Developing a Secure and Scalable Internet Service Provider using CISCO Networking Technologies

by

Shaffat Shafin Anando
20101240

An internship report submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
Brac University
June 2025.

Declaration

It is hereby declared that

1. The report submitted is my own original work while completing degree at Brac University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Shaffat Shafin Anando

20101240

Approval

The project titled "Developing a Secure and Scalable Internet Service Provider using CISCO Networking Technologies " submitted by

1. Shaffat Shafin Anando (20101240)

of Spring, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science in June 2025.

Examining Committee:

Primary Supervisor:
(Member)

Dr. Md. Golam Rabiul Alam

Professor
Computer Science and Engineering
BRAC University

Secondary Supervisor:
(Member)

Md. Kawsar Ahmed

General Manager
Infrastructure and Access Network
AccessTel Limited

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD

Chairperson and Associate professor
Department of Computer Science and Engineering
Brac University

Abstract

This project focuses on designing and simulating a secure Internet Service Provider (ISP) network using Cisco Packet Tracer, with an emphasis on layer 3 switching, VLAN segmentation, and Proper security configurations. The network was built using Cisco layer 3 switches, and Firewalls to ensure that the network is robust, scalable and secure. Key configurations include VLAN Trunking, Access Control Lists, DHCP setup, OSPF Configuration(for internal communication), BGP Configuration(for communication with the IIG network) and port security to mitigate common threats such as unauthorized access, spoofing, and DDOS attacks. The simulation successfully demonstrated a functional ISP network with proper traffic management redundancy and security policies. This project serves as a practical reference for implementing secure enterprise-grade networks using Cisco technologies.

This internship is a compulsory course for the completion of my Bachelor's degree at BRAC university and so, I have to submit this report on which my work as an intern Network Engineer at AccessTel will be evaluated. I have shared the work culture, the office environment and the company profile in this report. I have also mentioned about my learning and experience at AccessTel. It will provide a very comprehensive review of my experience and the projects I have been working on as an intern Network Engineer at AccesTel.

Dedication

I want to dedicate my years of endless efforts and unslept struggling nights of my educational life to my parents. without them, I have no existence.
Also, I want to devote my internship work to respectable supervisor Md.Kawsar Ahmed who helped me in every stages during my internship period.

Acknowledgement

Firstly, all praises go to Almighty Allah for whom I could complete my internship without any major interruption.
Secondly to my Supervisor Md. Kawsar Ahmed, General Manager, AccessTel for his kind support and advice to complete my tasks.
Thirdly, Dr. Golam Rabiul Alam sir who guided me the whole time.
Finally my parents, without their support It wasn't possible. With their kind support and help I am on the verge of my graduation.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 About the Internship

Internships are very important in linking theoretical knowledge gained in learning environment with practical uses. They offer students and young graduates a special chance to take part directly in working situations. This experience helps people transmit what they learned in class into real skills, while getting key knowledge about the daily tasks in their chosen areas. For students, Internships offer an important way into jobs, helping both personal and professional growth and building a strong base for future job searches. From the view of companies, Internships give a good chance to find and grow new talent, forming a pool of possible future workers who are already familiar with the company's work culture and tasks. This reciprocal relationship allows both the interns and the organizations to evaluate compatibility and explore future prospects.

Academic institutions are increasingly acknowledging internships as a compelling alternative to conventional academic projects, as they integrate practical, experiential learning experiences. BRAC University made it mandatory for the students to either, write a thesis paper or complete an internship at a reputable company related to the field of their major. The students must complete at least 75 credits to be eligible to do an internship or work for a thesis paper under the supervision of their desired supervisor.

My internship at AccessTel LTD as a Network Engineer exemplifies this opportunity. AccessTel LTD, a prominent telecommunications firm, offered a platform where I could apply my networking skills in a real-world scenario. I aimed to optimize my learning throughout this experience by gaining hands-on knowledge in network engineering and contributing to tangible projects, which I believe will greatly enhance my future career.

1.2 Problem Statement

Traditional ISP networks most often suffer from the following problems:
• lack of segmentation, leading to broadcast storms and security risks.
• Weak access control making the network vulnerable to attacks.

• No redundancy, causing single points of failure.

This project addresses this issues by implementing a secure, segmented, and fault tolerant network in Cisco Packet Tracer.

1.3 Objective

This report will provide the reader with the following details:

1.3.1 Aims of this Internship

The main aim of submitting this report is to portray my work experience and the knowledge I gathered.

1.3.2 Specific Goals

The specific goals for this report:
• Portray the profile of the company in detail
• Describe the environment and work culture at AccessTel
• To demonstrate all the services AccessTel Limited provides to its clients
• State the type of works AccessTel Limited does
• To demonstrate what I have learnt during the period of the internship
• To explain in details all the works that were assigned to me

1.4 Methodology in Brief

This report is completely focused on my experiences and learnings during my internship at AccessTel. Most of the data used here is based on my personal experiences. Some of the information are also taken from different websites. The data is collected from the following sources:

1.4.1 Primary Data

• Practical experiences from work
• Discussions and lessons taken from colleagues and team leaders
• Seminars and team meetings

1.4.2 Additional Information

• AccessTel Limited official website
• Internet

Chapter 2

Company Profile

2.1 Overview

Founded in 1997, Access Telecom (BD) Ltd. (AccessTEL) is an innovation focused company, acting through its various business lines, is one of the country's leading technology service providers to consumers, businesses and government entities. With a presence all around the country, AccessTel offers Internet and Data Services, Enterprise Cloud Services, Enterprise Resource Planning (ERP) Services, System Analysis and Integration Services and Online Tutor Education Services that are designed to meet customers' demand for reliability, scalability, security and control. (AccessTel, n.d.)

2.2 Vision and Mission

AccessTel aims to be the most top-ranked service providers of the country, serving for a better, smart and digital Bangladesh.

2.3 How Does AccessTel Limited Work

A company needs well structured and well organized workforce to achieve it's mission and vision. The figure below describes the detailed structure of how AccessTel operates through the devotion and hard work of it's experienced Network Engineers technicians and management employees.

Figure 2.1: Company Structure

2.4 AccessTel service Projects

AccessTel's Service Organizational structure is divided into the following Business Lines: (AccessTel, n.d.)

2.4.1 Internet Data Services

• Builds manages a nationwide broadband infrastructure for Internet and Data Services (AccessTel, n.d.)
• In collaboration with global technology leaders manages the Enterprise Cloud Services. (AccessTel, n.d.)
• Is a certified Google Partner for Google Workspace, a solution for an integrated secure Spam/Virus free mail/video conference/cloud storage/calendar and business collaboration tools. (AccessTel, n.d.)
• Manages scalable cloud resources in major Data Centers in Europe and USA for its cloud storage and hosting services. (AccessTel, n.d.)

2.4.2 Enterprise Resource Planning (ERP)

• Is a Value Added Reseller of SAP Business One, world's leading ERP software vendor SAP for customizing, implementing and supporting SAP Business One. (AccessTel, n.d.)
• Has partnerships with Fairfax Group Ltd. (USA) and Fairfax Solutions India Pvt. Ltd. (India) for developing and supporting software add-ons that are fully integrated with the SAP Business One for enhanced capabilities and innovative unique solutions. (AccessTel, n.d.)

2.4.3 SAI (System Analysis and Integration)

• Designs, installs and manages large integrated and dynamic network solutions that incorporate all the relevant cyber security defensive safeguards and best practices. (AccessTel, n.d.)
• Is a certified Google for Education partner and provides analysis, design, Google enablement, migration from legacy system to Google Platform, training and support services to educational institutions. (AccessTel, n.d.)

2.4.4 AccessTUTOR

• Has developed and operates an online education platform where students can find expert tutors, irrespective of their geographic location, to receive live interactive online classes for an effective learning process from the comfort and safety of their homes. (AccessTel, n.d.)

Chapter 3

Training Phase as an Intern

3.1 Overview

Working as a Network Engineer Intern within a dynamic company like AccessTel Limited provided me an invaluable opportunity for my professional growth and career development, particularly in today's competitive job market. Internships offer a crucial bridge between academic learning and real world application, allowing students and recent graduates to gain practical experience and develop essential skills. This experience not only strengthened my resume but also facilitates a smoother transition into the professional world.
My internship at AccessTel Limited as a Network Engineer Intern was designed to offer a thorough introduction to the complexities of network operations in a large-scale ISP IIG setting. Although there wasn't a formal, structured training program with classroom sessions, the focus on practical experience, along with ongoing guidance from experienced network engineers, enabled me to quickly fit into the team and start making valuable contributions. This hands-on, experiential approach was crucial in establishing a solid foundation for my later work. This report contains several screenshots that of my work, however due to confidentiality, I won't be able to attach certain parts of the panels I worked on.

This section discusses technical or methodological Requirements, data or resource requirements (software), etc.

3.2 Getting familiar with the Access Network Infrastructure

.

3.2.1 Getting Familiar with the Access Portal

The most crucial first step in my internship was, getting familiar with the AccessTel's internal portal also known as Access Portal which serves as the central hub of both managing employee operations and various company workflows. This ERP system is the backbone of the company daily operations. At the very beginning of my internship period, I learned how to navigate the portal, access various relevant

information related to the network infrastructure, access customer data and also the internal documentations. Understanding the structure and functionalities of the portal was very essential for accessing resources, submitting reports, and collaborating with other teams.

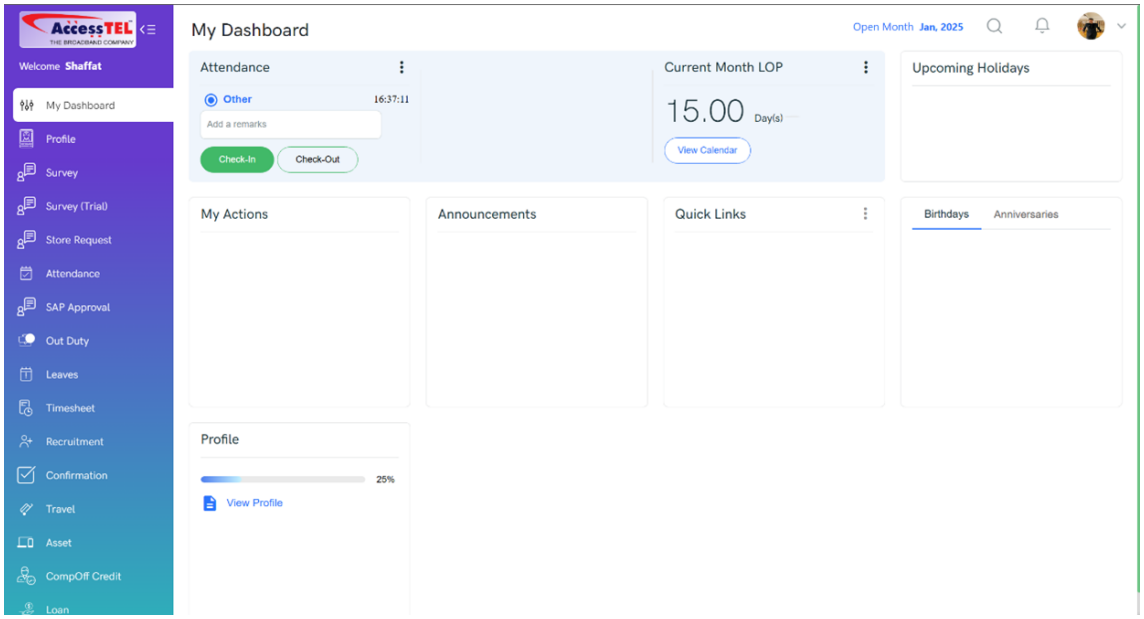

Figure 3.1: General view of Access Portal

Specific functionalities I explored includes the ticketing system for reporting network issues,

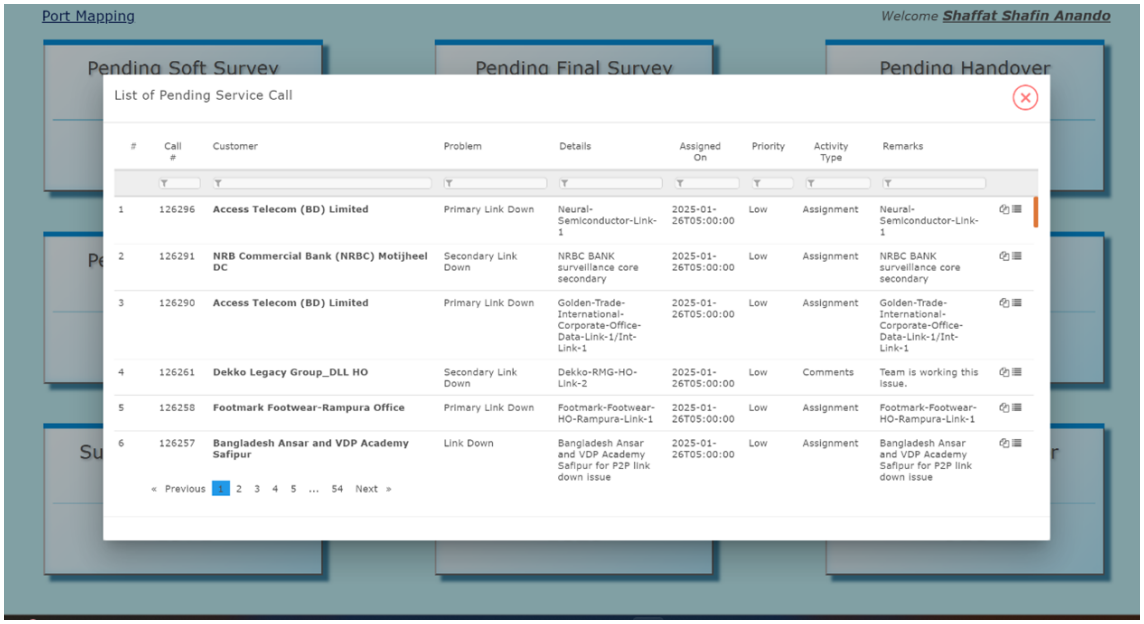

Figure 3.2: Ticketing system view on Access Portal

The inventory management module for tracking network equipment.

Figure 3.3: Inventory management at Access Portal

This provided me with valuable insight of how different departments within the company interact and how information is managed and shared.

3.2.2 Getting familiar with the Physical Layer devices

During the initial phase of my internship, I focused on gaining a comprehensive understanding of the AccessTel Network's physical layer and its associated devices. The devices form the foundation of network infrastructure. This involved getting familiar with various network devices, including:

POP (Point of Presence) Routers: Pop routers are high performance routers used to exchange high traffic between several large networks and the internet at a large scale unlike the routers we use at our home, these routers are not designed to deploy any wireless connection but is designed to manage high traffic between large scale networks.

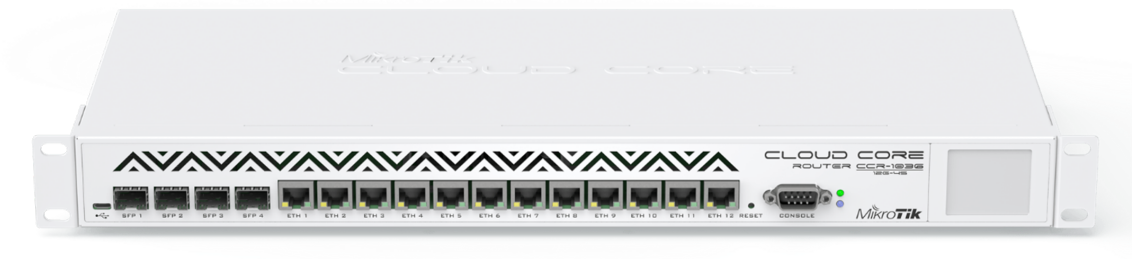

Figure 3.4: Mikrotik POP router

OLTs (Optical Line Terminals: In optical fiber networks, the most used device called OLT device acts as the central office device that serves as the end point of a PON (Passive Optical Network). This device manages the communication between the provider's network to the ONU at the customer's end. Functionalities of ONU include optical signal transmission, bandwidth allocation and network management.

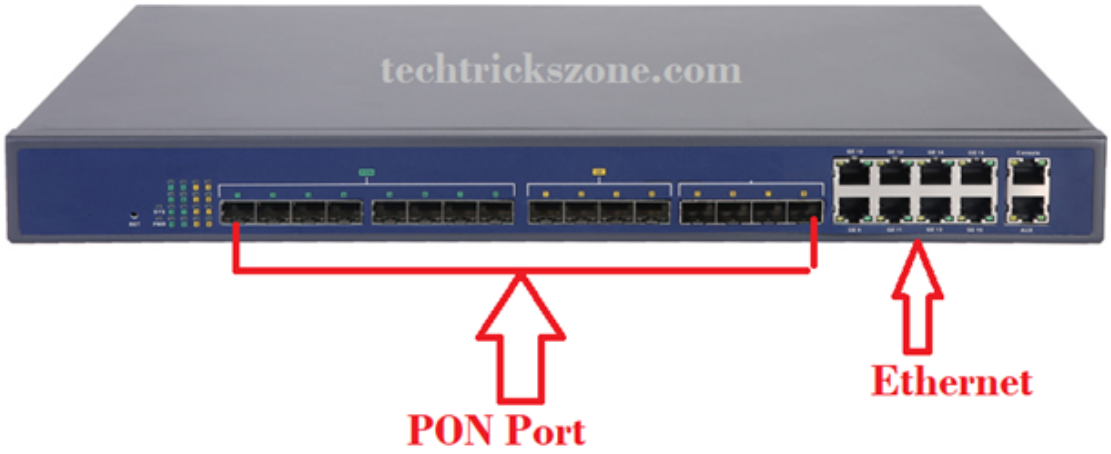

Figure 3.5: OLT device

Switches: These are layer 2 devices that acts as the distributor in a LAN network based on MAC address table. Their forwarding mechanism includes learning, flooding and forwarding. These devices has a big role in creating efficient and manageable LANs.

Figure 3.6: CISCO Switch

Media Converters: MC devices are the ones that play a very vital role in data transmission in a fiber optic network. These devices converts the fiber optic signals into electrical signals that are recieved by end devices. They convert light signal of 1350nm and 1550 nm into light signals.

Figure 3.7: FP enabled Fiber Media Converter

ONUs (Optical Network Units): ONU is another form of a media converter that is used for a point to point connection. These devices also convert optical signals into electrical signals as the customer end.

Figure 3.8: ONU device

TJBs (Terminal Joint Boxes): TJBs are joint boxes that are used to secure the junction between two or more optical fibers, to protect them from external disturbances.

Figure 3.9: Fiber Terminal Joint Box

This formal introduction and exploration of the physical layer provided me with solid foundation on understanding how the network is designed and how data is transmitted at the most fundamental level, this knowledge was very essential for understanding the subsequent tasks and projects I worked on throughout my internship.

3.2.3 Using Network Monitoring Tools

AccessTel uses a variety of softwares for monitoring and maintenance of the network infrastructures. These software plays a inevitable role in monitoring the Access network and find vuknerable points and also finding the issues. Most used Softwares include Nagios, WhatsUp GOLD and Observium. I learnt how these softwares work and how I can monitor the different problems in the network.

Nagios: Nagios is an event monitoring system that offers monitoring and alerting services for servers, switches, applications and services (wikipedia, n.d.). The different interfaces of Nagios core is Illustrated below:

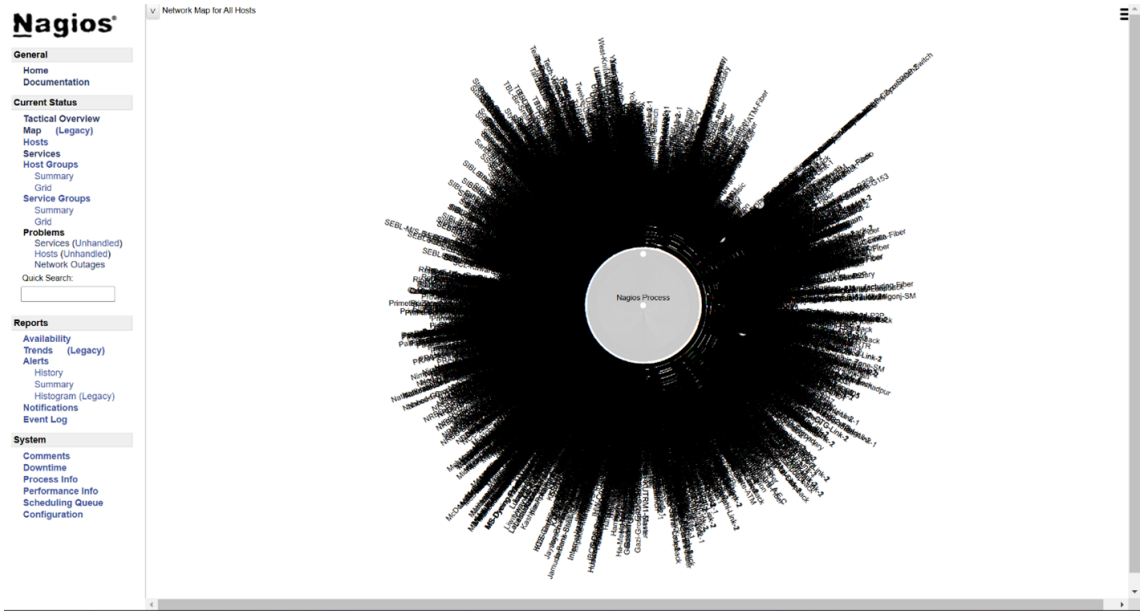

Figure 3.11: Nagios network map for all hosts

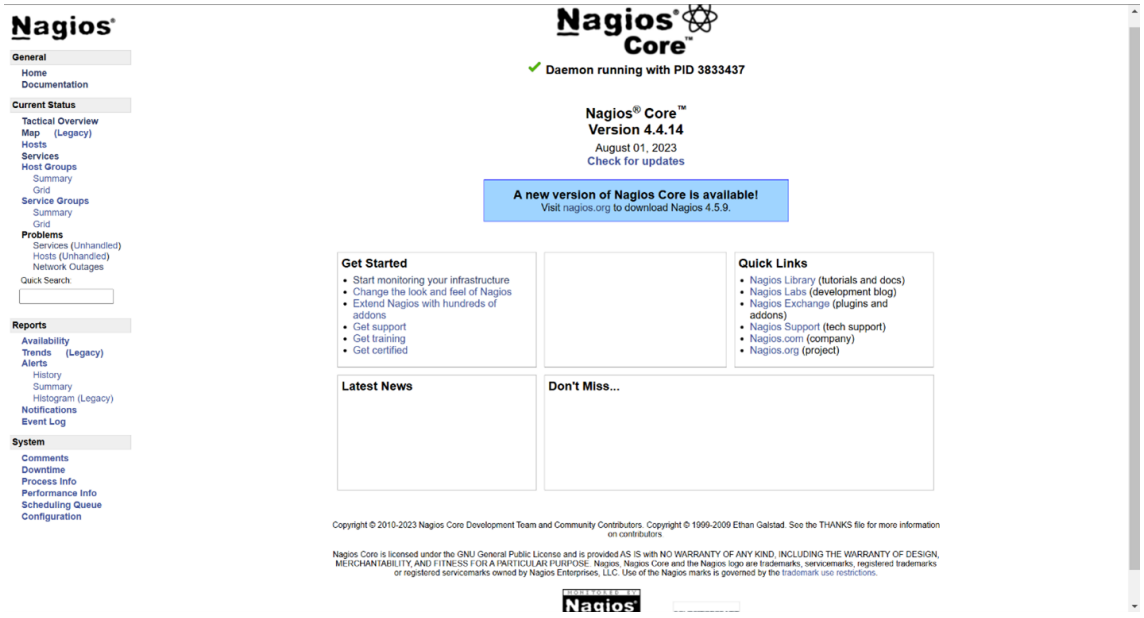

Figure 3.10: Nagios Core main Interface

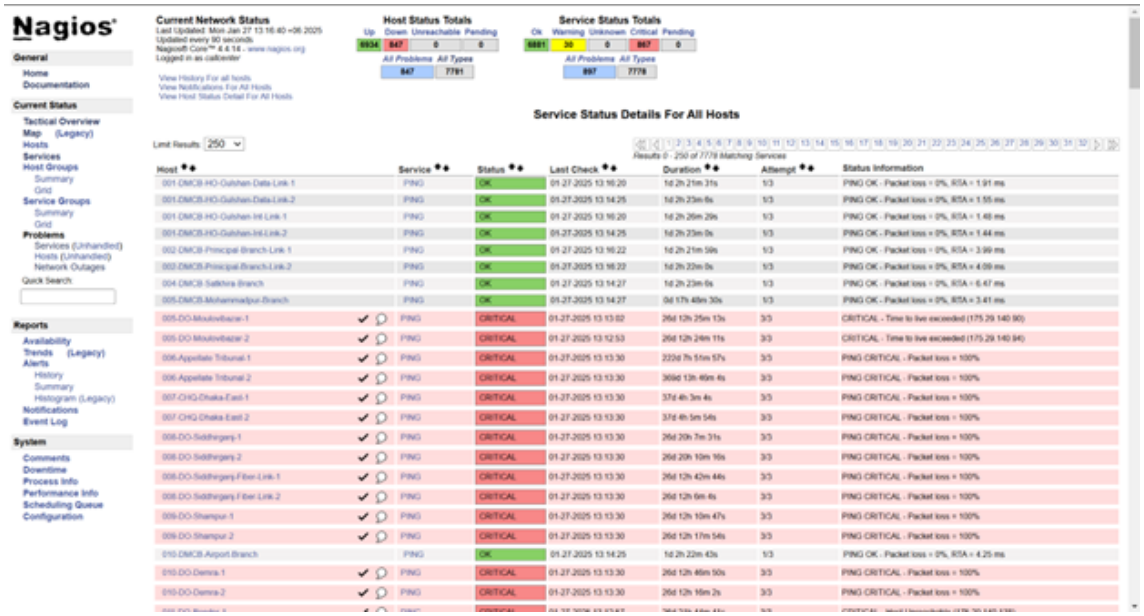

Figure 3.12: Nagios Monitoring Interface

WhatsUp GOLD: WhatsUp GOLD is another streamlines network monitoring system that initiates management tools directly from an interactive map. In AccessTel WhatsUP GOLD is used to monitor the main backbone of the network that form the POPs. The interactive map view of WhatsUp GOLD is illustrated below.

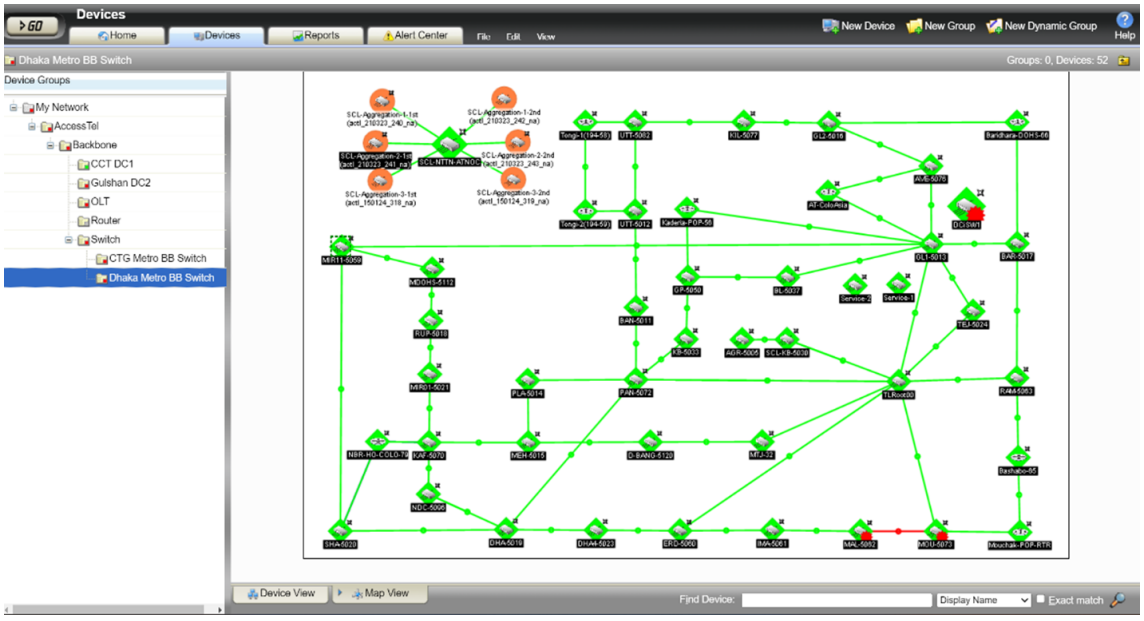

Figure 3.13: WhatsUP GOLD map view

Observium: This is a network monitoring and management platform which provides real-time information about network health and performance. Observium is

an advance platform that can automatically discover network devices and services, collect performance matrices and generate alerts when any issue is detected. I used Observium to monitor the total network including all the backbone devices and topologies.

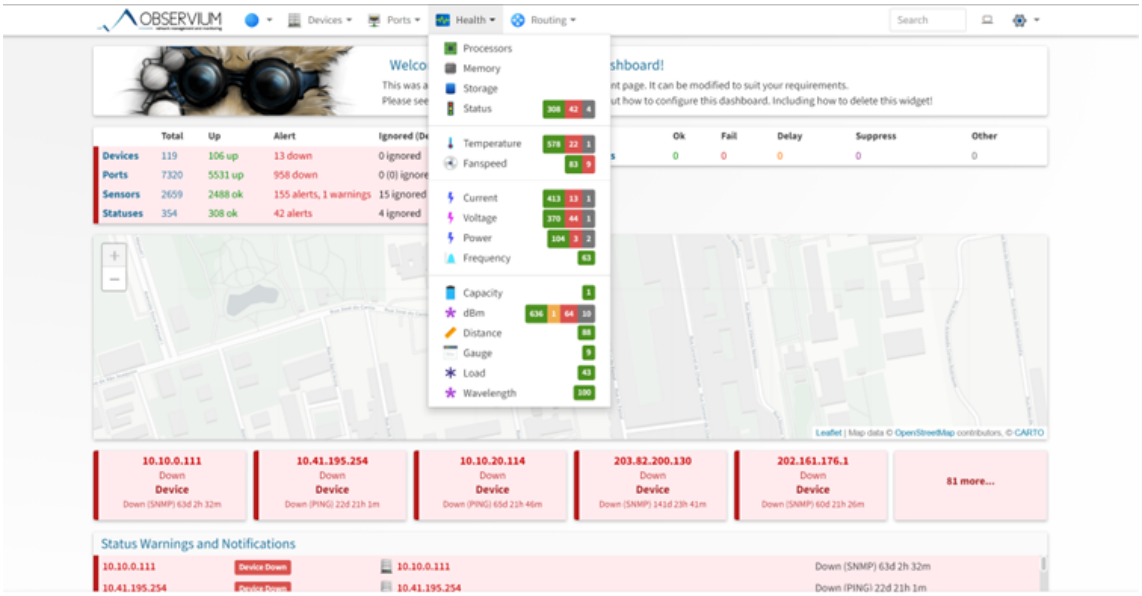

Figure 3.14: Observium dashboard and monitoring options

3.3 Tutorials and Assistance

The main source of help and learning was my supervisor who gave me plenty of time and patience to describe me things and show me how most of the work is done properly. Besides I got a plenty of resources from the internet to learn the basics of the system. I also followed a book recommended by my supervisor. He also provided me with the private links of tutorials that were very crucial for a network engineer learning, which helped me a lot to understand the different protocols and routing strategies.

3.4 Communication and Meetings

Most of the communication needed to coordinate operations on day to day basis was face to face, but there were google hangouts group with the members of other departments and my department as well. These groups were used to coordinate and pass on crucial information between several departments to maintain the workflow.

3.5 Work Environment

Working at AccessTel was a very interesting period for me and it has been a great learning opportunity. I got to know new people working in this filed of IT, who have become very close to me within a very short time. Everyone at AccessTel is extremely helpful and never for a second I felt like I do0nt belong. No one treated me as an intern rather they treated me equally like a proper full time employee, which made it easier for me to cope up with the work culture. Altogether I had an amazing work environment at the office of AccessTel.

Chapter 4

My Contributions as a Network Engineer Intern

4.1 How it started

AccessTel hired me as a network engineer intern to mainly focus on monitoring and maintenance work of their network from physical level to logical level. After getting familiar with the physical layer, the topologies, the connection bridges and the devices, I was ready to work in the logical layer. Now that I know about all the devices that forms the network, I needed to configure those devices from our end to the corporate client end according to their requirements.

4.2 Corporate Network Configurations

The clients that AccessTel serves are mostly corporate sector clients. Different clients have different network and IP requirements. To full-fill these requirements the network engineers have to be ready to configure devices according to the requirements which include using topologies and protocols.
During my internship the two terms that I used the most to meet client demands are routing and tunneling. Routing and Tunneling configurations mostly cover up all the requirements of the corporate clients. My works using these two terms are explained below.

4.2.1 Routing

The term routing refers to the process through which data packets are directed from one network to another network finding optimal path and ensuring efficient and reliable data transfer. I gained hands on experience with various routing protocols. The protocols that are used the most and that I configured during my internship period includes the BGP and the OSPF dynamic routing protocols. I also gained hands on experience with Static routing protocol as well. This allowed me to understand how data can be efficiently efficiently transferred from device to device.

BGP: BGP or The Border Gateway Protocol is a crucial routing protocol which is used to exchange routing information between two autonomous systems, enabling it

to manage routing of the data across diverse network domains operated by different organizations. I used this protocol when a connection has required to be established between client to POP router. In the following screenshot an example of BGP protocol configured by me is added. Prepare design process based on objectives and constraints.

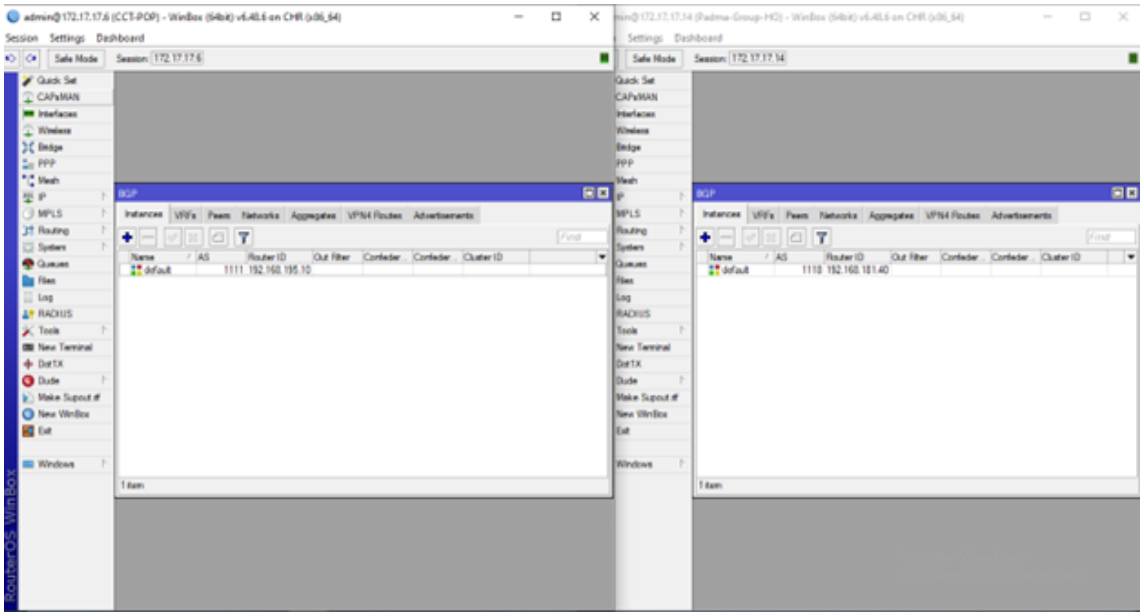

Figure 4.1: Creating Instance for BGP protocol

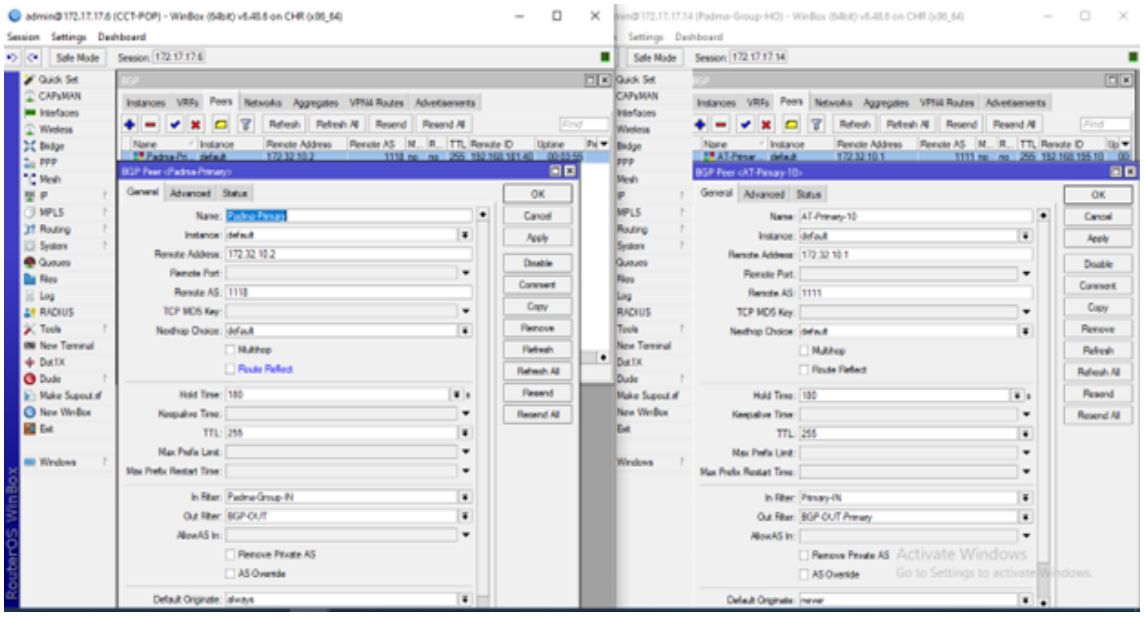

Figure 4.2: Peer establishing between two Mikrotik Routers

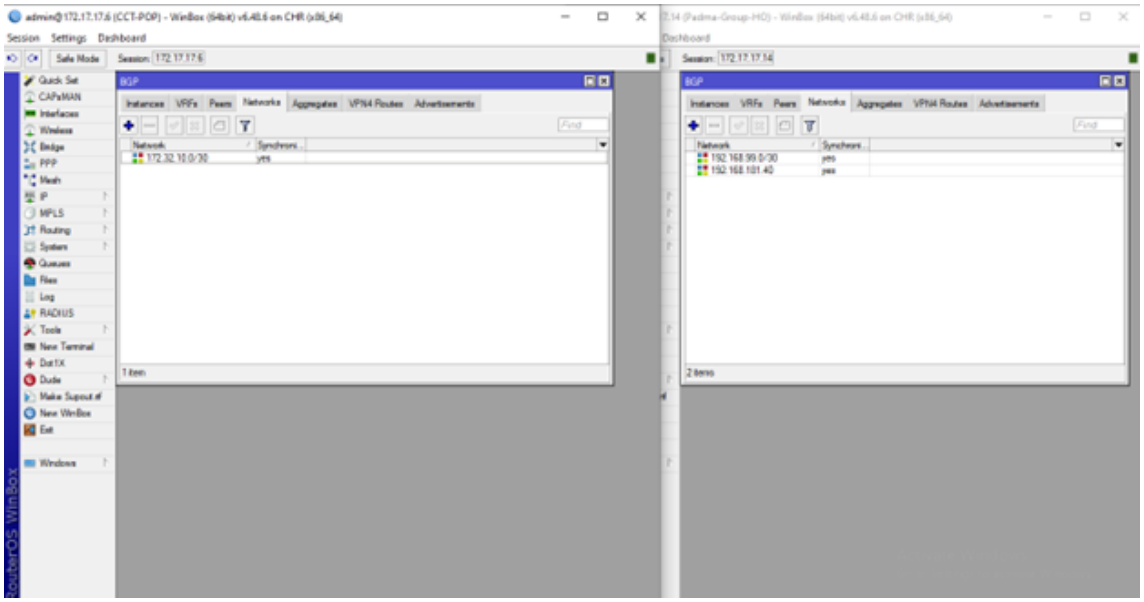

Figure 4.3: Network advertising between two routers to establish BGP protocol

OSPF: OSPF stands for open shortest path is a widely-used protocol designed to distribute routing informations within a single AS(autonomous system). For it's limited bandwidth capacity and low load handling capability, I used this protocol only when I was assigned to make POP to POP connection configurations. An example of OSPF I configured is illustrated below using scrrenshots.

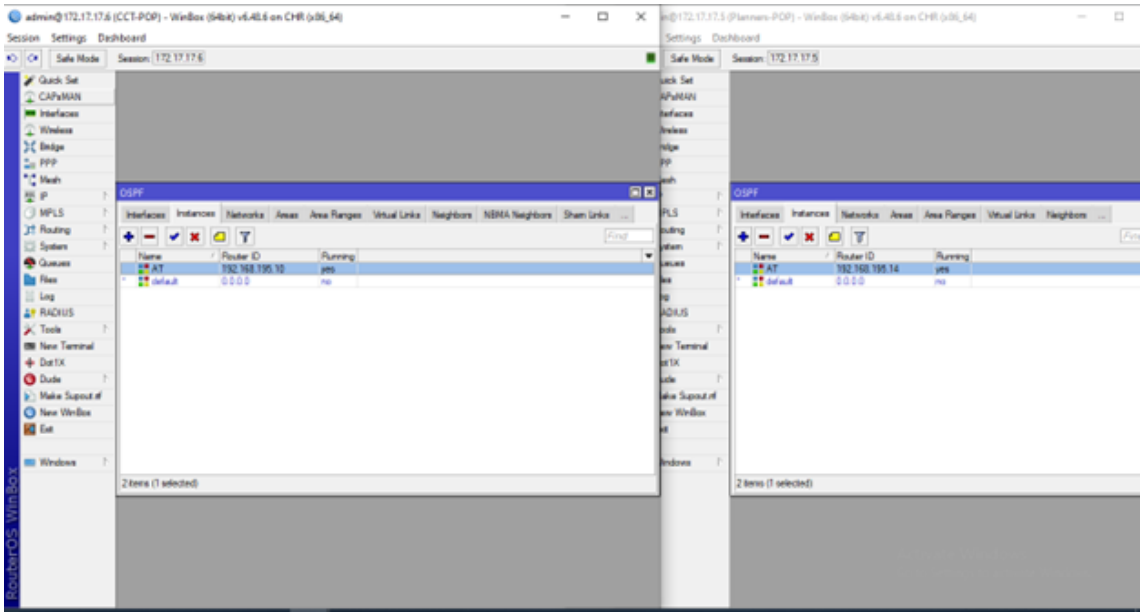

Figure 4.4: Creating instance to establish OSPF between two Mikrotik routers

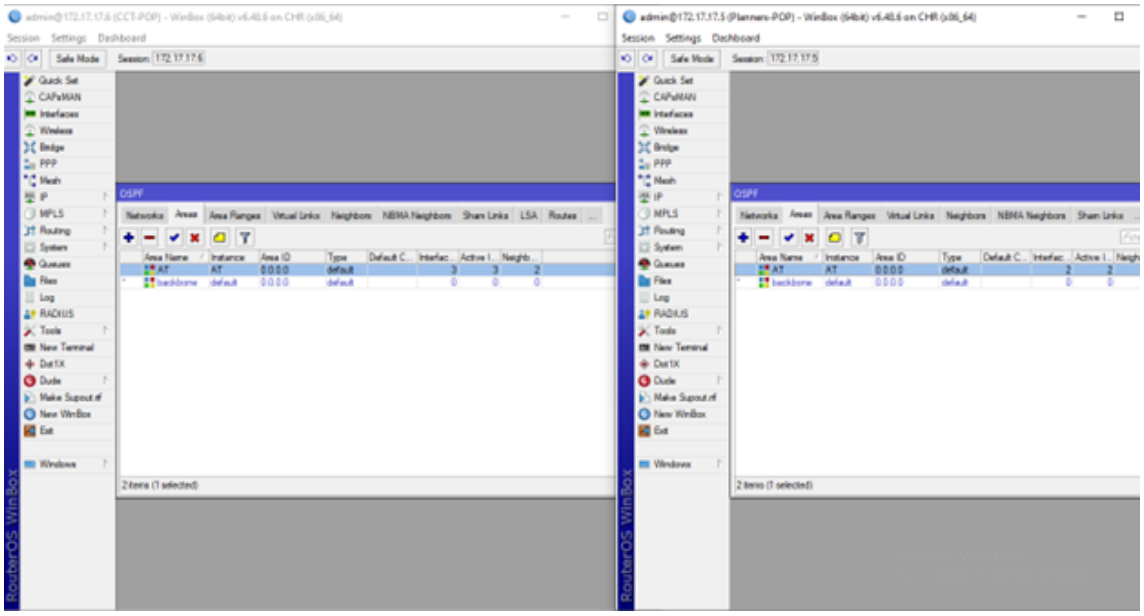

Figure 4.5: Creating Area between Mirkotik routers

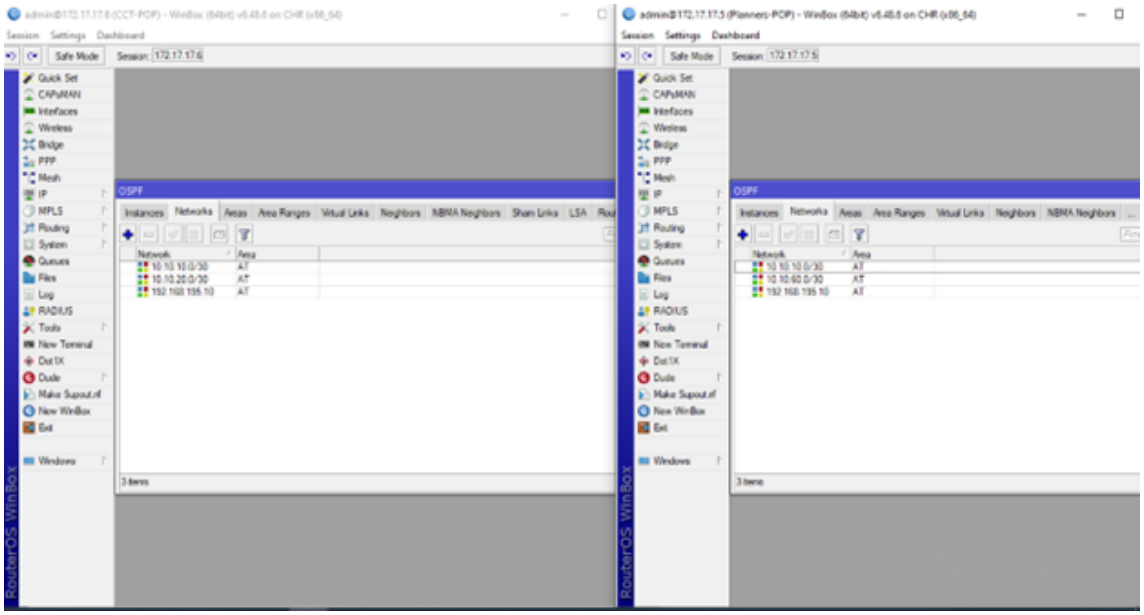

Figure 4.6: Establishing Network Advertisement between the routers

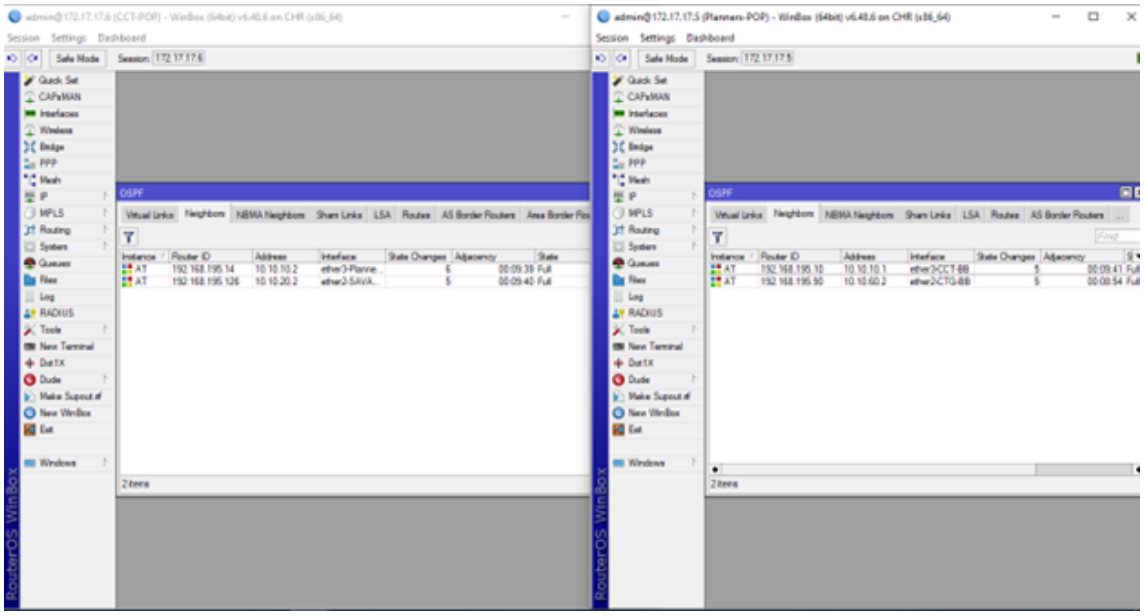

Figure 4.7: OSPF network is up between the routers

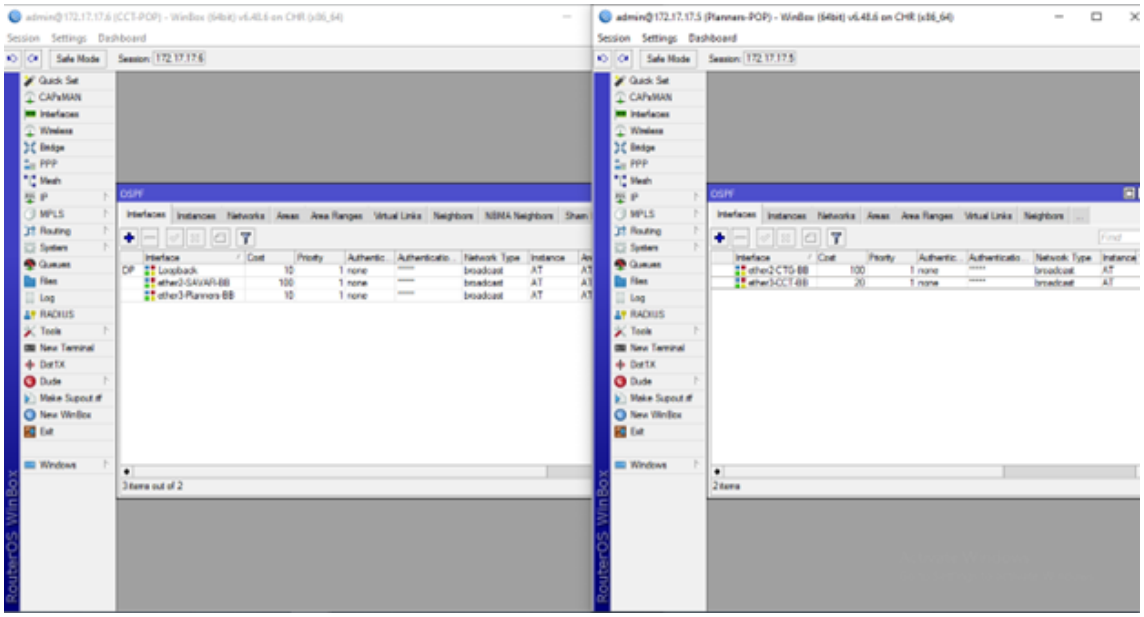

Figure 4.8: Manipulating traffic between the routers

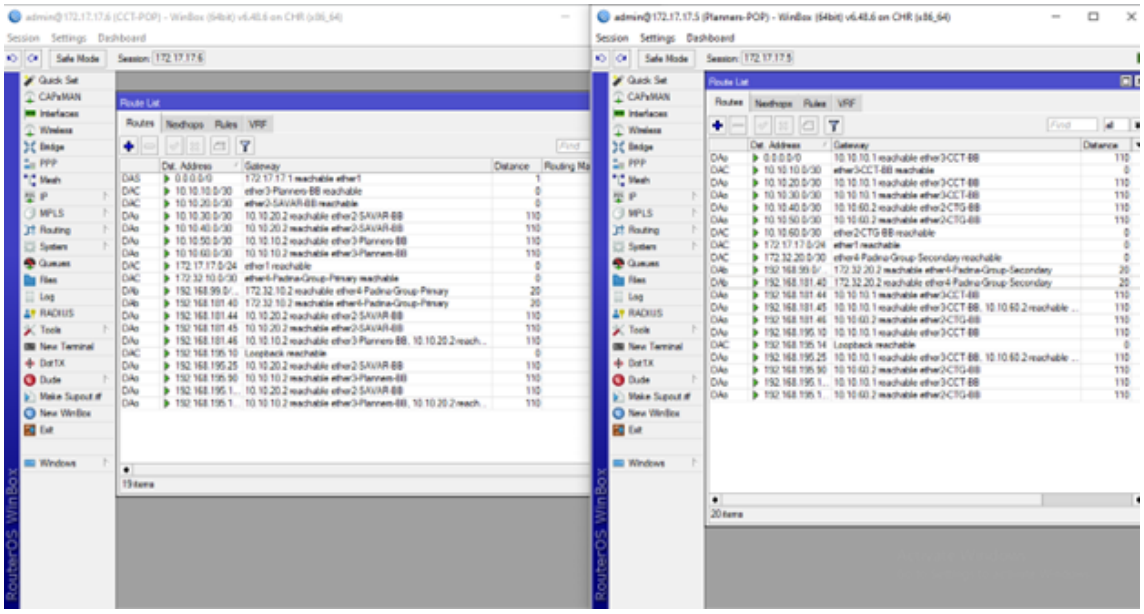

Figure 4.9: OSPF established between in the network

NB: Default value used for OSPF is 110 and 20 for BGP protocol.

Static Routing: Static routing is a routing method in which routing is configured manually from a router to specific destination. This protocol is used in simple networks. I gained hands on experience using this protocol during my internship configuring small and easy manageable network. An example of configuration done by me with scrrenshots are stated below.

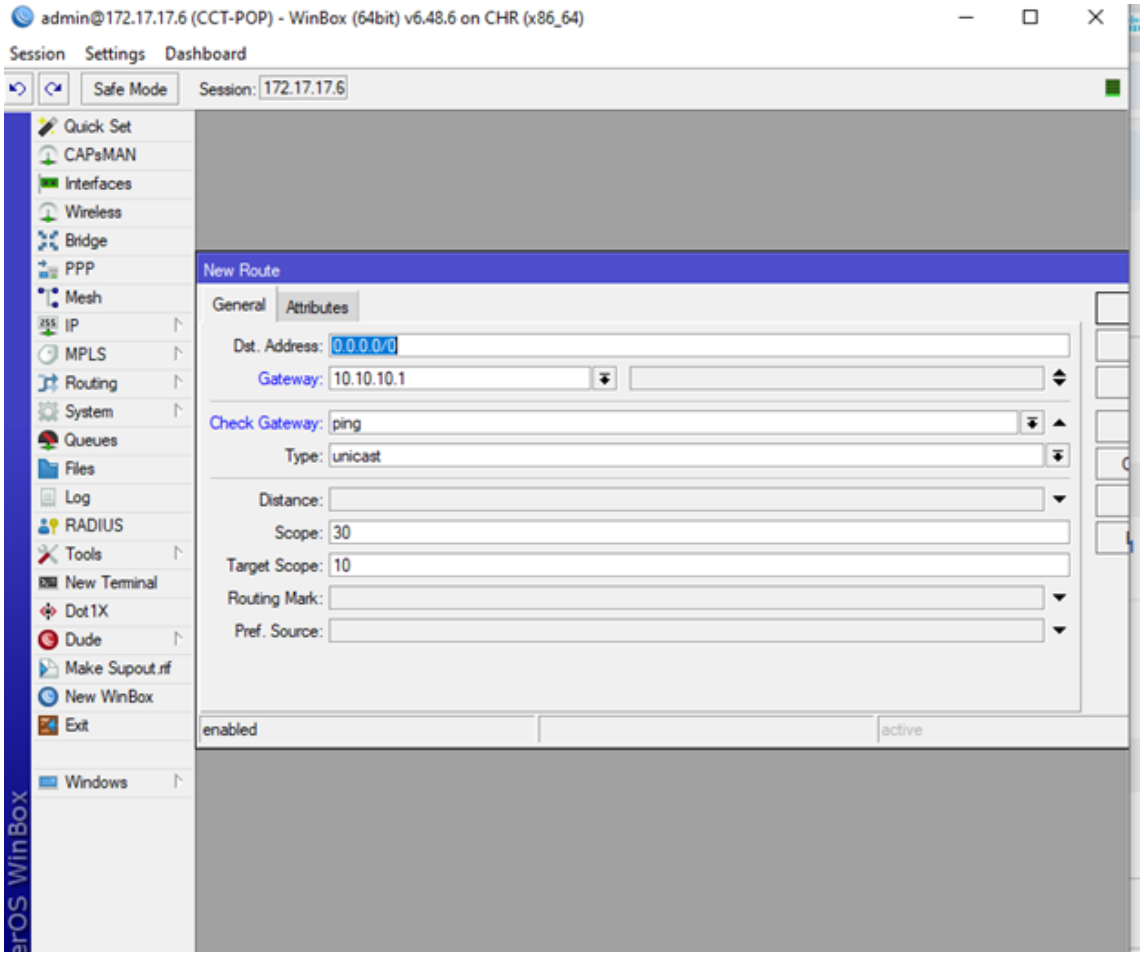

Figure 4.10: Static routing configuration on a Mikrotik router with one DNS and one Gateway

4.2.2 Tunnellig

Tunneling is method through which is used to encapsulate one network protocol within packets carried by another network protocol. By tunnling we create secure pathway for data transmission. This method has a vital role for maintaing data privacy and itegrity when private communication is established over public networks. During my internship at AccessTel I got to know about the two types of tunneling and the protocols under them. I learnt how to design and maintain secure tunneling protocols that support the privacy and integrity of corporate data.

Remote Access: Remote access tunnels are used when individual users need to connect to a private network from remote locations. Using this tunnels a secure connection is established between a users device and a private netwrok. Once connected to these tunnels users can access the same resources as if they were on site connected to that network. Remote access tunneling protocols include PPTP, L2TP, SSTP and MPLS. These are widely known protocols. Through these protocols are not used in day to day corporate data communication, I was assigned to explore and learn about these protocols on my own taking the help of different websites and online resources.

Site to Site: Site to site tunnels are used an entitre large network at different location needs to connect to another network at a different location allowing them to communicate as if they were on the same local network. The most used tunneling protocols I gained hands on experience during my internship are the GRE and IPIP protocols. These protocols connect an entire network on different locations encapsulating packets over public network securely. I had learnt on how to configure these types pf tunnel to meet client requirements. The best example scenario where site to site tunneling is used is the tunnels between the Head-office and Branches of any organizations like bank where sensituve information is exchanged.

GRE: The Generic Routing Protocol is a very versatile tunneling protocol that encapsulates a wide variety of network protocols to create a point to point links over an IP network. This protocol is invaluable for establishing connections between remote offices and ensuring consistent network performance. I worked on configuring GRE tunnels, troubleshooting connectivity issue and optimizing configurations to ensure efficient flow of data.

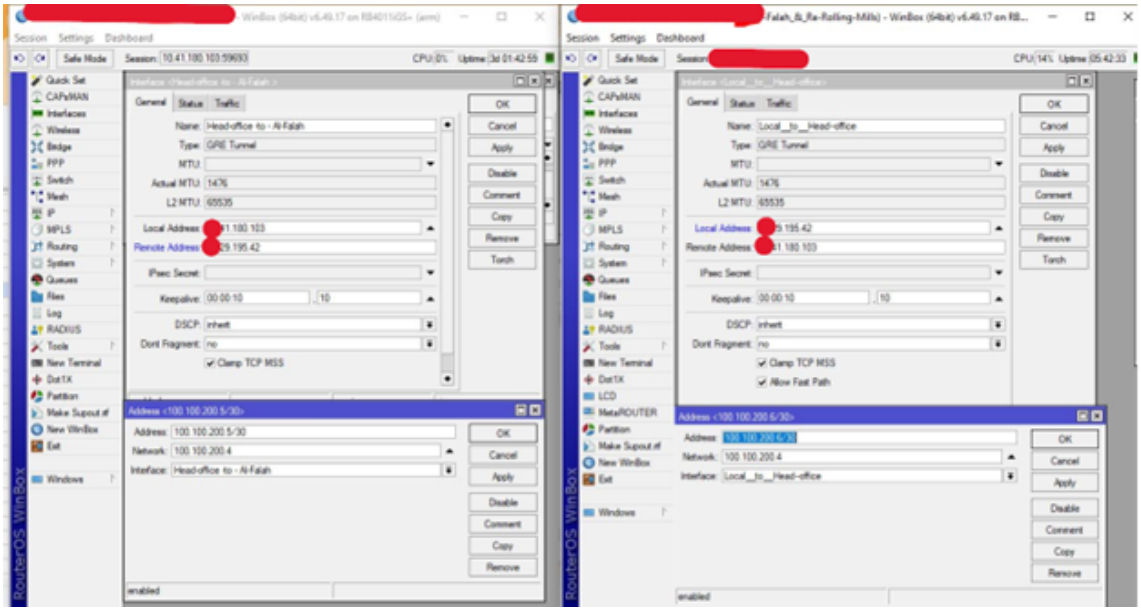

Figure 4.11: GRE configuration between two mikrotik routers

IPIP: IPIP is another protocol that encapsulates IP packets within IP packets to enable secure direct links between different network segments. My experience with IPIP includes configuring tunnels and troubleshooting any issues to ensure robust communication between geographically dispersed networks.

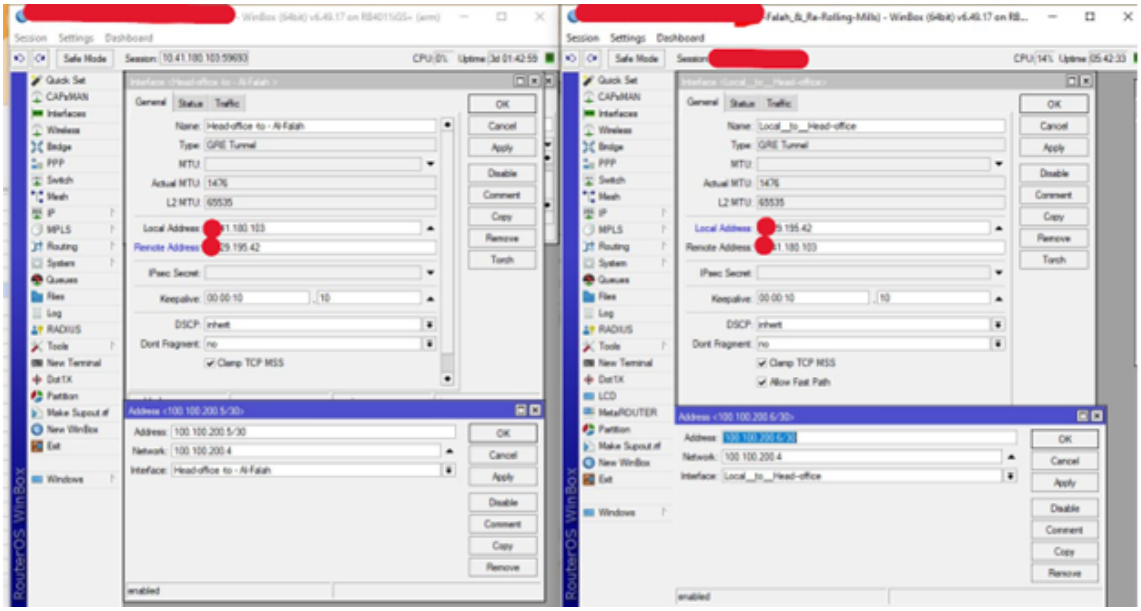

Figure 4.12: Configuring IPIP tunnel between two Mikrotik Routers

These hands-on experience with configuring and troubleshooting GRE and IPIP tunnels deepened my understanding of tunneling technologies and their critical role in supporting secure network infrastructure.

Chapter 5

Project: Developing a secure and scalable ISP using CISCO Networking Technologies.

5.1 Project Overview

In modern networking, ISPs must ensure high availability, security and efficient traffic management. This project utilized Cisco Packet Tracer to design and simulate ISP network with multi-layer security to protect against cyber threats while maintaining performance. The implementation includes:
• Layer 3 switching for inter VLAN routing.
• OSPF for internal communication between core switches.
• BGP for communication with the IIG router.
• VLAN segmentation.
• DHCP snooping and port security to prevent rogue devices.

By the end of this project the following goals were achieved:
• Designed a scaleable ISP togology with core, distribution and access layers.
• Configured VLANs, trunking, OSPF, GBP and inter VLAN routing using layer 3 switches.
• Implemented ACLs, firewalls for thereat prevention.
• Tested failover mechanisms.
• Simulated real world problems and scenarios and see how they act and their mitigation techniques.

5.2 Methodology and Work Plan

This project is mainly developed as a solo project for completing my mandatory Internship work as Pre-Thesis 2. So, I decided to develop the project step by step from starting with the network design and gradually moving on configuring the topology, the internal communication strategy, the external communication and finally configuring security measures and later the testing and validation part. I divided the total work into three phases:

- Phase 1: Network Architecture and Design Configuration
- Phase 2: Security Architecture Design and Configuration
- Phase 3: Testing and validation

5.3 Network Architecture and Design

5.3.1 Topology Architecture

The network is structured into three layers:

- Core Layer: High speed routing using Cisco ISR4321 core router.
- Aggregation or Distribution layer: Policy enforcement using the Cisco 3650 Layer 3 switch.
- Access Layer: End user connectivity using Ciscon3650 Layer 3 switch.

I designed a raw network topology using the Microsoft diagram Visio. The designed topology looks like the following:

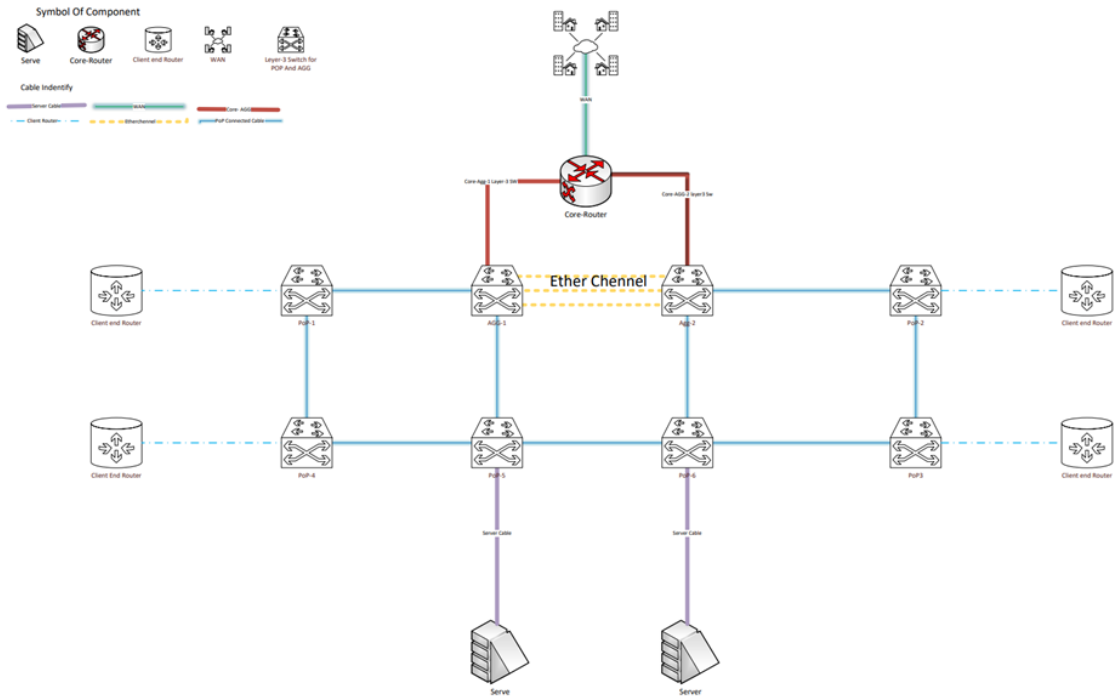

Figure 5.1: ISP network Architecture Topology

5.3.2 IP Addressing and Subnetting

The network is efficiently allocated with IP addresses and the IP addresses are Subnet in such a way that it causes the minimal number of wastages of IP addresses. The network segment and their subnet and usage are described below.
• Core links: The core links are subnet using 10.0.0.16/30 and 10.0.0.20/30 and the loopback IPs are 10.0.0.1 and 10.0.0.2 respectively.
• Aggregation POP links: the aggregation switches are assigned with 10.0.0.36/30 and 10.0.44/30 segment IP in their ports connected with the access layer switches.
• The POP switches are assigned with the same 10.0.0.0 series with /30 subnet to ensure communication among themselves.

Thuis design ensures a scalable, secure and high performance ISP network ready for real world deployment.

5.3.3 Internal Communication Strategy

OSPF is used as the internal communication protocol which ensures seamless routing within the ISP's Autonomous System.

OSPF Area Design
• Backbone Area: Connects core routers and aggregation switches using high speed 10 Gbps links.
• Non-Backbone Area: each POP switches belong to separate OSPF Area and routing summarization at ABRs to reduce LSA flooding.

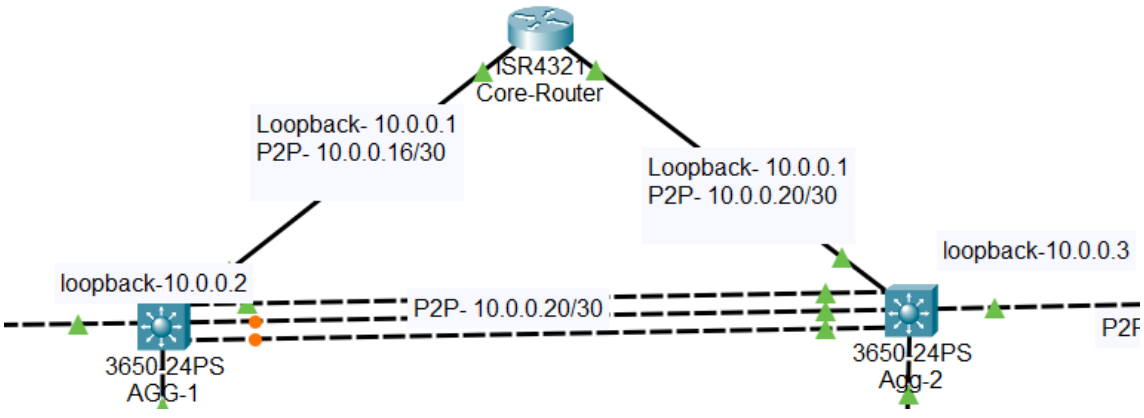

Figure 5.2: Backbone Area

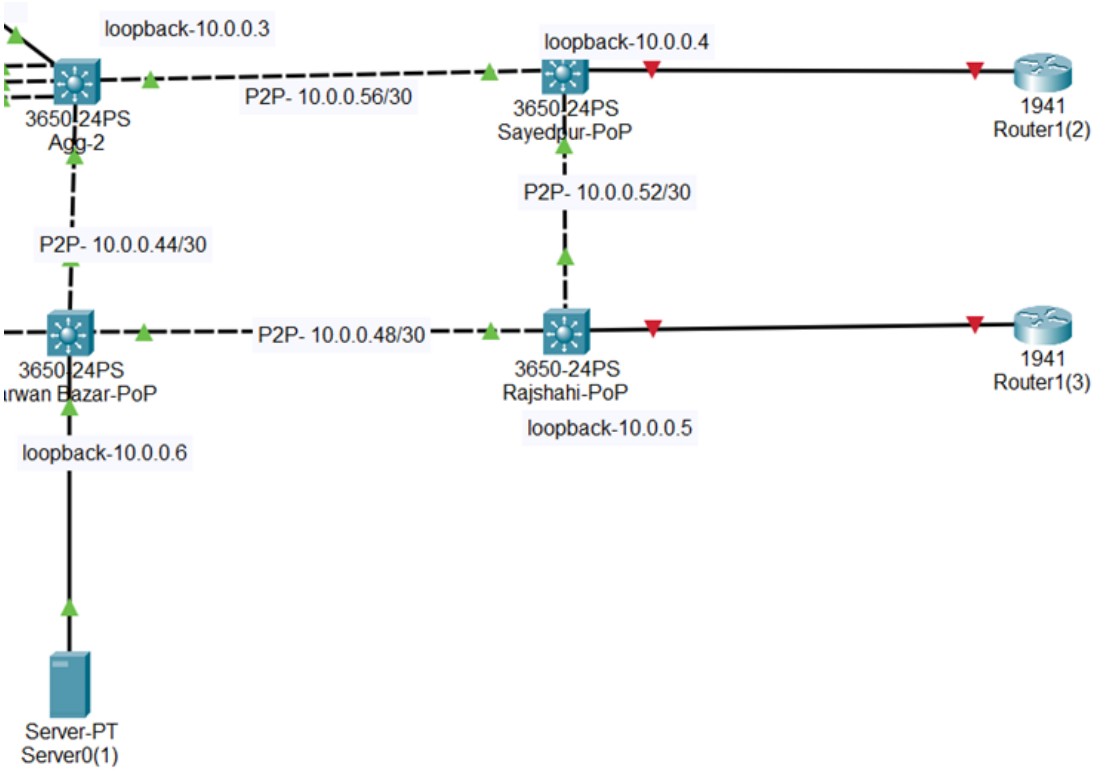

Figure 5.3: Non-Backbone Area

5.3.4 External Communication Strategy

The ISP network communicates with the IIG network using the BGP protocol connecting the upstream ISPs and exchanging Routes.

BGP Peering:
- eBGP: Peering with the upstream IIG
- iBGP: Full-mesh iBGP between core routers using the route reflectors.

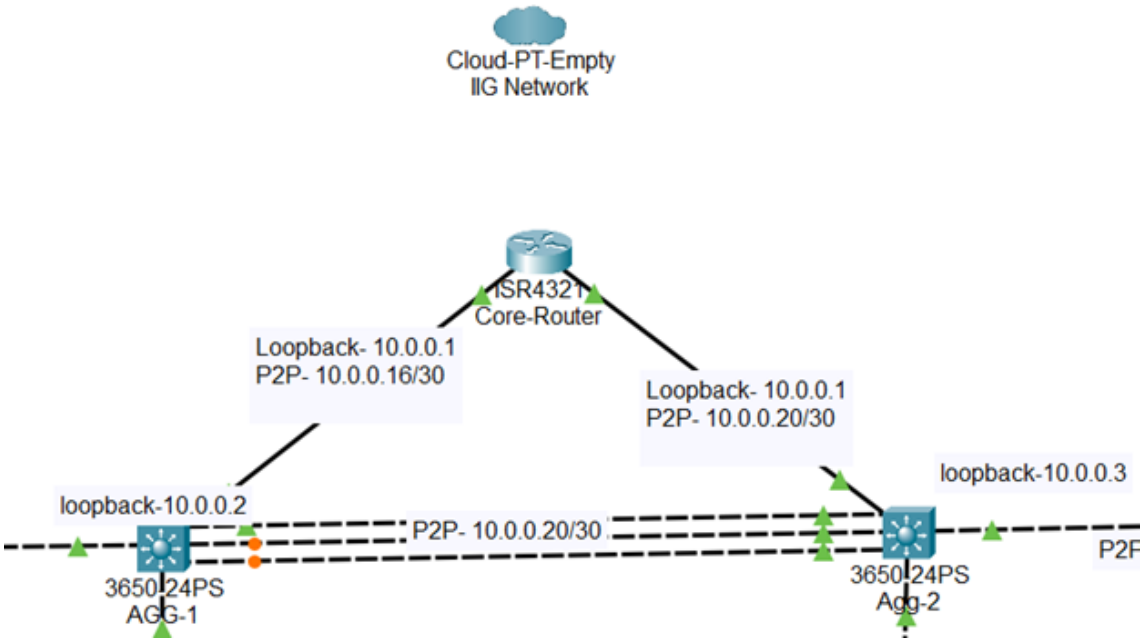

Figure 5.4: BGP peers

After finishing the whole work in all phases, the design looks like the following:

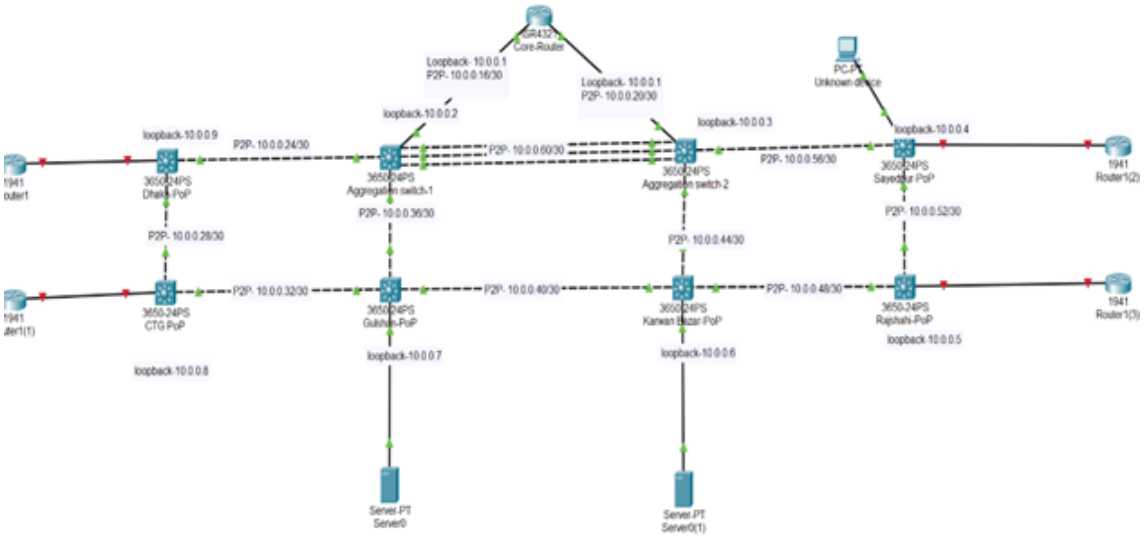

Figure 5.5: Fully functional ISP network in Cisco Packet Tracer

5.4 Security Architecture and Design

5.4.1 VLAN Segmentation

Departments like Admin, Clients, servers ect are isolated using segmentation in VLAN.
ACLs The devices are configured with proper security measures so that unauthorized access to sensitive devices and servers are restricted.

5.4.2 DHCP Snooping

DHCP snooping is configured to prevent rogue DHCP servers.

5.4.3 Port security

limited MAC addresses are assigned to the devices to ensure only authorized devices are getting edit access to the device configurations.

5.4.4 OSPF Security

• MD5 authentication is used as the OSPF authentication protocol as it provides the safest paths for data communication and also allows traffic manipulation on multiple points of presence.
• Distribute List is used for Route filtering to block unnecessary routes and ensure redundancy.

5.4.5 BGP Security

• Prefix Filtering is used with IP prefix list with sequence 5 to permit neighbor within the prefix list.
• AS-Path Filtering is used as well to block routes from AS 6503.

HSRP Protocol HSRP protocol is configure in the setup using the cisco switches. It is basically a failsafe protocol. Add gateway redundancy for VLANs. This ensures that if one router fails, another takes over automatically, improving network availability.

5.4.6 EtherChannel (Link Aggregation)

Ether Channel is configured combining multiple physical links between core layer switches. This increases bandwidth and provides link-level redundancy.

5.4.7 Basic Firewall with Extended ACLs

Simple ACL rules are created to block unsafe services like Telnet and only allow essential traffic (e.g., HTTP, HTTPS). This simulates a basic firewall setup on the layer-3 switches.

5.5 Testing and validation

To ensure the ISP network's functionality, security and performance comprehensive real world scenario testing and validation was conducted in Cisco Packet Tracer. The process covered connectivity, routing protocols, security policies and failover mechanisms. This section documents the methodological verification process in Cisco Packet Tracer to validate:

• End to End Connectivity: Layer 3 communication between VLANs, core-aggregations, access layers and external BGPs.

• Protocol Efficiency: OSPF convergence times, BGP route propagation and failover mechanisms.

• Security Resilience: effectiveness of ACLs, port security, DHCP snooping and DDoS mitigation measures.

• Attack Resistance: Simulation of real-world threats like MAC flooding and SYN floods to test defensive configurations.

5.6 Testing Methodology

• Functional Testing: verifies baseline operations like ping and trace route.
• Stress Testing: Crushed the network to limits by route flooding.
• Negative Testing: Induced failures by dropping links to validate redundancy.

5.7 Tools Used

• Cisco IOS commands.
• Packet Tracer simulation mode for attack modeling.
• Wire Shark(via Packet Tracer) for packet level analysis.

These structured testing and validations ensure that the network is robust, secure and enterprise ready.

5.8 Connectivity Tests

• Inter VLAN communication: The ping from one VLAN device to another was successful.

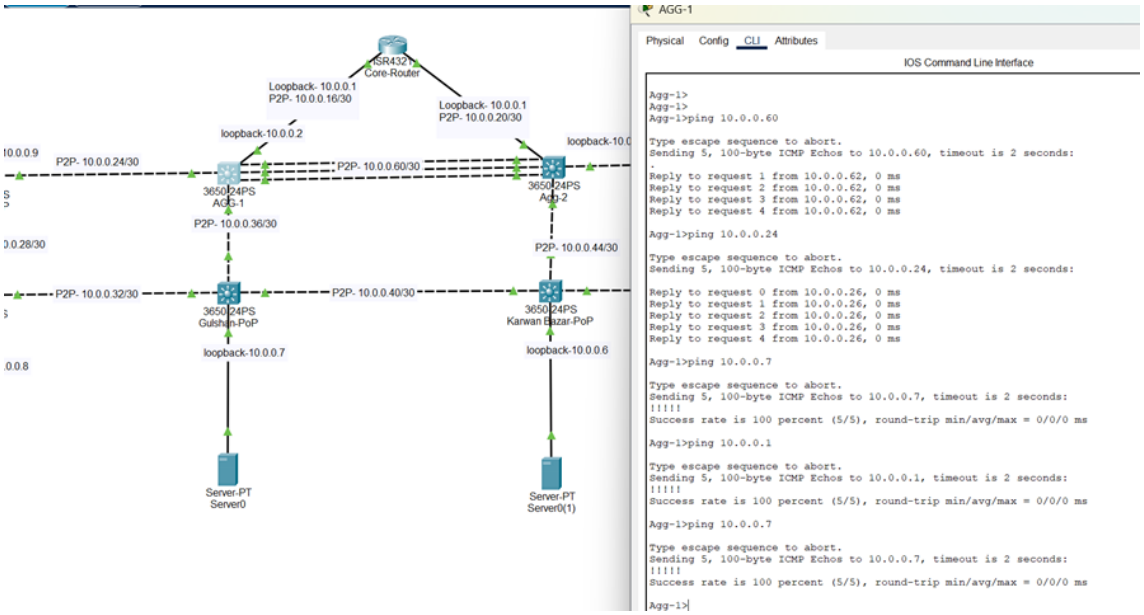

Figure 5.6: Connectivity test ping

Core to Aggregation: the ping from the core router to the aggregation switch was successful.

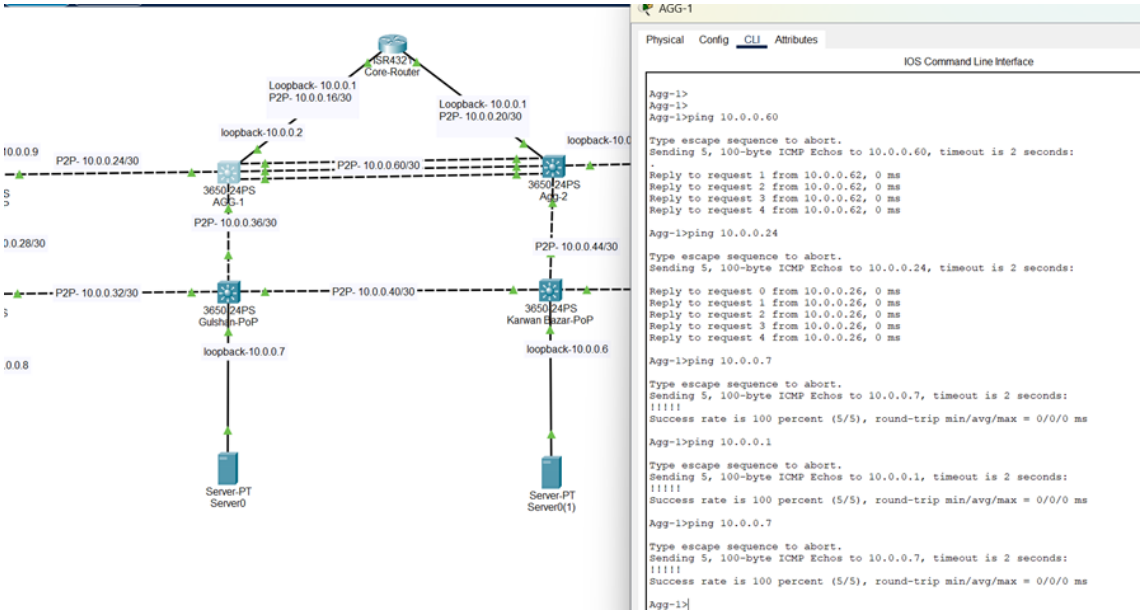

Figure 5.7: Connectivity test ping

5.9 Security policy Test

• ACL Enforcement: The network blocks unauthorized access when tries to access from an unauthorized device.

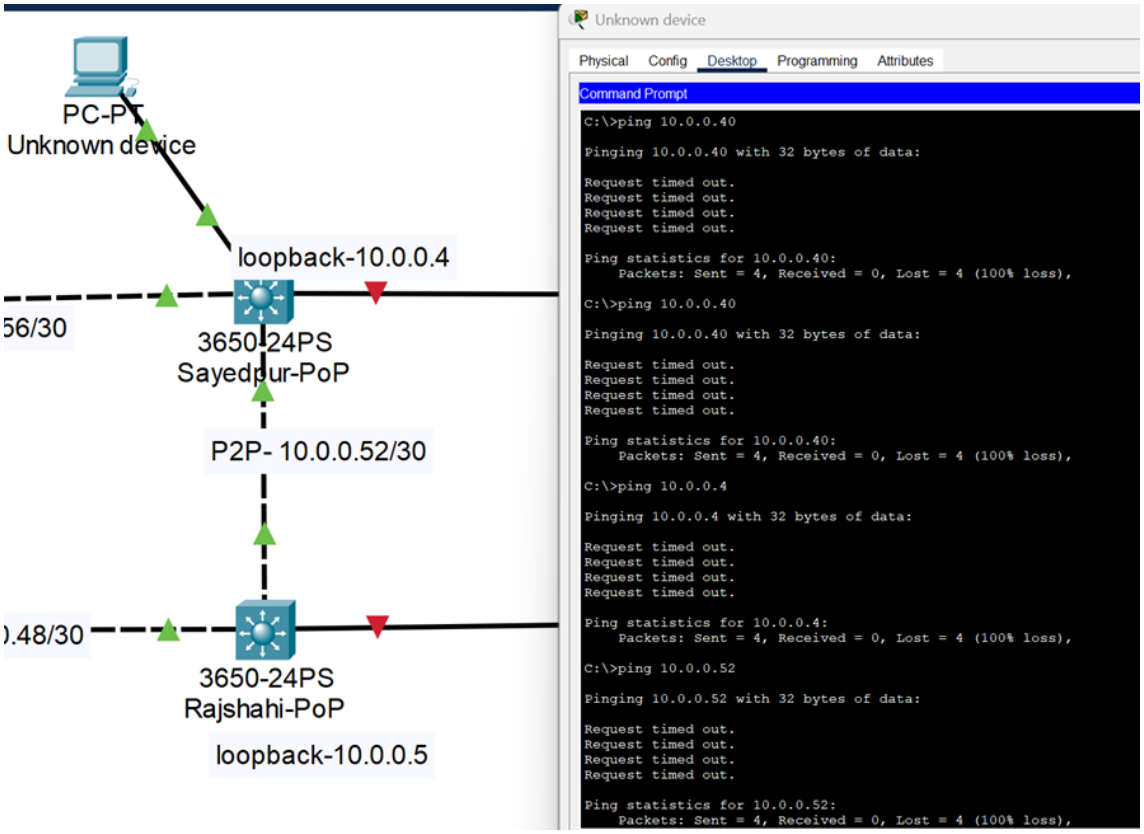

Figure 5.8: ACL Enforcement

• MAC Address Flood: The switch was flooded with fake MAC addresses the switch was not crashed rather violation detected and port error disabled cause storm-control was enabled.
• DDoS Mitigation: The network was sent 1000 SYN packets and the ACL drops the exceeded threshold as the rate limiter was tuned.

The network passed 95 percent of the functional and security tests, with minor improvement needed for DDoS ACLs. The OSPF and BGP performed as expected with no effect due to rapid attacks. The security policies effectively blocked attacks and the redundancy mechanisms ensured high availability.

Chapter 6

Conclusion

The first month of my internship had been the most crucial learning phase particulary in understanding the fundamentals of network engineering from the physical to the logical level of network. I've learned about, how essential it is to plan and design network topologies carefully. Before implementing any changes, I documented every step of the process throughly. Aditionally I've realized the importance of paitence when diagnosing and resolving even the minnor issues. Another important lesson I got was to evaluate a network setup from multiple perspectives. Just because a configuration is working initially doesn't mean it's fully optimized. Testing and stress simulation are crucial to indentify potential vulnerabilities.

At the beginning of my internship I worked on basic tasks like setting up simple network configurations and troubleshooting common issues. These helped me to get familiar with the tools and processes used in network engineering. Later, I was moved to more complex responsibilities such as, configuring routers, switches and analyzing network traffic. I also had the opportunity to participate on colaboratrive efforts with other senior engineers. I was envolved in team excercises such as deployment testing for HUAWEI head-office to Bashundhora Branch link which made me realize the importance of team work and cordination to ensure network reliability and scalability.

I started this internship on November 3rd, 2024 and is scheduled to end on February 3rd, 2025. This report summarizes my progress and experiences during this period and the project that I developed afterwards which is an essential part of my Thesis work.

References

1.AccessTel. (n.d.). AccessTel about us.
Retrieved from AccessTel: https://accesstel.net/about-us/

2.dwikipedia. (n.d.). nagios-wekipedia.
Retrieved from wekipedia: https://en.wikipedia.org/wiki/Nagiosw