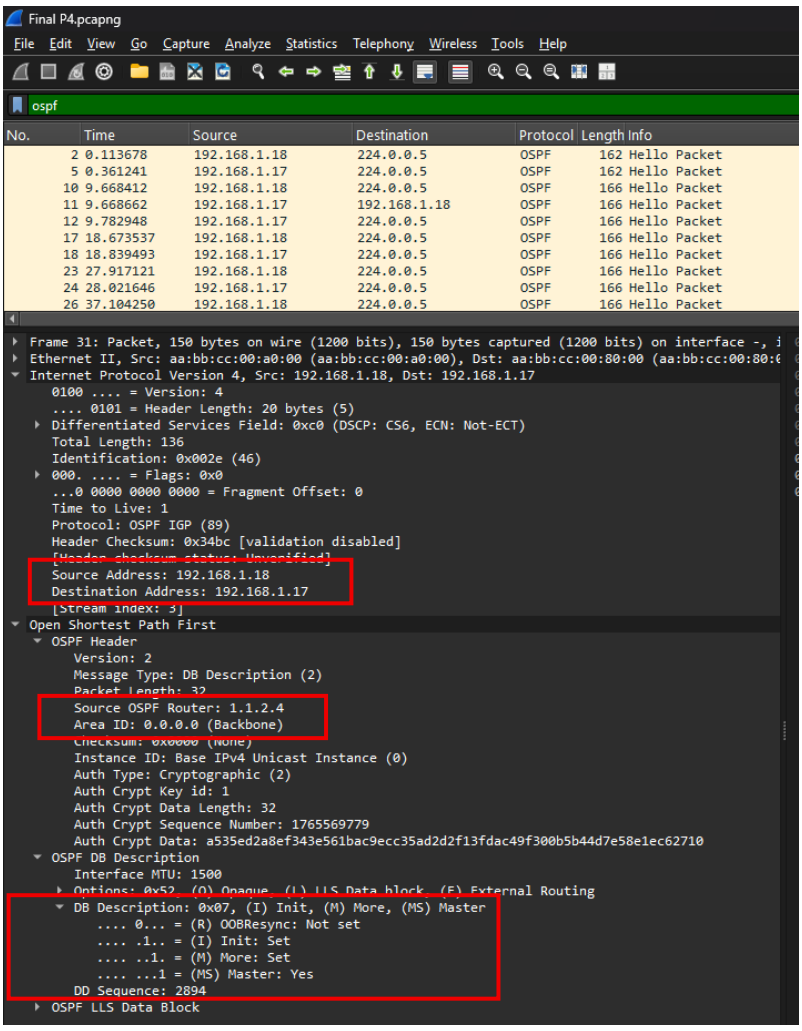

Figure 24 OSPF DBD Phase 1 Packet Inspection from Kalam-P4

In phase 1 both routers Kalam-P2 and Kalam-P4 will have the Set value for all of these variable (I) Init, (M) More and (MS) Master since both routers in the initiate phase.

After the DBD phase 1 packet exchange and the role of the master and slave are selected by the routers. The DBD phase 2 is started, and the phase 2 packet are being sent to compare the LSA headers between the routers.

The next two figure shows the DBD phase 2 packet exchange between the source 192.168.1.17 (Kalam-P2) and the destination 192.168.1.18 (Kalam-P4) with the inspection of the phase 2 parameters which include the LSA header which includes LSA-type 1 header with the link state ID of 1.1.2.2 which represents the advertised IP and the advertising router which represents the source router who advertise this prefix to the other neighbors which is 1.1.2.2, the role of the router which is elected as the slave router,. In addition to the LSA-type 10 which belongs to the TE (Coming in later part).

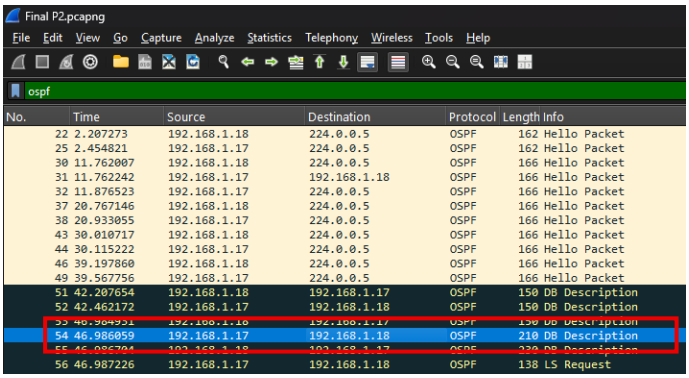

Figure 25 OSPF DBD Phase 2 Packet from Kalam-P2

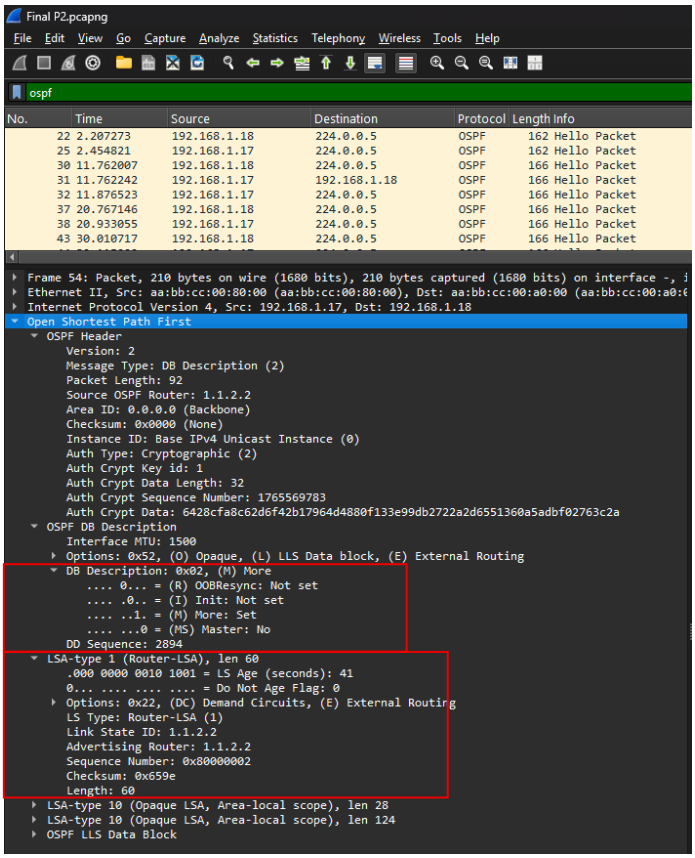

Figure 26 OSPF DBD Phase 2 Packet Inspection from Kalam-P2

For Kalam-P4 both figures below explain the DBD phase 2 packet which have similar information as the Kalam-P2 but with different values such as the source address 192.168.1.18, destination address 192.168.1.17 and the LSA-type 1 header with the link state ID of 1.1.2.4, the source advertising router of 1.1.2.4 and the role of the router which is selected as the master.

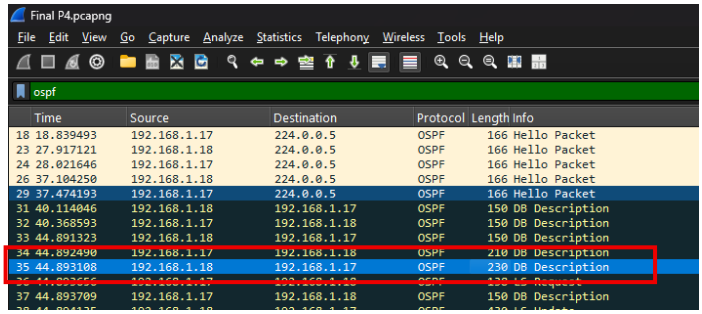

Figure 27 OSPF DBD Phase 2 Packet from Kalam-P4

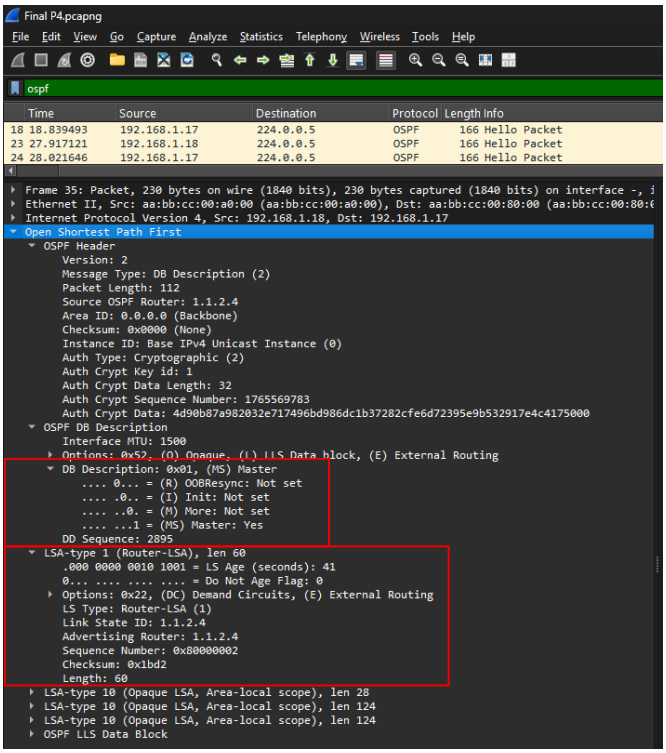

Figure 28 OSPF DBD Phase 2 Packet Inspection from Kalam-P4

OSPF Link State Request (LSR) Packets

After both phases of the DBD has been completed successfully, the router moves on to the Link State Request (LSR) phase to request any missing or outdated LSA entries which has been discovered while was in the DBD packet exchange.

The upcoming figures outlines the LSR packet originating from Kalam-P2 with an IP of 192.168.1.17 to the destination router Kalam-P4 with an IP of 192.168.1.18 to request the full router LSA that has been originated by router ID 1.1.2.4 which either can be from Kalam-P4 as the original originator. In addition, to all the other LSA types such as LSA type 10 (upcoming later).

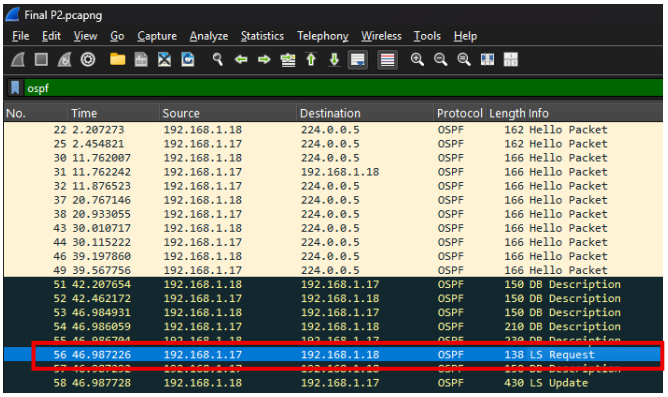

Figure 29 OSPF Link State Request Packet from Kalam-P2 to Kalam-P4

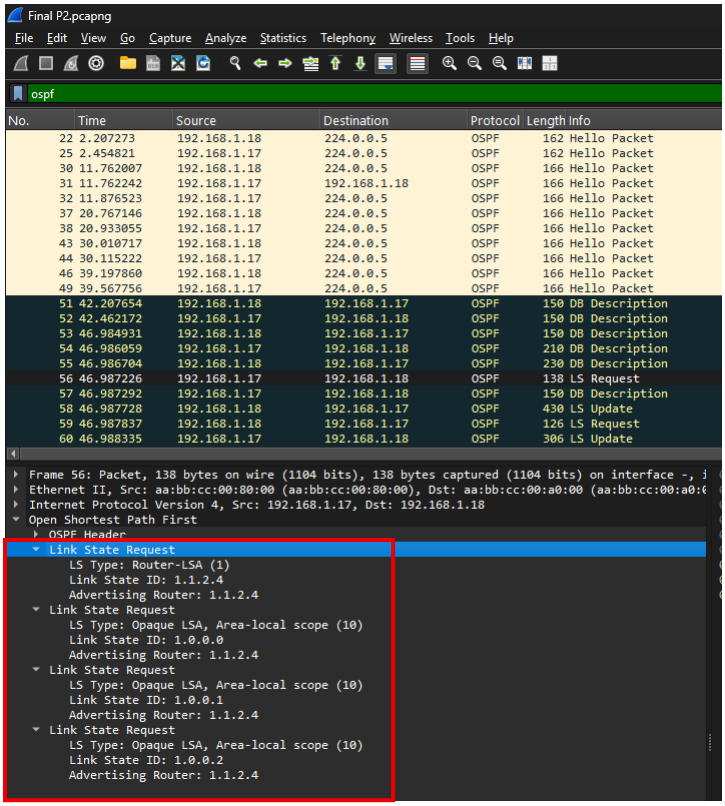

Figure 30 OSPF Link State Request Packet Inspection from Kalam-P2

Kalam-P4 on the other side will send similar LSR packet but with different values to requests all the LSAs that are missing or outdated that either has been originated by Kalam-P2 or Kalam-P2 has received it from another neighbor.

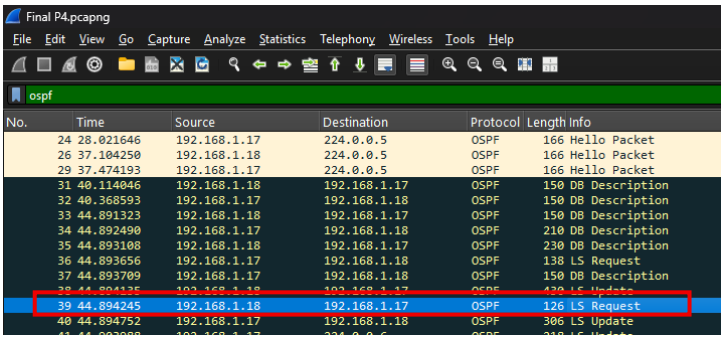

Figure 31 OSPF Link State Request Packet from Kalam-P4 to Kalam-P2

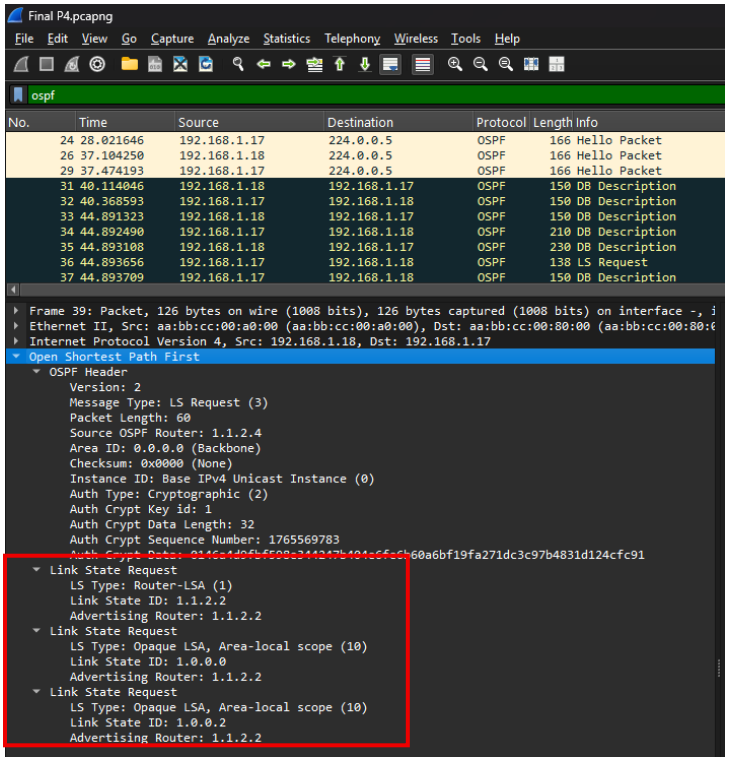

Figure 32 OSPF Link State Request Packet Inspection from Kalam-P4

OSPF Link State Update (LSU) Packets

After the router determine which LSA needs to be updated or retrieved from the neighbor and after the router send a request packet with that information. The Link State Update packets start to be sent to the neighbor who sent the LSR packet to update its LSDB. The LSU packet only exchange the requested LSA from the neighbor router and there is no additional information within the LSU packet.

The figures below will continue upon the previous figures, and they will be reversed in terms of order. Both LSR and LSU are needed to complete each other for the adjacency sequence. These figures will be the response of the LSR that was sent by Kalam-P2 with an IP of 192.168.1.17 to Kalam-P4 with an IP of 192.168.1.18. This packet contains all the IP prefixes that was advertised by Kalam-P4 either directly connected to or the router own interfaces.

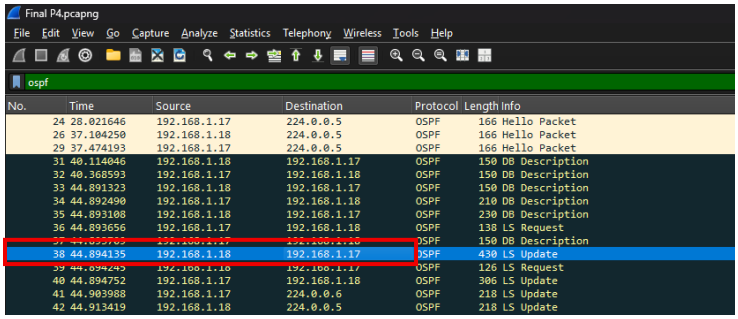

Figure 33 OSPF Link State Update Packet from Kalam-P4 to Kalam-P2

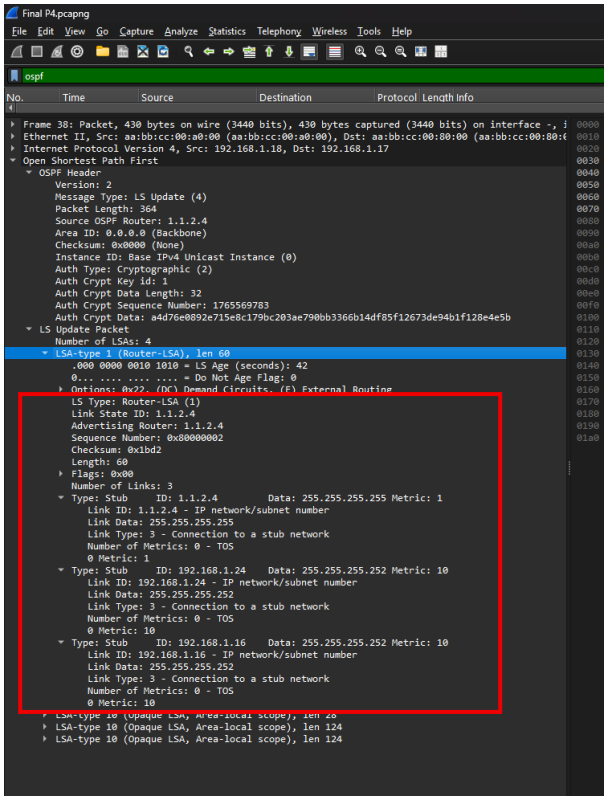

Figure 34 OSPF Link State Update Packet Inspection from Kalam-P4

In the other side, Kalam-P2 also response to the LSR that was originated by Kalam-P4 which has an IP of 192.168.1.18 (Shown in LSR Section above).

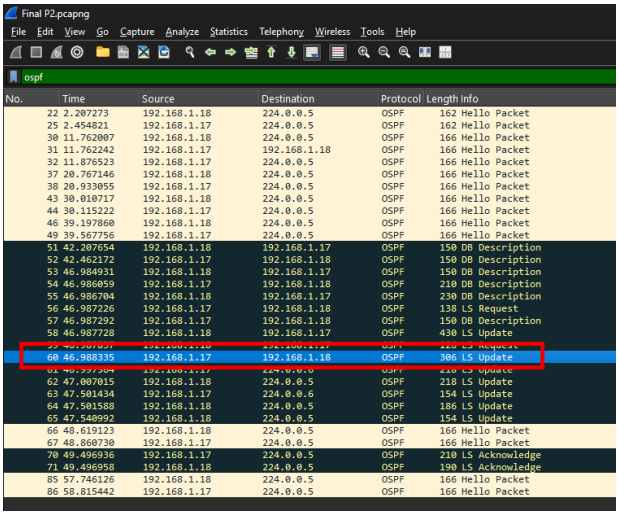

Figure 35 OSPF Link State Update Packet from Kalam-P2 to Kalam-P4

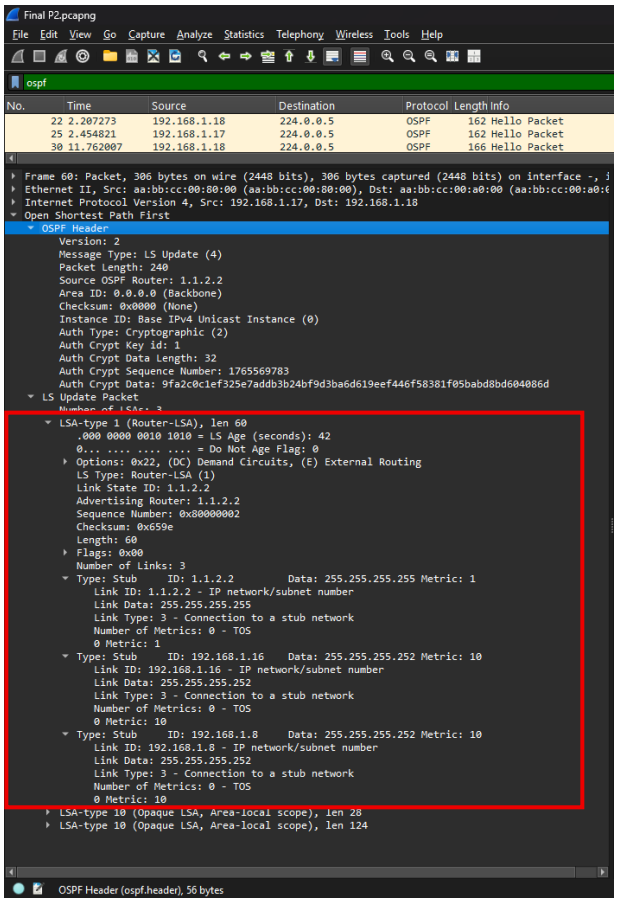

Figure 36 OSPF Link State Update Packet Inspection from Kalam-P2

OSPF Link State Acknowledgement (LSAck) Packets

After both routers receives the requested LSU packets from each other, the Link State Acknowledgement packet are sent to confirm that all the LSU packets received from each other are installed into both routers LSDB. This marks the green light to form the OSPF adjacency with each other.

The next two figures shows the Link State Acknowledgement packet from Kalam-P2 and it content before establishes the OSPF adjacency. The acknowledgement packet that originated from Kalam-P2 includes all the received LSA from the previous LSU that was sent by Kalam-P4 earlier, then Kalam-P2 resends it to Kalam-P4 to informing it that I received and acknowledged your already sent LSU packets.

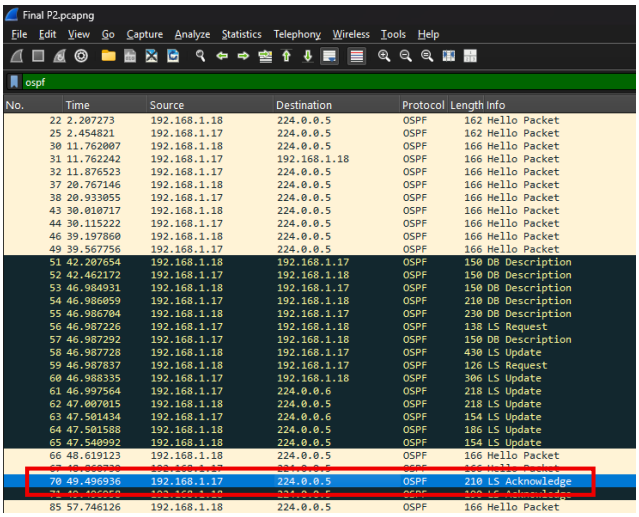

Figure 37 OSPF Link State Acknowledgement Packet from Kalam-P2

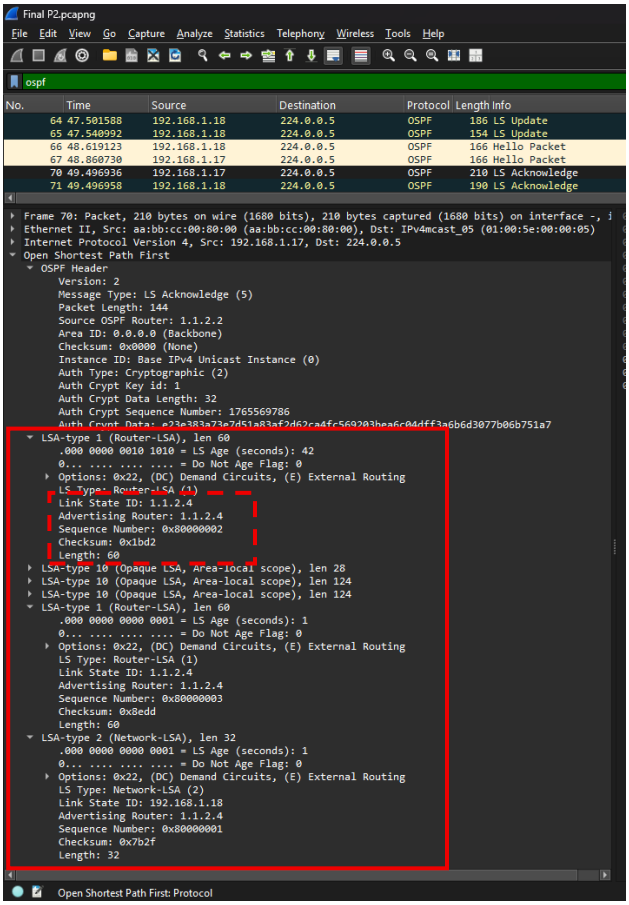

Figure 38 OSPF Link State Acknowledgement Packet Inspection from Kalam-P2

Similarly, Kalam-P4 also sends an acknowledgement packet to the neighboring router. Kalam-P4 will include the LSA information that has been received by the LSU packet from Kalam-P2 into its own acknowledgement packet to inform Kalam-P2 that I Kalam-P4 received the packet and I acknowledge your already sent LSU packet.

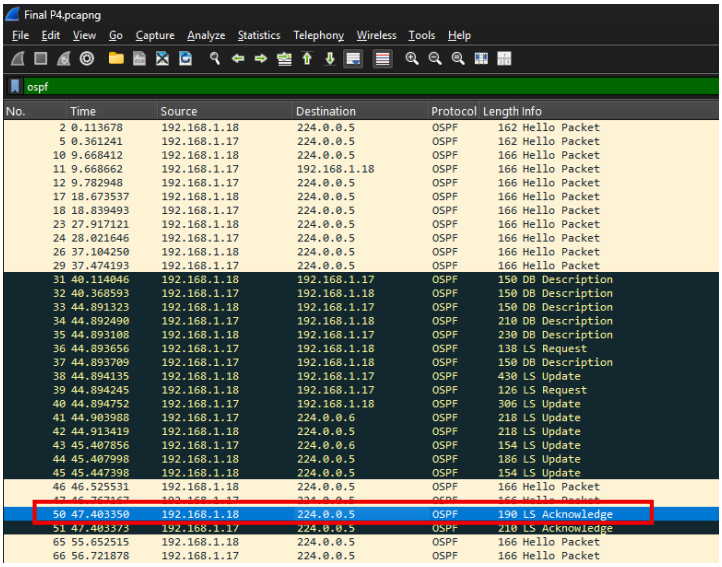

Figure 39 OSPF Link State Acknowledgement Packet from Kalam-P4

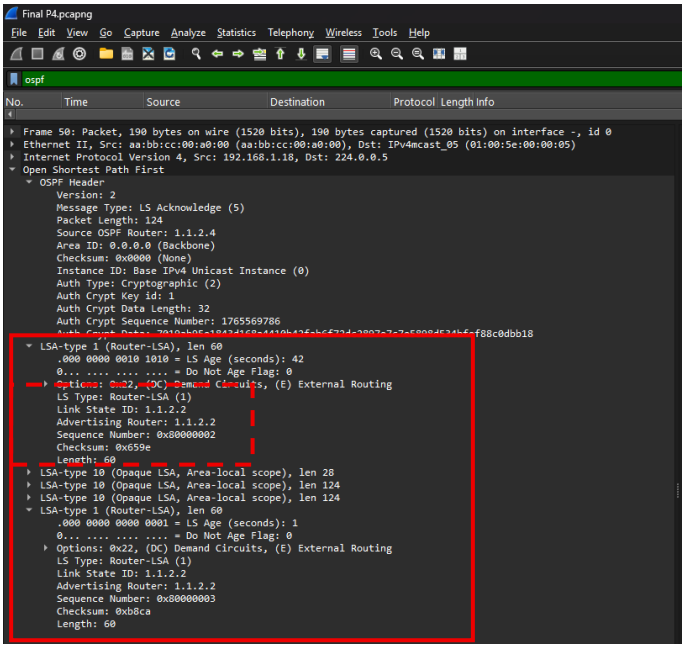

Figure 40 OSPF Link State Acknowledgement Packet Inspection from Kalam-P4

OSPF 5 Routing implementation details:

- Initiate the routing process
- Assigning router ID
- Advertise the network
- Verify neighbor relationship

The figure below shows all the devices that participate in OSPF 5:

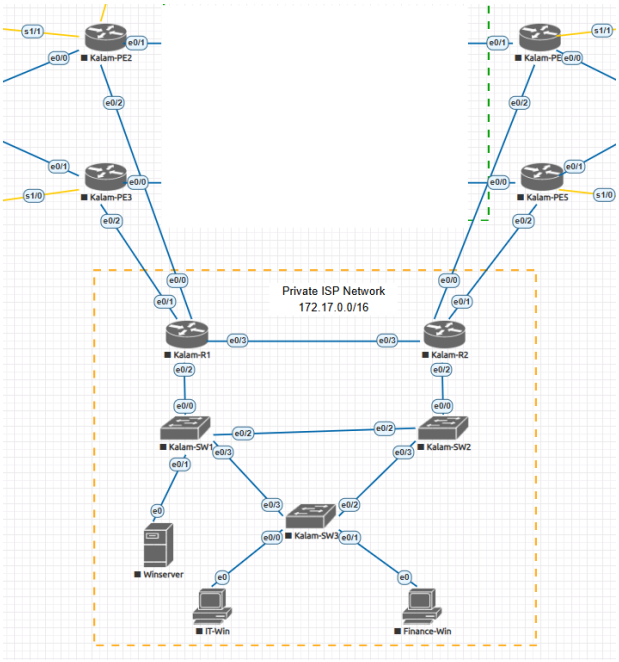

Figure 41 OSPF 5 Devices

OSPF 5 process configuration:

The figures below shows the OSPF process 5 configuration on Kalam-R1, Kalam-R2, Kalam-PE2, Kalam-PE3, Kalam-PE5 and Kalam-PE6. These devices are considered to be from the internal network and edge layer which uses process ID 5 to manage all the routing information between the internal network and the edge inside Kalam Telecom infrastructure.

The router IDs are manually assigned to all the devices under OSPF process 5. Kalam-R1 assigned with 1.1.3.1, Kalam-R2 assigned with 1.1.3.2, Kalam-PE2 assigned with 11.11.11.2, Kalam-PE3 assigned with 11.11.11.3, Kalam-PE5 assigned with 11.11.11.5 and Kalam-PE6 assigned with 11.11.11.6. Furthermore, the network statement is manually added to OSPF 5 to advertise the IP prefix to the neighbors.

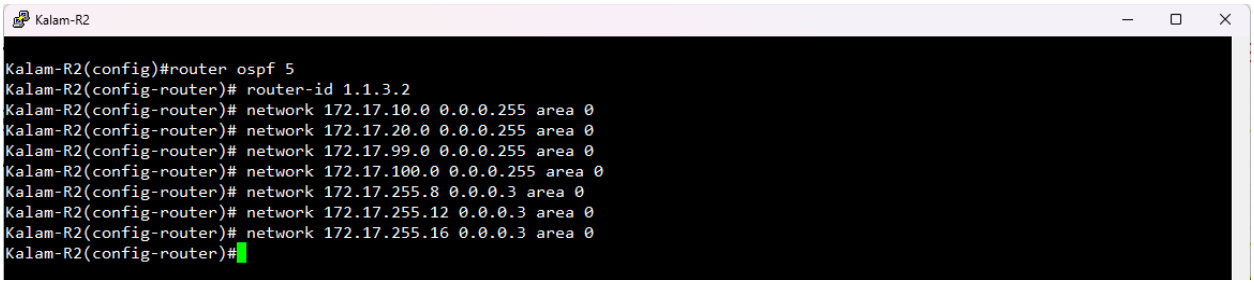

Figure 42 Kalam-R2 OSPF 5 Configuration Commands

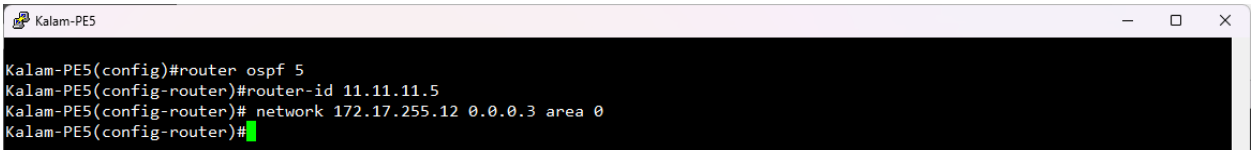

Figure 43 Kalam-PE5 OSPF 5 Configuration Commands

Adjacency verification for OSPF 5:

The next figures shows and outlines the OSPF 5 routing and adjacency between the OSPF process 5 devices.

Note: The verification section contains a different set of routers than those used in the configuration section. This approach is used to show that all routers are successfully forming OSPF adjacencies for the OSPF process 5. For this verification section, the selected routers for are Kalam-R1 and Kalam-PE3.

Based on the output below an OSPF adjacency has been successfully formed between Kalam-R1 and Kalam-PE3 in OSPF process 5. This is verified by the routing table entries that have “O”, which is indicating that the routes are learned via OSPF. As the figures below shows network 172.17.255.12/30 and 172.17.10.0/24 through 172.17.100.0/24, which were configured under

OSPF 5 on Kalam-R2 and Kalam-PE5, are successfully exchanged between the OSPF 5 routers. The prefix 172.17.255.12/30 are visible on the routing table of Kalam-R1 and Kalam-PE3, While the prefixes 172.17.10.0/24 through 172.17.100.0/24 are visible on Kalam-PE3. This confirms that OSPF process 5 is configured correctly.

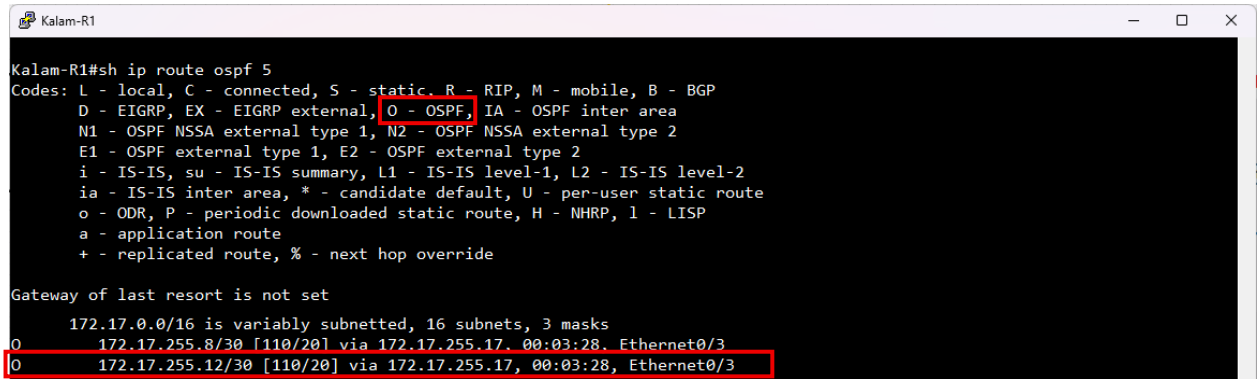

Figure 44 Kalam-R1 OSPF 5 Routing table

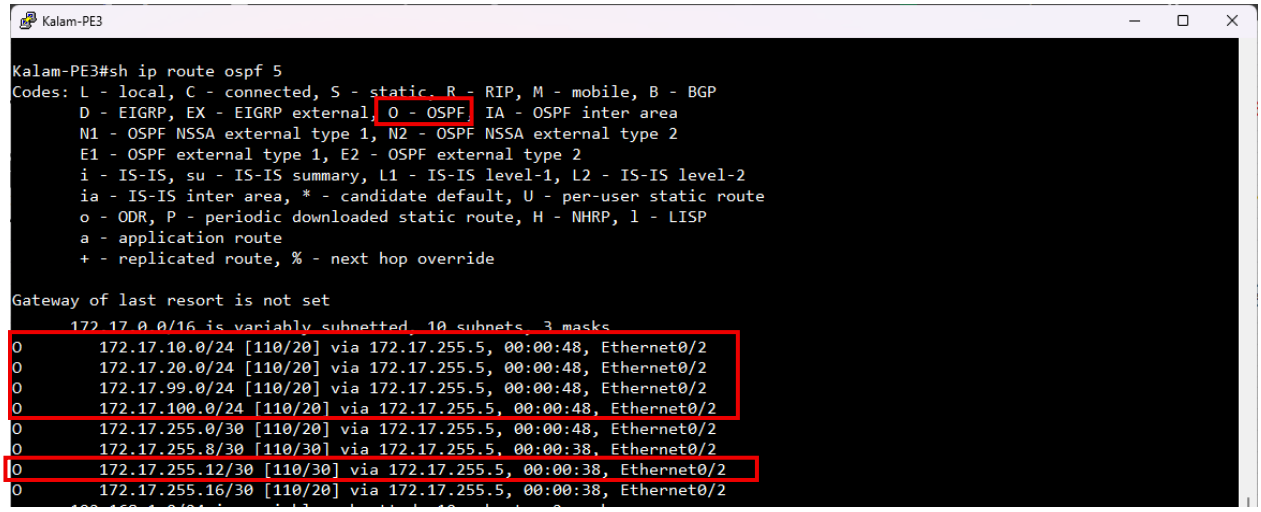

Figure 45 Kalam-PE3 OSPF 5 Routing Table

Redistribution between OSPF 1 and OSPF 5

To bridge the connection between OSPF Process 1 and OSPF Process 5, Route redistribution is configured on a router which have both Process running on it to allow the routers learned in one OSPF process to be advertised into the other. This approach ensures that networks

associated with both Process 1 and Process 5 are reachable across the entire network while still maintaining separate OSPF processes.

The below figures shows the configuration of the redistribution process to bridge both process 1 and process 5. Kalam-PE2, Kalam-PE3, Kalam-PE5 and Kalam-PE6 all of these router have OSPF process running on them, which the redistribution will be configured on all of those 4 routers. The figure will show the Kalam-PE3 configuration only.

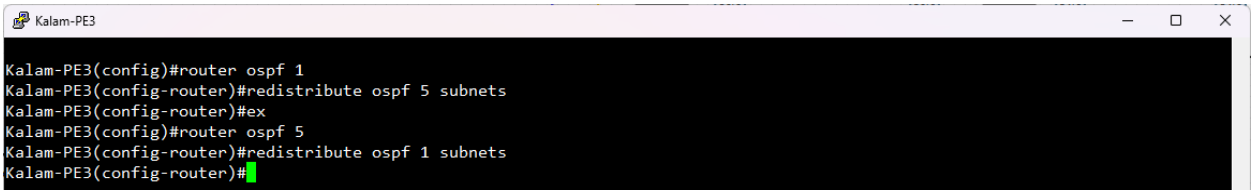

Figure 46 OSPF Redistribution

For the verification section of the redistribution, different sets of routers are used than those used above for the redistribution configuration. This approach ensures that all OSPF routes are visible across any router without any redistribution.

The next two figures will show the redistribution verification process by using the routing table of Kalam-R2 which resides in OSPF process 5 and Kalam-PE1 which resides in OSPF process 1.

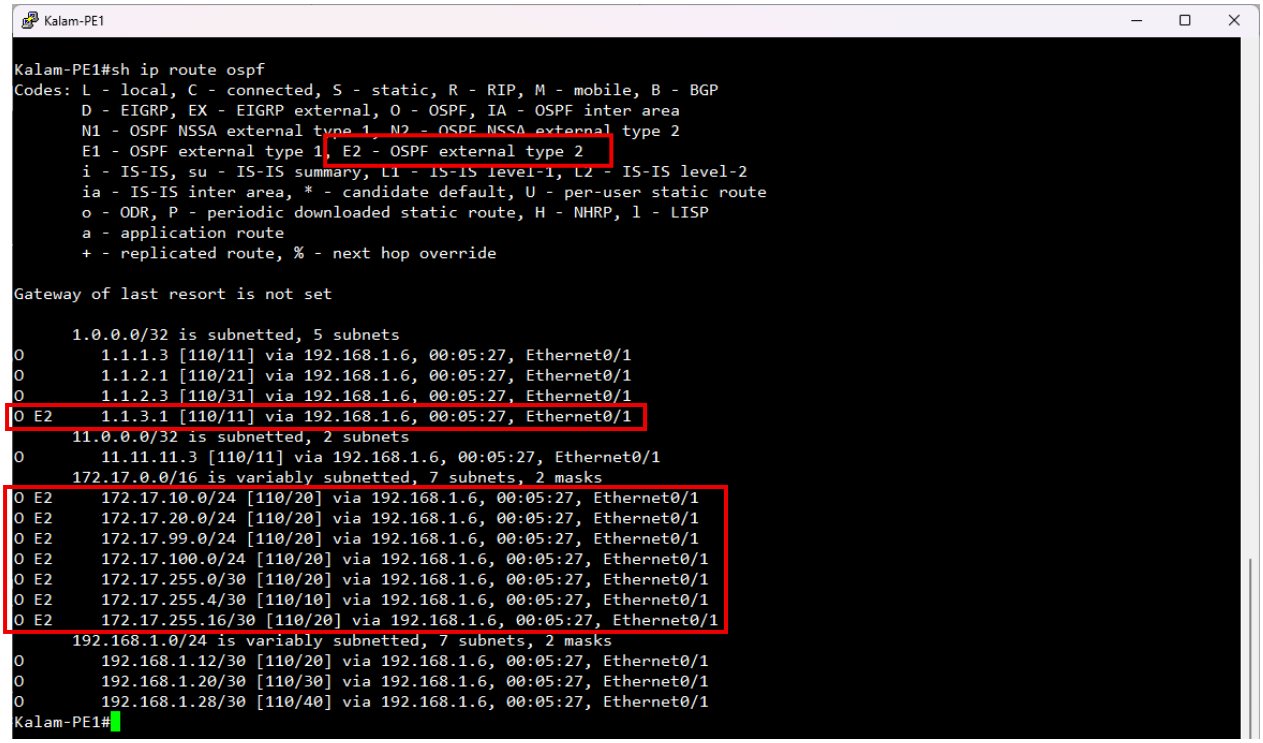

Figure 47 Redistribution Verification from Kalam-PE1

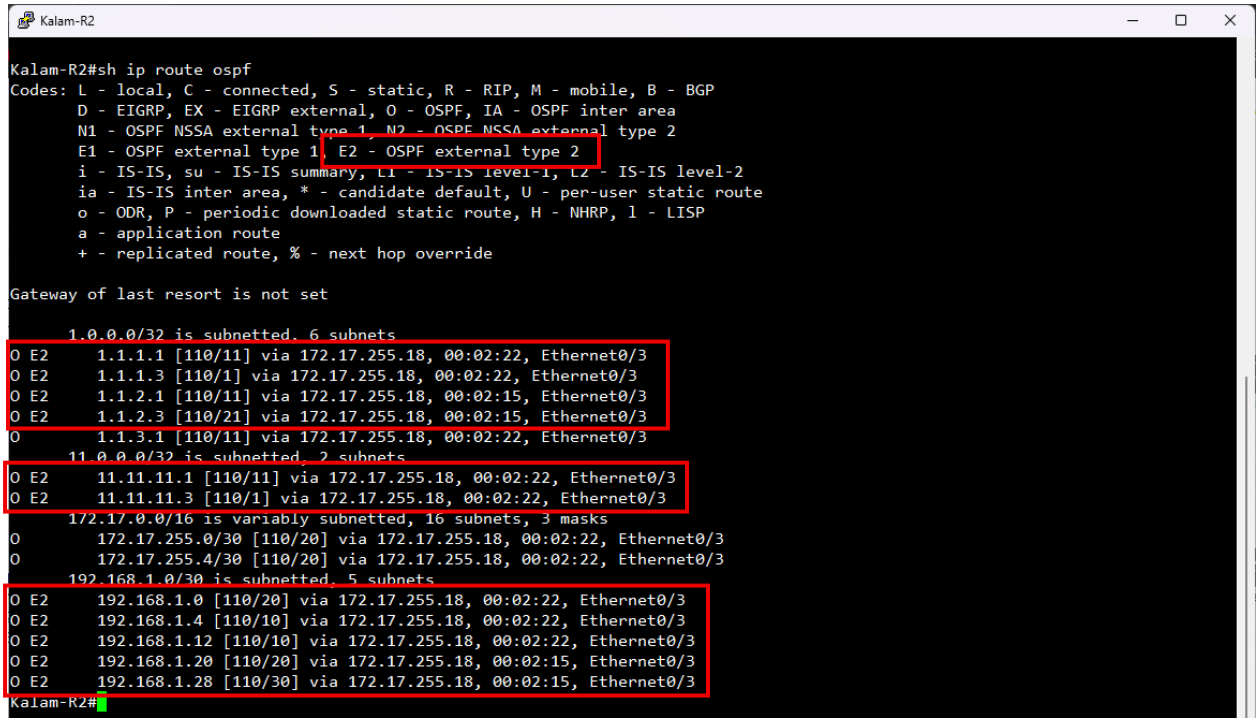

Figure 48 Redistribution Verification from Kalam-R2

Address summarization

To reduce the routing table of the MPLS backbone layer, route summarization is configured to aggregate multiple IP prefixes into a single summarized address. The summarization is applied on the router that participate in both OSPF process 1 and OSPF process 5, allowing the networks 172.17.10.0/24 through 172.17.100.0/24 to be summarized into a single prefix of 172.17.0.0/21.

The upcoming figures shows the configuration of the address summarization to reduce the routing table of MPLS backbone layer. Kalam-PE2, Kalam-PE3, Kalam-PE5 and Kalam-PE6 all of these routers participate in both OSPF process 1 and OSPF process 5, which the summary address will be configured on all of those 4 routers. The figure will show the Kalam-PE6 configuration only. Additionally, the summarization calculation for 172.17.10.0/24, 172.17.20.0/24, 172.17.30.0/24, 172.17.99.0/24 and 172.17.100.0/24 is performed by examining the binary values of these IP addresses to determine the longest common prefix as Illustrated in the below figure. Each one of those IP addresses are converted into its binary representation, then the bits are compared from the left to the right. As you can see the first 17 binary bits are identical across all of the five IP addresses, starting from the 18th bit the binary value varies, this indicates that the prefix 172.17.0.0/17 is the longest summary address of the 5 IP prefixes above.

172.17.10.0	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 1	0 0 0 0 1 0 1 0	0 0 0 0 0 0 0 0
172.17.20.0	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 1	0 0 0 1 0 1 0 0	0 0 0 0 0 0 0 0
172.17.30.0	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 1	0 0 0 1 1 1 1 0	0 0 0 0 0 0 0 0
172.17.99.0	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 1	0 1 1 0 0 0 1 1	0 0 0 0 0 0 0 0
172.17.100.0	1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 1	0 1 1 0 0 1 0 0	0 0 0 0 0 0 0 0
172.17.0.0	172	17	0	0

Figure 49 Route Summarization calculation

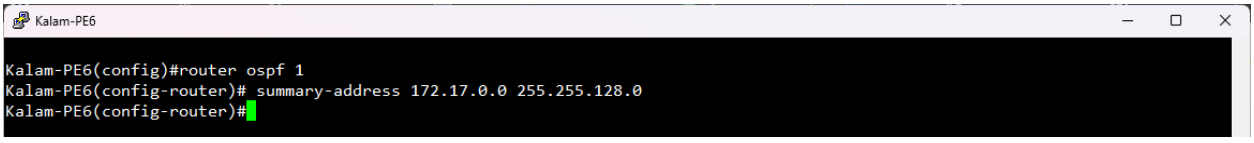

Figure 50 Kalam-PE6 Route Summarization Configuration Command

Address summarization Verification

Note: For the verification of the route summarization, different sets of routers are used than those used above for the summarization configuration. This approach ensures that all summarized OSPF routes are visible across the network.

The next figure will show that the summary address taken place into the MPLS backbone layer to ensures that the routing table does not have so many routes inside it.

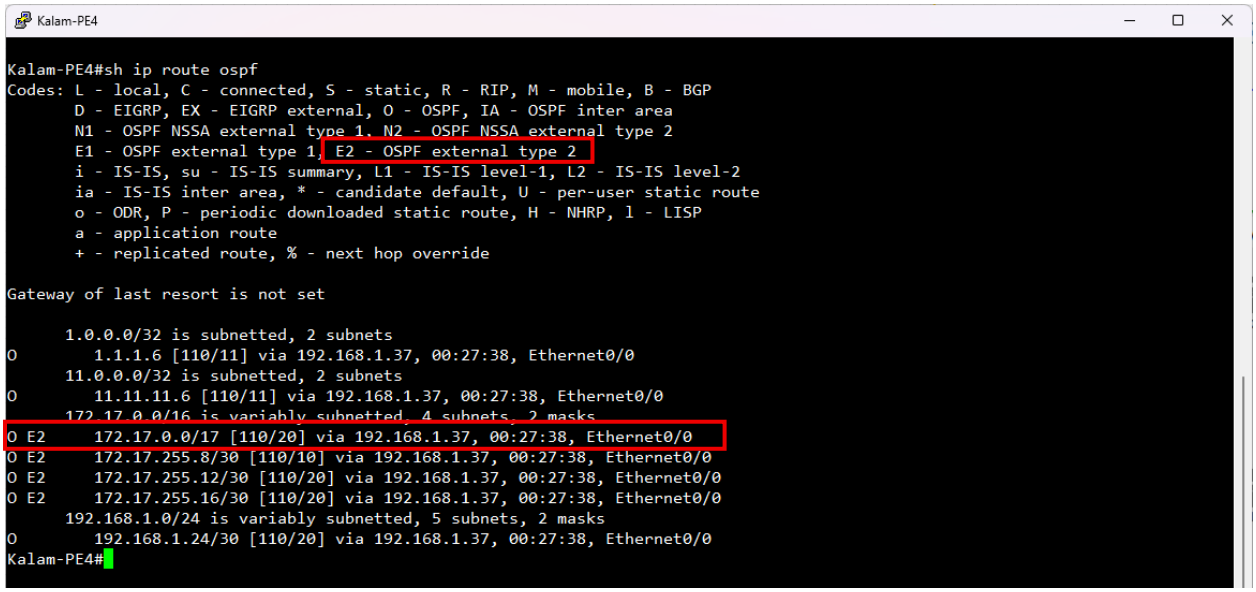

Figure 51 Route Summarization Verification

EIGRP

The EIGRP is mainly applied to the customer facing interfaces to connects the customer to the ISP.

Routing Implementation details:

- Initiate the routing process
- Enter the address family
- Assigning router ID
- Advertise the network
- Verify neighbor relationship

The figure below shows all the devices under EIGRP:

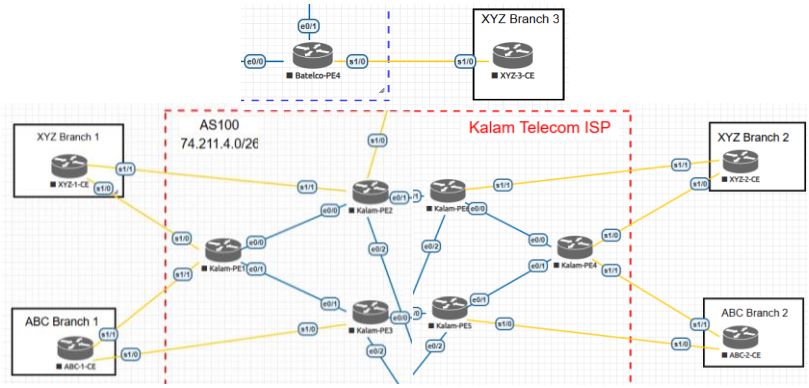

Figure 52 EIGRP Devices

EIGRP process configuration:

The figures below shows the EIGRP process configuration, Kalam-PE1 through Kalam-PE6 are running a named EIGRP with the name of MPLS with two VRF address families (AF), one for ABC company with the AS number of 10 and the second for the XYZ company with the AS number of 20. Moreover, ABC-1-CE and ABC-2-CE are running normal EIGRP process with the AS number of

10 and XYZ-1-CE and XYZ-2-CE are also running normal EIGRP process with AS number of 20. All of these EIGRP processes are mainly used to connects the customer to the ISP MPLS backbone.

The router ID are manually assigned for each router in both of these processes. For the named EIGRP, Kalam-PE1 assigned with 1.1.1.1, Kalam-PE2 assigned with 1.1.1.2, Kalam-PE3 assigned with 1.1.1.3, Kalam-PE4 assigned with 1.1.1.4, Kalam-PE5 assigned with 1.1.1.5 and Kalam-PE6 assigned with 1.1.1.6. The normal EIGRP, ABC-1-CE assigned with 10.10.10.10, ABC-2-CE assigned with 20.20.20.20, XYZ-1-CE assigned with 110.110.110.110 and XYZ-2-CE assigned with 120.120.120.120. Additionally, the Batelco-PE4 assigned with 2.2.2.4 and ABC-3-CE assigned with 130.130.130.130. Furthermore, the EIGRP process has a keychain for each AS, ABC_AuthenKey Specific for AS 10 and XYZ_AuthenKey specific for AS 20 along with a key value and a key string to ensure that the communication line between the ISP and customers are always authenticated before sending and receiving any packets.

Explaining the commands:

- “key chain <chain name>” ⇨ create a key chain.
- “key <value>” ⇨ assign a key value for the key chain.
- “key-string <string>” ⇨ assign the string to be applied on the key chain.
- “af-interface <interface id>” ⇨ points to a specific interface on the EIGRP.
- “authentication mode <type>” ⇨ assign an authentication type.
- “authentication keychain <chain name>” ⇨ assign the key chain to the EIGRP process.
- “network <IP address> <mask>” ⇨ used to advertise a network.
- “eigrp router-id <ID>” ⇨ assign a manual router ID.

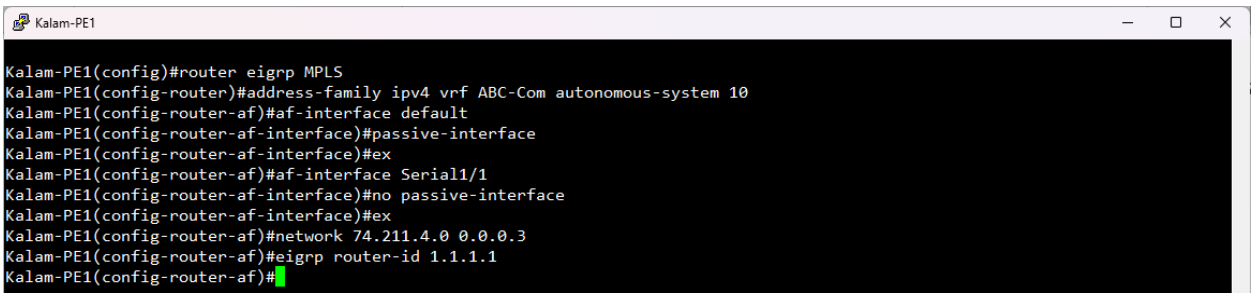

Figure 53 Kalam-PE1 Named EIGRP AF 10 Configuration Commands

Figure 54 Kalam-PE1 Named EIGRP Authentication Configuration Commands for AF 10

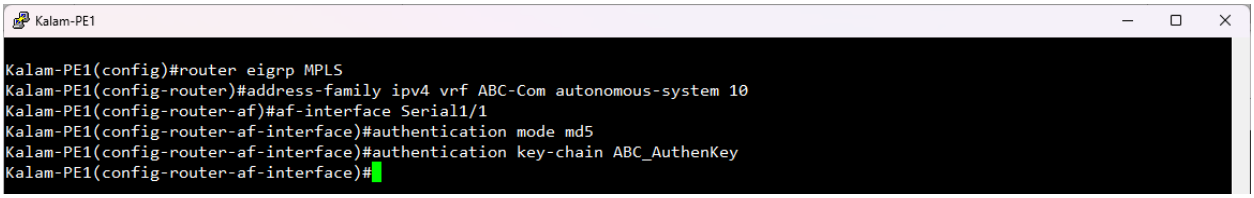

Figure 55 Kalam-PE1 Applying EIGRP Authentication on Named EIGRP AF 10

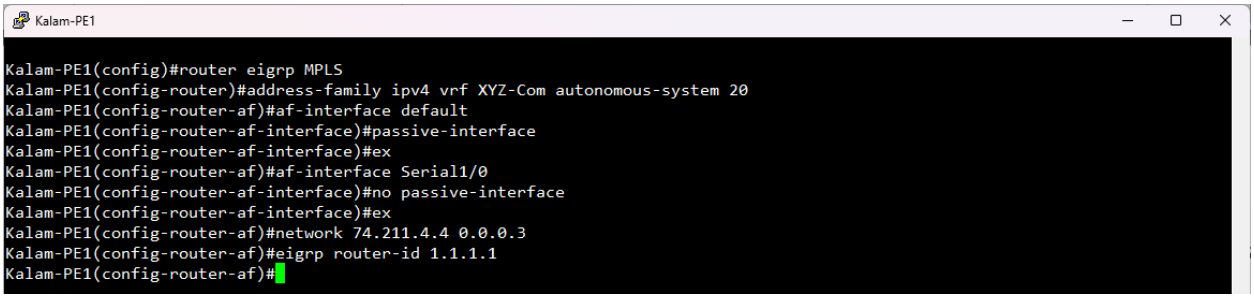

Figure 56 Kalam-PE1 Named EIGRP AF 20 Configuration Commands

Figure 57 Kalam-PE1 Named EIGRP Authentication Configuration Commands for AF 20

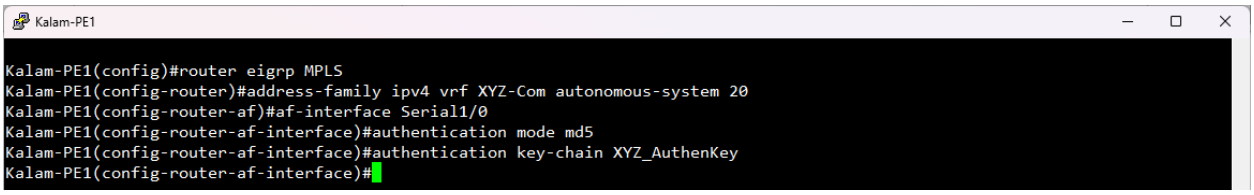

Figure 58 Kalam-PE1 Applying EIGRP Authentication on Named EIGRP AF 20

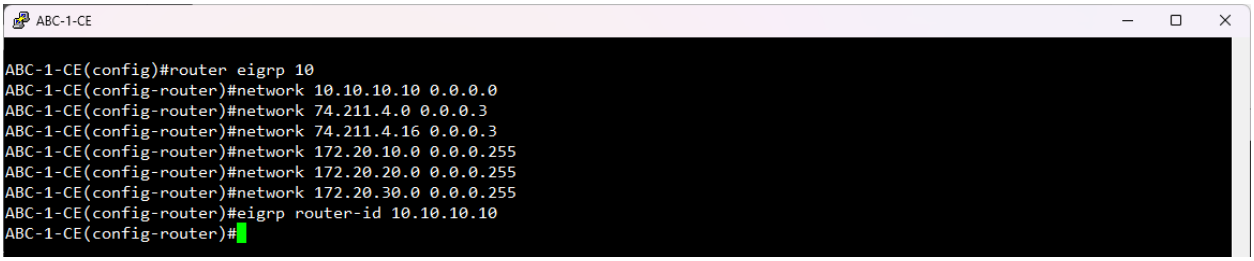

Figure 59 ABC-1-CE Normal EIGRP 10 Configuration Commands

Figure 60 ABC-1-CE Normal EIGRP Authentication Configuration Commands for EIGRP 10

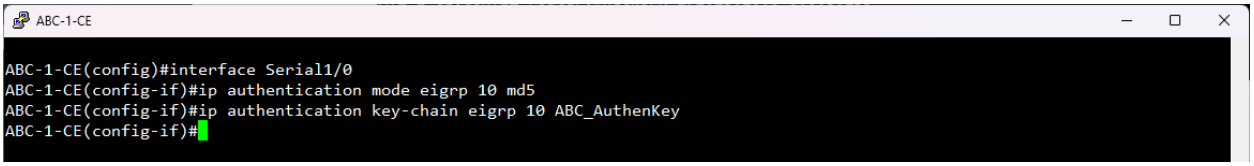

Figure 61 ABC-1-CE Applying EIGRP Authentication on Normal EIGRP 10

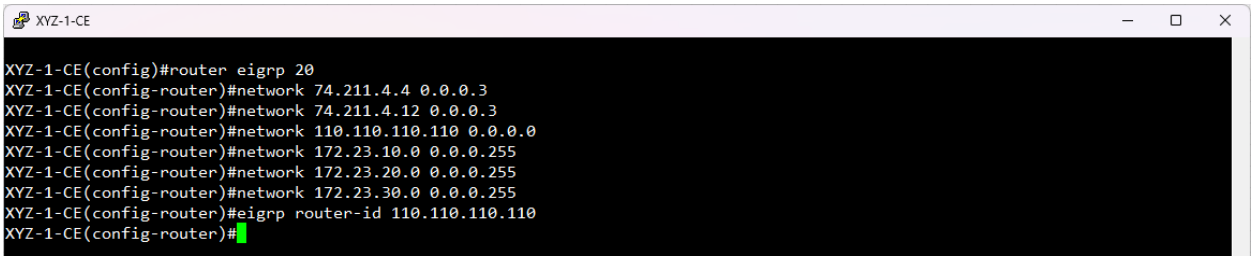

Figure 62 XYZ-1-CE Normal EIGRP 20 Configuration Commands

Figure 63 XYZ-1-CE Normal EIGRP Authentication Configuration Commands for EIGRP 20

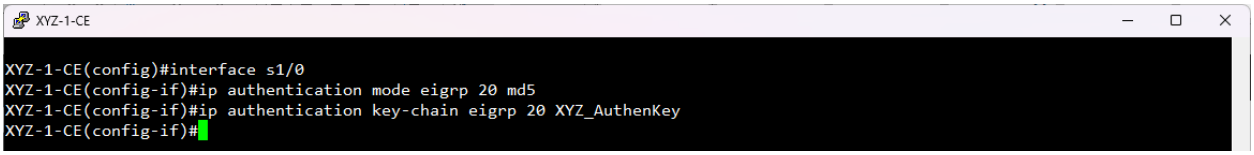

Figure 64 XYZ-1-CE Applying EIGRP Authentication on Normal EIGRP 20

Adjacency verification for EIGRP:

The upcoming figures verifies that the EIGRP has exchanged routing information between Kalam-PE1 and both ABC-1-CE and XYZ-1-CE.

In the routing table each “D” (EIGRP) indicates that the specific route has been learned by EIGRP routing protocol. Additionally, the two numbers shown between the brackets represents the administrative distance (AD) and the EIGRP metric. The AD indicates how trustworthy the

routing protocol is in comparison to the other routing protocol. The AD determines if the routing protocol is used for packet forwarding. The second number is the EIGRP metric which is calculated based on the K-values of the EIGRP and the metric is used as a second decision factor to determine the best path after the AD value has been decided within EIGRP domain. As the routing table figures outlines that the AD for both ASes, AS 10 for ABC-Com and AS 20 for XYZ-Com have a value of 90 and the EIGRP metric is different for each AS depends on the K-values and other parameters. For the AS 10 the EIGRP metric are 1536000 and 3584000. In the other hand the EIGRP metric for AS 20 are 16116062 and 14068062.

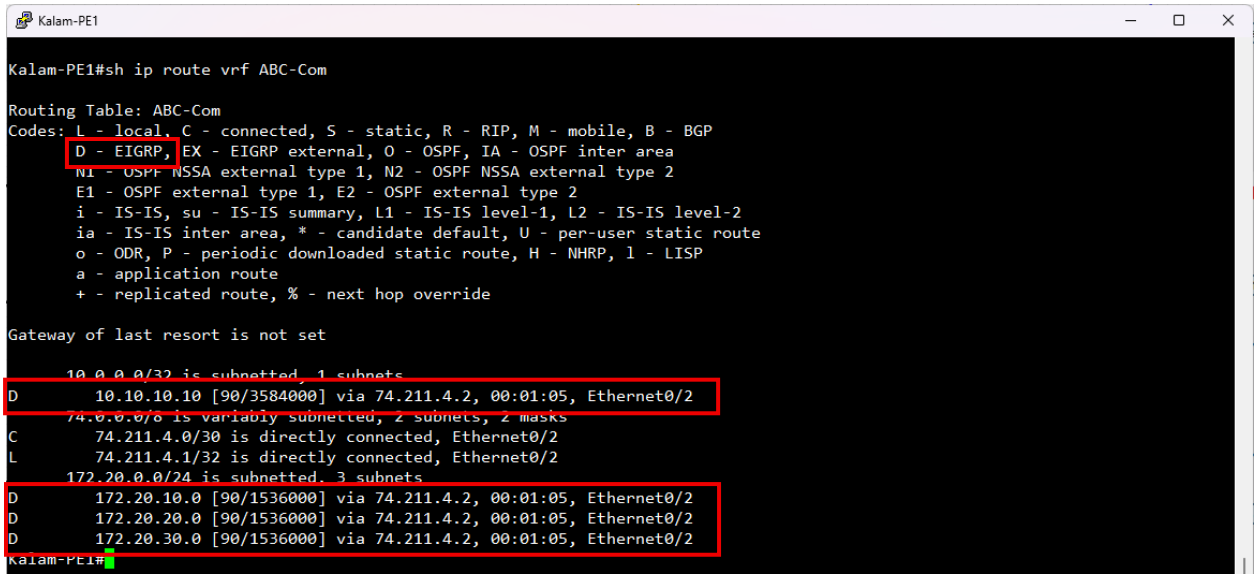

Figure 65 EIGRP AS 10 Routing Table Verification

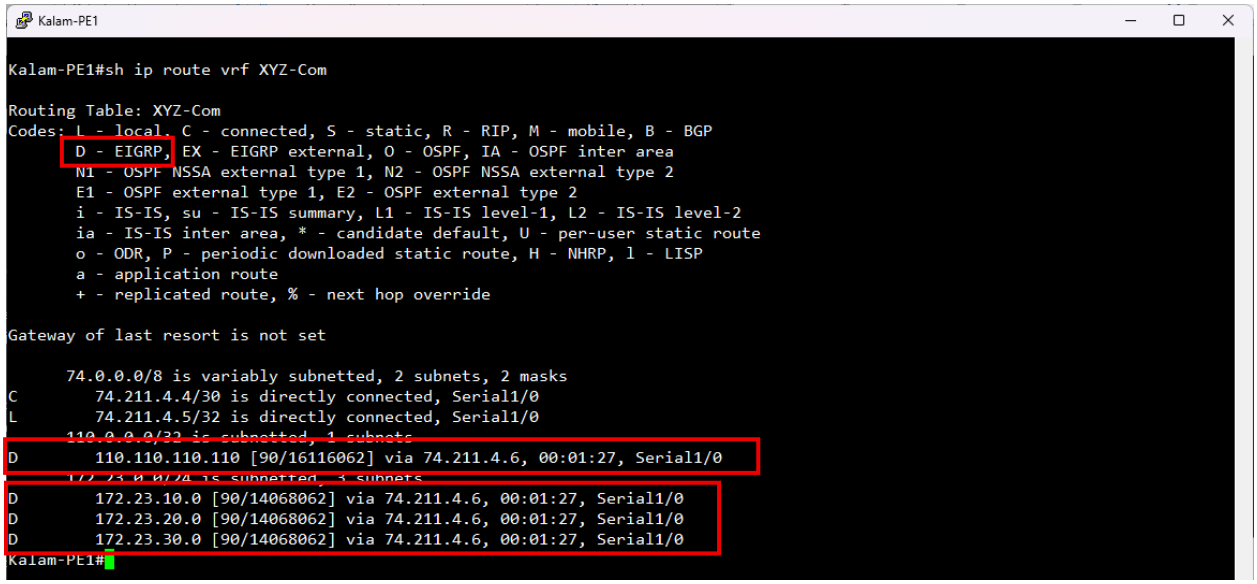

Figure 66 EIGRP AS 20 Routing Table Verification

EIGRP Wireshark Packet Capturing:

The next figures will demonstrate a Wireshark packet capturing for two routers Kalam-PE1 and ABC-1-CE which are involved in EIGRP 10 process, the Kalam-PE1 using Named EIGRP and ABC-1-CE using normal EIGRP.

These figures will explain the packets sent by both Kalam-PE1 and ABC-1-CE which will include a hello packet, update packet, query packet, reply packet and finally the ack packets. All of those packets take a massive part when forming the EIGRP adjacency.

Note: In my topology the query and reply packet are not applicable. Therefore, only the Hello packet, Update packet and Acknowledgement packet are explained below. It should also be noted that multiple packets of the same type were captured for both ABC-1-CE and Kalam-PE1; however, for the sake of time, not all of them are included below.

Hello packets are used to discover EIGRP neighbors and verify and the required parameters before forming a neighbor relationship. These parameters include the AS number, K-values and the authentication setting if configured. One neighbor relationship is established. Update packets are exchanged to advertise the routing information and allow each other networks to

be reachable from one another. If router loses a route for the neighboring network. A Query packet is sent to the neighboring router to request an alternative route. When the neighboring router response to the query packet, it sends a replay packet indicating whether there is an alternative route to that specific destination or not. The acknowledgement packets are sent to confirms the successful receipt of update, query and replay packets.

EIGRP Hello Packets

The figures below shows that Kalam-PE1 sends a Hello Packet with the source address of 74.211.4.1 to the destination address 224.0.0.10 which represents the multicast address for all EIGRP router that runs AS 10. For the layer 3 header of Hello Packet, it also shows that the source address and the destination address in addition to the protocol name and port. Additionally, the EIGRP header of this Hello Packet shows the sequence number, which is 0, similarly acknowledgement number is also a 0, the autonomous system number, which is 10, time to live and the holding timer in their default values in addition to the authentication method with it is parameters such as the Key ID, length and type. Finally, it also mention the K-values which is important to form adjacencies and the opcode value of “Hello” which indicate that this is a hello packet.

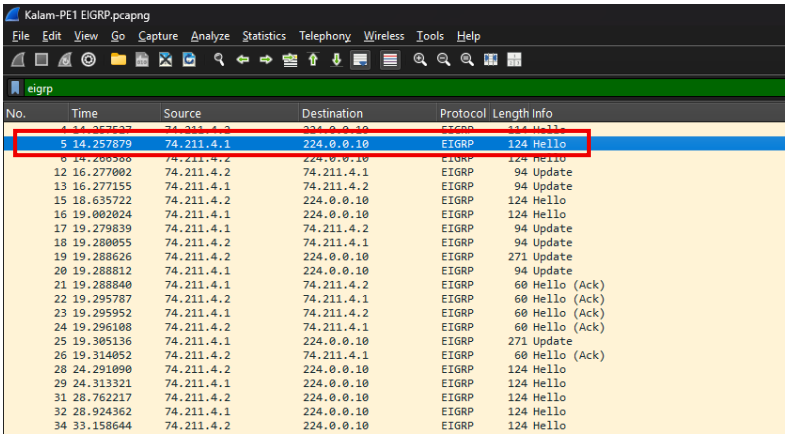

Figure 67 Kalam-PE1 EIGRP Hello Packet

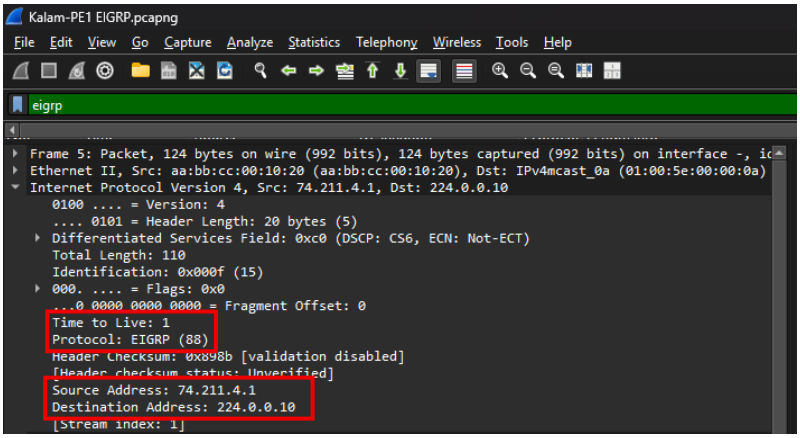

Figure 68 Kalam-PE1 EIGRP Hello Packet Layer 3 Header Inspection

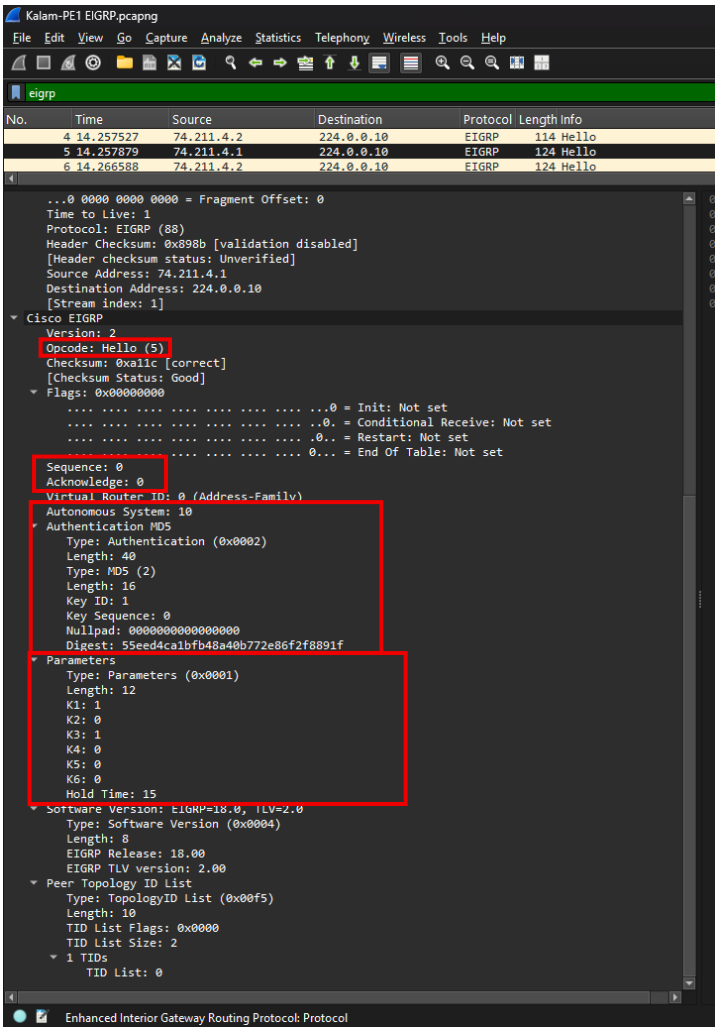

Figure 69 Kalam-PE1 EIGRP Hello Packet EIGRP header Inspection

In the other hand, ABC-1-CE also sends a EIGRP hello packets but with different values such as source address of 74.211.4.2 and a destination address of 224.0.0.10. similarly to Kalam-PE1. For the layer 3 header of ABC-1-CE hello packet it also show similar values such as the source, destination addresses and protocol port number. Additionally, the EIGRP header for ABC-1-CE has similar output to Kalam-PE1 which include the sequence, acknowledgement and the k-values in addition to the opcode.

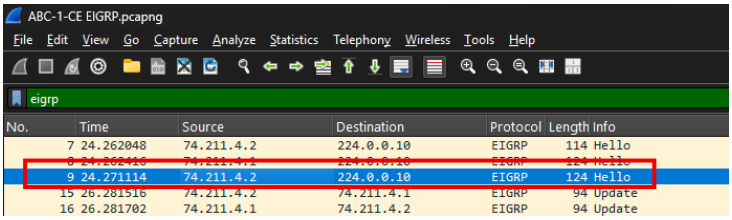

Figure 70 ABC-1-CE EIGRP Hello Packet

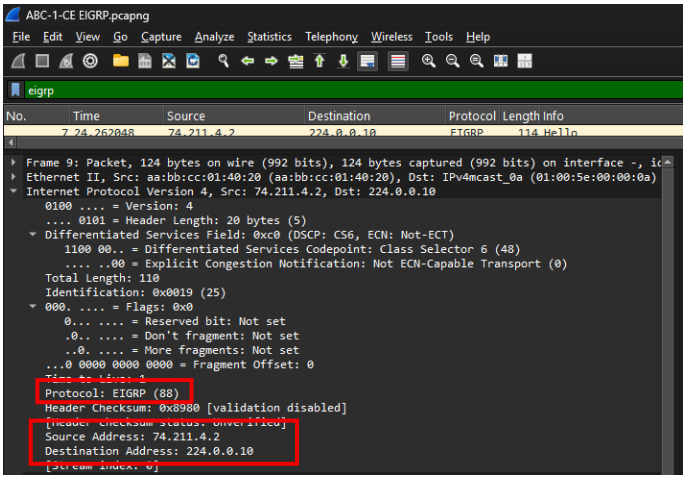

Figure 71 ABC-1-CE EIGRP Hello Packet Layer 3 Header Inspection

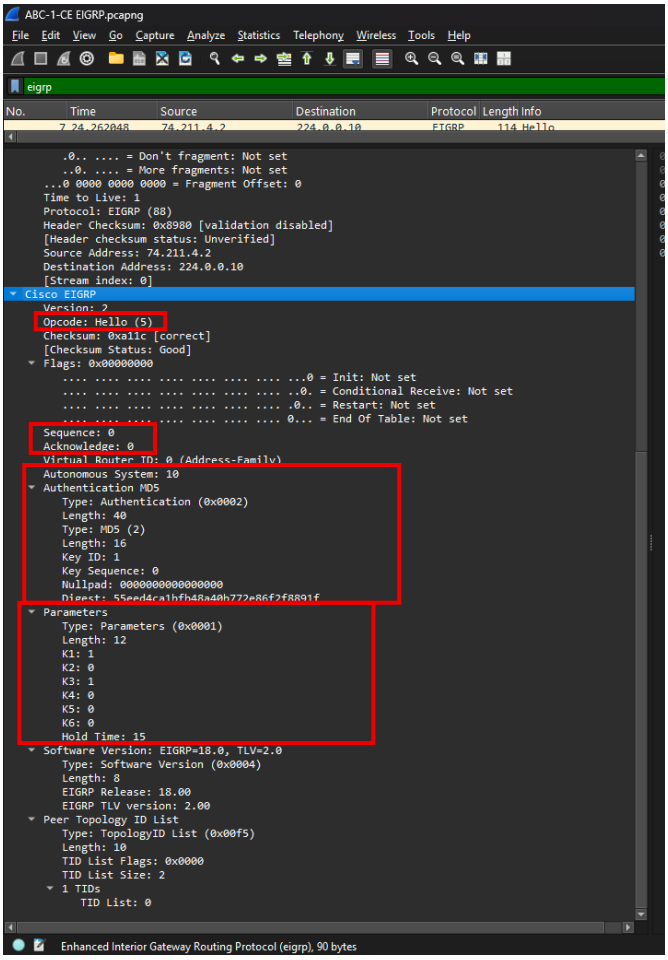

Figure 72 ABC-1-CE EIGRP Hello Packet EIGRP header Inspection

EIGRP Update Packets

After the Hello packets are exchanged and the necessary parameters has been checked and matched, the Update packets are sent to exchange and advertise the routing information between the routing neighbors.

The upcoming figures shows that the update packets are being exchanged. The inspection of Kalam-PE1 update packet shows a source address of 74.211.4.1 and a destination address of 74.211.4.2 this time the connection is a unicast indicating that this is a response of the previous hello packets. When it comes to the Layer 3 header it contains the normal layer 3 values such as the source and destination addresses similarly to the previous figures and examples. However, the EIGRP header for this update packet is a little bit different than the hello packets as the figure shows that the opcode value of this packet is an update and not a hello that mean that this packet is 100% an update packet, also the sequence number has been incremented by 1 indicating that this packet is not the first packet between those neighbors. Additionally, the flags section play an important role in the update packet as well as the other types of packet, as the figure illustrate that the flags section has the init sub-flag with the value “Set” which mean that this is the packet that marks the beginning of routing information exchange which will lead to an adjacency being established later.

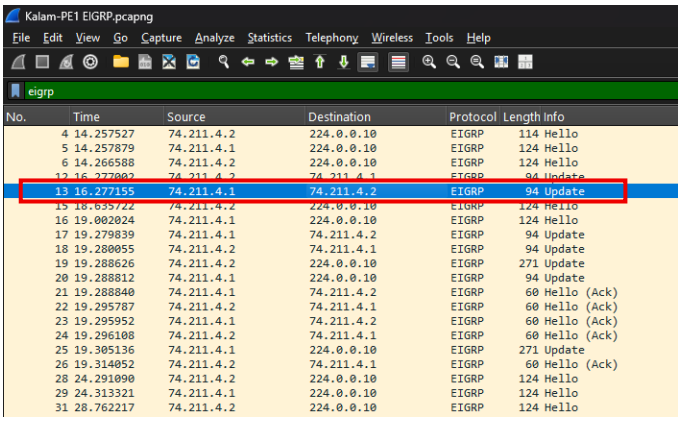

Figure 73 Kalam-PE1 EIGRP Update Packet

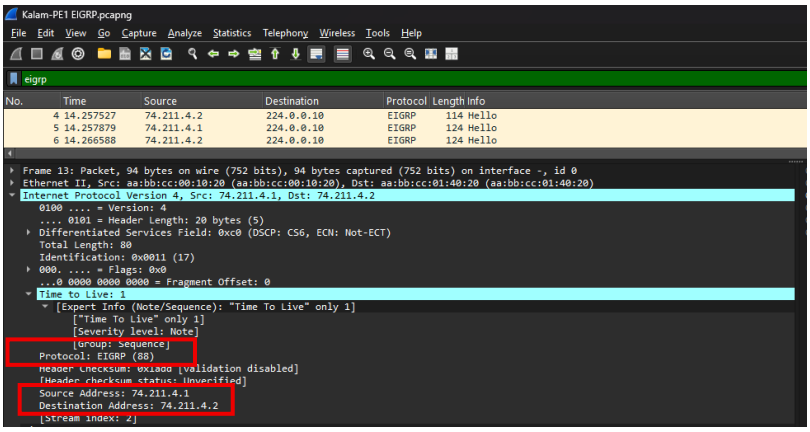

Figure 74 Kalam-PE1 EIGRP Update Packet Layer 3 Header Inspection

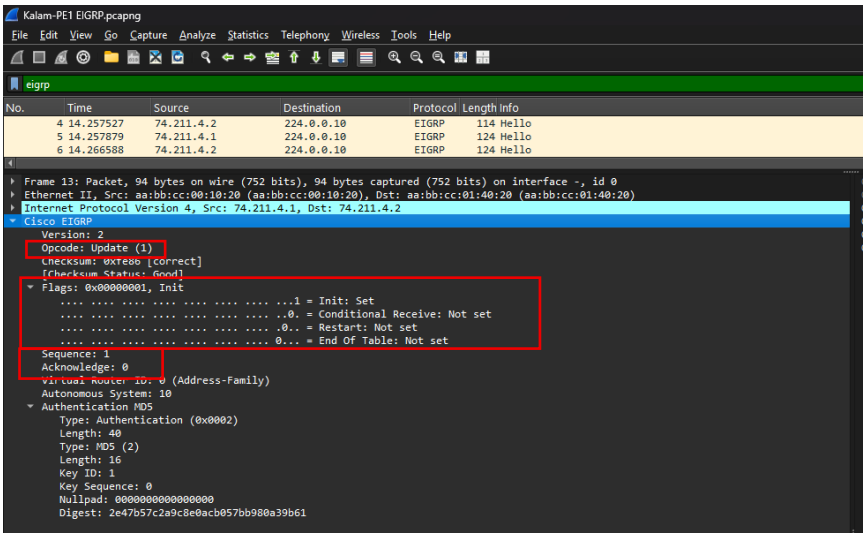

Figure 75 Kalam-PE1 EIGRP Update Packet EIGRP Header Inspection

On the other side of this packet exchange process, ABC-1-CE also sends an update packet for Kalam-PE1 with a source of 74.211.4.2 and a destination of 74.211.4.1, in addition to all the other values such as the time to live in the layer 3 header. In addition to the layer 3 header information, we also have the EIGRP header information and similar to what has been explained in Kalam-PE1 update packet EIGRP header, all the values are similar since this packet is an update packet for Kalam-PE1 hello packets. For both router these packets marks the beginning of adjacency formation.

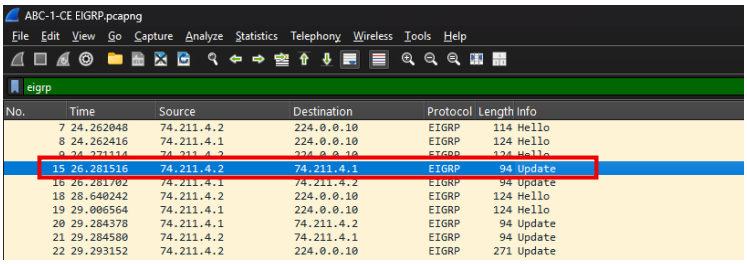

Figure 76 ABC-1-CE EIGRP Update Packet

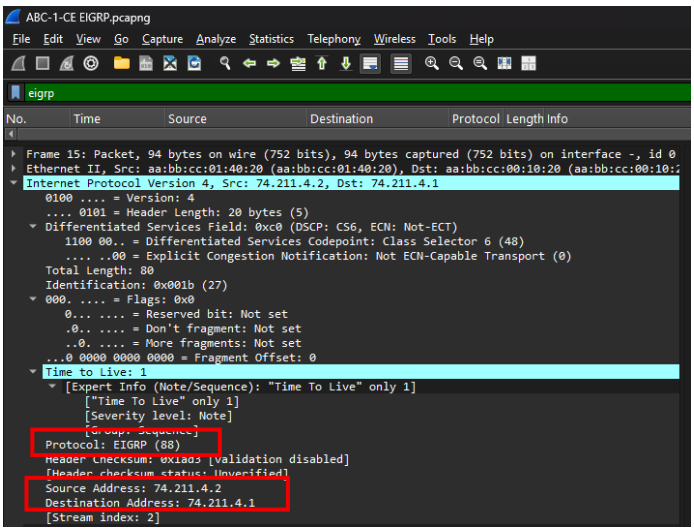

Figure 77 ABC-1-CE EIGRP Update Packet Layer 3 Header Inspection

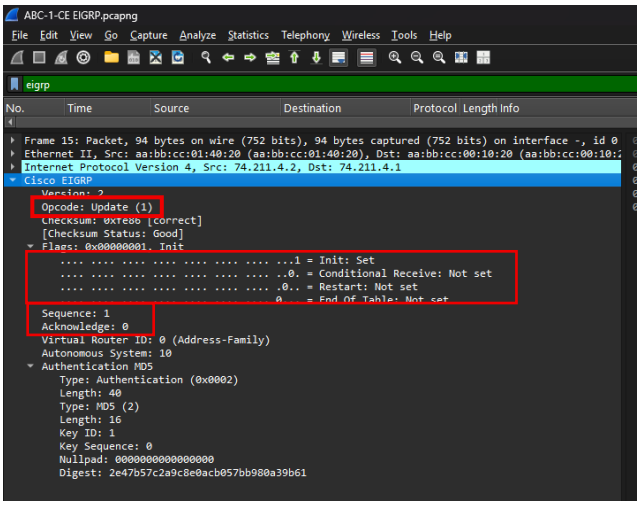

Figure 78 ABC-1-CE EIGRP Update Packet EIGRP Header Inspection

EIGRP Acknowledgement packets

After the update packets are exchanged alongside with the initial routing information. The acknowledgement packet comes in place to verifies that each neighboring router has received the update packet successfully.

The upcoming figures demonstrate and inspects the acknowledgement packets in the EIGRP packet exchange process. The inspection of the Kalam-PE1 acknowledgement packet shows the usual information such as the source address 74.211.4.1, destination address 74.211.1.2, protocol name and number EIGRP, number 88. In addition to the information presented in the layer 3 header. The EIGRP header shows limited amount of information since it just an acknowledgement packet as the figure show that the EIGRP header only show the opcode and the acknowledgement values of 1 and sequence value of 0 which indicates that this packet is an acknowledgement packet and not a hello packet.

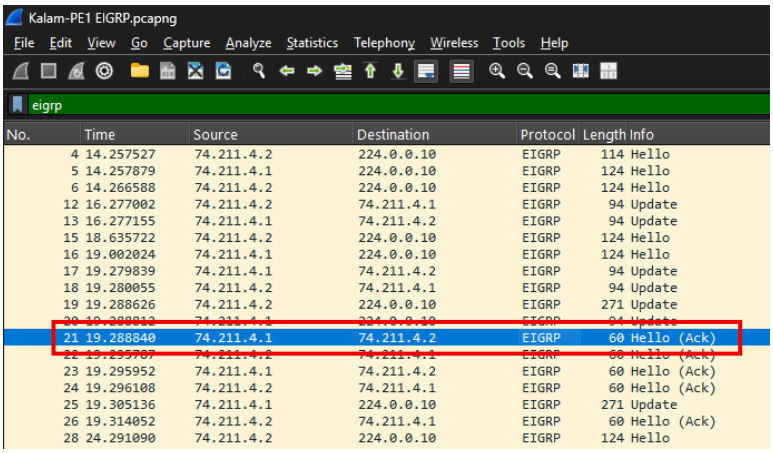

Figure 79 Kalam-PE1 EIGRP Acknowledgement Packet

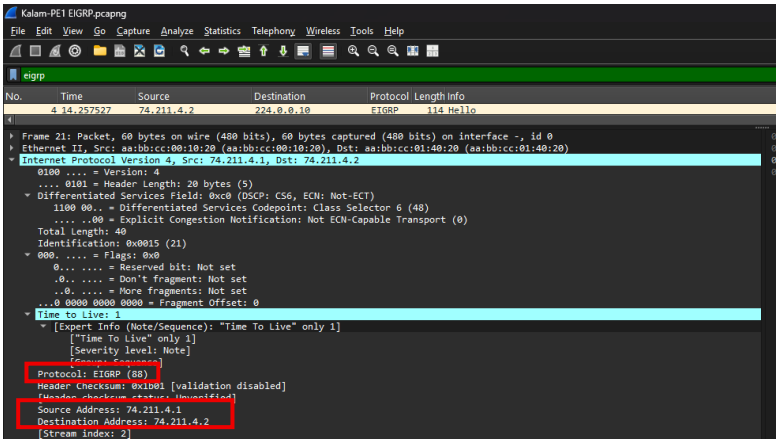

Figure 80 Kalam-PE1 EIGRP Acknowledgment Packet Layer Header 3 Inspection

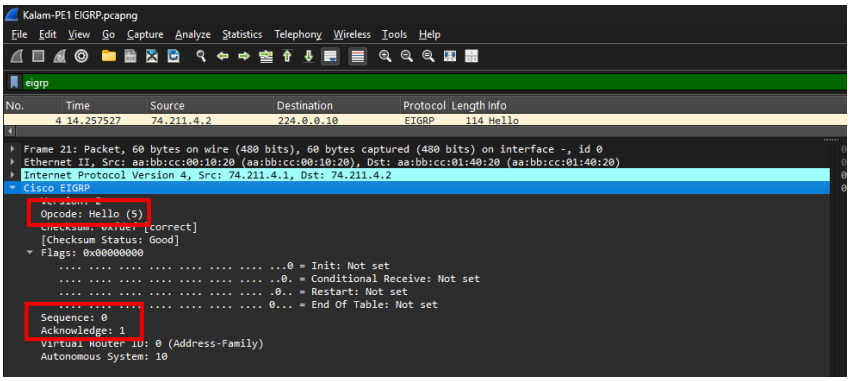

Figure 81 Kalam-PE1 EIGRP Acknowledgment Packet EIGRP Header Inspection

On the other side of this EIGRP process, ABC-1-CE also sends an acknowledgement packet to inform Kalam-PE1 of a successful receipt of its packets. The below figures show exactly the same structure with different values.

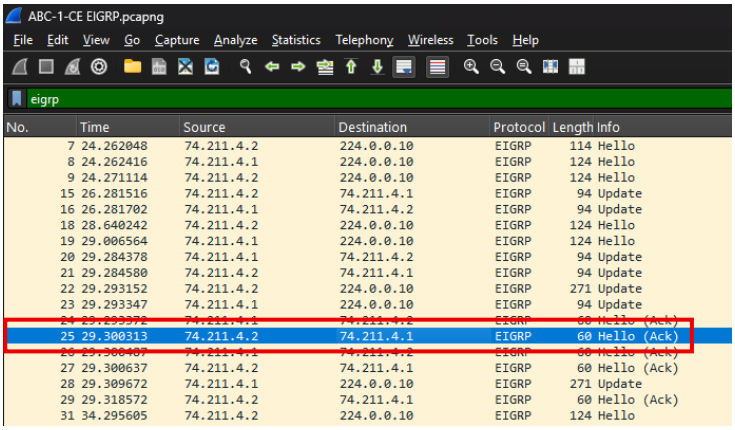

Figure 82 ABC-1-CE EIGRP Acknowledgment Packet

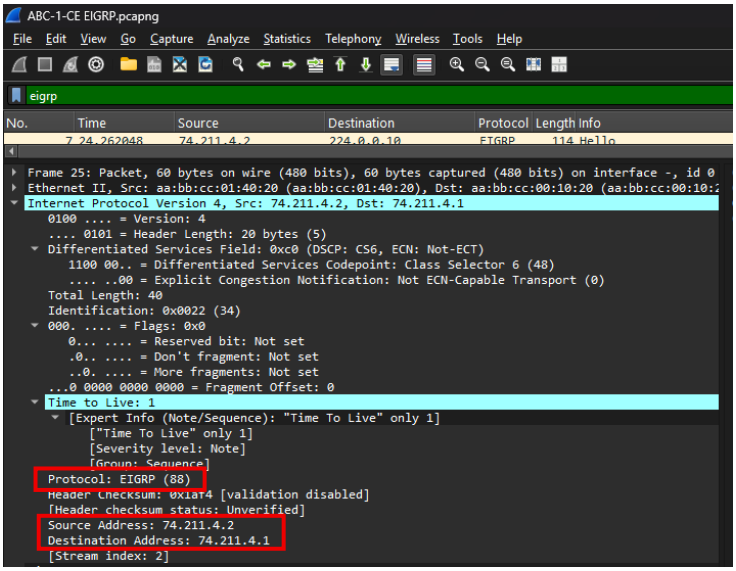

Figure 83 ABC-1-CE EIGRP Acknowledgment Packet Layer Header 3 Inspection

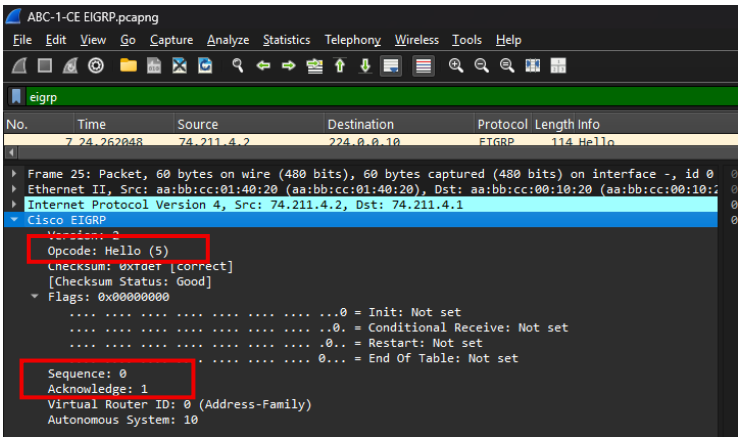

Figure 84 ABC-1-CE EIGRP Acknowledgment Packet EIGRP Header Inspection

BGP

The BGP is mainly used to connects the ISP network to the neighboring ISP networks. MP-BGP is mainly used to carry the customer routes between the ISPs internal routers.

Routing Implementation details:

- Initiate the routing process
- Enter the address family
- Assigning router ID
- Advertise the network
- Verify neighbor relationship

The figure below shows all devices under the BGP:

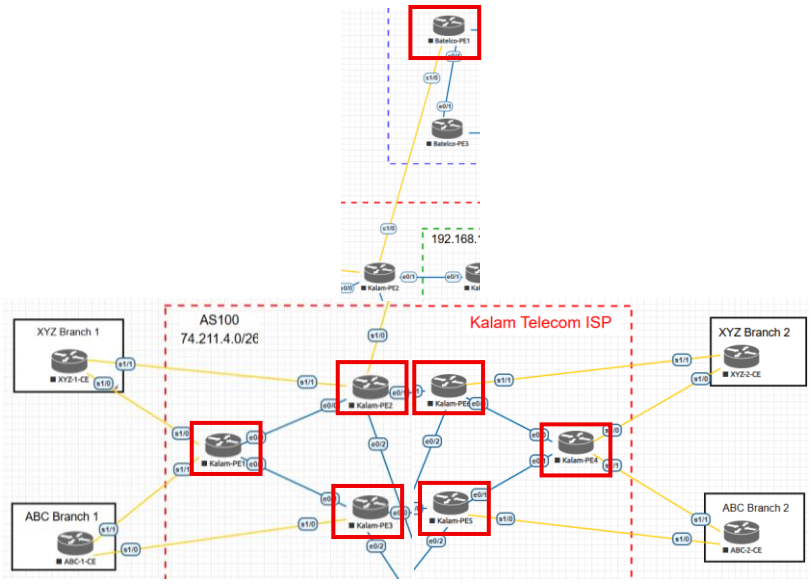

Figure 85 BGP Devices

BGP process configuration:

The figure below shows the BGP process 100 configuration on Kalam-PE1, Kalam-PE2, Kalam-PE3, Kalam-PE4, Kalam-PE5 and Kalam-PE6. All these devices are considered to be the main

component that transfer the customer labels inside the ISP. BGP protocol is suitable for this position due to it has the capability to transfer customer vrf inside the ISP.

The BGP router IDs are assigned manually to Kalam-PE1 have 1.1.1.1 as the ID, Kalam-PE2 have 1.1.1.2 as the ID, Kalam-PE3 have 1.1.1.3 as the ID, Kalam-PE4 have 1.1.1.4 as the ID, Kalam-PE5 have 1.1.1.5 as the ID and Kalam-PE6 have 1.1.1.6 as the ID. In addition, the process of automatic adjacency has been changed to disabled by using the “no bgp default ipv4-unicast” to ensure what neighbor should have an adjacency. The establishment of the neighbor relationship configured manually by using the command “neighbor <ip address> remote-as <neighbor AS>” and the source of the interface also has been configured manually by the “update-source” command. Furthermore, the activation of the adjacency is also configured manually by using the “neighbor <ip address> activate”.

Explaining the commands:

- “no bgp default ipv4-default” ⇨ disable the automatic adjacency.
- “bgp router-id <ID>” ⇨ assign a manual ID.
- “neighbor <neighbor IP> remote-as < neighbor AS number>” ⇨ identifies the BGP neighbor and its AS number.
- “neighbor <neighbor IP> update-source <interface ID>” ⇨ This command tells BGP to use a specific interface as the source of BGP updates.
- “neighbor <neighbor IP> activate” ⇨ activate and enables the BGP neighbor.

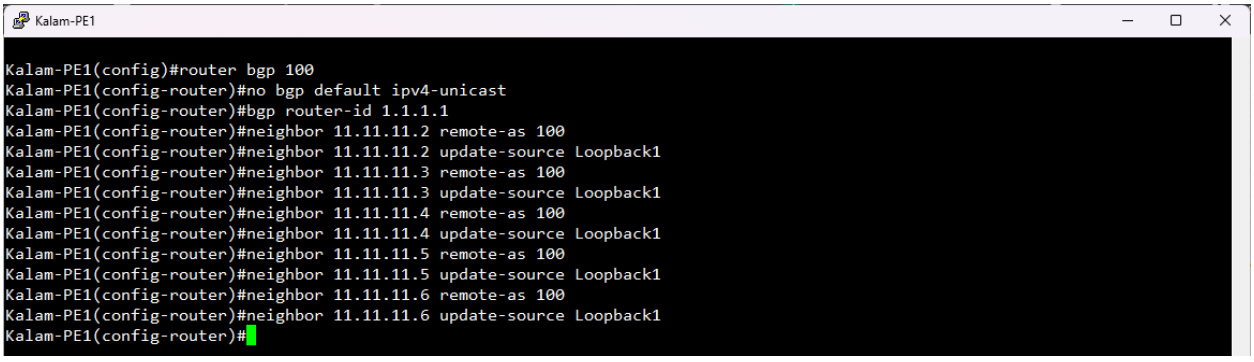

Figure 86 Kalam-PE1 BGP Configuration Command – Part (A)

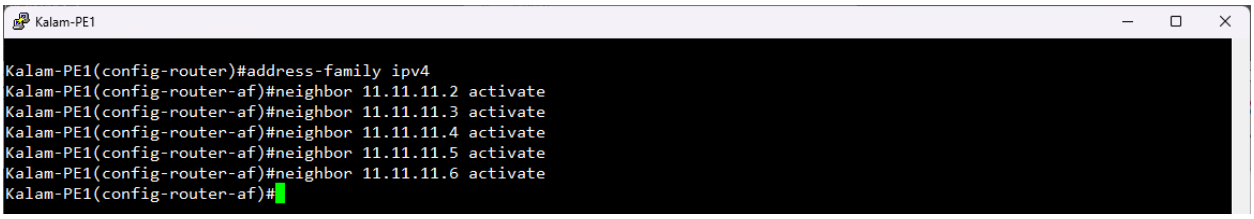

Figure 87 Kalam-PE1 BGP Configuration Command – Part (B)

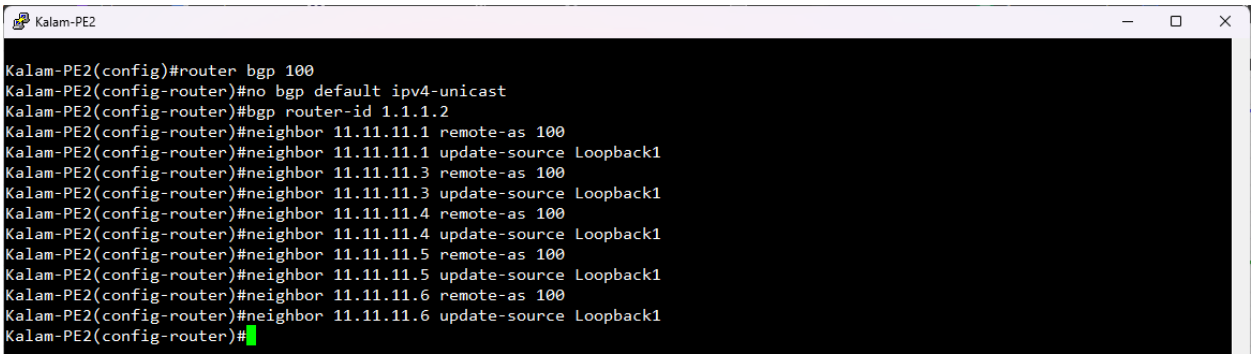

Figure 88 Kalam-PE2 BGP Configuration Command – Part (A)

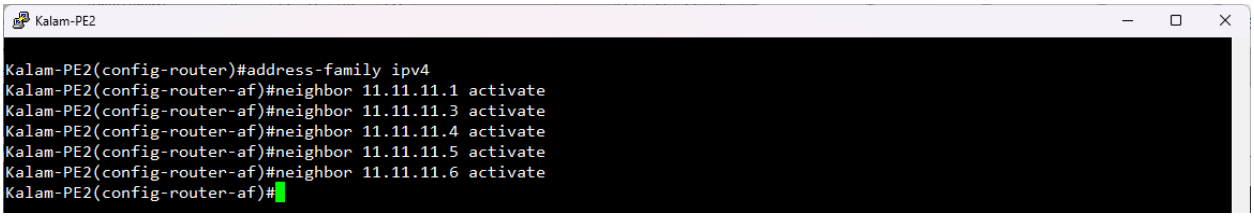

Figure 89 Kalam-PE2 BGP Configuration Command – Part (B)

Adjacency verification for BGP 100:

The upcoming figures shows and outlines the BGP neighbor relationship and the uptime of that neighbor relationship.

Note: This verification section contains different set of routers than those used in the configuration section. This approach is used to show that all routers are successfully forming an BGP adjacencies for BGP process 100. For this verification section, the selected routers for are Kalam-PE4 and Kalam-PE6.

In the verification figures we can see that the first two figures show the neighbor and it information such as the neighbor IP address, neighbor AS number, link type, BGP version

number and the neighbor router ID in addition to the number of open packets, notification packets, updates packets and keepalive packets. Also, The other figure show the uptime of each neighbor, message received by the neighboring router, message sent to the neighboring router. Furthermore, we can see the TbVer which tells us the table version which indicates how much the routing information has been changed between the neighbors and the InQ outlines the number of messages which received from the neighboring router but yet to be processed. Moreover, the OutQ show the number of packets that are waiting to be sent to the neighboring router. Finally, the State/PfxPRcd counts how many prefixes has been received from that neighbor. The TbVer, InQ and OutQ are considered to be very important verification attributes since it shows if the routers are in sync or desync.

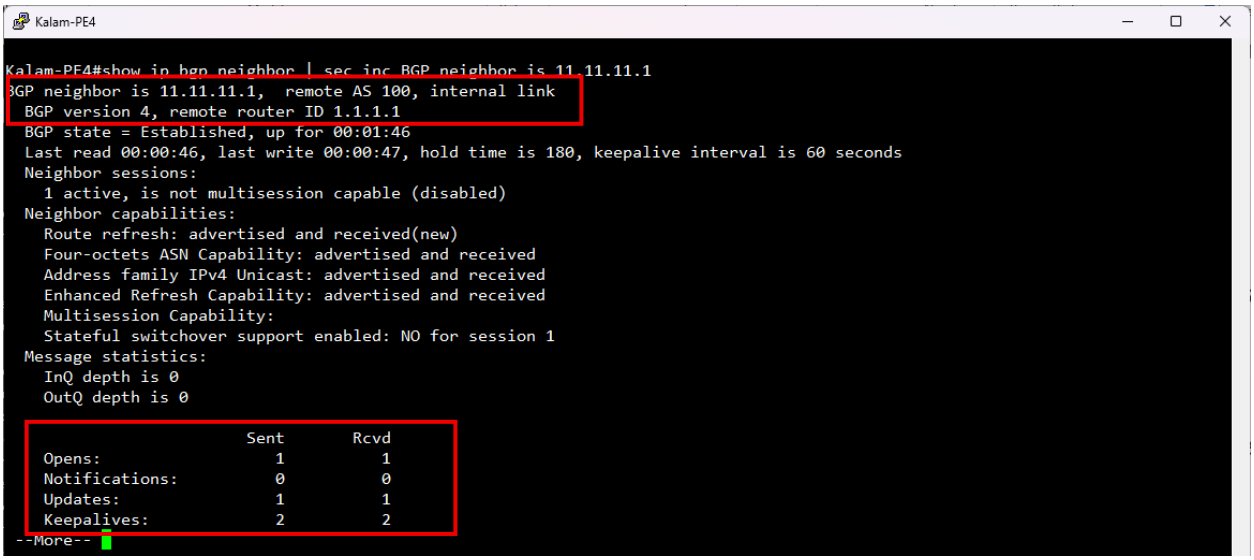

Figure 90 Kalam-PE4 Neighbor Output - Neighbor A

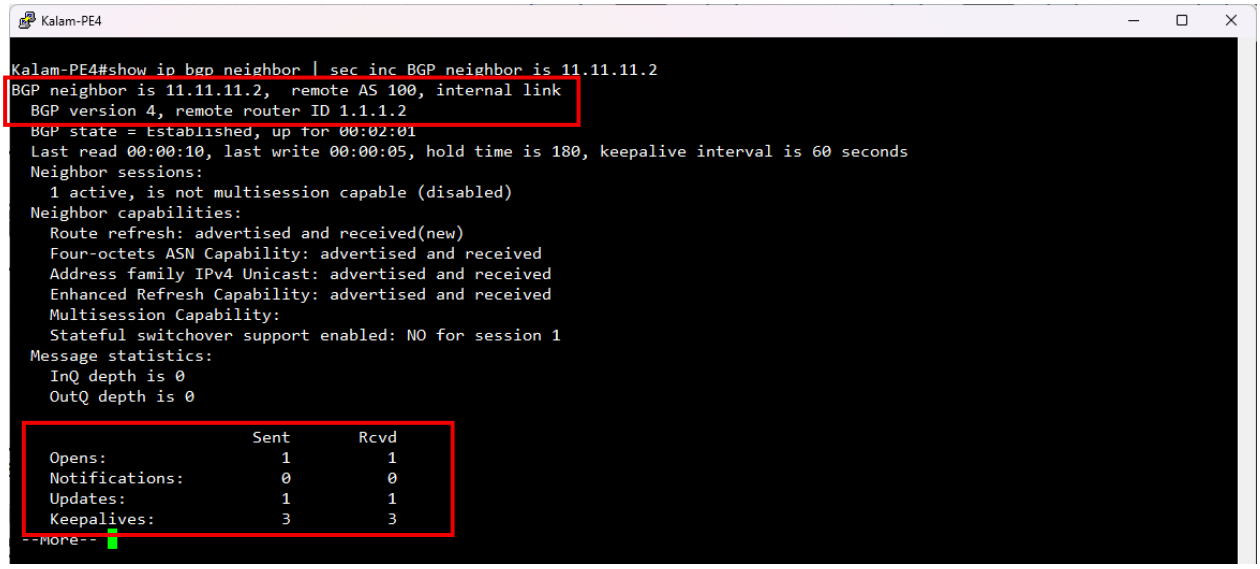

Figure 91 Kalam-PE4 Neighbor Output - Neighbor B

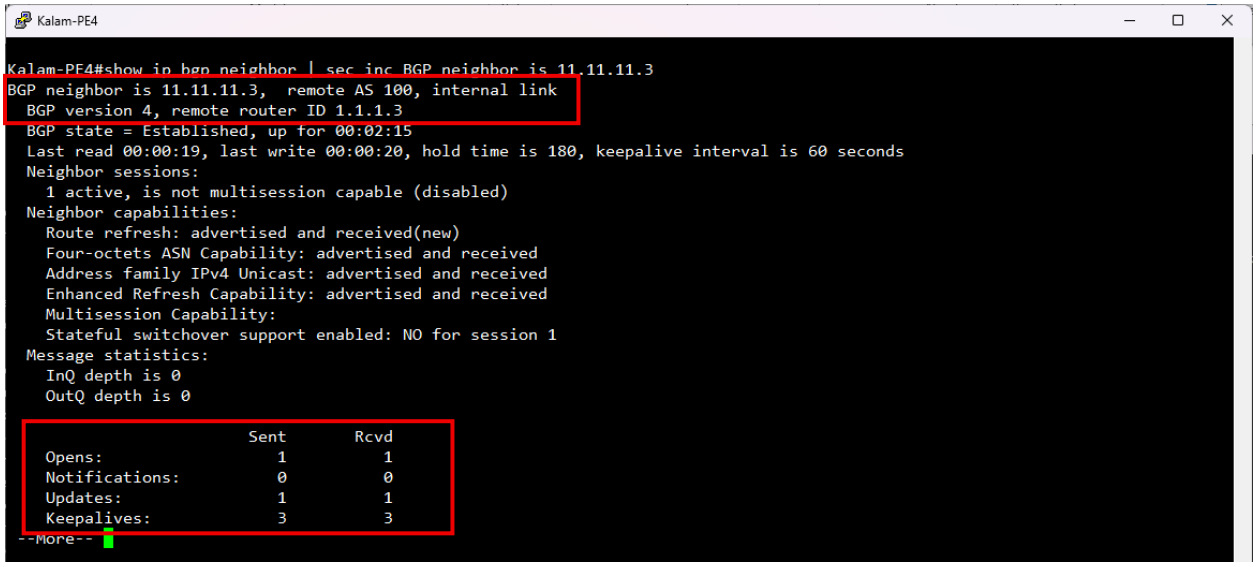

Figure 92 Kalam-PE4 Neighbor Output - Neighbor C

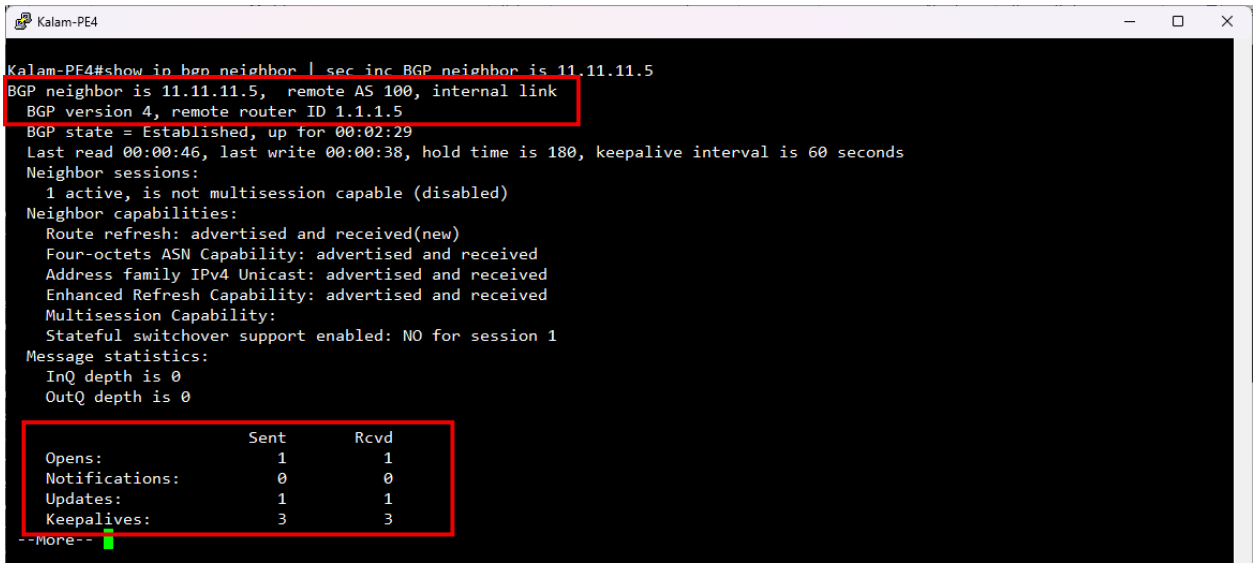

Figure 93 Kalam-PE4 Neighbor Output - Neighbor D

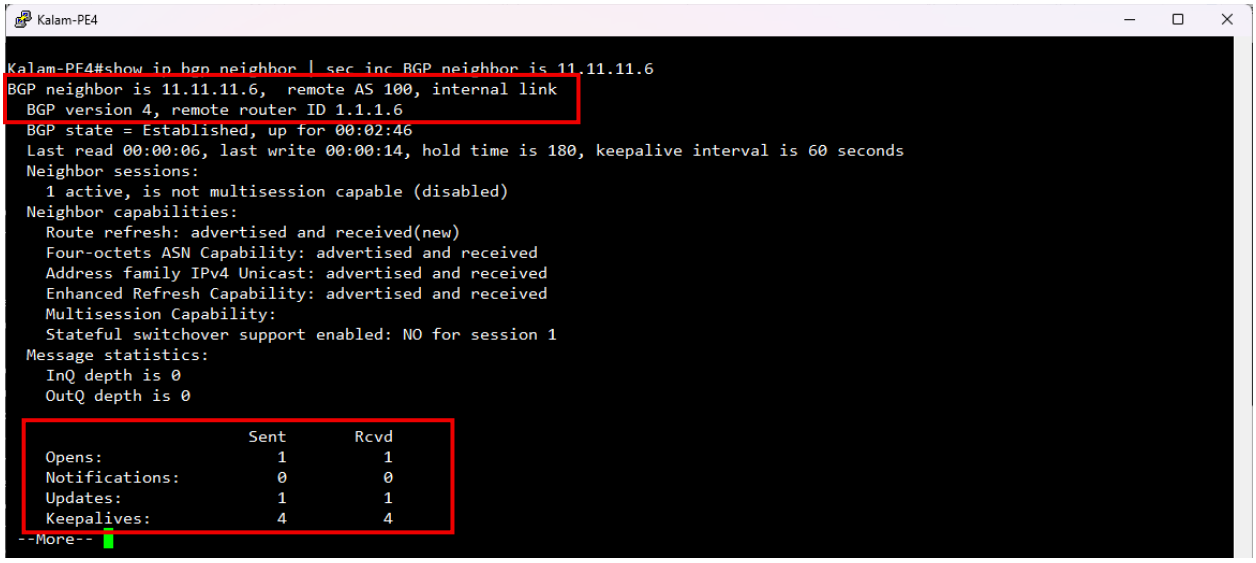

Figure 94 Kalam-PE4 Neighbor Output - Neighbor E

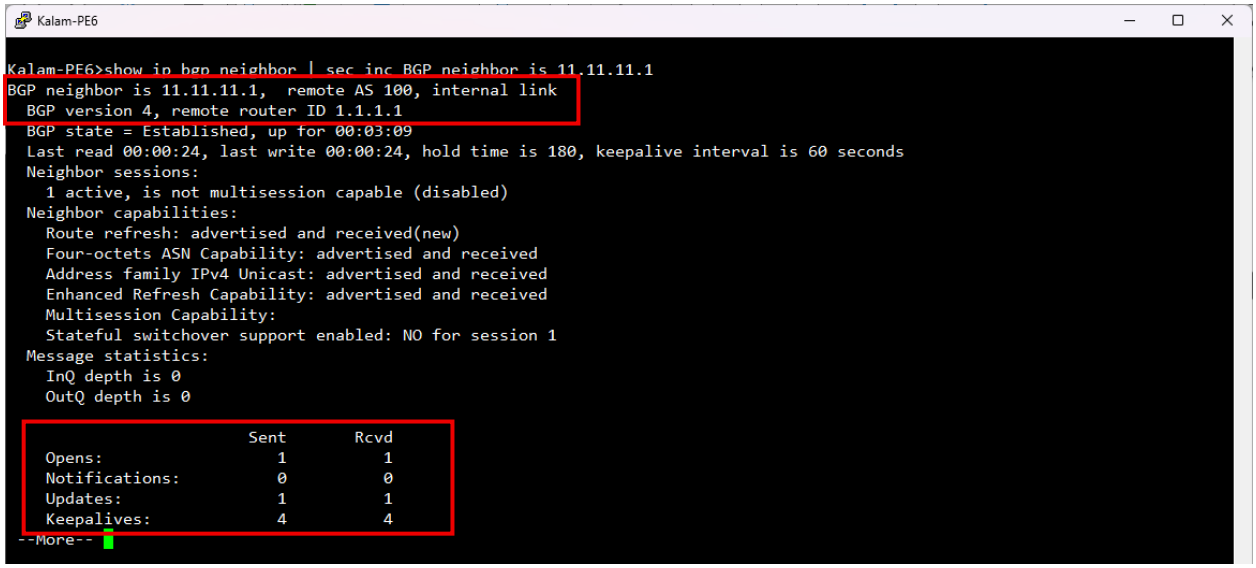

Figure 95 Kalam-PE6 Neighbor Output - Neighbor A

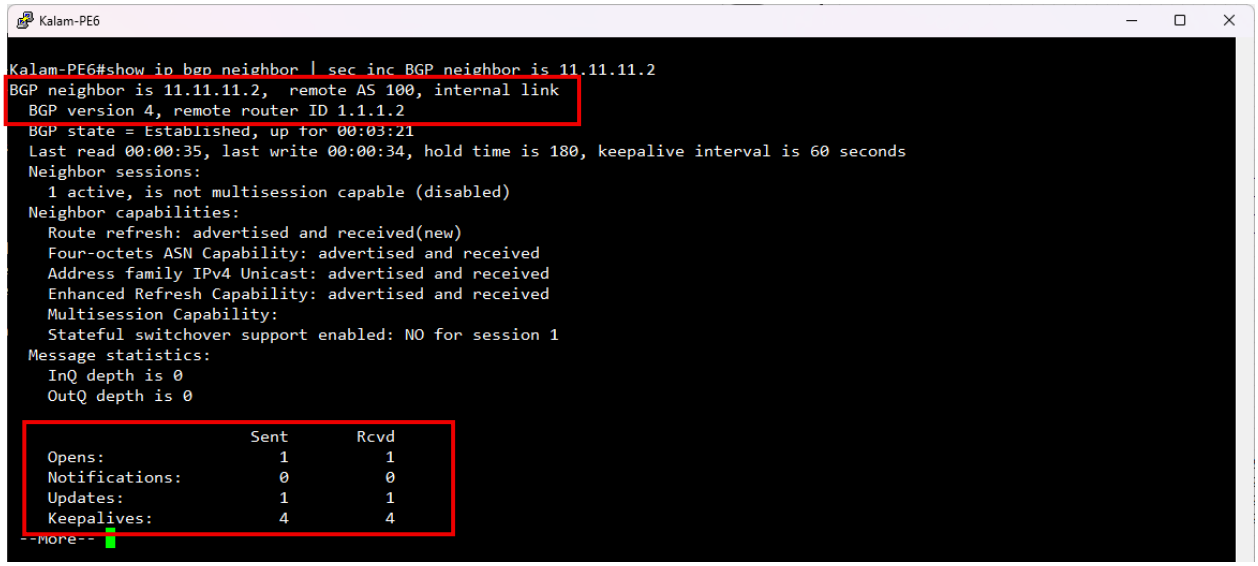

Figure 96 Kalam-PE6 Neighbor Output - Neighbor B

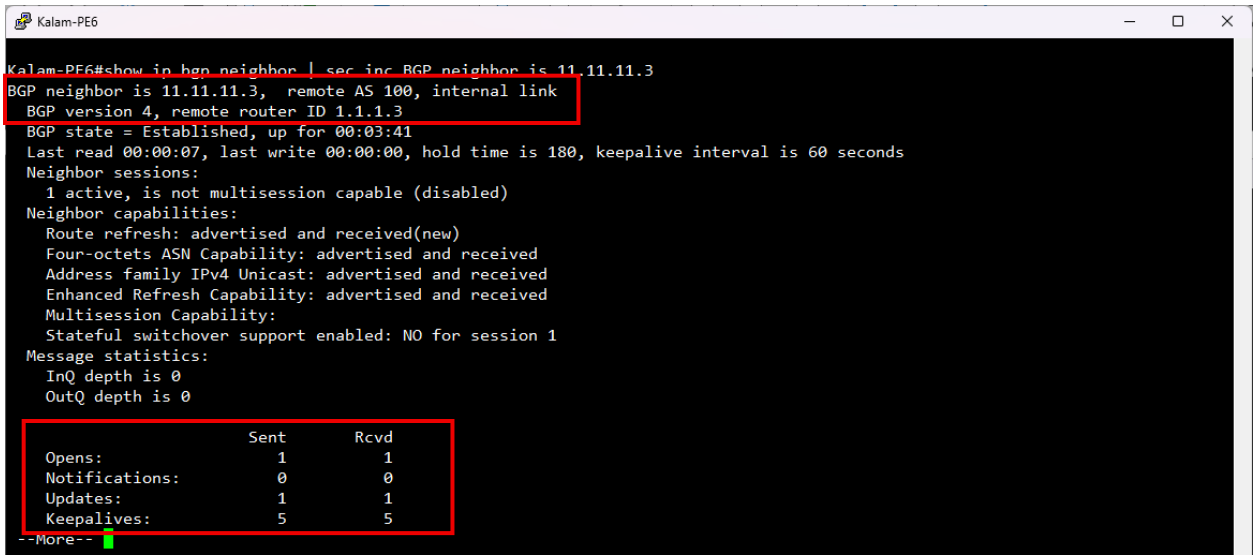

Figure 97 Kalam-PE6 Neighbor Output - Neighbor C

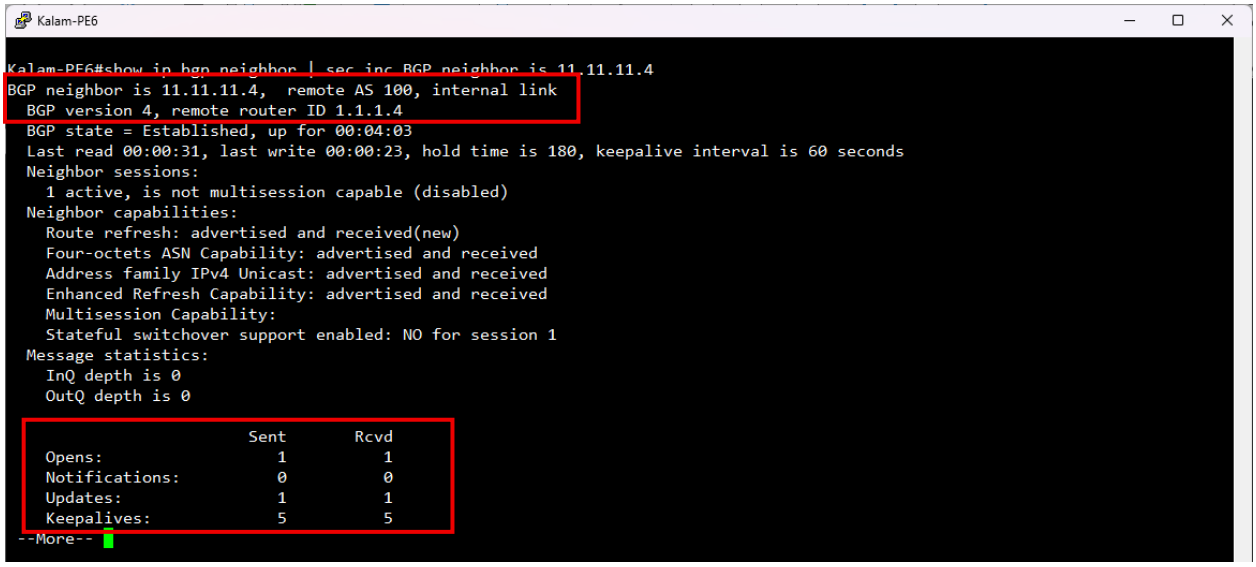

Figure 98 Kalam-PE6 Neighbor Output - Neighbor D

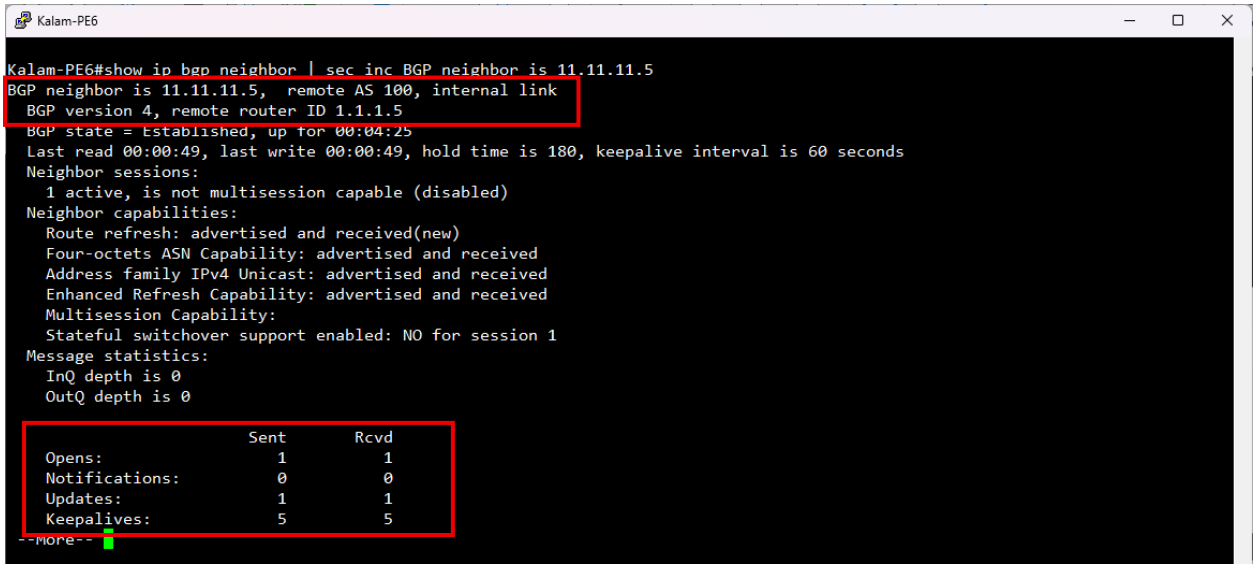

Figure 99 Kalam-PE6 Neighbor Output - Neighbor E

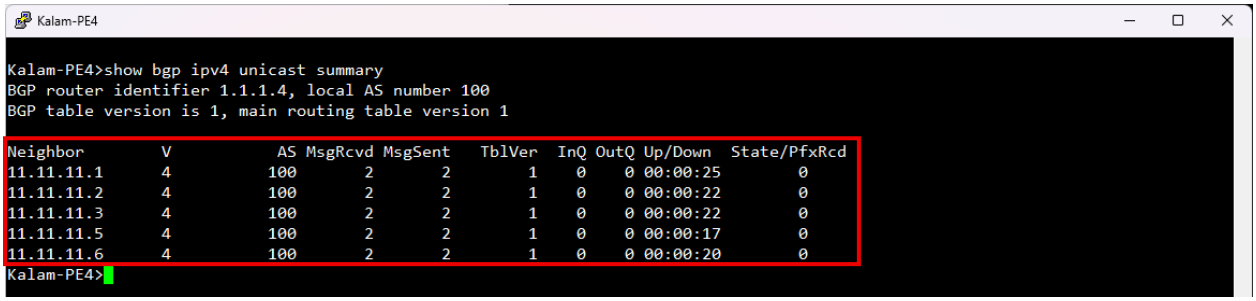

Figure 100 Kalam-PE4 BGP neighbor Uptime

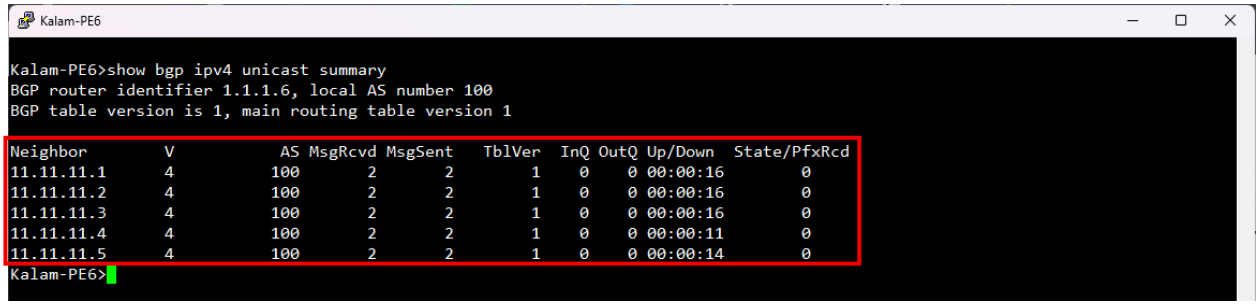

Figure 101 Kalam-PE6 BGP neighbor Uptime

BGP Wireshark Capture

The next figures will demonstrate a packet capturing using Wireshark for BGP adjacency between Kalam-PE1 and Kalam-PE2 for BGP process 100.

Note: In my topology the notification packets are not applicable. Therefore, only the open packet, Update packet and Keepalive packet are explained below. It should also be noted that multiple packets of the same type were captured for both Kalam-PE1 and Kalam-PE2; however, for the sake of time, not all of them are included below since they have the same contents.

Open packets are mainly sent to exchange the initiate session packets and negotiate the essential values and parameters between the routers. These values and parameters are BGP version, AS number, router IDs and hold timing. After the neighbors settled down on those parameter the keepalive packets started to be sent out to notify each other of a successful receipt of the previous open packets, then both routers moves from the open state to the established state which means that the adjacency has been established successfully. After a successful adjacency the update packet will be sent to exchanged, advertise or withdraw routes depending on the situation and routing policies.

Open Packets

The figures below shows that the open packets are being exchanged between the neighbors and the inspection of Kalam-PE1 shows that the packet has a source address of 11.11.11.1, which represents the loopback1 address of Kalam-PE1 router and a destination address of 11.11.11.2, which also represents the loopback1 address of the neighboring router which is Kalam-PE2. For the layer 3 header of the open packet, it shows the source address and destination address in addition to the protocol type and number which is TCP with a number of 6 and time to live of 255. Furthermore, the TCP header has a massive amount of useful information about this BGP open packet such as the source port 56349 which is a temporary port the router is using to send the packet to the BGP service of the neighboring router and destination port 179 which is the port that the BGP services uses. Additionally, the TCP header also includes the sequence number, which indicates the starting position of the carried data in the Kalam-PE1 open packet within the full TCP stream. It also shows the next sequence number which represents the byte position of the next carried data in the TCP stream. Furthermore, the

TCP header also show the segment length of the inspected packet which indicate the size of the payload carried. Moreover, we have the BGP header which have little bit of information such as the marker field which is used to help the routers detect that this packet is a valid BGP message within a TCP byte stream also the BGP header contains the length of the BGP message, type of the message, the BGP version, the AS number, hold time value and the router ID.

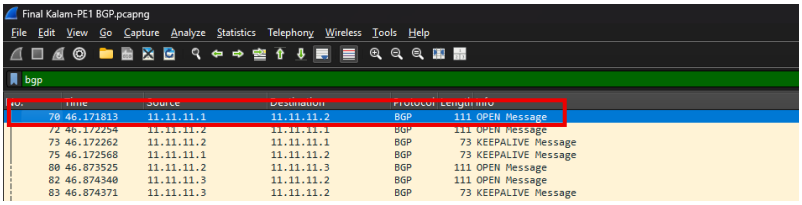

Figure 102 Kalam-PE1 BGP Open Packet

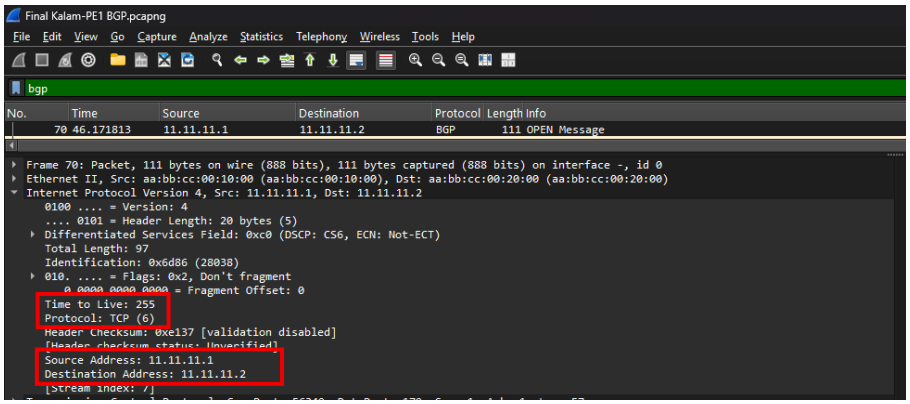

Figure 103 Kalam-PE1 BGP Open Packet Layer 3 Header Inspection

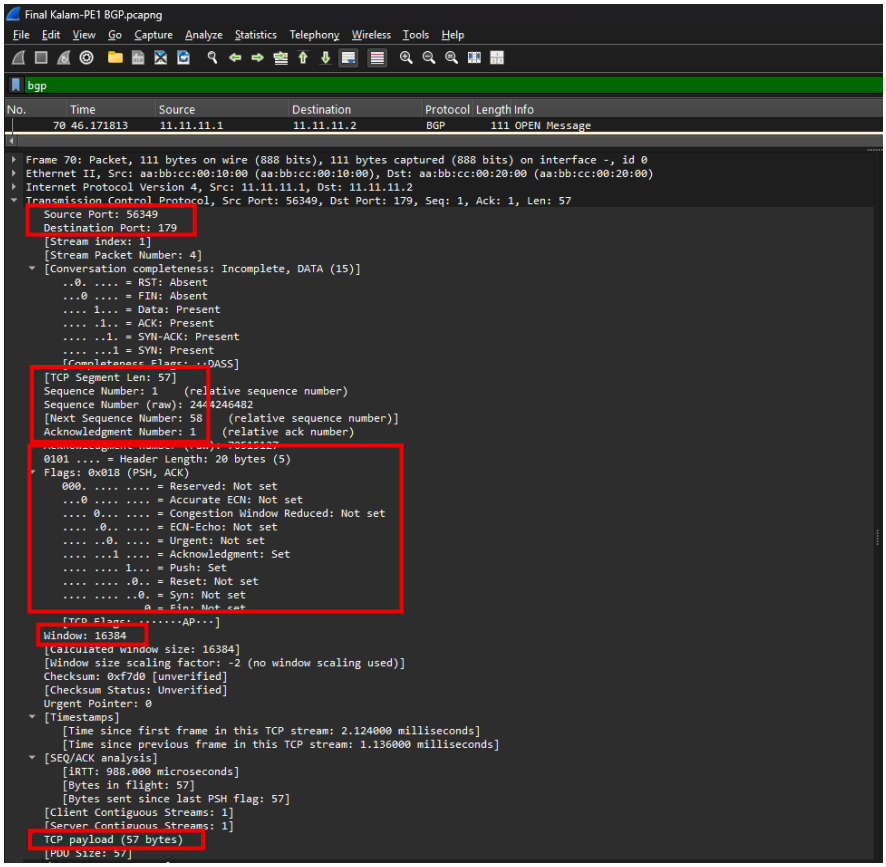

Figure 104 Kalam-PE1 BGP Open Packet TCP Header Inspection

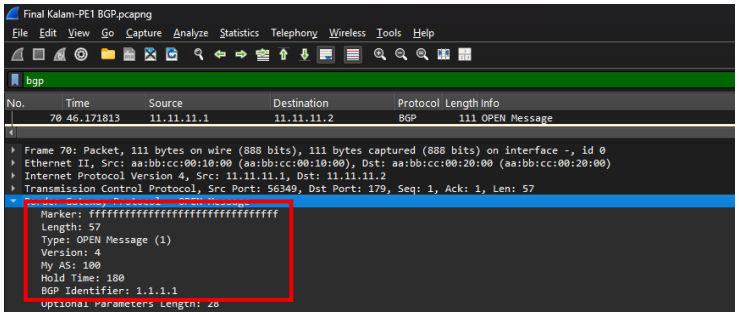

Figure 105 Kalam-PE1 BGP Open Packet BGP Header Inspection

Similarly, Kalam-PE2 has the exact same output but with different IPs and values such as the source address and destination address in the layer 3 header also in the TCP header there is some different values such as the source port of 179 and a destination of 56349. Furthermore, the router ID in the BGP header will be different since these packet are sent by Kalam-PE2.

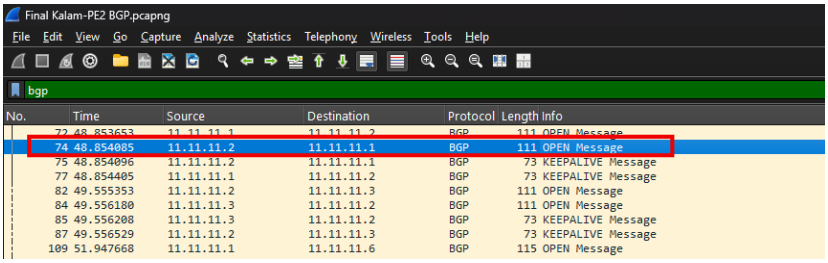

Figure 106 Kalam-PE2 BGP Open Packet

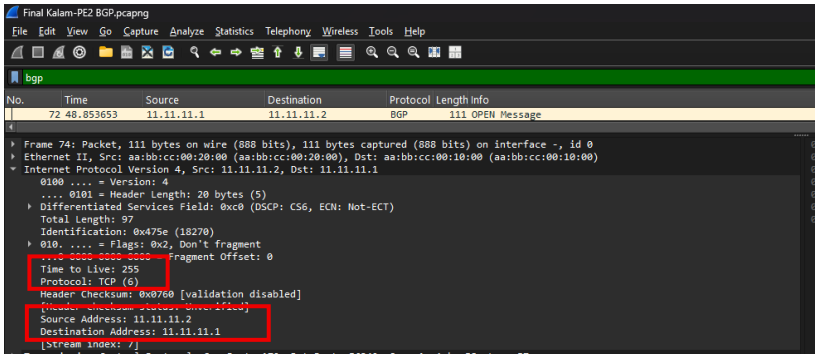

Figure 107 Kalam-PE2 BGP Open Packet Layer 3 Header Inspection

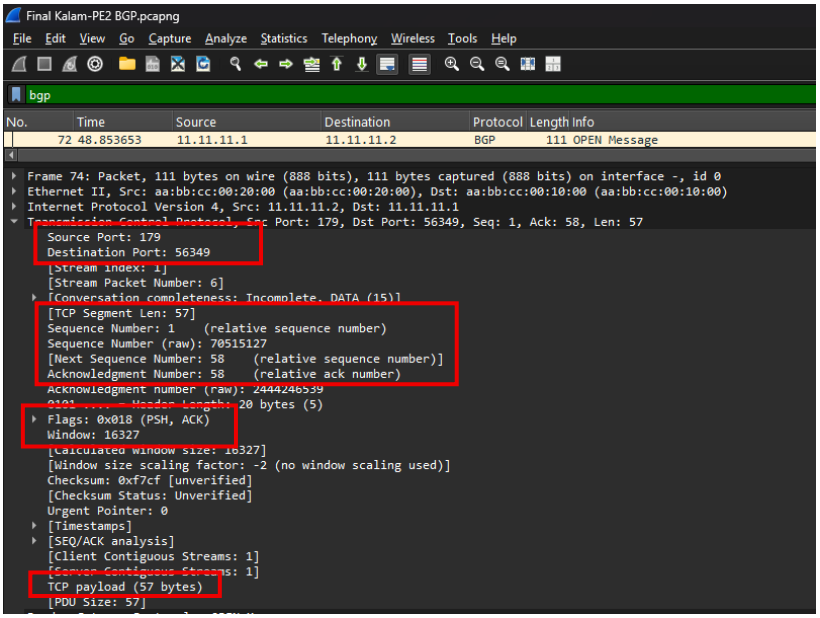

Figure 108 Kalam-PE2 BGP Open Packet TCP Header Inspection

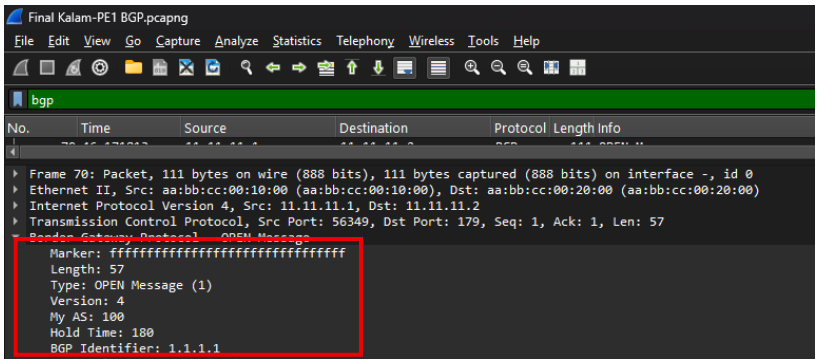

Figure 109 Kalam-PE2 BGP Open Packet BGP Header Inspection

Keepalive Packets

After the open packets are exchanged between the neighbors the keepalive packet will be used to tell each neighbor that the open packets has been received and examined successfully and all the parameters are matched correctly, therefore the second phase of the BGP adjacency is now undergoing.

The following pictures will show and inspect the keepalive packet sent by Kalam-PE1. The inspection of Kalam-PE1 keepalive packet shows a source address of 11.11.11.1 which indicates that this keepalive packet is sent by Kalam-PE1 headed to 11.11.11.2 which is Kalam-PE2. For the Layer 3 header there is no new thing to explore since most of the data is similar to the open packets explained previously. However, the TCP header is slightly different in some of the values such as the sequence number which starts from 58 which proves that this keepalive packet is a response to the open packet sent previously by Kalam-PE2 to Kalam-PE1. Additionally, the next sequence number is also different since the keepalive packet only needs 19 byte from the TCP stream. Furthermore, the BGP header for the keepalive packet does not have too much data except for the marker field to indicate that this is a valid BGP message within the TCP stream and the message type which is keepalive to indicate that this is a keepalive packet and not an open or update packet.

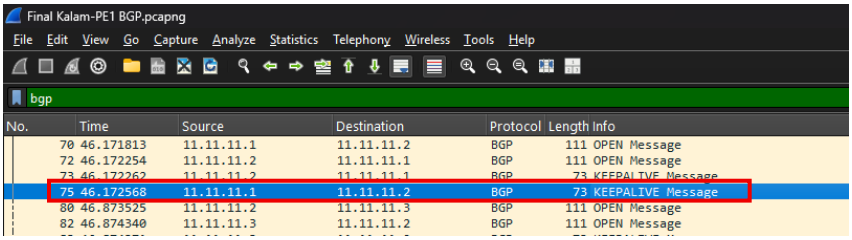

Figure 110 Kalam-PE1 BGP Keepalive Packet

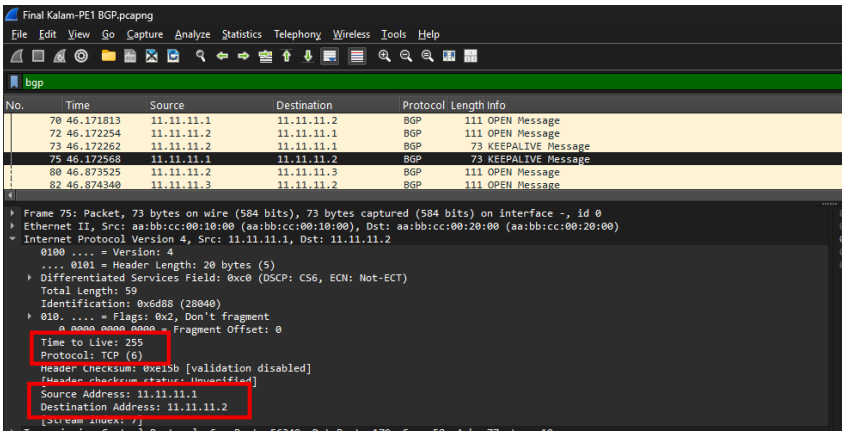

Figure 111 Kalam-PE1 BGP Keepalive Packet Layer 3 Header Inspection

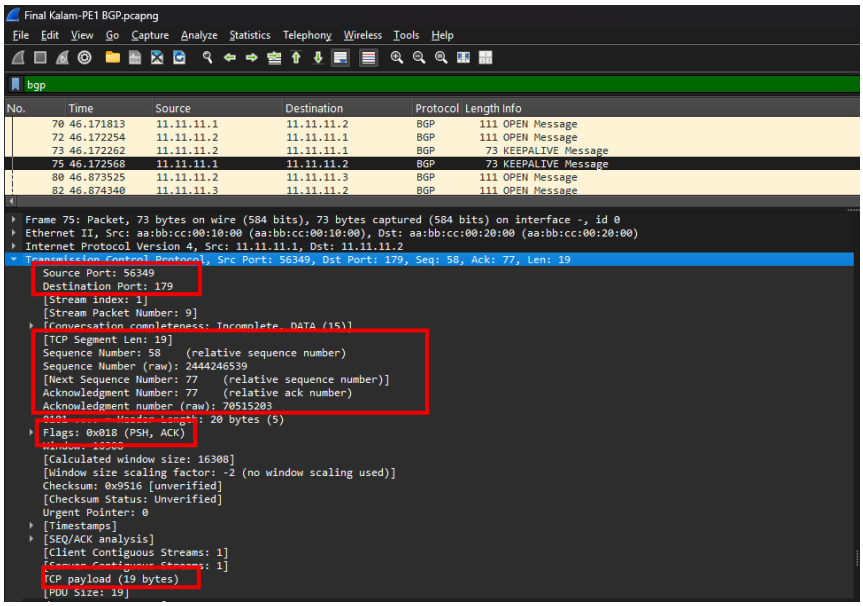

Figure 112 Kalam-PE1 BGP Keepalive Packet TCP Header Inspection

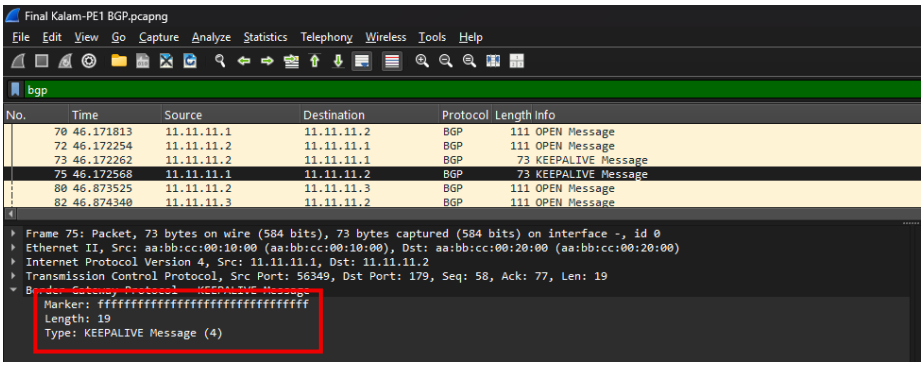

Figure 113 Kalam-PE1 BGP Keepalive Packet BGP Header Inspection

On the other side, Kalam-PE2 also sends a keepalive packet with different values such as the source address 11.11.11.2 and a destination address 11.11.11.1. all the other attributes are similar to Kalam-PE1 keepalive packet but with different values as the figures below shows.

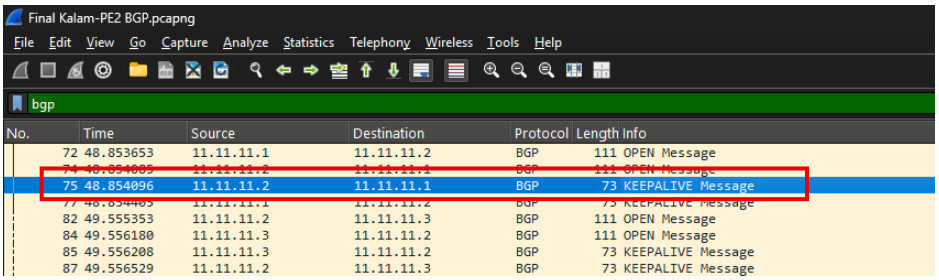

Figure 114 alam-PE2 BGP Keepalive Packet

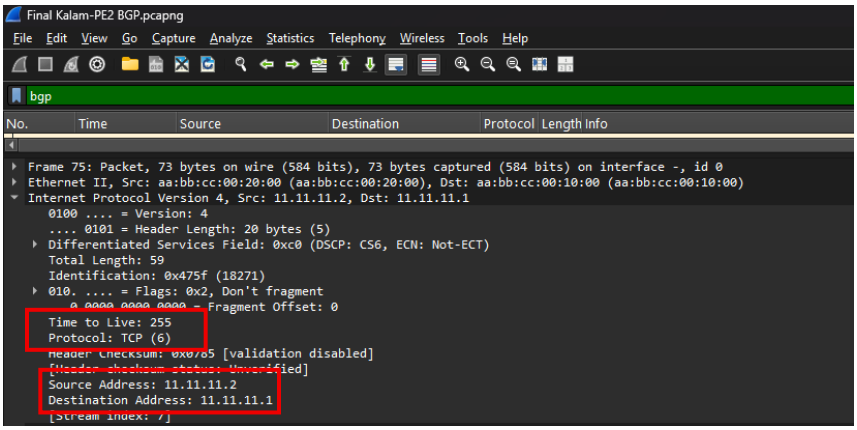

Figure 115 Kalam-PE2 BGP Keepalive Packet Layer 3 Header Inspection

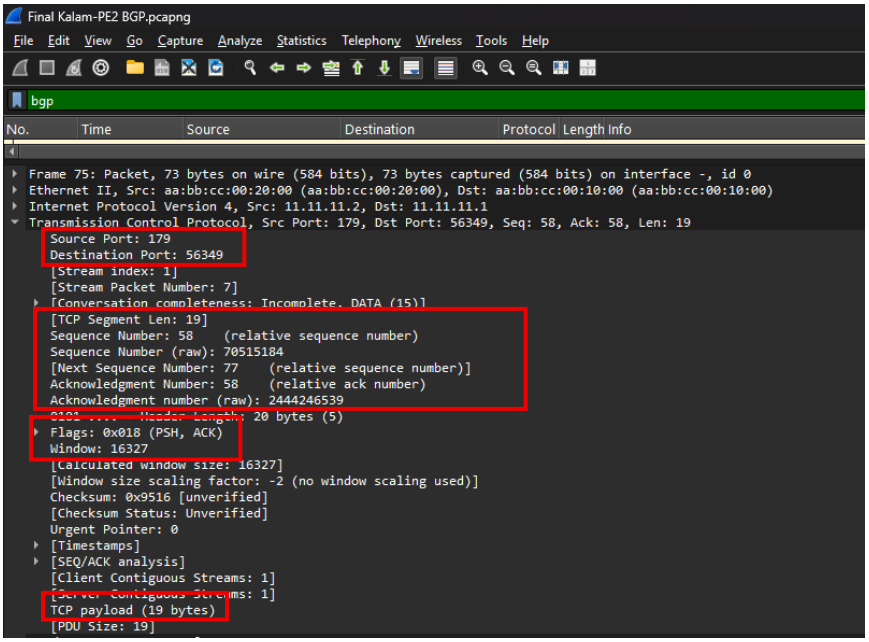

Figure 116 Kalam-PE2 BGP Keepalive Packet TCP Header Inspection

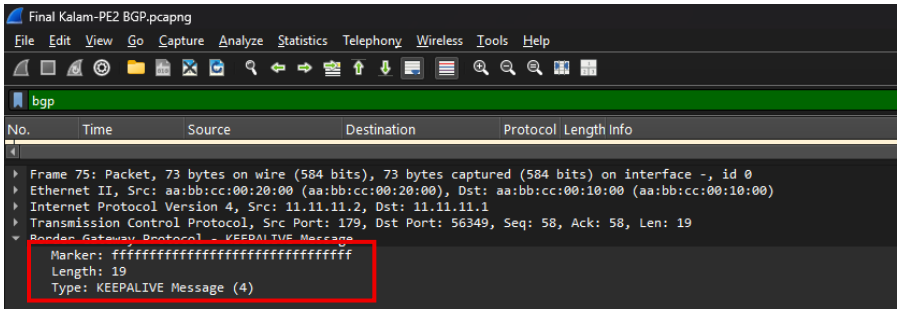

Figure 117 Kalam-PE2 BGP Keepalive Packet BGP Header Inspection

Update Packets

After the Keepalive packets exchange is done between the neighbors, the update packets are started to be sent out to exchanging routing information between the routers. Update packets are usually containing information about network reachability, path attributes and route withdrawal information. These packets are usually exchanged after the BGP adjacency has been established also these packet are responsible for propagates the routing table of the BGP.

The upcoming figures outlines the parameters that lives inside the update packets of Kalam-PE1. Some of those parameters are already explained earlier in this paper such as the source address 11.11.11.1, destination address 11.11.11.2, protocol name and number which is TCP

with a number of 6 and the time to live which equal to 255. In addition to the source port 56349, destination port 179 and all the other values. The only difference is in the BGP header, there is dedicated attributes for withdraw routes which specifies a specific route to withdraw if needed.

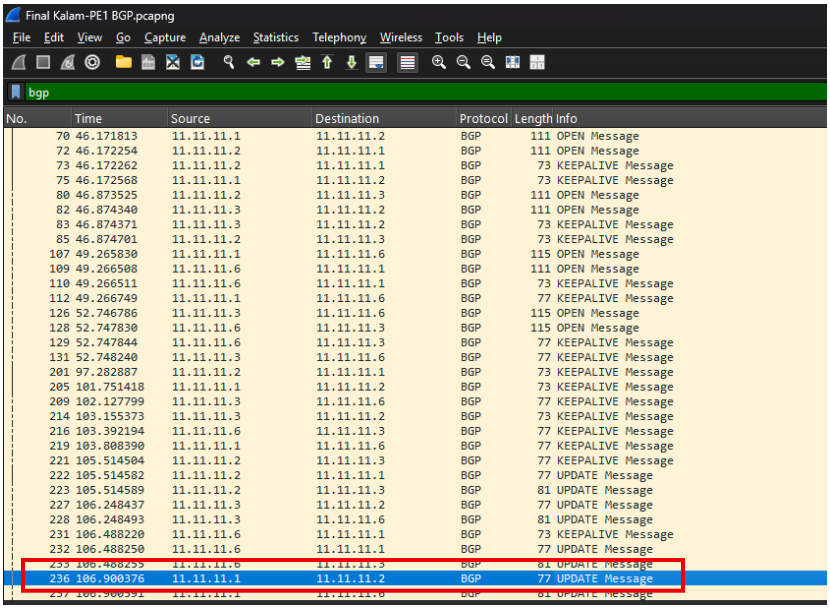

Figure 118 alam-PE1 BGP Update Packet

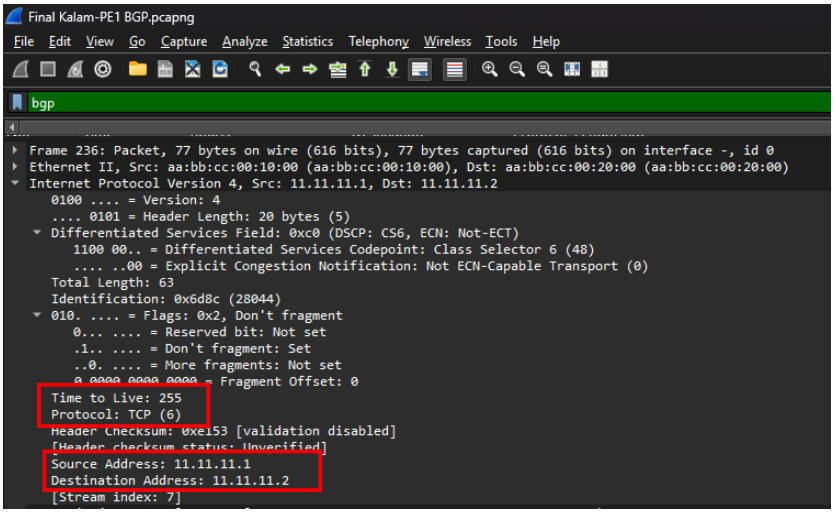

Figure 119 Kalam-PE1 BGP Update Packet Layer 3 Header Inspection

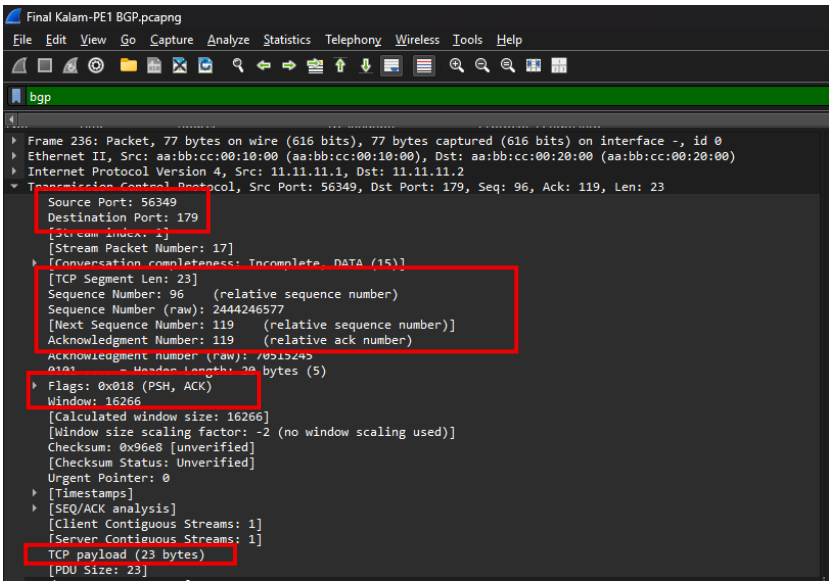

Figure 120 Kalam-PE1 BGP Update TCP Header Inspection

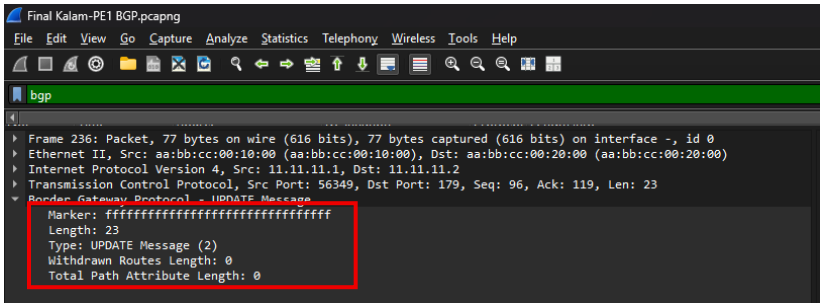

Figure 121 Kalam-PE1 BGP Update Packet BGP Header Inspection

Kalam-PE2 has a similar packet layout but with Kalam-PE2 information and IPs. As we can see the source address 11.11.11.2, destination address 11.11.11.1, source port of 179, destination port 56349, sequence number of 96.

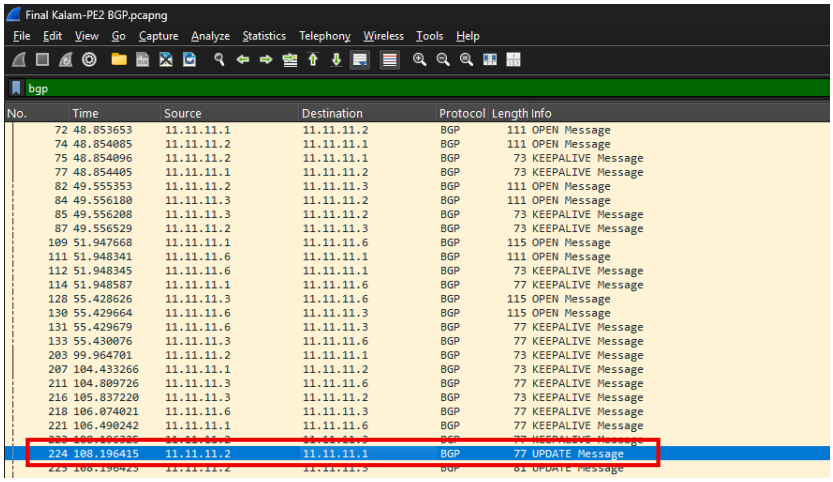

Figure 122 alam-PE2 BGP Update Packet

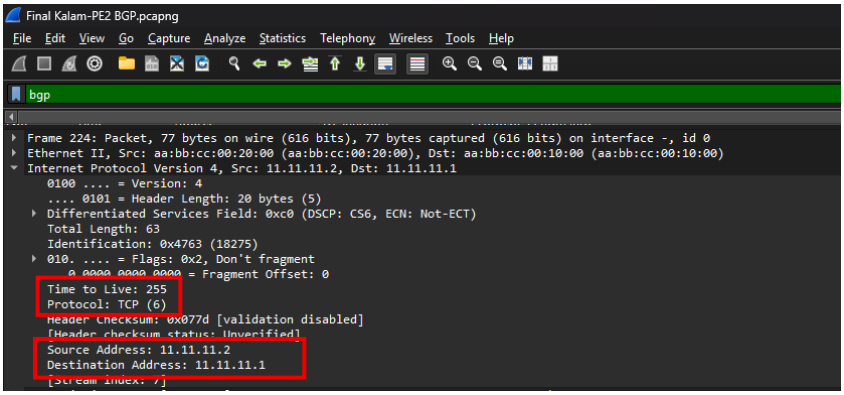

Figure 123 Kalam-PE2 BGP Update Packet Layer 3 Header Inspection

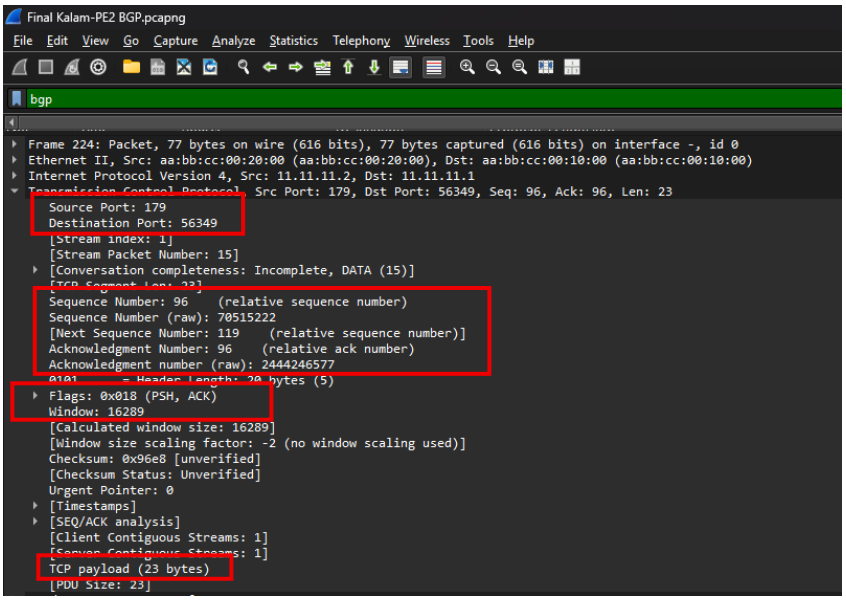

Figure 124 Kalam-PE2 BGP Update TCP Header Inspection

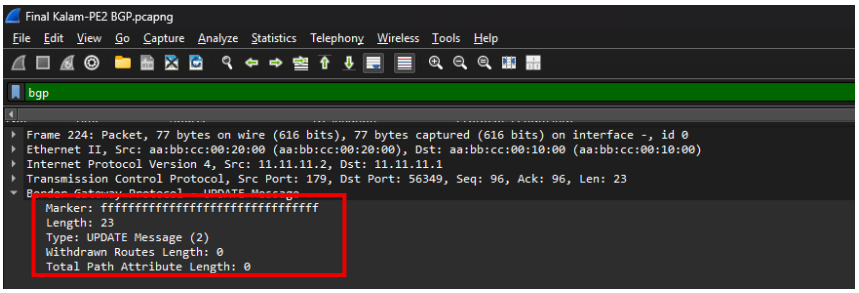

Figure 125 Kalam-PE2 BGP Update Packet BGP Header Inspection

MPLS configuration for Kalam Telecom routers

The multiprotocol label switching (MPLS) is used on all of the PE routers and P routers as well. MPLS is deployed on the backbone layer to enable efficient routing by sending the packet based on labels. MPLS uses label distribution protocol (LDP) to establish label switched path between routers.

implementation details of this section:

- Enable MPLS on the interfaces
- Assign a router-ID for MPLS
- Create a VRF instance for each customer on the PE routers
- Modify the EIGRP and BGP routing protocol

The figure below shows all the devices that participate in the MPLS protocol:

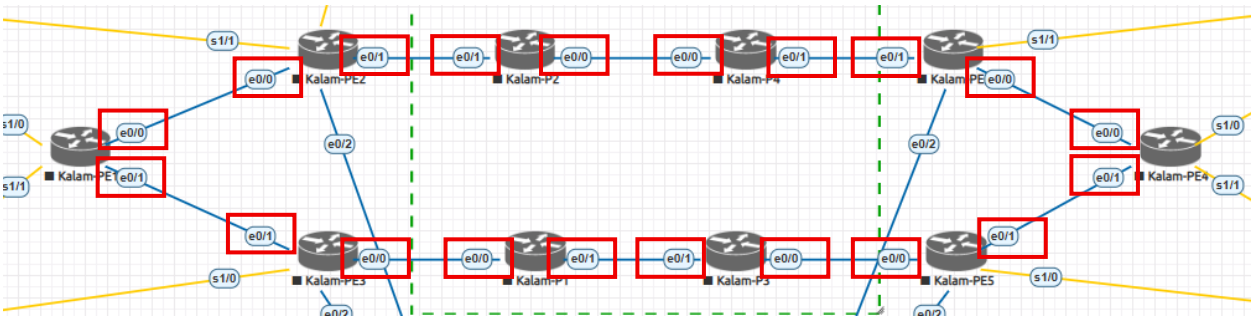

Figure 126 MPLS Devices

MPLS Configuration process:

The next couple of figures will explain a detailed step by step to configure MPLS LDP on the router. The MPLS will be configured on Kalam-PE1, PE2, PE3, PE4, PE5, PE6 as well as the Kalam-P1, P2, P3 and P4.

The router ID of the MPLS will be assigned manually to all routers as it is the best practice. Kalam-PE1 will have the loopback0 interface 1.1.1.1 as the MPLS router ID, Kalam-PE2 will

have the loopback0 interface 1.1.1.2 as the MPLS router ID, Kalam-PE3 will have the loopback0 interface 1.1.1.3 as the MPLS router ID until Kalam-PE6 will have the loopback0 interface 1.1.1.6 as the MPLS router ID. Additionally, Kalam-P1 will have the loopback0 interface 1.1.2.1, Kalam-P2 will have the loopback0 interface 1.1.2.2 as the MPLS router ID, Kalam-P3 will have the loopback0 interface 1.1.2.3 as the MPLS router ID and Kalam-P4 will have the loopback0 interface 1.1.2.4 as the MPLS router ID.

Explaining the commands:

- "mpls ip" ⇨ enable the mpls on the interface.
- "mpls ldp router-id lo0 force" ⇨ assign the router ID for the MPLS process.

Figure 127 Kalam-PE1 MPLS LDP Configuration Commands

Figure 128 Kalam-PE2 MPLS LDP Configuration Commands

Virtual and routing forwarding instance:

The next figures demonstrate how the Virtual and routing forwarding (VRF) is configured on the Provider Edge (PE) Routers only. Each PE router will have either a VRF dedicated to ABC Company or XYZ Company or two VRFs, each dedicated to ABC and XYZ companies. The VRF is mainly used on the PE routers to ensures that each connected customer has a separated virtual routing instance which is isolated from the main routing instance and any other virtual routing instance. After assigning the VRF to the interface, the router will send a

system message states that the IP address of that interface has been removed due to the VRF assignment and the IP should be reassigned to the interface. Additionally, each VRF needs to have a route distinguisher to distinguish each route from the other and it needs a route target to control route import and export between VRFs. The tables below show the VRF parameters.

VRF IDs	
ABC company	100
XYZ Company	200

Table 3 VRF IDs Table

Route Distinguisher (RD) Table		
VRF	Route Distinguisher	Router / Interface
ABC company	1.1.1.1:100	Kalam-PE1 / S1/1
	1.1.1.3:100	Kalam-PE3 / S1/0
	1.1.1.4:100	Kalam -PE4 / S1/1
	1.1.1.5:100	Kalam -PE5 / S1/0
XYZ Company	1.1.1.1:200	Kalam -PE1 / S1/0
	1.1.1.2:200	Kalam -PE2 / S1/1
	1.1.1.4:200	Kalam -PE4 / S1/0
	1.1.1.6:200	Kalam -PE6/ S1/1
	2.2.2.4:200	Batelco-PE4 / S1/0

Table 4 VRF Route Distinguisher Table

Route Target (RT) Table	
VRF	Route Target
ABC company	65001:100
XYZ Company	65002:200

Table 5 VRF Route Target Table

Explaining commands:

- “ip vrf <vrf name>” ⇨ Create a vrf with a specific name.
- “rd <identifier> ⇨ define the route distinguisher.
- “route-target < identifier>” ⇨ define the route target.
- “ip vrf forwarding <vrf name>” ⇨ assigning the vrf into an interface”.

Figure 129 Kalam-PE1 ABC VRF Instance Configuration

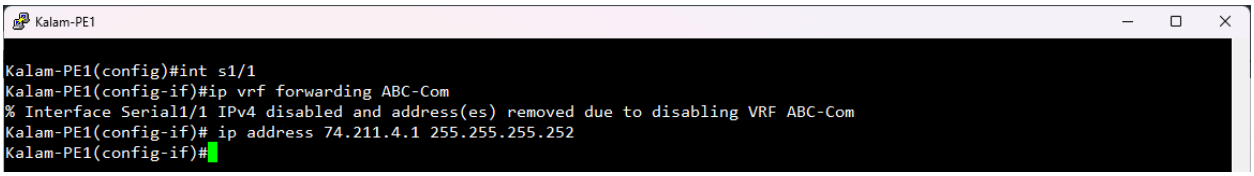

Figure 130 Kalam-PE1 ABC VRF Interface Assignment

Figure 131 Kalam-PE1 XYZ VRF Instance Configuration

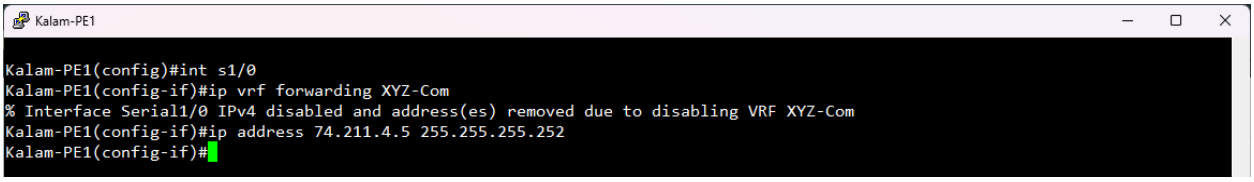

Figure 132 Kalam-PE1 XYZ VRF Interface Assignment

EIGRP and BGP instances Modification for the PE routers:

The next figures will demonstrate the necessary modification for the MPLS network to function properly. The modification is applied on both AF instance under the EIGRP and BGP. For the EIGRP process, two instances are configured, one for ABC Company with AS 10 and another for XYZ Company with AS 20. Similarly, the BGP is also configured with 2 instances, one for ABC Company and the second for XYZ Company.

The modification is implemented on both protocols to enable end-to-end route visibility across the network. the end-to-end visibility is achieved by adding redistribution statements. These modifications allows the routes learned via the EIGRP which is between the customer edge (CE) routers and provider edge (PE) routers to be redistributed to the BGP which is connecting all the ISP PE routers to gather and vice vera.

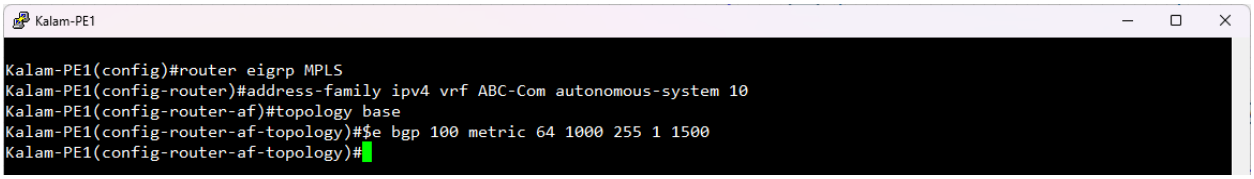

Figure 133 Kalam-PE1 EIGRP ABC VRF Instance Modification

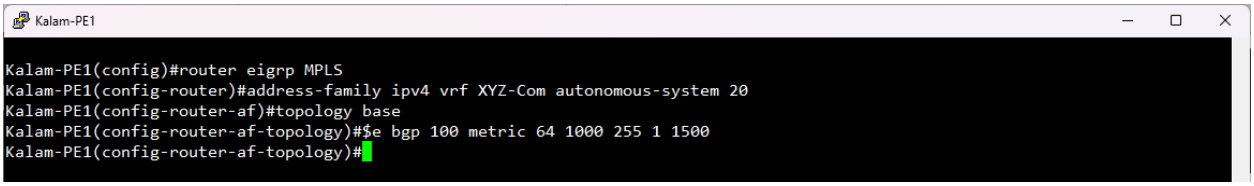

Figure 134 Kalam-PE1 EIGRP XYZ VRF Instance Modification

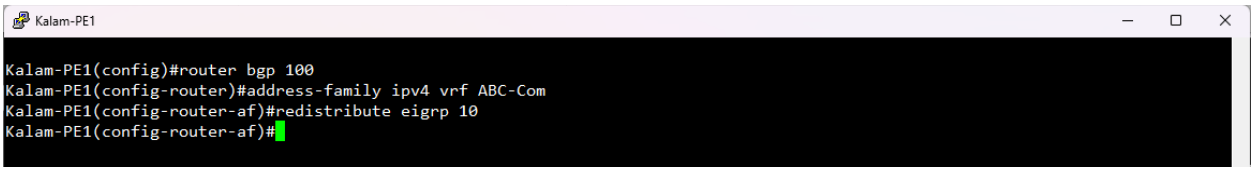

Figure 135 Kalam-PE1 BGP ABC VRF Instance Modification

Figure 136 Kalam-PE1 BGP XYZ VRF Instance Modification

MPLS Verification:

The following section will outline the verification of the MPLS LDP, which will explain the inner labels on the PE routers along with the outer label which will always change when being forwarded.

As the below figures show, the MPLS label binding, which include all IP prefixes and their corresponding assigned labels. There are two types of ldp binding, first one is generated by the local router (i.e. Kalam-PE1) so the neighboring router (i.e. Kalam-PE3) can use it when there is any label packet for Kalam-PE1 prefixes which is called local binding labels. The second type of ldp binding is the opposite of the previous one, the second type is generated by the neighboring router (i.e. Kalam-PE3) so the local router (i.e. Kalam-PE1) can use it if it has any labeled packet destined for any of the neighboring prefixes which is called

neighbor binding labels. The MPLS VPN labels are also used in a similar way, but these labels are used only to distinguish customer routes and vrf. To clear the confusion of the ldp labels and MPLS VPN labels, usually the MPLS VPN labels are called inner labels and the ldp labels called outside label but there is two types of them, the inner outside label and the outer outside label. The inner outside label points to the local ldp assigned label and the outer outside label points to the next hop label of the neighboring router. Finally, the MPLS forwarding table combines the ldp binding labels only, which are the inner outside labels and the outer outside labels in one comprehensive table.

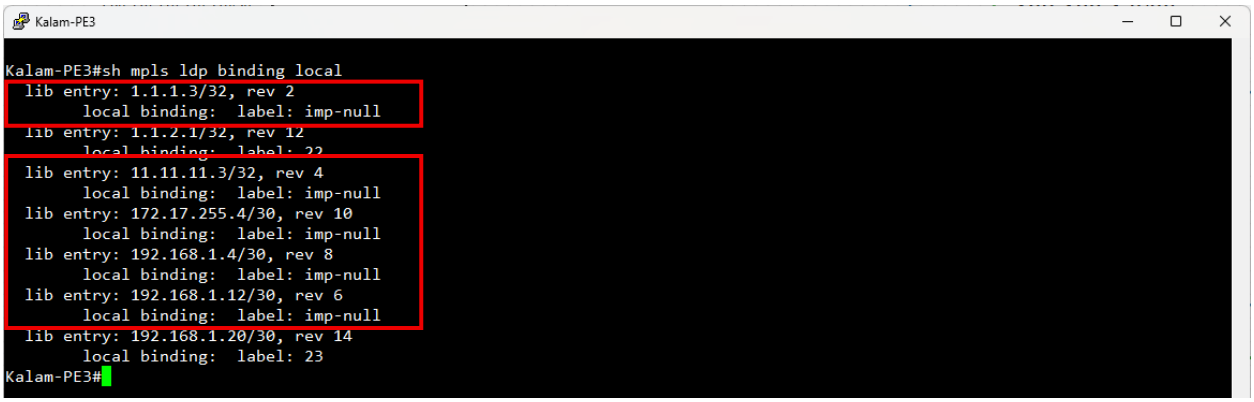

Figure 137 Kalam-PE3 MPLS Verification of Local Labels

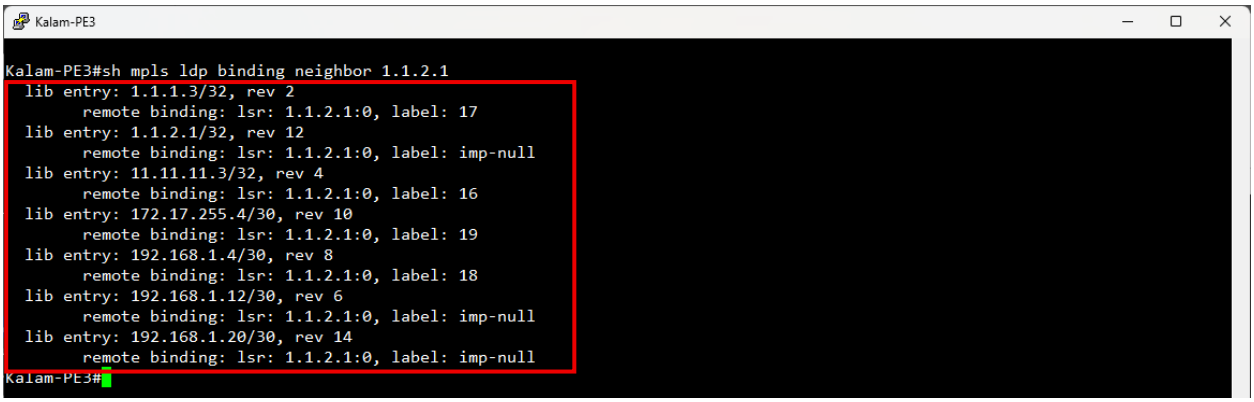

Figure 138 Kalam-PE3 MPLS Verification of Neighbor Labels

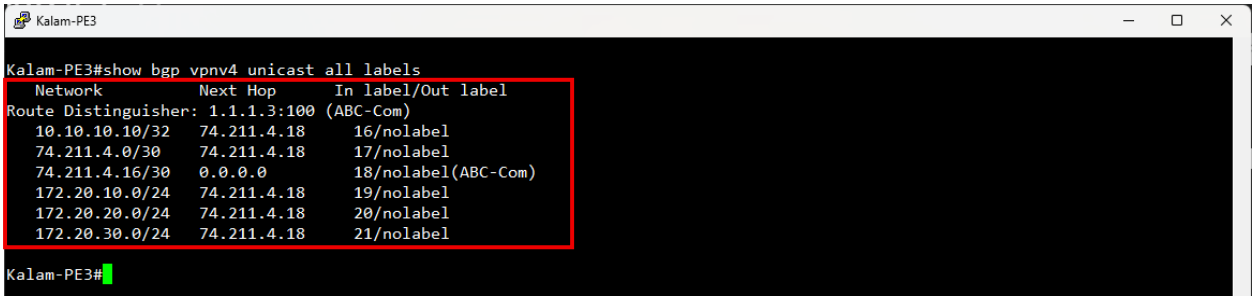

Figure 139 Kalam-PE3 MPLS Verification of MPLS VPN Labels

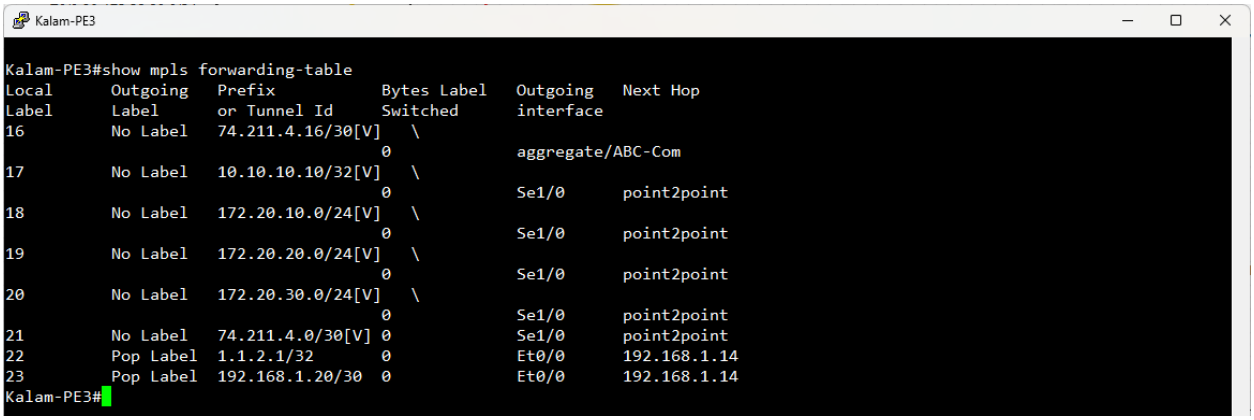

Figure 140 Kalam-PE3 MPLS Verification of MPLS Forwarding Table

MPLS LDP Wireshark Packet Capture

The following figures of the Wireshark packet capturing will show detailed information about how the MPLS forms adjacency between two routers.

The LDP hello packet are used to discover whether any MPLS enabled router is active or not. One a router discovers that there is an MPLS neighbor, its initiates a TCP three-way handshake to establishes a session with that neighbor. After the TCP session is successfully established the router sends an LDP initiate message over the TCP connection. This message are used to negotiate the parameters of the MPLS adjacency. After the parameters are matched and confirmed the router send an LDP keepalive packet similar in function to the BGP keepalive packet, it is sent to confirm that the adjacency has been established. Finally, the router send a Label mapping message, which is used to exchange MPLS labels.

LDP hello packets:

The following figures shows the LDP Hello packet from Kalam-P2 with a source address of 192.168.1.17 and a destination address of 224.0.0.2, which is a multicast address reserved for all routers on the local link. In the layer 3 header the protocol field indicates that the protocol are a UDP, identified by number 17. Furthermore, in the UDP header both the source and destination ports are set to uses port 646, which is the well-known port for LDP communications. Additionally, the LDP header has the most amount of information that are required in establishing LDP adjacencies. These information are the LDP version, which is version 1, the LSR ID of 1.1.2.2 and Label space ID, which a value of 0 indicating a per-platform label space. Moreover, the LDP message type is identified as a Hello packet also the header indicates the hold timer along with the targeted field and link hello, indicating that this packet is exchanged over a directly connected interface.

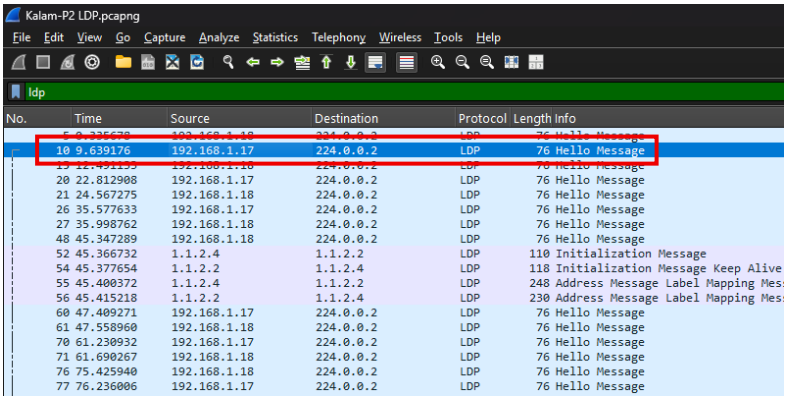

Figure 141 Kalam-P2 LDP Hello Packet

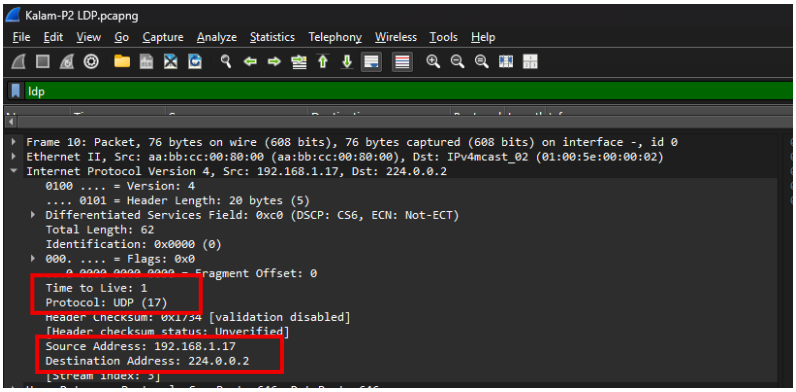

Figure 142 Kalam-P2 LDP Hello Packet Layer 3 Header Inspection

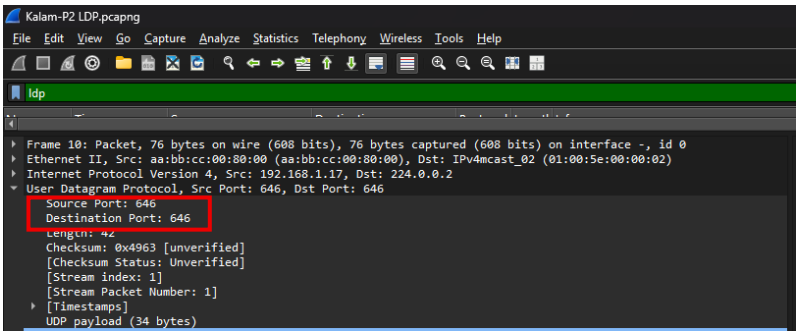

Figure 143 Kalam-P2 LDP Hello Packet UDP Header Inspection

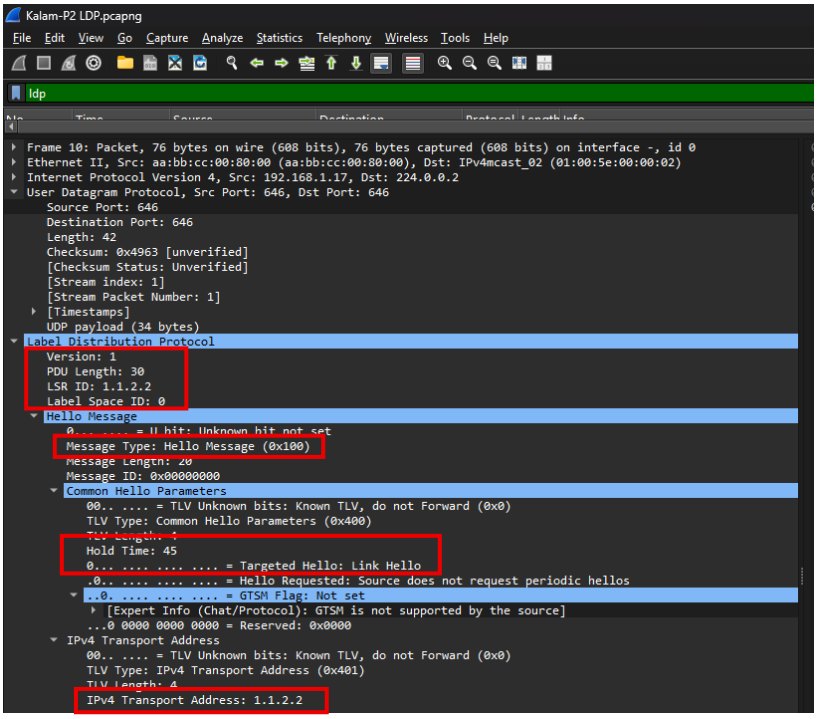

Figure 144 Kalam-P2 LDP Hello Packet LDP Header Inspection

Similar to the previous figures, Kalam-P4 also sends an LDP hello packet with the same set of parameters with different source address. In the layer 3 header, the source address is 192.168.1.18, reflecting that this is Kalam-P4 hello packet. The entire UDP header information remains the same without any changed. However, in the LDP header it remains the same except for the LSR ID which now indicates that 1.1.2.4 is the sender which is Kalam-P4.

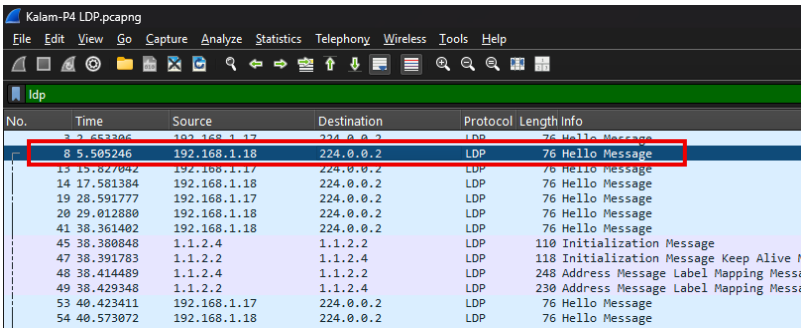

Figure 145 Kalam-P4 LDP Hello Packet

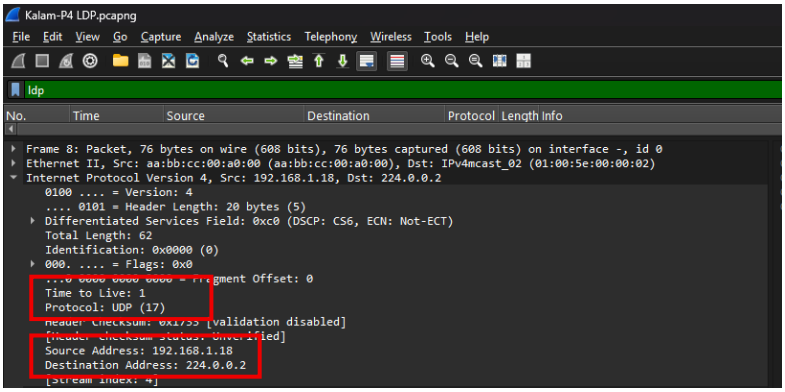

Figure 146 Kalam-P4 LDP Hello Packet Layer 3 Header Inspection

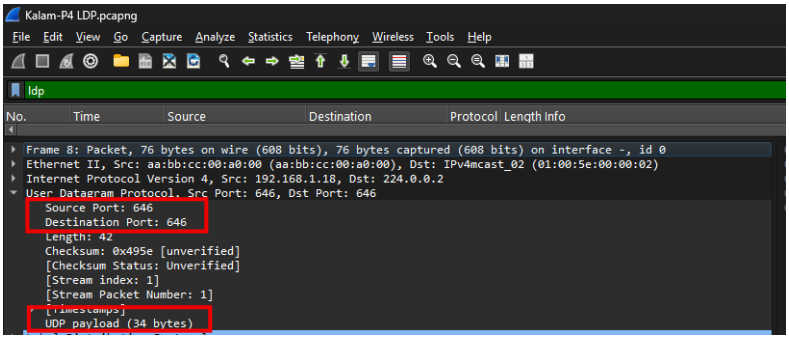

Figure 147 Kalam-P4 LDP Hello Packet UDP Header Inspection

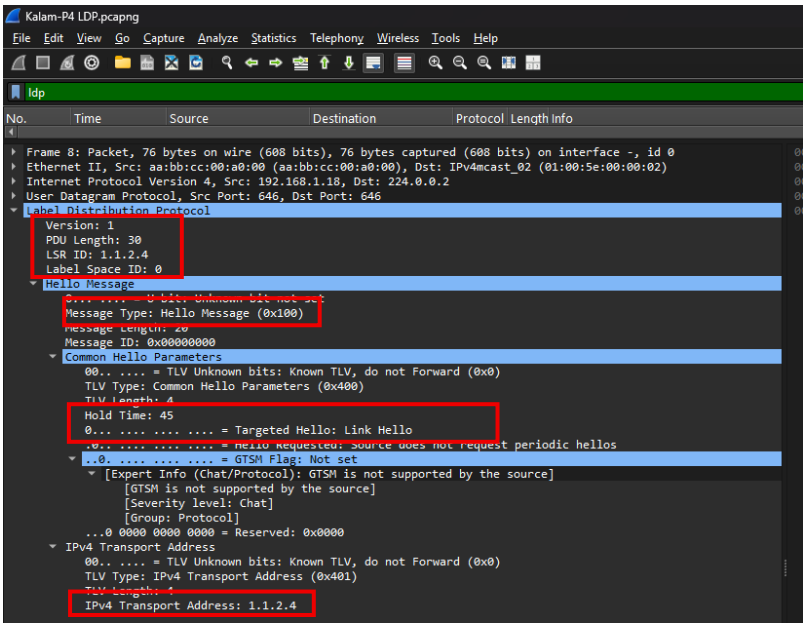

Figure 148 Kalam-P4 LDP Hello Packet LDP Header Inspection

LDP initiate Packets:

After a successful exchange of the hello packet between the routers. The LDP initiate packet are sent after the three-way-handshake. The three-way-handshake are performed between the hello packet and initiate packet phases. After the TCP three-way-handshake is perform the initiate packets are rolled out. The upcoming figures will inspect the initiate packet of Kalam-P2. In the layer 3 header, the source address of 1.1.2.2 indicates that this packet originated by Kalam-P2 to the destination address 1.1.2.4 which is Kalam-P4. Additionally, the communication now has switched from using the User Diagram Protocol (UDP) to Transmission Control Protocol (TCP), this is proof that the three-way-handshake has been established successfully also the TCP header shows the source port, which is 36847, a temporary port used to communicate to the destination port of the LDP protocol which is 646. Furthermore, the LDP header maintains some of the essential LDP information such as the LDP version, which is 1 and the LSR ID of 1.1.2.2. Moreover, the LDP header also contains the keepalive timer, the session label advertisement discipline,

session loop detection and the session receiver LSR ID which is the other router in this MPLS connection.

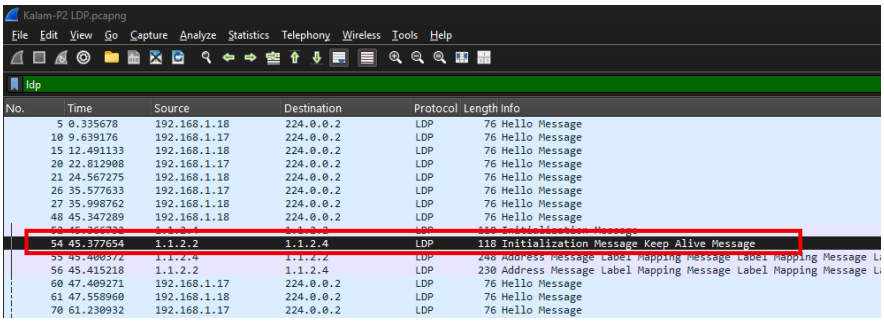

Figure 149 Kalam-P2 LDP Initiate Packet

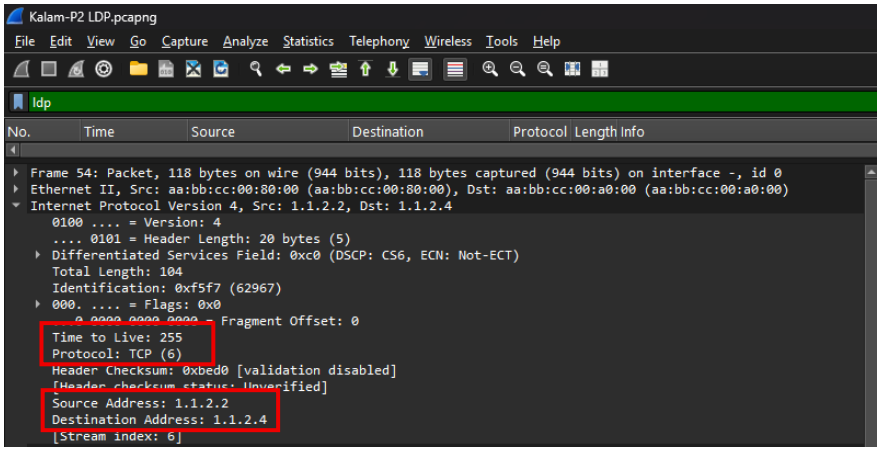

Figure 150 Kalam-P2 LDP Initiate Packet Layer 3 Header Inspection

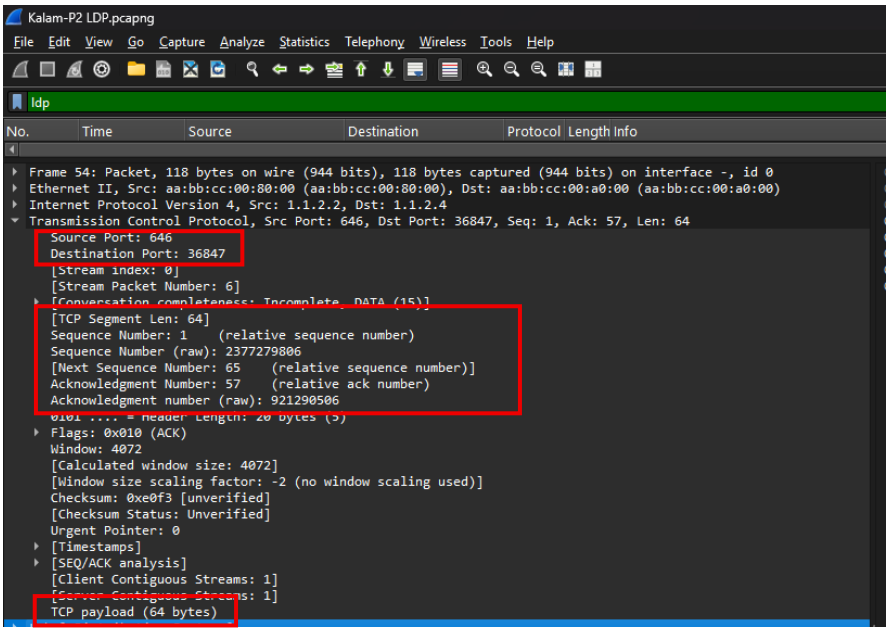

Figure 151 Kalam-P2 LDP Initiate Packet TCP Header Inspection

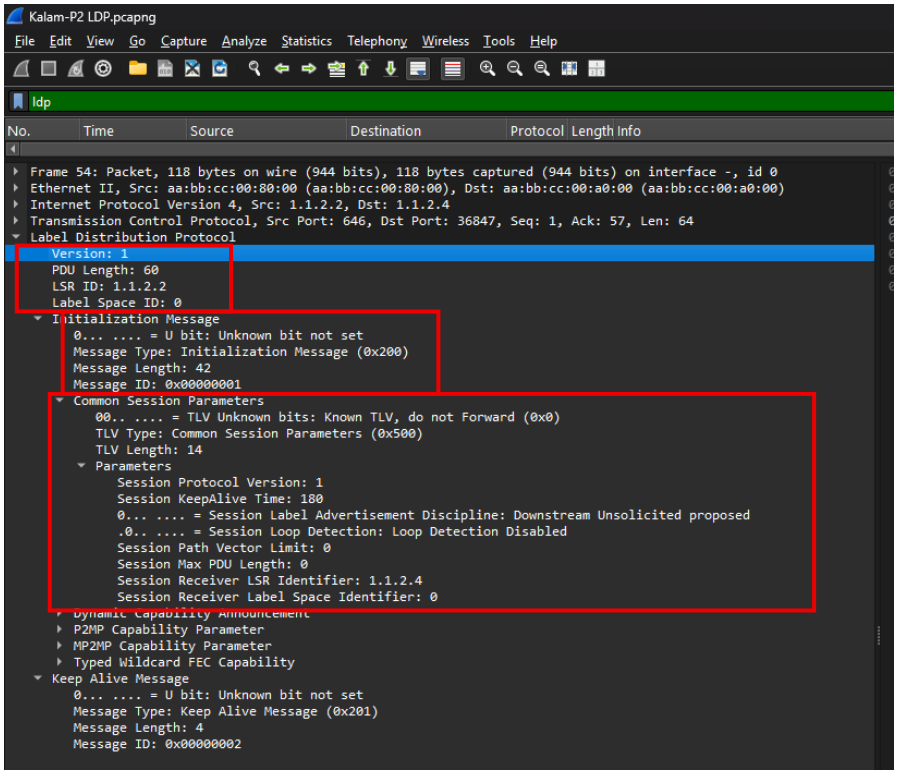

Figure 152 Kalam-P2 LDP initiate Packet LDP Header Inspection

On the other hand, Kalam-P4 also sends a corresponding LDP initiation message with the same parameters, while the information that identifies the router is changed to identify Kalam-P4.

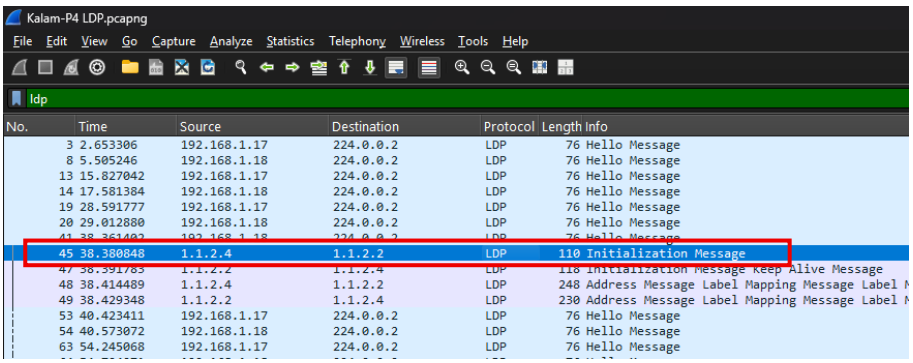

Figure 153 Kalam-P4 LDP Initiate Packet

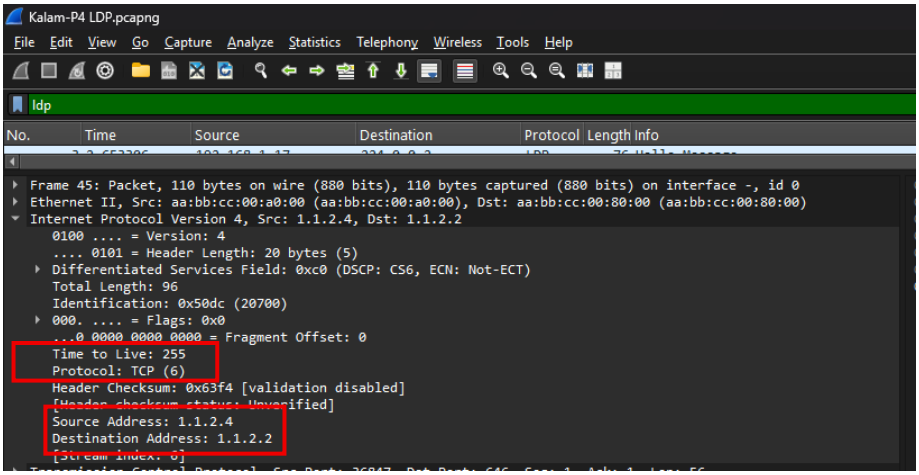

Figure 154 Kalam-P4 LDP Initiate Packet Layer 3 Header Inspection

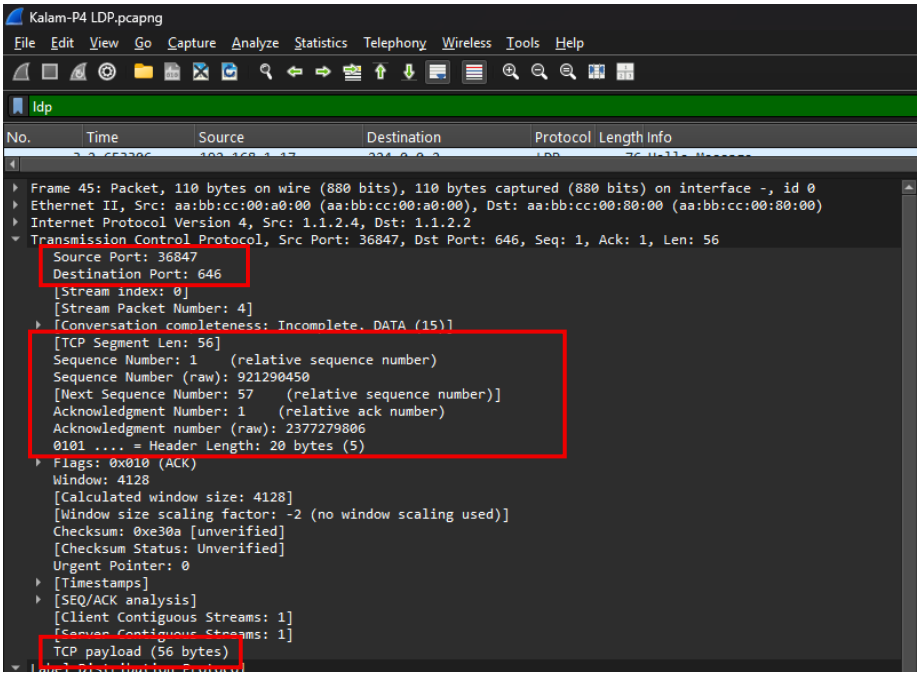

Figure 155 Kalam-P4 LDP Initiate Packet TCP Header Inspection

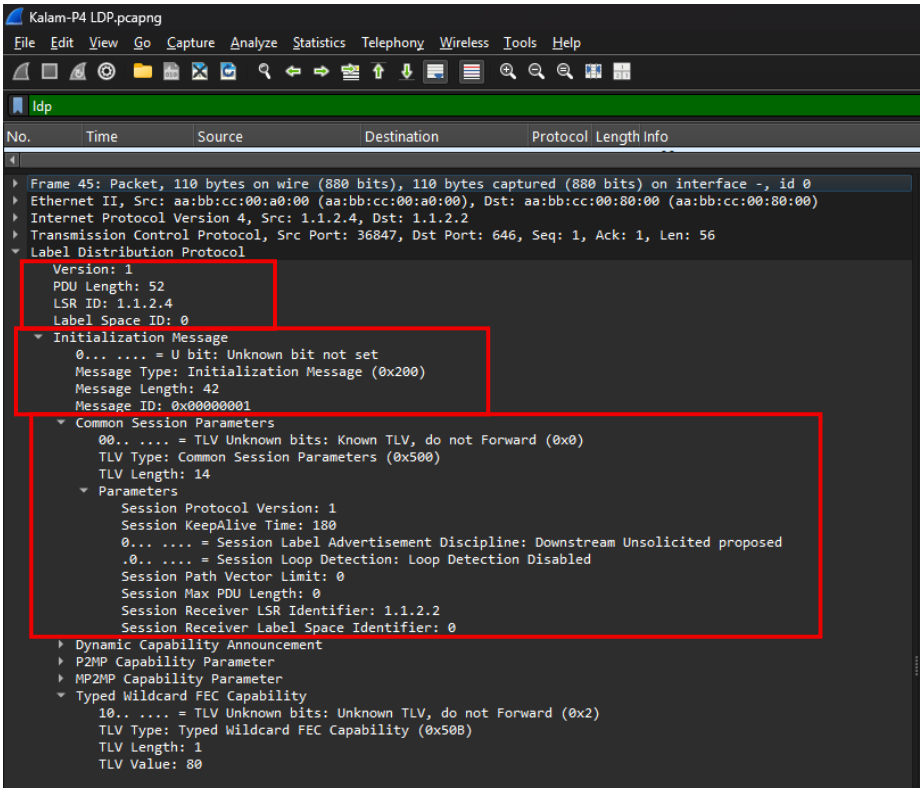

Figure 156 Kalam-P4 LDP initiate Packet LDP Header Inspection

Label Mapping Message Packet:

After the successful exchange of LDP initiation and keepalive messages between Kalam-P2 and Kalam-P4. The MPLS adjacency is now fully established. At this stage, label mapping messages are exchanged, which are used to advertise MPLS labels between the neighbors.

The figures below inspects the captured label mapping message packet from Kalam-P2. The layer 3 header of the captured packet indicates that this packet originates from Kalam-P2 since the source address is 1.1.2.2 and the destination address is 1.1.2.4. In the TCP header most of the parameters remain the same except for the sequence numbers differ from one router to another. Furthermore, the LDP header contains all the advertised labels with their corresponding prefixes.

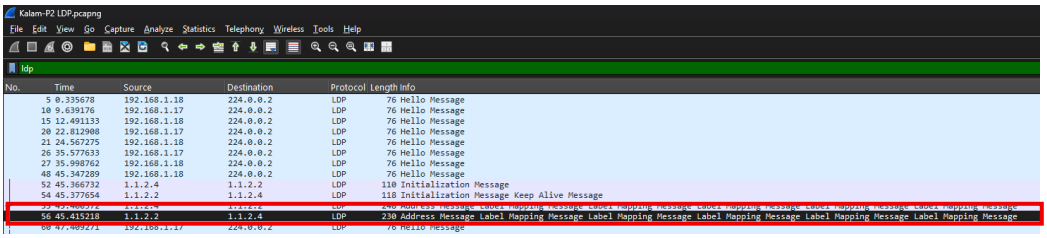

Figure 157 Kalam-P2 LDP Label Mapping Message Packet

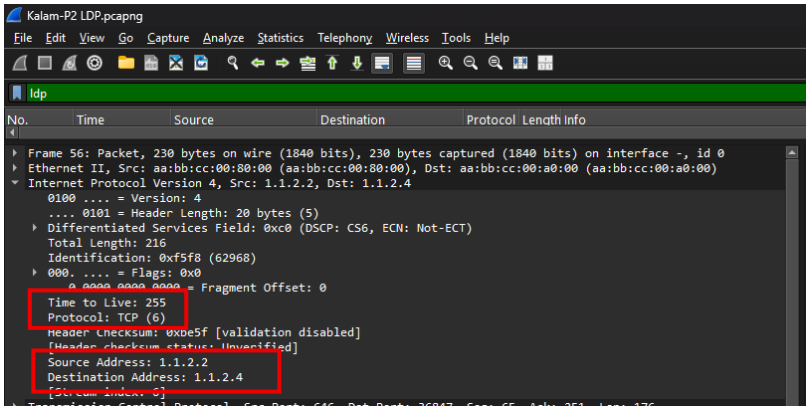

Figure 158 Kalam-P2 LDP Label Mapping Message Packet Layer 3 Header Inspection

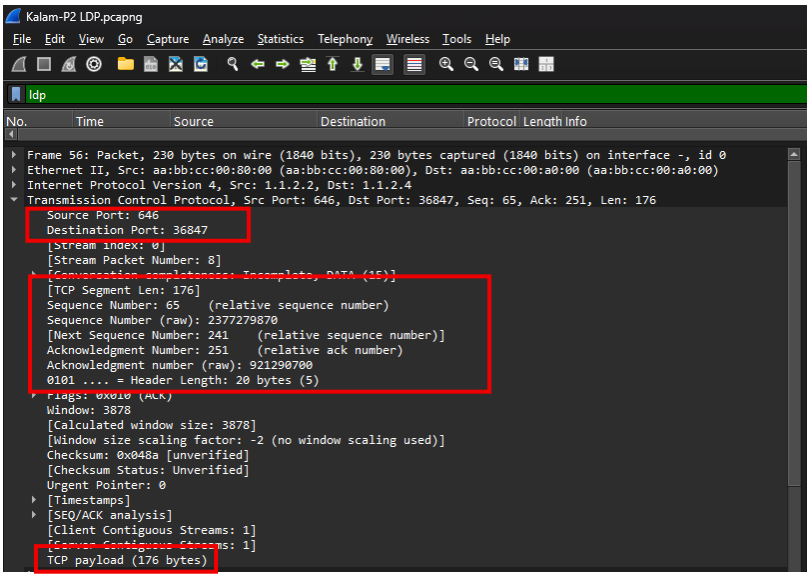

Figure 159 Kalam-P2 LDP Label Mapping Message Packet TCP Header Inspection

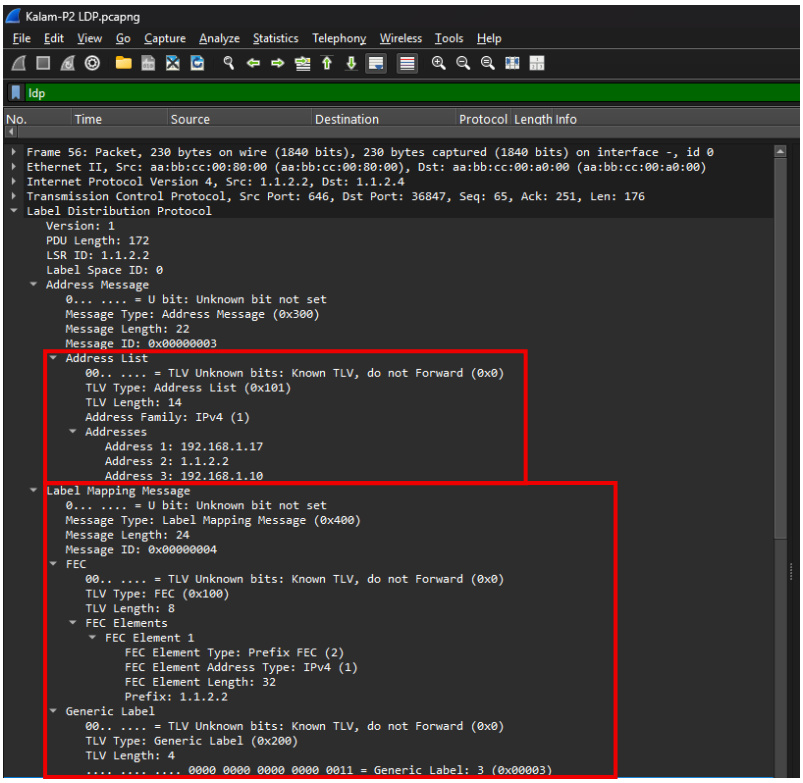

Figure 160 Kalam-P2 LDP Label Mapping Message Packet LDP Header Inspection – Part A

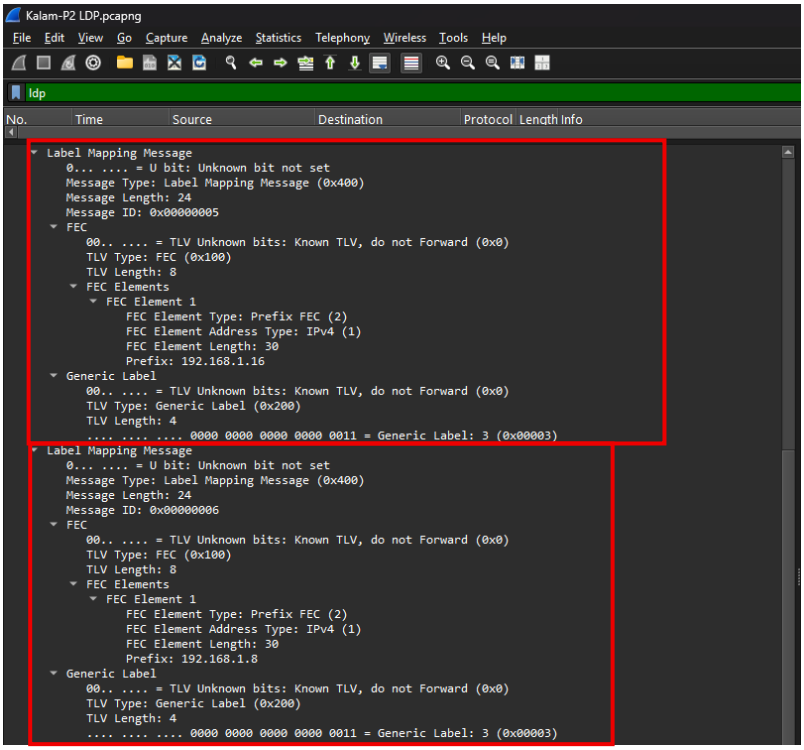

Figure 161 Kalam-P2 LDP Label Mapping Message Packet LDP Header Inspection – Part B

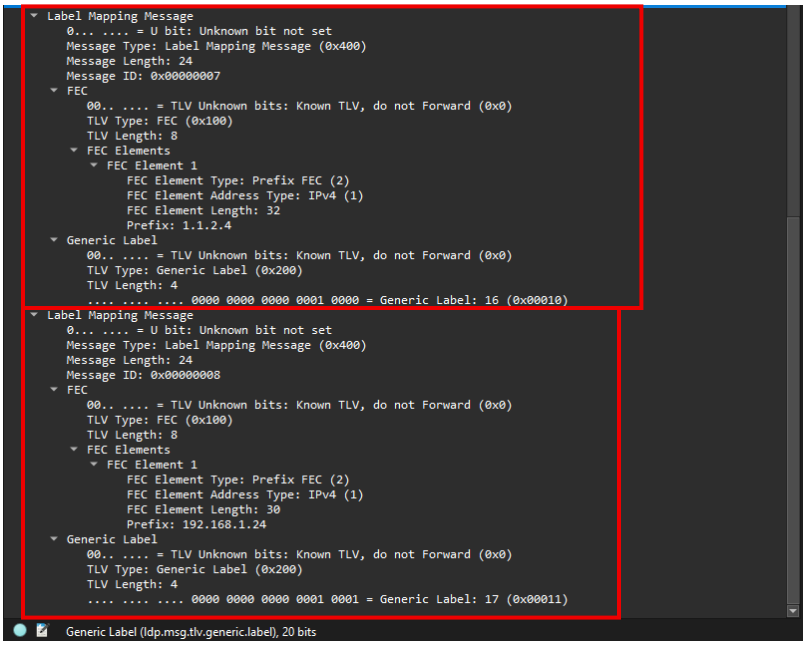

Figure 162 Kalam-P2 LDP Label Mapping Message Packet LDP Header Inspection – Part C

Similar thing for Kalam-P4, it will send a label mapping message to Kalam-P2. The figures below inspects the Kalam-P4 packets.

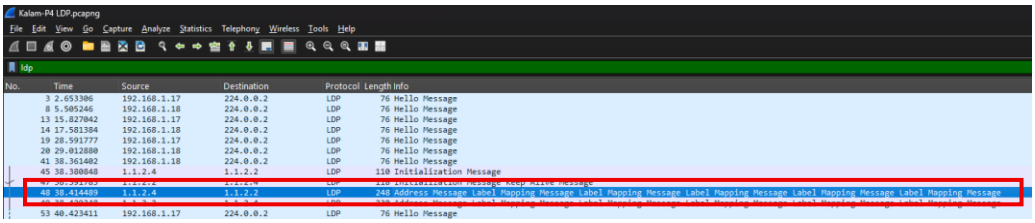

Figure 163 Kalam-P4 LDP Label Mapping Message Packet

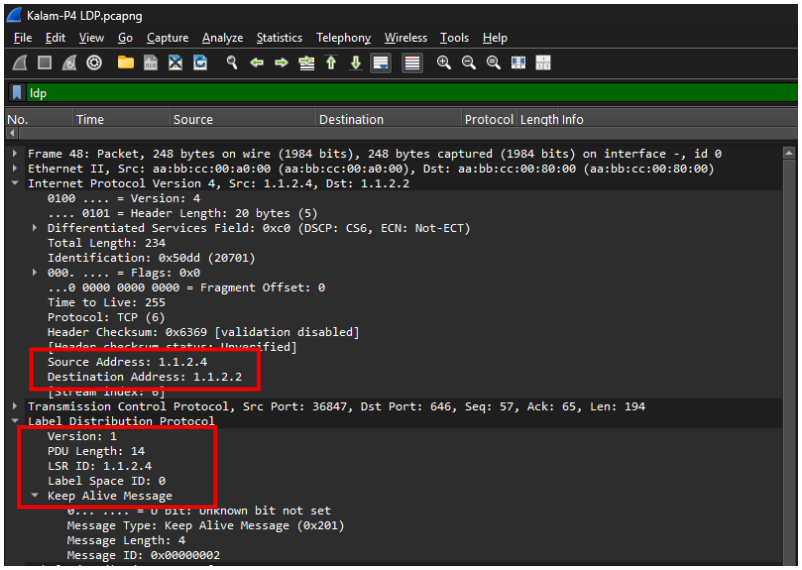

Figure 164 Kalam-P4 LDP Label Mapping Message Packet Layer 3 Header Inspection

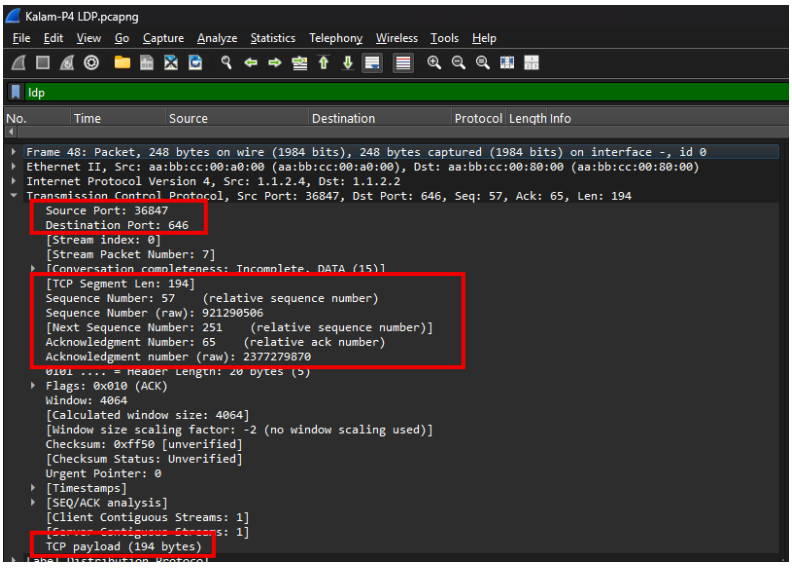

Figure 165 Kalam-P4 LDP Label Mapping Message Packet TCP Header Inspection

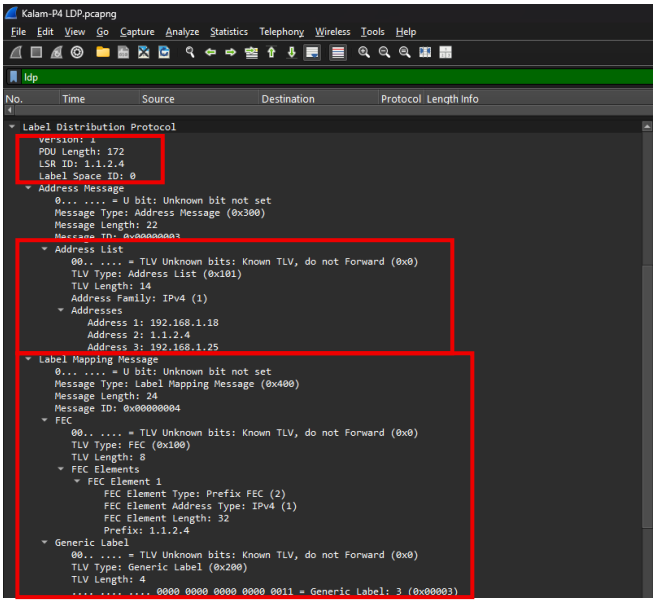

Figure 166Kalam-P4 LDP Label Mapping Message Packet LDP Header Inspection – Part A

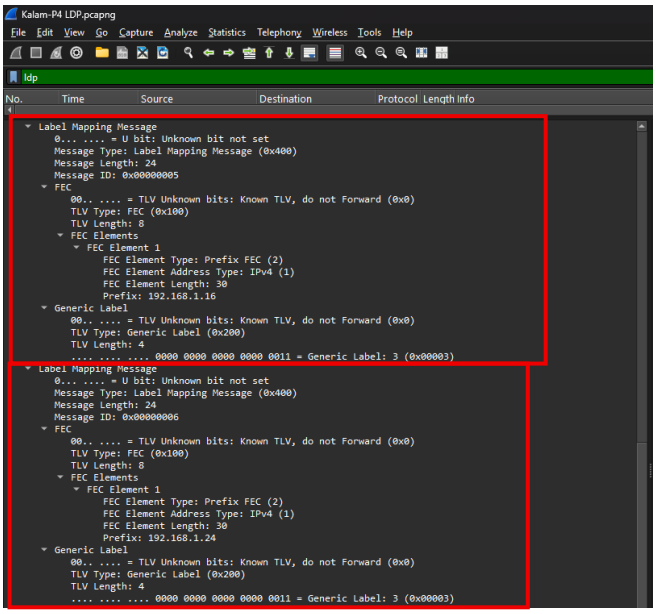

Figure 167 Kalam-P4 LDP Label Mapping Message Packet LDP Header Inspection – Part B

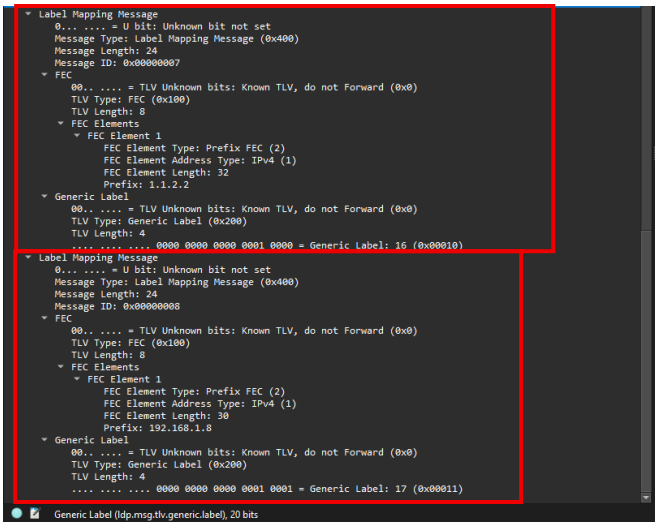

Figure 168 Kalam-P4 LDP Label Mapping Message Packet LDP Header Inspection – Part C

Traffic engineering configuration for Kalam Telecom routers

Traffic engineering is applied on the MPLS backbone layer and configured om certain devices. MPLS-TE is applied to provides enhanced traffic management by defining explicit label switched path. MPLS-TE operate in conjunction with the Internal routing protocol by enabling the IGP extension to support TE.

implementation details of this section:

- Enable MPLS-TE on the PE and P router globally
- Enable MPLS TE on the interfaces
- Assigning RSVP values
- Enable MPLS-TE extension on the IGP
- Create the Tunnel interfaces

The figure below highlights the PE router that will host MPLS Tunnels:

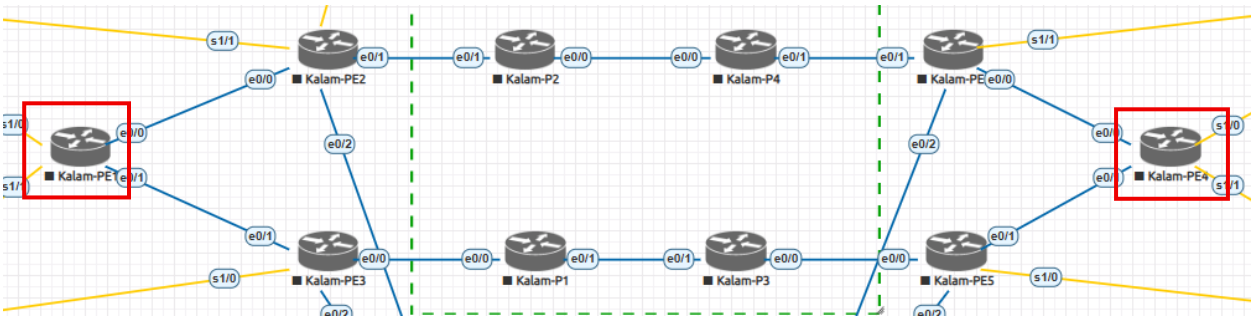

Figure 169 Devices That Host The Tunnel

MPLS-TE Configuration:

The following figures demonstrate the configuration steps required to enable MPLS-TE on the Kalam-PE1 through Kalam-PE6 in addition to P1 to P4. There will be 2 tunnel interfaces, the first tunnel will be from PE1 to PE4, and the second tunnel will be from PE4 to PE1.

However, unlike the MPLS LDP, MPLS-TE does not require extensive configuration since the MPLS-TE is an extension of the IGP which is already configured above.

MPLS-TE also needs a router ID similarly to the underlaying IGP which MPLS-TE transverse over TE's router ID will follow the same approach as IGP's router ID. PE1 takes 1.1.1.1, PE2 takes 1.1.1.2, PE3 takes 1.1.1.3, PE4 takes 1.1.1.4, PE5 takes 1.1.1.5 and PE6 takes 1.1.1.6. Also, the P1 takes 1.1.2.1, P2 takes 1.1.2.2, P3 take 1.1.2.3 and P4 1.1.2.4. in addition, RSVP is enabled on the MPLS-TE links with a reserved bandwidth value which defines the amount of bandwidth that are allocated for the TE label switched path. The RSVP bandwidth is used during the MPLS-TE computation process to ensure sufficient resources are available before using the path to establish the tunnels. Furthermore, this section also covers the configuration of the tunnel interfaces by assigning the loopback 0 as the IP address of the tunnel also the tunnel mode is set to be a MPLS-TE additionally, the destination of this tunnel is set to the loopback0 of Kalam-PE4.

Explaining the commands:

- “Mpls traffic-eng tunnels” ⇨ used to configure and enable the MPLS-TE on the router.

- “ip rsvp bandwidth <value>” ⇨ reserve a certain bandwidth usually in byte for the MPLS-TE tunnel.

- “ip unnumbered <interface ID>” ⇨ configure the tunnel to use the specific interface as the IP address of the tunnel.

- “tunnel mode mpls traffic-eng” ⇨ set the mode of the tunnel to MPLS TE.

- “tunnel destination <destination IP>” ⇨ set the destination of the tunnel.

- “tunnel mpls traffic-eng autoroute announce” ⇨ allow the MPLS-TE tunnel to be automatically installed in the routing table.

- “tunnel mpls traffic-eng priority <value> <value>” ⇨ sets priority of the setup and holding of the MPLS-TE.

- “tunnel mpls traffic-eng bandwidth <value>” ⇨ set the amount that the tunnel will always use to transfer data.

- “tunnel mpls traffic-eng path-option 1 dynamic” ⇨ set the calculation to dynamic mode which will uses the IGP calculation method.

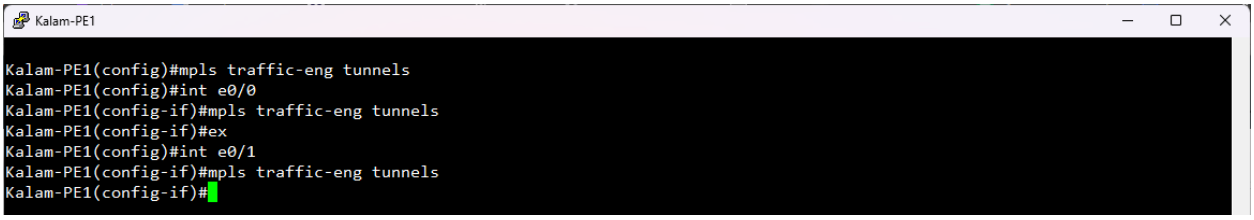

Figure 170 Kalam-PE1 Enabling TE Command on the Global and interfaces

Figure 171 Kalam-PE1 RSVP Configuration Commands

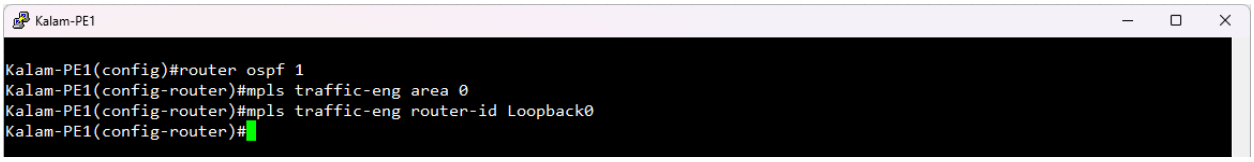

Figure 172 Kalam-PE1 MPLS TE IGP Extension Configuration Command

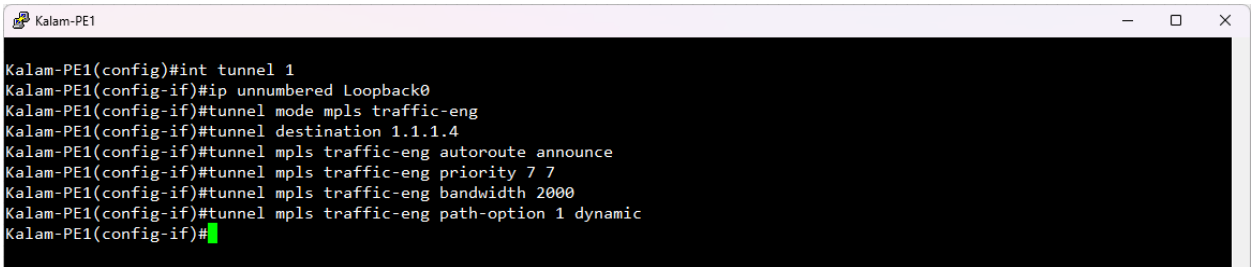

Figure 173 Kalam-PE1 Tunnel Configuration Command

MPLS-TE verification:

The following figures outline the MPLS-TE information, including some of the key tunnel parameters such as the router that initiate the tunnel and the destination address of the other router in the tunnel. The tunnel status is also shown indicating if the tunnel is operational. In addition to other important information such as the outgoing label value, source IP, tunnel id and tunnel instance. Furthermore, it also outlines which path the tunnel it taking along with the RSVP information plus the uptime of the tunnel. Additionally, the other figure also shows the OSPF TE information, including the number of tunnels that are running inside the OSPF routing protocol along with the OSPF-TE router ID. The OSPF-TE maximum bandwidth is also visible with the reserved bandwidth for the TE tunnels. Finally, the last two figures show the OSPF opaque type-10 LSAs information which are primarily used to stores and exchange the RSVP and TE information since those LSAs already transverse over the IGP, which is OSPF. The OSPF Opaque LSAs includes the LSA aging time, opaque ID, the advertising router of the opaque LSA. In addition to the LSA length.

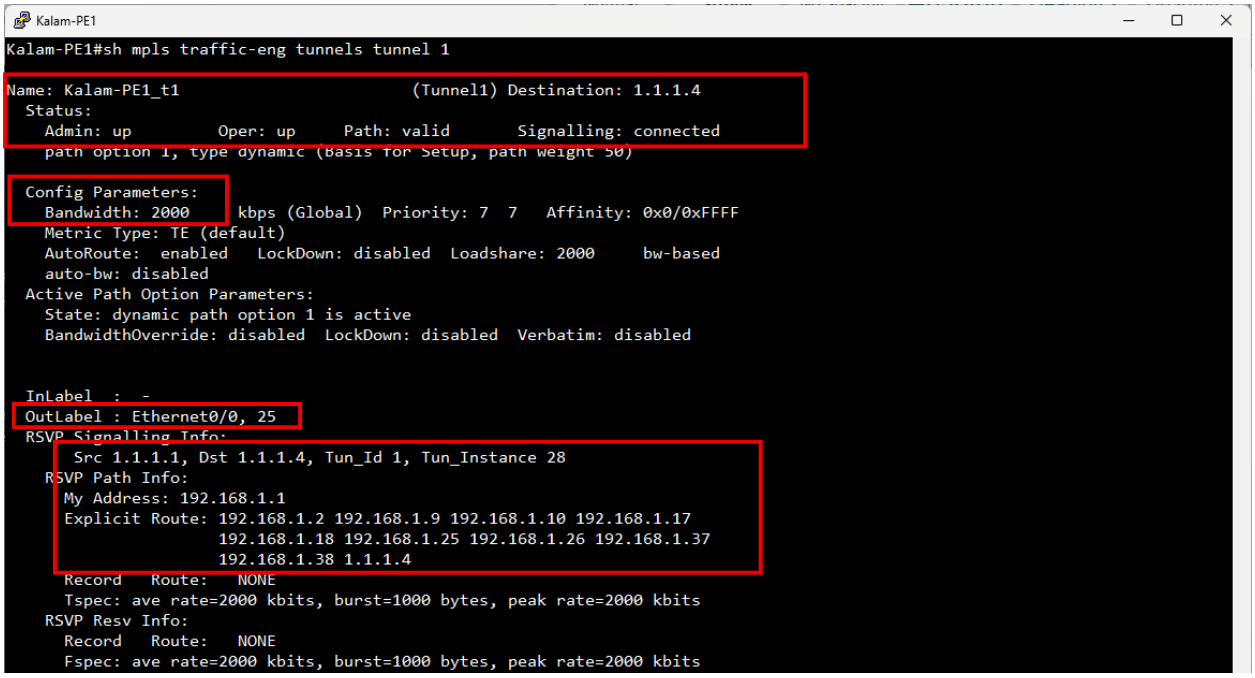

Figure 174 Kalam-PE1 MPLS-TE Verification Information - Part A

```
  Shortest Unconstrained Path Info:
    Path Weight: 50 (TE)
    Explicit Route: 192.168.1.1 192.168.1.2 192.168.1.9 192.168.1.10
                    192.168.1.17 192.168.1.18 192.168.1.25 192.168.1.26
                    192.168.1.37 192.168.1.38 1.1.1.4
  History:
    Tunnel:
      Time since created: 5 minutes, 30 seconds
      Time since path change: 1 minutes, 25 seconds
      Number of LSP IDs (Tun_Instances) used: 28
    Current LSP:
      Uptime: 1 minutes, 25 seconds
Kalam-PE1#
```

Figure 175 Kalam-PE1 MPLS-TE Verification Information - Part B

```
Kalam-PE1

Kalam-PE1#sh ip ospf mpls traffic-eng link

          OSPF Router with ID (11.11.11.1) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 4.

  Links in hash bucket 8.
    Link is associated with fragment 1. Link instance is 4
      Link connected to Broadcast network
      Link ID : 192.168.1.2
      Interface Address : 192.168.1.1
      Admin Metric te: 10 igp: 10
      Maximum bandwidth : 1250000
      Maximum reservable bandwidth : 625000
      Number of Priority : 8
      Priority 0 : 625000       Priority 1 : 625000
      Priority 2 : 625000       Priority 3 : 625000
      Priority 4 : 625000       Priority 5 : 625000
      Priority 6 : 625000       Priority 7 : 375000
      Affinity Bit : 0x0
```

Figure 176 MPLS-TE Routing Information

```
Kalam-PE1

Kalam-PE1#$database opaque-area  | begin  MPLS TE router ID : 1.1.1.2
    MPLS TE router ID : 1.1.1.2

    Number of Links : 0

  LS age: 267
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.1
  Opaque Type: 1
  Opaque ID: 1
  Advertising Router: 1.1.1.4
  LS Seq Number: 80000002
  Checksum: 0x2C44
  Length: 124
  Fragment number : 1

    Link connected to Broadcast network
      Link ID : 192.168.1.37
      Interface Address : 192.168.1.38
      Admin Metric : 10
      Maximum bandwidth : 1250000
      Maximum reservable bandwidth : 625000
      Number of Priority : 8
      Priority 0 : 625000       Priority 1 : 625000
      Priority 2 : 625000       Priority 3 : 625000
      Priority 4 : 625000       Priority 5 : 625000
      Priority 6 : 625000       Priority 7 : 375000
      Affinity Bit : 0x0
      IGP Metric : 10

    Number of Links : 1
```

Figure 177 MPLS TE Opaque Database Information

Quality of Services configuration for Kalam Telecom routers

QoS is implemented across the entire network to prioritize the traffic based on the service requirement and usage. QoS allows different traffic to be classified and forwarded according to their importance level, which ensures that critical data will have special treatment over less critical data. By applying QoS to the infrastructure packets are controlled to reduce traffic congestion, minimize delays and maintain consistent network performance.

implementation details of this section:

- Create a class map for incoming customer traffic
- Create a policy map to define QoS actions for incoming customer traffic
- Apply the service policy on the customer facing interface
- Create a class map for traffic traversing over the ISP network
- Create a policy map to define QoS action for traffic traversing over the ISP network
- Apply the service policy on the core interface

The figure below highlights the Interfaces that will have QoS configured on:

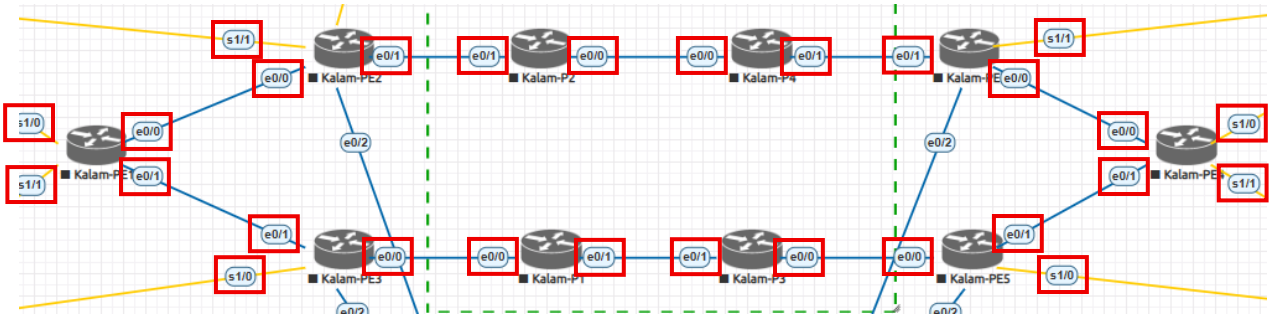

Figure 178 QoS Configured Interface

QoS Configuration process:

To ensure an efficient and excellent QoS for the enterprises customers of Kalam Telecom, the QoS configuration will focus on prioritizing the critical business data across all the

network to differentiate them from the other types of traffic. The QoS does not require extensive configuration compared to other protocols so this section might be shorter than the others. QoS primarily focuses on specifying which traffic to match using the class map then defining how that traffic should be handled using a policy map and finally, applying these class and policy maps to interface through a service policy.

The QoS will be configured on all the ISP devices from Kalam-PE1, PE2, PE3, PE4, PE5, PE6, P1, P2, P3 and P4.

Class Map:

Class maps are mainly used to identify specific types of network traffic. It defines the matching criteria that are used to determine which packet belongs to which traffic class such as protocol types or by DSCP values which is a way to group similar traffic together in different prioritize groups.

Explaining commands:

- "class-map <match type> <class map name>" ⇨ defines a traffic by specifying how packets should be matched.
- "match protocol <protocol name>" ⇨ identifies the specific protocol or traffic type to be classified.

Figure 179 Kalam-PE1 QoS Matching Protocols Using Class Map

Policy Map:

Policy maps are mainly used to define the action that should be applied to the traffic once it has been classified and identified with set of rules by the class maps. The policy map

action may include changing the priority level, marking packet with certain DSCP values or applying queuing.

Explaining commands:

- “policy-map <policy map name>” ⇨ defines how the matched traffic will be handled.
- “set dscp <dscp value>” ⇨ mark the classified traffic with a DSCP value

Figure 180 Kalam-PE1 QoS Applying QoS Classification Using Policy Map

Service Policy:

Service policies are mainly used to apply a certain policy map to a specific interface of networking devices alongside with the direction either in or out. once the service policy is applied it will enforce the rules that has been set by the policy map on any packet that passes through it.

Explaining commands:

- “service-policy <direction> <policy map name>” ⇨ Applies the QoS policy to an interface.

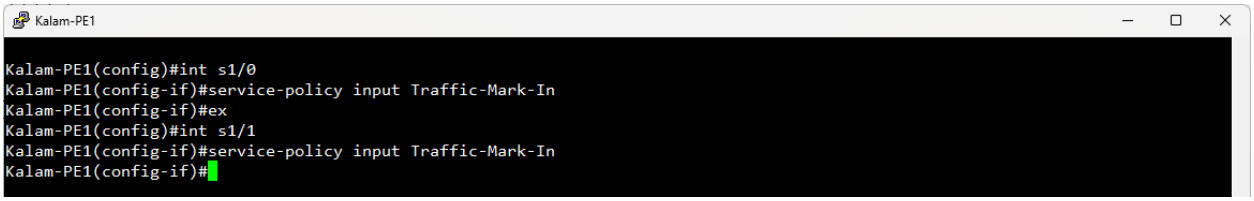

Figure 181 Assigning the QoS Configuration to an Interfaces Using Service Policy

Verification for the QoS classification:

for the verification section of the QoS, Wireshark will be used to capture and inspects the ICMP packet in order to verify if the DSCP values has modified as expected. This approach has been taken due to the limited availability of resources to demonstrate QoS behavior under real world traffic conditions.

The next figures will illustrate the DSCP value for the ICMP before and after it passes through an interface with a QoS service policy configuration. In the first figure the packet has a source of 74.211.4.2 and a destination of 74.211.4.1, which indicates that the packet did not pass through the ISP facing interface. As a result, the Differentiated Services Code Point (DSCP) value remains at the default setting. However, in the second figure, the packet has a source address of 74.211.4.1 and a destination address of 74.211.4.2, confirming that the packet is a response from the ISP router. The differentiate service field shows a DSCP value of af31, which mean that the QoS service policy has successfully modified the DSCP value of the ICMP as expected.

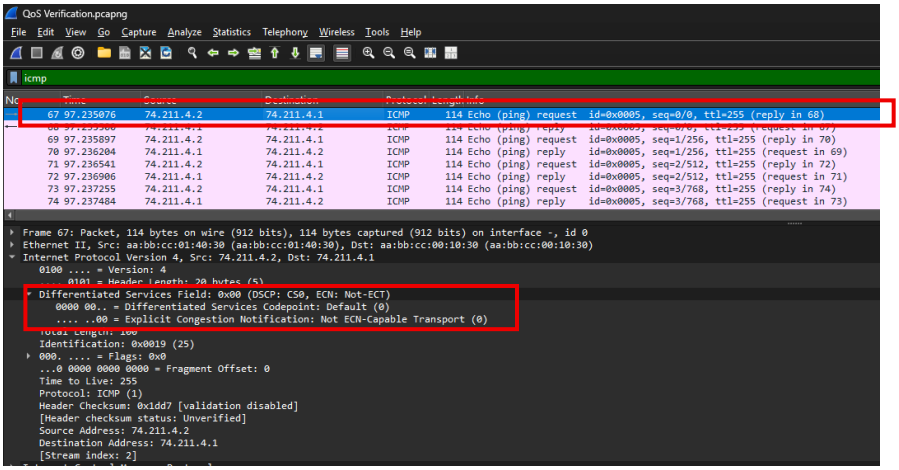

Figure 182 Kalam-PE1 ICMP Packet Before QoS

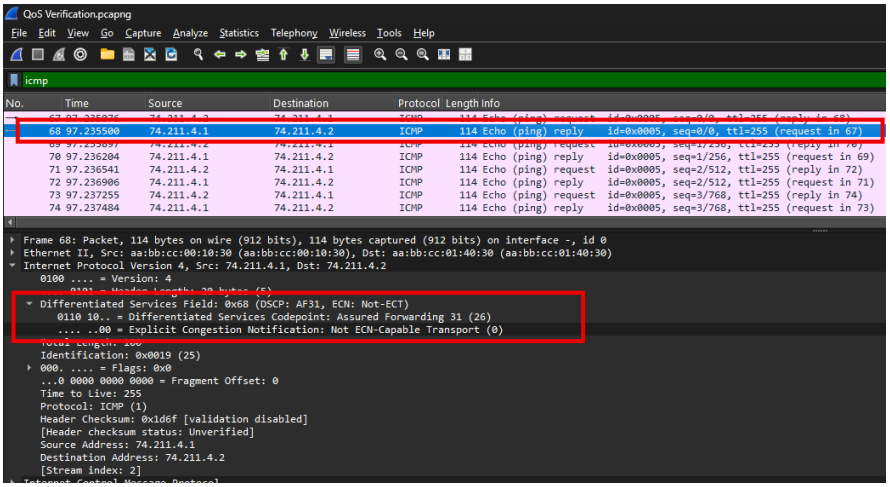

Figure 183 Kalam-PE1 ICMP Packet After QoS

AAA and Syslog service configuration

Authentication, authorization and accounting (AAA) is an essential service that provides a centralized system for managing access to network devices. Authentication is used to verify whether the user is allowed to access the devices and resources or not, authorization is mainly used to define the level of access the user have after authenticating with the AAA and accounting is used to records the user activities for monitoring purposes.

Syslog complements the AAA by adding centralized logging and monitoring of network activities. While the AAA controls who can access the network resources and what privileges they have, the syslog logs and stores the messages that are generated by the network devices, such as authentication messages, configuration changes and system messages. Syslog enables the network administrator to monitor the network behavior from a single place.

AAA configuration process:

The next figures will demonstrate the configuration process of the AAA server. starting with the creation of the Open Database connectivity (ODBC) and the definition of the database connectivity name. This section also illustrate how to create a user's within the AAA database as well as how to display and verify the configured users. In addition, it also covers the configuration of AAA authentication and accounting ports on the AAA service. Finally, the router side of configuration is also presented, where AAA parameters such as the login method, backup login method, authentication port and accounting port. The table below shows the local username and password along side with the radius username and password.

Usernames & Passwords		
Username	Password	Device
LocalAdmin	123456	Local Device
RadAdmin	654321	Radius Server

Table 6 AAA Username and Password

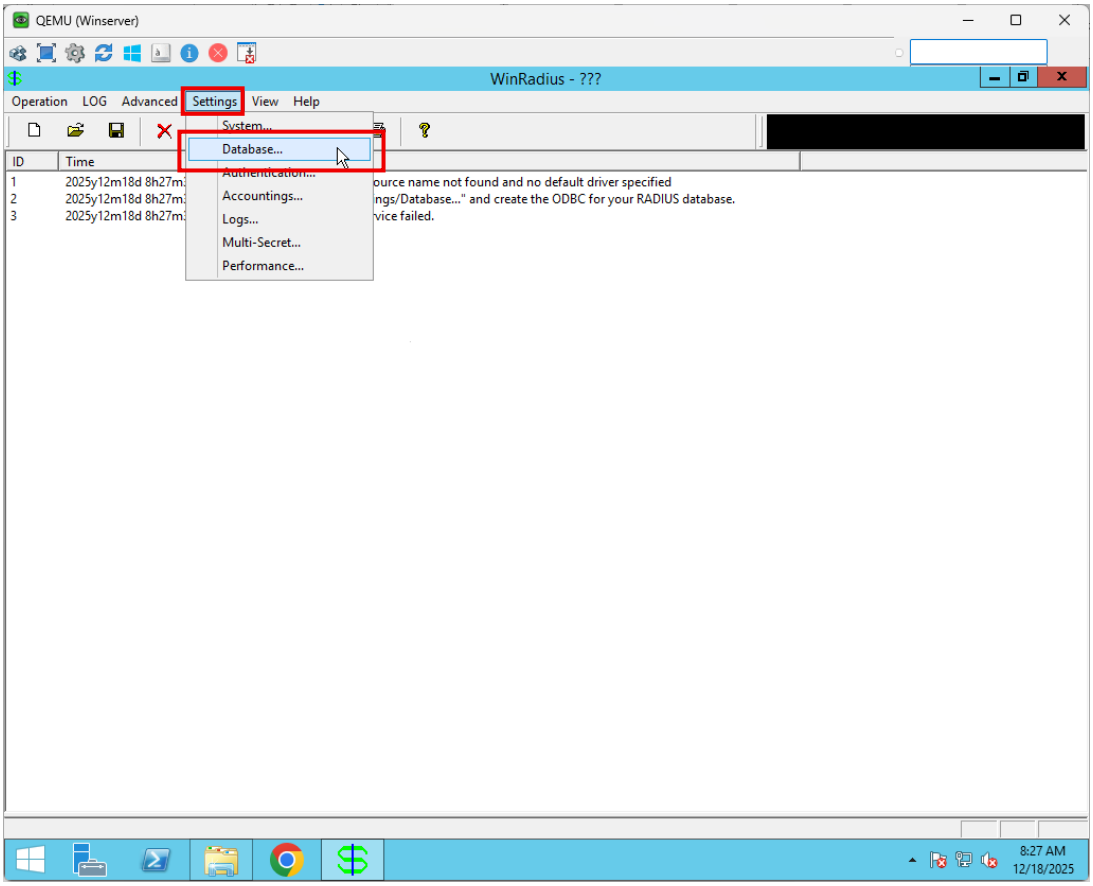

Figure 184 AAA WinRadius ODBC Creation – Part A

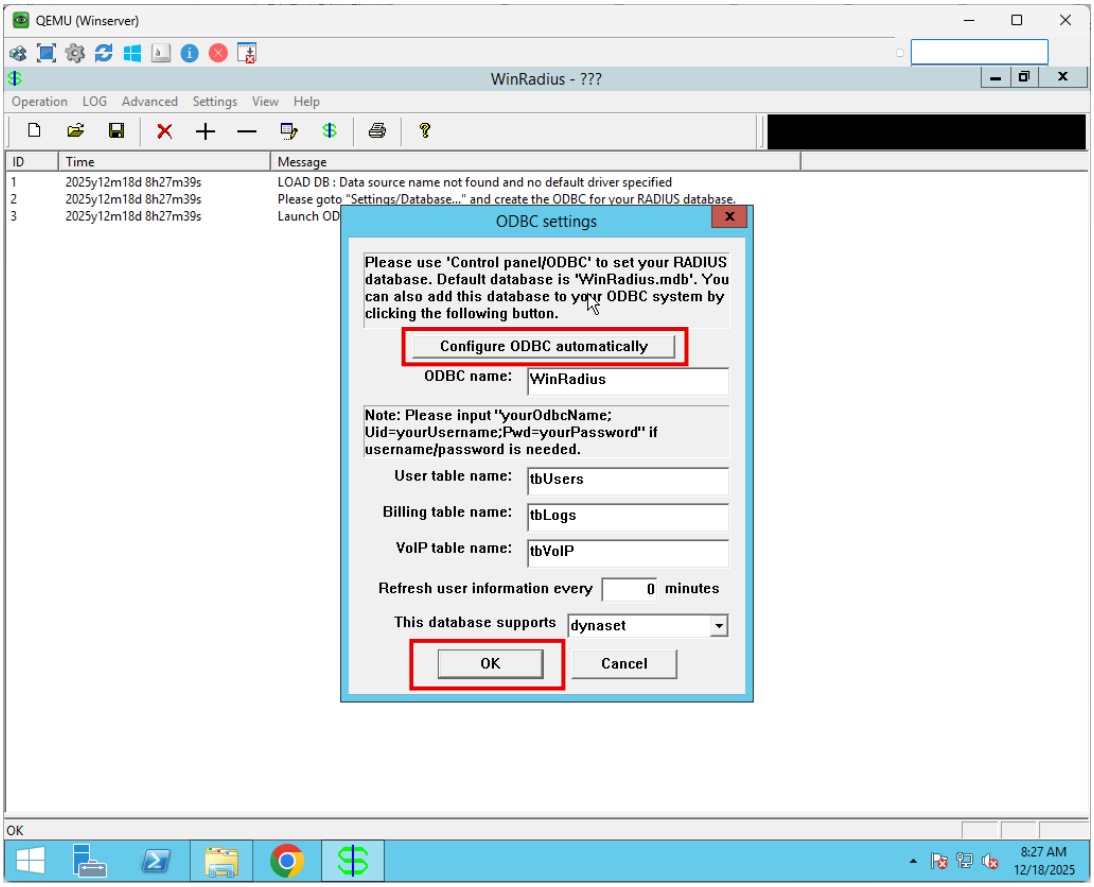

Figure 185 AAA WinRadius ODBC Creation – Part B

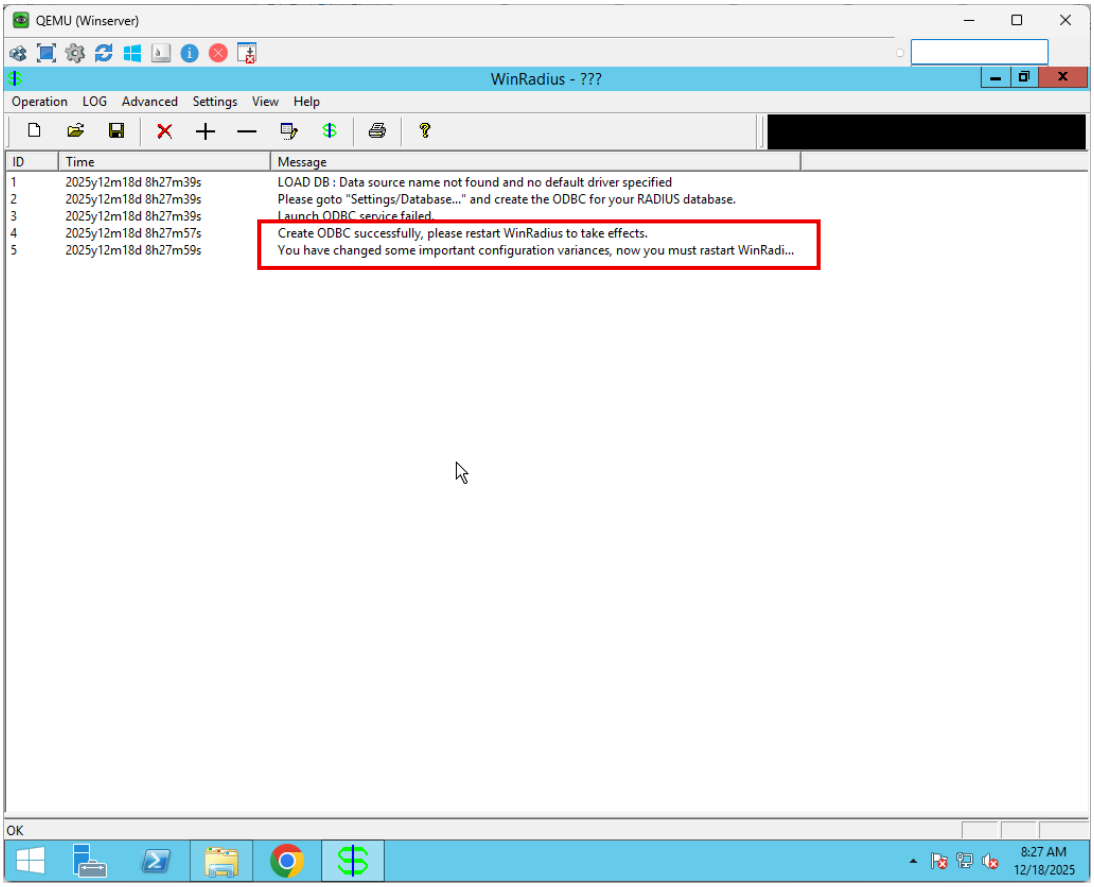

Figure 186 AAA WinRadius ODBC Creation – Part C

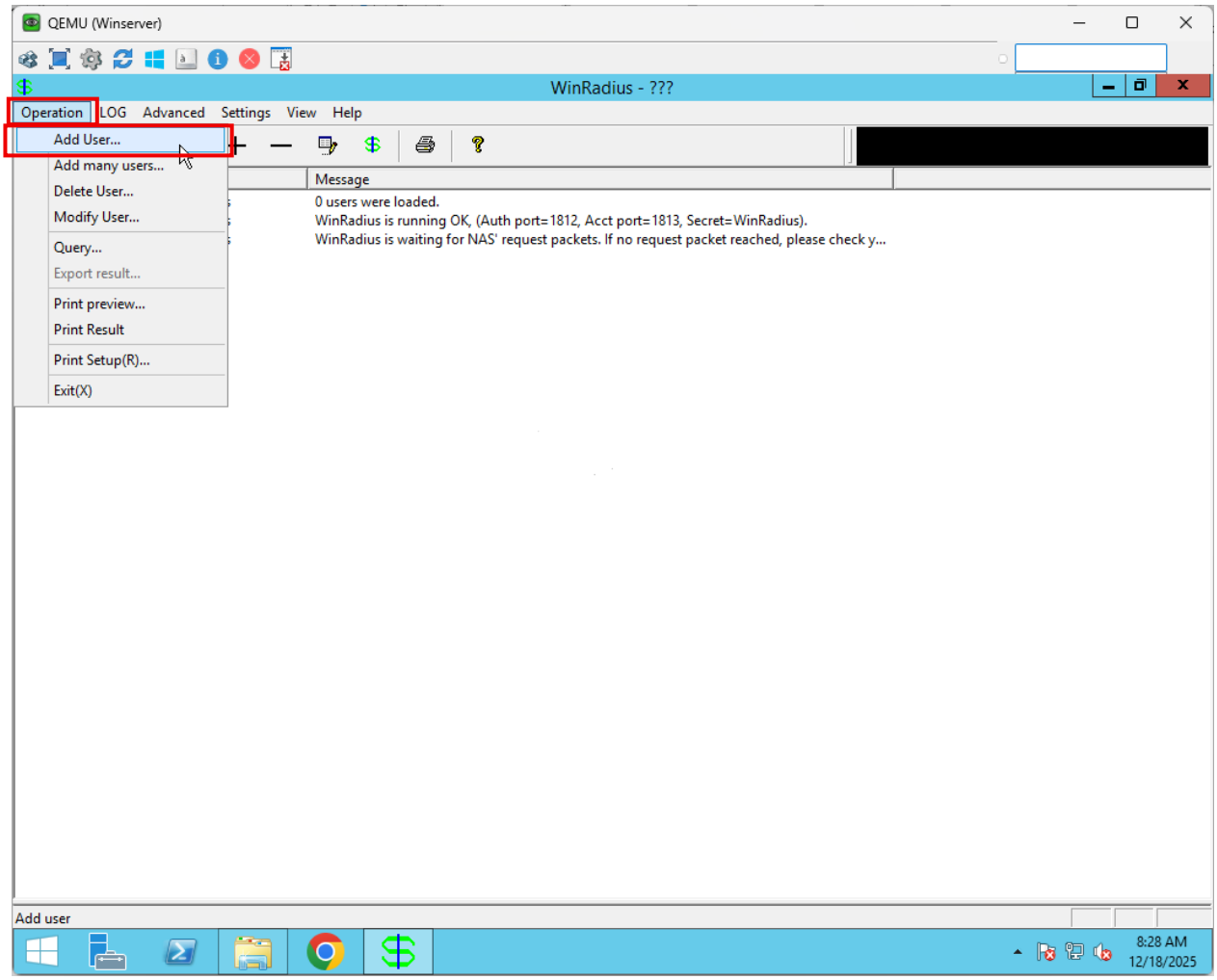

Figure 187 AAA WinRadius Creating User - Part A

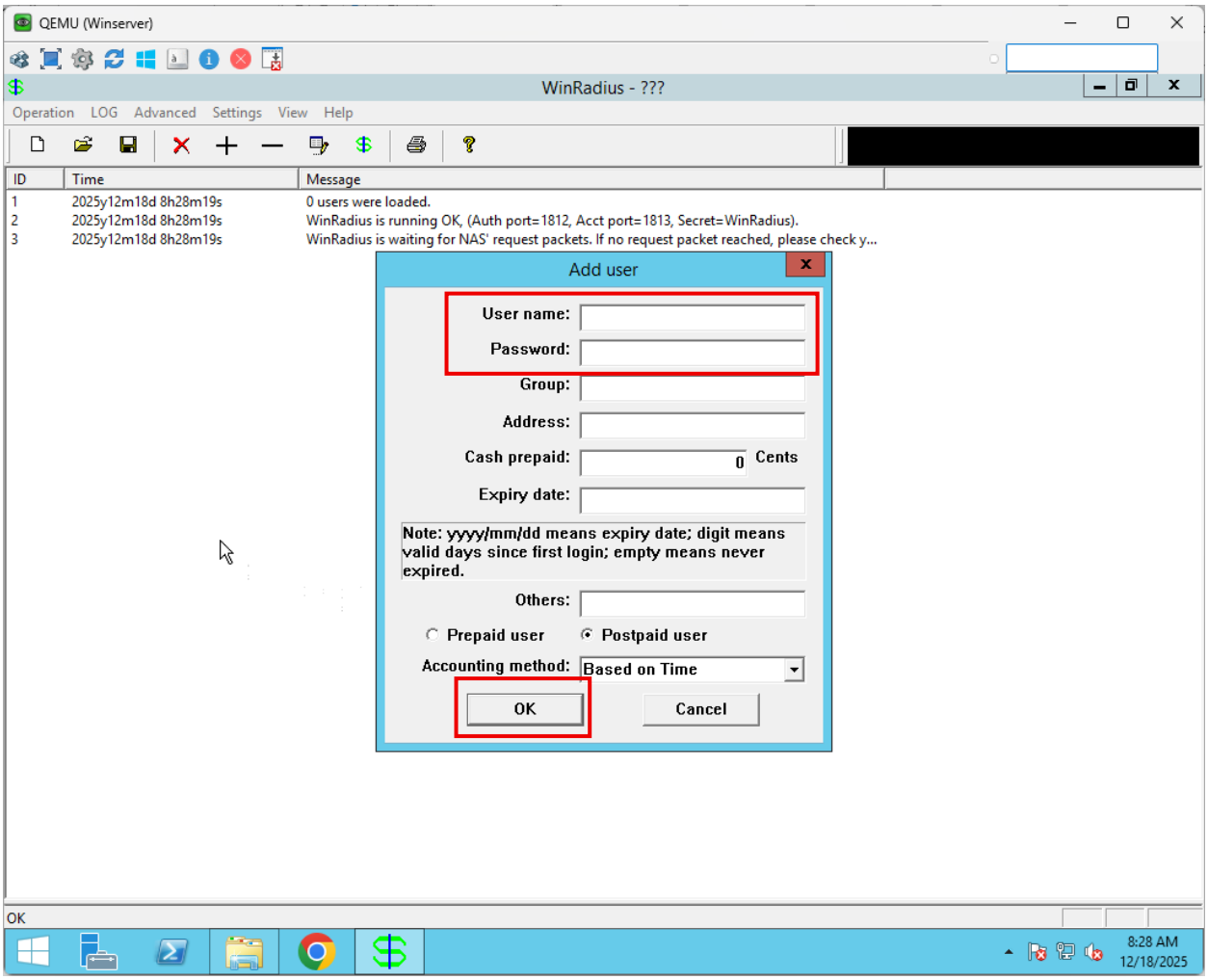

Figure 188 WinRadius Creating User - Part B

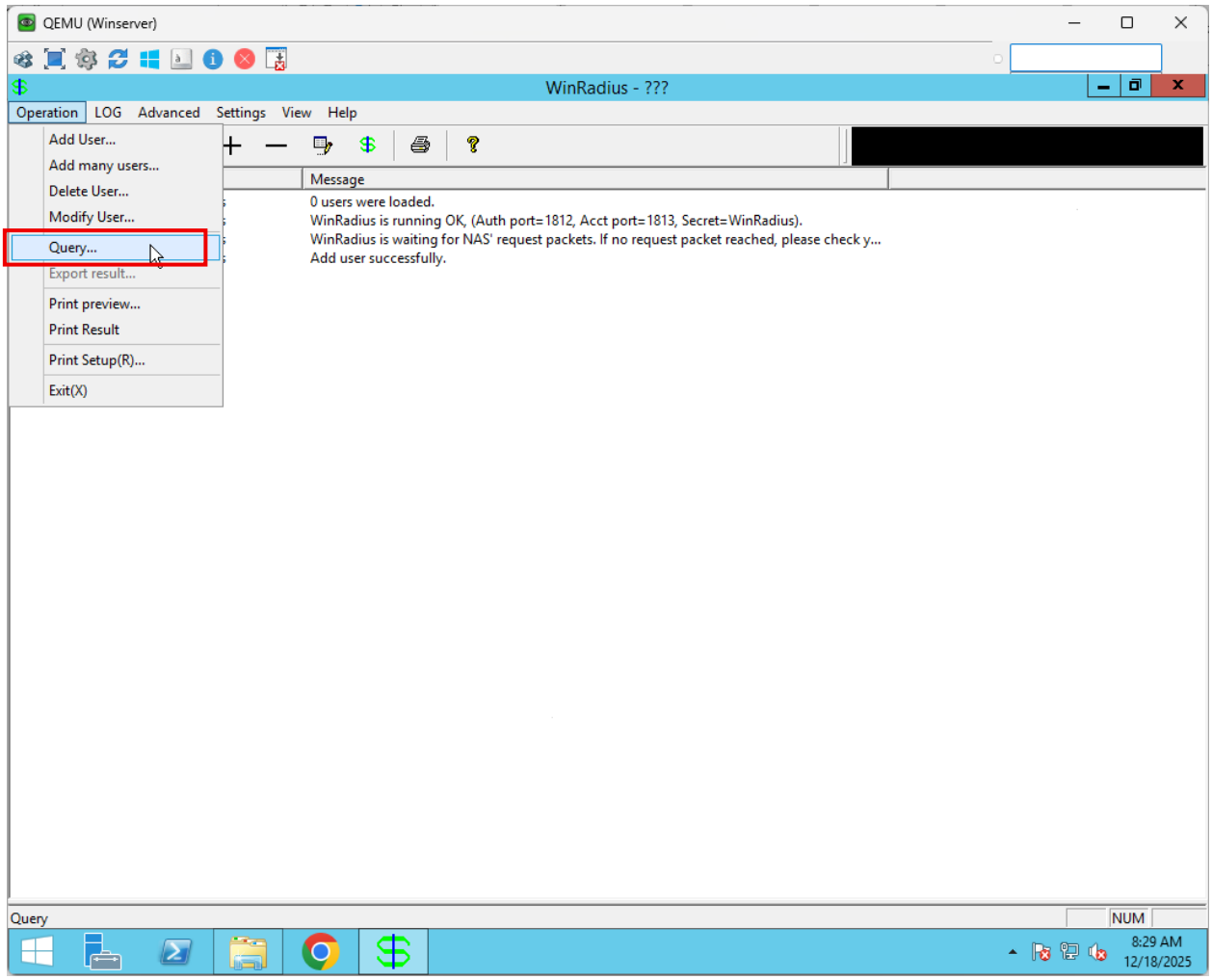

Figure 189 AAA WinRadius Users Query – Part A

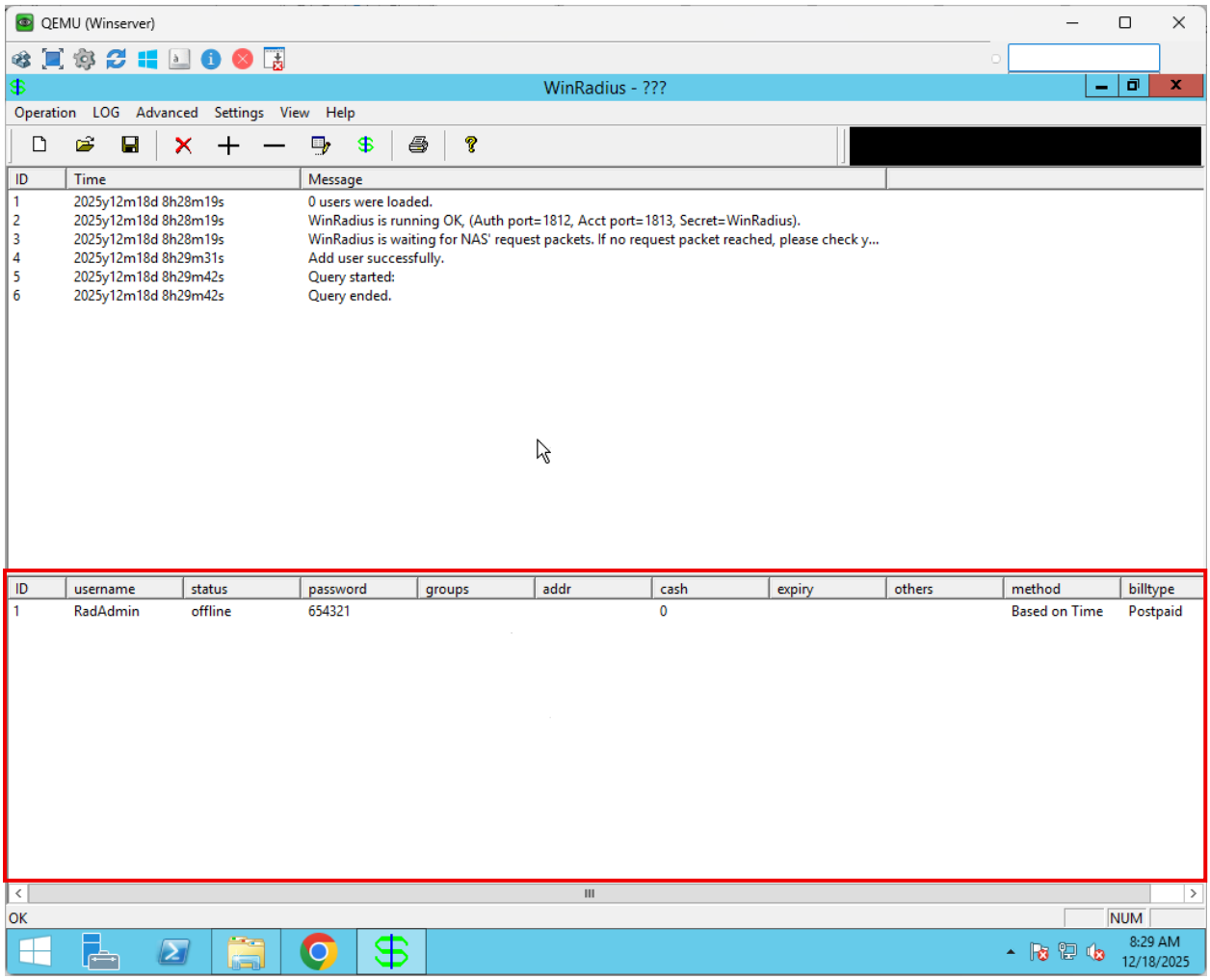

Figure 190 AAA WinRadius Users Query – Part B

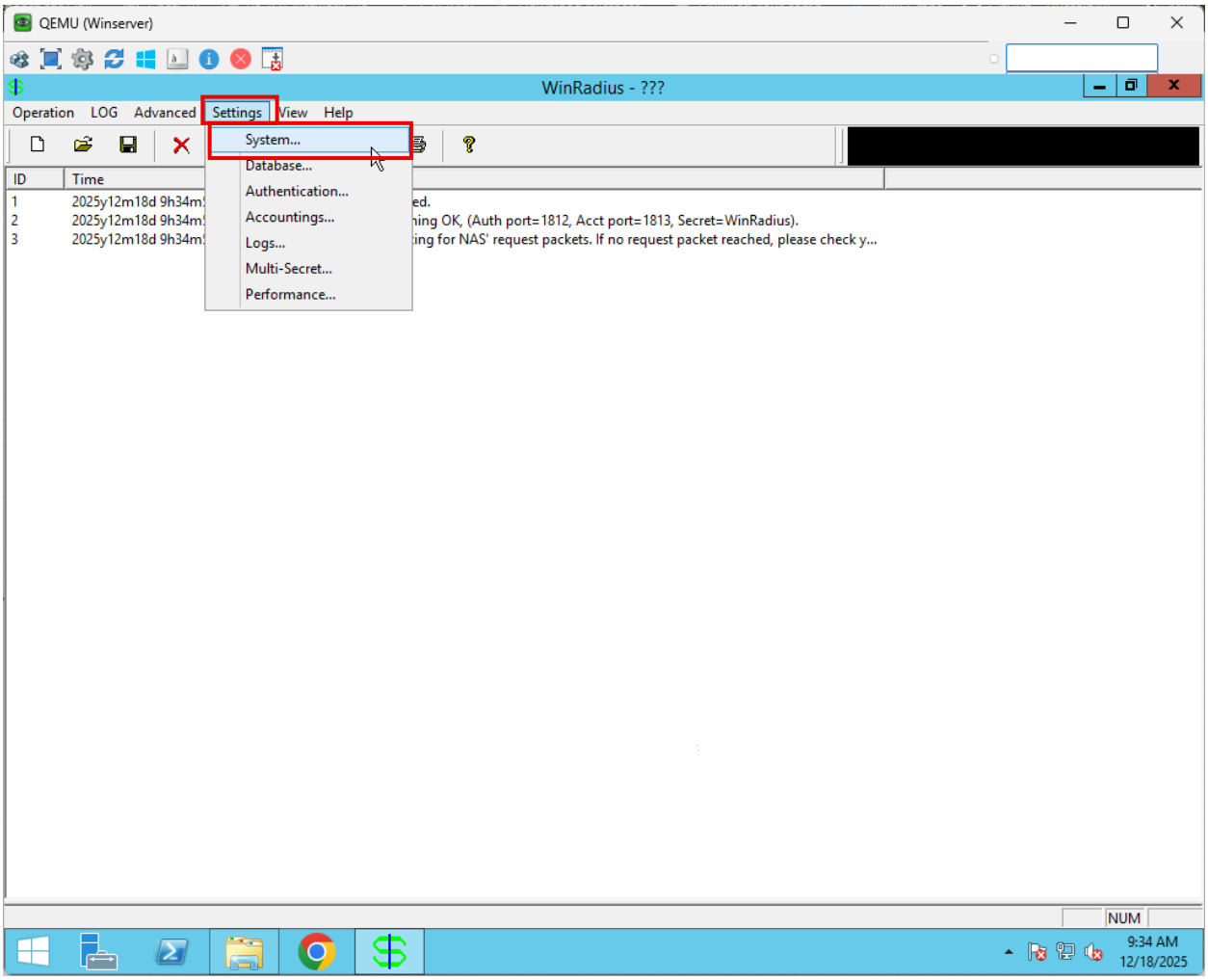

Figure 191 AAA WinRadius Authentication and Accounting Ports – Part A

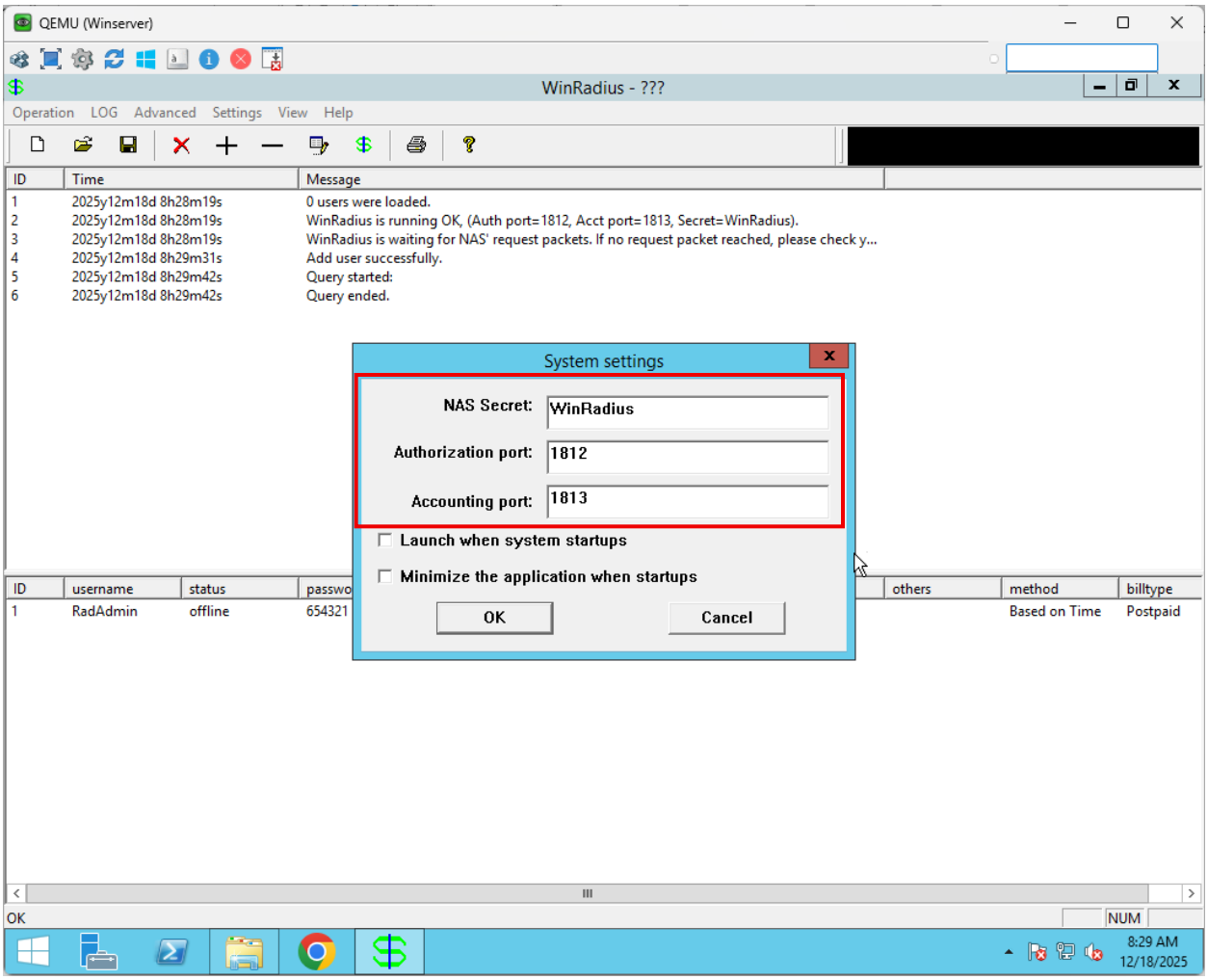

Figure 192 AAA WinRadius Authentication and Accounting Ports – Part B

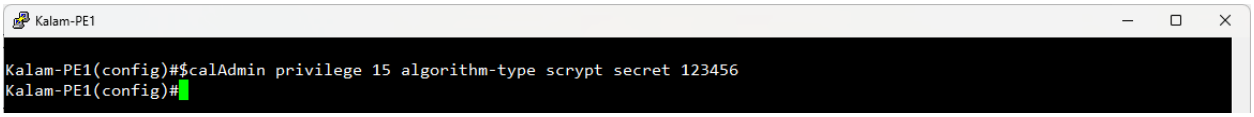

Figure 193 AAA WinRadius Router Configuration - Creating a Backup Local Username

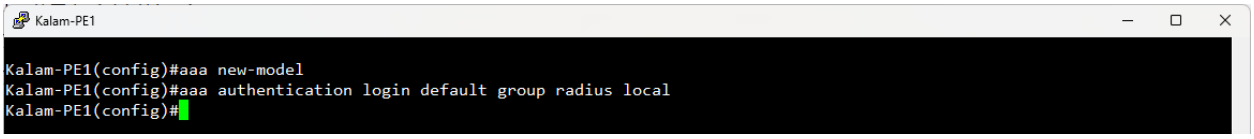

Figure 194 AAA WinRadius Router Configuration - Defining AAA Parameters Part A

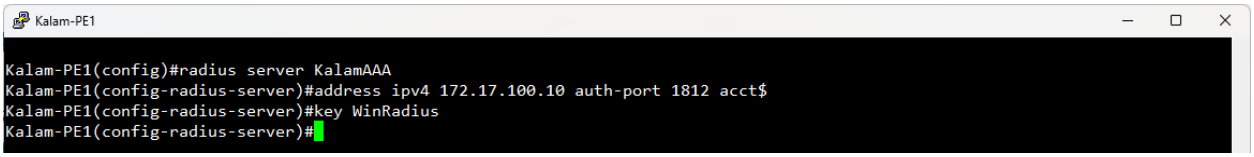

Figure 195 AAA WinRadius Router Configuration - Defining AAA Parameters Part B

Syslog Configuration:

The next figures demonstrate the configuration of Syslog for both the server and the router. Syslog services does not require a lot of configuration compared to the AAA, as syslog mainly requires configuration on the router side. For the server side, the configuration is very simple, defining the port and the number of displayed lines in addition to start the syslog service. On the router side, several configurations command are required to ensure a successful connection with the syslog server.

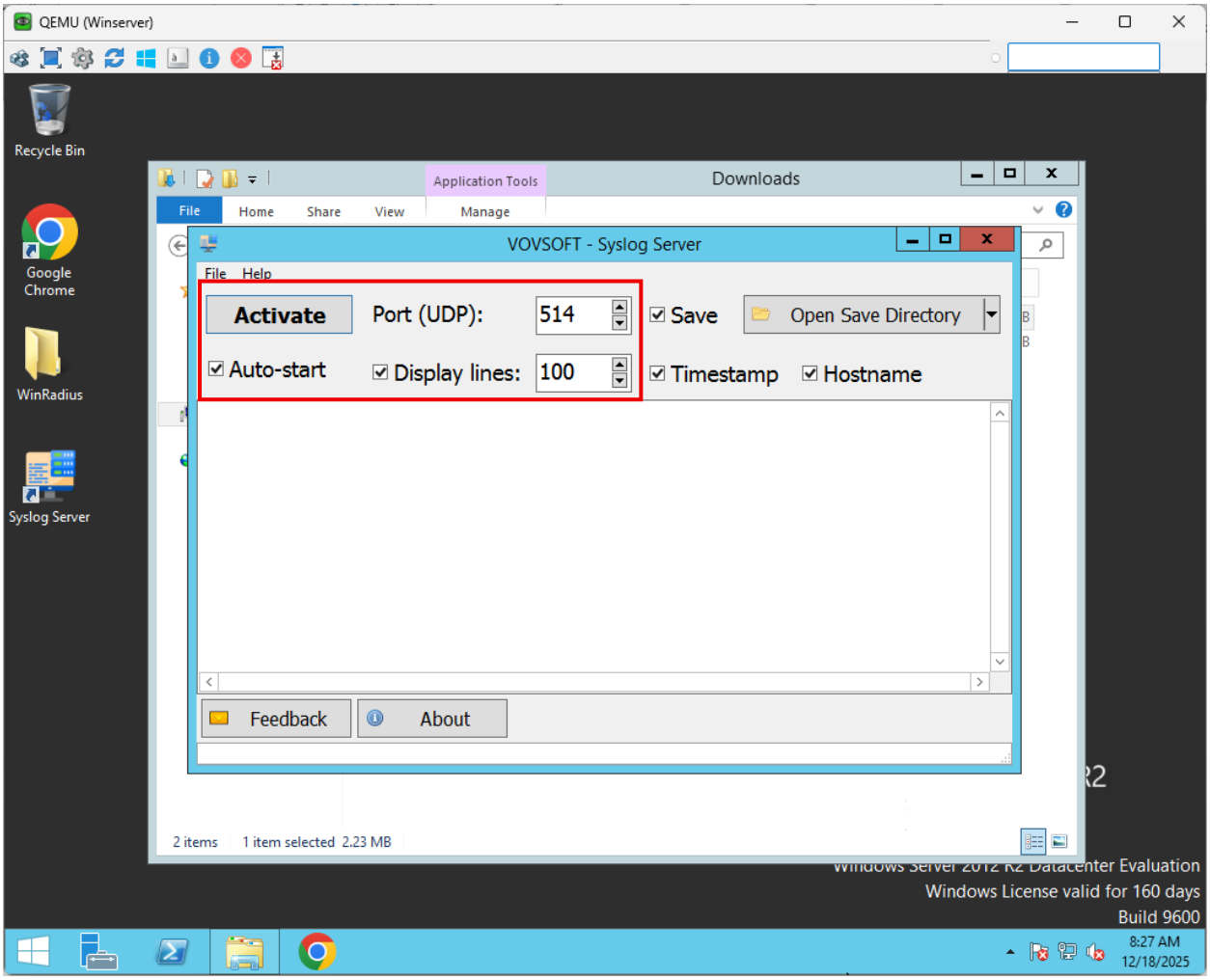

Figure 196 Syslog Server Configuration

Figure 197 Syslog Router Configuration

LAN configuration for Kalam Telecom routers

This section of the implementation part will describe the implementation of VLAN segmentation with the internal network. To make the internal network function properly the VLANs are used with the inter-VLAN routing. The HSRP is also used to ensure that the internal network does not have an internet connection issues while having a redundant gateway. Additionally, the ACL is also implemented to enhance the VLAN segmentation by restricting some devices from accessing other things in the network.

VLANs

VLAN, which stands for Virtual Local Area Network, are implemented to separate the departments logically into individual domains, each of those domains have its own isolated broadcast domain. By assigning each department to a dedicated VLAN any unnecessary broadcast traffic will be reduced since the targeted devices will be from that VLAN instead of the entire network.

VLAN configuration:

The figure below will show the VLAN configuration on Kalam-SW1. These VLANs has been configured based on the Kalam Telecom Internal Network VLANs ID table below. All the VLANs will be propagated to the other switched through the VTP Protocol which will be configured later.

Kalam Telecom VLANs	
IT Department	10
Finance Department	20
HR Department	30
SWManagement VLAN	99
Infrastructure Devices	100

Table 7 Kalam Telecom Internal Network VLANs ID

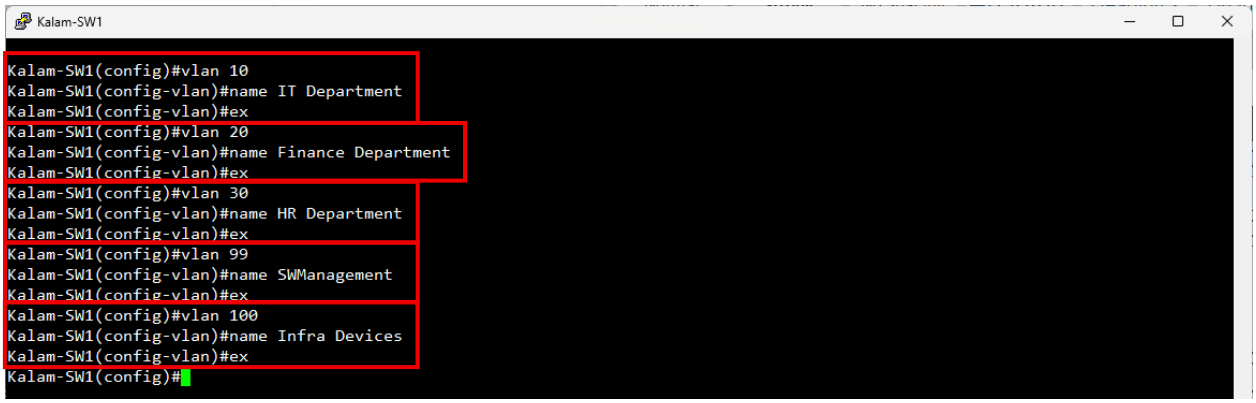

Figure 198 VLAN Configuration on Kalam-SW1

VLAN Verification:

The following images shows that the VLANs has been configured successfully inside Kalam-SW1. The inspection of the configuration matches the VLAN ID table. VLAN 10 assigned to IT, VLAN 20 assigned to Finance, VLAN 30 assigned to the HR and both of VLAN 99 and 100 are assigned to the network infrastructure.

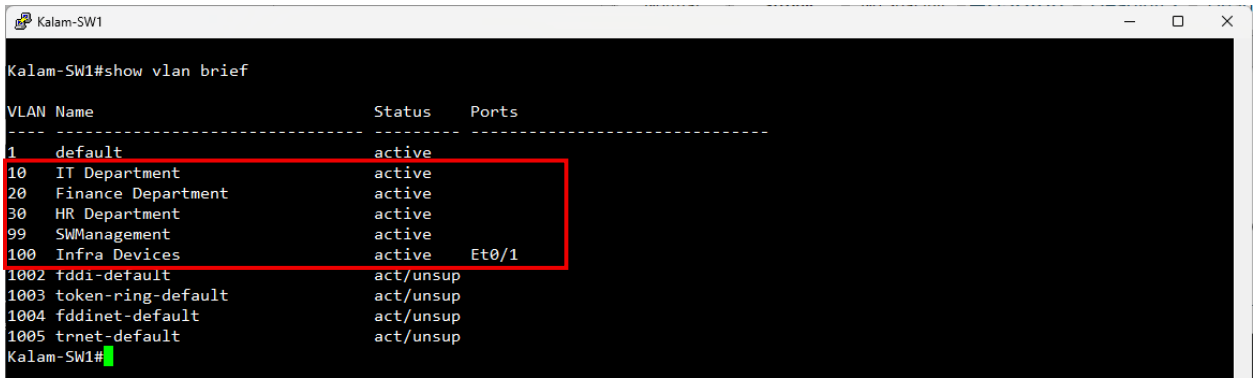

Table 8 VLANs Verification

Inter-VLAN

Inter-VLAN is a routing method used to allow communication between the VLANs when it is needed by using a layer 3 device sub-interface where each sub-interface is associated to a specific VLAN and configured with an IEEE 802.1Q encapsulation to route traffic from one VLAN to another while still maintaining the logical separation. This approach enables the

necessary inter-department communication without compromising the network segmentations.

Inter-VLAN routing configuration:

The below figures illustrate the Inter-VLAN routing configuration for both Kalam-R1 and Kalam-R2. Inter-VLAN routing is configured on these router to ensure controlled communication between the VLANs in line with Kalam Telecom internal network design.

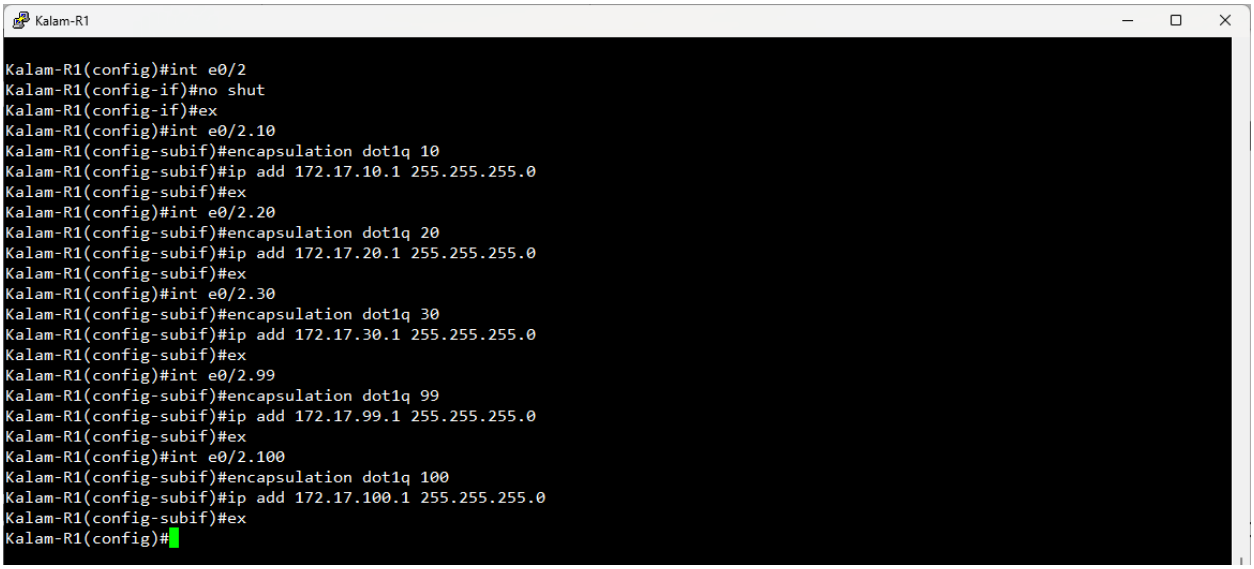

Figure 199 Inter-VLAN Configuration On Kalam-R1

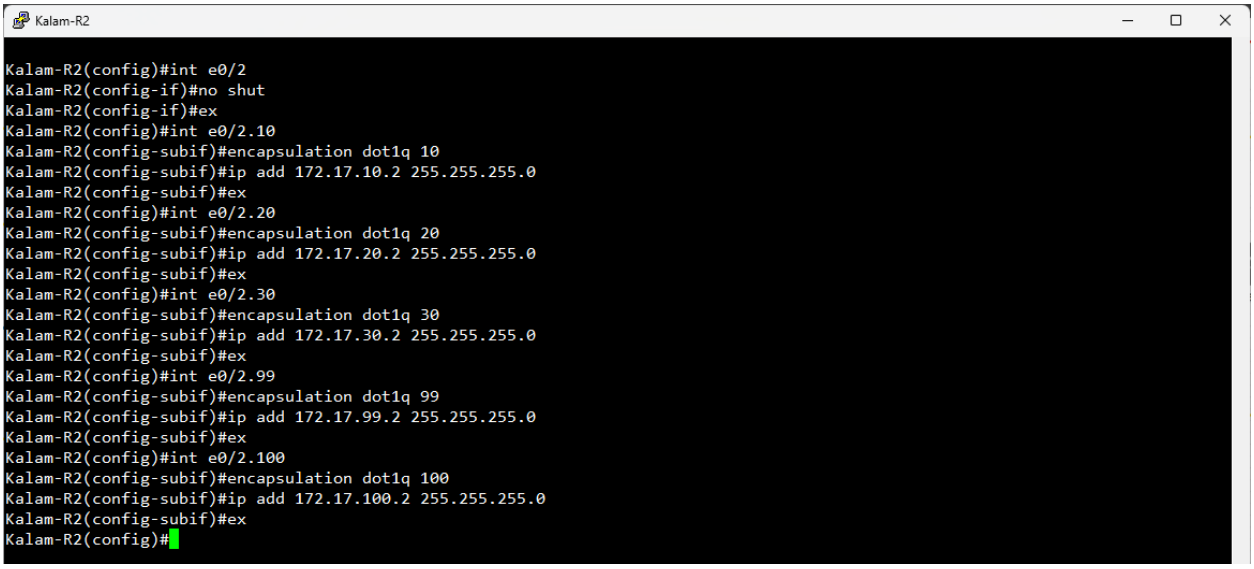

Figure 200 Inter-VLAN Configuration On Kalam-R2

Inter-VLAN Verification:

The next figures demonstrate that the inter-VLAN routing is functioning properly, as the evidence below show the successful ping test initiated from the IT department with an IP 172.17.10.10 to the Finance department with an IP 172.17.20.10. This proves that the Inter-VLAN routing is successfully configured.

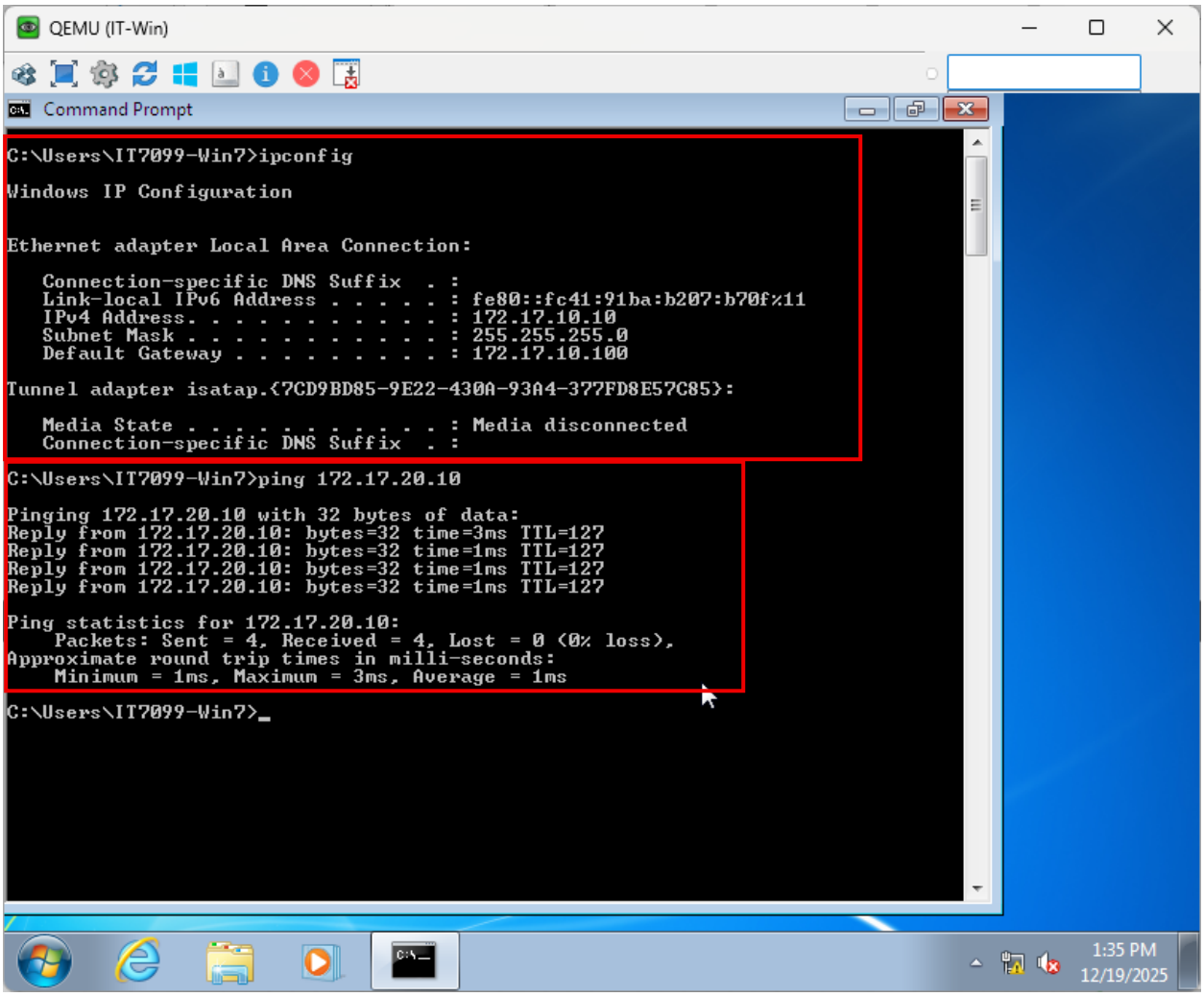

Figure 201 Inter-VLAN Verification IT Pinging Finance

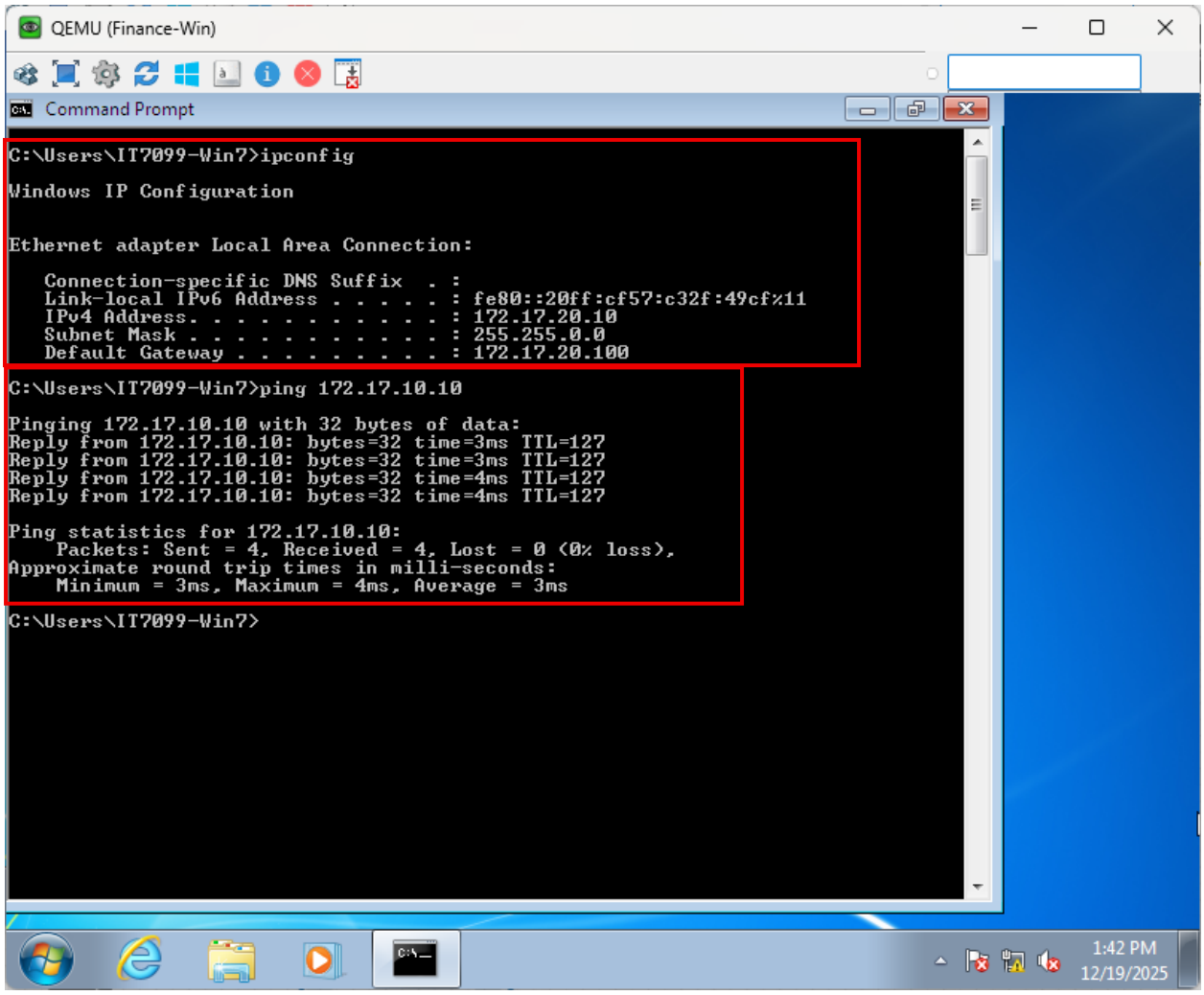

Figure 202 Inter-VLAN Verification Finance Pinging IT

HSRP

HSRP, which stands for Host Standby Router Protocol, is deployed on multiple routers to provide a gateway redundancy for the VLANs. HSRP allows multiple routers to share a virtual gateway IP address to ensure continuous network connectivity. If the active router fails, the standby router will automatically take other to reduce service disruption.

HSRP Configuration:

The below figures will show the configuration of Kalam-R1 and Kalam-R2, where both of routers shares a virtual gateway IP address using HSRP. To utilize the both routers effectively, the VLANs will be distributed evenly between the R1 and R2, with VLAN 10 and 20 configured as active on Kalam-R1 and standby on Kalam-R2, while VLANs 30, 99 and 100 are configured as active on Kalam-R2 and standby on Kalam-R1.

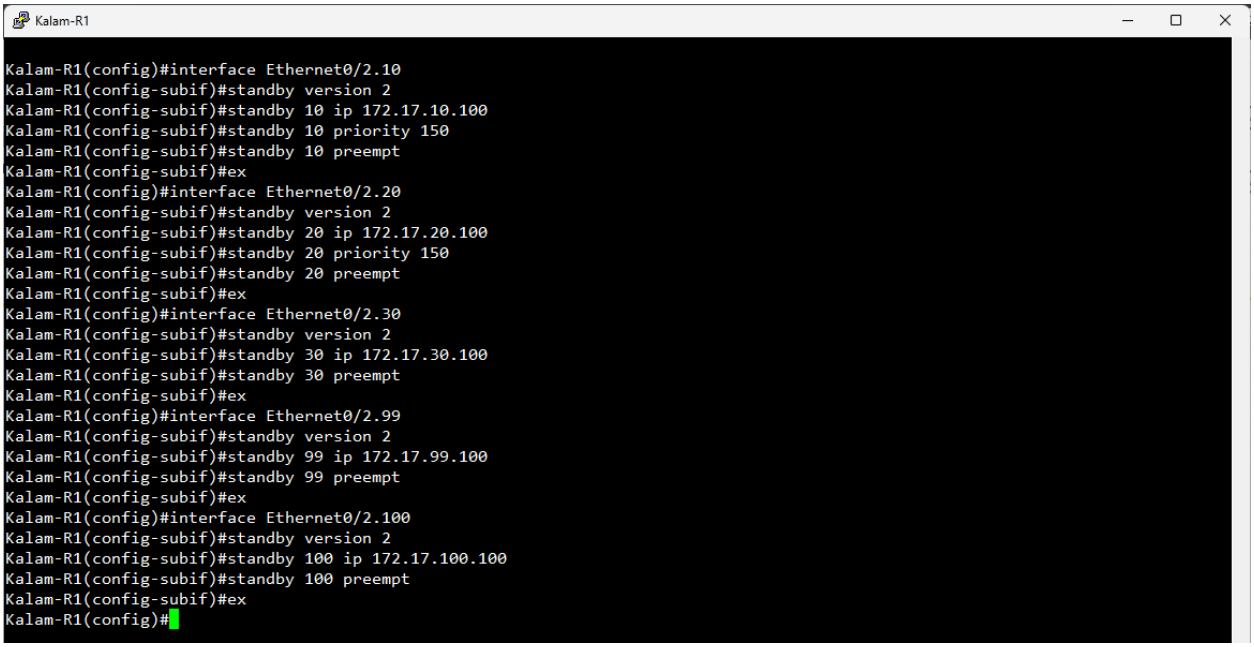

Figure 203 HSRP Kalam-R1 Configuration Commands

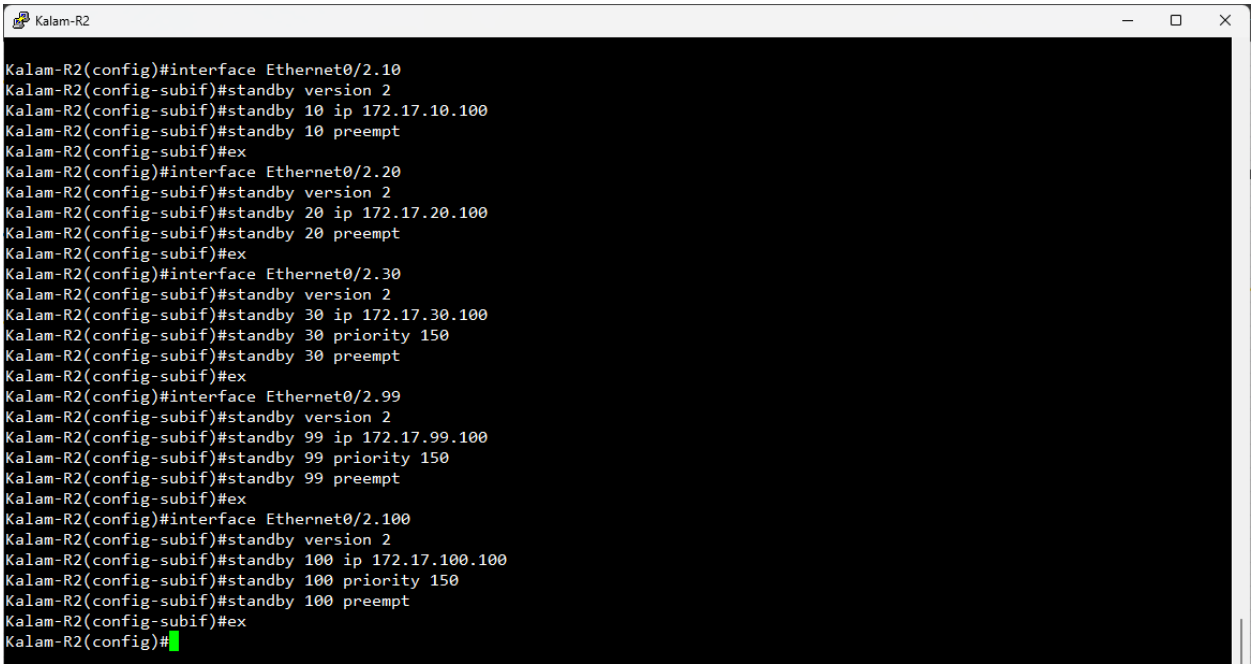

Figure 204 HSRP Kalam-R2 Configuration Commands

HSRP Verification:

The next figures will show the HSRP active/standby router for all the VLANs to verify whether the HSRP are configured per the Kalam Telecom Internal network design or not.

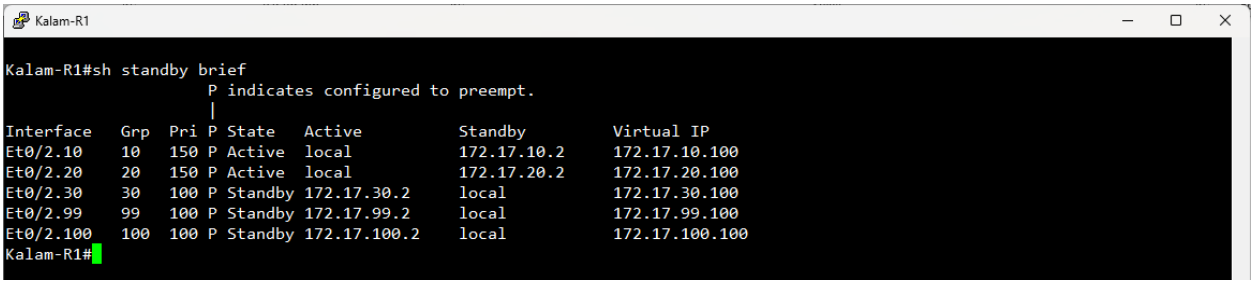

Figure 205 Kalam-R1 HSRP Verification

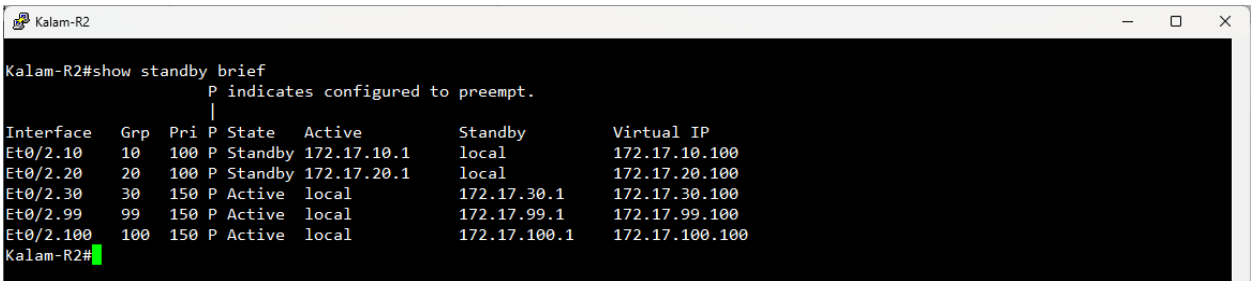

Figure 206 Kalam-R2 HSRP Verification

VTP

VTP, which stands for VLAN Trunking Protocol. is used to propagate all the VLANs from one main switch to all other switched. VTP offers centralized management for all the VLANs across the network. VTP ensures the consistency of VLANs IDs and names on all switches.

VTP configurations:

The figure below will show the configuration of VTP domain, mode and password, which are defined to ensures consistency VTP domains in the network.

VTP	
VTP Domain Name	KalamVTP
VTP Password	123@Kalam

Table 9 VTP Parameters

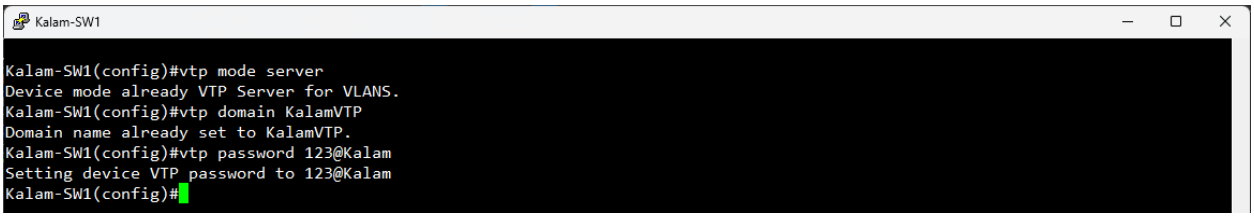

Figure 207 VTP Server Configuration

Figure 208 VTP Client Configuration

ACL

ACL, which stands for Access Control List. ACL are mainly applied to control and enhance VLAN segmentation in environments where Inter-VLAN routing is configured. ACL either allows or deny traffic based on the defined rules that has been set by the ISP, allowing the administrators to enforce custom security policies across the network.

ACL configuration:

The next figures will demonstrate the configuration of multiple ACLs. The ACLs are applied within the internal network, including Fin-ACL, IT-ACL, SWM-ACL and Infra-ACL. Each ACL is designed to enforce specific security policies based on departmental needs. This approach ensures that the internal network remains under control and secure, even with the presence of Inter-VLAN.

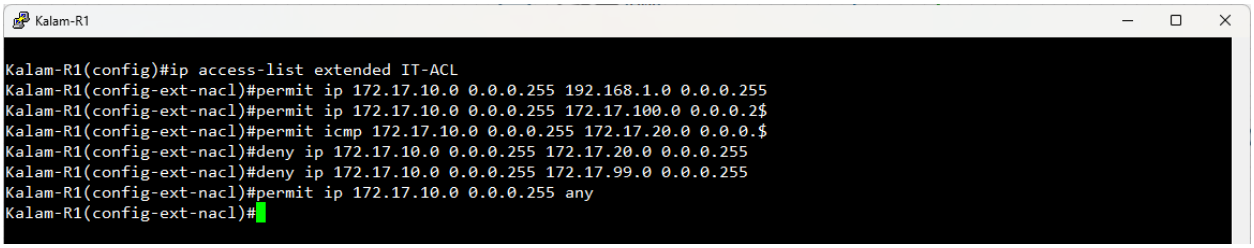

Figure 209 IT Department ACL

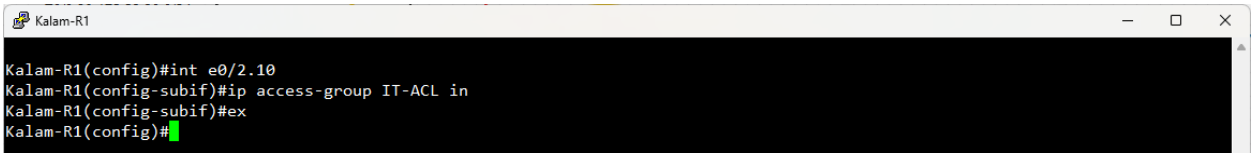

Figure 210 Applying the IT ACL on the IT Sub-interface

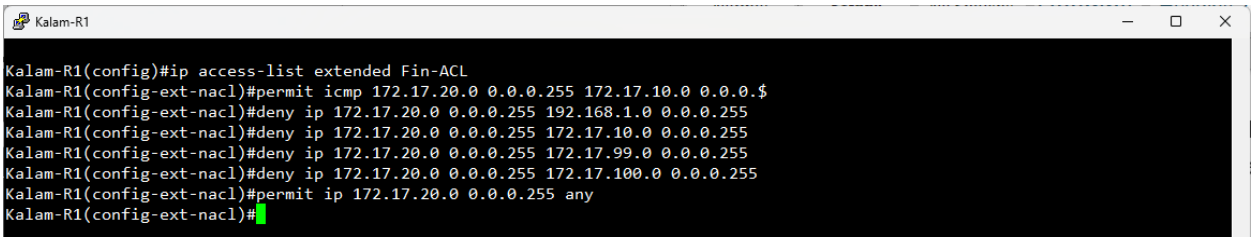

Figure 211 Finance Department ACL

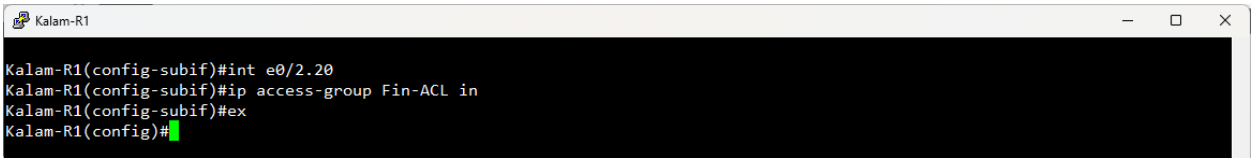

Figure 212 Applying the Finance ACL on the Finance Sub-interface

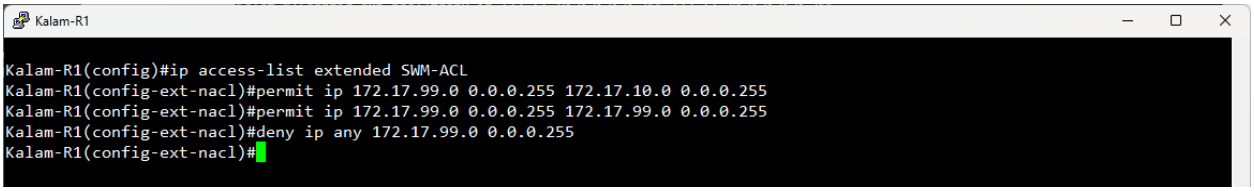

Figure 213 SWManagement ACL

Figure 214 Applying the SWManagement ACL on the SWManagement Sub-interface

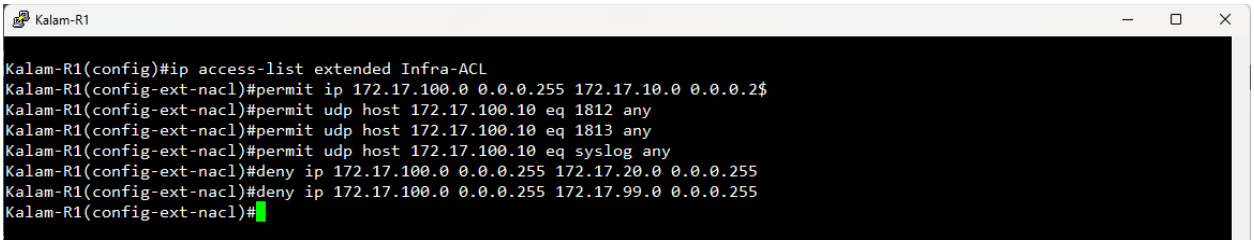

Figure 215 Infrastructure Devices ACL

Figure 216 Applying the Infrastructure Devices ACL on the Infrastructure Devices Sub-interface

ACL Verification:

The following figures will demonstrate the verification of the IT department ACL which is configured to allow the IT department to reach the MPLS backbone and the Infrastructure Devices using any protocol. The IT ACL also permits the ICMP traffic specifically echo requests to the Finance Department, while blocking all other protocol to the Finance department as well as the SWManagement network.

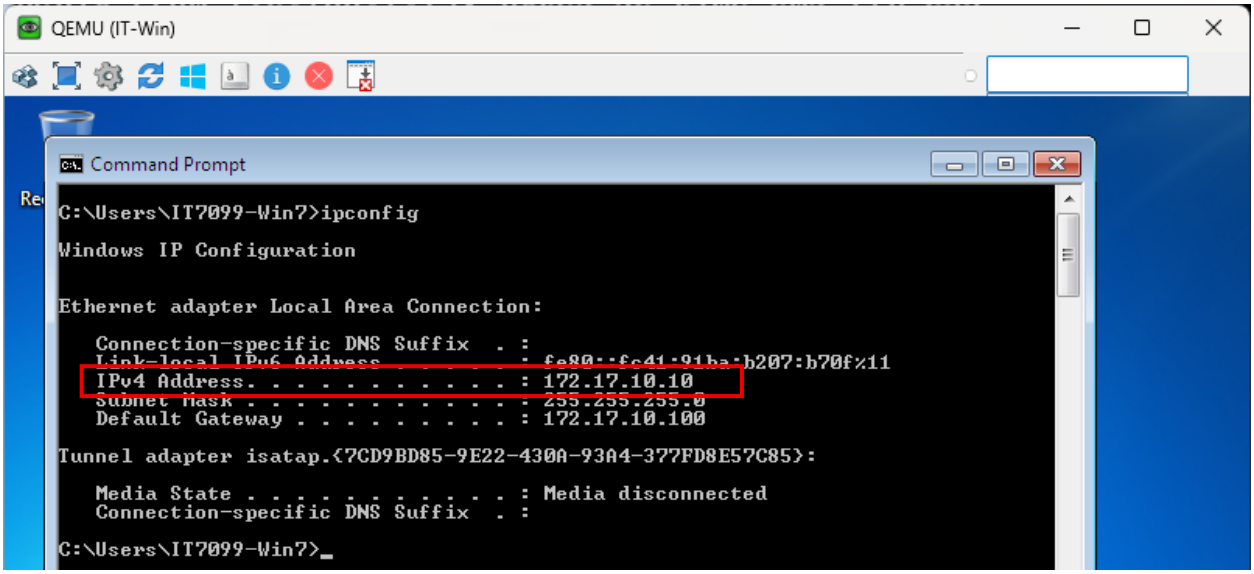

Figure 217 IP address of the IT Department PC

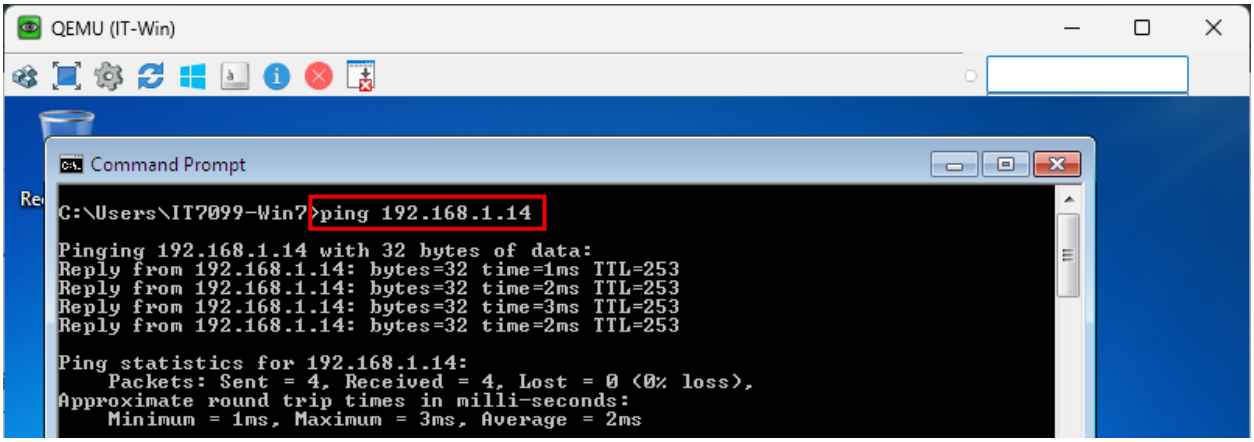

Figure 218 IT PC Pinging MPLS backbone - ACL Verification

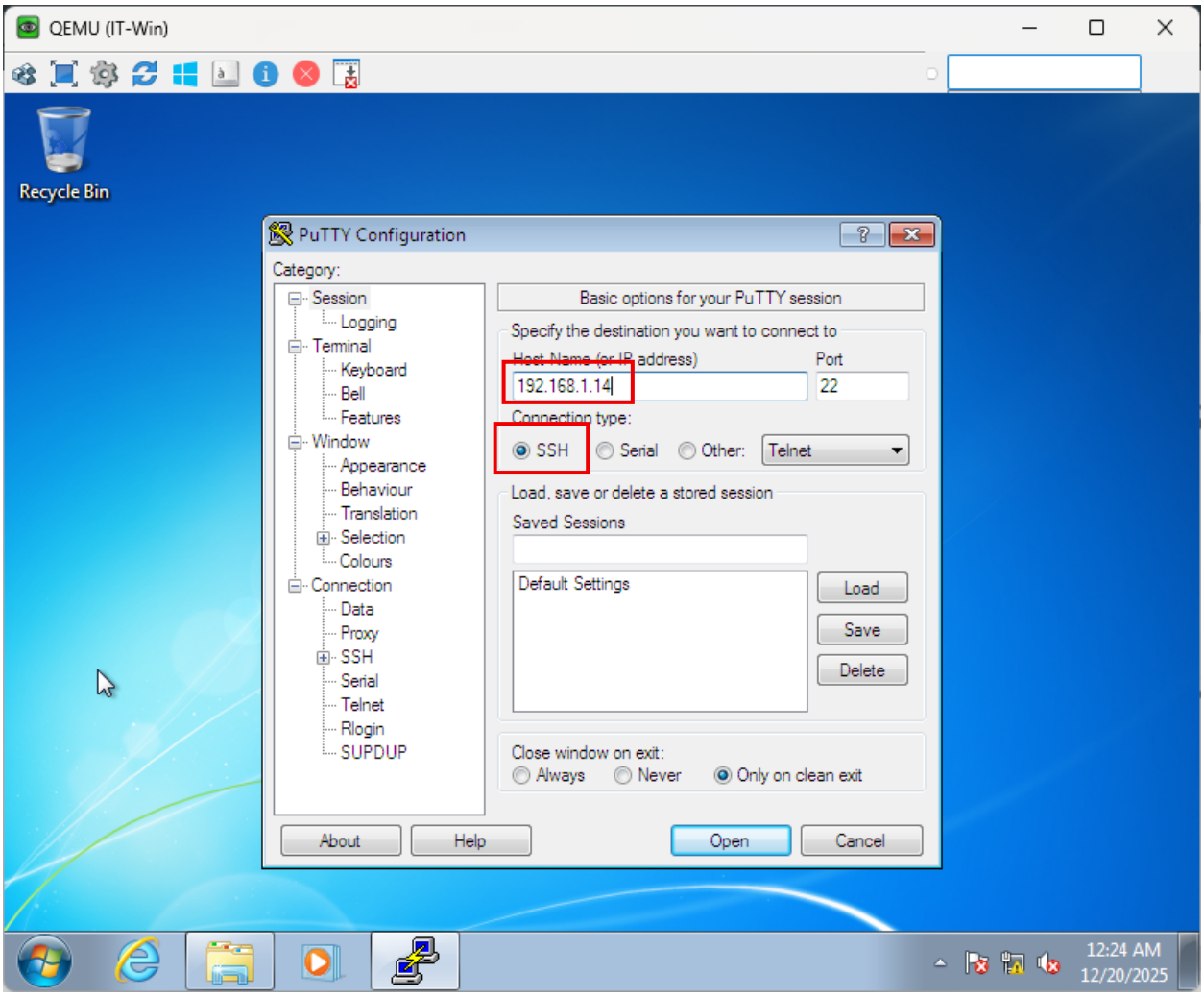

Figure 219 IT PC SSH MPLS backbone - ACL Verification

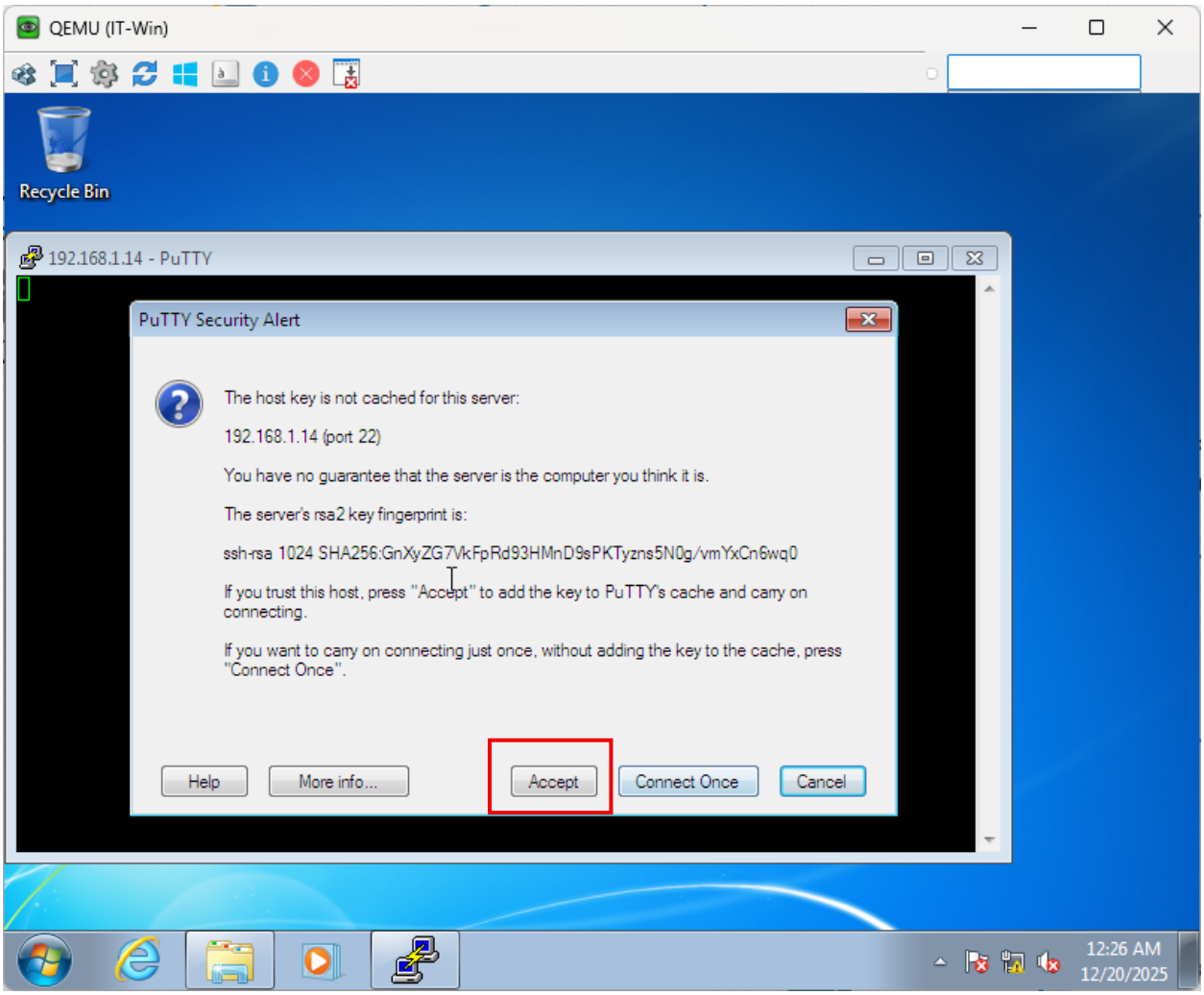

Figure 220 IT PC SSH MPLS backbone - ACL Verification

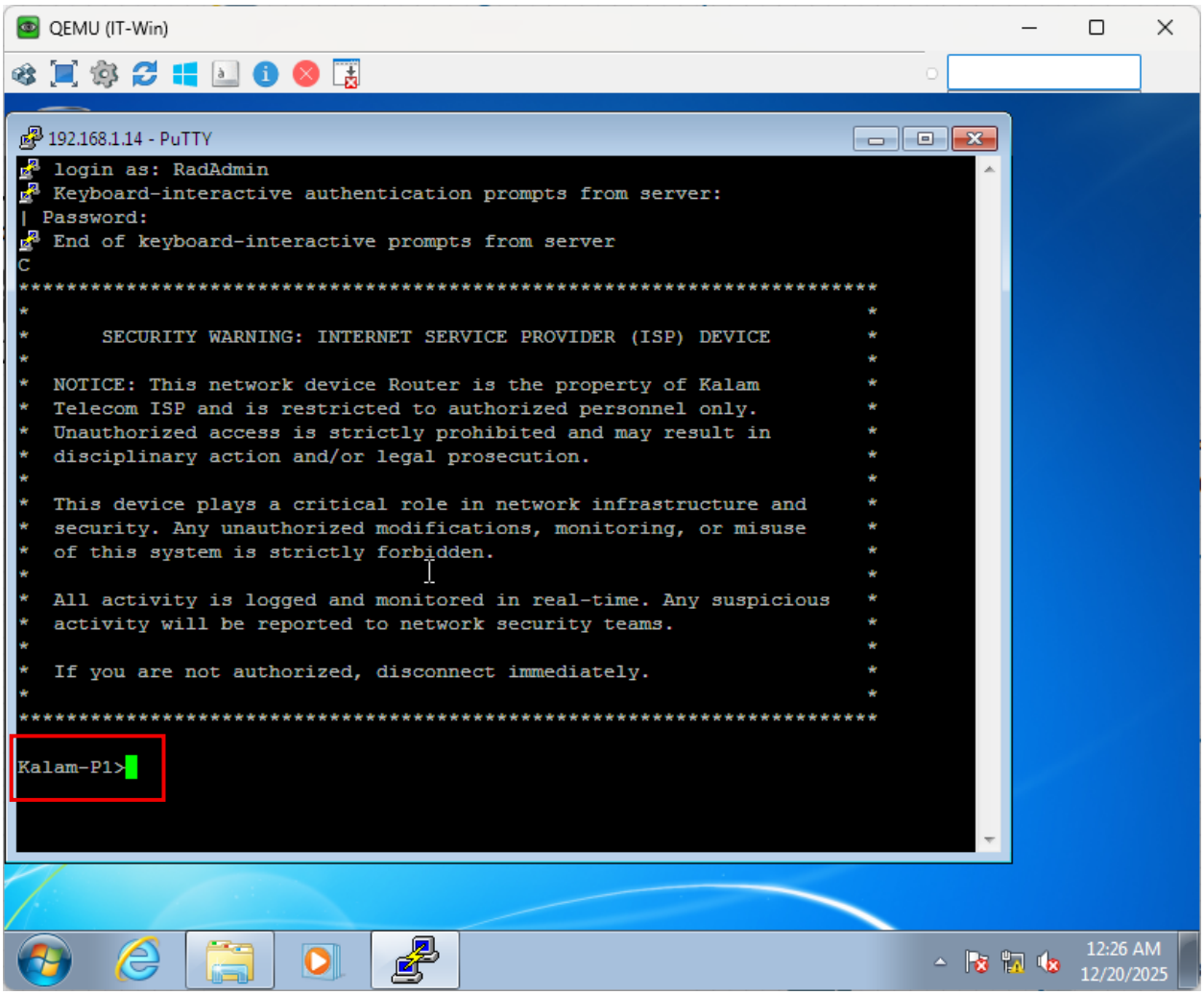

Figure 221 IT PC SSH MPLS backbone - ACL Verification Part C

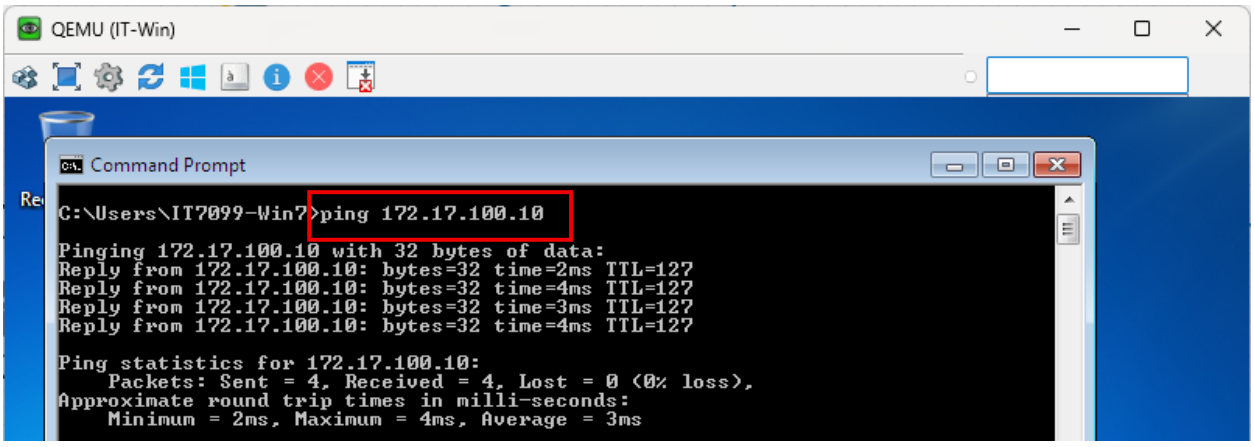

Figure 222 IT PC Pinging Infrastructure Devices - ACL Verification

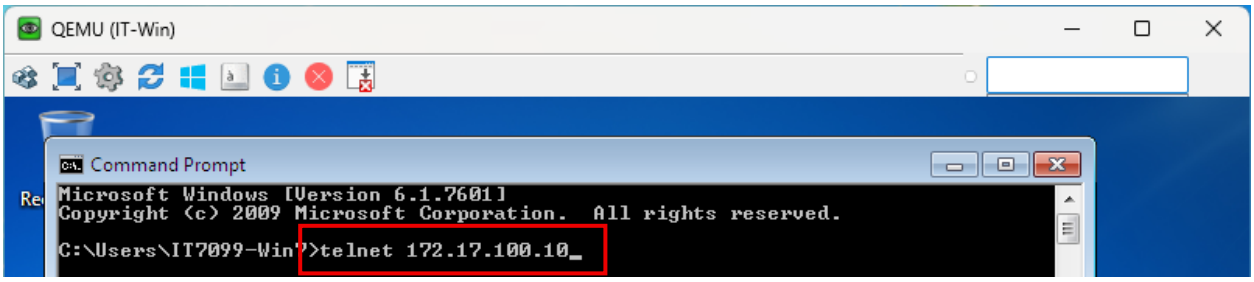

Figure 223 IT PC Telnet to Infrastructure Devices - ACL Verification Part A

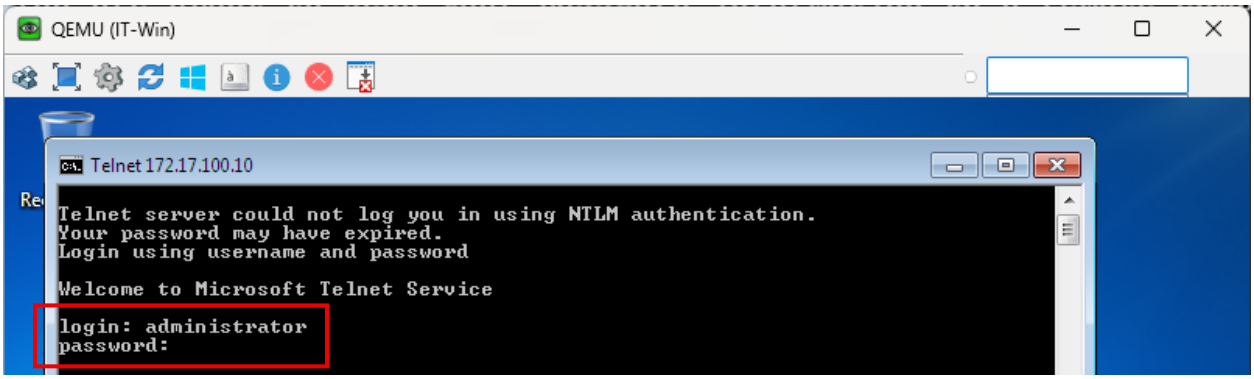

Figure 224 IT PC Telnet to Infrastructure Devices – ACL Verification Part B

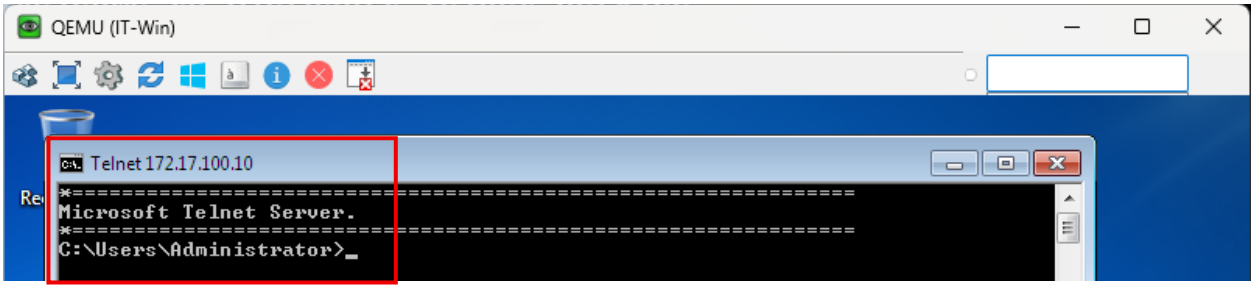

Figure 225 IT PC Telnet to Infrastructure Devices - ACL Verification Part C

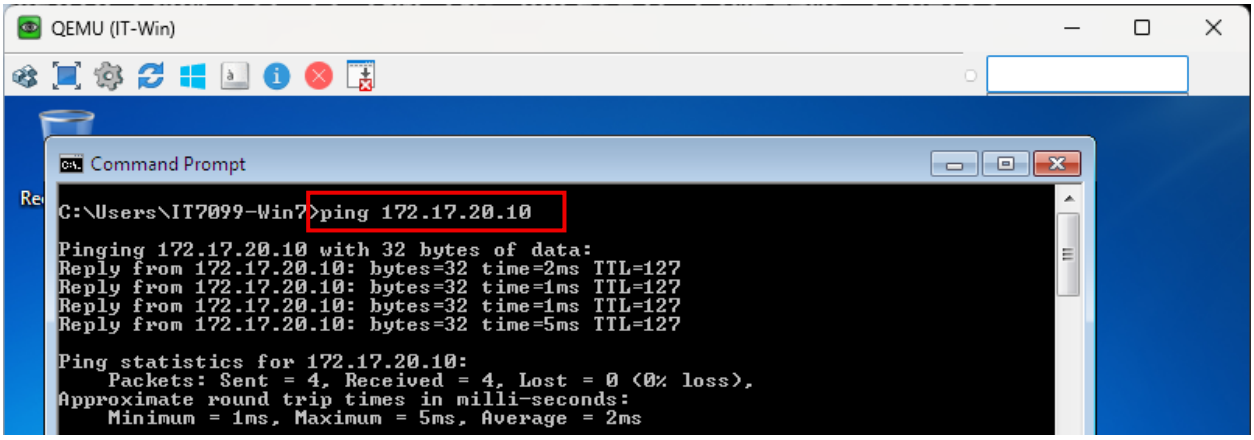

Figure 226 IT PC Pinging Finance Department - ACL Verification

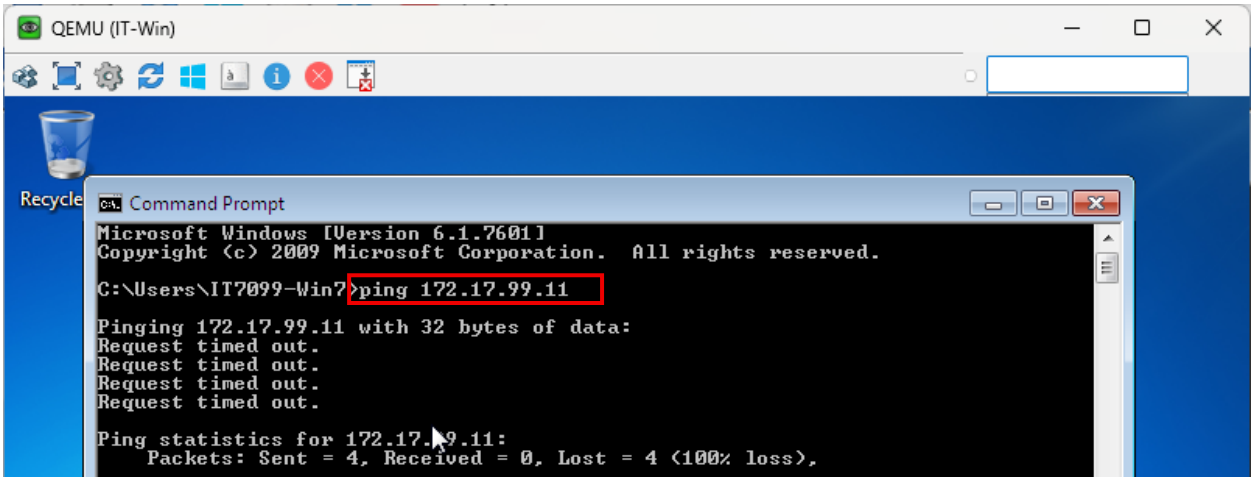

Figure 227 IT PC Pinging SWManagement Devices - ACL Verification

Testing

Testing is a critical phase that needs to be applied after the MPLS backbone is fully configured because testing scenarios always confirms if the implemented MPLS backbone behaves as intended and whether it achieved the functional requirements and the network design. This section describes all the approaches, actions and tasks that took place to make sure that the MPLS backbone solutions are effective and efficient.

All testing experiments are implemented inside a virtual environment using EVE-NG network emulation platform.

Test Plan

This test plan shows and outlines the scenarios that has been taken into consideration to confirms that Kalam Telecom MPLS backbone is operating successfully and correctly as intendent. The testing scenarios are restricted to the elements that is a part of the project objectives.

The test plan covers the following scenarios:

- Testing that all functional requirements are operating and achieved.
- evaluate the internal routing protocol.
- assessment of MPLS VPN label exchange between Inter-AS MPLS
- Testing the MPLS labeling
- Validating if the customer traffic is isolated
- Perform Inter-VLAN routing testing
- Verification of network services such as AAA and Syslog

Participants

Involving other people in the testing phase is very helpful approach, since it will provide you with different perspectives and vision that will not be identified by a single tester. This approach also open a new opportunity to find errors or missing configuration on the MPLS backbone. The participants for this testing phase were selected based on their knowledge and experience in networking topics that are related to this project.

Participant Order	Name of the Participants	Age	Gender	Participant Backgrounds
1	Ahmed Ali	22	Male	Year 4 ICT cyber security student with knowledge in enterprise networking security
2	Khalid Abdulla	24	Male	ICT graduate specializing in WAN technologies.
3	Salma Rashid	23	Male	ICT networking student with academic experience with network design

Table 10 Test Phase Participants

Test Cases Results

To ensure that every aspects of Kalam Telecom network is functions correctly as planned in the network design a couple of testing scenarios has been carried out to check the system functionality. By comparing the expected with the actual results, each scenario verify that the system functionality is achieved.

Test Case ID	Scenarios	Result Expected	Actual Result	Status (Pass/Fail)
1	verify the routing protocol of the MPLS backbone layer	OSPF process 1 neighbor adjacency established with routing information exchanged	Neighbor adjacency formed with a successful routes exchange	Pass
2	verify the routing protocol of the	OSPF process 5 router has exchanged their	All routes in the internal network has been	Pass

	Internal network of kalam Telecom	routes between each other	advertised and exchanged	
3	Verify that OSPF process 1 and process 5 are correctly redistributed	MPLS backbone routers has received the internal network routes and installed them onto the routing table and vice versa	MPLS backbone router has successfully learned about the internal network routes and vice versa	Pass
4	Verify the connection between the PE routers and CE routers	The EIGRP connectivity is established	EIGRP adjacencies are established and routing information are exchanged without any issues	Pass
5	Test the MPLS VPN Inter-AS connectivity	VPN label exchanged between ISPs	VPN labels are being exchanged between the ISPs in both direction with no issues	Pass
6	Test the MPLS connectivity inside Kalam Telecom	Core routers must establish connectivity	All core routers has established connectivity with each other	Pass
7	Verify the isolation between the customer network	Each customer has its own VRF	Customers are isolated from each other using multiple VRFs	Pass
8	Customer End-to End connectivity	Connectivity between all customer branches	All the customer branches can reach each other successfully	Pass
9	Evaluate the AAA service	AAA authenticate users across the network	AAA Is configured correctly and authenticate	Pass

			users across the network	
10	Verify the Syslog service	Syslog are configured across the entire network	Syslog are correctly configured across the network towards the Syslog server	Pass

Table 11 Test Cases Table

Test Cases Verification

This section will validate the testing scenario above to confirm that the Kalam Telecom MPLS backbone network is work and functions properly as intendent. Each scenario test has been created to make sure that a certain system functions such as network protocol availability, customer inter-connection sites and verifies the system services.

verify the routing protocol of the MPLS backbone:

Figure 228 Testing Phase Kalam-P2 show run

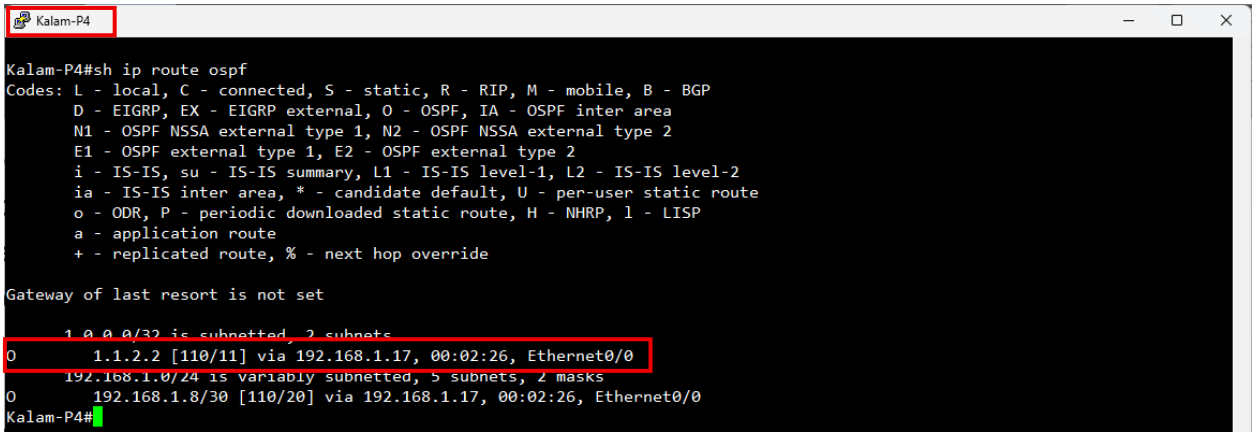

Figure 229 Testing Phase Kalam-P4 routing table

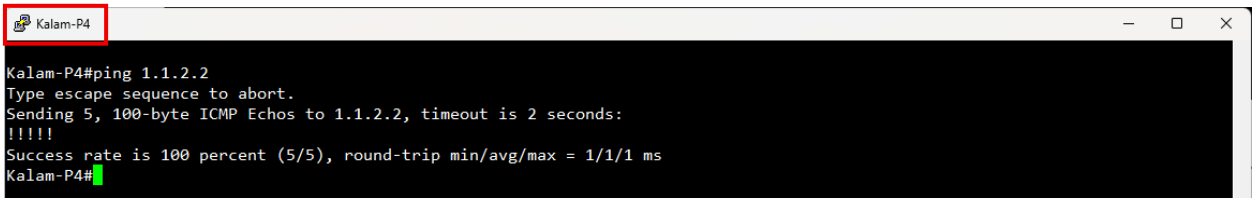

Figure 230 Testing Phase Ping testing on Kalam-P4

This test was carried out to confirms that Kalam-P2 has been exchanging their routes information with the other neighbor such as Kalam-P4. The main idea of this test is to verify that the neighboring adjacency is applied on the MPLS backbone layer.

Kalam-P2, which has an loopback0 IP address of 1.1.2.2 and this IP address has been exchanged with Kalam-P4 to be installed in P4 routing table. After this the P4 tries to ping the P2 loopback interface to demonstrate successful reachability.

Test Result: Pass

verify the routing protocol of the Internal network of kalam Telecom:

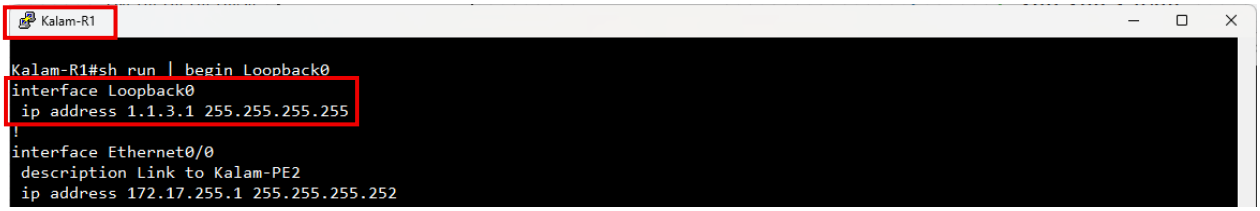

Figure 231 Testing Phase Kalam-R1 show run

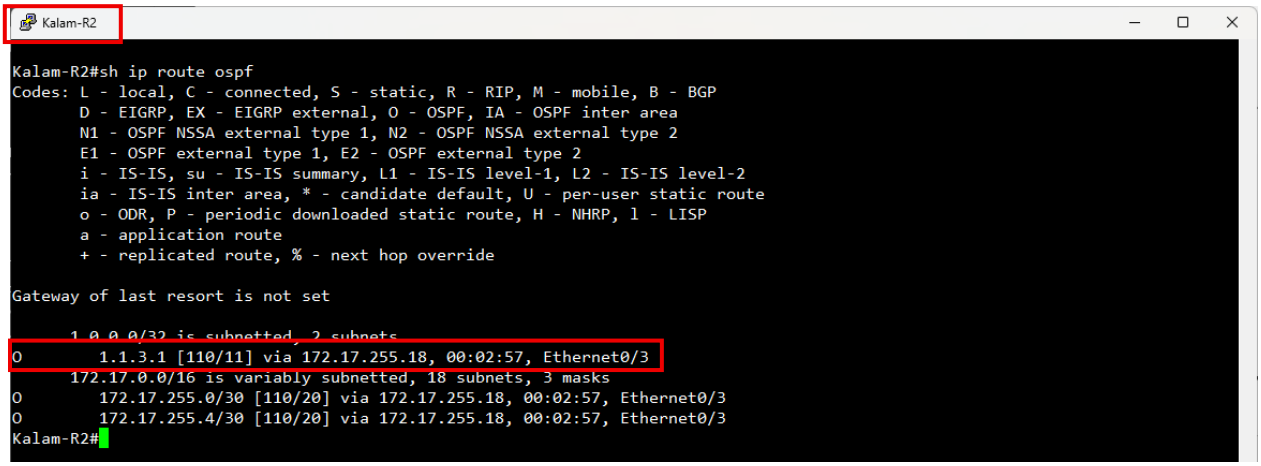

Figure 232 Testing Phase Kalam-R2 routing table

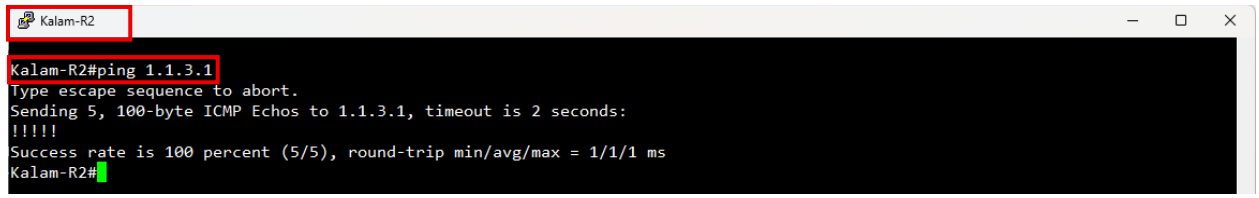

Figure 233 Testing Phase Ping testing on Kalam-R2

This test was carried out to confirms that Kalam-R1 has been exchanging their routes information with the other neighbor such as Kalam-R2. The main idea of this test is to verify that the neighboring adjacency is applied on the internal network of kalam telecom.

Kalam-R1, which has a loopback0 IP address of 1.1.3.1 and this IP address has been exchanged with Kalam-R2 to be installed in R2 routing table. After this process the R2 tries to ping the R1 loopback interface to demonstrate successful reachability

Test Result: Pass

Verify that OSPF process 1 and process 5 are correctly redistributed:

Figure 234 Testing Phase Kalam-R1 show run

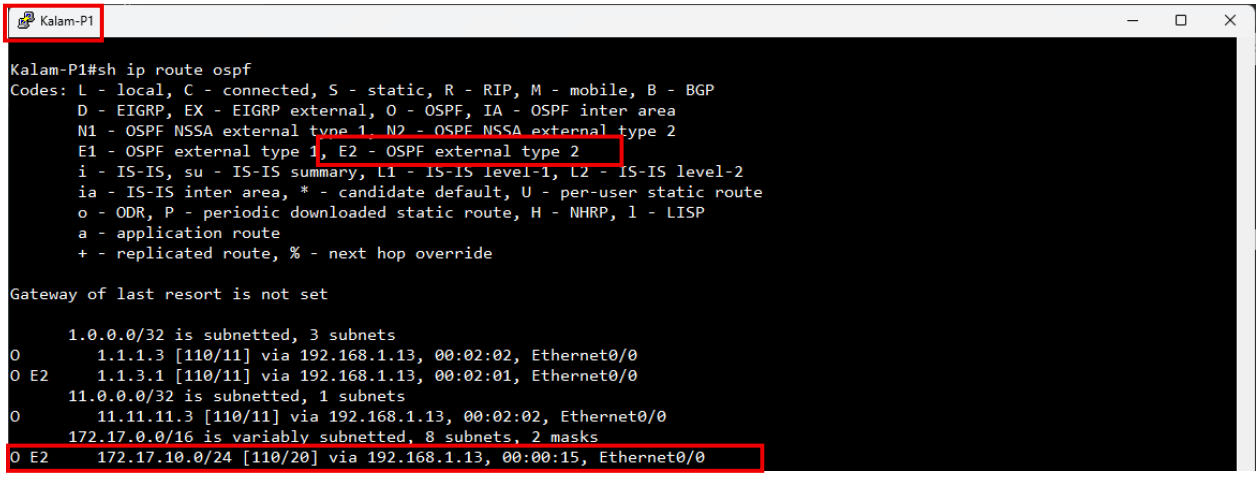

Figure 235 Testing Phase Kalam-P1 routing table

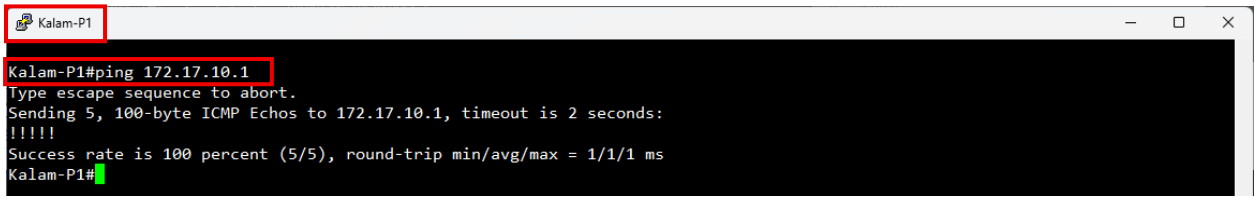

Figure 236 Testing Phase Ping testing on Kalam-P1

This test was carried out to confirms that Kalam-R1 from OSPF process 5 has been exchanging their routes information with the other neighbor such as Kalam-P1 from OSPF process 1. The main idea of this test is to verify that the redistribution is applied between the OSPF process 5 and OSPF process 1.

Kalam-R1, which has a sub-interface Ethernet 0/2.10 with an IP address of 172.17.10.1 and this IP address has been exchanged with Kalam-P1 to be installed in P1 routing table. After this process the P1 tries to ping the R1 sub-interface interface to demonstrate successful reachability

Test Result: Pass

Verify the connection between the PE routers and CE routers:

Figure 237 Testing Phase XYZ-1-CE show run

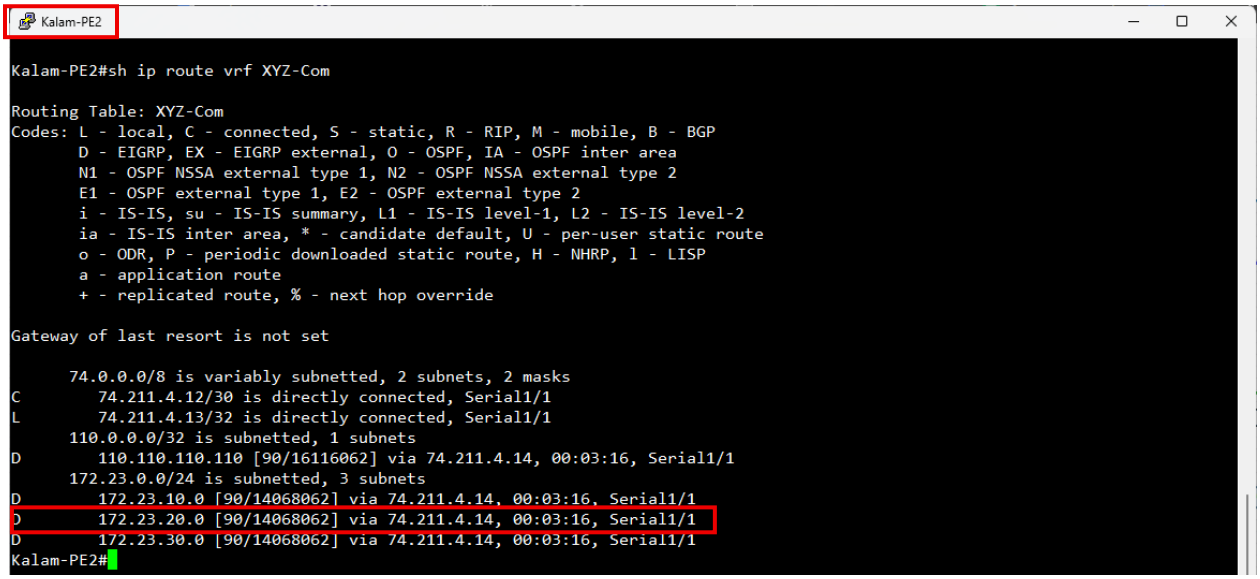

Figure 238 Testing Phase Kalam-PE2 routing table

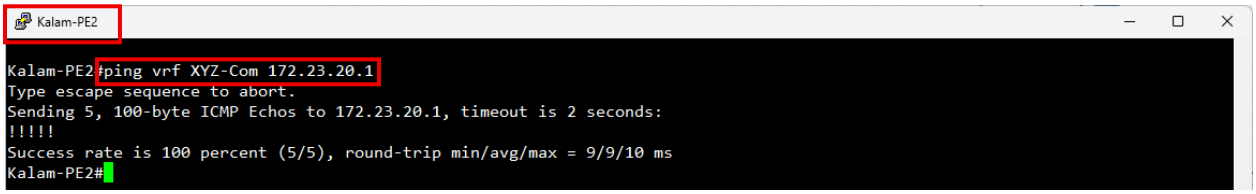

Figure 239 Testing Phase Ping testing on Kalam-PE2

This test was carried out to confirms that the EIGRP connection between XYZ Company and Kalam Telecom ISP is up and running. Also, this test confirms that the two routers are

exchanging their routes information with the other. XYZ-1-CE is advertising its own IPs into the EIGRP process to Kalam-PE2 router.

XYZ-1-CE, which has a sub-interface Ethernet 0/0.20 with an IP address of 172.23.20.1 and this IP address has been exchanged with Kalam-PE2 and installed into PE2 routing table. After this process the PE2 tries to ping the XYZ-1-CE sub-interface interface to demonstrate successful reachability

Test Result: Pass

Test the MPLS VPN Inter-AS connectivity:

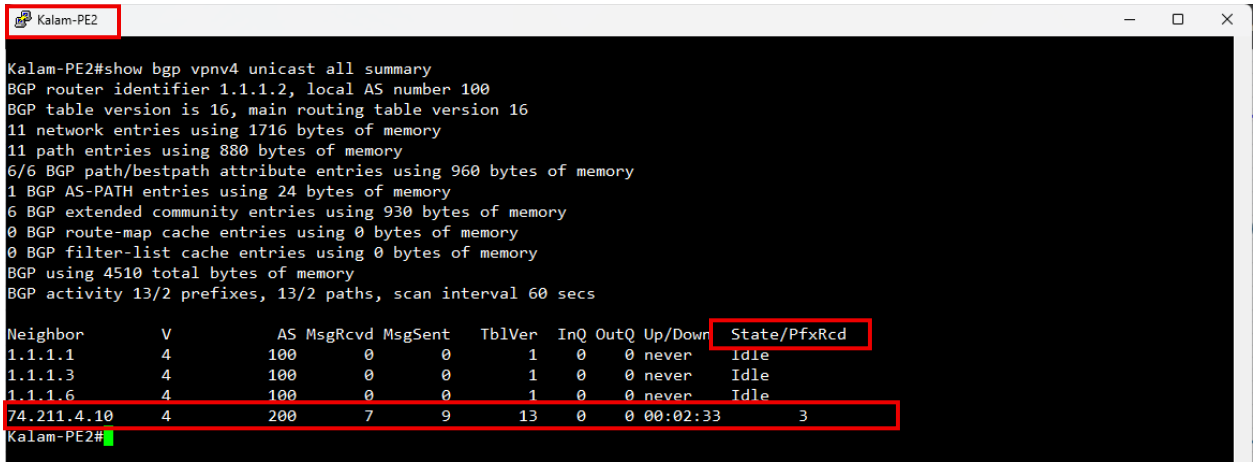

Figure 240 VPN Labels Exchanged

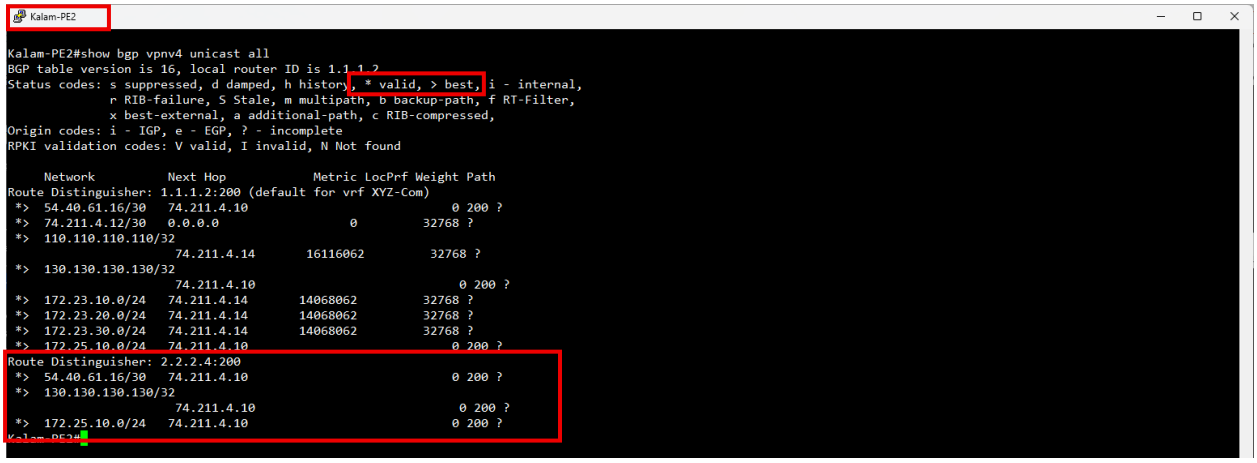

Figure 241 Prefixes Exchanged via VPN labels

This test was carried out to confirms that the VPN labels are exchanged between the two ISPs. The 130.130.130.130 IP address is allocated for the Loopback address of XYZ Company under Batelco ISP. The second figures show that on Kalam-PE2 which is the ASBR router, that the 130.130.130.130 has been received as a VPN label with a RD of 2.2.2.4:200. This demonstrate a successful VPN labels exchanged.

Test Result: Pass

Test the MPLS connectivity inside Kalam Telecom:

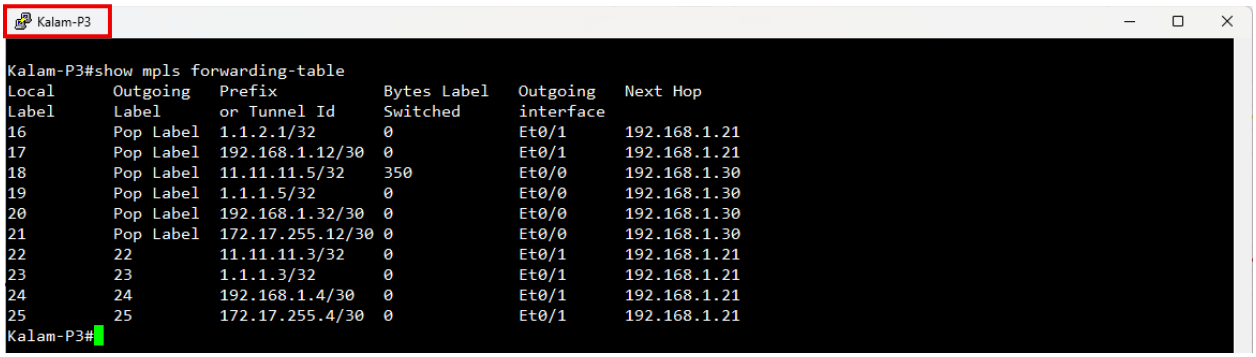

Figure 242 MPLS Labels on Kalam-P3

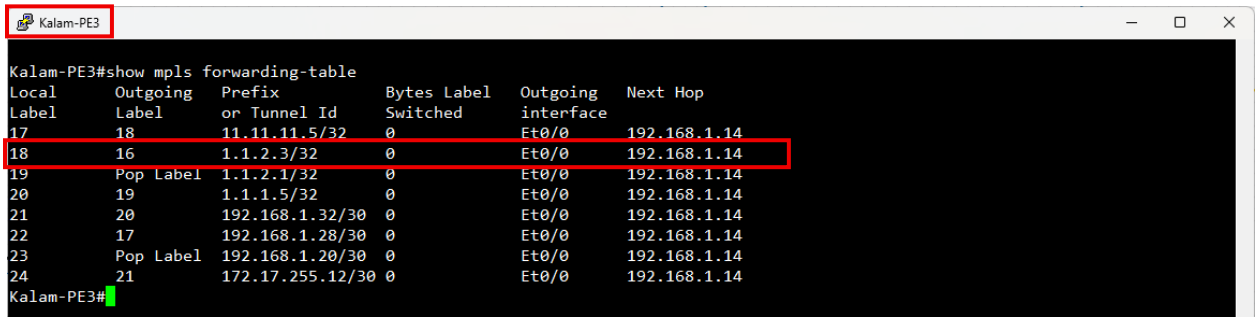

Figure 243 MPLS Labels on Kalam-PE3

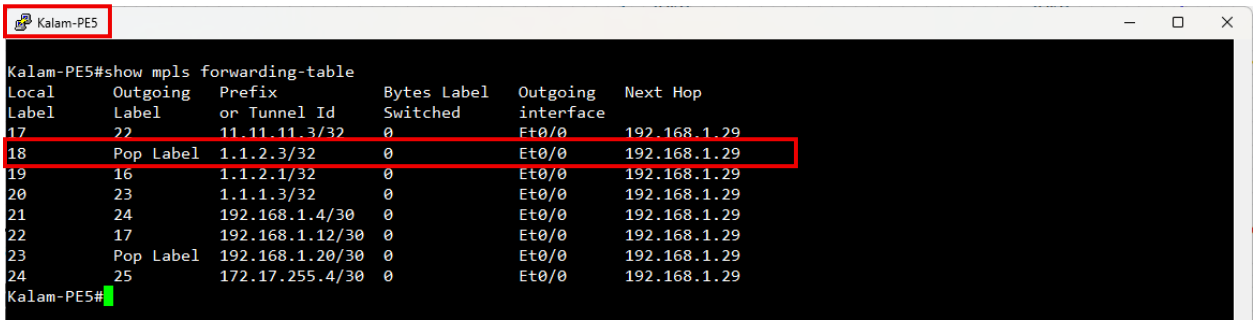

Figure 244 MPLS Labels on Kalam-PE5

This test was carried out to confirms that MPLS labels are exchanged between the backbone devices. These images show that each router has exchanged labels with each other since both Kalam-PE3 and PE5 receives labels that are assigned to the prefix 1.1.2.3 which belongs to Kalam-P3. This demonstrate successful labels exchanged between them

Test Result: Pass

Verify the isolation and customer End-to End connectivity:

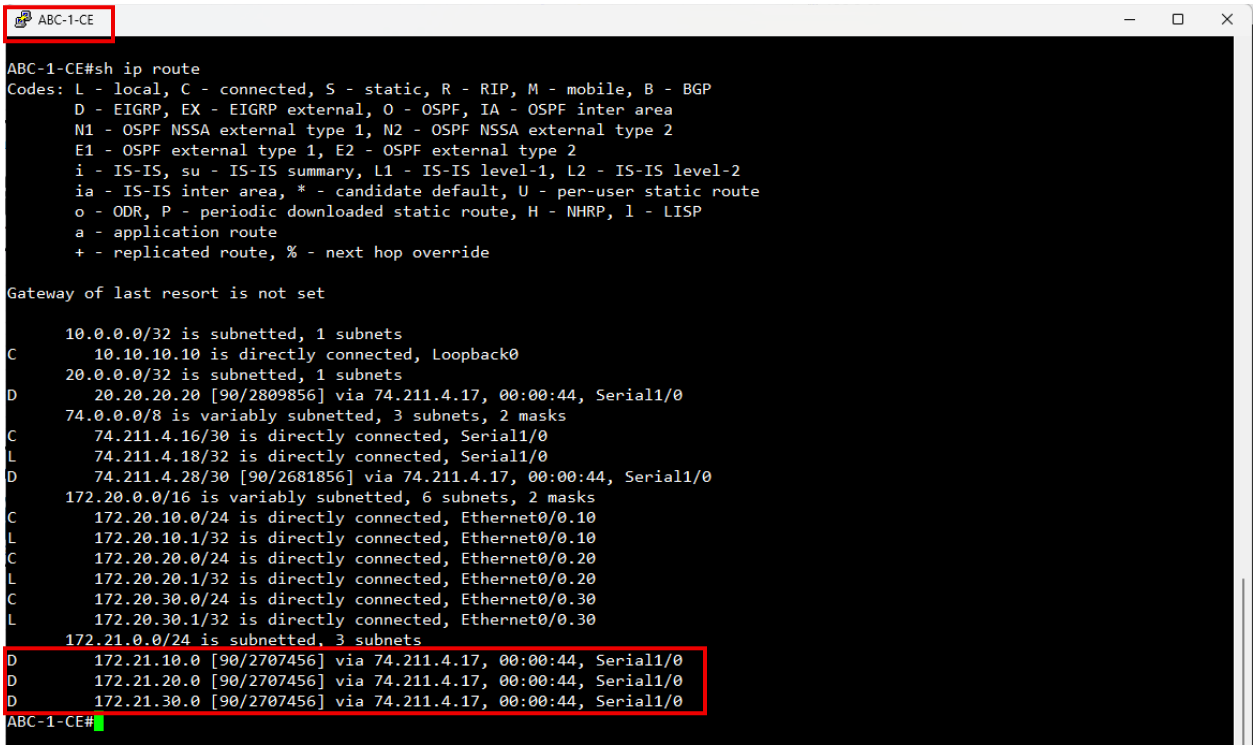

Figure 245 ABC-1-CE Routing Table

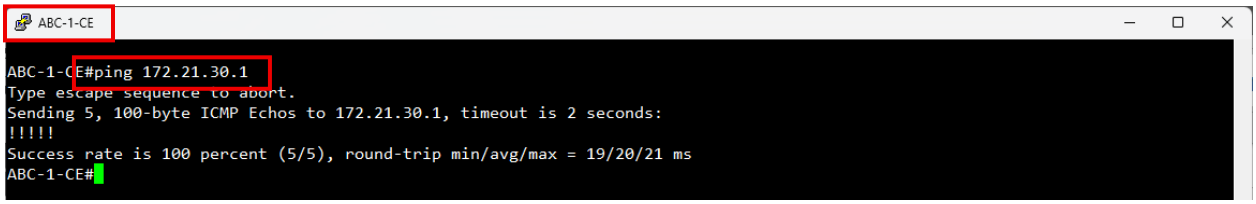

Figure 246 ABC-1-CE Ping Connectivity

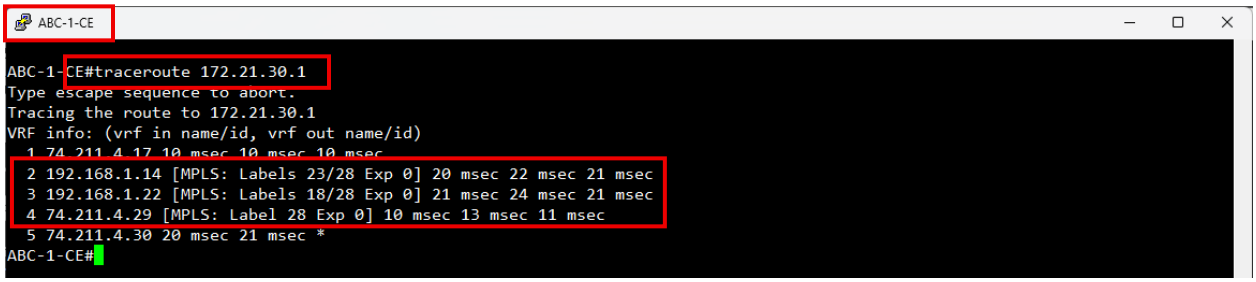

Figure 247 ABC-1-CE Traceroute

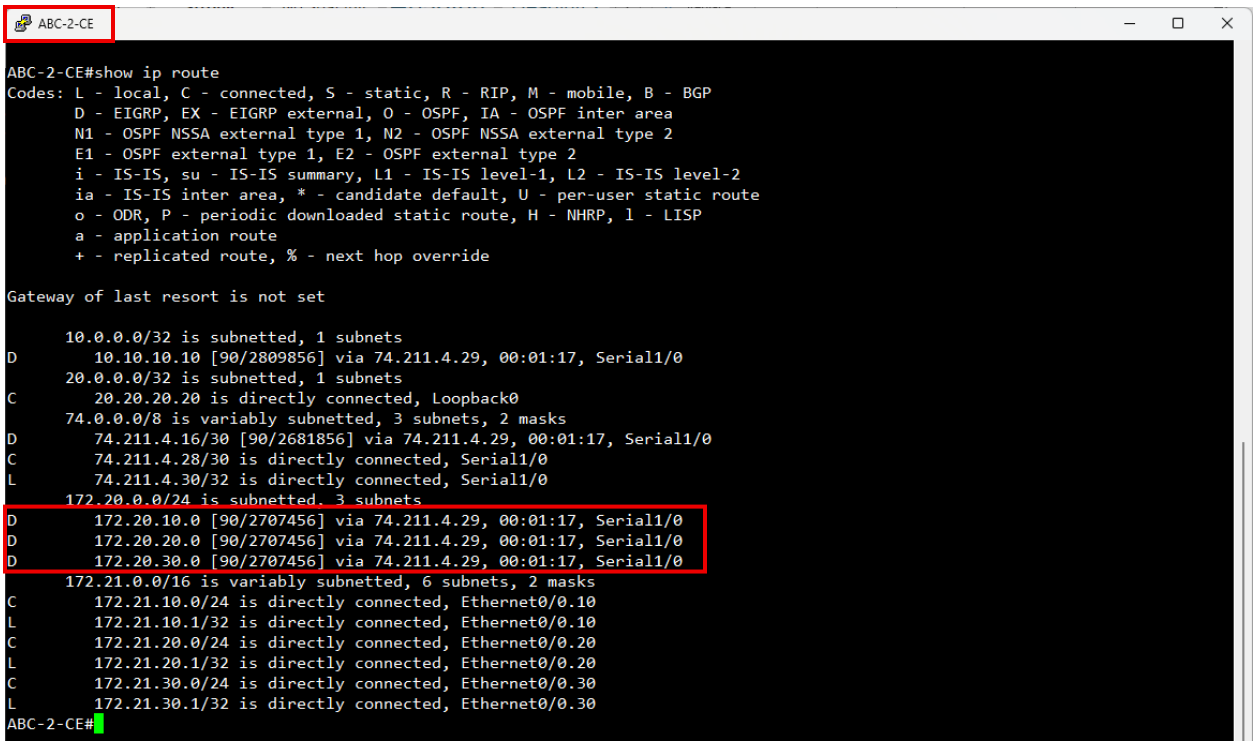

Figure 248 ABC-2-CE Routing Table

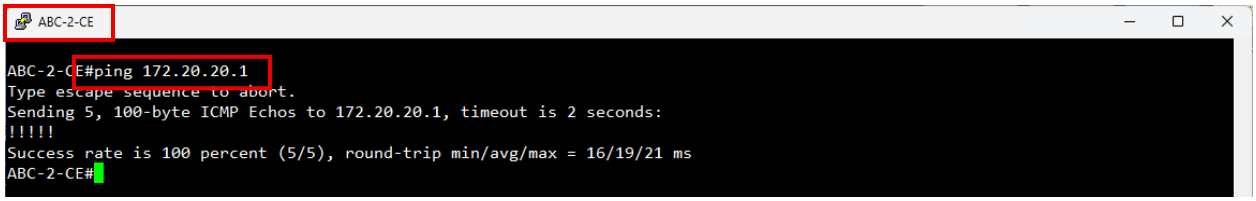

Figure 249 ABC-2-CE Ping Connectivity

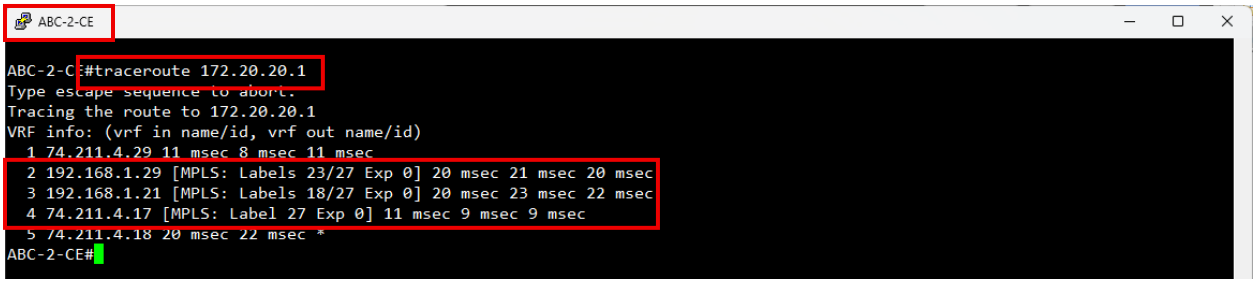

Figure 250 ABC-2-CE Traceroute

This test scenario has been performed to verify whether the customer branch has end-to-end connectivity is functional or not. At ABC-1-CE routing table, there is 3 entries for one for 172.21.10.0, one for 172.21.20.0 and 172.21.30.0 which all of them belong to the ABC-2-CE router. The ping test shows that the end-to-end connectivity is functional. Additionally,

the traceroute testing shows in the output that the packet passes through an MPLS by this specific line [MPLS: Labels]. Furthermore, this test scenarios show that all the IP addresses that have been exchanged between the ABC company are only for ABC company.

Test Result: Pass

Evaluate the AAA service:

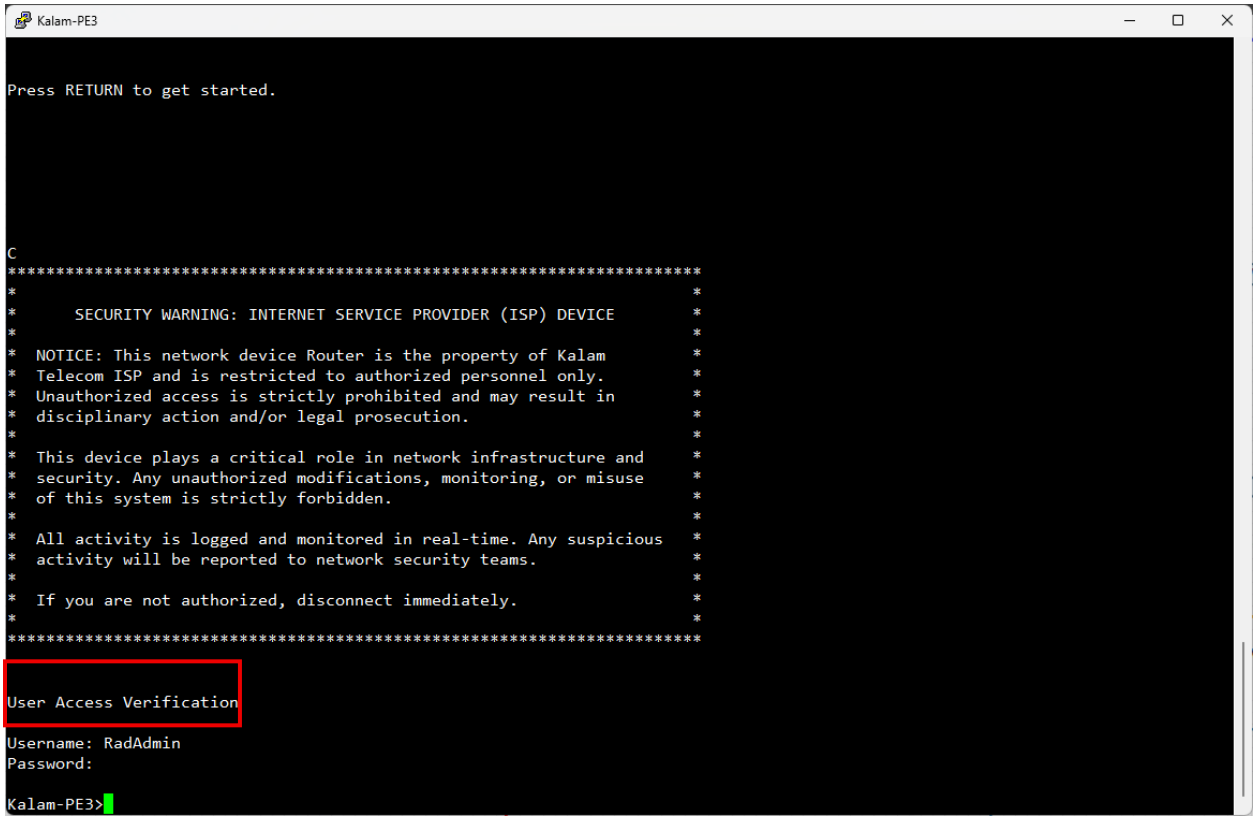

Figure 251 AAA User Login

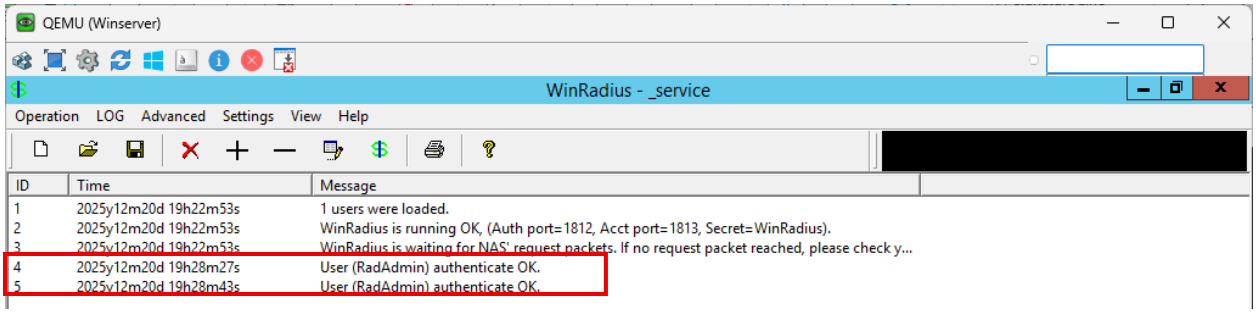

Figure 252 AAA User authenticated Successfully

This scenario test case is performed to check and evaluate if the AAA service is function properly as intended or not. The figures shows that the router has successfully authenticated the user RadAdmin using the WinRadius users database that are located on the server.

Testing Result: Pass

Verify the Syslog service:

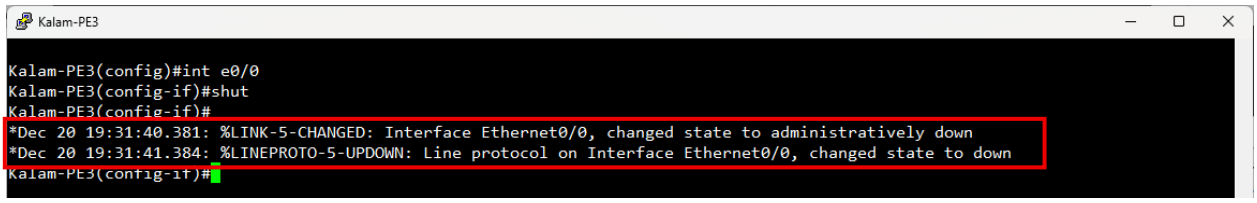

Figure 253 Syslog Output

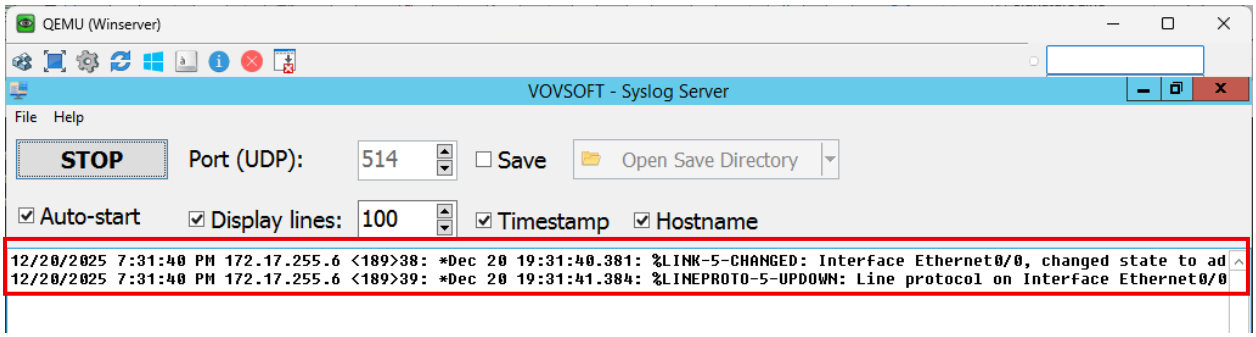

Figure 254 Syslog Output on the Server

The following test is performed to evaluate the functionality of the syslog service. As you can see, the router has sent a log to the syslog server after a changed occurs in the configuration of the router.

Testing Result: Pass

Acceptance Tests Results

After successful functionality testing, the acceptance of the participant has been conducted and taken to ensure that the implemented solution which is the MPLS backbone network meets the outlined requirement of the project and the operational expectations. This acceptance process focused on evaluating the system from a operational perspective alongside the practical perspective rather than only examining a bunch of configuration documents.

Participant	Process	Result
Ahmed Ali	Verified the security measures of the backbone, internal network and the servers	All security protocols are configured with a excellent amount of protection and security.
Khalid Abdulla	Validates WAN protocols and technologies such as the MPLS, BGP and MP-BGP in addition to the End-to-End connectivity in the customer side	Routing protocols are secured using an authentication key chain before exchanging any information
Salma Rashid	Confirmed that the internal routing are designed correctly and used efficiently in addition to the validation of the internal services such as AAA and Syslog	All internal network was able to communication with each other successfully in addition, the internal network can reach the network service without any problems.

Table 12 Acceptance Tests Results Table

Usability Testing Statistics

The main objective of conducting the usability testing statistics is to examine how much the topology can operate without any of the devices experiencing failure within the EVE-NG simulation environment. This type of testing does improve and help when doing the evaluation of the overall stability of the implemented solution design inside EVE-NG.

With the current resources that has been assigned to the EVE-NG, the testing has been performed 15 times in a row to obtain these information.

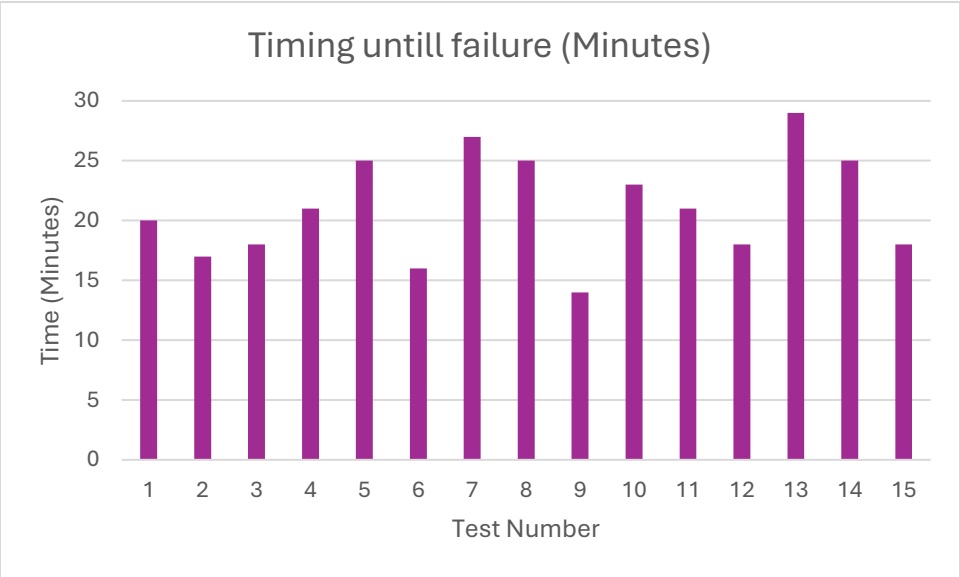

Figure 255 Usability Testing Time Until Failure

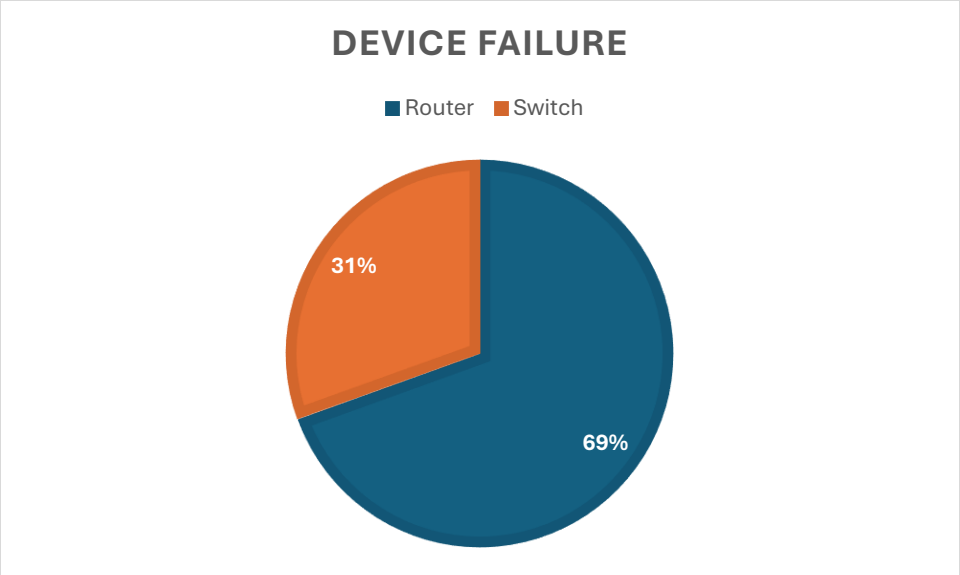

Figure 256 Device Failure Type Percentage

Based on the figures above, the results demonstrates the time duration until either a switch or router experience a failure during the simulation. The shortest time was 14 minutes, while the longest time was 29. On average device failure occurred after approximately 21 minutes of continuous operations, Furthermore, the pie chart indicates that more than 50% of the device failure has occurs by router rather than switches. This outcome is predictable and expected as any router needs more processing power to perform the routing calculation.

Discussions, LESPI and Conclusion

This final part of the thesis reflects on the overall outcomes of this project by outlining the functionality of the system and how it has been achieved, outlining the achieved objectives and goals of the project and it also addresses the issues and difficulties that arose through each phase of the project cycle such as the design, implementation and testing and evaluation. Additionally, this section will cover the backup plan for the simulated project and will also mention the future and improvements that will be applied on the project.

The summary of the experience gained from this project is also included in this section. Additionally, the relevant Legal, Ethical, Social and Professional Issues associated with the deploying an ISP network such as data privacy and service responsibility are also examined in this section.

Functionality of the system

The final deployed Kalam Telecom infrastructure solution demonstrate that the MPLS-based backbone network operates in accordance with the proposed network design and satisfies the requirements of the project. The system show a successful support and integration of the internal routing protocols such as OSPF, EIGRP, external routing protocols such as BGP, MPLS label switching, separation of customer traffic through the use of MPLS VPN, quality of service to prioritize network traffic and traffic engineered tunnels.

These functionalities combined enable scalable, reliable and secure server delivery which is suitable for ISP infrastructure. The interaction between all the protocols, MPLS services, VPN services and the supporting services such as AAA and syslog confirms that the designed solution was effectively translated and implemented into a working network infrastructure.

Achieved Objectives

Objective No.	Objective	Description	Achievement Status
1	Design a scalable ISP backbone	Develop a hierarchical network design	Achieved
2	Implement internal routing protocols	Configure OSPF and EIGRP	Achieved
3	Implement external routing	Establish external connectivity using BGP	Achieved
4	Deploying MPLS and traffic engineering	Enable and configure MPLS and Traffic engineer across the infrastructure	Achieved
5	Implement MPLS VPN services	Provide secure and separate traffic for customers	Achieved
6	Apply Quality of Service (QoS)	Prioritize critical traffic to ensure reliability and high-performance network	Achieved
7	Validate system through testing	Verify the functionality against the proposed design and requirements	Achieved
8	Conduct large-scale performance benchmarking	Measure the performance inside the simulated environment	Achieved

Table 13 Achieved Objective Table

Project issues

During the implementation phase of Kalam Telecom MPLS project, several practical problems were encountered that required reevaluation and problem-solving sessions to determines the backup plans or alternatives options. The practical problems were mainly related to software compatibility and resource limitations within the emulated environment.

One of the biggest issues I faced is using windows server 2016 inside EVE-NG environments. Windows server 2016 was chosen since it was one of the most widely used operating system in the real world. It did not function correctly inside EVE-NG because it has frequent instability issues such as crashing, the windows server goes unresponsive and performance issues which effects the service stability during the simulation testing. This problem was caused by two main points, the first one is that there is no enough resource to run these kinds of OSes in multiple quantities, the second issues was that there was a compatibility issue between the windows server secure boot feature and EVE-NG. As a backup plan, Windows Server 2012 R2 was deployed instead. This version proves to be lightweight, stable and compatible compared to the 2016 version.

Second challenge was when using windows 10 operating system. Because of the higher resource requirements, windows 10 did not perform effectively in EVE-NG environment, which leads to slow response times and crashes and occasional failure. To fix this problem windows 7 was selected as the backup option. Windows 7 requires fewer resources and provides more stable user experience while performing testing. Making it more suitable for the simulation.

Third problem was involves the resources which has been used to run the EVE-NG simulated environment. The available resources were insufficient to fully simulate two MPLS networks alongside with the multiple routing processes such as OSPF, EIGRP, BGP, MP-BGP, QoS and Traffic engineering tunnels. The limitations was primarily caused by the CPU since most of consumer CPUs don’t have an excellent number of cores. To reduce this

issues without chaining the CPU the topology was implemented and tested in stages which enable different feature to be validated independently without overload the CPU.

Finally, SolarWinds Kiwi Syslog Server comes with configuration complexity that makes it unsuitable for this project. As an alternative WinRadius was used since it's an open-source and a lightweight radius AAA solution. WinRadius was easier to deploy, install and configure and it also supports the authentication required for the project.

Backup Plan

A backup plan was established to ensure that the availability and integrity of the project data and the configuration of the systems throughout the development of the MPLS-based network. This plan is focusing on protecting the critical configuration files, virtual machines and documentation from any unexpected failure with the simulated environment.

For system and configuration backups, regular backups are performed for all network devices configuration after each major steps, which including OSPF configuration, EIGRP configuration, BGP and MP-BGP configuration, MPLS services and VPN configuration in addition to the Quality of Services and Traffic engineering. Those configuration files were stored using the 3-2-1 backup methods which means to make three copy of the data, one in my device, one on my external drive and one in GitHub repository. These backup uses two different media type physical and online, with one copy stored offsite on GitHub.

For system disaster recovery, a simple plan was defined to restore the system state in case of any failure. This plan involve reloading configuration, restoring virtual machine snapshots, having multiple version of the entire virtual machine or restarting the EVE-NG services if administrative access are accessible.

In terms of the security and availability of the backups, any backed up files whether it's on a physical media or on the cloud. All of these files will be encrypted using a strong encryption algorithm such as RSA or AES to ensure that only authorized people have access to them.

Future Work

This section discuss the future work that adds more depth into the project:

- **Deployment of ASA and Firewall Technologies**:

  One potential improvement is to integrate a dedicated firewall solution like Cisco Adaptive Security Appliance to strengthen and improve the security of the ISP backbone.

- **Implementation of BGP Route Reflector**:

  The Route Reflector can be one of the future work improvements since it reduces the number of BGP sessions within the infrastructure also the route reflector helps in ease of configuration when scaling the network since the configuration will be much less.

- **Deployment of additional Internal Services**:

  The current system can be enhanced by adding some more of the internal services such as NTP, FTP, DNS and DHCP to support internal departments and their operational needs since these services will improve time synchronization, centralized file management, automated IP addressing, and name resolution.

- **Enhanced Security through advanced route maps and ACLs**:

  Security can be one of the future upgrades since it can be improved by implementing advanced access control list across the network also the adding of route maps will offer extended security since it can be applied between ISPs to control the inbound and outbound traffic.

- **Integration of traffic generators and monitoring tools**:

Further enhancement of the system is to include some kind of traffic generator and network monitoring tools to test and evaluate the network performance such as throughput, latency, jitter and packet loss in different network topology states.

- **Segment Routing over MPLS (SR-MPLS)**:

One potential massive improvement is to deploy a Segment Routing over MPLS as it gives simplified control planes while providing greater flexibility when using traffic engineering.

- **Automation**

One good improvement for future work is to deploy some sort of automation since these can reduce some of the work and time to get through the router setup or configuration.

Summary of my experience

This project provided me with valuable hands-on experience in the designing, implementation and testing on the MPLS protocol and its many use case scenarios, which allowed me to apply theoretical concepts into a single practical environments. While working on the project I have developed a deeper understanding of the routing protocol such as OSPF, EIGRP and BGP. The most protocol I have learned about from this project is BGP, especially when it comes to inter-AS connectivity also, I have understood the concept of MPLS VPN services and how it operates. In addition, to the Quality of services and traffic engineering. Furthermore, this project have improved my problem-solving, critical thinking and planning methods since I have faced so many obstacles that need to be addressed to keep the project going.

I believe that the knowledge and the experience I have gained from this project will significantly help to in the future to secure a training position which will leads me to a job offer.

Bahraini Perspectives

From a Bahraini cultural perspective, the implementation of this project has an effects related how digital infrastructure supports communications, privacy and social interaction within the society. The society of Bahrain have a strong cultural value put on trust, privacy and responsibility when using technology. As this project focuses on upgrading the network of an ISP, the project does not directly interact with any cultural content. However, the project are indirectly influences how the individual people, families and businesses communicating and accessing the network and other digital services. Furthermore, ensuring that the customer data remains private and protected, as any misuse of these data could conflict with the Bahraini expectations.

This project also contributes positively in by supporting all the national digital transformation by enhancing the reliability of the network for education, business and social media. The improved stability and quality of the infrastructure can help in by masking online learning and remote working easier and more accessible to all citizens, all of these align with the Bahraini efforts to modernize while still keeping the current cultural identity. However, if the infrastructure upgrading process did not managed correctly, some potential risks such as service disruption, unequal access to the network and misusing any of the data might have a negative affect on the public trust and confidence.

Legal, Ethical, Social and Professional Issues

Legal Issues

The implementation of an MPLS infrastructure introduces several legal responsibility that must be considered carefully since the project is involved a core telecommunication network infrastructure, all activity going inside or outside this infrastructure are required to comply with the regulatory framework of the Kingdom of Bahrain, specifically Legislative Decree No.48 of 2002, which controls the telecommunication services. In addition, ISPs must operate under a valid license issued by Telecommunication Regulatory Authority (TRA). Furthermore, the upgraded network must not violate any national regulatory conditions. Moreover, since the project handles customer data the ISP must strictly follow Personal Data Protection Law No. 30 of 2018.

Ethical Issues

Ethical responsibility is critical in this project since the nature of the network operation with sensitive data and customer information. Ethical judgement is required to ensure that the privacy of the customers is respected at all times and places and that the customer data is not accessed and monitored beyond what is approved by the government for networks operations. All customer data must be and remain confidential and protected from any misused and exploits to be aligned with Bahrain's data protection regulations. Furthermore, service delivery needs transparency in billing practices as outlined in the Customer Protection Regulation (2017). Maintaining honesty and fairness through the project are essential to preserving customers trust.

Social Issues

The project has the potential to positively impact society by improving and enhancing network connectivity and service reliability across the entire Bahrain. The project support

all of the goals that are declared in Bahrain Economic Vision for 2030 by improving the underlaying digital infrastructure that are benefiting the user, business and public services. Fair pricing should be taken in consideration to ensure that improved service are accessible for small to medium businesses. Additionally, service interruption during infrastructure upgrades must be reduced according to the TRA Quality of Service Framework.

Professional Issues

Maintaining professional integrity are essential throughout this project. This includes obeying the international professional standards such as PMI code of ethics and professional conduct that are outlined in the PMBOK 7th edition. Documentation accuracy and transparent reporting are necessary to ensure accountability. All team members are expected to be technical competence and receive relevant training to perform their duty in a complete way to be aligned with the national labor regulation. To comply with the IEEE code of ethics and internal organization policies all employees must follow the enforced policies since it help to protect the professionality of each team member and ensures that the project reflects the best practices in the ICT field.

Conclusion

In conclusion, this project enhanced practical understanding of designing, implementing and testing an ISP carrier grade network with MPLS architecture by applying the MPLS theoretical concept into a realistic simulated environment. The key learning outcomes that gained from this project include hands-on experience on real-world protocols such as MPLS, MPLS VPN, Quality of services, BGP, MP-BGP, as well as networking testing and monitoring. This project also gave me an insight into the importance of a structured network design and problem solving when working with complex network systems that are being used in Bahrain and around the world. Although there was several limitation that affected this project overall, the experience gained from it was both very interesting and information rich.

References

Al-Selwi , A. (2013). *Anas Al-Selwi Multiprotocol Label Switching Virtual Private Network*. Retrieved from https://www.theseus.fi/bitstream/handle/10024/57879/AlSelwi-Anas.pdf?sequence=1&isAllowed=y

Allen, S. (2023, June 8). ISP Networks: Understanding the Fundamentals | Shaun Allen. Retrieved from Shaun Allen website: https://www.shaunallen.co.uk/blog/isp-networks/#isp-network-architecture

Atlassian. (2025). Architecture Diagram: Definition, Types, and Best Practices | Atlassian. Retrieved from Atlassian website: https://www.atlassian.com/work-management/project-management/architecture-diagram

AWS. (2024). What is Architecture Diagramming? - Software & System Architecture Diagramming Explained - AWS. Retrieved from Amazon Web Services, Inc. website: https://aws.amazon.com/what-is/architecture-diagramming/

Cloudflare. (2024). What Is BGP? | BGP Routing Explained | Cloudflare. *Cloudflare*. Retrieved from https://www.cloudflare.com/learning/security/glossary/what-is-bgp/

D. Awduche, Malcolm, J. R., Agogbua, J., M. O'Dell, & McManus, J. F. (1999). Requirements for Traffic Engineering Over MPLS. *Www.rfc-Editor.org*, (RFC 2702). https://doi.org/10.17487/rfc2702

Ergun, O. (2023, March 7). Introduction to MPLS Traffic Engineering (MPLS TE). Retrieved from orhanergun.net website: https://orhanergun.net/mpls-te

Fortinet. (2023a). What Is Authentication, Authorization, And Accounting (AAA) Security? Retrieved from Fortinet website: https://www.fortinet.com/resources/cyberglossary/aaa-security

Fortinet. (2023b). What Is QoS (Quality of Service)? Retrieved from Fortinet website: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service

GeeksforGeeks. (2017, October 26). Activity Diagrams Unified Modeling Language (UML). Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/system-design/unified-modeling-language-uml-activity-diagrams/

GeeksforGeeks. (2018, October 29). Computer Network | Quality of Service and Multimedia. Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/computer-networks/computer-network-quality-of-service-and-multimedia/

GeeksforGeeks. (2022, November 11). Hierarchical Network Design. Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/computer-networks/hierarchical-network-design/

GeeksforGeeks. (2023, November 24). Use Case Diagram Unified Modeling Language (UML). Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/system-design/use-case-diagram/

GeeksforGeeks. (2024, March). Deployment Diagram in Unified Modeling Language(UML). Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/system-design/deployment-diagram-unified-modeling-languageuml/

Gurung, S. (2015a). *IMPLEMENTATION OF MPLS VPN*. Retrieved from https://www.theseus.fi/bitstream/handle/10024/103442/Sanjib%20Gurungthesis.pdf?sequence=1&isAllowed=y

Gurung, S. (2015b). Implementation of MPLS VPN. *Theseus.fi*. urn:NBN:fi:amk-2015121721270

Guthrie, G. (2021, August 6). What is an architecture diagram, and why do you need one? Retrieved from Nulab website: https://nulab.com/learn/software-development/what-is-an-architecture-diagram-and-why-do-you-need-one/

Honig, J. C., Katz, D., Mathis, M., Rekhter, Y., & Yu, J. Y. (1990). Application of the Border Gateway Protocol in the Internet. *Www.rfc-Editor.org*, (RFC 1164). https://doi.org/10.17487/rfc1164

Howard, H. (2016). *Homer L. Howard*. Cisco.

IBM. (2024, October 24). Network topology. Retrieved from IBM website: https://www.ibm.com/think/topics/network-topology

Moy, J. (1994). OSPF Version 2. *Www.rfc-Editor.org*, (RFC 2178). https://doi.org/10.17487/rfc1583

Popa, L. (2021, July 20). What is Hierarchical Network Design? | Auvik Networks. Retrieved from Auvik Networks Inc. website: https://www.auvik.com/franklyit/blog/hierarchical-network-design/

Rosen, E., Viswanathan, A., & Callon, R. (2001). Multiprotocol Label Switching Architecture. *Www.rfc-Editor.org*, (RFC 3031). https://doi.org/10.17487/RFC3031

Rosen, E., & Yakov Rekhter. (2006). BGP/MPLS IP Virtual Private Networks (VPNs). *Www.rfc-Editor.org*, (RFC 4364). https://doi.org/10.17487/rfc4364

Savage, D., Ng, J., Moore, S., Slice, D., Paluch, P., & White, R. (2016). Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). *Www.rfc-Editor.org*, (RFC 7868). https://doi.org/10.17487/RFC7868

Selwi, A. (2025). Multiprotocol Label Switching Virtual Private Network. *Theseus.fi*. urn:NBN:fi:amk-201305087211

solarwinds. (n.d.). What is Syslog? - IT Glossary | SolarWinds. Retrieved from www.solarwinds.com website: https://www.solarwinds.com/resources/it-glossary/syslog

Team, C. (n.d.). Networking Software (IOS & NX-OS) - Cisco IOS. Retrieved from Cisco website: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html

Team, D. (2025). What are SSH, Telnet and Rlogin? - PuTTY Documentation. Retrieved December 20, 2025, from Documentation.help website: https://documentation.help/PuTTY/you-what.html#S1.1

Team, E. (2019, August 15). Network Topology - NETWORK ENCYCLOPEDIA. Retrieved from NETWORK ENCYCLOPEDIA website: https://networkencyclopedia.com/network-topology/

Team, E. (n.d.). Documentation. Retrieved from EVE-ND Documentation website: https://www.eve-ng.net/index.php/documentation/

Team, L. (2025, August 22). UML Use Case Diagram Tutorial. Retrieved from Lucidchart website: https://www.lucidchart.com/pages/tutorial/uml-use-case-diagram

Team, M. (2020). How to make an activity diagram. Retrieved December 20, 2025, from Mindmanager.com website: https://www.mindmanager.com/en/features/activity-diagram/?srsltid=AfmBOopxiZ1zwyhA8UoL7ZTUIf_kCvd7qHNQQokxA4gHEskZC9lz5qOT

Team, M. (2025, October 25). UML Deployment Diagrams Guide | Miro. Retrieved from https://miro.com/ website: https://miro.com/diagramming/what-is-a-uml-deployment-diagram/

Team, N. (2024). Radware Captcha Page. Retrieved from Networklessons.com website: https://networklessons.com/quality-of-service/introduction-qos-quality-service

Team, Ovh. (2020). What Is VMware? Retrieved December 20, 2025, from OVHcloud website: https://www.ovhcloud.com/en/learn/what-is-vmware/

Visual Paradigm. (2019). What is Activity Diagram? Retrieved from Visual-paradigm.com website: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/

Appendices

Appendix 1: Manuals for System and Users

This appendix section will take a look at the manuals for this project which includes:

- User manual
- System manual

User manual:

To access the Kalam Telecom network infrastructure. VMware must be installed and running in the host device. VMware is used to run the simulated environment which is EVE-NG in addition, you will need a telnet application such as Putty.

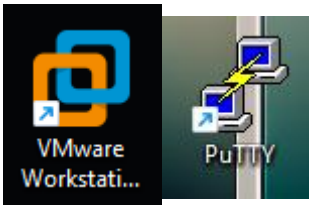

Figure 257 VMware & Putty Icons

To import and create the EVE-NG VM you chose either the “Create A New Virtual Machine” or “Open a Virtual Machine” options.

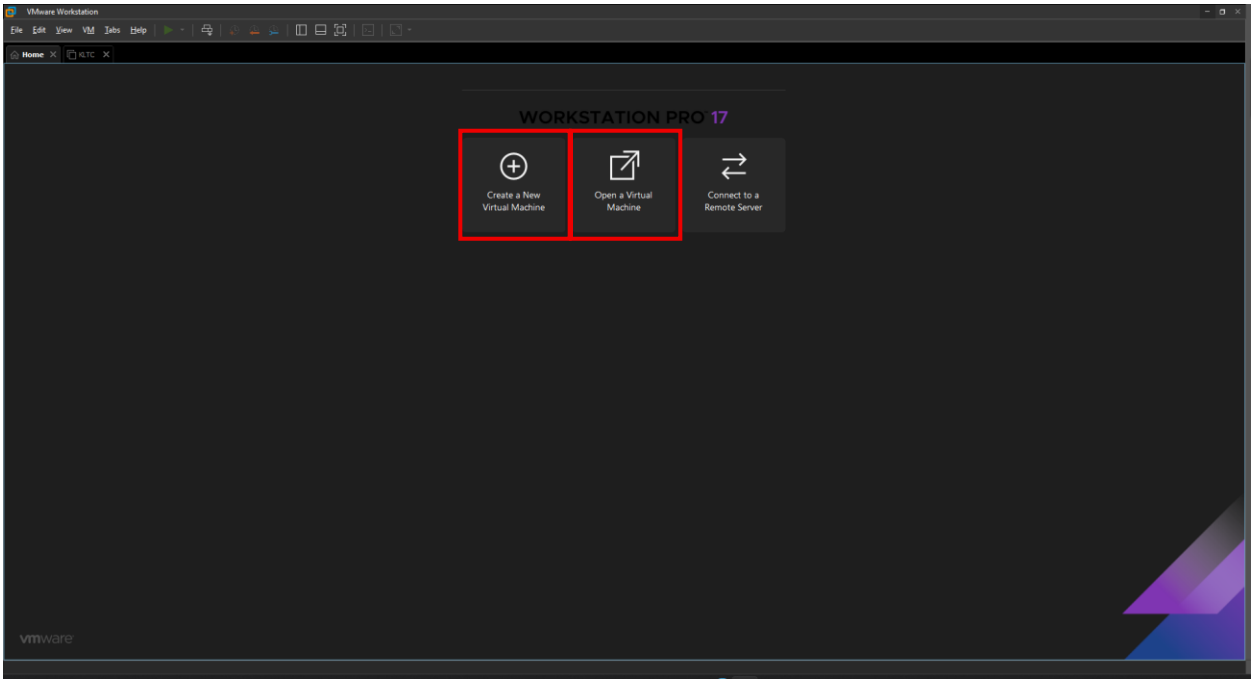

Figure 258 Create or Importing the Virtual Machine

After importing or create the Virtual Machine you click on the "Power on the virtual machine" to start the VM.

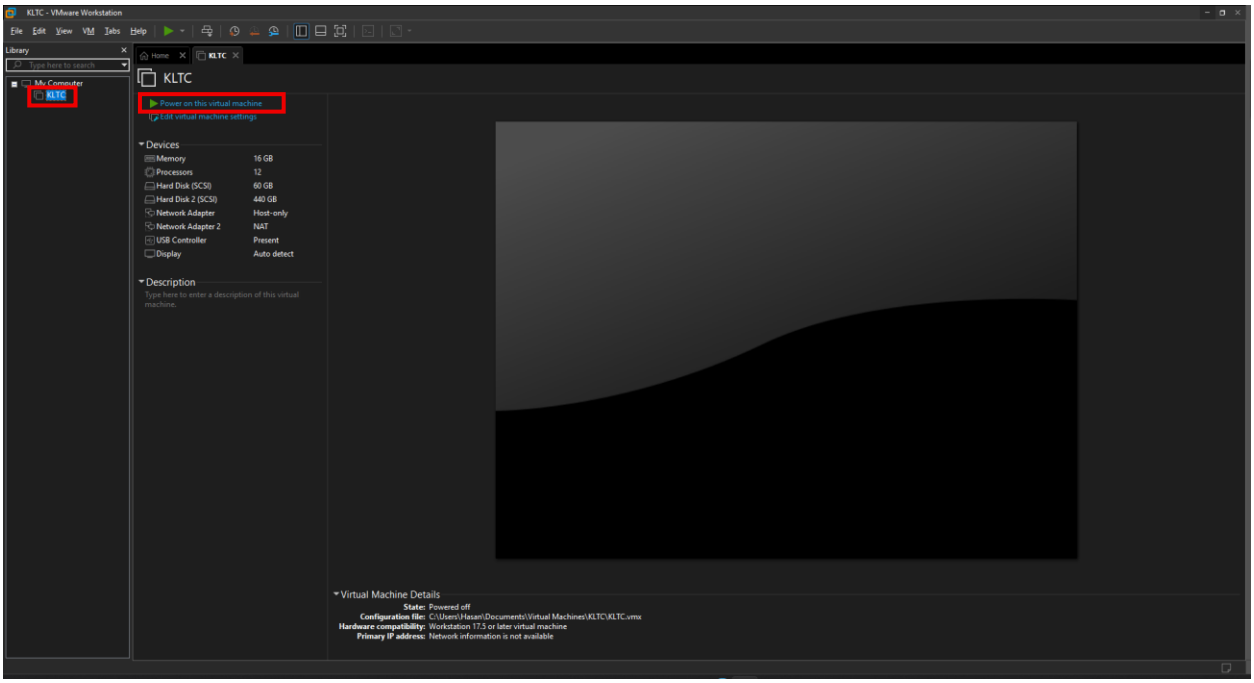

Figure 259 Starting the VM

Once the VM starts you should note down the IP shown on your screen to access it through the web browser. Please note that the IP will be different on your device.

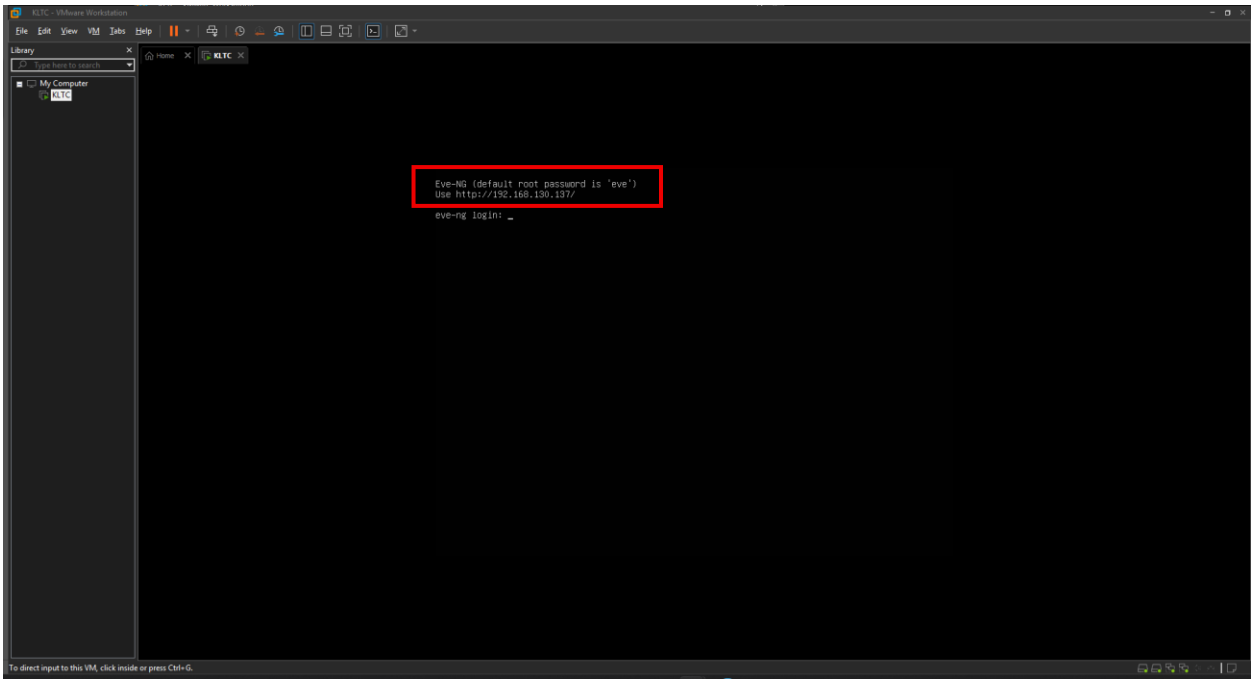

Figure 260 VM Login - Part A

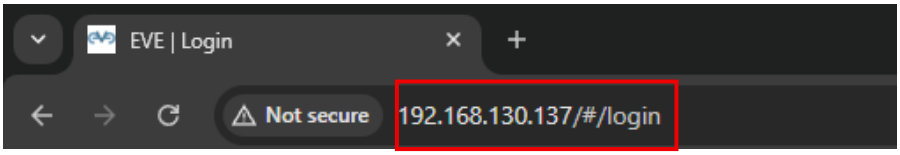

Figure 261 VM Login - Part B

After you access the IP you will be faced with this login console. The web interface requires credentials:

- **Username:** admin
- **Password:** eve

Figure 262 Login Credentials Page

After a successful login you will be present with the list of topology inside the EVE-NG VM. The Kalam Telecom Topology can be accessed by selecting the Kalam Telecom MPLS Backbone file.

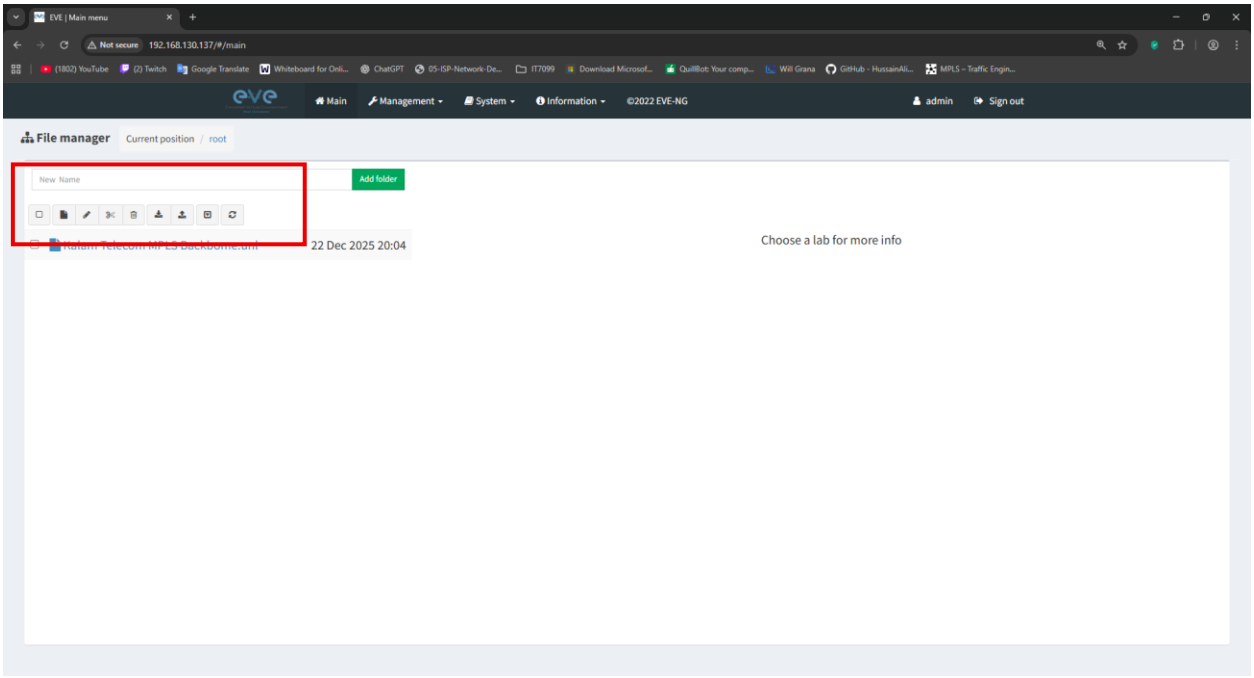

Figure 263 Accessing the Topology

To start any device from the topology just click on the icon and press start.

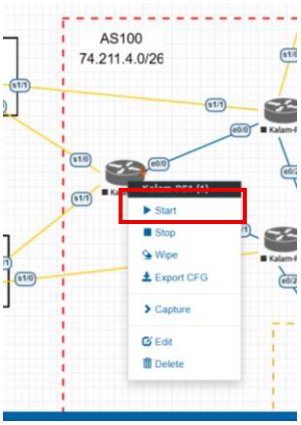

Figure 264 Starting the routers

To access the router, you should hover on top on the running router, the system will display the management IP that has been assigned to router by the EVE-NG for accessing it via Putty or any alternative solution.

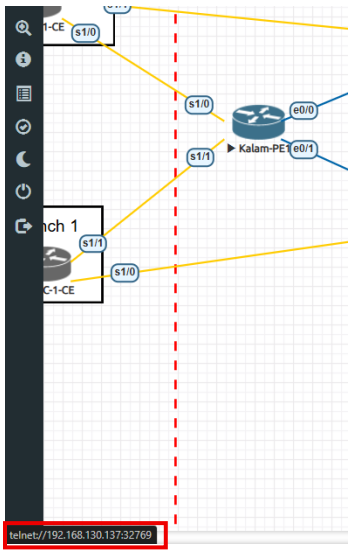

Figure 265 accessing the router – Part A

After this run the putty application and write down the management IP shows in the above figure

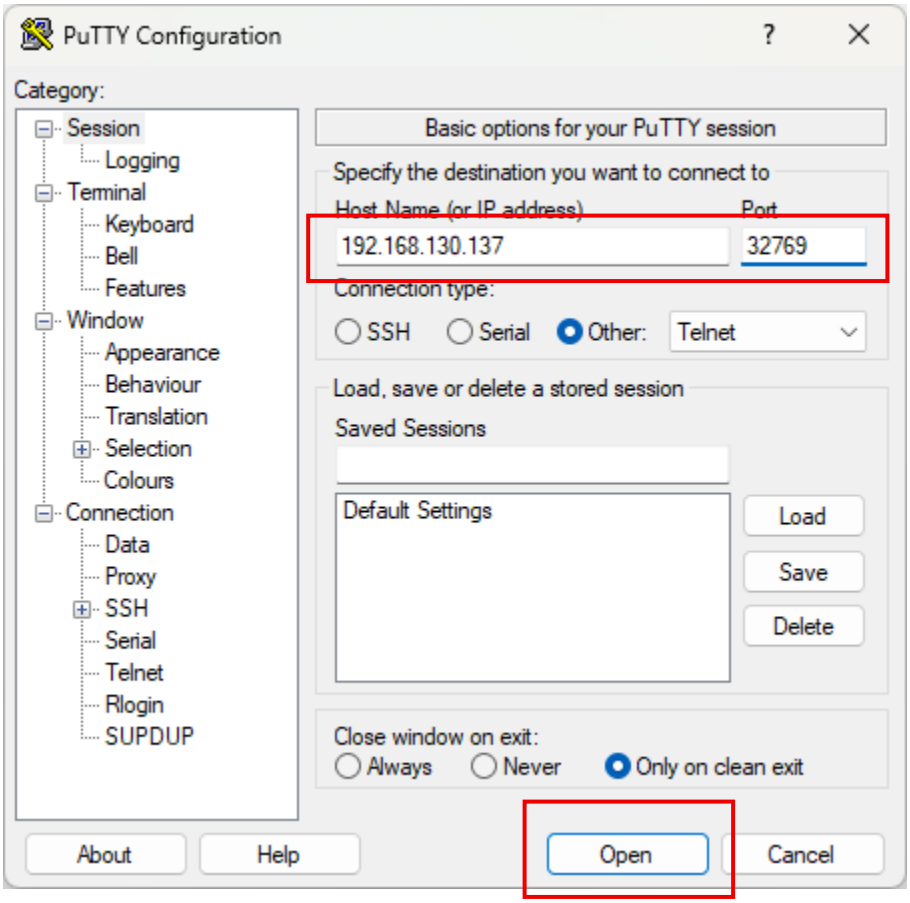

Figure 266 accessing the router – Part B

Additionally, EVE has alternative methods to access the devices by double clicking on the router and clicking on "Open SSH, Telnet client POP UP"

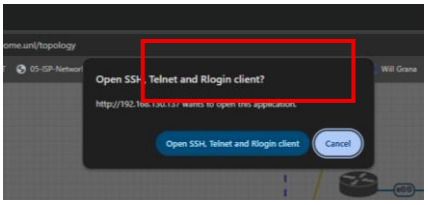

Figure 267 Accessing the router - alternative solution

Once the connection is established using either method the router will show the configuration CLI or the router. This confirms a successful connection to the router.

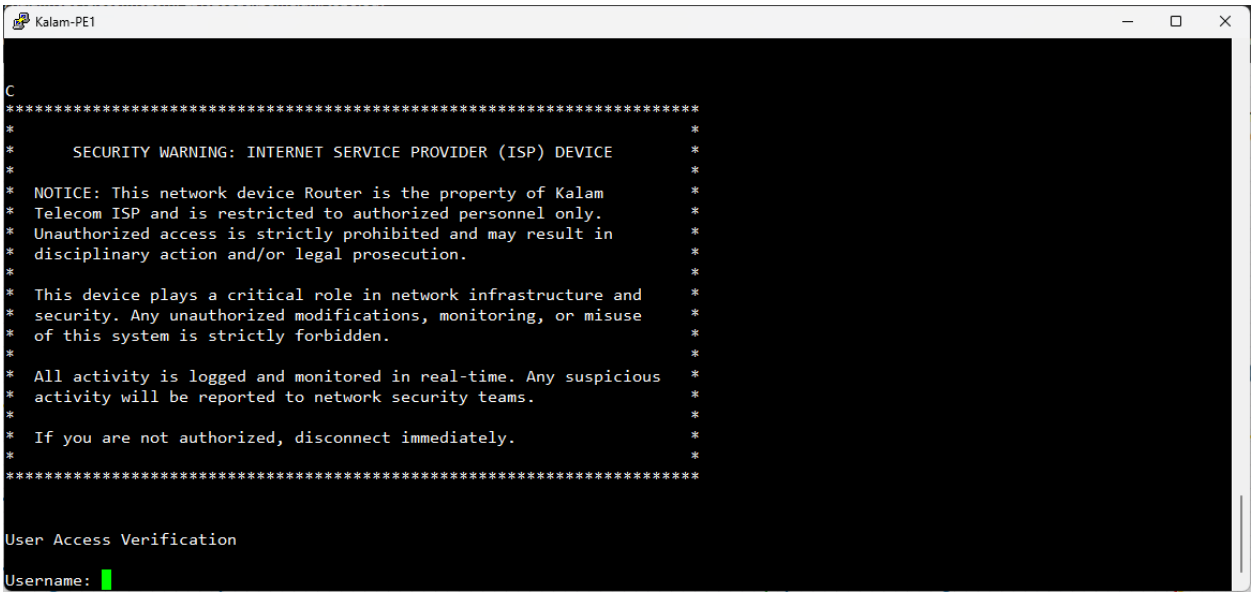

Figure 268 accessing the router – Part C

System Manual:

To upload the router, switches and windows ISO and Images into the EVE-NG VM you need a application called WinSCP, WinSCP is used to connected the main EVE-NG VM using the SFTP protocol to exchange file and folders between the host machine and EVE-NG VM.

Figure 269 WinSCP Icon Logo

To access the EVE-NG filesystem you need to connect to the VM using its IP address that was obtained earlier alongside with administrative credentials:

- **Username:** root
- **Password:** eve

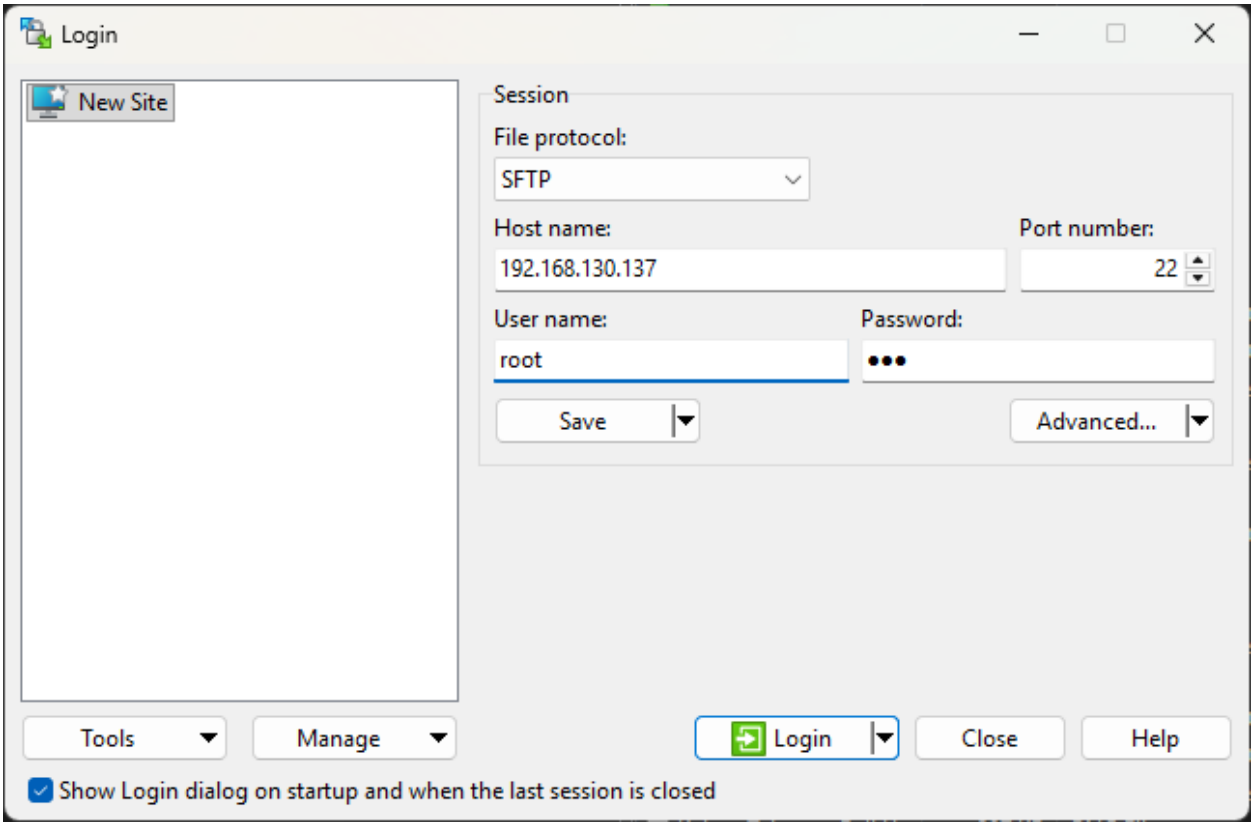

Figure 270 Accessing EVE using WinSCP - Part A

After a successful login credential you will be prompted to with this windows which has two panels, the left one is you host machine and the right side is the EVE-NG VM.

If you want to add the router, switches or windows images inside EVE you need to go to this directory "/opt/unetlab/addons" then you will find multiple folders we will focus on IOL and QEMU folders:

- IOL used for routers and switches images
- QEMU used for the Windows server 2012R2 and Windows 7

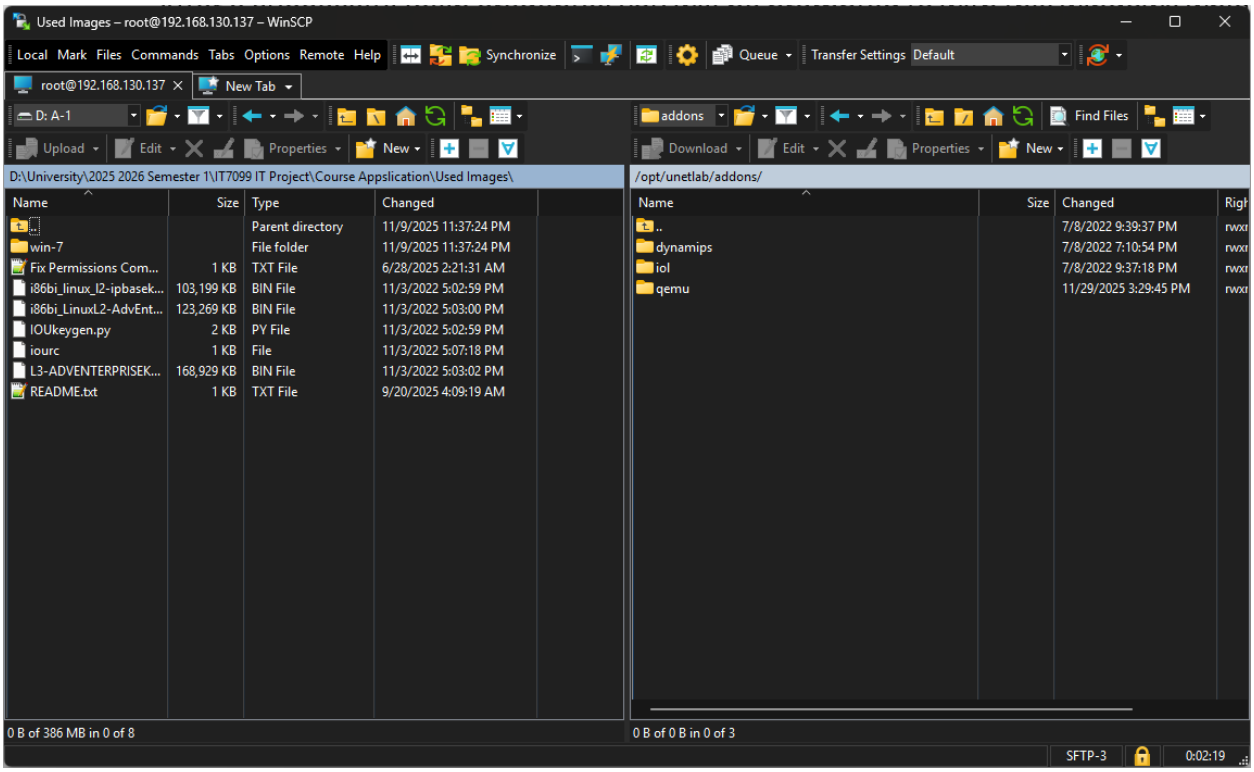

Figure 271 Accessing EVE using WinSCP - Part B

As you can see on the left side, we have multiple files which all of them representing either a router or switch in our host machine. If you want to add any image just drag and drop them inside this “opt/unetlab/iol/bin”. For this lab we will need the two images:

- i86bi_LinuxL2-AdvEnterpriseK9-M_152_May_2018
- L3-ADVENTERPRISEK9-M-15.5-2T

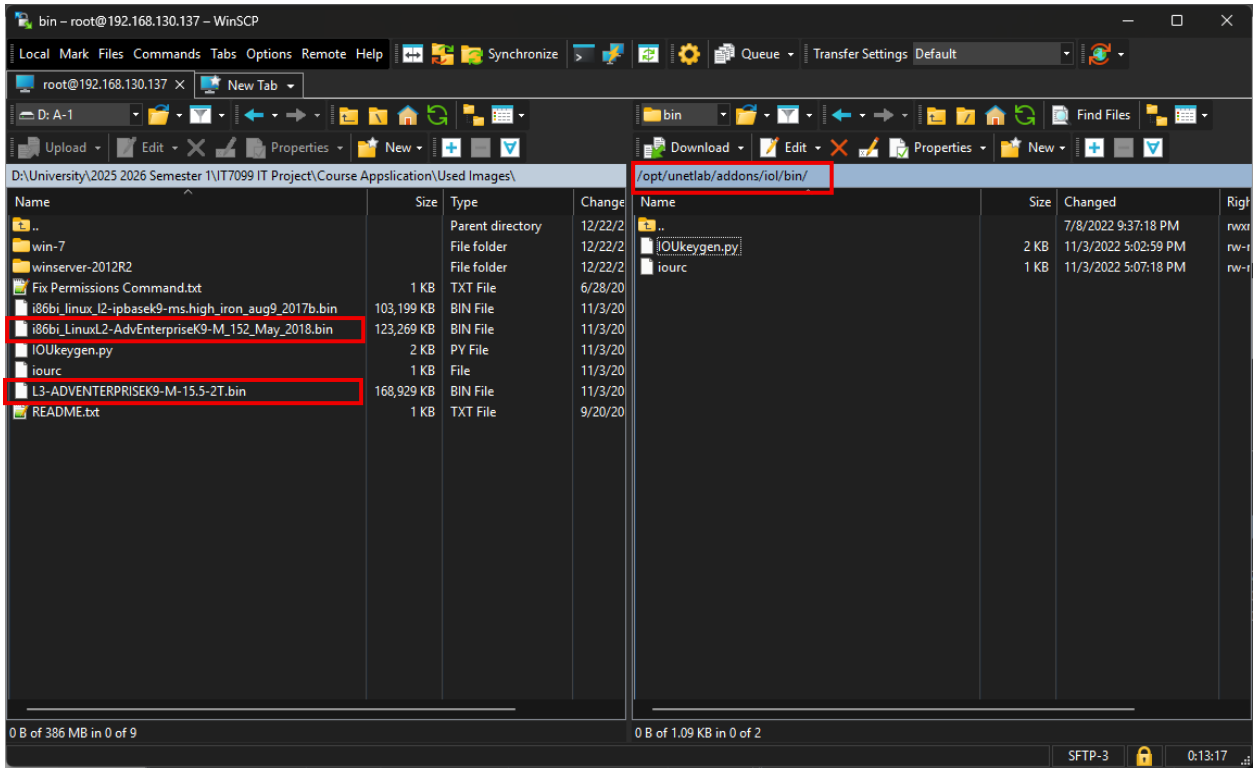

Figure 272 Accessing EVE using WinSCP - Part C

For windows devices such as the Windows 7 and Windows Server 2012 we need to go to “opt/unetlab/qemu” and do the same thing which is drag and drop the needed images or devices.

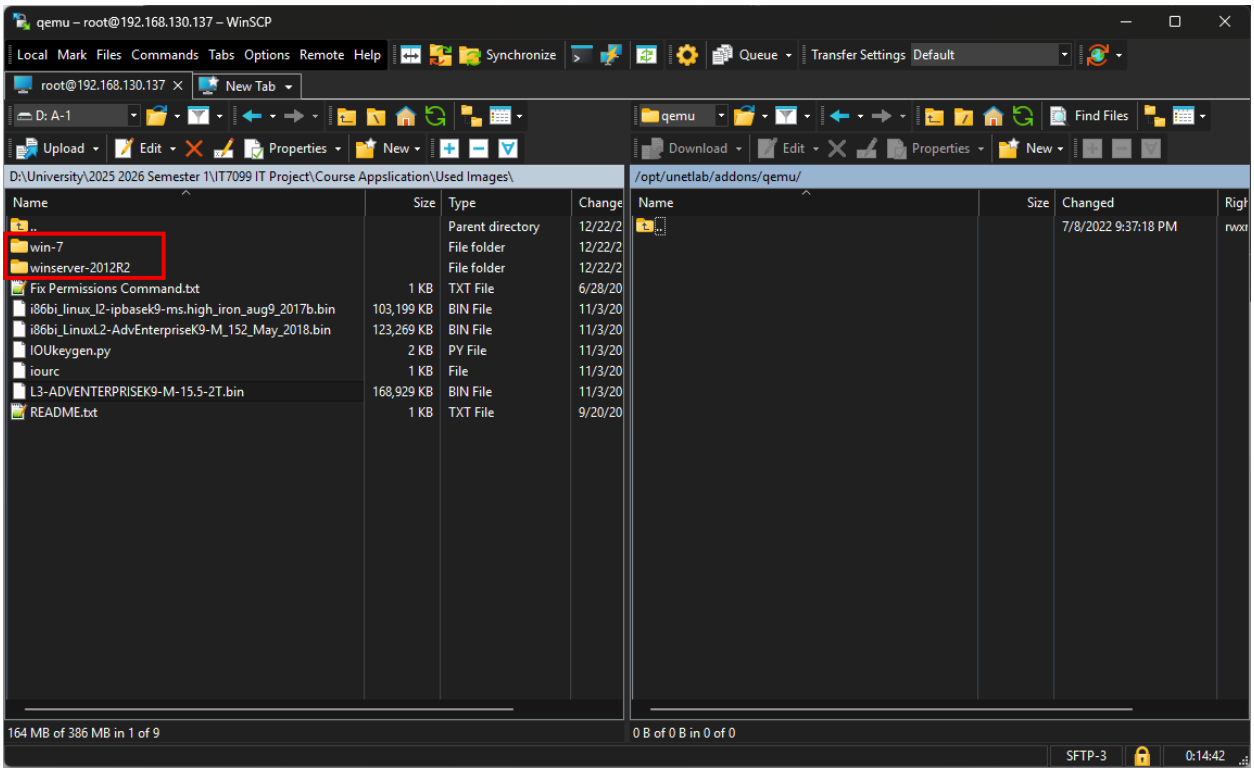

Figure 273 Accessing EVE using WinSCP - Part D

After that you will find the images inside the EVE web interface are they are ready to use.

Appendix 2: Design Specifications

This appendix outlines the detailed network design 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 section of the appendix is to describe and discuss the design, architecture and the technical elements required to implement and deploy the upgraded backbone infrastructure. This section 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 section 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

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

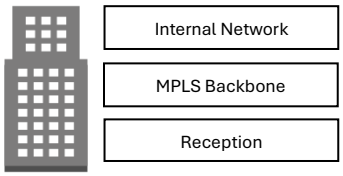

Figure 274 Building Icon

Kalam Telecom network involves three primary site categories:

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

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 and Syslog 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

Table 14 IP addresses Summary

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

Table 15 Internal Network VLAN Distribution

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-Desktop	E0	172.17.20.10	255.255.255.0	172.17.20.100
AAA-Syslog Server	E0	172.17.100.10	255.255.255.0	172.17.100.100

Table 16 Kalam Telecom IP address Scheme

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

Table 17 Batelco IP address Scheme

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

Table 18 ABC Company IP address Scheme

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

Table 19 XYZ Company IP address Scheme

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.

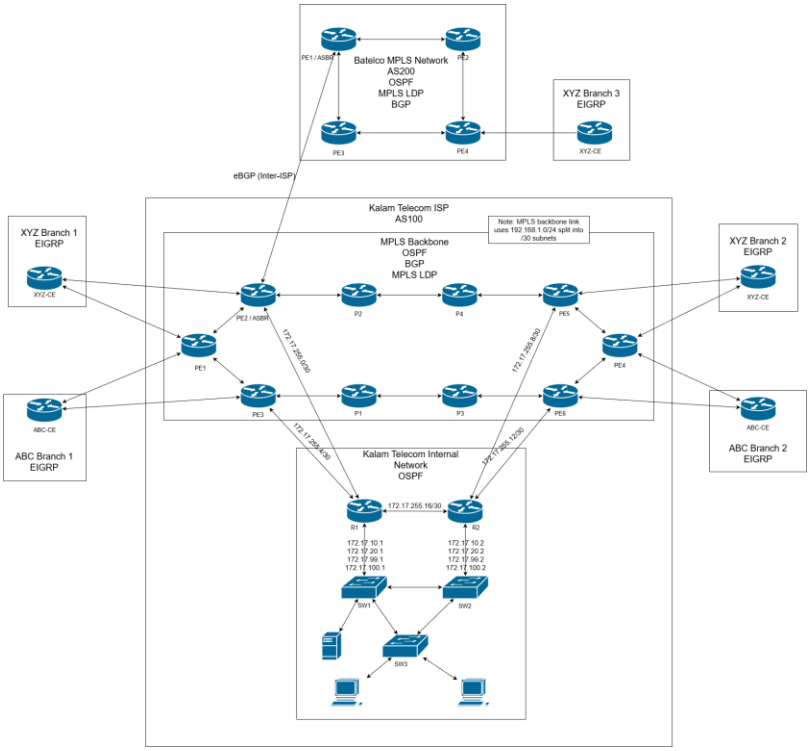

Figure 275 Network Topology – Logical Design

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 others for inter-AS routing
- Exchange labelled VPNv4 routes using the MPLS VPN inter-AS Option B
- Extend 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 is 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 isolating 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.

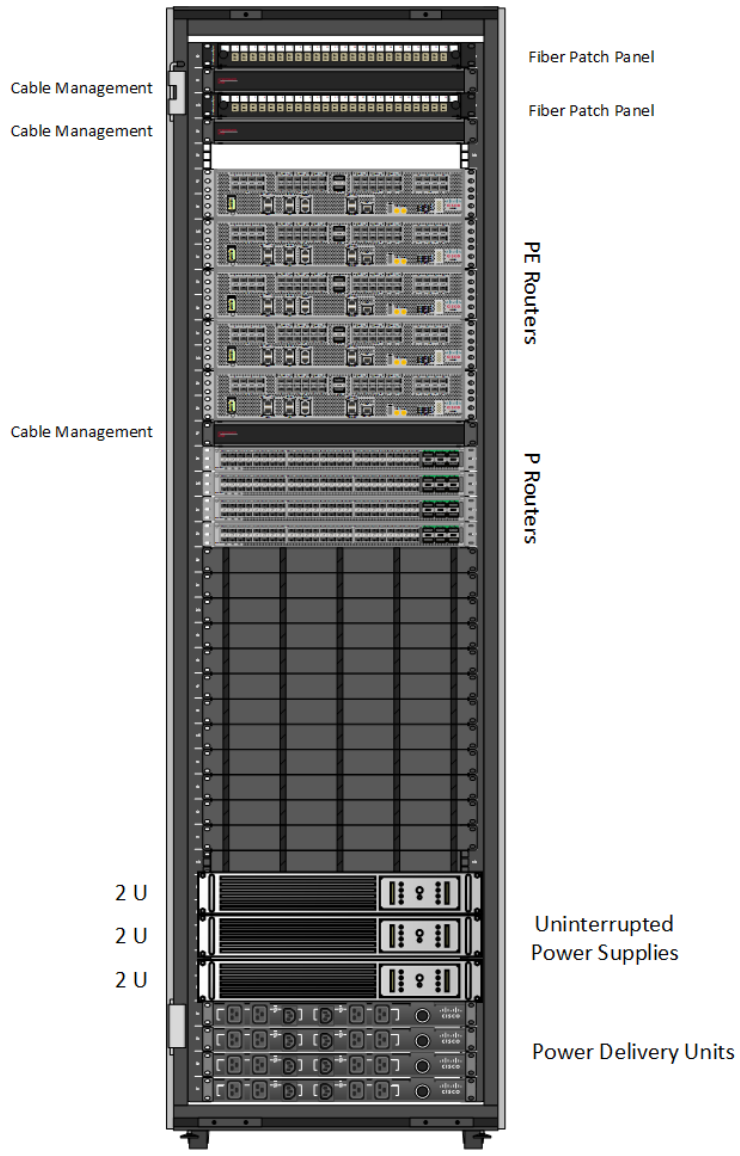

Figure 276 MPLS Core Rack Design

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.

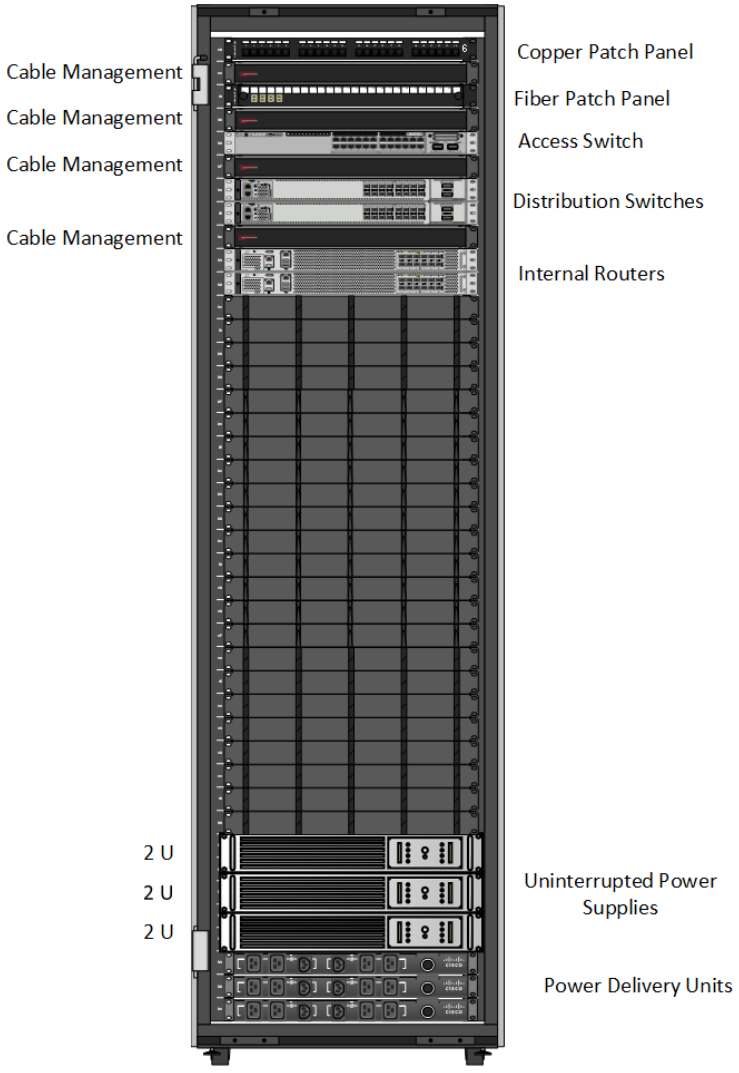

Figure 277 Internal Network Rack Design

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

Appendix 3: System Implementation

The following appendix provides the full configuration for two example routers to illustrate the practical part of the MPLS backbone project. These two router which has the Core MPLS configuration and the MPLS VPN configuration. All remaining configuration for the other router and switches can be viewed and downloaded through the GitHub repository or in the below word object file. This approach has been used due to the large number of configuration lines, including those configuration lines in this thesis document will increase the instability of the word file. Therefore, the best option is to use GitHub and Object file as a backup.

```
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Kalam-PE3
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
```

```
!
!
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone KSA 3 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
!
!
!
!
!
!
!
!


!
ip vrf ABC-Com
 rd 1.1.1.3:100
 route-target export 65001:100
 route-target import 65001:100
!
!
!
!
ip domain name KalamTelecom
ip cef
no ipv6 cef
!
```

```
multilink bundle-name authenticated
mpls ldp discovery hello interval 15
mpls ldp discovery hello holdtime 45
mpls traffic-eng tunnels
!
!
!
key chain OSPF_AuthenKey
 key 1
  key-string KalamOSPF1
  cryptographic-algorithm hmac-sha-256
key chain ABC_AuthenKey
 key 1
  key-string ABC-Kalam10
!
!
!
!
!
cts logging verbose
!
!
username LocalAdmin privilege 15 secret 9
$9$kO0FNYVi20AA2n$8Bs1dFt7VHYla4pLmvy..gul49FkATqpf6RpTw4dFTg
!
redundancy
!
!
ip ssh time-out 90
ip ssh version 2
!
class-map match-any Cus-ICMP-Q
 match dscp af31
class-map match-any Cus-Voice
 match ip dscp ef
class-map match-any Cus-Voice-Q
 match dscp ef
```

```
class-map match-any Cus-ICMP
 match protocol icmp
!
policy-map QoS-Core
 class Cus-Voice-Q
  priority 1024
 class Cus-ICMP-Q
  bandwidth percent 30
 class class-default
  fair-queue
policy-map Traffic-Mark-In
 class Cus-Voice
  set dscp ef
 class Cus-ICMP
  set dscp af31
 class class-default
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 no shutdown
 ip address 1.1.1.3 255.255.255.255
!
interface Loopback1
 no shutdown
 ip address 11.11.11.3 255.255.255.255
```

```
!
interface Ethernet0/0
 no shutdown
 description Link to Kalam-P1
 ip address 192.168.1.13 255.255.255.252
 ip ospf authentication key-chain OSPF_AuthenKey
 mpls traffic-eng tunnels
 mpls ip
 service-policy output QoS-Core
 ip rsvp bandwidth 5000
!
interface Ethernet0/1
 no shutdown
 description Link to Kalam-PE1
 ip address 192.168.1.6 255.255.255.252
 ip ospf authentication key-chain OSPF_AuthenKey
 mpls traffic-eng tunnels
 mpls ip
 service-policy output QoS-Core
 ip rsvp bandwidth 5000
!
interface Ethernet0/2
 no shutdown
 description Link to Kalam-R2
 ip address 172.17.255.6 255.255.255.252
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
!
interface Serial1/0
 no shutdown
 description Link to ABC-1-CE
 ip vrf forwarding ABC-Com
 ip address 74.211.4.17 255.255.255.252
 serial restart-delay 0
```

```
 service-policy input Traffic-Mark-In
!
interface Serial1/1
 no shutdown
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no shutdown
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no shutdown
 no ip address
 shutdown
 serial restart-delay 0
!
!
router eigrp MPLS
 !
 address-family ipv4 unicast vrf ABC-Com autonomous-system 10
  !
  af-interface default
   passive-interface
  exit-af-interface
  !
  af-interface Serial1/0
   authentication mode md5
   authentication key-chain ABC_AuthenKey
   no passive-interface
  exit-af-interface
  !
  topology base
   redistribute bgp 100 metric 64 1000 255 1 1500
```

```
  exit-af-topology
  network 74.211.4.16 0.0.0.3
 exit-address-family
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 router-id 1.1.1.3
 summary-address 172.17.0.0 255.255.128.0
 redistribute ospf 5 subnets
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
 network 1.1.1.3 0.0.0.0 area 0
 network 11.11.11.3 0.0.0.0 area 0
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.1.12 0.0.0.3 area 0
 network 192.168.1.48 0.0.0.3 area 0
!
router ospf 5
 redistribute ospf 1 subnets
 network 172.17.255.4 0.0.0.3 area 0
!
router bgp 100
 bgp router-id 1.1.1.3
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 1.1.1.2 remote-as 100
 neighbor 1.1.1.2 update-source Loopback0
 neighbor 1.1.1.5 remote-as 100
 neighbor 1.1.1.5 update-source Loopback0
 neighbor 11.11.11.1 remote-as 100
 neighbor 11.11.11.1 update-source Loopback1
 neighbor 11.11.11.2 remote-as 100
 neighbor 11.11.11.2 update-source Loopback1
```

```
 neighbor 11.11.11.4 remote-as 100
 neighbor 11.11.11.4 update-source Loopback1
 neighbor 11.11.11.5 remote-as 100
 neighbor 11.11.11.5 update-source Loopback1
 neighbor 11.11.11.6 remote-as 100
 neighbor 11.11.11.6 update-source Loopback1
 !
 address-family ipv4
  neighbor 11.11.11.1 activate
  neighbor 11.11.11.2 activate
  neighbor 11.11.11.4 activate
  neighbor 11.11.11.5 activate
  neighbor 11.11.11.6 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community both
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 send-community both
  neighbor 1.1.1.5 activate
  neighbor 1.1.1.5 send-community both
 exit-address-family
 !
 address-family ipv4 vrf ABC-Com
  redistribute eigrp 10
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list standard SSH-ACL
 permit 172.17.10.0 0.0.0.255
!
```

```
logging host 172.17.100.10
!
!
mpls ldp router-id Loopback0 force
!
!
radius server KalamAAA
 address ipv4 172.17.100.10 auth-port 1812 acct-port 1813
 key WinRadius
!
!
control-plane
!
!
!
!
!
!
!
banner motd ————————————————C
**************************************************************************
*                                                                        *
*     SECURITY WARNING: INTERNET SERVICE PROVIDER (ISP) DEVICE       *
*                                                                        *
*  NOTICE: This network device Router is the property of Kalam        *
*  Telecom ISP and is restricted to authorized personnel only.        *
*  Unauthorized access is strictly prohibited and may result in       *
*  disciplinary action and/or legal prosecution.                  *
*                                                                        *
*  This device plays a critical role in network infrastructure and     *
*  security. Any unauthorized modifications, monitoring, or misuse     *
*  of this system is strictly forbidden.                          *
*                                                                        *
*  All activity is logged and monitored in real-time. Any suspicious   *
*  activity will be reported to network security teams.               *
*                                                                        *
*  If you are not authorized, disconnect immediately.                *
```

```
*                                                                    *
**********************************************************************
```

```
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 access-class SSH-ACL in
 transport input ssh
!
ntp authentication-key 1 md5 15390A000527051018 7
ntp authenticate
ntp trusted-key 1
ntp server 11.11.11.1 key 1 prefer
ntp server 1.1.3.1 key 1
ntp server 11.11.11.4 key 1
!
End
```

```
!
! Last configuration change at 18:21:17 KSA Thu Dec 11 2025 by LocalAdmin
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Kalam-P1
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
```

```
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
!
!
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone KSA 3 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
```

```
ip domain name KalamTelecom
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
mpls ldp discovery hello interval 15
mpls ldp discovery hello holdtime 45
mpls traffic-eng tunnels
!
!
!
key chain OSPF_AuthenKey
 key 1
  key-string KalamOSPF1
  cryptographic-algorithm hmac-sha-256
!
!
!
!
!
cts logging verbose
!
!
username LocalAdmin privilege 15 secret 9
$9$rC2iQXHIoL9zIX$AAdbEMql08Vy1MX6tUUvY2tEMLDZ/LOVHmg/Rc7JPAQ
!
redundancy
!
!
ip ssh time-out 90
ip ssh version 2
!
class-map match-any Cus-ICMP-Q
 match dscp af31
class-map match-any Cus-Voice-Q
 match dscp ef
!
```

```
policy-map QoS-Core
 class Cus-Voice-Q
  priority 1024
 class Cus-ICMP-Q
  bandwidth percent 30
 class class-default
  fair-queue
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 no shutdown
 ip address 1.1.2.1 255.255.255.255
!
interface Ethernet0/0
 no shutdown
 description Link to Kalam-PE3
 ip address 192.168.1.14 255.255.255.252
 ip ospf authentication key-chain OSPF_AuthenKey
 mpls traffic-eng tunnels
 mpls ip
 service-policy output QoS-Core
 ip rsvp bandwidth 5000
!
interface Ethernet0/1
 no shutdown
```

```
 description Link to Kalam-P3
 ip address 192.168.1.21 255.255.255.252
 ip ospf authentication key-chain OSPF_AuthenKey
 mpls traffic-eng tunnels
 mpls ip
 service-policy output QoS-Core
 ip rsvp bandwidth 5000
!
interface Ethernet0/2
 no shutdown
 no ip address
 shutdown
!
interface Ethernet0/3
 no shutdown
 no ip address
 shutdown
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 router-id 1.1.2.1
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
 network 1.1.2.1 0.0.0.0 area 0
 network 192.168.1.12 0.0.0.3 area 0
 network 192.168.1.20 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list standard SSH-ACL
 permit 172.17.10.0 0.0.0.255
```

```
!
logging host 172.17.100.10
!
!
mpls ldp router-id Loopback0 force
!
!
radius server KalamAAA
 address ipv4 172.17.100.10 auth-port 1812 acct-port 1813
 key WinRadius
!
!
control-plane
!
!
!
!
!
!
!
banner motd ————————————————C
**********************************************************************
*                                                                    *
*     SECURITY WARNING: INTERNET SERVICE PROVIDER (ISP) DEVICE       *
*                                                                    *
*  NOTICE: This network device Router is the property of Kalam       *
*  Telecom ISP and is restricted to authorized personnel only.       *
*  Unauthorized access is strictly prohibited and may result in      *
*  disciplinary action and/or legal prosecution.                     *
*                                                                    *
*  This device plays a critical role in network infrastructure and   *
*  security. Any unauthorized modifications, monitoring, or misuse   *
*  of this system is strictly forbidden.                             *
*                                                                    *
*  All activity is logged and monitored in real-time. Any suspicious *
*  activity will be reported to network security teams.              *
*                                                                    *
```

```
*  If you are not authorized, disconnect immediately.                *
*                                                                     *
**********************************************************************
```

```
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 access-class SSH-ACL in
 transport input ssh
!
ntp authentication-key 1 md5 11221809161F253834 7
ntp authenticate
ntp trusted-key 1
ntp server 11.11.11.1 key 1 prefer
ntp server 1.1.3.1 key 1
ntp server 11.11.11.4 key 1
!
End
```

Object File - Kalam Telecom Complete Cc